BRAIN-MEDIA.DE

PROFESSIONELLES INTERNET- UND OPEN-SOURCE-KNOW-HOW

Holger Reibold

Nmap kompakt

Gratis! Zwei E-Books zum Security Scanning zum Download

Security.Edition

Praxiseinstieg in die Netzwerkerkennung und das Security Scanning

Holger Reibold

Nmap kompakt

Alle Rechte vorbehalten. Ohne ausdrückliche, schriftliche Genehmigung des Verlags ist es nicht gestattet, das Buch oder Teile daraus in irgendeiner Form durch Fotokopien oder ein anderes Verfahren zu vervielfältigen oder zu verbreiten. Dasselbe gilt auch für das Recht der öffentlichen Wiedergabe. Der Verlag macht darauf aufmerksam, dass die genannten Firmen- und Markennamen sowie Produktbezeichnungen in der Regel marken-, patent- oder warenrechtlichem Schutz unterliegen.

Verlag und Autor übernehmen keine Gewähr für die Funktionsfähigkeit beschriebener Verfahren und Standards.

© 2015 Brain-Media.de

Herausgeber: Dr. Holger Reibold

Umschlaggestaltung: Brain-Media.de

Satz: Brain-Media.de

Coverbild: U5 / photocase.de

Korrektur: Theresa Tting

Inhaltsverzeichnis

Vorwort

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.

Neben dem theoretischen Wissen um die Relevanz des Penetration Testing benötigten Sie natürlich auch ein geeignetes Werkzeug. Mit Nmap steht Ihnen ein Klassiker zur Verfügung, der in jeden Admin-Werkzeugkasten gehört. Nmap (Network Mapper) ist von Haus aus ein Werkzeug für die Ermittlung von Netzwerkkomponenten und Diensten sowie der Auditierung.

Das Programm unterstützt Administratoren bei der Inventarisierung, dem Verwalten von Services und dem Monitoring von Services und Hosts. Nmap verwendet dabei IP-Pakete in einer neuen Art und Weise, um die Verfügbarkeit und Erreichbarkeit zu prüfen. Dabei kann der Netzwerk-Mapper verschiedenste Informationen von den gefundenen Hosts ermitteln.

Doch damit nicht genug: Nmap kann auf allen relevanten Betriebssystemen ausgeführt werden, insbesondere unter Mac OS X, Linux und Windows. Die klassische Ausführung erfolgt dabei auf der Konsole. Alternativ steht Anwendern mit Zenmap eine komfortable GUI zur Verfügung. Mit Ncat steht Ihnen ein weiterer Helfer zur Verfügung, mit dem Sie Daten transferieren, umleiten und debuggen können. Wenn Sie die Scan-Ergebnisse vergleichen wollen, greifen Sie zu Ndiff. Und dann steht Ihnen mit Nping ein weiteres Hilfsprogramm für das Generieren von Paketen und der Antwortanalyse zur Verfügung.

In diesem Einstieg lernen Sie die wichtigsten Funktionen von Nmap kennen. Bleibt mir nur noch, Ihnen viel Spaß und Erfolg beim Einstieg in die Welt der Netzwerkermittlung und dem Security Scanning zu wünschen!

Herzlichst,

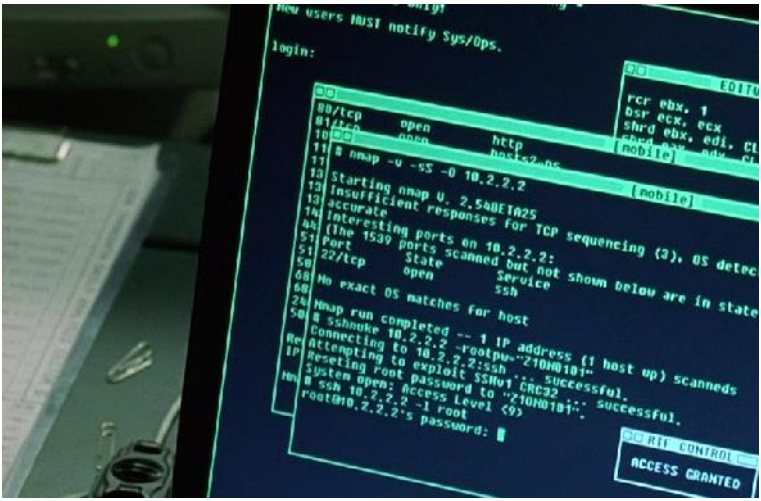
Holger Reibold

(Oktober 2015)

1 Nmap – der Einstieg

Ohne Computer, ohne Netzwerke, ohne Internet und ohne mehr oder minder aufwändige Server-Anwendungen ist unser Alltag kaum mehr vorstellbar. Die Computer- und Netzwerktechnik ist allgegenwärtig, sei es am Arbeitsrechner, im Handy, industriellen Produktionsmaschinen oder dem Auto. Und dieser Trend wird sich vorsetzen und weiter verstärken, bis jedes scheinbar noch so unwichtige Teil unseres Lebens in irgendeiner Weise vernetzt ist.

