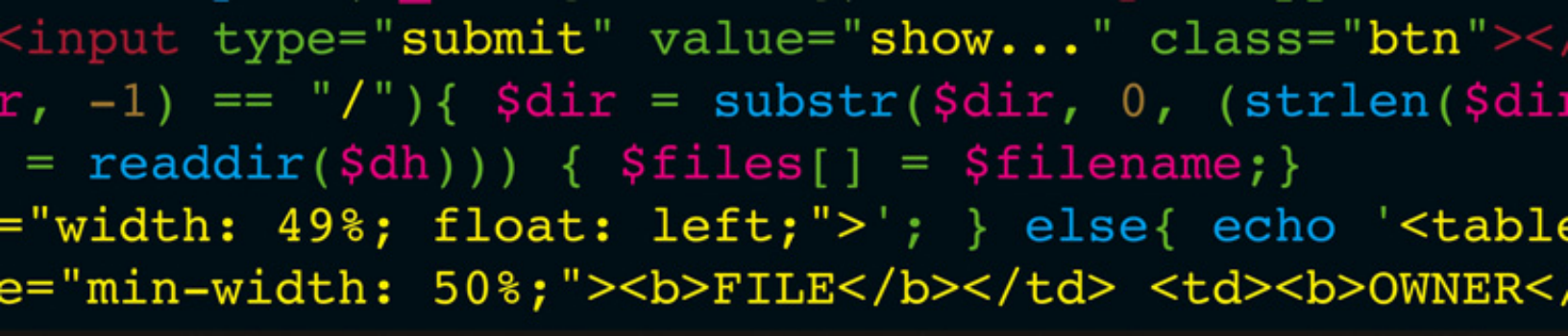


Mark B.

Webseiten hacken

Schnelleinstieg inkl. Entwicklung eigener Angriffsscripte

Danksagung und Vorwort

Zunächst möchte ich mich an dieser Stelle bei all denjenigen bedanken, die mich während der Arbeit an diesem Buchs unterstützt und motiviert haben.

Ganz besonders gilt der Dank meiner Freundin, die mich während der gesamten Zeit motiviert hat und es mir nicht übel nahm, dass ich so viel von unserer gemeinsamen Freizeit in dieses Projekt steckte - danke Schatz!

Dieses Buch baut stark auf meinen ersten Buch auf. Sie sollten also Grundlegende Linux-Kenntnisse oder "Hacken mit Kali-Linux" gelesen haben. Darüber hinaus werden wir in dem Buch einige eigene Angriffscodes entwickeln und daher sollten Sie zumindest einige HTML, JS und PHP Grundkenntnisse mitbringen um einigen Beispielen etwas leichter folgen zu können. Dazu kommen noch einige Beispiele in Python 3. Programmierkenntnisse in zumindest irgendeiner Sprache sind also definitiv von Vorteil...

Für diejenigen Leser, die diese nicht besitzen werde ich die wichtigsten Grundlagen aber dennoch beiläufig erwähnen. Dies ersetzt aber keinesfalls eine fundierte Einführung in Linux, das Arbeiten mit der Bash oder eine Programmiersprache!

Ein Wort der Warnung

An dieser Stelle will ich in aller Deutlichkeit sagen - **wer das hier Erlernte gegen fremde Webseiten oder Server ohne Zustimmung der Eigentümer einsetzt macht sich strafbar!** Wer allerdings die Tools und die hier entwickelten Scripts dafür benutzt seine eigene Seite zu testen wird die Sicherheit enorm steigern können, indem er mögliche Einfallstore und Schwachstellen identifiziert und danach beheben kann.

Wer seine eigenen Webseiten angreift sollte auf jeden Fall vorab den Hoster um Erlaubnis fragen, damit die Administratoren bescheid wissen und nicht sofort einen Abuse-Report an Ihren Internetanbieter senden. Darüber hinaus ist es auch ratsam den eigenen Provider zu informieren, damit der nicht vorsorglich Ihren Internet-Anschluss sperrt, sobald er merkt was Sie da treiben.

Ich will an dieser Stelle nochmals in aller Deutlichkeit sagen: Dieses Buch ist nicht als Anleitung zum Begehen von Straftaten gedacht und auch nicht als Anleitung wie man einer eventuellen Strafverfolgung entgehen kann!

