IN DIESEM KAPITEL

Entwicklung und Geschichte von Kali Linux

Überblick über die verschiedenen Einsatzzwecke

Kapitel 1
Die Grundlagen zu Kali Linux erfahren

COPYRIGHTED MATERIAL

Die meisten Personen, die in der IT-Sicherheit Fuß gefasst haben, werden zwangsläufig von *Kali Linux* gehört haben. Bis 2013 unter dem Namen *BackTrack Linux* bekannt, handelt es sich generell um eine populäre freie Linux-Distribution, die sich hauptsächlich an IT-Sicherheitsspezialisten richtet. Sie basiert auf Debian Linux und beinhaltet mehr als 600 vorinstallierte Programme, aufgeteilt in 13 Kategorien. Diese unterstützen die Nutzer beim Durchführen von spezifischen IT-Sicherheitstätigkeiten.

Dieses Kapitel ermöglicht Ihnen einen effizienten Einstieg in das Thema der Einrichtung eines Kali-Linux-Systems. Dazu werden die notwendigen Installations- sowie Einrichtungsschritte kurz beschrieben, damit auch Linux-Novizen möglichst schnell mit den im Buch beschrieben Hacking-Tools durchstarten können. Sollten Sie bereits mit der Installation oder der Benutzerführung vertraut sein, können Sie die entsprechenden Kapitel getrost überspringen. Ein Blick in Kapitel 3, »Erste Schritte«, kann jedoch nicht schaden, um den Einstieg zu erleichtern.

Zudem erfahren Sie, wie Sie das verwundbare Testsystem *Metasploitable 2* installieren, um die in diesem Buch erlernten Angriffstechniken auch praktisch anwenden zu können.

Das Kali-Linux-Projekt wird derzeit aktiv von der US-amerikanischen Firma *OffSec* (ehemals *Offensive Security*) gesponsort und weiterentwickelt, die von den Hauptentwicklern gegründet wurde.

Die Einsatzzwecke von Kali Linux verstehen

Kali Linux wird primär als Basis-System für das Durchführen von sogenannten Penetrationstests eingesetzt.

Penetrationstest

Bei einem Penetrationstest (häufig auch als Pentest bezeichnet) handelt es sich um eine erlaubte Untersuchung von Schwachstellen in IT-Systemen. Der Tester schlüpft hierbei in die Rolle eines Angreifers. Er versucht anschließend, etwa unter Zuhilfenahme der Hacking-Tools in Kali Linux, möglichst viele Schwachstellen aufzudecken. Die Firma ist im Anschluss in der Lage, die gefundenen Sicherheitslücken zu schließen, sodass diese nicht mehr ausgenutzt werden können.

Weitere Informationen zu dem Konzept eines Penetrationstests finden Sie in einer Studie des Bundesamtes für Sicherheit in der Informationstechnologie: `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Penetrationstest/penetrationstest.pdf`

Das System wird außerdem mit vorinstallierten Tools zum Durchführen von *Reverse Engineering* und *digitaler Forensik* ausgeliefert. Während Ersteres den Umfang des Buches sprengen würde, erhalten Sie ab Teil VII einen Einblick in forensische Vorgehensweisen.

Verschiedene Varianten von Kali Linux kennenlernen

Beim Besuch der Download-Seite (`https://www.kali.org/get-kali/`) fällt Ihnen sicher auf, dass Sie Kali Linux in verschiedenen Varianten herunterladen können. Diese richten sich hauptsächlich nach der gewünschten PC-Architektur, Installationsform und Anzahl der beinhalteten Programme und Tools. Während Sie in diesem Kapitel die Unterschiede noch genauer erläutert bekommen, erfahren Sie im nächsten Kapitel, wie Sie Kali Linux als virtuelle Maschine installieren und einsetzen.

Die folgenden verschiedenen Versionen von Kali Linux stehen Ihnen zum Download zur Verfügung. Wie Sie ebenfalls in Abbildung 1.1 sehen, sind »Installer Images« und »Virtual Machines« die empfohlenen Installationsvarianten.

