

Linux-Basics für Hacker

Einstieg in die Hacking-Grundlagen mit Kali Linux:
Netzwerke, Scripting und Security

» Hier geht's
direkt
zum Buch

DAS VORWORT

Einführung

Hacking ist die wichtigste Fertigkeit des 21. Jahrhunderts! Ich sage das nicht so leichthin. Die Schlagzeilen, die uns seit einigen Jahren jeden Morgen erwarten, bestätigen es. Nationen spähen einander aus, Cyberkriminelle stehlen Milliarden Dollar, digitale Würmer erpressen Lösegelder von ihren Opfern, politische Gegner beeinflussen Wahlen und Kriegsparteien schalten die Kampfmittel ihrer Feinde aus. Betrachten Sie nur einmal den Cyberkrieg zwischen der Ukraine und Russland als Beispiel. Diese Ereignisse sind alle das Werk von Hackern und man beginnt jetzt erst, ihre Macht in unserer zunehmend digitalen Welt zu verstehen.

Ich beschloss, das Buch zu schreiben, nachdem ich mit Zehntausenden angehenden Hackern bei Null-Byte, Hackers Arise (<https://www.hackers-arise.com>) und in nahezu jedem Zweig von US-Militär, Nachrichtendiensten und Ermittlungsbehörden gearbeitet habe (einschließlich NSA, DIA, CIA und FBI). Diese Erfahrungen haben mich gelehrt, dass viele aufstrebende Hacker kaum oder gar keine Erfahrungen mit Linux haben. Dieser Mangel an Erfahrung ist die größte Hürde, die ihrem Weg zum Profi im Weg steht. Die meisten der besten Hacker-Tools laufen unter Linux, sodass Sie zumindest grundlegende Linux-Kenntnisse benötigen, wenn Sie professioneller Hacker werden wollen. Ich habe dieses Buch geschrieben, um Ihnen über diese Hürde zu helfen.

Hacking ist im IT-Bereich ein Eliteberuf. Entsprechend erfordert es ein umfassendes und detailliertes Verständnis von IT-Konzepten und -Technologien. Linux ist das grundlegende Fundament. Ich empfehle Ihnen dringend, die Zeit und Energie aufzuwenden, um es zu verstehen, wenn Sie Hacking und Informationssicherheit tatsächlich als Karriereweg wählen möchten.

Dieses Buch richtet sich nicht an erfahrene Hackerinnen oder Linux-Admins. Stattdessen ist es für all jene gedacht, die noch am Anfang des aufregenden Wegs von Hacking, Cybersecurity und Pentesting stehen. Es soll auch keine vollständige Abhandlung über Linux oder Hacking sein, sondern will lediglich als Startpunkt in diese Welten dienen. Es beginnt mit den wesentlichen Linux-Elementen und einigen Skripting-Grundlagen in bash und Python. Wo immer es angemessen erscheint, nutze ich Hacking-Beispiele, um die Linux-Prinzipien zu verdeutlichen.

In dieser Einführung erhalten Sie einen Einblick in die Entwicklung des ethischen Hackings für die Cybersecurity und ich zeige Ihnen die Vorgehensweise für das

Aufsetzen einer virtuellen Maschine, damit Sie auf Ihrem System Kali Linux installieren können, ohne das Betriebssystem zu stören, das Sie bereits benutzen.

Was Sie in diesem Buch erwartet

In den ersten Kapiteln machen Sie sich mit den Grundlagen von Linux vertraut. **Kapitel 1** stellt Ihnen das Dateisystem und das Terminal vor und zeigt Ihnen einige grundlegende Befehle. In **Kapitel 2** erfahren Sie, wie Sie Text manipulieren, um Software und Dateien zu finden, zu untersuchen und zu verändern.

In **Kapitel 3** befassen Sie sich mit Netzwerken. Sie werden nach Netzwerken scannen, Informationen über Verbindungen finden und sich selbst tarnen, indem Sie Ihre Netzwerk- und DNS-Informationen verschleiern.

Kapitel 4 lehrt Sie, Software zu installieren, zu entfernen und zu aktualisieren. Außerdem erfahren Sie, wie Sie Ihr System auf dem neuesten Stand halten.

In **Kapitel 5** manipulieren Sie Datei- und Verzeichnisberechtigungen, um zu kontrollieren, wer worauf zugreifen darf. Sie lernen außerdem einige Eskalationstechniken für Berechtigungen kennen.

In **Kapitel 6** erfahren Sie, wie Sie Dienste verwalten. Dazu gehört das Starten und Stoppen von Prozessen und das Zuweisen von Ressourcen, um Ihnen eine größere Kontrolle zu gewähren. In **Kapitel 7** arbeiten Sie mit Umgebungsvariablen für eine optimale Leistung, zur größeren Bequemlichkeit und sogar zur Tarnung. Sie werden Variablen suchen und filtern, Ihre PATH-Variable ändern und neue Umgebungsvariablen erzeugen.

