Penetration Testing mit Metasploit

Eine praktische Einführung

von
Frank Neugebauer

1. Auflage

Thematische Gliederung:

Computersicherheit

dpunkt.verlag 2011

Verlag C.H. Beck im Internet:
www.beck.de
ISBN 978 3 89864 739 7

Inhaltsverzeichnis: Penetration Testing mit Metasploit – Neugebauer

2 Die Testumgebung

Wenn man sich ausgiebig mit den Möglichkeiten von Metasploit beschäftigen möchte, ist es sinnvoll, sich eine Testumgebung einzurichten. Wie bereits erwähnt, ist das Framework auf verschiedenen Plattformen nutzbar. Wir werden hier zumindest die Betriebssysteme Windows und Linux etwas näher betrachten. Außerdem bietet es sich an, verschiedene virtuelle Umgebungen einzurichten, um die Wirkung auf den verschiedenen Plattformen auszutesten.

Derzeit gibt es einige kostenlose Produkte, um virtuelle Server oder Workstations in einem Netzwerk darzustellen. So kann z.B. der Microsoft Virtual Server 2005 R2 kostenfrei von der Microsoft-Webseite[1] bezogen werden. Er bietet eine umfassende Kompatibilität mit x86-Gastbetriebssystemen und x64-Hostunterstützung bzw. eine individuelle Zuweisung von CPU-und Arbeitsspeicherressourcen. Virtuelle Computer werden als VHD-Datei in portierbaren virtuellen Festplatten eingekapselt. Die Konfiguration, Versionsverwaltung und Bereitstellung von Ressourcen ist somit optimal gewährleistet.

Als weitere Möglichkeit wird hier auf das Virtual-Box-Projekt[2] verwiesen. Es bietet ebenfalls eine Möglichkeit, virtuelle Umgebungen im Unternehmen und im privaten Umfeld einzurichten. Derzeit läuft es unter den Betriebssystemen Windows, Linux, Mac OS X und Open Solaris. Es wird ständig in der Community weiterentwickelt und entspricht professionellen Standards.

Als dritte Möglichkeit wird hier der VMware-Server vorgestellt. Mit seiner Hilfe wird im Weiteren die Installation und Einrichtung auf einem Linux-System beschrieben. Der VMware-Server unterstützt Multiprozessorsysteme (Intel64 und AMD64) und ist kostenlos nach einer Registrierung beim Hersteller[3] zu beziehen. Folgendes System wird nun als Testumgebung installiert:

Hardware: Intel Core 2 Quad Q8300, 4 GB RAM, 1 TB Festplatte
Software: Ubuntu 8.0.4.4 Server 64 bit, VMware-Server Version 2.0.2 | 203138

1. *http://www.microsoft.com/germany/virtualserver/uebersicht/default.mspx*
2. *http://www.virtualbox.org/*
3. *http://www.vmware.com*

2.1 VMware-Server 2.0.2 installieren

Um den VMware-Server von der Herstellerseite herunterladen zu können, ist es zunächst notwendig, sich zu registrieren. Nutzen Sie dazu die folgende URL:

http://www.vmware.com/de/products/server/

Nach der Registrierung erhalten Sie eine E-Mail mit den Lizenzschlüsseln und werden auf einen Server weitergeleitet, der die entsprechenden Ressourcen bereitstellt. Laden Sie hier die folgende Datei herunter und speichern Sie sie im Verzeichnis `/home/user/`.

```
VMware-server-2.0.2-xx.x86_64.tar.gz
```

Der Dateiname kann je nach Version variieren. Sollten Sie ein 32-Bit-Betriebssystem bevorzugen, so laden Sie eine entsprechende Installationsdatei herunter.

Nach der Registrierung können Sie sich jederzeit mittels der E-Mail-Adresse und Ihrem Passwort auf folgender Webseite einloggen und die zugeteilten Lizenzen einsehen bzw. weitere Programme und Module herunterladen:

https://www.vmware.com/tryvmware/activate_login.php

Nachdem die Datei auf Ihrem Linux-System heruntergeladen wurde, loggen Sie sich als `root` ein und installieren den VMware-Server mit den folgenden Kommandos:

```
sudo apt-get install linux-headers-`uname -r` build-essential xinetd
cd /home/user
tar xvfz VMware-server-*.tar.gz
cd vmware-server-distrib
sudo ./vmware-install.pl
```

Listing 2–1 *Installation von VMware-Server 2.0.2*

Während der Installation werden viele Fragen gestellt. Bitte lesen Sie sie aufmerksam durch. In eckigen Klammern [] werden jeweils die Defaultwerte angegeben. In den meisten Fällen können diese einfach mit einem ENTER bestätigt und übernommen werden. Sie können jederzeit die Konfiguration mittels des Kommandos `/usr/bin/vmware-config.pl` erneut durchführen bzw. Änderungen an der aktuellen Konfiguration vornehmen.

Nach erfolgreicher Installation kann man den VMware-Server mit folgenden Kommandos starten, stoppen und den derzeitigen Status abfragen:

```
/etc/init.d/vmware start
/etc/init.d/vmware stop
/etc/init.d/vmware status
```

Listing 2–2 *VMware starten und stoppen*

Der VMware-Server kann nun über einen Webbrowser lokal, aber auch remote konfiguriert und verwaltet werden. Hierzu sind standardmäßig folgende URLs aufzurufen:

http://<IP ADRESSE >:8222 oder *https://<IP ADRESSE>:8333*

Damit das Webinterface mit den verschiedenen Browsern problemlos zusammenarbeitet, sollten die entsprechenden Brower-Plug-ins vom Server auf das entsprechende System kopiert werden. Sie finden die zugehörigen Dateien im folgenden Verzeichnis auf dem Linux-Server:

`/usr/lib64/vmware/webAccess/tomcat/apache-tomcat-6.0.16/webapps/ui/plugin/`

Nutzen Sie die `*.xpi`-Dateien für den Firefox-Browser bzw. `*.exe` für den Internet Explorer.

- `vmware-vmrc-linux-x64.xpi`
- `vmware-vmrc-linux-x86.xpi`
- `vmware-vmrc-win32-x86.exe`
- `vmware-vmrc-win32-x86.xpi`

In Abbildung 2–1 wird die Login-Seite dargestellt. Verwenden Sie hier den bei der Installation angegebenen Nutzernamen und das entsprechende Passwort.

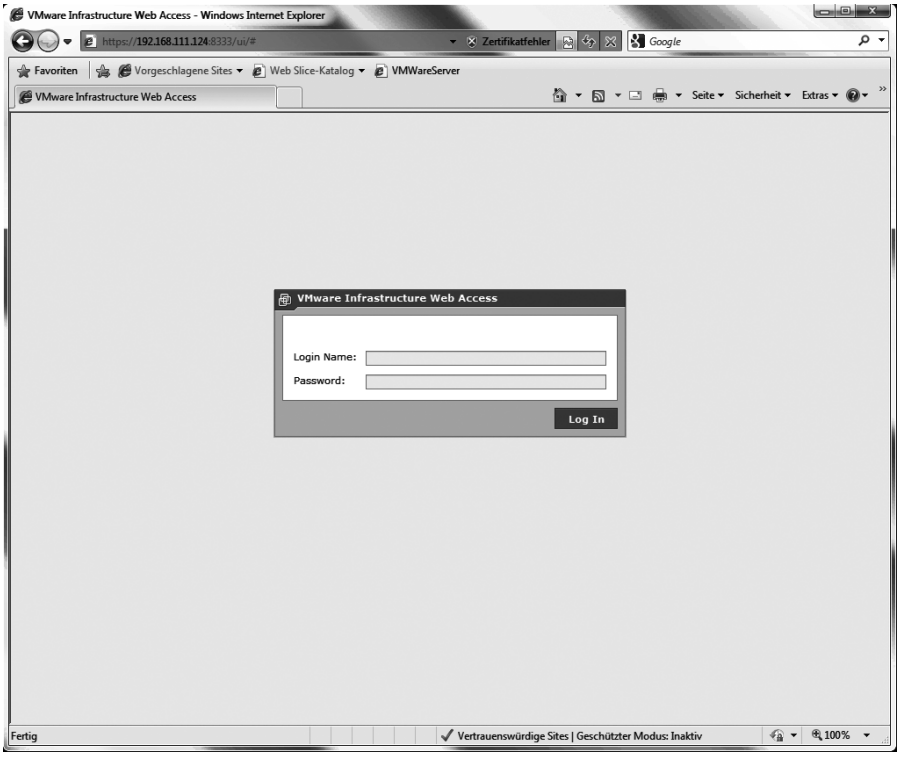

Abb. 2–1 *Webinterface-Login des VMware-Servers*

Mittels der aufgerufenen Oberflächen sind Sie nun in der Lage, virtuelle Maschinen zu erzeugen und zu verwalten.