- ✔ **Installer Images** Diese Abbilder erlauben eine direkte Installation von Kali Linux auf einem PC-System mit direktem Hardware-Zugriff- wozu auch gerne der Begriff »Bare-Metal-Installation« genutzt wird. Dadurch sind eine hohe Performance und eine einfache Einbindung von Hacking-Hardware gewährleistet.
- ✔ **Virtual Machines** Hierbei handelt es sich um Abbilder, die eine vorgefertigte Installation des Betriebssystems für virtualisierte Umgebungen bereithalten. Unterstützte Virtualisierungsprogramme sind beispielsweise der VMware Player (`https://www.vmware.com/de/products/workstation-player/workstation-player-evaluation.html`) oder Oracle VirtualBox (`https://www.virtualbox.org/`).

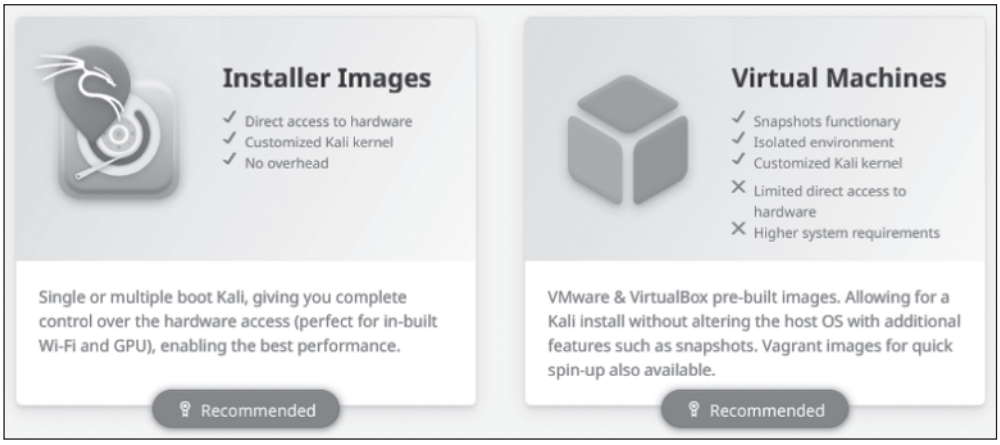

Abbildung 1.1: Empfohlene Image-Downloads auf der Webseite von Kali Linux

- ✔ **ARM** Sollten Sie Kali Linux auf einem System mit ARM-Prozessor ausführen wollen, ist dies das korrekte Abbild. Zu den unterstützten Geräten gehören etwa Single-Board-Computer wie ein Raspberry Pi.
- ✔ **Mobile/NetHunter** Das speziell für Android entwickelte *Kali Linux NetHunter* ermöglicht die mobile Nutzung des Betriebssystems für unterstützte Smartphones. Dank einer speziell für Kali Linux NetHunter programmierten App können Angriffe auf Funknetzwerke einfach umgesetzt werden.
- ✔ **Containers** Container bieten ähnlich wie virtuelle Maschinen eine getrennte Laufzeitumgebung für Anwendungen, jedoch mit einem geringeren Performanceverlust. *OffSec* stellt Kali-Linux-Images für die Containertechnologien Docker und LXC zur Verfügung.
- ✔ **WSL** Das Windows Subsystem for Linux erlaubt das Ausführen Linux-basierter Betriebssysteme innerhalb einer Windows-Installation und ermöglicht eine bessere Integration in Bezug auf die Benutzerführung.

Für einen reibungslosen Ablauf mit den in diesem Buch beschriebenen Angriffen wird eine Installation von Kali Linux mittels **Installer Image** oder **Virtual Machine** empfohlen. Aus diesem Grund finden Sie in den folgenden Kapiteln eine Installationsanleitung für diese beiden Methoden.

Andernfalls können Schwierigkeiten in Bezug auf den Zugriff auf zusätzliche Hacking-Hardware entstehen. So ist etwa das Durchreichen eines Netzwerkadapters bei den genannten Installationsmethoden einfacher möglich.

Die relevanten Installationsvarianten sind zudem in weitere Versionen unterteilt. So können Sie unter anderem bei den **Installer Images** im Anschluss noch eine spezifische Download-Variante wählen, wie in Abbildung 1.2 dargestellt. Diese unterscheiden sich in der Anzahl

der bereits vorinstallierten Pakete und demnach auch in ihrer Download-Größe, wie in folgender Liste erläutert. Achten Sie ebenso auf die korrekte Auswahl der PC-Architektur.

