Einführung

Willkommen zu *Hacken für Dummies*. Vorab zur Klarstellung, um Missverständnisse gleich aus dem Weg zu räumen: Das Thema und der Begriff »Hacken« können in einer Reihe verschiedener Bedeutungen verwendet werden, die kaum noch etwas miteinander zu tun haben. Was Sie in diesem Buch nicht finden, sind direkte Anleitungen zum Hacken von Anwendungen, Entschlüsseln von Sicherheitscodes, Umgehen von Aktivierungen und was Sie vielleicht sonst noch anhand des Buchtitels in dieser Richtung an Aktivitäten von Programmierern erwarten könnten. Dieses Buch beschreibt zwar – in verständlicher Sprache – Tricks und Techniken von Computerhackern, es geht aber tatsächlich um Maßnahmen, um sich gegen diese möglichst gut zu wappnen und den Sicherheitsstand Ihrer IT-Systemumgebung zu beurteilen. Sie sollen seine Schwachstellen erkennen und diese beseitigen lernen, bevor kriminelle Hacker und/oder böswillige Benutzer Nutzen daraus ziehen. Diese legalen Aktivitäten im Bereich der Sicherheitstests, die ich hier als »*ethisches Hacken*« oder Verwundbarkeits- und Penetrationstests bezeichnen werde und um die es in diesem Buch geht, sind die professionelle und legale Art, eigene Sicherheitsmaßnahmen zu testen und zu implementieren.

Die Sicherheit von Computern und Netzwerken ist ein vielschichtiges Thema, das sich in ständiger Bewegung befindet. Sie müssen immer auf aktuellen Stand bleiben, da nur dann gewährleistet sein kann, dass Ihre Daten vor den Schurken weitgehend geschützt sind. Und genau dabei können Ihnen die Werkzeuge und Techniken helfen, die in diesem Buch vorgestellt werden.

Sie können alle möglichen Sicherheitstechnologien implementieren und den empfohlenen Vorgehensweisen folgen, um Ihre Rechnerumgebung nach bestem Wissen und Gewissen zu schützen. Solange Sie aber die Denkweise heimlicher Angreifer nicht nachvollziehen können, nicht über deren Wissen verfügen und die richtigen Werkzeuge nutzen, um eigene Systeme aus dieser Perspektive heraus »anzugreifen«, werden Sie kein wirkliches Gespür für die tatsächliche Sicherheit Ihrer Daten entwickeln können.

Ethisches Hacken oder einfacher ausgedrückt »Sicherheitsbeurteilungen«, die formale und methodische Verwundbarkeits- und Penetrationstests umfassen, ist erforderlich, um Sicherheitslücken ausfindig zu machen. Zudem werden Prüfungen durchgeführt, um sich davon zu überzeugen, dass die eigenen Informationssysteme auf Dauer wirklich sicher sind. Dieses Buch versorgt Sie mit dem notwendigen Wissen, um erfolgreich Programme für Sicherheitsbeurteilungen implementieren zu können, Sicherheitsprüfungen richtig durchzuführen und geeignete Gegenmaßnahmen einzurichten, um externe Hacker und böswillige Typen in Schach zu halten.

Über dieses Buch

Hacken für Dummies ist ein Leitfaden zum Hacken Ihrer Systeme, um deren Sicherheit zu verbessern und Geschäftsrisiken zu verringern. Die Vorgehensweise bei Sicherheitstests basiert auf geschriebenen und ungeschriebenen Regeln und bewährten Verfahren aus dem Computerbereich für Penetrations- und Schwachstellentests der Datensicherheit. Dieses Buch behandelt alle Maßnahmen vom Erstellen eines Plans für Systemtests bis hin zum Schließen der Lücken und der Verwaltung laufender Sicherheitstestprogramme.

Tatsächlich existieren für viele Netzwerke, Betriebssysteme und Anwendungen Abertausende mögliche Schwachstellen. Ich kann sie hier unmöglich alle aufführen, werde aber die meiner Einschätzung nach wichtigsten für die verschiedenen Plattformen und Systeme behandeln, die heute im Geschäftsbetrieb die größten Sicherheitsprobleme darstellen. Ich werde das *Paretoprinzip* (80/20-Regel) behandeln, bei dem es darum geht, jene 20 Prozent der Fragen zu untersuchen, die für 80 Prozent Ihrer Sicherheitsrisiken verantwortlich sein können. Ob Sie nun Sicherheitsschwächen in einem kleinen Heim- oder Büronetzwerk, dem Netzwerk eines mittelständischen Unternehmens oder in einem großen unternehmensweiten System aufspüren wollen, *Hacken für Dummies* liefert Ihnen die erforderlichen Informationen.

Dieses Buch versorgt Sie mit den folgenden Angaben:

- ✔ Verschiedene technische und nicht technische Tests und eine ausführliche Beschreibung der Vorgehensweisen
- ✔ Spezifische Gegenmaßnahmen zum Schutz vor Hacking-Angriffen und Einbrüchen

Bevor Sie beginnen, Ihre Systeme zu testen, sollten Sie sich mit den Informationen aus Teil I vertraut machen, um sich auf die anstehenden Aufgaben vorzubereiten. Das Sprichwort »Wenn Sie an der Planung scheitern, planen Sie Ihr Scheitern« gilt auch für das ethische Hacken. Für den eigenen Erfolg benötigen Sie die erforderlichen Berechtigungen und müssen einen ausgefeilten Schlachtplan besitzen.

Törichte Annahmen über den Leser

Haftungsausschluss: Dieses Buch dient IT- und Sicherheitsverantwortlichen einzig dazu, die Datensicherheit – entweder an eigenen oder Kundensystemen – mit entsprechender Genehmigung zu prüfen. Sollten Sie sich entschließen, Informationen aus diesem Buch einzusetzen, um heimlich und ohne Genehmigung in Computersysteme einzudringen, geschieht dies ausschließlich auf eigene Gefahr. Weder ich als Autor 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 vielleïcht durchführen, 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 sicherer können Sie Ihre Computer machen. Dieses Buch liefert die Grundlagen, um erfolgreiche Maßnahmen für die Sicherheitsbeurteilung und Ermittlung möglicher Angriffspunkte in Ihrem Unternehmen entwickeln und warten zu können und auf diesem Wege Geschäftsrisiken zu minimieren.

Abhängig von Ihrer Computer- und Netzwerkkonfiguration können Sie eventuell ganze Kapitel überspringen. Wenn Sie beispielsweise Linux nicht im Einsatz haben 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!