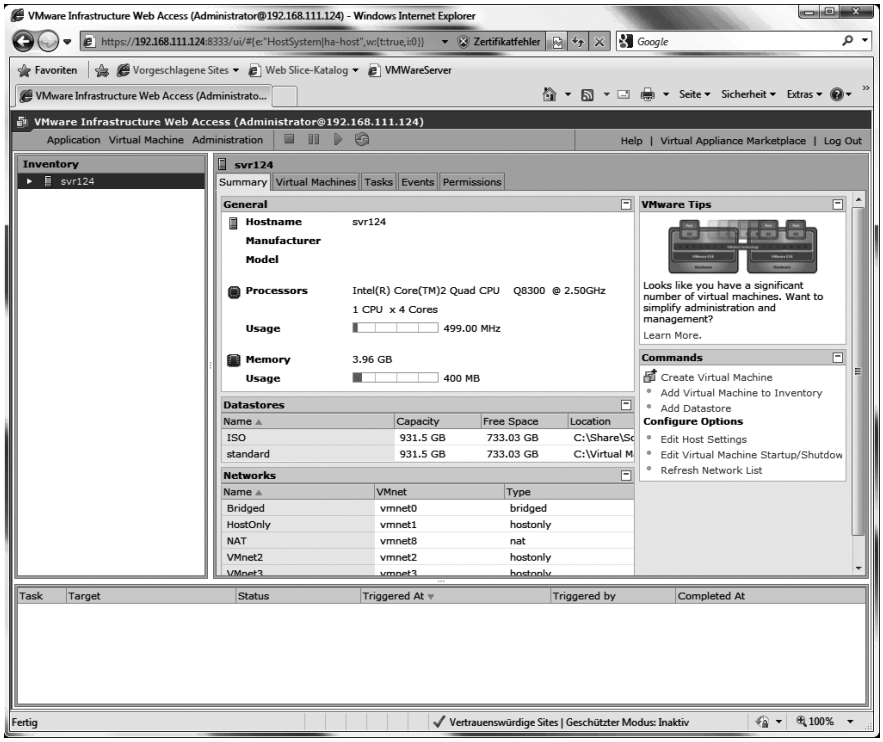

Abb. 2–2 *Administration des VMware-Servers*

2.2 Virtuelle Maschinen erstellen

Um unsere Tests an verschiedenen Systemen vornehmen zu können, sollten virtuelle Maschinen in ausreichender Anzahl erstellt werden. Haben Sie andere Produkte vom gleichen Hersteller (z.B. VMware Workstation, VMware Player) bereits genutzt, so besteht nun die Möglichkeit, auf bereits erstellte virtuelle Umgebungen zurückzugreifen und diese in den neuen Server zu übernehmen. Hierzu kopieren Sie die vorhandenen Dateien einfach in das während der Installation angelegte Verzeichnis. Wenn Sie die Defaulteinstellungen bei der Installation des Servers übernommen haben, sollte dafür der Ordner `/var/lib/vmware/Virtual Machines` bereitstehen.

Der Vorgang zur Erstellung der verschiedenen virtuellen Maschinen wird hier nicht näher erläutert. Bitte nutzen Sie bei offenen Fragen die umfangreiche Dokumentation, die Sie unter folgender URL finden können:

http://www.vmware.com/support/pubs/server_pubs.html

2.2.1 Windows XP mit Metasploit und Nmap

Die Installation von Metasploit auf einem Windows-XP-System gestaltet sich relativ einfach. Die Metasploit-Software steht auf der folgenden Webseite für die verschiedenen Betriebssysteme zum Download bereit:

http://www.metasploit.com/framework/download/

Laden Sie die Datei `Framework-3.x.x.exe` herunter und kopieren Sie sie auf Ihre virtuelle Maschine. Danach starten Sie die Installation und folgen den Anweisungen auf dem Bildschirm. Der Gestaltung Ihrer virtuellen Umgebungen sind natürlich keine Grenzen gesetzt. Installieren Sie z.B. weitere Tools, die Sie für die Durchführung der Tests benötigen. Um die Umgebungen später im »Eifer des Gefechts« nicht zu verwechseln, empfehle ich, diese mit verschiedenfarbigen Hintergründen zu versehen.

Neben dem Metasploit-Framework benötigen wir noch den Open-Source-Portscanner Nmap (Network Mapper). Das Werkzeug wird ständig erweitert und zeichnet sich vor allem durch die aktiven Techniken für OS-Fingerprinting aus (das Erkennen des eingesetzten Betriebssystems auf dem Zielhost). Das Tool ist sowohl bei Angreifern als auch bei Administratoren sehr beliebt, da es sehr effizient und zuverlässig arbeitet. In unseren Tests wird Nmap einen wichtigen Teil der Arbeit bei der Netzwerkdiagnose und Auswertung von Zielsystemen erledigen. Nicht zuletzt wird das Tool im Vulnerability-Scanner Nessus zur Erfassung offener Ports eingesetzt.

Nmap ist mittlerweile in der Version 5.51 erhältlich und kann über eine grafische Nutzeroberfläche (Zenmap GUI) oder über die Kommandozeile bedient werden. Laden Sie es von folgender Webseite herunter:

http://nmap.org/download.html

Die Installation gestaltet sich unter Windows recht einfach und sollte keine Hürde für uns darstellen.

Abbildung 2–3 zeigt die installierte Umgebung auf der Windows-XP-Plattform. Rechts sehen Sie die Verknüpfungen mit den drei wichtigen Komponenten:

- Nmap – Zenmap GUI
- Metasploit Console
- Cygwin Shell

In den nachfolgenden Kapiteln werden wir die installierten Tools ausgiebig nutzen und dann genauer darauf eingehen.

Abb. 2–3 *Windows-XP-Umgebung mit Metasploit*

2.2.2 Backtrack mit Nessus und NeXpose installieren

Backtrack ist *das* ultimative Tool für Penetrationstester und Administratoren. Es vereint viele Tools und Programme unter einer einheitlichen Oberfläche und ist als Live-DVD erhältlich. Die Version 4 der Software wurde im Januar 2010 veröffentlicht und setzt nun auf einem Ubuntu-System auf. Backtrack lässt sich direkt von der DVD starten, kann aber auch auf Festplatten bzw. auf USB-Sticks installiert werden. Es beinhaltet Softwaretools, die Sicherheitsvorkehrungen in Netzwerken umgehen, Daten ausspähen und Passworte knacken können. Somit kann bereits der Besitz oder Vertrieb strafbar sein, sofern die Absicht zur illegalen Nutzung nach § 202a StGB oder § 202b StGB besteht. Nach einer Entscheidung des Bundesverfassungsgerichts[4] sind diese Programme als Dual-Use-Software

einzustufen, sofern sie nach den Regeln eines Penetrationstests (siehe dazu auch Kapitel 4 eingesetzt werden.

Die Installation und Einrichtung in einer virtuellen Umgebung stellt kein großes Problem dar. Außerdem kann ein VMware-Image von folgender Webseite heruntergeladen werden:

http://www.backtrack-linux.org

Zunächst werden wir Backtrack 4 als virtuelle Maschine aufsetzen und dann die Vulnerability-Scanner Nessus und NeXpose in das System integrieren.

Backtrack 4 als virtuelle Maschine

Um Backtrack individuell anpassen zu können, werden wir es nun in einer virtuellen Umgebung installieren und dazu das offizielle ISO-Image nutzen. Laden Sie dazu die Datei `bt4-final.iso` von der o.g. Webseite herunter und speichern Sie sie im Data Storage Ihres VMware-Servers. Gehen Sie bei der Einrichtung der virtuellen Maschine wie folgt vor:

Nutzen Sie Web Access (siehe Abb. 2–1) und loggen Sie sich auf dem VMware-Server ein.

Erstellen Sie eine neue virtuelle Maschine mit *Virtual Machine – Create Virtual Machine*.

- Name: Backtrack 4, Datastore: standard
- Operating System: Linux operating system (Ubuntu 32bit)
- Size: *1024 MB*, Count: *1*
- Hard Disk: Create a new Virtual Disk
- Capacity: *30 GB* Location: *standard*
- Network Connection: *Bridged*, Connect at Power on: *Yes*
- Use an ISO Image, Image File: *bt4-final.iso*
- Don't Add a Floppy Drive
- Add a USB Controller
- Finish

Klicken Sie nun in den Bereich *Console* und starten Sie die virtuelle Maschine. Der Startbildschirm wird in Abbildung 2–4 dargestellt.

Nach der Bestätigung mit ENTER wird das System hochgefahren. Danach starten Sie die grafische Oberfläche mittels `startx` und führen das Installationsskript `install.sh` aus. Die Installation auf die Festplatte wird nun in sieben Schritten ausgeführt.

Um Probleme mit der Darstellung zu vermeiden, führen wir von der Konsole den Befehl `fix-splash` als `root` aus.

---

4. *http://www.bundesverfassungsgericht.de/entscheidungen/rk20090518_2bvr223307.html*

Abb. 2–4 *Startbildschirm bei der Backtrack-4-Installation*

Nach einem anschließenden Neustart des Systems erledigen wir die abschließenden Maßnahmen. Dabei stellen wir das Tastaturlayout auf *Deutsch* ein, konfigurieren das Netzwerk, führen ein Update der gesamten Distribution und der Tools aus und installieren die VMware-Tools.

Loggen Sie sich dazu zunächst als `root` mit dem Passwort `toor` ein und starten Sie erneut die grafische Oberfläche mittels `startx`.