- ✔ **Installer:** Diese Variante beinhaltet bereits eine lokale Kopie der wichtigsten Hacking-Tools, weswegen auch eine Installation ohne Internetverbindung möglich ist. Es ist das von *OffSec* empfohlene Installationsabbild.
- ✔ **NetInstaller:** Während einer Installation mit diesem Image werden die Hacking-Tools direkt aus dem Internet heruntergeladen und installiert. Dies kann die Installationszeit verlängern, dafür ist der initiale Download des Installer Images kleiner und Ihr System ist nach der Installation auf dem aktuellsten Stand.
- ✔ **Everything:** Dieses Abbild beinhaltet die Gesamtheit aller für Kali Linux verfügbaren Hacking-Tools und ist demnach besonders für einen Einsatz fernab eines Internetzugangs tauglich.
- ✔ **Weekly:** *OffSec* stellt auch wöchentlich geupdatete Abbilder zum Download bereit. Die Funktionalität der Tools wird jedoch nicht getestet und kann zu Problemen führen.

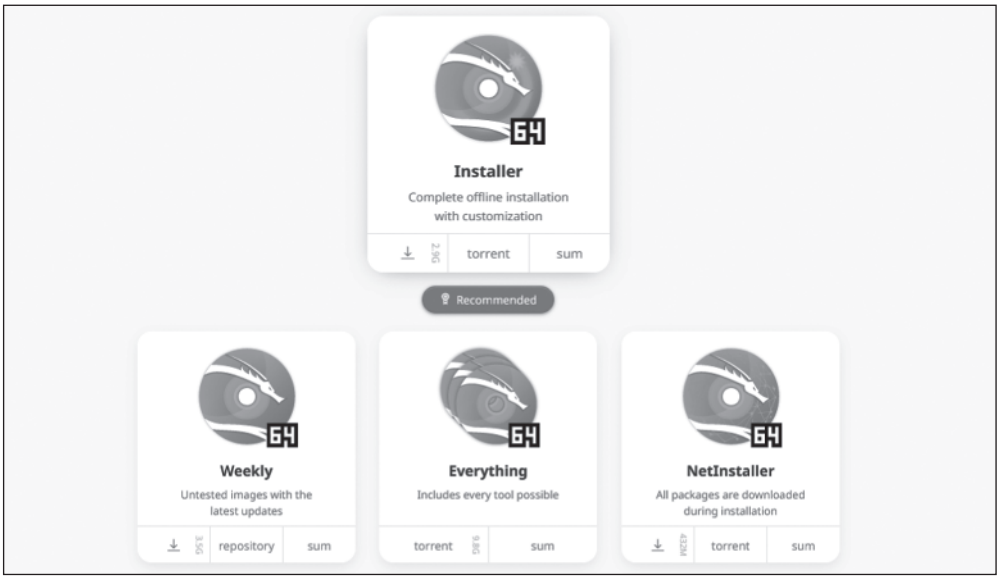

Abbildung 1.2: Installationstypen der Installer-Images

Machen Sie sich keine Sorgen um das Alter der installierten Programme, wenn Sie sich nicht für das NetInstaller-Image entschieden haben. Diese können einfach über den Paketmanager des Systems im Nachhinein aktualisiert werden, wie Sie im Kapitel »Die ersten Schritte ausführen« herausfinden werden.

Wenn Sie den Weg des geringsten Widerstands wählen und schnellstmöglich mit den Angriffen in diesem Buch starten möchten, empfiehlt sich die Nutzung einer der vorgefertigten

Virtual Machines für Kali Linux. Dadurch muss das Betriebssystem nicht mehr installiert werden, sondern kann einfach in die Virtualisierungslösung Ihrer Wahl importiert werden. Im Rahmen einer virtualisierten Installation läuft Kali Linux als virtuelle Maschine in einem Host-Hypervisor. Im Gegensatz zur Bare-Metal-Installation kann hier keine Auswahl des Tool-Umfangs getroffen werden – die virtualisierte Variante ist der Bare-Metal-Installer-Variante am nächsten. Achten Sie im Voraus auf die Wahl der richtigen PC-Architektur.

