Kali Linux Hacking-Tools für Dummies

Die Tools der Angreifer für Ihre IT-Sicherheit nutzen

DAS VORWORT

Einleitung

Willkommen zu *Kali Linux Hacking-Tools für Dummies*. Es vergeht nahezu kein Tag, an dem es keine Meldung zu einem IT-Sicherheitsvorfall in die Berichterstattung der Medien schafft. Mit immer spektakuläreren Hacks und gefährlichen Ransomware-Attacken, die ganze Unternehmen für Wochen lahmlegen, scheint es keine verlässliche IT-Sicherheit zu geben. Angesichts dieser scheinbar aussichtslosen Lage gleich vorab eine gute Botschaft: Bei all der Komplexität von IT-Systemen, mit der schier unüberschaubaren Anzahl von unterschiedlichen Komponenten, lassen sich Angriffe auf IT-Systeme doch verschiedenen Strategien zuordnen und einzelne Methoden extrahieren. Der erste Schritt einer effizienten Gegenmaßnahme ist, die Werkzeuge der Angreifenden kennenzulernen, um überhaupt einen Schutz zu realisieren.

Dabei bewegen wir uns im Bereich der sogenannten »offensiven Sicherheitsmaßnahmen«. Unter der Bezeichnung »offensive Sicherheitsmaßnahmen« werden Maßnahmen zusammengefasst, mit denen eigene Systeme selbst angegriffen werden, um herauszufinden, welche Auswirkungen ein echter Angriff haben könnte. Sie beschäftigen sich bereits mit *Kali Linux* – schließlich haben Sie begonnen, in diesem Buch zu lesen –, und vermutlich haben Sie bereits berechtigte Vermutungen oder erste Informationen dazu, was Kali Linux leistet. So werden alle, die sich mit proaktiver IT-Sicherheit beschäftigen, eher früher als später über den Namen Kali Linux stolpern. Also: Was ist Kali Linux genau?

Kali Linux ist ein Linux-Betriebssystem mit zahlreichen vorinstallierten Tools in den Bereichen Penetrationstests und digitale Forensik. Dabei sind die gleichen Hacking-Tools installiert, die auch von Angreifenden eingesetzt werden. Kali Linux ist somit das Standardwerkzeug in der IT-Sicherheitsbranche und ein geeignetes Mittel für die Überprüfung der Systemsicherheit im Unternehmen.

Über dieses Buch

Kali Linux Hacking-Tools für Dummies ist ein anwendungsorientierter Leitfaden, um einen einfachen Einstieg in das System zu geben, um einzelne Bereiche von IT-Systemen effektiv und ohne umfangreiche Einarbeitung testen zu können.

Mit diesem Buch schlüpfen Sie also in die Rolle eines Angreifers, um Ihre eigenen Systeme zu hacken und daraufhin die Sicherheit zu verbessern.

Mit diesem Buch sind Sie in der Lage,

- ✔ das Kali-Linux-System einzurichten und die darin enthaltenen Tools zu nutzen,
- ✔ zu verstehen, wie Angreifende vorgehen und welche Hacking-Tools sie dabei einsetzen,

- ✔ offensive Sicherheitstests durchzuführen, um Schwachstellen in der eigenen Abwehr zu finden,
- ✔ die IT-Sicherheit Ihrer eigenen Systeme durch die Anwendung der vorgestellten Hacking-Tools zu verbessern.

Es gibt unzählige Hacking-Tools für die verschiedensten Aufgaben. Viele davon sind in Kali Linux vorinstalliert und noch einige mehr können nachinstalliert werden. Insgesamt gibt es mehr als 2300 verschiedenen Softwarepakete (`https://www.kali.org/tools/all-tools/`), die installiert werden können. Wir haben für Sie die besten Tools aus verschiedenen Kategorien ausgewählt und zeigen Ihnen, wie Sie sie am effektivsten einsetzen.

Törichte Annahmen über den Leser

Sie wissen, dass Menschen ihr Wissen zum Umgang mit Hacking-Tools auch dazu verwenden können, um Schaden anzurichten. Es wäre töricht anzunehmen, dass Sie das hier gewonnene Wissen anders als zur Prüfung und Verbesserung der Sicherheit Ihrer Systeme einsetzen wollten. Dennoch müssen und wollen wir Ihnen den Inhalt des folgenden Hinweises sehr ans Herz legen.

Die in diesem Buch beschriebene Methoden und Tools dürfen nur auf eigene Systeme oder im Kundenauftrag mit Genehmigung zum Zugriff auf diese Systeme angewendet werden. Sollten Sie sich entschließen, Informationen aus diesem Buch einzusetzen, um heimlich und ohne Genehmigung in Rechnersysteme einzudringen, geschieht dies ausschließlich auf eigene Gefahr. Weder die Autoren noch irgendjemand sonst, der mit der Herstellung und dem Vertrieb dieses Buches zu tun hat, kann für Ihre unethischen oder kriminellen Handlungen haftbar gemacht werden, die Sie vielleicht durchführen, indem Sie auf hier beschriebene Methoden und Werkzeuge zurückgreifen.

