BRAIN-MEDIA.DE

PROFESSIONELLES INTERNET- UND OPEN-SOURCE-KNOW-HOW

Holger Reibold

Hacking kompakt

Security.Edition

Die Kunst des Penetration Testing – der Schnelleinstieg in die Welt der Hacker

Holger Reibold

Hacking kompakt

© 2015 Brain-Media.de

Herausgeber: Dr. Holger Reibold

Umschlaggestaltung: Brain-Media.de

Satz: Brain-Media.de

Coverbild: john krempl / photocase.de

Korrektur: Therea Tting

ISBN: 978-3-95444-161-7

Inhaltsverzeichnis

Vorwort

Wenn mir jemand in meiner Schulzeit prophezeit hätte, dass ich in 20 oder 30 Jahren mal ein Buch schreiben würde, so hätte ich ihn vermutlich spontan ausgelacht. Und schon gar nicht ein Fachbuch zu einem Thema wie Penetration Testing. „Nie im Leben“, wäre vermutlich die prompte Antwort gewesen. Heute weiß ich es besser: Es ist anders gekommen, ganz anders sogar. In den vergangenen Jahren sind es inzwischen weit über 100 Bücher geworden – längst habe ich aufgehört, zu zählen.

Auch wenn ich heute routinierter an solche Projekte gehe, sind der Spaß und die Neugierde bei der Arbeit geblieben. Es gibt Themen, die drängen sich förmlich auf, weil man mit dieser oder jener Software oder einem Gerät täglich in Berührung kommt, Andere „reifen“ mit der Zeit bis sie dann einen Punkt erreichen, der förmlich nach ihrer Umsetzung schreit.

Ich publizierte 2004 ein Buch zum Security Scanner Nessus 2.x. Es folgte 2008 ein weiteres zu Version 3.x. Leider entschied sich das Nessus-Team, Ihren Scanner in eine kommerzielle Lizenz überzuführen. Aus dem anfänglichen Verlust für die Open Source-Gemeinde entstand mit OpenVAS ein freier Nessus-Fork, der mit erheblicher finanzieller Unterstützung durch das BSI (Bundesamt für Sicherheit in der Informationstechnik) sich zu einem ebenbürtigen Konkurrenten zur kommerziellen Nessus-Version entwickelte.

Was hat das alles nun mit dem vorliegenden Buch zu tun? IT- und Systemadministratoren müssen heute immer komplexer werdende Infrastrukturen permanent auf Schwachstellen und Sicherheitslücken überprüfen. Das Aufdecken von Schwachstellen, das Testen der Anfälligkeit und das Schließen sind heute essentielle administrative Aufgaben.

Fast täglich kann man in den Medien von erfolgreichen Hacker-Attacken hören. Prominentes Opfer war im Sommer 2015 das Netzwerk des Bundestages, das – vermeintlich aus Russland – gehackt worden sein soll. Das BSI, das für die Wartung und die Sicherheit dieses Netzwerks zuständig ist, blamierte sich in diesem Zusammenhang, weil man weder in der Lage war, das Netzwerk ausreichend zu schützen, noch zeitnah eine sichere Umgebung herzustellen.

Solch prominente Geschehnisse sind nur die Spitze eines Eisbergs. Tag für Tag werden Millionen Hacker-Attacken gefahren. Manchmal sind es nur Skript-Kiddies, die ihre erworbenen Hacker-Fähigkeiten testen, doch die überwiegende Anzahl der Attacken dürfte einen kriminellen Hintergrund haben. Oftmals geht es um Wirtschaftsspionage.

Wenn auch Sie für die Sicherheit eines Netzwerks zuständig sind, müssen Sie dieses kontinuierlich auf Sicherheitslücken und sonstige Schwachstellen hin überprüfen. Fachleute sprechen von Penetrationstests. Sie dienen dazu, Netzwerkkomponenten auf bekannte Schwächen hin zu überprüfen.

