Einstieg in Ethical Hacking

Penetration Testing & Hacking-Tools
für die IT-Security

» Hier geht's direkt zum Buch

DAS VORWORT

Einleitung

Es ist noch nicht lange her, dass Hacking eher ein Tabu war, und es gab auch keine Schulungen dazu. Aber inzwischen hat sich die Erkenntnis breitgemacht, dass auch ein offensiver Ansatz einen Mehrwert für die IT-Sicherheit liefert. Diese neue Herangehensweise wird von vielen Organisationen aller Größen und Branchen begrüßt: Staatliche Stellen machen inzwischen Ernst mit offensiver Sicherheit, Regierungen geben auch offiziell zu, dass sie daran arbeiten.

Für das Sicherheitskonzept einer Organisation spielen vor allem Penetrationstests eine wichtige Rolle. Richtlinien, Risikobewertungen, Notfallpläne und die Wiederherstellung nach Katastrophen sind zu unverzichtbaren Maßnahmen zum Erhalt der IT-Sicherheit geworden und genauso müssen auch Penetrationstests in die Gesamtplanung für die Sicherheit aufgenommen worden. Mit solchen Tests können Sie erkennen, wie Sie vom Feind wahrgenommen werden. Das kann zu vielen überraschenden Entdeckungen führen und Ihnen kostbare Zeit geben, um Ihre Systeme zu verbessern, bevor es einen echten Angriff gibt.

Für das Hacking stehen heutzutage viele gute Werkzeuge zur Verfügung. Viele davon sind nicht einfach nur »da«, sondern laufen aufgrund der langjährigen Entwicklungszeit auch sehr stabil. Noch wichtiger ist für viele die Tatsache, dass die meisten dieser Tools kostenlos erhältlich sind.

Das ist zwar schön, aber Sie müssen diese Werkzeuge erst einmal finden, kompilieren und installieren, bevor auch nur der einfachste Penetrationstest durchgeführt werden kann. Auf den modernen Linux-Betriebssystemen geht das zwar relativ einfach, aber für Neulinge kann es immer noch eine abschreckende Aufgabe sein. Auch für Fortgeschrittene ist es mühsam, alle Tools erst mal zusammenzusuchen und zu installieren.

Die Security-Community ist glücklicherweise eine sehr aktive und freigiebige Gruppe. Mehrere Organisationen haben unermüdlich daran gearbeitet, verschiedene Linux-Distributionen für Hacking und Penetrationstests zu erstellen. Eine Distribution (kurz Distro) ist eine Variante von Linux. Für Hacking und Penetrationstests gibt es Linux-Distros wie

- Parrot Security OS
- BlackBox
- BlackArch
- Fedora Security Spin

- Samurai Web Testing Framework
- Pentoo Linux
- DEFT Linux
- Caine
- Network Security Toolkit (NST)
- Kali Linux

Die bekannteste Distro für Penetrationstests ist Kali Linux. Wir werden in diesem Buch deshalb auch Kali Linux verwenden, um die verschiedenen Tools fürs Hacking zu nutzen, die aber auch in allen anderen Linux-Distributionen und teilweise sogar unter Windows verwendet werden können. Mit Kali Linux, aber auch den anderen Betriebssystemen für das Hacking, erhalten angehende Sicherheitsexperten, Pentester und IT-Verantwortliche eine umfangreiche Plattform, um digitale Attacken zu planen und durchzuführen.

Warum sollte man das tun wollen?

Einerseits, um sich mit potenziellen Angriffen auf die eigenen Systeme auseinanderzusetzen, und andererseits, um interne und externe Schwachstellen besser zu verstehen.

Ein »Hacker-Betriebssystem« wie Kali Linux & Co. ist standardmäßig schon voller Tools, die Sicherheitsexperten und IT-Verantwortlichen entweder den Schlaf rauben oder ihre Augen glitzern lassen.

Die Hacker-Betriebssysteme enthalten eigentlich nichts Exklusives – man kann sich jedes Tool, jede Software und jedes Skript auf jedem beliebigen Linux (teilweise auch Windows) installieren –, dennoch greifen viele Sicherheitsforscher auf eine Distribution wie Kali zurück.

Der Grund, warum gerne Distributionen wie Kali & Co. verwendet werden, ist, dass die meisten Programme samt den passenden Einstellungen bereits mit der Installation der Distribution mitgeliefert werden oder einfach aus den Repositorien installiert werden können. Ein weiterer Grund ist, dass Kali sich sehr gut als isolierte Umgebung betreiben lässt. Sollte doch mal etwas schiefgehen, kann das System rasch neu installiert werden und man kann von vorne anfangen – das ist natürlich um vieles besser, als sich eine Produktivumgebung komplett zu zerschießen.

Vorsicht

Die falsche Anwendung von Security-Tools in Ihrem Netzwerk – vor allem ohne Erlaubnis – kann irreparablen Schaden mit erheblichen Folgen anrichten. Testen bzw. greifen Sie nie Systeme ohne Erlaubnis an.

Über dieses Buch

Dieses Buch ist ein praktischer Leitfaden für alle, die sich für das Thema Ethical Hacking und Penetration Testing interessieren. Es richtet sich sowohl an Einsteiger als auch an Fortgeschrittene, die ihre Fähigkeiten im Bereich der IT-Sicherheit erweitern wollen. Das Buch erklärt die Grundlagen des Ethical Hacking, die rechtlichen und ethischen Aspekte, sowie die wichtigsten Methoden und Werkzeuge, die Hacker verwenden, um Schwachstellen in Netzwerken und Systemen zu finden und auszunutzen. Anhand von zahlreichen Beispielen lernen Sie, wie Sie selbst Sicherheitstests durchführen können.

Ich habe das Buch so aufgebaut, dass Sie es auch verwenden können, wenn Sie noch keine Erfahrungen mit Security-Assessments haben bzw. noch nicht mit Linux gearbeitet haben. Wenn Sie das Buch gelesen haben, sollten Sie als Penetrationstester – auch wenn Sie ein Anfänger sind – Security-Assessments erfolgreich durchführen können.

Im ersten Teil des Buches finden Sie alle Grundlagen, die Sie für das Ethical Hacking brauchen, insbesondere eine kurze Einführung in Kali Linux, die Einrichtung Ihres Hacking-Labors sowie die wichtigsten Linux-Grundlagen, damit Sie, falls Sie Linux-Anfänger sind, keine Probleme haben, den Anleitungen im Buch zu folgen. Sie erfahren, welche Arten von Security-Assessments es gibt und welche Rolle das Penetration Testing dabei spielt. Weiterhin erhalten Sie einen Überblick über die Funktionsweise der Programmiersprache Python sowie BASH-Skripte, die für die Anpassung bestehender Hacking-Tools bzw. die Automatisierung nützlich sind.

Der zweite Teil des Buches konzentriert sich auf die Planung und Durchführung von Penetrationstests. Sie lernen die verschiedenen Testphasen sowie eine Vielzahl von Attacken und passender Hacking-Tools im Detail kennen und erfahren, welche Richtlinien Sie bei der Durchführung Ihrer Tests einhalten sollten, um sicher und ethisch zu hacken.

Weitere Infos

Um Interessierte über die aktuellen Security-Themen und Änderungen in meinen Büchern auf dem Laufenden zu halten, habe ich eine Homepage (`https://www.jürgenebner.com/`) eingerichtet. Hier können Sie mir auch Feedback zu meinen Büchern geben, damit wir weitere Auflagen verbessern können.