Die Computertechnik kommt längst nicht mehr nur in technologisch geprägten Unternehmen zum Einsatz, sondern kommt selbst in kleinen Schreinereien oder in jedem Müllauto der städtischen Müllabfuhr zur Müllerfassung zum Einsatz. Auch in unseres Privatleben wird die Technik immer weiter vordringen: Abgesehen von der allgemeinen Internet- und Smartphone-Nutzung denke man nur an das Stichwort Smart Home, das vernetzte Zuhause.

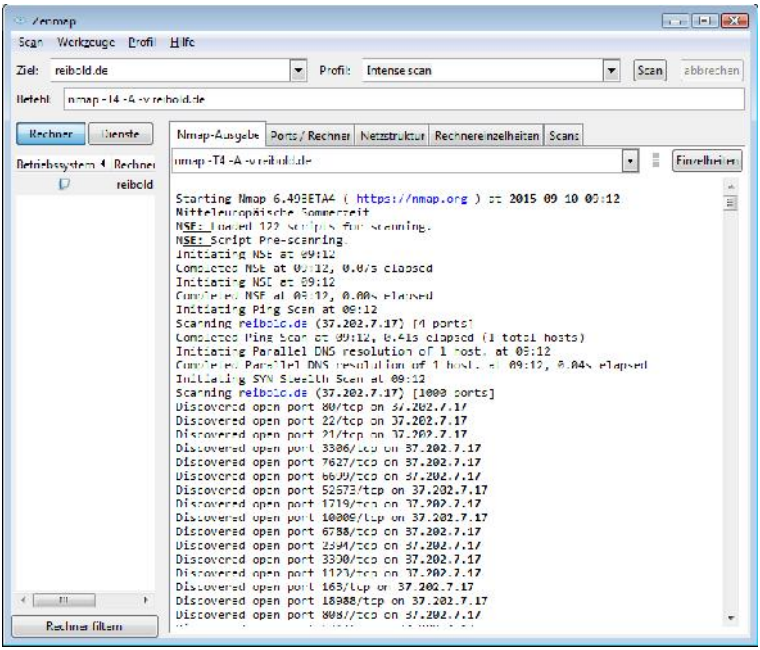


Starker Auftritt: Nmap in *Matrix Reload*.

Die Computertechnik bringt uns im Alltag viele Vorteile, aber je intensiver wir sie nutzen und um so mehr wir uns von ihr abhängig machen, umso angreifbarer sind

wir. Der Preis für die Produktivitätsgewinn und die Abhängigkeit ist hoch: Fallen kritische Systeme aus oder werden Daten zerstört oder entwendet, belaufen sich die Schäden oftmals in Dimensionen, die auch ein solides Unternehmen schnell ins Wanken bringen können.

Für jeden Betreiber von kritischen Computer- und Netzwerkkomponenten ist es daher unverzichtbar, die Sicherheit der Systeme zu prüfen, Schwachstellen zu identifizieren, um diese dann im nächsten Schritt zu schließen. Auf der Suche nach Schwachstellen und möglichen Angriffspunkten sind die Ports der zweite wichtige Ansatzpunkt. Um mehr über die Ports, deren Verwendung und deren Status zu erfahren, benötigen Sie einen Portscanner. Der Klassiker unter diesen Werkzeugen ist Nmap. Aber Nmap kann noch weit mehr.



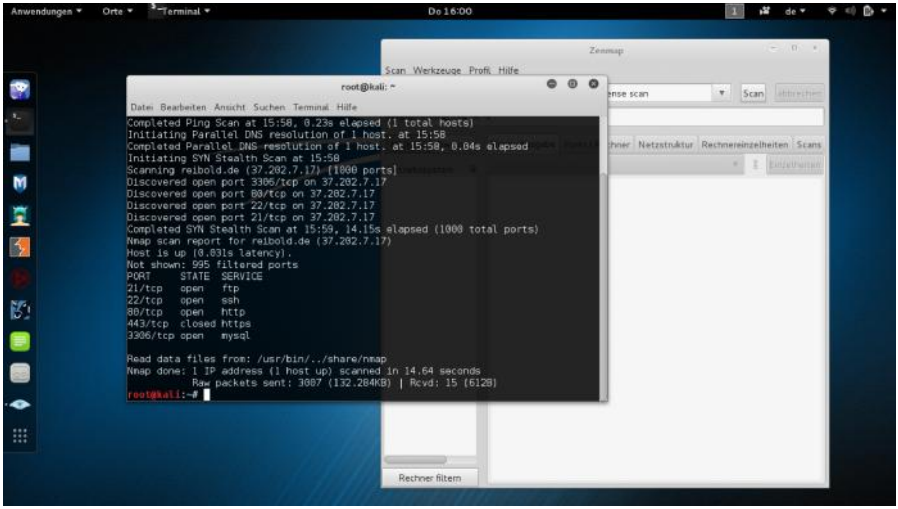
Der Einsatz der Nmap-GUI Zenmap unter Windows.