Dieses Buch richtet sich primär an Fachinformatiker (Systemintegration oder Anwendungsentwicklung), Studierende und Absolventinnen und Absolventen der Informatik oder vergleichbarer Studiengänge. Zur Zielgruppe gehören alle, die sich mit IT-Systemen beschäftigen und sich mit den Themen IT-Sicherheit, Datenschutz und Cybercrime intensiver auseinandersetzen möchten und das Ziel haben, die Welt sicherer zu machen.

Wir erklären in diesem Buch jedes Tool Schritt für Schritt, damit können auch Leserinnen und Leser ohne fundierte Vorkenntnisse den Ausführungen folgen. Allerdings ist es vorteilhaft, wenn Sie bereits Erfahrungen in den folgenden Bereichen haben:

- ✔ Grundkenntnisse im Bereich Linux-Systeme
- ✔ Umgang mit dem Linux-Terminal und den gängigsten Kommandos
- ✔ Basiswissen in den Bereichen virtualisierte Systeme und Netzwerktechnik

Wie dieses Buch aufgebaut ist

Das Buch besteht aus insgesamt sieben verschiedenen Teilen. Der Aufbau orientiert sich grob an der Struktur des Startmenüs von Kali Linux. Im ersten Teil werden alle wichtigen Infos zu Kali Linux behandelt, die Sie benötigen, um im Anschluss die verschiedenen Werkzeuge einsetzen zu können. In den Teilen zwei bis sieben werden die verschiedenen Hacking-Tools von Kali Linux vorgestellt und erläutert. Nach dem einführenden Teil können Sie direkt zu einem beliebigen Teil springen, der Sie besonders interessiert. Jeder Teil ist für sich eigenständig, Sie müssen das Buch daher nicht von vorne bis hinten komplett lesen, um loslegen zu können.

Teil I: Erste Schritte mit Kali Linux

Es geht los mit einer kompakten Einführung zu Kali Linux. Im ersten Teil bekommen Sie gezeigt, wie Sie das System in einer virtuellen Laborumgebung einrichten, damit Sie alle Tools selbst testen können. Sie lernen die Bedienung des Systems und die wichtigsten Funktionen genauer kennen.

Teil II: Information Gathering – verdeckte Informationen sammeln

Im zweiten Teil geht es dann richtig los und Sie sammeln sicherheitsrelevante Daten und Informationen. Mit verschieden Tools scannen Sie unauffällig Netzwerke, ermitteln alle Aspekte über Domains und IP-Adressen, untersuchen intensiv die Dienste von Servern und sammeln aus verschieden Quellen Informationen, die als Grundlage für Angriffe verwendet werden.

Teil III: Password Attacks – Passwörter knacken

Jeder benutzt unzählige Passwörter und meldet sich mehrmals am Tag an einem Gerät oder einem Onlinedienst an. Im dritten Teil setzen Sie Tools ein, um Passwörter zu knacken. Sie nutzen Passwortlisten aus vergangenen Hacks für Angriffe, testen die Sicherheit von Logins und berechnen geschützte Passwörter.

Teil IV: Web Application Analysis – Websites untersuchen

Im vierten Teil geht es danach um das Thema Sicherheit von Webanwendungen. Immer mehr klassische Anwendungen werden als Online-Anwendung umgesetzt, und Sie lernen, mit welchen Tools Sie diese untersuchen. So spüren Sie potenzielle Ziele auf, die normalerweise nicht direkt erreichbar sind, analysieren die Kommunikation zwischen Client und Server und testen auf Fehlkonfigurationen und Schwachstellen.

Teil V: Wireless Attacks – WLANs angreifen / Sicherheit testen

So gut wie jeder beziehungsweise jede nutzt tagtäglich kabellose Netzwerke, und diese werden in nahezu allen Bereichen eingesetzt. Mit welchen Tools Sie die Sicherheit von WLANs überprüfen, erfahren Sie im fünften Teil. Sie finden versteckte Netzwerke, greifen die Verschlüsselung an und erstellen Fake-Netzwerke, um Zugangsdaten abzufangen.

Teil VI: Sniffing und Spoofing – Netzwerke unterwandern

Netzwerke sind das Rückgrat unserer modernen digitalen Gesellschaft. Im sechsten Teil geht es darum, mit welchen Tools Netzwerkverbindungen abgehört werden. Sie erfahren außerdem, mit welchen Tools die gesamte Netzwerkübertragung aufgezeichnet, Datenströme umgeleitet und Netzwerkverkehr manipuliert wird.