Widmen wir uns zuerst der Netzwerkkonfiguration, um eine Verbindung ins Internet sicherzustellen. Wir haben bei der Installation der virtuellen Maschine die Netzwerkkarte auf *bridged* eingestellt. Dies werden wir später ändern. Zunächst soll es eine einfache Konfiguration gewährleisten. Befindet sich im Netzwerk ein DHCP-Server, können die Netzwerkeinstellungen von der Konsole mittels des Kommandos `dhclient` vorgenommen werden.

In Listing 2–3 wird die manuelle Konfiguration des Netzwerkes dargestellt. Nutzen Sie dabei die IP-Daten Ihres Netzwerks:

```
ifconfig eth0 192.168.111.130 netmask 255.255.255.0
route add default gw 192.168.111.1
echo "nameserver 192.168.111.1" >> /etc/resolv.conf
```

Listing 2–3 *Manuelle Netzwerkkonfiguration*

Nun sollte dem Zugang ins Internet nichts mehr im Weg stehen. Mit dem Kommando `nslookup www.google.de` prüfen wir, ob die Namen richtig aufgelöst werden.

```
Server:         192.168.111.1
Address:        192.168.111.1#53

Non-authoritative answer:
www.google.de   canonical name = www.google.com.
www.google.com  canonical name = www.l.google.com.
Name:   www.l.google.com
Address: 209.85.135.99
Name:   www.l.google.com
Address: 209.85.135.103
Name:   www.l.google.com
Address: 209.85.135.104
Name:   www.l.google.com
Address: 209.85.135.105
Name:   www.l.google.com
Address: 209.85.135.106
Name:   www.l.google.com
Address: 209.85.135.147
```

Listing 2–4 *Das nslookup-Kommando*

Der große Vorteil dieser Installation ist nun, dass seit der Version 4 von Backtrack ein Update der Distribution und aller Tools möglich ist. Wir werden dies abschließend, wie in Listing 2–5 dargestellt, durchführen.

```
apt-get update
apt-get upgrade
apt-get install linux-source
apt-get dist-upgrade
```

Listing 2–5 *Backtrack-4-Update*

Backtrack 4 bietet standardmäßig das amerikanische Tastaturlayout. Da wir sehr viel von der Konsole arbeiten werden, sollte ein deutsches Tastaturlayout eingestellt werden. Klicken Sie dazu mit der rechten Maustaste auf die Flagge in der Taskleiste und wählen Sie den Menüpunkt *Configure* aus. Im darauffolgenden Fenster löschen (*Remove*) Sie alle anderen Einträge in der Rubrik *Active layouts*, bis nur noch *Germany* eingestellt ist. Mittels *OK* werden die Einstellungen gespeichert.

Kommen wir nun zur Installation der VMware-Tools. Listing 2–6 zeigt die notwendigen Schritte, die von der Konsole ausgeführt werden müssen. Vorbereitend dazu öffnen Sie zunächst das Webinterface des VMware-Servers und klicken im Bereich *Status* auf *Install Vmware Tools*. . .und dann auf *Install*. Die notwendigen

Dateien werden nun über das CD/DVD-Laufwerk bereitgestellt. Das Skript (`vmware-install.pl`) gewährleistet später die Installation und Konfiguration der VMware-Tools. Bei den nun gestellten Fragen sollten Sie jeweils die *Default*-Werte verwenden und diese einfach mit ENTER bestätigen.

```
cd /usr/src
tar jxpf linux-source-{version}.tar.bz2
ln -s linux-source-{version} linux
cd linux
zcat /proc/config.gz > .config
make scripts
make prepare
mkdir /mnt/cdrom
mount /dev/cdrom3 /mnt/cdrom
cp /mnt/cdrom/VMwareTools-{version}.tar.gz /tmp/
cd /tmp/
tar zxpf VMwareTools-{version}.tar.gz
cd vmware-tools-distrib
./vmware-install.pl
/usr/bin/vmware-config-tools.pl
```

Listing 2–6 *Installation der VMware-Tools*

Um die Aktualisierung zu komplettieren, werden wir nun auch Metasploit auf den aktuellen Stand bringen. Dies kann von der Metasploit-Konsole durchgeführt werden. Öffnen Sie diese nun über *K-Menü – Backtrack – Penetration – Metasploit Exploitation Framework – Framework Version 3 – Msfconsole* und führen Sie hier das Kommando `svn update`, wie in Abbildung 2–5 dargestellt, aus.

Die Nessus-Installation auf Backtrack 4

Der Security-Scanner `Nessus` von Tenable Network Security [5] untersucht übers Netz das Zielsystem auf konkrete Angriffsmöglichkeiten. Auf Wunsch probiert er sogar konkrete Angriffe aus. Nessus hat dazu in seiner Datenbank eine große Anzahl von Schwachstellen verzeichnet, die das ganze Spektrum von CGI-Lücken (CGI = Common Gateway Interface) bis hin zu spezifischen Windows-Schwachstellen abdecken. Nessus ist mittels einer Webschnittstelle komfortabel zu bedienen. Die Software wird mittlerweile in zwei Versionen bereitgestellt. Professionelle Anwender müssen eine kommerzielle Lizenz erwerben, um Nessus zu nutzen (Professional Feed). Für den »Home User« wird die Software mit geringen Einschränkungen kostenfrei zur Verfügung gestellt. Voraussetzung für die Nutzung ist die Registrierung beim Hersteller und der Erwerb eines Lizenz-Schlüssels. Dieser wird normalerweise nach der Registrierung per E-Mail übermittelt.

5. *http://www.nessus.org*

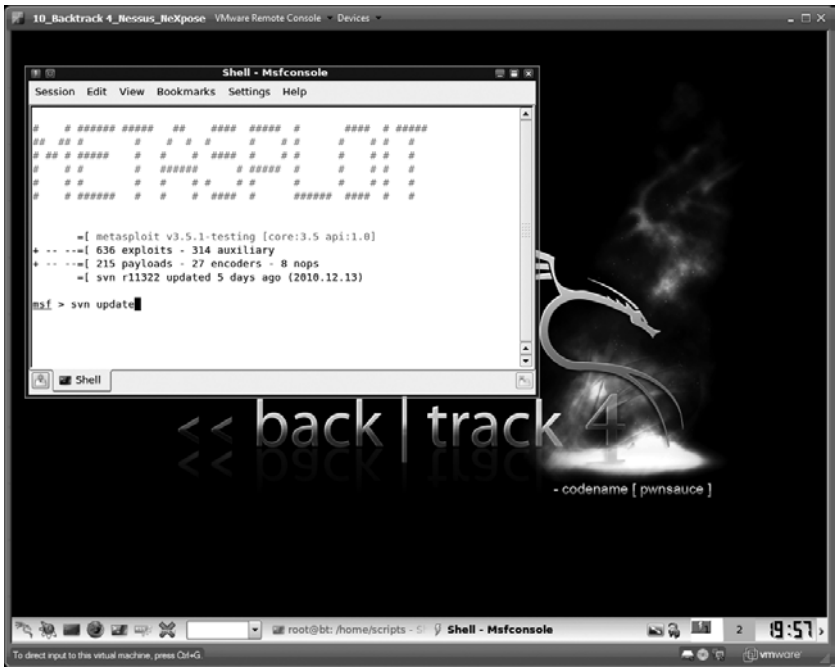

Abb. 2–5 *Metasploit aktualisieren*

Laden Sie zunächst die aktuelle Version von folgender Webseite herunter:

http://www.nessus.org/download/

Wählen Sie dazu die Datei für Ubuntu 8.04 (32 bit) aus und speichern Sie sie in Ihrer virtuellen Maschine ab. Je nach aktueller Version sollte dies folgende Datei sein:

`Nessus-4.x.x-ubuntu804_i386.deb`

Die Installation der Software ist relativ einfach. Öffnen Sie eine Konsole und führen Sie die Kommandos gemäß Listing 2–7 aus:

```
cd /root
sudo dpkg –i Nessus-4.2.x-ubuntu804_i386.deb
/opt/nessus/sbin/nessus-adduser
/opt/nessus/bin/nessus-fetch  --register [your key]
```

Listing 2–7 *Nessus-Installation*

Wie in Zeile 3 des Listings 2–7 zu sehen ist, wird mittels des Kommandos `nessus-adduser` ein Nutzer angelegt. Dieser ist für die erfolgreiche Arbeit mit Nessus dringend erforderlich. Erstellen Sie einen Nutzer und weisen Sie ihm ein Passwort zu. Die Frage: *Do you want this user to be a Nessus »admin« user?* beantworten Sie

mit *y*. Das Anlegen eines zusätzlichen *rule sets* ist nicht erforderlich. Bestätigen Sie diese Frage mit einem ENTER und speichern Sie anschließend die Einstellungen.

Als letzter Schritt ist die Registrierung der Software mittels des per E-Mail zugesandten Lizenzschlüssels erforderlich. Besteht eine Internetverbindung, werden nun automatisch die entsprechen Plug-ins heruntergeladen und installiert.