Anfang September 1997 veröffentlichte Gordon “Fyodor” Lyon die erste Version des Security Scanners Nmap. Damals bestand das Programm gerade einmal aus drei Dateien mit einer gesamten Code-Länge von 2.000 Zeilen. Die erste Version unterstützt lediglich Linux-Betriebssysteme.

Angesicht des holprigen Starts war nicht abzusehen, dass Nmap einmal der populärste Network Security Scanner werden würden (auch dank einer starken Community). Im Laufe der Jahre hat Nmap funktional stark zugelegt und es kamen verschiedene erweiterte Funktionen wie die Remote-Betriebssystemerkennung und die Nmap Scripting Engine hinzu.

Nmap kam auch in einigen weltweit erfolgreichen Filmen zum Einsatz, beispielsweise in *Matrix Reloaded*, das *Bourne Ultimatum* und in *Die Hard Teil 4*. Auch in dem deutschen Cyber-Thriller *Who Am I - Kein System ist sicher* hat Nmap einen Gastauftritt.

Nmap ist so konzipiert, dass das Programm schnell große Netzwerke scannen kann, aber auch einzelne Hosts genau unter die Lupe nimmt. Dabei ist Nmap nichts für schwache Nerven: Das Programm unterstützt mehr als 100 Kommandozeilenoptionen. Das dürfte selbst für routinierte Netzwerk-Gurus mehr als genug sein.



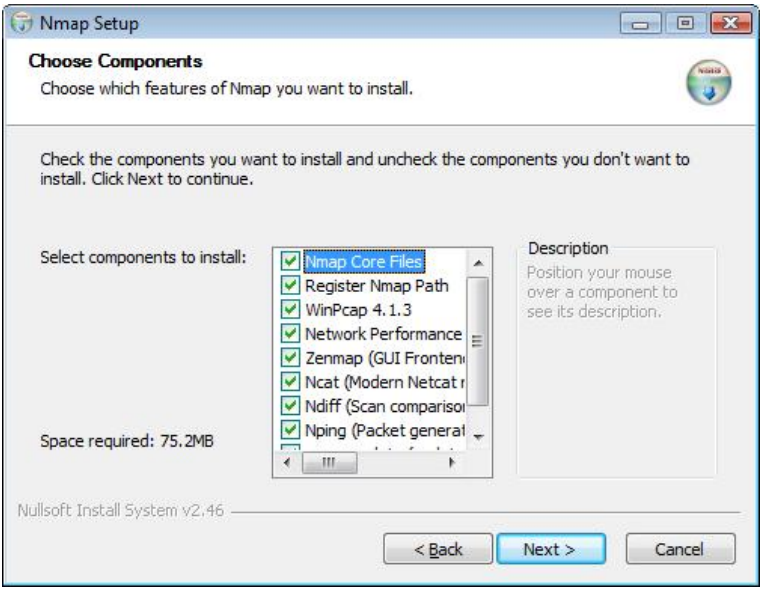
Ein Muss für Penetration Tester: Kali Linux.

1.1 Nmap in Betrieb nehmen

Bevor Sie in den Genuss der vielen Möglichkeiten gelangen, die Ihnen Nmap bietet, müssen Sie das Programm in Betrieb nehmen. Sicherheitsexperten und Penetration Tester greifen meist zu Kali Linux, eine spezielle Linux-Distribution, die Hunderte Tools für das Testen von Infrastrukturkomponenten enthält.

In Kali Linux sind (natürlich) auch Nmap und die GUI Zenmap vorinstalliert. Die Konsolenvariante starten Sie einfach im Terminal. Auch Zenmap greifen Sie über das *Anwendungen*-Menü *Informationsbeschaffung* > *Zenmap* zu. Wir kommen in Kapitel 6 detailliert auf Zenmap zu sprechen.

