1 Einleitung

Nach nur einem Tag war es den Angreifern gelungen, aktuelle personenbezogene Daten einzusehen, nach zwei Tagen hatten sie Zugriff auf die aktuellen und noch unveröffentlichten Ergebnisse der Entwicklungsabteilung, nach drei Tagen hatten sie administrativen Zugang zu den wichtigsten Servern der Firma.

Wo sind die Schwachstellen in Ihrem Netzwerk und ist es ausreichend vor Angriffen geschützt? Was wird in Ihrer Firma unternommen, um den Schutz der IT-Infrastruktur zu gewährleisten?

Potenzielle Angreifer können die Vertraulichkeit, Integrität und Verfügbarkeit der Daten in Computernetzwerken gefährden und somit große Schäden anrichten. Dies bedeutet:

- Daten könnten so geändert werden, dass die *Integrität* nicht mehr belegt werden kann.
- Angreifern könnte es gelingen, ein Netzwerk so zu manipulieren, dass bestimmte Dienste und Funktonalitäten nicht mehr genutzt werden können und somit die *Verfügbarkeit* nicht mehr gewährleistet ist. Oftmals werden in diesem Zusammenhang Daten gelöscht bzw. verfälscht oder z.B. Webauftritte der Firma mit Denial-of-Service-Angriffen blockiert.
- Häufig kommen die Täter dann an Informationen, die nur einem eingeschränkten Personenkreis kenntlich gemacht und somit *vertraulich* behandelt werden sollten.
- In vielen Fällen ist die *Authentizität* der Angreifer nicht festzustellen, da diese mittels verschiedener Methoden eine falsche Identität vortäuschen oder geschickt ihre Spuren verwischen.

Bei diesen Angriffsversuchen werden mehrfach Schwachstellen ausgenutzt, die durch Programmierfehler in der Software oder falsche Konfiguration von Diensten entstanden sind. In sehr vielen Fällen bleiben diese Lücken in Computernetzwerken über einen längeren Zeitraum unentdeckt.

In diesem Zusammenhang ist es wichtig, die eingesetzte Software aktuell zu halten und die Netzwerkkonfiguration turnusmäßig auf Schwachstellen zu prüfen.

Die erforderlichen Schutzmaßnahmen sollten im IT-Sicherheitskonzept der Firma festgehalten und durch entsprechende Penetrationstests ergänzt werden.

Ein Penetrationstest ist ein Angriff auf ein Computernetzwerk im Auftrag des Eigentümers. Der Angriff soll die Schwachstellen ermitteln und helfen, sie zu beseitigen. Nach der Auswertung der Ergebnisse werden dann geeignete erweiterte Schutzmaßnahmen (z.B. Firewall, Einbrucherkennungssysteme) eingeführt, um die Risiken zu minimieren.

1.1 Was ist das Metasploit-Framework?

Das Metasploit-Framework ist ein Open-Source-Projekt, das im Jahr 2003 von HD Moore gegründet wurde. Es wurde über die Jahre ständig weiterentwickelt und stellt mittlerweile eine umfangreiche Plattform für Penetrationstester dar. Somit ist nicht verwunderlich, dass die Zahl der Nutzer im IT-Sicherheitsbereich ständig anwächst.

Zunächst mittels der Programmiersprache Perl entwickelt, wurde es für die Version 3 vollständig neu geschrieben und wird seitdem mit Ruby weiterentwickelt. Metasploit ist auf den herkömmlichen Plattformen wie Windows, Linux, BSD und auch Mac OS X lauffähig und kann sowohl per Kommandozeile als auch über eine grafische Oberfläche bedient werden.

Als Gegenstück zu kostenintensiven kommerziellen Produkten, wie CoreImpact, CANVAS oder Metasploit Pro, stellt das Metasploit-Framework eine kostenfreie Umgebung zur Verfügung. Admin- und IT-Sicherheitspersonal sind somit in der Lage, die ihnen anvertrauten Netzwerke effizient nach Schwachstellen zu untersuchen und entsprechende Gegenmaßnahmen zu entwickeln. So können z.B. die gewonnenen Erkenntnisse in die Entwicklung von Signaturen für Intrusion-Detection- und Intrusion-Prevention-Systeme einfließen.

Das Framework kann mit Tools wie Portscannern und Vulnerability-Scannern zusammenarbeiten und entsprechende Daten importieren bzw. exportieren. Als Beispiel seien hier nur die Tools Nmap, Nessus, Nikto und Nexpose genannt.

1.2 Ziel des Buches

Lance Spitzner, einer der Mitbegründer des Honeynet-Projektes[1], sagte: »How can we defend against an enemy, when we don't even know who the enemy is?«

Abgewandelt kann man sagen, dass die erfolgreiche Abwehr von Angriffen die genaue Kenntnis der Strategie und Methoden der Angreifer voraussetzt. Nur so können effektive Gegenmaßnahmen entwickelt und angewendet werden.

Das Buch beschäftigt sich daher primär mit dem Aufbau, der Entwicklung und dem praktischen Einsatz des Metasploit-Frameworks aus der Sicht eines Angrei-

1. *http://www.honeynet.org*

fers. Es bezieht aber auch andere Produkte – kostenlos verfügbare und kommerzielle – in die Betrachtung ein.

Ziel ist es, dem Leser das Metasploit-Framework in einer praktischen Art und Weise näherzubringen und das mögliche Zusammenspiel mit anderen Programmen aufzuzeigen. Das Buch soll die möglichen Methoden der Angreifer darlegen und Denkanstöße zur Abwehr der Angriffe liefern.