Ihr Ziel muss es sein, potenziellen Hackern zuvorzukommen. Das Zauberwort lautet dabei: Waffengleichheit. Nur dann, wenn Sie wissen, wie Hacker vorgehen und welche Tools sie dabei einsetzen, sind sie in der Lage, ihnen mit gleichen Mitteln zu begegnen. Dabei sind Sie potenziellen Angreifern klar im Vorteil, denn Sie kennen die kritischen Infrastrukturkomponenten, die Netzwerk-Topologie, potenziellen Angriffspunkte, die ausgeführten Services und Server etc.

Um Ihre eigene Infrastruktur so sicher wie möglich zu machen, müssen Sie immer und immer wieder folgende Schritte ausführen:

1. Identifizierung von Schwachstellen und deren Risiko.
2. Praktische Ausnutzung und Testen der Schwachstellen in einer gesicherten Umgebung.
3. Tests in einer realen Umgebung.
4. Schließen von gefundenen Schwachstellen.

Wenn Sie bei Punkt 4 angelangt sind, fängt alles wieder von vorne an – ein permanenter Kreislauf. Wenn Sie diese Schritte verinnerlichen und kontinuierlich die Sicherheit kritischer Systeme im Blick haben, wird Ihre Umgebung mit jeder Maßnahme sicherer. Das wiederum spart Ihnen langfristig viel Zeit und Ärger, denn Sie geben Hackern kaum eine Chance, ihr Unwesen zu treiben.

Sie können das Ganze auch sportlich betrachten und als Spiel sehen. Jeder hat dabei seine Mittel: Mitspieler, technische Geräte und Techniken. Am Ende ist nur wichtig, dass Sie als Sieger vom Platz gehen.

Bleibt mir nur noch, Ihnen viel Spaß und Erfolg beim Einstieg in die Welt der Penetrationtests zu wünschen!

Herzlichst,

Holger Reibold

(Juli 2015)

1 Einstieg in das Penetration Testing

Genug der Vorrede! Sie wollen loslegen. Am liebsten jetzt direkt. Wie aber können die ersten Schritte aussehen? Und wo soll man beginnen? Noch bevor Sie sich Gedanken darüber machen, welche Systeme zuerst einer Sicherheitsanalayse unterzogen werden, müssen Sie zunächst ein Penetration Testing-System aufsetzen und sich mit bewährten Vorgehensweisen vertraut machen.

In der Praxis kommt dabei ein handlicher Werkzeugkasten zum Einsatz, der alle notwendigen Tools zur Verfügung stellt. Deren Einsatz ist in der Regel längst nicht so kompliziert, wie viele meinen. Wenn Sie die Grundtechniken drauf haben, sind Sie bereits ein guter Penetration-Tester und können sich auch an harte Nüsse herantrauen.

In diesem Einstieg dreht es sich zunächst um den Werkzeugkasten, den Sie zusammenstellen müssen, um Ihre Infrastruktursysteme auf Herz und Nieren prüfen zu können. Dabei kommt Ihnen zugute, dass die besten Tools für Penetrations-Tester frei verfügbar sind. Wenn Sie professionell Sicherheitstests durchführen, so können Sie ergänzend zu dem einen oder anderen kommerziellen Werkzeug greifen.

Ein kleines Problem für Penetration-Tester ist allerdings der Umstand, dass die meisten Tools auf Linux als Betriebssystem setzen, es aber auch einige Windows-Programme gibt, auf die man nicht verzichten möchte. Dieses Problem können Sie mit zwei Rechnern lösen: ein Linux- und ein Windows-Penetration Testing-Rechner. Sie profitieren dann insbesondere davon, weil es für unterschiedliche Plattformen spefizische Tools gibt, die beispielsweise für das Wiederherstellen von Passwörtern oder WLAN-Schlüssel spezialisiert sind.

Da das Hantieren mit zwei Rechnern umständlich ist, können Sie auch einen einfachen Weg einschlagen und somit zwei Fliegen mit einer Klappe schlagen: Führen Sie ein System in einer Virtuellen Maschine aus. Sie können nach dem Einrichten einer Penetration Testing-Umgebung diese einfach pausieren und dann bei Bedarf fortsetzen.