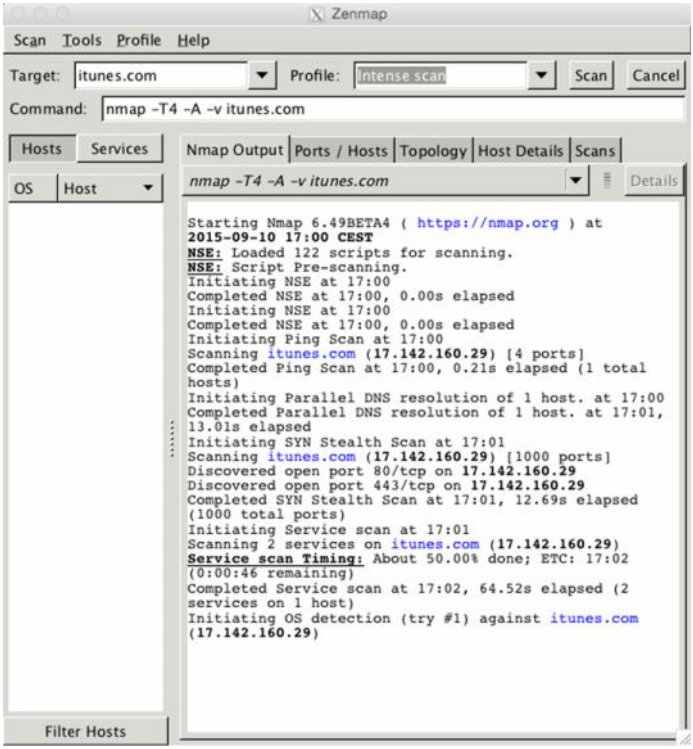
Sie können Nmap natürlich auch auf jedem anderen Linux-Betriebssystem installieren, sofern es dort nicht vorinstalliert ist. Der einfachste Weg: Sie greifen zum Paketmanager des jeweiligen Betriebssystems. Alles andere ist einfach. Den Umweg über das manuelle Installieren können Sie sich in der Regel schenken.



Die Installation von Nmap unter Windows.

Die Inbetriebnahme von Nmap unter Windows ist kinderleicht. Laden Sie sich einfach von der Projekt-Site (*https://nmap.org/download.html*) das aktuelle Installationsprogramm herunter. Diesem Buch liegt Version 6.49 zugrunde. Das zugehörige Installationspaket trägt die Bezeichnung *nmap-6.49-setup.exe*. Starten Sie das Installationsprogramm und folgen Sie den Anweisungen am Bildschirm. In der Regel können Sie einfach immer mit *Next* einen Schritt nach dem anderen abarbeiten. Das Interessante an der Windows-Version: Neben der Konsolenvariante und den verschiedenen oben genannten Tools kann das Installationsprogramm in der Windows-Registry verschiedene Einstellungen bearbeiten, um die Scan-

Performance zu optimieren. Außerdem ist ein Update-Mechanismus verfügbar, der im Bedarfsfall architekturunabhängige Dateien aktualisieren kann.



Zenmap unter Mac OS X.

Unter Penetration Testern ist Mac OS X aufgrund seiner hohen Stabilität eine beliebte Plattform. Auch hier ist die Inbetriebnahme einfach. Einzige Voraussetzung: Die Zenmap-Komponenten setzt eine bestehende X11-Installation voraus. Anschließend können Sie das DMG-Paket von der Projekt-Site herunterladen und ausführen. Da das Paket von dem Betriebssystem als unsicher klassifiziert wird, müssen Sie zunächst die *Crtl*-Taste drücken, dann die Installationsdatei markieren und mit dem Befehl *Öffnen* die Installation starten. Folgen Sie anschließend den Anweisungen am Bildschirm. Nmap ist anschließend über das Terminal verfügbar, die Nmap-GUI Zenmap finden Sie unter *Programme*.

1.2 Erste Schritte mit Nmap

Nmap stammt wie bereits erwähnt ursprünglich aus dem Linux-Umfeld. Daher wird es Sie nicht weiter verwundern, dass der Scanner üblicherweise auf der Konsole verwendet wird. Die Ausführung des Netzwerk-Analysewerkzeugs und Sicherheits-/Port-Scanners erfolgt nach diesem Schema:

```
nmap [ <Scan-Typ>...] [ <Optionen> ] { <Ziel-Spezifikation> }
```

Nmap gibt dabei eine Liste der gescannten Hosts inklusive verschiedener Zusatzinformationen aus. Welche Zusatzinformationen dies sind, ist von den verwendeten Optionen und natürlich von den Zielen abhängig. Die Scan-Ergebnisse werden in Tabellenform ausgegeben. Dort werden konkret der Port und das Protokoll sowie dem Dienstnamen und der Zustand aufgeführt. Mögliche Zustände sind:

- offen
- gefiltert
- geschlossen
- ungefiltert

Die Statusangaben werden durch den jeweiligen englischsprachigen Begriff angezeigt, also *open*, *filtered*, *closed* und *unfiltered*.

Was bedeuten diese Statusinformationen nun konkret? Der Status *offen* bedeutet, dass auf dem Port des Zielrechners eine Anwendung auf eingehende Verbindungen/Pakete lauscht. Dabei handelt es sich oftmals um webbasierte Anwendungen, die über Port 80 und 443 angesprochen werden.

Der Status *gefiltert* zeigt an, dass eine Firewall, ein Filter oder ein anderer Dienst den Port blockiert. In einem solchen Fall kann Nmap nicht in Erfahrung bringen, ob der Port geschlossen oder doch offen ist.

Auf geschlossenen Ports wird keine Anwendung ausgeführt, die auf eingehende Requests wartet. Dann gibt es noch den Status *ungefiltert*. Kann Nmap nicht feststellen, ob es sich um einen offenen oder geschlossenen Port handelt, wird er als *ungefiltert* klassifiziert.