Teil VII: Forensic Tools – IT-Forensik Analysen

Anschließend geht es im siebten Teil um die Tools für eine forensische Untersuchung. Diese wenden Sie an, um ein Rechnersystem nach einem Sicherheitsvorfall zu untersuchen und relevante digitale Spuren zu sichern. Dabei lernen Sie, wie forensische Sicherungen erstellt und wie versteckte Informationen ausgelesen werden.

Teil VIII: Der Top-Ten-Teil

Im letzten Teil haben wir für Sie noch einmal die wichtigsten Kali-Linux-Hacking-Tools für Sie zusammengefasst. In Kapitel 27, »Top-Ten-Tools im Überblick«, zeigen wir Ihnen für die fünf wichtigsten Kategorien von Kali Linux die zehn besten Hacking-Tools. Anschließend gibt es in Kapitel 28, »Top-Ten-Alternativen zu Kali Linux«, noch einen Blick über den Tellerrand und Sie lernen weitere spannende Systeme im Bereich IT-Sicherheit kennen.

Symbole, die in diesem Buch verwendet werden

In diesem Buch werden Sie die folgenden Symbole finden:

Die Glühbirne weist Sie auf Tipps hin, die Ihnen helfen, typische Probleme zu umgehen oder komplexere Situationen elegant zu lösen. Tipps bringen Sie somit schneller zum Ziel.

Das Warndreieck erscheint immer, wenn die Gefahr besteht, dass Sie mit einem Aufruf schnell Schaden anrichten können. Lesen Sie diese Stelle besonders aufmerksam, damit Sie nicht aus Versehen ein fremdes System lahmlegen …

Der Wegweiser weist Sie auf eine spannende externe Quelle hin. Dabei kann es sich zum Beispiel um ein interessantes Projekt oder um weitere Beispiele, Scripte etc. handeln.

Das Fernglas gibt Ihnen einen Hinweis auf alternative Tools, die für den gleichen Zweck eingesetzt werden können, jedoch im Rahmen dieses Buches nicht weiter erläutert werden.

Sobald es technischer wird, gibt es die Information in einem zusätzlichen Kasten:

Technische Hintergrundinformationen

Das ist der Techniker. Er erscheint immer dann, wenn eine technische Erklärung folgt. Sie lernen dort den Hintergrund zu einer Technologie oder einem Protokoll kennen und verstehen so die Zusammenhänge besser.

Konventionen in diesem Buch

Wir setzen immer Namen von Tools in *kursiver* Schrift, damit Sie sie schneller erkennen können. BUTTONS und SCHALTFLÄCHEN werden wie hier durch Kapitälchen gesondert hervorgehoben. Parameter, Pfade, Dateinamen oder kurze Kommandos im Fließtext werden in `Nicht-proportional-Schrift` dargestellt. »Ausgaben« werden zusätzlich mit Guillemets gekennzeichnet. Befehle für das Terminal (Linux-Bash) stehen in einer separaten Zeile:

```
$ echo "Kali Linux Hacking-Tools"
```

Für Beispielaufrufe verwenden wir hier im Buch die Domain `example.com`. Ersetzen Sie sie für eigene Untersuchungen durch Ihre eigene Domain. Aufgrund der Tatsache, dass eine Untersuchung kein Ergebnis liefert, haben wir in den Screenshots andere Domains verwendet, die wir teilweise anonymisiert haben.

Falls die Listings im E-Book-Display nicht gut lesbar sind oder nicht korrekt dargestellt werden, empfehlen wir Ihnen, sich die Beispieldateien von der Webseite des Buches herunterzuladen:

`https://www.wiley-vch.de/9783527719105`

Eine persönliche Anmerkung zum Gendern in diesem Buch: Unser Buch ist für alle Menschen geschrieben, die sich in ihrer Ausbildung oder beruflich mit IT beschäftigen – ganz bewusst unabhängig vom Geschlecht. Wir haben dem Ausdruck verliehen, indem wir nach Möglichkeit geschlechtsneutrale Formulierungen oder paarweise und abwechselnd die weibliche oder männliche Form verwendet haben.

Wie es weitergeht

Im ersten Teil zeigen wir Ihnen, wie Sie ein Kali-Linux-Labor einrichten. In dieser virtuellen Maschine können Sie alle Hacking-Tools von Kali Linux ohne Risiko für Ihr eigenes System testen. Danach können Sie zu einem beliebigen Kapitel springen und die darin beschriebenen Hacking-Tools von Kali Linux ausprobieren. Wir wünschen Ihnen viel Spaß und Erfolg beim rechtlich korrekten Hacken.