Nessus ist jetzt so eingestellt, dass die Software nach dem Hochfahren der virtuellen Umgebung (Backtrack 4) automatisch gestartet wird. Zusätzlich dazu kann die Steuerung manuell erfolgen:

```
/etc/init.d/nessusd start
/etc/init.d/nessusd stop
/etc/init.d/nessusd restart
```

Listing 2–8 *Nessus Daemon*

Wie weiter oben bereits erwähnt, wird Nessus über ein Webinterface (Port 8834) gesteuert. Verwenden Sie den Browser Ihrer Wahl und loggen Sie sich mit dem eben erstellten Nessus-Nutzer ein:

https://localhost:8834
https://IP_Adresse:8834

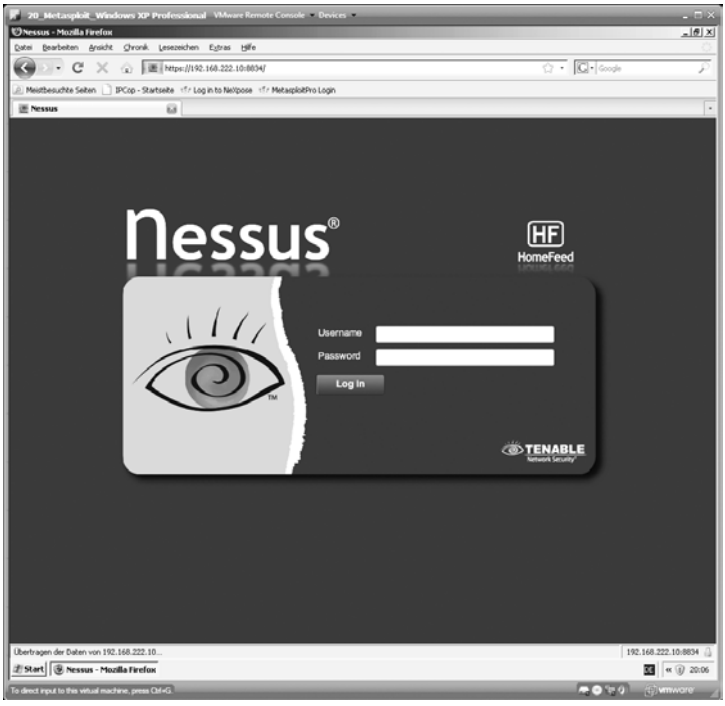

Abb. 2–6 *Login ins Webinterface von Nessus*

Nessus speichert alle Vorgänge in einer Logdatei ab. Man sollte also bei Problemen mit der Software einen Blick in diese Daten werfen. Mit dem in Listing 2–9 aufgezeigten Befehl lässt sich die Logdatei in der Konsole permanent anzeigen.

```
cd /opt/nessus/var/nessus/logs
tail –f nessusd.messages
```

Listing 2–9 *Nessus-Logfile permanent anzeigen*

Zum Abschluss möchte ich noch auf zwei nützliche Kommandos aufmerksam machen, die die praktische Arbeit mit Nessus erleichtern. Nessus arbeitet mit einer Unmenge an Plug-ins, die ständig aktualisiert werden. Der aktuelle Stand der Plug-ins wird mit folgendem Kommando angezeigt:

```
root@bt:/# cat /opt/nessus/lib/nessus/plugins/plugin_feed_info.inc
PLUGIN_SET = "201010010234";
PLUGIN_FEED = "HomeFeed (Non-commercial use only)";
```

Listing 2–10 *Nessus-Feed-Info anzeigen*

Im hier gezeigten Beispiel befinden sich die installierten Plug-ins auf einem Stand vom 01.10.2010 02:34 Uhr.

Normalerweise werden neue Plug-ins automatisch hinzugefügt. Ein manuelles Update erreichen Sie mit folgendem Kommando:

```
root@bt:/# /opt/nessus/sbin/nessus-update-plugins
Fetching the newest updates from nessus.org...
Done. The Nessus server will restart when its scans are finished
```

Listing 2–11 *Nessus-Plug-ins aktualisieren*

Die NeXpose-Installation auf Backtrack 4

NeXpose ist ein relativ neuer Vulnerability-Scanner von Rapid7[6]. Er ist in der Lage, potenzielle Schwachstellen in einem Netzwerk mit verschiedenen Komponenten zu erkennen, und hilft dabei, die vorhandenen Risiken abzuschätzen. Ein Highlight dieser Software stellt die Möglichkeit dar, auch Webapplikationen scannen zu können. NeXpose arbeitet »out of the box« mit dem Metasploit-Framework zusammen und zeigt verfügbare Exploits gemäß den gefundenen Schwachstellen an.

Neben den kommerziellen Versionen (Enterprise, Consultant und Express) wird NeXpose auch als kostenfreie Community-Version angeboten. Als Unterschied zu Nessus ist diese auch kostenlos für die kommerzielle Nutzung freigege-

6. *http://www.rapid7.com*

ben. Wer mit der Einschränkung leben kann, nur 32 IP-Adressen gleichzeitig scannen zu können, dem sei diese Software dringend ans Herz gelegt. Leider können Sie mit dieser Version keine Webapplikationen prüfen.

Die NeXpose Community Edition kann nach Registrierung unter folgender Webseite heruntergeladen werden:

http://www.rapid7.com/vulnerability-scanner.jsp

Nach erfolgreicher Registrierung erhalten Sie eine E-Mail mit den entsprechenden Links und dem Lizenzschlüssel. Laden Sie nun die Datei `NeXposeSetup-Linux32.bin` herunter und speichern Sie sie im `temp`-Verzeichnis. Wir werden nach einigen vorbereitenden Arbeiten die Installation durchführen.

Hierzu müssen wir zunächst einige zusätzliche Ubuntu-Pakete für Backtrack 4 abrufen und installieren. Führen Sie dazu die Schritte wie in Listing 2–12 beschrieben als `root` aus.

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

apt-get install libstdc++5
apt-get install xvfb
apt-get install xfonts-base
apt-get install xfonts-75dpi
apt-get install xserver-xorg
apt-get install libxtst6
apt-get install libxp6
apt-get install libxt6
```

Listing 2–12 *Notwendige Ubuntu-Pakete installieren*

Nun wird es Zeit, die Installation vorzunehmen. Achten Sie beim folgenden Skript darauf, dass als Installationspfad `/opt/rapid7/nexpose` angegeben wird. Wählen Sie als Installationstyp *Typical* aus und halten Sie den Lizenzschlüssel zur Eingabe bereit. Listing 2–13 beschreibt die notwendigen Schritte:

```
cd /tmp
./NeXposeSetup-Linux32.bin
cd /opt/rapid7/nexpose/nsc/
./nsc.sh
cp /opt/rapid7/nexpose/nsc/nexposeconsole.rc   /etc/init.d/nexpose
chmod 755 /etc/init.d/nexpose
```

Listing 2–13 *NeXpose-Installation*

Das Skript `nsc.sh` konfiguriert NeXpose und lädt die erforderlichen Daten direkt aus dem Internet herunter. Mit den letzten zwei Zeilen des Listings 2–13 richten

wir NeXpose so ein, dass es wie gewohnt als Daemon gestartet und gestoppt werden kann.

