Jürgen Ebner

4. 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

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 978-3-7475-0735-3
4. Auflage 2024

www.mitp.de

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

Lektorat: Janina Vervost
Sprachkorrektorat: Petra Heubach-Erdmann
Covergestaltung: Christian Kalkert
Bildnachweis: © Sergey Nivens / stock.adobe.com
Satz: III-satz, Kiel, 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 worden. 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 schwerer wiegt für viele die Tatsache, dass die meisten dieser Tools kostenlos erhältlich sind.

Abb. 1: Kali Linux Homepage

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.

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.

Vorsicht

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

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.

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

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 empfehlen, 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:

- **Einzelner Benutzer, Root-Zugriff per Design:** Die Art von Security-Audits verlangt es, dass Kali Linux zur Benutzung auf ein »Einzelner Root-Benutzer«-Szenario ausgelegt ist.
- **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

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.

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.

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.

Mit dem Release 2020.1 wurde eine wesentliche Änderung beim User durchgeführt: Der root-User ist nicht mehr Standard. Das bedeutet, um root-Rechte zu erhalten, muss man zusätzlich vor dem Befehl sudo eingeben. Es gibt auch die Möglichkeit, den Root Terminal Emulator zu verwenden, dadurch ersparen Sie sich die Eingabe von sudo vor dem Befehl.

Beim letzten Release im Jahr 2020 (2020.4) wurde die bash durch zsh[2] als Standard-Shell abgelöst. Der Vorteil von zsh als Shell ist, dass diese viele Verbesserungen und Eigenschaften von bash, ksh und tcsh vereint.

Bei den Releases 2021 wurden vor allem neue Tools in das Repository aufgenommen. Mit 2021.2 wurde darüber hinaus auch die NetHunter-Unterstützung für Android 11 veröffentlicht. Bei der Version 2021.3 wurde die VM-Funktionen verbessert und NetHunter ist nun auch für Smartwatches verfügbar.

Das Jahr 2022 brachte kaum Neuerungen, da sich das Entwickler-Team Verbesserungen widmete. Neben einigen neuen Tools, wie z.B. dnsrecon, scapy und einigen weiteren, wurde vor allem an der Verbesserung der bestehenden Tools und

2 zsh (Z shell) ist eine Unix-Shell, die sowohl als interaktive Login-Shell als auch Kommandozeileninterpreter für Shellskripte verwendet werden kann. Die Z shell wird neben Kali Linux seit MacOS Catalina derzeit auch von Apple verwendet.

Anwendungen gearbeitet. Es wurde damit begonnen, eine Testumgebung in Kali Linux zu integrieren, die im Release 2022.3 veröffentlicht wurde. Mit dem Release 2022.4 ist auch Kali Linux im Microsoft Azure Store verfügbar.

2023 wurde Kali Linux zehn Jahre alt und dies wurde mit einer neuen Kali-Version zur Verteidigung gefeiert – Kali Purple. Im ersten Release des Jahres erfolgte ein Update der Desktop-Version auf Xfce 4.18 und Plasma 5.27. Beim Release 2023.2 ist auch ein Hyper-V VM Image auf der Homepage erhältlich. Im August wurde schließlich noch das Release 2023.3 veröffentlicht. Mit diesem Release begann die Umstellung auf Debian 12, die bei der Veröffentlichung noch nicht vollständig abgeschlossen war. Es ist geplant, diese bis Jahresende vollständig umgesetzt zu haben. In diesem Release wurde auch der Kali Autopilot, ein Framework für automatisierte Angriffe, veröffentlicht. Dieses Tool dient dazu, die Defensive zu testen.

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[3] für jeden kostenlos zum Download angeboten.