Gelegentlich begegnen Sie auch den Zustandskombinationen *offen|gefiltert* und *geschlossen|gefiltert*. Diese Statusmeldungen zeigen an, dass Nmap nicht feststellen kann, in welchem der beiden Zustände sich ein Port befindet.

Ob mit der Port-Tabelle auch weitere Informationen wie die Software-Version ausgegeben werden, ist von der verwendeten Scan-Konfiguration abhängig. Auch das verwendete Betriebssystem, der Gerätetyp und die MAC-Adresse können mit Nmap abgerufen werden.

Besonders bequem ist die Scan-Konfiguration mit Hilfe von Zenmap. Wenn Sie einen intensiven Scan (intense scan) ausführen, verwendet Nmap folgende Konfiguration:

```
nmap -T4 -A -v server.de
```

In diesem ersten Beispiel kommen zwei wichtige Optionen zum Einsatz: *-T4* sorgt für eine schnellere Ausführung, *-A* für die Betriebssystem- und Versionserkennung, Script-Scanning und Traceroute.

Wenn Sie Nmap ohne irgendeine Argument ausführen, gibt das Programm die Hilfe aus, der Sie wichtigste Informationen entnehmen können. In diesem einführenden Kapitel werfen wird einen kurzen Blick auf die Argumente, die Sie kennen sollten. Im weiteren Verlauf dieses Einstiegs werden wir dann einen genaueren Blick auf die verschiedenen Optionen werfen.

Eine zwingende Angabe für eine Scan ist die Ziel-Spezifikation. Sie können dabei einen Host-Namen, eine IP-Adresse, ein Netzwerk oder ein Netzwerksegment angeben. Oben haben Sie bereits ein Beispiel kennengelernt. Alternative Argumente sind beispielsweise folgende:

```
192.168.0.1
```

```
10.0.0-255.1-254
```

```
server.de/24
```

```
scanme.nmap.org
```

Wenn Sie neu sind in der Welt der Netzwerk- und Sicherheitsscanner, sollten Sie auf keinen Fall Ihre aktuellen Produktivitätssysteme unter Beschuss nehmen. Denn noch wissen Sie ja garnicht, welchen Schaden Sie womöglich mit der Ausführung einer bestimmten Konfiguration anrichten können. Das Nmap-Entwicklerteam stellt Ihnen daher einen eigenen Server zur Verfügung, den Sie gefahrenlos unter die Lupe nehmen können:

```
scanme.nmap.org
```

Wenn Sie ein wenig Erfahrung mit Nmap gesammelt haben, können Sie auch eine lokale Testumgebung aufsetzen und damit beispielsweise eigene kritischen Infrastrukturkomponenten abbilden und diese dann mit Nmap unter die Lupe nehmen (siehe Anhang B).

Anstelle einer IP-Adresse oder eines ganzen Netzwerksegments können Sie auch eine Liste mit Hostnamen und Netzwerken verwenden. Die hierfür zuständige Option:

```
-iL <dateiname>
```

Um eine zufällige Auswahl von Zielen zu scannen, verwenden Sie folgendes Argument:

```
-iR <hosts>
```

Sie können außerdem Hosts und Netzwerke explizit vom Scannen ausnehmen. Dabei können Sie die Hosts einzeln oder in Form einer Liste angeben. Auf diesem Weg können Sie gezielt bestimmte Systeme aus einem Scan-Vorgang ausnehmen:

```
--exclude <host1[,host2][,host3],...>
```

```
--excludefile <ausschlussdatei>
```

Ein weiteres Highlight von Nmap sind die umfangreichen Möglichkeiten zur Host-Ermittlung. Um die Liste der Ziele auszugeben, verwenden Sie das Argument *-sL*.

Um den Ping-Port-Scan zu deaktivieren, verwenden Sie die Option *-sn*. Sie können die Host-Ermittlung deaktivieren. Dann geht Nmap davon aus, dass alle Hosts online sind. Das hierfür relevante Argument lautet *-Pn*. Sie können auch die DNS-Auflösung aktivieren bzw. deaktivieren. Das hierfür zuständige Argument sieht wie folgt aus:

```
-n/-R
```

Wollen Sie bestimmte DNS-Server für die Namensauflösung verwenden, spezifizieren Sie diese wie folgt:

```
--dns-servers <serv1[,serv2],...>
```

Um den Weg der Datenpakete zu verfolgen, verwenden Sie die Option *-traceroute*. Allerdings ist dabei zu beachten, dass nicht immer exakt der zurückgelegte Weg nachgebildet wird.