```
/etc/init.d/nexpose start
/etc/init.d/nexpose stop
/etc/init.d/nexpose restart
```

Listing 2–14 *NeXpose Daemon starten und stoppen*

Ähnlich wie Nessus wird auch NeXpose über ein Webinterface (Port 3780) gesteuert. Rufen Sie dazu folgende URLs mittels Ihres favorisierten Webbrowsers auf:

https://localhost:3780
https://IP_Adresse:3780

Nutzen Sie zum Einloggen in das Webinterface den Nutzernamen `nxadmin` und das bei der Installation erstellte Passwort.

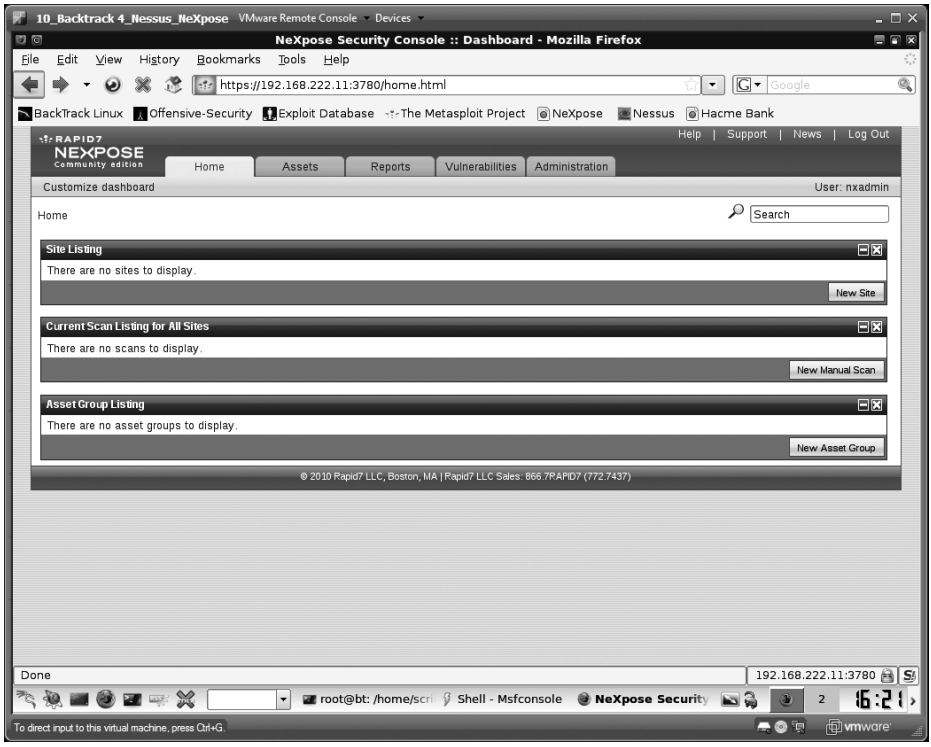

Abb. 2–7 *NeXpose-Webinterface*

2.3 Das Testumfeld für Webapplikationen

Um die Auswirkungen der verschiedenen Schwachstellen auf Webapplikationen testen zu können, sollte man sich hier zunächst Gedanken über eine effektive Trainingsumgebung machen. Die Nutzung der verfügbaren Tools und Programme im produktiven Umfeld könnte unter Umständen einen Ausfall des Systems zur Folge haben. Aus diesem Grund sollte der Einsatz in Unternehmen nur im Rahmen einer betrieblichen Vereinbarung erfolgen.

Die verschiedenen Hersteller der Webapplication-Vulnerability-Scanner stellen zum Test ihrer Produkte verschiedene Onlinesysteme zur Verfügung. Die wichtigsten sind hier aufgelistet:

- HP WebInspect: Free Bank Online[7]
- IBM Appscan: Online Bank Altoro Mutual[8]
- Acunetix ASP-Testseite[9], PHP-Testseite[10]

Diese Systeme sind für die einzelnen Tests sicherlich sehr brauchbar. Wir verfolgen aber das Ziel, unsere eigene Testumgebung in Form des VMware-Servers zu nutzen. Hier stellt uns das Internet ebenfalls interessante Umgebungen zur Verfügung, die in den verschiedensten Konfigurationen und Betriebssystemen nutzbar sind. Im Folgenden werden drei Lösungen vorgestellt, die wir in unser virtuelles Netzwerk übernehmen.

2.3.1 Damn Vulnerable Web Application (DVWA)

DVWA ist eine PHP/MySQL-Webapplikation, die diverse Schwachstellen aufweist und dadurch besonders für unsere Tests geeignet ist. Sie kann als Windows- oder Linux-System erstellt werden. Die Installation wird durch den Einsatz fertig konfigurierter Systeme (z.B. XAMPP[11]) vereinfacht.

Wir werden die ebenfalls auf der Webseite verfügbare Live-CD[12] in unsere virtuelle Umgebung einbinden. Sie basiert auf dem Betriebssystem Ubuntu Server 10.04, Apache 2.2.14, MySQL 5.1 und PHP 5.3.1.

Die Installation wird im Folgenden kurz erläutert:

Laden Sie sich zunächst die aktuelle ISO-Datei von der Projektwebseite herunter und speichern Sie sie auf dem VMware-Server.

Starten Sie das Webinterface des VMware-Servers und erstellen Sie eine neue virtuelle Maschine durch Klicken auf *Virtual Machine – Create Virtual Machine*.

---

7. *http://zero.webappsecurity.com*
8. *http://demo.testfire.net*
9. *http://testasp.vulnweb.com/*
10. *http://testphp.vulnweb.com/*
11. *http://www.apachefriends.org/de/xampp.html*
12. *http://www.dvwa.co.uk/download.php*

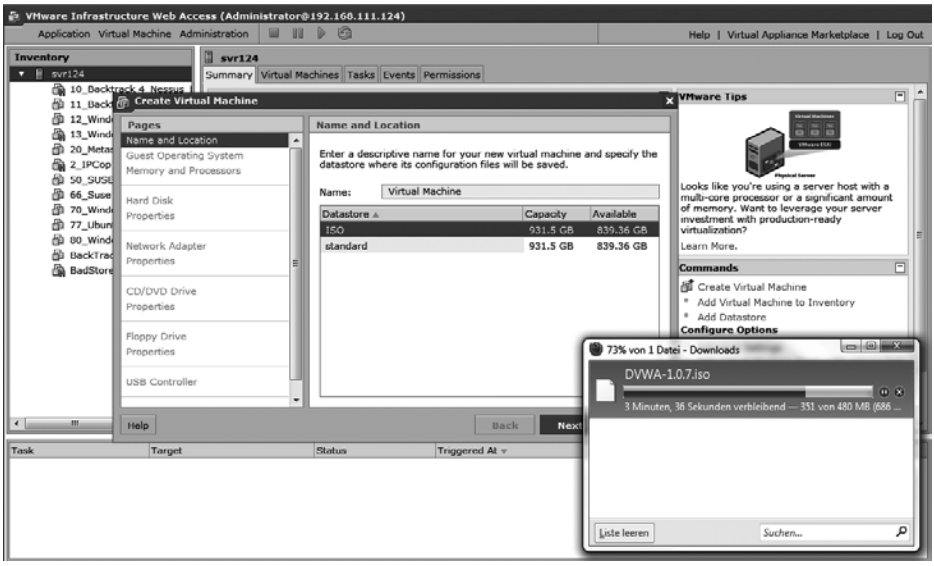

Abb. 2–8 *Neue virtuelle Maschine für DVWA erstellen*

Wählen Sie den Datastore *standard* und nach einem Klick auf *Next* als Betriebssystem *Linux operating System*, *Ubuntu Linux (32-bit)* aus. Für die nachfolgenden Einstellungen übernehmen Sie einfach die Defaulteinträge und wählen als Netzwerkadapter wieder *HostOnly* aus.

Bei der Option *CD/DVD Drive* angelangt, wählen Sie nun *Use an ISO Image* und im Inventory die Datei `DVWA-1.0.7.iso` aus.

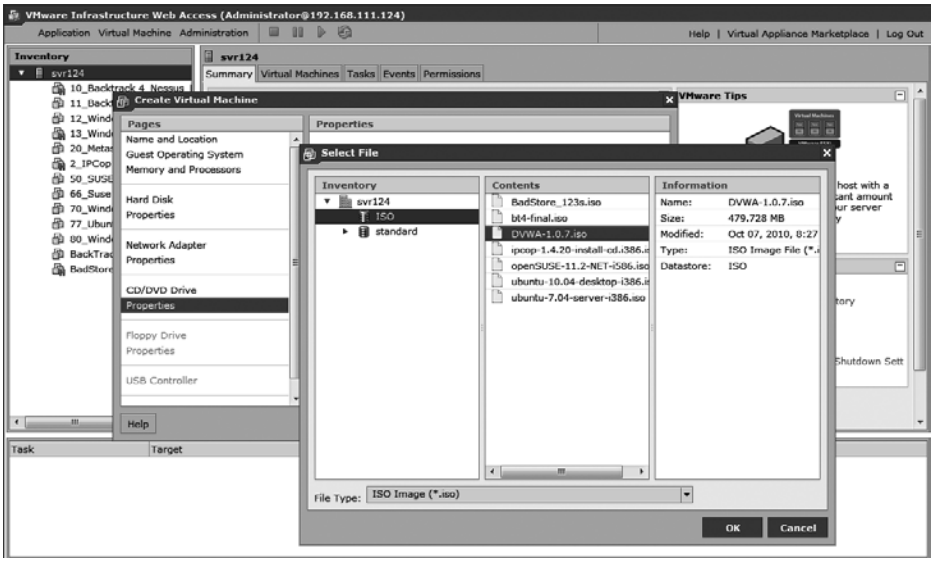

Abb. 2–9 *ISO-Datei auswählen*

Folgen Sie den weiteren Anweisungen auf dem Bildschirm und starten Sie die neu erstellte virtuelle Maschine wie gewohnt. Hat alles funktioniert, begrüßt DVWA Sie mit einem Bootmenü. Wählen Sie hier die Option *live – boot the Live System* aus.

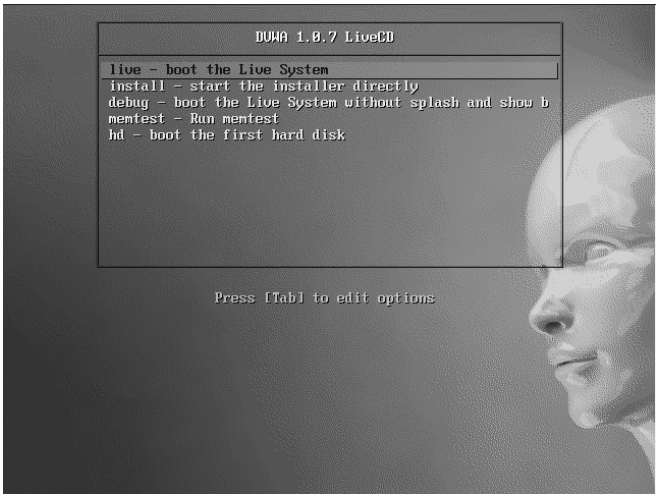

Abb. 2–10 *Bootmenü der DVWA-Live-CD*

DVWA ist nun arbeitsbereit. Um auf die Webseiten zugreifen zu können, müssen wir nur noch die Netzwerkkonfiguration vornehmen. Wählen Sie dazu einfach eine freie IP-Adresse in Ihrem virtuellen LAN aus und konfigurieren Sie eth0 wie folgt:

