LERNEN EINFACH GEMACHT

5. Auflage

Hacken

für dummies®

Windows- und Linux-Hacks verhindern

Die neuesten Hacker-Werkzeuge und -Techniken einsetzen

Einen Plan für ethisches Hacken entwickeln

Kevin Beaver

gemacht werden, die Sie vielleicht ausüben, indem Sie auf hier beschriebene Methoden und Werkzeuge zurückgreifen.

Nachdem das nun geklärt ist, wird es Zeit für etwas angenehmere Dinge! Dieses Buch richtet sich an Sie, wenn Sie Netzwerkadministrator, Verantwortlicher für Datensicherheit, Berater oder Auditor für Sicherheitsfragen, Compliance Manager (*Richtlinienbeauftragter*) oder einfach nur daran interessiert sind, mehr über legales und ethisches Testen von Computersystemen und IT-Umgebungen herauszufinden, um sie langfristig sicherer zu machen.

Außerdem setze ich bei Ihnen als angehendem IT- oder Sicherheitsprofi einige Dinge voraus:

- Sie sind vertraut mit grundlegenden Konzepten der Computer-, Netzwerk- und Datensicherheit und entsprechenden Begriffen.
- Sie können auf einen Computer und ein Netzwerk zugreifen und können/dürfen die hier vorgestellten Techniken und Werkzeuge ausprobieren und damit aus dem Internet herunterladen.
- Sie verfügen über die erforderlichen Berechtigungen und Genehmigungen Ihres Arbeitgebers oder Klienten, um die in diesem Buch beschriebenen Techniken des Hackens ausführen zu können.

Symbole, die in diesem Buch verwendet werden

In diesem Buch werden Ihnen die folgenden Symbole begegnen:


Dieses Symbol weist auf Informationen hin, bei denen es sich lohnt, sie sich zu merken.


Dieses Symbol weist auf Informationen hin, die sich negativ auf Ihre Verwundbarkeits- und Penetrationstests auswirken können. Sie sollten sie daher besser lesen!


Dieses Symbol weist auf Tipps hin, die dazu beitragen können, wichtige Punkte besser zu beleuchten oder zu klären.


Dieses Symbol weist auf technische Informationen hin, die zwar interessant sind,

aber nicht unbedingt benötigt werden, um das gerade behandelte Thema zu verstehen.

Wie es weitergeht

Je mehr Sie über die Arbeitsweise externer Hacker und schurkischer Insider und mögliche Tests Ihrer Systeme wissen, desto besser können Sie Ihre Computer sicherer machen. Dieses Buch liefert die Grundlagen, um erfolgreiche Programme für die Sicherheitsbeurteilung und Ermittlung möglicher Angriffspunkte in Ihrem Unternehmen entwickeln und warten zu können, um auf diesem Wege Geschäftsrisiken zu minimieren.

Abhängig von Ihrer Computer- und Netzwerkkonfiguration können Sie eventuell ganze Kapitel überspringen. Wenn Sie beispielsweise Linux nicht benutzen oder keine drahtlosen Netzwerke nutzen, können Sie die entsprechenden Kapitel überspringen. Passen Sie aber auf. Schnell meint man, bestimmte Systeme nicht einzusetzen, obwohl sie irgendwo im Netzwerk doch laufen und nur darauf warten, geknackt zu werden.

Vergessen Sie nicht, dass sich die Konzepte bei Sicherheitstests nicht so oft ändern wie die spezifischen Schwachstellen, gegen die es sich zu schützen gilt. Ethisches Hacken wird ein Bereich zwischen Kunst und Wissenschaft bleiben, der sich fortwährend ändert. Sie müssen immer mit den neuesten Technologien der Hard- und Software vertraut sein und dabei die verschiedenen Schwachstellen kennen, die hier täglich, monatlich und jährlich neu auftauchen.

Sie werden niemals nur einen optimalen Weg für das Hacken und Testen Ihrer Systeme finden, weshalb Sie die hier vorgestellten Materialien nach Lust und Laune an Ihre konkreten Anforderungen anpassen können und sollten. Und damit auf zum fröhlichen (ethischen) Hacken!

Teil I

Den Grundstock für Sicherheitstests legen

IN DIESEM TEIL …

- ✔ Lernen Sie die Grundlagen von Schwachstellen- und Penetrationstests kennen
- ✔ Erhalten Sie Einblicke in die Köpfe von Hackern, um verstehen zu können, warum und wie sie so handeln, wie sie es tun
- ✔ Entwickeln Sie einen Plan für Sicherheitstests
- ✔ Verstehen Sie die Verfahren, mit denen man die meisten (und übelsten) Schwachstellen finden kann

Kapitel 1

Einführung in Schwachstellen- und Penetrationstests

IN DIESEM KAPITEL

- Die Unterschiede zwischen den Zielen ethischer Hacker und bösartiger Angreifer
- Entstehungsgeschichte und Entwicklung von Sicherheitstests
- Gefahren für Computersysteme
- Erste Schritte beim Durchführen von Sicherheitstests

In diesem Buch geht es um das Testen Ihrer Computer und Netzwerke, um Sicherheitslücken aufzuspüren und aufgefundene Schwachstellen zu beheben, bevor die Schurken Gelegenheit bekommen, sie auszunutzen.

Begriffserklärungen

Jeder dürfte bereits etwas von Hackern und böswilligen Benutzern gehört haben. Viele Anwender mussten bereits selbst unter den Folgen krimineller Hackerangriffe leiden. Um wen handelt es sich bei diesen Leuten? Und was sollte man über sie wissen? Die folgenden Abschnitte sollen Ihnen einige grundlegende Fakten über diese Angreifer vermitteln.

 Ich verwende in diesem Buch diese Terminologie:

- **Hacker** (oder externe Angreifer) versuchen, Computer und sensible Daten üblicherweise als Außenstehende und Unberechtigte anzugreifen, um illegale Ziele zu erreichen. Hacker greifen beinahe alle Systeme an, die sie als Angriffsziel für lohnend halten. Einige streben bevorzugt nach Ruhm und Prestige und attackieren gut geschützte Systeme. Generell gilt aber eigentlich, dass der eigene Status in Hackerkreisen steigt, wenn es überhaupt gelingt, in fremde Systeme einzudringen.
- **Böswillige Benutzer** (externe oder interne Angreifer) versuchen, als