Wie in Abbildung 1.3 dargestellt, haben Sie die Wahl zwischen drei Hypervisor-Varianten für die virtuelle Maschine.

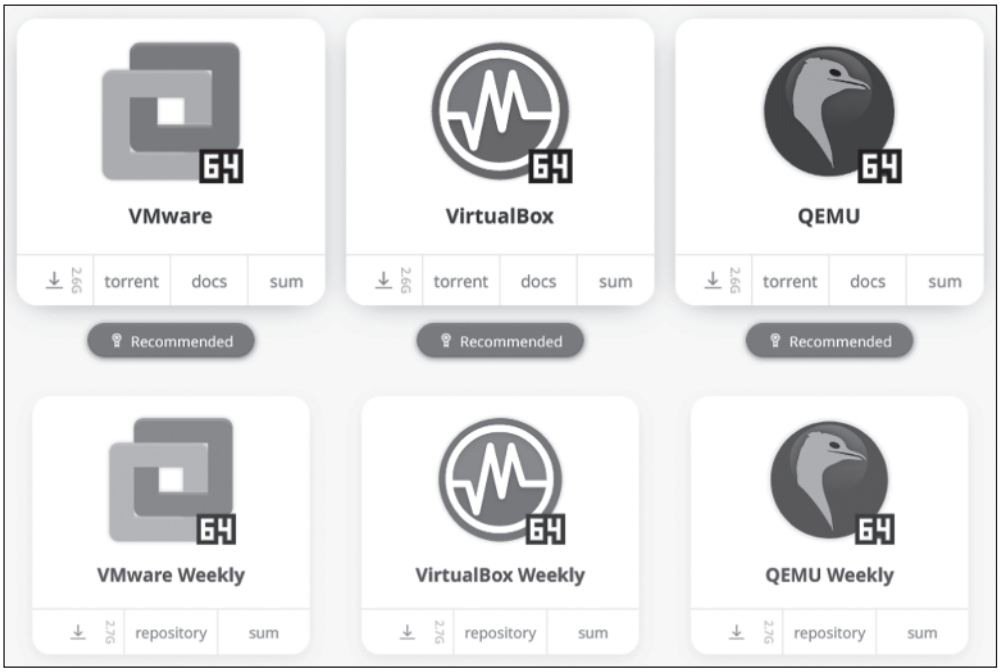

Abbildung 1.3: Installationstypen der Virtual-Machine-Abbilder

- ✔ **VMware (Weekly):** Sofern ein Hypervisor aus den Reihen von VMware wie Workstation, Workstation Player oder ESXi verwendet werden soll, ist dieses Image das korrekte. Die Weekly-Variante wird dabei wöchentlich aktualisiert. Dies kann ein Nachteil sein, da bestimmte Programme durch Änderungen eventuell nicht mehr funktionieren. Im Gegensatz dazu sind die normalen Images ausführlicher getestet und werden quartalsweise aktualisiert.
- ✔ **VirtualBox (Weekly):** Für eine Installation im freien Hypervisor VirtualBox muss diese Variante heruntergeladen werden. Wie bei der VMware-Variante ist auch hier der Download einer Weekly-Variante möglich.
- ✔ **QEMU (Weekly):** Bei QEMU handelt es sich um eine Open-Source-Software zum Emulieren von Betriebssystemen, auch über unterschiedliche Prozessorarchitekturen

hinweg. Dieses Image eignet sich für fortgeschrittene Nutzer, welche die größtmögliche Flexibilität bei der virtualisierten Nutzung von Kali Linux suchen.

Mehr über Kali Linux herausfinden

Aktuelle Informationen zum Thema Kali Linux erhalten Sie unter den gelisteten Webseiten. Anleitungen zu spezifischen Themen können in der Dokumentation von Kali Linux aufgefunden werden.

- ✔ **Webseite:** `https://www.kali.org/`
- ✔ **Dokumentation:** `https://www.kali.org/docs/`
- ✔ **Downloads:** `https://www.kali.org/get-kali/`