```
sudo su
ifconfig eth0 192.168.222.91 netmask 255.255.255.0
```

Listing 2–15 *Netzwerkkonfiguration*

Standardmäßig ist als Root-Passwort *password* festgelegt. Benennen Sie dies am besten um.

Für das Login auf die Webseite wählen Sie als Nutzernamen *admin* und als Passwort *password* aus.

Als Erstes sollten Sie die einzelnen Menüs und Einstellungen untersuchen. Jeder Eintrag ist einer potenziellen Schwachstelle zugeordnet. (Abb. 2–11)

Alternativ zu der dargestellten Lösung (Live-CD) können Sie auch Ihren eigenen virtuellen Server mittels XAMPP erstellen.

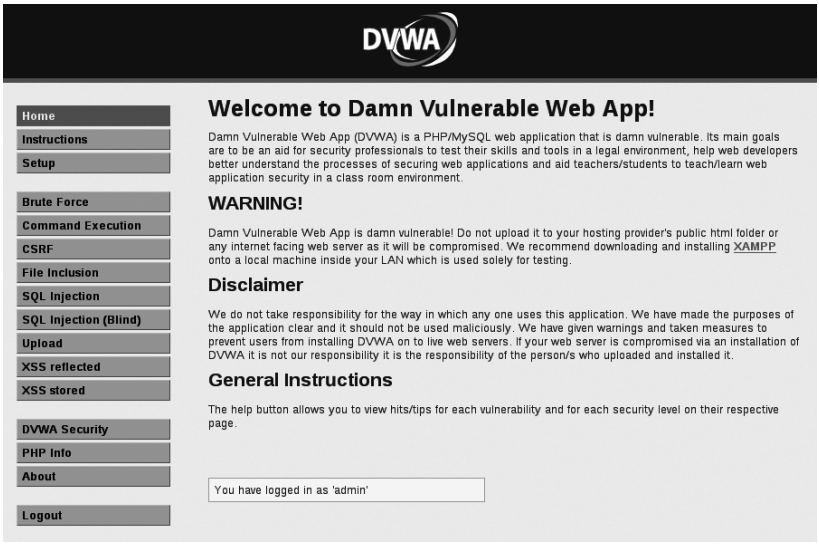

Abb. 2–11 *DVWA-Webinterface*

2.3.2 Badstore Online Shop

Badstore ist eine Webapplikation, die man zu Demonstrationszwecken in Sicherheitstrainings oder einfach als Testumgebung nutzen kann. Sie ist auf der Basis einer Linux-Distribution erstellt und enthält einen Apache-Webserver, eine CGI-Applikation und einen MySQL-Server.

Dieser verwundbare Onlineshop[13] ist ebenfalls als ISO-Datei verfügbar und lässt sich somit sehr gut in die virtuelle Umgebung integrieren. Ein Neustart der Umgebung setzt alle Einstellungen wieder auf die Standardwerte zurück. Dies ist besonders dann von Vorteil, wenn man durch bestimmte Angriffe die Webapplikation bzw. die Datenbank beschädigt hat.

Badstore enthält verschiedene Schwachstellen, die sich durch bestimmte Angriffe ausnutzen lassen, um den kompletten Webserver zu übernehmen. Diese sind u.a.:

- Cross-Site Scripting (XSS)
- SQL Injection
- Command Injection
- Cookie/Session Poisoning

Die Installation ist analog der bereits weiter oben beschriebenen Webapplikation DVWA vorzunehmen.

13. *http://www.badstore.net/*

Abb. 2–12 *Badstore: Ein Onlineshop mit diversen Schwachstellen*

2.3.3 Hacme Bank von Foundstone

Auf der Foundstone-Webseite kann man sich einige kostenlos verfügbare Programme und Tools herunterladen und für die eigene Ausbildung nutzen. In diesem Abschnitt interessieren wir uns folgerichtig für die Foundstone SASS Tools[14] und insbesondere für Hacme Bank.

Diese Webapplikation ist mit diversen Schwachstellen versehen, die nur darauf warten, gefunden zu werden. Die Installation auf einem Windows-Betriebssystem gestaltet sich relativ einfach und ist in wenigen Handgriffen erledigt. Als zusätzliche Komponenten werden das Windows .NET Framework v1.1, Microsoft IIS und der Microsoft SQL Server 2000 bzw. MSDE benötigt. Gehen wir also wieder Schritt für Schritt vor.

Laden Sie zunächst die beiden gepackten Dateien (Installer und Quelldateien) herunter. Wie der Dateiname bereits vermuten lässt, befinden sich nach dem Auspacken der ZIP-Dateien darin beide Teilprogramme für die Installation des Webservice und der eigentlichen Webseite. Lesen Sie zunächst die Anweisungen im *Foundstone Hacme Bank User and Solution Guide* v2.0 aufmerksam durch; sie

14. *http://www.foundstone.com/us/resources-free-tools.asp*

liegen im PDF-Format vor. Hier werden wichtige Hinweise für die Installation und die Arbeit mit dieser Webapplikation gegeben. In den Lektionen werden die einzelnen Schwachstellen nachvollziehbar dargestellt und umfassend erläutert.

Beachten Sie die Reihenfolge bei der Installation und gehen Sie wie folgt vor.

Legen Sie eine neue virtuelle Maschine in Ihrem VMware-Server an. Nutzen Sie dazu ein Windows-Betriebssystem (Windows XP oder Windows 2000 Server), vorzugsweise in einer englischsprachigen Version.

Sollten Sie nicht über die Software MS SQL Server 2000 verfügen, laden Sie sich zunächst MSDE 2000 Release A von der Microsoft-Webseite herunter. Das Gleiche trifft für das .NET Framework v1.1 zu.

Nachdem Sie MSDE 2000 durch Doppelklick auf die heruntergeladene EXE-Datei ausgepackt haben, führen Sie folgenden Befehl von der Windows-Kommandozeile aus:

```
c:\MSDERelA\Setup SAPWD=password SECURITYMODE=MIXED DISABLENETWORKPROTOCOLS=0
```

Installieren Sie nun das .NET-Framework und führen Sie nach anschließendem Neustart der virtuellen Maschine folgenden Befehl von der Windows-Kommandozeile aus:

```
net start MSSQLSERVER
```

Die Umgebung ist für die Installation der einzelnen Komponenten und Webseiten vorbereitet. Starten Sie nun die beiden MSI-Dateien und beginnen Sie, wie im o.g. Dokument beschrieben, mit der Installation des *Hacme Bank WebService*.

Wichtig: Um Verbindungsprobleme zu vermeiden, wählen Sie beim Datenbank-Setup unbedingt die Option *Trusted Connection* aus!

Nach erfolgreicher Installation sollten Sie die Webseite mittels folgender URL aufrufen können:

http://localhost/HacmeBank_v2_Website

Die Ersteller dieser Webapplikationen haben bereits drei Nutzer-Accounts angelegt. Melden Sie sich zunächst mit dem Nutzernamen *jv* und dem Passwort *jv789* an und prüfen Sie, ob die Zusammenarbeit der Webseite mit der Datenbank ordnungsgemäß funktioniert.

Sollte die Webapplikation trotz gestarteter MS-SQL-Datenbank eine Verbindung nicht zulassen, sollten Sie folgende Änderung in der Registrierungsdatenbank von Windows vornehmen. Setzen die den Eintrag `LoginMode` von 1 auf 0.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer\MSSQLServer\LoginMode
```

Wie Sie vielleicht bereits bei den Tests bemerkt haben, kann die Webseite derzeit nur vom lokalen System aus aufgerufen werden. Die Entwickler wollen damit

dem Missbrauch dieser Webapplikation auf Produktivsystemen vorbeugen. Für unsere Zwecke ist diese Einstellung aber so nicht geeignet. Wir haben vor, diese Webseite von anderen virtuellen Maschinen aus anzugreifen. Folgende Änderungen in der Konfiguration der Webseite wird unser Vorhaben aber dennoch ermöglichen.

In den Verzeichnissen `c:\Inetpub\wwroot\HacmeBank_v2_Website` und `c:\Inetpub\wwroot\HacmeBank_v2_WS` befindet sich jeweils die Datei `web.config`. Hier nehmen wir in beiden Fällen folgende Änderung vor:

```
<!--
<add name ="HttpModule_onlyAllowLocalAccess"
type="HacmeBank_v2_Website.httpModules.HttpModule_onlyAllowLocalAccess,
HacmeBank_v2_WS"/>
-->
```

Listing 2–16 *Änderungen an web.config*

Wir kommentieren das Modul `HttpModule_onlyAllowLocalAccess` in der abgebildeten Weise einfach aus und verhindern so die Ausführung.

Nun sollte die Hacme Bank auch von anderen Systemen aus erreichbar sein. Rufen Sie dazu folgende URL auf:

http://192.168.222.13/HacmeBank_v2_Website/aspx/login.aspx

Abb. 2–13 *Eine Onlinebank mit Schwachstellen*

Die Testumgebung ist nun vorbereitet. Sie kann natürlich jederzeit durch weitere Webapplikationen ergänzt werden.

Wir werden zu einem späteren Zeitpunkt auf die einzelnen Schwachstellen eingehen und diese Webapplikation mit Nikto prüfen (siehe Abschnitt 5.10).