Auch für die Durchführung von Scans stehen Ihnen umfangreiche Steuer- und Konfigurationsmöglichkeiten zur Verfügung. Mit den folgenden Argumenten führen Sie TCP SYN-/Connect()-/ACK-/Window- und Maimon-Scans durch:

```
-sS/sT/sA/sW/sM
```

Eine UDP-Scan starten Sie mit folgender Option:

```
-sU
```

Mit Nmap können Sie auch TCP-Null-, FIN- und Xmas-Scans durchführen. Was das alles genau ist, erfahren Sie später.

```
-sN/sF/sX
```

Sie können auch TCP-Scan-Flags anpassen:

```
--scanflags <flags>
```

Wenn Sie mit Nmap einen SCTP INIT- oder COOKIE-ECHO-Scan durchführen wollen, verwenden Sie folgende Schalter:

```
-sY/sZ
```

Einen IP-Protokoll-Scan initiieren Sie wie folgt:

```
-sO
```

Um einen FTP-Bounce-Scan durchzuführen, verwenden Sie das folgende Argument:

```
-b <FTP Relay Host>
```

Nicht minder beeindruckend ist die Vielfalt an Möglichkeiten, die Ihnen Nmap für das Port-Spezifikation und die Scan-Reihenfolge zur Verfügung stellt. Um ledig einen bestimmten Port-Bereich zu scannen, geben Sie diesen wie folgt an:

```
-p <port-bereich>
```

Hier einige Beispiele:

```
-p24; -p1-65555; -p U:52,111,137,T:21-25,80,139,8080,S:9
```

Auch der Ausschluss von Ports ist möglich. Die entsprechende Spezifikation sieht wie folgt aus:

```
--exclude-ports <port-bereich>
```

Wenn Sie einen ersten Schnelldurchlauf starten wollen, verwenden Sie den Schnellmodus. Dabei werden weniger Ports als beim Standard-Scan durchgeführt:

```
-F
```

Um die angegebenen Ports anstelle einer zufälligen Reihenfolge der Reihe nach zu testen, verwenden Sie das folgende Argument:

```
-r
```

Sie können einen Scan-Vorgang auch einfach auf die am häufigsten verwendeten Ports beschränken:

```
--top-ports <Zahl>
```

Nmap bietet Ihnen verschiedenste Optionen für das Erkennen von Service und Versionen. Um die auf offenen Ports laufende Dienste und deren Versionen zu bestimmen, verwenden Sie folgendes Argument:

```
-sV
```

Wenn Sie sich für die Details eines Scan-Vorgangs interessieren, verwenden Sie folgendes Argument, das insbesondere für das Debugging interessant ist:

```
--version-trace
```

Oftmals interessiert man sich auch das Betriebssystem auf dem Zielsystem identifizieren. Die Betriebssystemerkennung aktivieren Sie mit folgendem Argument:

```
-O
```

Sie können die Betriebssystemerkennung auch auf vielversprechende Ziele beschränken:

```
--osscan-limit
```

Um das Betriebssystem aggressiver zu bestimmen, verwenden Sie folgendes Argument:

```
--osscan-guess
```

Sie können die Ausführung aus verschiedene Zeit- und Performance-Parameter definieren. Dabei wird der Wert Zeit in Millisekunden (ms), Sekunden (s), Minuten (m) oder Stunden (h) angegeben.

Was Sie bislang noch nicht wissen können: Nmap besitzt sogenannte Timing-Templates. Deren Ausführung bestimmen Sie mit folgendem Argument, wobei eine höherer Wert für eine schnellere Ausführung steht:

```
-T<0-5>
```

Sie können die minimale und maximale Größe von Hostgruppen bestimmen, die parallel geprüft werden:

```
--min-hostgroup/max-hostgroup <größe>
```

Den Timeout-Wert für die Host-Prüfung bestimmen Sie mit folgendem Argument:

```
--host-timeout <zeitspanne>
```

Die Zeitspanne zwischen zwei Tests bestimmen Sie wie folgt:

```
--scan-delay/--max-scan-delay <zeit>
```

Firewalls und Intrusion Detection-Systeme dienen dazu, unerwünschten Traffic in einem Netzwerk zu verhindern bzw. mögliche Attacken und deren Vorbereitungen zu erkennen. Dazu gehören auch Port-Scans, wie sie von Nmap durchgeführt werden. Auch hierfür stehen Ihnen verschiedene Konfigurationsparameter und Einstellungen zur Verfügumg. Sie können beispielsweise Pakete fragmentieren und den MTU-Wert bestimmen:

```
-f; --mtu <wert>
```

Um einen Scan mit einem Köder zu verbergen, verwenden Sie folgendes Argument:

```
-D <koeder1,koeder2...>
```

Nmap erlaubt auch das Spoofen, also Fälschen, der eigenen IP-Adresse:

```
-S <IP-Adresse>
```

Um eine spezifische Schnittstelle zu verwenden, bestimmen Sie diese mit folgendem Argument:

```
-e <interface>
```

Entsprechend können Sie auch den Port vorgeben:

```
-g/--source-port <port-nummer>
```

Auch wenn Nmap eigentlich kein Exploit-Werkzeug ist, um etwaige Schwachstellen zu testen, können Sie dennoch einen benutzerdefinierten Payload an die Pakete anhängen:

```
--data <hex string>
```