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

1.3.1 Varianten von Kali Linux

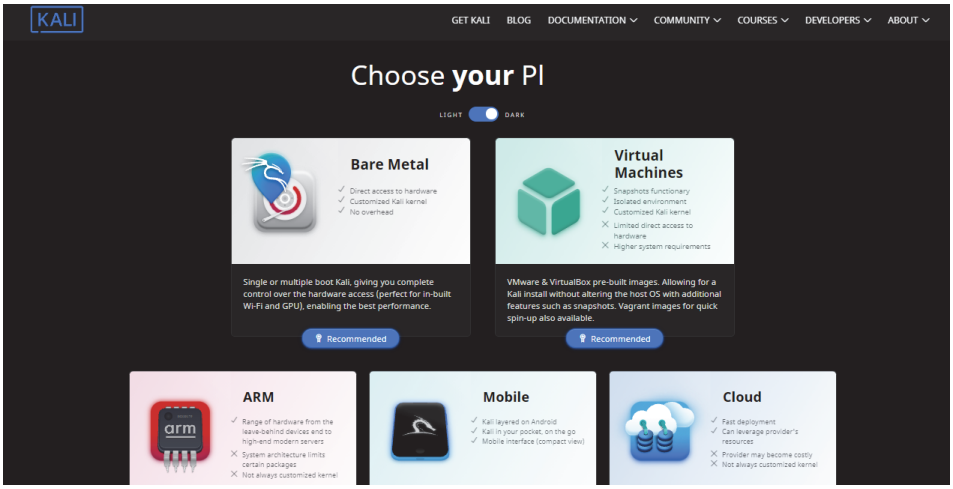

Abb. 1.1: Download von Kali Linux für verschiedene Plattformen

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

Installer Images

Hier kann man das aktuellste Image von Kali Linux herunterladen. Alle Images gibt es in der 64-bit-, 32-bit- und der Apple-M1-Version. Es handelt sich jedoch um ein reines Installationsabbild, das nicht als Live-Boot verwendet werden kann.

Sie haben die Wahl zwischen drei verschiedenen Optionen für das Image:

- **Installer:** Dabei handelt es sich um eine vollständige Offline-Installation. Das Image enthält die Meta-Pakete »Top10«, »Standard« und »Large«, damit eine vollständige Offline-Installation durchgeführt werden kann, ohne dass eine Internetverbindung notwendig ist.
- **NetInstaller:** kann verwendet werden, wenn Sie bei jeder Installation von Kali Linux das neueste Paket verwenden möchten, oder das Standard-Installations-Image zu groß zum Herunterladen ist. Das Image ist sehr klein, denn es enthält keine lokale Kopie der zu installierenden Meta-Pakete. Diese werden im Zuge der Installation heruntergeladen, deshalb ist in diesem Fall unbedingt eine Netzwerkverbindung notwendig.
- **Weekly:** Mit diesem ISO erhalten Sie ungetestete Images mit den aktuellsten Updates.
- **Everything:** Es ist eine Sonderversion des Installer-Images, das sämtliche verfügbaren Pakete und Meta-Pakete enthält.

Virtuelle Images

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

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

Zusätzlich gibt es mit Vagrant noch ein Tool zum Erstellen und Verwalten von Umgebungen mit virtuellen Maschinen. Mit einer einzelnen Konfigurations-Datei können eine Basis-»Box« und zusätzliche Konfigurationen erstellt werden wie z.B. das Hinzufügen einer zusätzlichen Netzwerkschnittstelle, das Festlegen der Anzahl der CPU-Kerne und des Arbeitsspeichers.

ARM

Diese Version ist für ARM-basierte Geräte angedacht. Wobei es hier eher ratsam ist, auf die speziellen Distributionen zurückzugreifen. Hier finden Sie Versionen für:

- Raspberry PI
- Pine64
- WithSecure
- Gateworks

Mobile

Die NetHunter-Variante ist eine Version von Kali für mobile Endgeräte. Aufgrund der unterschiedlichen Chipsätze und diversen Einschränkungen mobiler Systeme wird derzeit offiziell nur eine Auswahl der Geräte folgender Hersteller unterstützt:

- OnePlus
- Xiaomi
- Nexus
- Samsung
- Gemini
- LG
- Nokia
- Sony Xperia

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 derzeit im Amazon AWS Marketplace[4], bei Digital Ocean[5], Linode[6] und Microsoft Azure[7] erhältlich.