Sie können sogar noch einen Schritt weiter gehen und in einer virtuellen Umgebung ein Linux- und ein Windows-System aufsetzen und diese dann einfach exportieren und auf anderen Rechnern wieder importieren. Der Vorteil: Sie haben mit minimalem Aufwand eine eingerichtete Testumgebung zur Verfügung, die sich innerhalb von wenigen Minuten auch auf anderen Rechnern in Betrieb nehmen lässt.

Damit haben Sie sozusagen eine flexible Testumgebung, die sie natürlich auch an neue Anforderungen anpassen und erweitern können.

1.1 Die richtige Hard- und Software

Bevor Sie sich an die Auswahl geeigneter Software machen, benötigen Sie zunächst einen Rechner, auf dem Sie Ihre Hacker-Werkzeuge ausführen. Ich empfehle ein modernes Notebook, damit Sie auch über einen WLAN-Adapter verfügen, mit dem Sie auch die Sicherheit von Access Points prüfen können. Das Notebook sollte mit mindestens 8 MB Arbeitsspeicher ausgestattet sein. Sie sollten über mindestens 500 GB freien Speicherplatz verfügen.

Ein Quad Core-Prozessor ist empfehlenswert. Für das Social Engineering sollten Sie außerdem über einen Flash-Speicher verfügen. Gelegentlich ist auch ein weiterer externer WLAN-Adapter sinnvoll. Das sind die wesentlichen Hardware-spezifischen Eigenschaften, die Ihr Rechner erfüllen sollte.

Kommen wir zur Software-Ausstattung. Zunächst benötigen Sie einen Security Scanner. Mit diesem Tool können Sie das bzw. die Zielsysteme auf existierende Schwachstellen hin überprüfen. Hierfür bietet sich der freie verfügbare OpenVAS-Scanner an. Alternativ können Sie auch zu Nessus oder Nexpose greifen. Beides sind kommerzielle Programme, die aber in abgespeckten Versionen kostenlos für den Einstieg in das Security-Scannen verfügbar sind.

!

Tipp: FreeBooks zu Nessus OpenVAS

Zu den beiden Security-Scannern Nessus und OpenVAS stehen über die Verlags-Website jeweils umfangreiche E-Books zum Download zur Verfügung. Sie finden die beiden Bücher im FreeBooks-Bereich von Brain-Media.de (http://www.brain-media.de/freebooks.html).

Wenn Sie Web-Applikationen unter die Lupe nehmen wollen, so ist der Einsatz eines speziellen Web Application Scanners wie der Burp Suite (*http://portswigger.net/burp/*) sinnvoll. Auch hierbei handelt es sich um ein kommerzielles Produkt. Allerdings ist in Kali Linux, das Sie im nächsten Abschnitt kennenlernen, in einer einfachen, abgespeckten Fassung enthalten. Das Herzstück Ihres Penetration Testing-Systems bildet Kali Linux (*https://www.kali.org*). Dabei handelt es sich um eine vollständig auf Debian basierte Linux-Distribution, die nahezu alle (und das meine ich so, wie ich es schreibe) relevante Werkzeuge für Sie bereitstellt.

Sie werden nicht schlecht staunen: Kali Linux enthält über 300 Hilfsmittel, mit denen Sie die Sicherheit von Computersystemen prüfen und bewerten können. Sie können diese Tools auch unter anderen Linux-Distributionen einsetzen, manche auch unter Windows.

Ein erster Blick auf Kali Linux und die Top 10-Sicherheitsprogramme.

Im Unterschied zur Einzelinstallationen sind die Tools in Kali Linux bestens aufeinander abgestimmt und verfügen über angepasste und modifizierte Treiber, so beispielsweise für aircrack-ng.

Laut Angaben des Kali Linux-Teams werden die Programme viermal täglich aus dem Debian-Repository bezogen. Somit ist sichergestellt, dass die Anwender von Kali über eine solide Software-Basis mit den neuesten Sicherheits-Updates verfügen.