Sie können auch ASCII-Zeichenfolgen an die Pakete hängen:

```
--data-string <string>
```

Auch das Fälschen einer MAC-Adresse ist einfach:

```
--spoof-mac <mac-addresse/präfix/hersteller>
```

Sie können auch das Ausgabeformat bestimmen, in dem die Scan-Ergebnisse ausgegeben werden. Um die Ausgabe im Textformat oder im XML-Format zu erhalten, verwenden Sie folgende Argumente (die Ausgabe wird in die entsprechende Datei geschrieben:

```
-oN/-oX <datei>
```

Um das Scan-Ergebnis in allen drei wichtigen Formaten zu schreiben, verwenden Sie folgendes Argument:

```
-oA <ausgabedatei>
```

Um die Geschwätzigkeit der Ausgabe zu erhöhen, verwenden Sie folgende Option (wobei Sie diese mit *-vv* etc. weiter erhöhen können):

```
-v
```

Den Debug-Level können Sie mit folgendem Schalter erhöhen (auch hier können Sie diesem mit *-dd* etc. weiter erhöhen):

-d

Um die Anzeige lediglich auf offene Ports zu beschränken, verwenden Sie dieses Argument:

```
--open
```

Sie können auch alle gesendeten und empfangenen Pakete anzeigen:

```
--packet-trace
```

Um einen unterbrochenen Scan-Vorgang fortzusetzen, verwenden Sie folgende Option:

```
--resume <dateiname>
```

Nmap kann die XML-Aufgabe auch mit Angabe eines XSL-Stylesheets in ein HTML-Dokument schreiben:

```
--stylesheet <pfad/URL>
```

Zum Abschluss dieses einleitenden Kapitels schauen wir uns zwei einige weitere Argumente an. Wenn Sie das IPv6-Scanning aktiveren wollen, verwenden Sie dieses Argument:

```
-6
```

Um die Betriebsystem- und Versionserkennung, das Skript-Scanning und Traceoute auf einen Schlag zu verwenden, führen Sie Nmap mit diesem Argument aus:

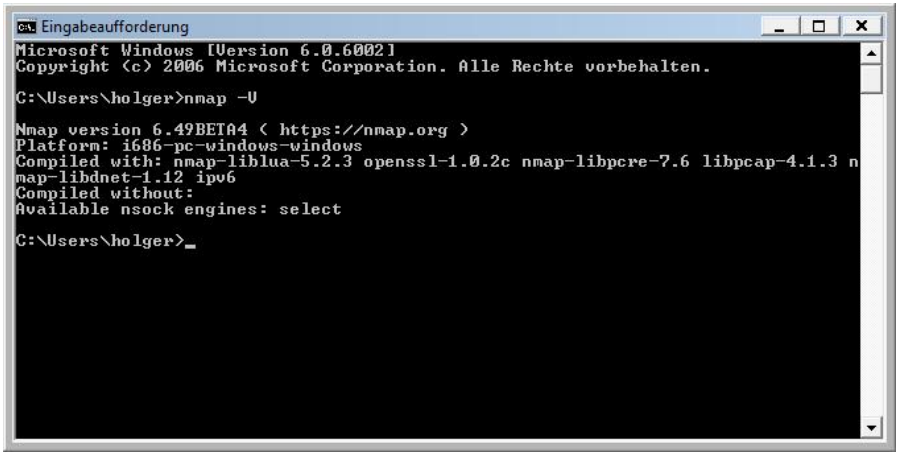
```
-A
```

Sie können auch ein speziellem Verzeichnis für die Nmap-Daten angeben:

```
--datadir <verzeichnisname>
```

Um anzunehmen, dass der Benutzer die vollständigen Rechte besitzt, geben Sie Nmap das folgende Argument mit auf den Weg:

```
--privileged
```



Die Ausgabe der verwendeten Programmversion mit dem Argument *-V*.

Ein letztes Argument sollten Sie für den Einstieg noch kennen, die Versionsausgabe:

```
-V
```

Damit haben Sie einen ersten Überblick über das, was Sie mit Nmap anstellen können. Sie haben auch einen ersten Eindruck erhalten, wie flexibel Sie bei der Verwendung der Optionen sind, die Sie ja miteinander kombinieren können. Im weiteren Verlauf dieses Buches werden wir diese Möglichkeiten weiter vertiefen.

Index

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

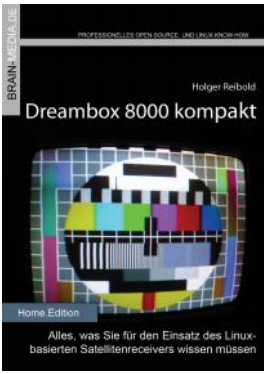
V

W

X

Z

Weitere Brain-Media.de-Bücher



Dreambox 8000 kompakt

Die Dreambox 8000 stellt ihre Vorgänger allesamt in den Schatten. Was Sie alles mit der Dreambox 8000 anfangen können, verrät Ihnen die Neuauflage unseres Dreambox-Klassikers. Mit einem Vorwort des Dream Multimedia-Geschäftsführers Karasu.