4 https://aws.amazon.com/marketplace/pp/B01M26MMTT
5 https://www.digitalocean.com
6 https://www.linode.com/marketplace/apps/kali-linux/kali-linux
7 https://azuremarketplace.microsoft.com/en/marketplace/apps/kali-linux.kali

Egal, für welche Version Sie sich entscheiden – wenn bei der Installation etwas schiefgeht, werden in der offiziellen Dokumentation[8] so ziemlich alle Fälle abgedeckt und Sie finden dort auch viele weitere Details bei Fragen und Problemen.

Container

Mit Container-Technologien wie Docker und LXC/LXD wird es Ihnen ermöglicht, mit den Kali-Containern über Ihr Host-Betriebssystem auf das Kali-Toolset zuzugreifen, ohne den Aufwand, ein zusätzliches vollständiges Betriebssystem ausführen zu müssen. Der Nachteil dabei ist, dass damit Einschränkungen verbunden sind, da kein direkter Hardwarezugriff möglich ist. Der Umgang mit eingehenden Verbindungen zu Tools, die im Kali-Container ausgeführt werden, kann deshalb kompliziert sein.

Live-Boot

Mit dem Live-Image von Kali Linux auf einem Speichermedium (USB, DVD, PXE) haben Sie Zugriff auf eine vollständige Bare-Metal-Kali-Installation, ohne das Betriebssystem installieren zu müssen. Dadurch haben Sie einen schnellen und einfachen Zugriff auf das Kali-Toolset mit allen Vorteilen einer Bare-Metal-Installation.

WSL (Windows Subsystem for Linux)

Seit 2018 gibt es mit WSL auch eine Möglichkeit, Kali Linux direkt aus Windows 10 heraus zu nutzen. Das setzt aber voraus, dass WSL aktiviert ist. Bei WSL handelt es sich um ein Softwarepaket, mit dem Sie Linux neben Ihrem Windows-System in einem optimierten Container ausführen können. Das Kali-WSL-Paket ermöglicht einen einfachen Zugriff auf das Kali-Toolset. Dies hat die gleichen Nachteile wie bei einer Standard-VM, verursacht jedoch weniger Overhead und ermöglicht eine engere Integration mit Ihrem Windows-System. Das Softwarepaket kann über den Microsoft Store installiert werden.

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.

8 https://docs.kali.org

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.

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[9] 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.
- **ARM-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.

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

- **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.
- **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.

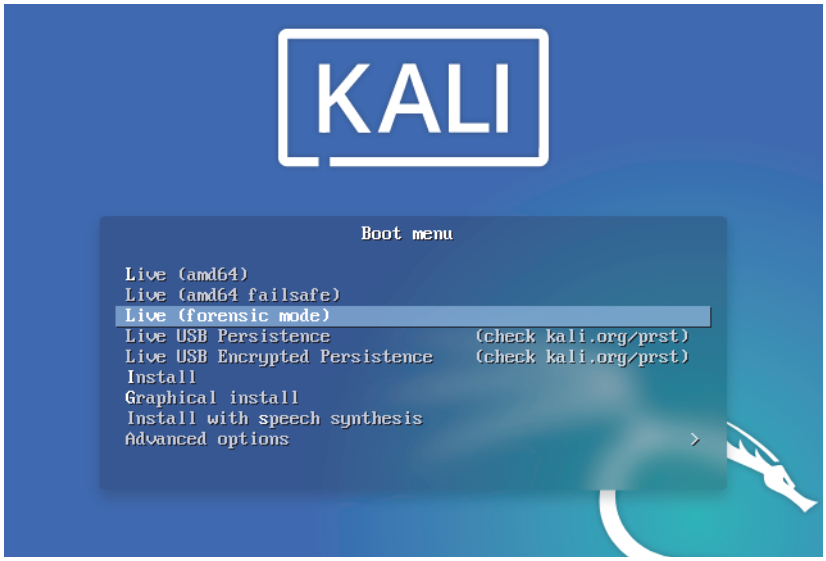

Abb. 1.2: Startmenü – Auswahl des Forensik-Modus

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[10], wird diese nicht genutzt. Interne Festplatten werden niemals automatisch gestartet.

10 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.

- Wechselmedien werden ebenfalls nicht automatisch gemountet. Das heißt, USB-Sticks, CDs und Ähnliches werden beim Einlegen nicht automatisch geladen.

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[11] 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.
```

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