Von den in Kali Linux enthaltenen Programmen sollen hier für den Moment nur einige wichtige genannt werden:

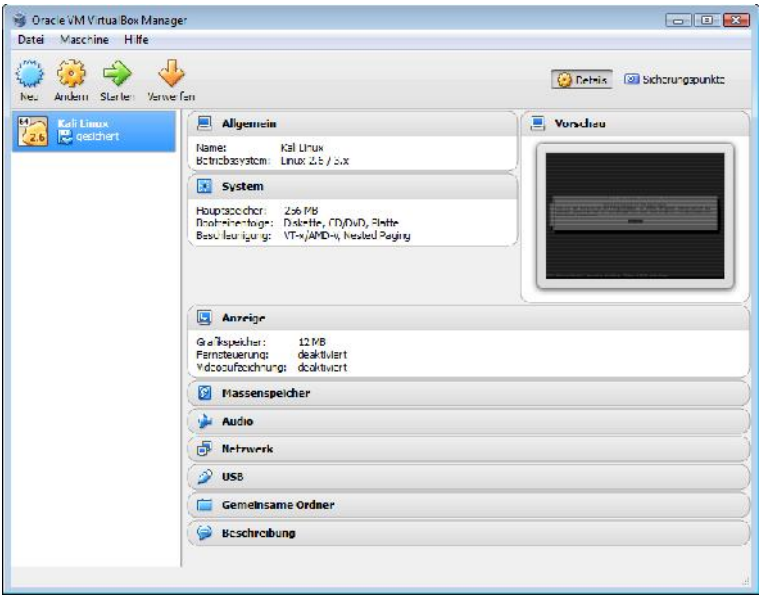
- **OpenVAS**: Der einzige freie Security Scanner, der professionellen Ansprüchen genügt.
- **Maltego**: Dieses Programm dient dazu, Daten über Einzelpersonen oder Unternehmen im Internet zu sammeln.
- **Kismet**: Hierbei handelt es sich um einen passiven Sniffer zur Untersuchung von lokalen Funknetzen.
- **Social-Engineer Toolkit (SET)**: In diesem Paket sind verschiedene Programme für Penetrationstests mit dem Schwerpunkt auf Social Engineering enthalten.
- **Nmap**: Der bekannte Netzwerkscanner zur Analyse von Netzwerken ist in Kali Linux enthalten, auch die grafische Nmap-Benutzeroberfläche Zenmap.
- **Wireshark**: Der Klassiker unter den grafischen Netzwerksniffern ist in diesem System enthalten.
- **Ettercap**: Hierbei handelt es sich um ein Netzwerkmanipulationstool, mit dem Sie beispielsweise einen Man-in-the-middle-Angriff durchführen können.
- **John the Ripper**: Dieses Tool dient dem Knacken und Testen von Passwörtern.
- **Metasploit**: Der Klassiker für das Testen und Entwickeln von Exploits auf Zielsystemen. Mit eines der wichtigsten Werkzeuge für Penetrationtester.
- **Aircrack-ng**: Hierbei handelt es sich um eine Tool-Sammlung, mit der Sie Schwachstellen in WLANs analysieren und ausnutzen können.
- **Nemesis**: Dies ist ein Paketfälscher für Netzwerke.
- **RainbowCrack**: Mit diesem Programm steht Ihnen ein Cracker für LAN-Manager-Hashes zur Verfügung.

Neben dieser kleinen Auswahl enthalt die Spezial-Distribution jede Menge weitere interessante Werkzeuge. Die vermeintlich am häufigsten eingesetzten und wichtigsten Programme sind im Untermenü *Top 10 Security Tools* zusammengefasst. Bevor wir in die praktische Verwendung von Kali Linux einsteigen, sollten Sie noch rudimentär mit der rechtlichen Lage vertraut sein. Beim Einsatz von Kali Linux greift der sogenannte Hacker-Paragraph, § 202c StGB, der Ende Mai 2007 in Kraft getreten ist.