Kapitel 8 führt Sie in das bash-Skripting ein, quasi ein Muss für jeden ernsthaften Hacker. Sie lernen die Grundlagen der bash kennen und schreiben ein Skript zum Scannen nach Ziel-Ports, die Sie später vielleicht infiltrieren werden.

Kapitel 9 und **10** vermitteln Ihnen einige grundlegende Kenntnisse für die Dateiverwaltung. Sie erfahren hier, wie Sie Dateien komprimieren und archivieren, um Ihr System sauber zu halten, wie Sie ganze Speichergeräte kopieren und Informationen zu Dateien und verbundenen Festplatten erhalten.

In den später folgenden Kapiteln steigen Sie tiefer in die Hacking-Themen ein. In **Kapitel 11** benutzen und manipulieren Sie das Protokollierungs- bzw. das Loggingsystem, um an Informationen zu den Aktivitäten Ihres Ziels zu gelangen und Ihre eigenen Spuren zu verwischen. **Kapitel 12** zeigt Ihnen, wie Sie drei wichtige Linux-Dienste benutzen und missbrauchen: den Apache-Webserver, OpenSSH und MySQL. Sie werden einen Webserver anlegen, einen Remote-Kamera-Spion bauen und Datenbanken und deren Schwachstellen kennenlernen. In **Kapitel 13** lernen Sie, wie Sie mit Proxy-Servern, dem Tor-Netzwerk, virtuellen privaten Netzwerken und verschlüsselten E-Mails sicher und anonym bleiben.

In **Kapitel 14** geht es um drahtlose Netzwerke. Sie lernen die grundlegenden Netzwerkbefehle kennen, knacken dann Wi-Fi-Access-Points, machen Bluetooth-Signale ausfindig und verbinden sich mit Bluetooth-Geräten.

Kapitel 15 taucht dann tiefer in Linux selbst ein. Es gibt einen Überblick darüber, wie der Kernel funktioniert und wie man seine Treiber missbrauchen kann, sodass sie bössartige Software ausliefern. In **Kapitel 16** erwerben Sie wichtige Fähigkeiten, um Ihre Hacking-Skripte zu automatisieren. **Kapitel 17** lehrt Sie grundlegende Python-Konzepte und Sie entwickeln zwei Hacking-Tools: einen Scanner zum Ausspähen von TCP/IP-Verbindungen und einen einfachen Passwort-Cracker. **Kapitel 18** untersucht die Schnittstelle von Hacking und künstlicher Intelligenz, stellt einige grundlegende Konzepte vor und demonstriert, wie die KI Sie bei der Cybersecurity unterstützen kann.

Was ist ethisches Hacking?

Mit der Vergrößerung des Felds der Informationssicherheit in den letzten Jahren ging ein dramatisches Wachstum im Bereich des ethischen Hackings einher, das auch als White-Hat-Hacking bezeichnet wird (in alten Western waren die mit den weißen Hüten immer die Guten). Ethisches Hacking ist die Praxis des Infiltrierens und Ausspähen eines Systems, um dessen Schwächen zu ermitteln und es besser abzusichern. Ich unterteile das Feld des ethischen Hackings in zwei Hauptkomponenten: das Durchführen von Penetrationstests für ein rechtmäßiges Informationssicherheitsunternehmen und Tätigkeiten für die militärischen oder zivilen Nachrichtendienste Ihres Lands. Beides sind rasant wachsende Bereiche und die Nachfrage ist riesig.

Penetrationstests

Da das Sicherheitsbewusstsein von Unternehmen immer weiter zunimmt und die Kosten für Sicherheitsvorfälle exponentiell ansteigen, sind viele große Organisationen dazu übergegangen, die Sicherheitsdienste an externe Vertragspartner auszulagern. Zu den wichtigsten Sicherheitsdiensten zählt das Penetration Testing (auch: Pen Testing oder Pentesting). Ein *Penetrationstest* ist im Prinzip ein legal beauftragter Hack, der die Schwächen des Netzwerks und der Systeme eines Unternehmens aufdecken soll.

Im Allgemeinen führen Organisationen zuerst eine Schwachstellenanalyse durch, um potenzielle Schwächen in ihren Netzwerken, Betriebssystemen und Diensten zu finden. Ich schreibe extra »potenziell«, da dieser Schwachstellenscan eine beträchtliche Anzahl von falsch-positiven Ergebnissen enthält (Dinge, die als Schwachstellen identifiziert werden, obwohl sie es nicht sind). Aufgabe eines Penetrationstesters ist der Versuch, diese Schwachstellen zu hacken bzw. zu »pene-