Umfang: 450 Seiten plus CD
ISBN: 978-3-939316-90-9
Preis: 29,80 EUR

X-Plane 10 kompakt

Der Klassiker unter den Flugsimulatoren geht in die zehnte Runde. Viele neue Funktionen und verbessertes Handling warten auf die Anwender. Kein Wunder also, dass die Fangemeinde wächst und wächst. Unser Handbuch beschreibt alles, was Sie für das Fliegen mit X-Plane wissen sollten.

Umfang: 430 Seiten
ISBN: 978-3-939316-96-1
Preis: 24,80 EUR

Audacity 2.0 kompakt

Audacity ist zweifelsohne das beliebteste freie Audioprogramm. Vom anfänglichen Geheimtipp hat sich der Editor zum Standard für die Aufzeichnung und Bearbeitung von Audiodaten gemausert. Das Vorwort steuert der ehemalige Core-Entwickler Markus Meyer bei.

Umfang: 306 Seiten
ISBN: 978-3-95444-027-6
Preis: 24,80 EUR

Evernote kompakt

Bei der alltäglichen Informationsflut wird es immer schwieriger, Wichtiges von Unwichtigem zu trennen, Termine und Kontakte zu verwalten. Mit Evernote können Sie diese Flut bändigen und Ihren Alltag optimieren. "Evernote kompakt" vermittelt das notwendige Know-how für den Einsatz von Evernote auf Ihrem Desktop, Smartphone und online.

Umfang: 320 Seiten
ISBN: 978-3-95444-098-6
Preis: 22,80 EUR

Fire TV kompakt

Mit Fire TV hat Amazon eine tolle kleine Box für das Online-Entertainment auf den Markt gebracht, die für wenig Geld die gesamte Palette der Internet-basierten Unterhaltung abdeckt. In diesem Handbuch erfahren Sie, was Sie alles mit der kleinen Box anstellen können.

Umfang: 182 Seiten
ISBN: 978-3-95444-172-3
Preis: 16,80 EUR

Magento SEO kompakt

Magento ist die Standardumgebung für den Aufbau eines Online-Shops. Doch damit Sie mit Ihren Shop-Angebot auch im Internet wahrgenommen werden, müssen Sie ein wenig die Werbetrommel rühren und den Shop für Google & Co. optimieren. Mit wenigen Handgriffen machen Sie Ihren Online-Shop SEO-fest und maximieren Ihre Verkäufe.

Umfang: 100 Seiten
ISBN: 978-3-95444-098-6
Preis: 14,80 EUR

Wireshark kompakt

Wireshark ist der mit Abstand beliebteste Spezialist für die Netzwerk- und Protokollanalyse. In diesem Handbuch lernen Sie, wie Sie mit dem Tool typische Administratoraufgaben bewältigen. Das Buch beschränkt sich dabei auf die wesentlichen Aktionen, die im Admin-Alltag auf Sie warten, und verzichtet bewusst auf überflüssigen Ballast.

Umfang: 170 Seiten
ISBN: 978-3-95444-176-1
Preis: 16,80 EUR

Scribus 1.5 kompakt

Scribus ist längst ein ebenbürtiger Gegenspieler von InDesign & Co. In unserem Handbuch erfahren Sie alles, was Sie für den erfolgreichen Einstieg wissen müssen.

460 Seiten Praxis-Know-how. Dazu viele Tausend ClipArts und Schriften zum kostenlosen Download.

Umfang: 460 Seiten
ISBN: 978-3-95444-124-2
Preis: 27,80 EUR

Weitere Titel in Vorbereitung

Wir bauen unser Programm kontinuierlich aus. Aktuell befinden sich folgende Titel in Vorbereitung:

- Android Forensik
- Android Security
- Alfresco 5.0 kompakt
- WordPress 4.x kompakt
- Smart Home kompakt
- Das papierlose Büro
- wa3f kompakt
- SmoothWall kompakt

Plus+

Plus+ − unser neues Angebot für Sie ... alle E-Books im Abo. Sie können 1 Jahr alle Brain-Media-Bücher als E-Book herunterladen und diese auf Ihrem PC, Tablet, iPad und Kindle verwenden − und das ohne irgendwelche Einschränkungen. Das Beste: Plus+ schließt auch alle jene Bücher ein, die in diesem Jahr noch erscheinen.

Und das zum Sonderpreis von 29 Euro! Ein unschlagbares Angebot!

Auf unserer Website steht ein detaillierter Überblick aller Titel im PDF-Format zum Download bereit (ca. 6,2 MB), der bereits zu Plus+ gehörende Titel aufführt und die in naher Zukunft hinzukommen.