1.3 Wer sollte dieses Buch lesen?

Dieses Buch wendet sich an IT-Sicherheitsspezialisten und erfahrene Administratoren, die wissen wollen, wie man mit dem Metasploit-Framework und verwandten Programmen Penetrationstests durchführt. Es beschreibt die Installation und Nutzung von Metasploit in einer Testumgebung und erklärt den Umgang mit den verschiedenen Modulen und Exploits.

Leser, die sich über andere Quellen theoretische Kenntnisse über moderne Angriffsmethoden angeeignet haben, finden hier praktische Beispiele, die sie in einer sicheren Testumgebung nachvollziehen können.

In diese neue Auflage sind viele Hinweise und Vorschläge von Informatikstudenten eingeflossen. Auch hier hat sich gezeigt, dass insbesondere auch diese Lesergruppe großes Interesse an der Thematik hat. Sie sind die zukünftigen IT-Spezialisten, die die Herausforderungen der neuen Technologien annehmen und Informationstechnik in der Zukunft sicher gestalten wollen.

1.4 Was erwartet Sie in diesem Buch?

Im erstem Teil des Buches wird beschrieben, wie man eine Testumgebung auf Basis von VirtualBox als Linux-Server aufsetzt und die Angriffs- bzw. Zielsysteme in virtuellen Maschinen erstellt. Außerdem wird auf die Installation von hilfreichen Tools eingegangen (u.a. Nmap, Nessus und Nexpose). Die Konfiguration wird mit einer Firewall komplettiert, die die Aufteilung des virtuellen Netzes in verschiedene Netzwerksegmente praxisnah gestaltet.

Danach werden die einzelnen Komponenten des Metasploit-Frameworks vorgestellt und der mögliche Einsatz in den einzelnen Phasen eines Penetrationstests erläutert.

Zum Abschluss wird in praktischen Beispielen gezeigt, wie Sie mit dem Metasploit-Framework in einem Computernetzwerk Schwachstellen aufspüren und die gefundenen Sicherheitslücken mittels verschiedener Exploits ausnutzen können.

1.5 Was behandelt das Buch nicht?

Bitte beachten Sie, dass im Buch keine Grundlagenkenntnisse zu TCP/IP oder den Betriebssystemen Windows und Linux vermittelt werden. Die Leser sollten aus diesem Grund ausreichende Kenntnisse zur Administration und zum Umgang mit den genannten Systemen und deren Einbindung in Netzwerken besitzen.

Um die beigefügten Angriffsszenarien verstehen zu können, sollten Sie in die Problematik der IT-Sicherheit in Computernetzwerken eingeführt sein und praktische Erfahrungen im Umgang mit Sicherheitslücken und Schwachstellen haben.

In diesem Buch wird auch nicht auf die Anwendungsprogrammierung eingegangen. Es werden keine Kenntnisse über die Erstellung von Exploits und die Programmierung von Tools für Penetrationstester auf der Grundlage des Metasploit-Frameworks vermittelt.

1.6 Haftungsausschluss

Nicht zuletzt möchte ich darauf hinweisen, dass die hier vorgestellten Tools und Angriffsmethoden ein erhebliches Angriffspotenzial in Computernetzwerken darstellen können. Die unbefugte Nutzung von Metasploit in realen Umgebungen stellt somit kein Kavaliersdelikt dar und kann zu strafrechtlichen Konsequenzen führen.

Betreiben Sie Ihre Testumgebung immer in einem speziell kontrollierten Netzwerksegment und benutzen Sie keine Produktivsysteme innerhalb dieses Netzwerkes. Nutzen Sie zur Anmeldung an die virtuellen Computer keine regulären Passwörter oder Zugangsdaten. Speichern Sie keine persönlichen Informationen und Daten innerhalb dieses Netzwerkes und sichern Sie Ihre Testumgebung zum Internet ab.

Der Autor und der Verlag übernehmen keine Haftung für Schäden, die aus der Nutzung der im Buch veröffentlichten Informationen entstehen können.

1.7 Danksagung

Als mich René Schönfeldt vom dpunkt.verlag ca. sechs Monate nach Erscheinen der ersten Auflage des Buches (März 2011) ansprach und mich fragte, ob ich nicht Zeit und Lust habe, das Buch zu überarbeiten, war ich zunächst skeptisch. Dies lag sicher nicht daran, dass ich das Interesse an der Thematik verloren hätte, sondern mir war klar, dass ich aufgrund der rasanten Entwicklung in diesem Bereich noch einmal viel Zeit und Geduld in die Überarbeitung des Buches stecken müsste. Darüber hinaus sind viele interessante Werkzeuge und grafische Oberflächen hinzugekommen, die ich den Lesern nicht vorenthalten wollte. Doch das Feedback zur ersten Auflage hat mir gezeigt, dass weiterhin großes Interesse am

Metasploit-Framework in allen Lesergruppen besteht. Dies hat mich letztlich ermutigt, diesen Schritt zu gehen.

Folgenden Personen möchte ich besonders danken:

Meiner Frau, meinen Kindern und Eltern, die mir geholfen haben, meine Krankheit zu überwinden;

allen Arbeitskollegen und Freunden, die mich in guten und schlechten Zeiten unterstützt haben;

den fleißigen Helfern im dpunkt.verlag, insbesondere Herrn Schönfeldt, Herrn Heidt, Frau Zimpfer und Herrn Neumann;

Christian Kirsch von Rapid7 für die Unterstützung und die Testversionen;

HD Moore für das Geleitwort und das gesamte Rapid7-Team für die geleistete Arbeit am Framework;

Raphael Mudge für die geniale grafische Oberfläche Armitage.

Nicht zuletzt möchte ich mich bei allen Helfern, Gutachtern und Lesern für das tolle Feedback zur ersten Auflage bedanken und hoffe, dass auch das vorliegende Buch einige interessante Stunden am PC bereiten wird.