Danach enthält Kali Linux Programme, die teilweise Sicherheitsvorkehrungen umgehen können und als Computerprogramme zum Ausspähen von Daten aufgefasst werden. Aufgrund dieser Gesetzeslage kann bereits der Besitz oder Vertrieb strafbar sein, sofern die Absicht zu einer rechtswidrigen Nutzung nach § 202a StGB (Ausspähen von Daten) oder § 202b StGB (Abfangen von Daten) besteht. Damit ist klar: Sie dürfen Kali Linux nur dann zur Analyse von Infrastrukturen in Teilen bzw. Komponenten verwenden, für die Sie eine explizite Erlaubnis besitzen.

1.1.1 Kali Linux in Betrieb nehmen

Die Inbetriebnahme von Kali Linux ist wirklich einfach. Auf der Projekt-Site stehen für die verschiedenen Plattformen ISO-Images bereit, die Sie als Vollsystem installieren oder mit denen Sie eine Virtuelle Maschine (VM) einrichten können. Für den Betrieb von Kali Linux in einer VM benötigen Sie lediglich eine geeignete Host-Software. Hier bietet sich der Einsatz des ebenfalls freien VirtualBox (*http://www.virtualbox.org*) an. Auch diese Umgebung ist für alle wichtigen Plattformen verfügbar.



Kali Linux lässt sich besonders einfach als VM unter VirtulBox ausführen.

Das Beste dabei: Wenn Sie über ein ausreichend flottes Notebook verfügen, können Sie auf einer VM Kali Linux und auf einer weiteren eine Windows-Installation mit entsprechenden Werkzeugen betreiben. Ein weiterer Vorteil: Sie können die beiden VM parallel betreiben und dabei je nach Bedarf zwischen den beiden Plattformen hin- und herswitchen.

Unter Penetrationtestern erfreuen sich MacBooks wegen der hohen Stabilität großer Beliebtheit. Sie können VirtualBox auch auf einem Mac OS X-Notebook betreiben und dort Kali Linux und eine Windows-Installation einrichten. Auch hier ist wieder ein problemloses Switchen zwischen den beiden verschiedenen Plattformen möglich.

Ob Sie nun Kali Linux auf einem eigenen Rechner oder „nur“ in einer VM ausführen, spielt für das weitere Vorgehen keine Rolle. Wichtiger ist vielmehr, dass Sie als Nächstes gewisse Anpassungen an der Kali Linux-Installation vornehmen. Bei der Installation haben Sie für Root ein Passwort angelegt. Dieses können Sie über Terminal leicht ändern, in dem Sie folgenden Befehl verwenden:

```
passwd
```

Auf der Konsolenebene geben Sie das neue Passwort ein und bestätigen die Änderung.

Nach der Installation sollten Sie das Passwort Ihrer Kali Linux-Installation ändern.

Auch dann, wenn Sie ein aktuelles ISO-Image heruntergeladen und installiert haben, können sich sozusagen über Nacht kritische Funktionen geändert haben. Sie sollten daher ein Update Ihrer Installation ausführen. Dazu führen Sie die beiden folgenden Befehle aus:

```
apt-get update
```

```
apt-get dist-upgrade
```

Dem Upgrade müssen Sie explizit zustimmen, weil hier je nach Kali Linux-Installation meist mehrere Hundert Megabyte heruntergeladen werden müssen.

Wie wir später noch sehen werden, ist Metasploit ein essentielles Werkzeug, ohne das kaum etwas beim Penetration Testing geht. Metasploit liefert ihnen Informationen über Sicherheitslücken und wird üblicherweise bei Penetrationstests sowie der Entwicklung von IDS-Signaturen eingesetzt.

Da Metasploit seine Daten in einer PostgreSQL-Datenbank speichert, müssen Sie als Nächstes die Datenbank einrichten und beide als Service anlegen. Hierzu führen Sie die beiden folgenden Kommandos aus:

```
service postgresql start
```

```
service metasploit start
```

Ergänzend kann es sinnvoll sein, die Metasploit-Aktivitäten zu loggen, also zu protokollieren. Auch hierzu greifen Sie wieder zur Konsole:

```
echo “spool/root/msf_console.log“ > /root/.msf4/msfconsole.rc
```

Das Ergebnis dieses Befehls: Die Daten werden in der Datei */root/msf_console.log* aufgezeichnet. Die Protokolldateien von Metasploit werden sehr schnell sehr groß. Das gilt es beim Aktivieren der Protokollfunktion zu beachten.