2.4 Die Metasploit »Vulnerable VM«

Für den Test der eigenen Produkte stellt die Firma RAPID7[15] ein VM-Image zur Verfügung, das sowohl Nutzer der kommerziellen Produkte als auch Nutzer des Metasploit-Frameworks herunterladen und in ihre Testumgebung integrieren können. Es handelt sich dabei um ein Linux-System mit folgenden Komponenten:

- Linux Ubuntu 8.04
- ProFTP 1.3.1
- BIND 9.4.2
- Apache 2.2.8 und PHP 5.2.4
- Samba 3.0.30

Das VMware-Image kann über einen BitTorrent-Client heruntergeladen werden und ist hier zu beziehen:

```
http://www.metasploit.com/documents/express/Metasploitable.zip.torrent
```

Eine ausführliche Beschreibung der Schwachstellen, der nutzbaren Exploits sowie der verfügbaren Login-Daten und Passwörter finden Sie in Anhang A.14.

Zusätzlich dazu stehen zwei Webapplikationen zur Verfügung.

```
http://localhost/twiki/bin/view/Main/WebHome
http://localhost/tikiwiki/tiki-index.php
```

2.5 Debian 5.0 (Lenny) in einer virtuellen Umgebung

Debian[16] ist eine Linux-Distribution, die 1996 erstmals veröffentlicht wurde und sich noch heute großer Beliebtheit erfreut. In der Zwischenzeit sind weitere Linux-Distributionen aus Debian abgeleitet worden. Als bekannteste sei hier nur Ubuntu[17] erwähnt.

Das freie Betriebssystem wird weltweit in Universitäten, Schulen, Firmen und öffentlichen Behörden eingesetzt. Das IT-Migrationsprojekt LiMux[18] der Stadtverwaltung München basiert auf Debian und hat die vorher verwendeten Microsoft-Betriebssysteme erfolgreich ersetzt.

Ein Grund mehr, das erfolgreiche Betriebssystem in unsere Testumgebung aufzunehmen. Glücklicherweise stellt die »Open Source Company« eine virtuelle Umgebung[19] ins Internet, die Sie nur herunterladen und integrieren müssen. Die VMware-Konfiguration der Desktop-Umgebung sieht wie folgt aus:

---

15. *http://www.rapid7.com/*
16. *http://www.debian.org/*
17. *http://www.ubuntu.com/*
18. *http://www.muenchen.de/limux*
19. *http://www.opensource-company.de/content/downloads/vm-debian-lenny.php*

- Kernel: 2.6.26-1-686 (default)
- Arbeitsspeicher: 256
- Festplattenkapazität: 5.0 GB
- Netzwerk: NAT
- IP-Adresse: DHCP
- VMware-Tools aktiv: nein
- Bildschirmauflösung: 1024 × 768

Beim ersten Login verwenden Sie für den Nutzer `user` das Passwort `user` und für `root` das Kennwort `root`. Abbildung 2–14 zeigt die Desktop-Umgebung nach erfolgreicher Integration in unsere Testumgebung.

Abb. 2–14 *Debian 5.0 (Lenny) als Desktop-Umgebung*

2.6 Das Netzwerk und die Firewall

2.6.1 Das Netzwerk

Nun kann der VMware-Server seine Stärken ausspielen. Die Konfiguration des Netzwerkes sollte nicht allzu kompliziert sein. Hier bietet es sich an, die klassische Rot/Grün/Orange-Aufteilung (siehe Abbildung 2–15) zu nutzen: Dabei kennzeichnet der rot markierte Netzwerkbereich im Allgemeinen ein Netzwerk, dem nicht vertraut wird; daher sollte der Datenverkehr im grünen und orangen Netz entsprechend abgesichert werden. Im nächsten Abschnitt werden wir diese Abgrenzung durch eine Firewall vornehmen.

Um die in der nachfolgenden Tabelle dargestellte Konfiguration des Netzwerkes vorzunehmen, sollten Sie das Skript zur Konfiguration des VMware-Servers (`/usr/bin/vmware-config.pl`) nochmals ausführen. Hier ist es nun wichtig, die Netzwerkeinstellungen neu zu definieren. Alle anderen Einstellungen können wiederum übernommen und mit ENTER bestätigt werden. Legen Sie die Einstellungen für die Vmnet-Adapter wie folgt fest:

Name	VMnet	Type	IP-Adresse	Netzmaske
Bridged	Vmnet0	Bridged	192.168.111.0	255.255.255.0
HostOnly	Vmnet1	Hostonly	192.168.222.0	255.255.255.0
HostOnly (2)	Vmnet2	Hostonly	172.16.0.0	255.255.255.0

Der Netzwerkadapter Vmnet0 wird dabei auf `Bridged` gesetzt. Beim »Bridged Networking« befinden sich Gast- und Hostsystem in einem Netzwerk. Man kann es sich praktisch so vorstellen, dass beide scheinbar am gleichen Switch oder HUB hängen. In diesem Fall benötigt das Gastsystem eine IP-Adresse aus dem gleichen Netzwerksegment. Diese kann manuell eingetragen oder per DHCP zugewiesen werden. In Abbildung 2–15 wird die Netzwerkkonfiguration der Testumgebung wie folgt dargestellt:

Rot: Internet 192.168.111.0/24
Grün : LAN 192.168.222.0/24
Orange: DMZ 172.16.0.0/24

Wie in Abbildung 2–15 aufgezeigt, nutzen wir folgende virtuelle Netzwerkadapter:

ROT - Vmnt0 (bridged) – IP-Adresse: 192.168.111.122
GRÜN - Vmnt1 (HostOnly) – IP-Adresse: 192.168.222.1
ORANGE -Vmnt2 (HostOnly (2)) – IP-Adresse: 172.16.0.1

Vielleicht hilft es auch hier, wenn man sich die Adapter Vmnet1 und Vmnet2 ebenfalls als »virtuelle Switche« vorstellt. Die im jeweiligen Netzwerk befindli-

chen virtuellen Maschinen sind mit diesen »virtuellen Kopplungselementen« verbunden und müssen daher eine adäquate Netzwerkkonfiguration aufweisen, um miteinander kommunizieren zu können. Das Weiterleiten der Netzwerkpakete in andere Segmente unseres Testnetzwerkes oder des Internets wird durch die Firewall sichergestellt.

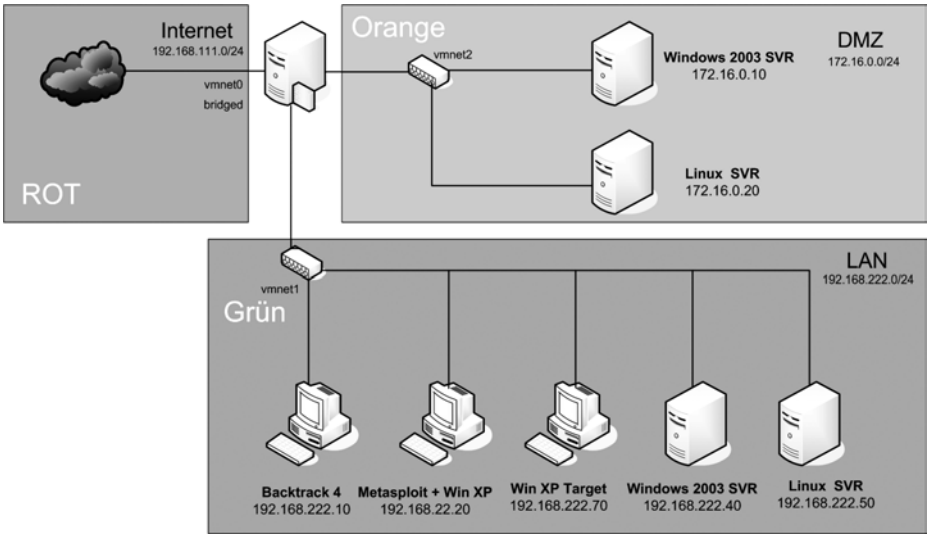

Abb. 2–15 *Netzwerkonfiguration der Testumgebung*

Die Installation der im grünen Segment befindlichen PCs (Backtrack 4 und Metasploit + Win XP) haben wir in Abschnitt 2.2 ausführlich beschrieben. Für die Durchführung unserer Tests benötigen wir Windows- und Linux-Systeme mit verschiedenen Patch-Ständen. Nun sollten weitere virtuelle Maschinen ergänzt werden. Hier sind dem Tester praktisch keine Grenzen gesetzt. Dabei ist es nicht immer notwendig, die virtuellen Maschinen selbst zu erstellen. Gängige Systeme können u.a. von der VMware-Webseite[20] (Virtual Appliance Marketplace) heruntergeladen werden.

2.6.2 Die Firewall

Um die Tests realistisch zu gestalten und ein Routing der Pakete zwischen den Netzwerksegmenten zu gewährleisten, werden wird nun eine Firewall installieren. Auch hier sind dem Tester keine Grenzen gesetzt. Man kann Testversionen kommerzieller Firewalls nutzen oder eine Open-Source-Lösung wählen.

Im Weiteren werden hier drei mögliche Lösungen vorgestellt.

20. *http://www.vmware.com/appliances/*

Die Astaro Security Gateway – Free Home Use Firewall[21] ist eine im Umfang reduzierte Version der kommerziellen Ausführung. Sie wird dem Privatanwender kostenlos und unverbindlich zur Verfügung gestellt. Ein Nutzer-Support ist dabei nicht inbegriffen. Die Software bietet umfassende Netzwerk-, Web- und E-Mail-Sicherheit mit VPN-Funktionalität und schützt bis zu 50 IP-Adressen. Sie enthält ein eigenes Betriebssystem und ist einfach mittels ISO-Image oder Boot-CD zu installieren.

Als zweite Möglichkeit sollte man sich unbedingt die Open-Source-Lösung PF-Sense anschauen. Sie basiert auf FreeBSD und ist als leistungsfähige Firewall oder Router-Plattform konzipiert. Das Projekt ist 2004 aus dem Vorgänger m0n0wall hervorgegangen und erfreut sich wachsender Beliebtheit in der User-Community. Insgesamt sind über 1 Million Downloads zu verzeichnen. Die Software kann direkt als VMware Appliance[22] heruntergeladen und in das Testsystem integriert werden.

Als Letztes wird hier die IPCop-Firewall vorgestellt. Sie ist ebenfalls eine Open-Source-Lösung und für den Home User sowie im SOHO-Bereich (SOHO = Small Office Home Office) einsetzbar. Die Software basiert auf einem Linux-System und lässt keine Wünsche bezüglich der Komponenten und Nutzung offen. Sehr interessant für unsere Zwecke stellt sich die Integration des Intrusion-Detection-Systems (IDS) Snort dar. Im Weiteren wird die Installation in einer virtuellen Umgebung beschrieben.

Laden Sie zunächst IPCop von folgender Webseite herunter und speichern Sie das ISO-Image im Store-Bereich des VMware-Servers:

http://www.ipcop.org

Gehen Sie zur Erstellung der virtuellen Machine wie folgt vor:

- Nutzen Sie Web Access (siehe Abb. 2–1) und loggen Sie sich auf dem VMware-Server ein.
- Erstellen Sie eine neue virtuelle Maschine mit *Virtual Machine – Create Virtual Machine*
- Name: *IPCop*, Datastore: *standard*
- Operating System: Linux operating system (Other 2.4x Linux (32 bit)
- Size: *512 MB*, Count: *1*
- Hard Disk: Create a new Virtual Disk
- Capacity: *8 GB* Location: *standard*
- Network Connection: *HostOnly*, Connect at Power on: *Yes*
- Use an ISO Image, Image File: ipcop-1.4.20-install-cd.i386.iso
- Don't Add a Floppy Drive
- Don't Add a USB Controller
- Finish

21. *http://www.astaro.com/landingpages/de-dach-homeuse*
22. *http://doc.pfsense.org/index.php/VMwareAppliance*

Gemäß unserer Netzwerkkonfiguration (siehe Abb. 2–15) benötigen wir zwei weitere Netzwerkkarten. Diese fügen wird mittels des Webinterface hinzu. Im Bereich *Commands* klicken Sie auf *Add Hardware – Network Adapters* und fügen jeweils einen Bridged Adapter (vmnet0) für das rote und einen HostOnly Adapter (vmnet2) für das orange Netz hinzu.

Nach dem Starten der virtuellen Maschine und der Bestätigung des Eingangsbildschirms läuft das Installationsprogramm ab. Folgen Sie den Anweisungen auf dem Bildschirm bis zur Konfiguration der Netzwerk-Schnittstellen. Nutzen Sie für die grüne Schnittstelle eine IP-Adresse, die die Verbindung zu Ihrem virtuellen LAN (Grün) über den Adapter vmnet1 gewährleisten kann. In unserem Beispiel vergeben wir die IP-Adresse 192.168.222.2/24. Alle weiteren Einstellungen können dann über den Webbrowser und folgende URLs vorgenommen werden:

http://192.168.222.2:81
https:// 192.168.222.2:445

IPCop ist bereits für unsere Netzwerkstruktur vorkonfiguriert. Im Abschnitt *Typ der Netzwerkkonfiguration* wählen Sie *GREEN + ORANGE + RED* aus. Für DNS-Server und Default-Gateway nutzen Sie wiederum die Einstellungen entsprechend Ihrem LAN (roter Bereich). Ein DHCP-Server kann später konfiguriert werden. Im Bereich *Treiber- und Karten-Zuordnungen* weisen Sie nun jeweils dem roten bzw. orangen Netz eine Netzwerkkarte mit den zugehörigen Einstellungen zu. Beachten Sie unbedingt die Reihenfolge der Zuweisung (zuerst RED und dann ORANGE) und schließen Sie die Konfiguration mit *Fertig* ab.

Weisen Sie nun dem roten und orangen Interface folgende IP-Adressen zu:

ROT: 192.168.111.122 Netzmaske: 255.255.255.0
ORANGE: 172.16.0.2 Netzmaske: 255.255.255.0

Zum Abschluss der Installation werden diverse Passwörter für die einzelnen Nutzenkonten angelegt. Mit dem Nutzernamen `admin` und dem festgelegten Passwort sind Sie nun in der Lage, sich über das Webinterface anzumelden. Starten Sie dazu eine weitere virtuelle Maschine, die sich ebenfalls im grünen Netzwerk befindet (z.B Metasploit + WinXP), und nutzen Sie Ihren bevorzugten Browser.

Sie können zu jeder Zeit die entsprechenden Einstellungen (Netzwerk, Gateway, DNS etc.) über die Konsole ändern. Loggen Sie sich dazu als `root` ein und führen Sie den Befehl `setup` aus.

Ändern Sie nun die Netzwerkeinstellungen auf den Clients im grünen und orangen Netz entsprechend. Nutzen Sie dazu statische IP-Adressen. Folgende Konfiguration ist z.B. sinnvoll:

Client im LAN: 192.168.222.10, GW: 192.168.222.2, DNS: 192.168.222.2
Server in der DMZ: 172.16.0.10, GW: 172.10.0.2, DNS: 172.16.0.2

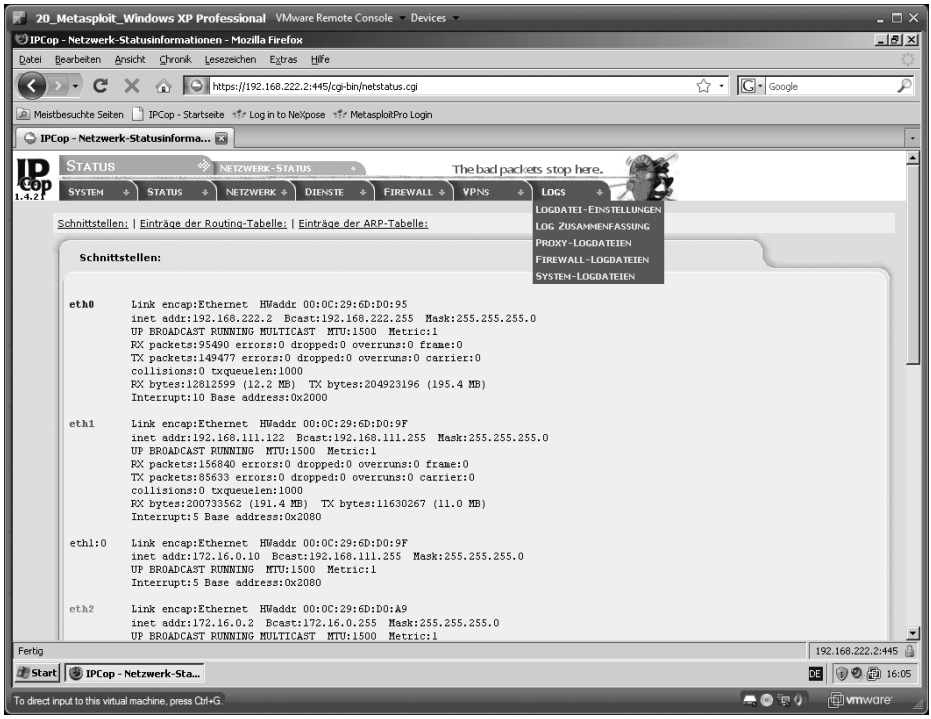

Abb. 2–16 *IPCop-Netzwerkkonfiguration*

2.7 Zusammenfassung

In diesem Kapitel sind wir ausführlich auf die Gestaltung eines Testnetzwerkes auf der Basis von VMware-Server 2.0.2 eingegangen. Damit ist ein wichtiger Grundstein für unsere weitere Arbeit gelegt. Die Konfiguration ist flexibel genug, um auf die verschiedenen Anforderungen reagieren zu können. Unser »Labor« kann natürlich jederzeit durch weitere virtuelle Maschinen ergänzt werden.

Zur praktischen Arbeit mit den virtuellen Umgebungen empfehle ich, vor Beginn der Penetrationtests Snapshots der einzelnen virtuellen Maschinen (VM) anzufertigen. Dies ist praktisch eine Kopie der auf der virtuellen Festplatte gespeicherten Daten. Leider kann hier je VM nur ein Snapshot angelegt werden. Sollte während der Arbeit etwas schiefgehen oder Daten ungewollt verändert werden, so kann man wieder problemlos zum Urzustand zurückkehren. Zum Anlegen dieser Wiederherstellungspunkte wählen Sie im Webinterface des VMware-Servers die Befehle *Commands – Snapshot – Take Snapshot* aus.