Der nächste Schritt dient der Installation der sogenannten Discover Scripts, die vorher als Backtrack-Skripts bezeichnet wurden. Diese Skripts können verschiedene Penetrationstests für Sie durchführen. Zur Installation führen Sie folgenden Befehl aus:

```
git clone git://github.com/leebaird/discover.git
/opt/scripts/
```

Um die Skripts zu installieren, wechseln Sie in das Skript-Verzeichnis und führen das Installationsprogramm aus:

```
cd /opt/discover/
./setup.sh
```

Bei der Installation wird auch eine FileZilla-Installation (FTP-Server) auf Ihrem System eingerichtet.

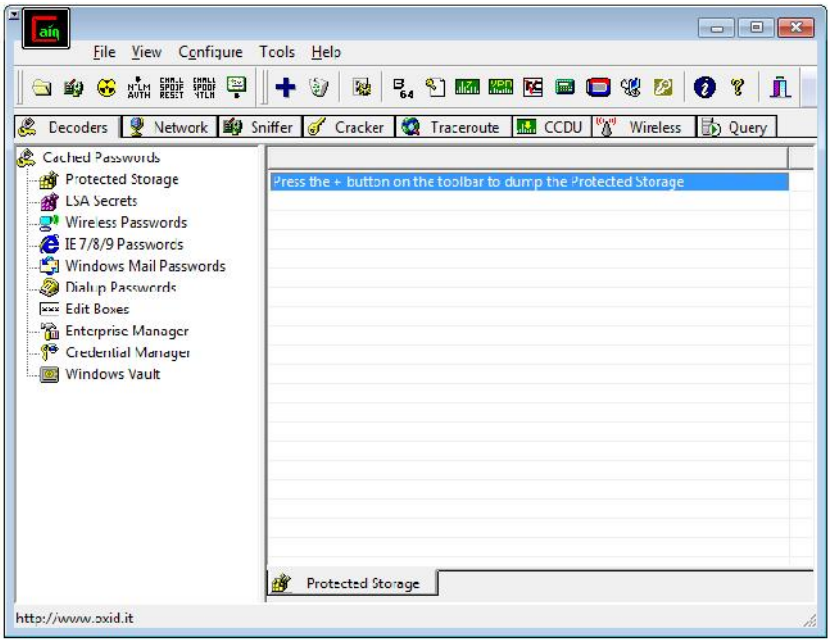
Die Verwendung des Skripts ist recht einfach. Führen Sie folgenden Befehl aus:

```
./discover.sh
```

Wir kommen gleich auf die Verwendung dieses Tools zu Testzwecken zu sprechen. Für den Moment soll die Installation dieser zusätzlichen Tools genügen. Sollten wir im Laufe dieses Buchs weitere Tools benötigen, so wird deren Installation dann beschrieben, wenn das Programm benötigt wird.

1.1.2 Windows als Penetration-Plattform

Kali Linux stellt Ihnen eine schier unüberschaubare Vielfalt an Programmen zur Verfügung, deren Stärken insbesondere in der Analyse von Linux-basierten Komponenten und Diensten liegen. Aber manchmal hat man Windows-spezifische Aufgaben zu lösen.



Mit Cain & Abel können Sie verlorene Passwörter zurückgewinnen, indem Sie das Netzwerk scanen, verschlüsselte Passwörter knacken und Protokolle analysieren.

Sie sollten daher auf Ihrem Windows-System folgende Tools installieren:

- Metasploit
- Nessus bzw. Nexpose
- Cain & Abel
- Nmap für Windows
- PowerSploit
- Firefox-Add-ons (Web Developer, Tamper Data, Foxy Proxy und User Agent Switcher)
- Wireshark