Inhalt

Warum ich dieses Buch geschrieben habe

Angriffe auf Webseiten lassen sich am einfachsten nach dem Ziel einteilen:

Angriffe, die auf den Server an sich abzielen dienen beispielsweise dazu, einen anonymen Speicherplatz zum Ablegen von illegalen Inhalten, Trojanern und dergleichen zu finden oder den Server für den Versand von Spam oder Phishing-Mails zu verwenden.

Manche Angreifer haben es auf die User der Seite abgesehen und wollen die Seite nur dazu verwenden Userrechner zu infizieren oder im großen Stiel Kreditkartendaten abgreifen, um diese selbst betrügerisch zu verwenden oder im Darknet zu verkaufen.

Angriffe, die auf den Domainnamen abzielen können verwendet werden Traffic zu stehlen und auf die eigene Homepage umzuleiten oder die Domain an sich zu entführen, um den eigentlichen Besitzer zu erpressen.

Um Ihr Ziel zu erreichen gibt es genausoviel Möglichkeiten wie Intentionen. Webserver bieten viele Dienste an - in der Regel sind neben dem eigentlichen Webserver auch Datenbank-Dienste, Mailserver, FTP-Server und oftmals noch einige weitere Services auf diesem Rechner untergebracht. Daher bieten sich viele Angriffspunkte auf den Server direkt. Darüber hinaus werden Webseiten oftmals schnell entwickelt bzw. weiterentwickelt, was

allzuoft zu unentdeckten Code-Fehlern führt, die ein Angreifer ausnutzen kann.

Oftmals wird es Angreifern zu einfach gemacht indem Server schlecht gewartet werden, der Webseiten-Quelltext übereilt oder ungenügend getestet online geht oder wesentliche Sicherheitsaspekte bei der Entwicklung oder Konfiguration übersehen werden.

Ich will mit diesem Buch zeigen mit welchen Mitteln Hacker vorgehen, um interessierten Lesern das Wissen zu vermitteln, das nötig ist, um die eigenen Seiten zu prüfen und Schwachstellen und Fehler zu identifizieren bevor es jemand anders macht.

Hacker, Cracker, Scriptkiddies, ...

Da es keine allgemeingültige Definition gibt und auch die Begriffe einen fließenden Übergang haben nenne ich Ihnen an dieser Stelle meine persönliche Definition:

Einen Hacker kann man als eine Person definieren, die sich mit der Sicherheit von Computersystemen und Computerprogrammen beschäftigt und darin nach Schwachstellen sucht. Dies kann unterschiedliche Gründe haben, vom Zeitvertreib bis hin zum Wissensdrang. Findet ein Hacker eine solche Schwachstelle dann wird er diese Veröffentlichen um die Welt auf den Fehler aufmerksam zu machen. Was ein Hacker aber nicht machen wird, ist diese Schwachstelle zum eigenen Vorteil auszunutzen, um daraus Kapital zu schlagen. Daher bezeichnet man diese Hacker auch als Whitehats.

Cracker hingegen sind jene Hacker, die nicht diesem Moralkodex folgen und in Systeme eindringen um Schaden anzurichten, Geheimnisse auszuspionieren um diese dann zu verkaufen, Computersysteme oder Webseiten lahmlegen um Geld zu erpressen, und so einiges mehr. Der Antrieb dieser Personen ist in der Regel Kapital aus Ihren Fähigkeiten zu schlagen und möglichst viel Geld in möglichst kurzer Zeit zu verdienen. Mittlerweile sind viele dieser Cracker Teile größerer Organisationen und für weltweit einige Milliarden Euro Schaden pro Jahr verantwortlich. Diese Gruppe wird auch als Blackhats bezeichnet.

Whitehats wie auch Blackhats sind technisch versiert und in der Lage Schwachstellen in Software zu finden und Tools zu entwickeln, die diese Schwachstellen ausnutzen.

Scriptkiddis besitzen diese Fähigkeiten nicht. Sie verfügen im besten Fall über Wissen wie man Hacker-Tools einsetz. Oftmals beschränkt sich Ihr Wissen sogar nur auf den Bruchteil der Funktionen diverser Tools. Weiters wissen Scriptkiddies in der Regel auch nicht wirklich wie genau die Tools mit denen sie hantieren, arbeiten und kennen die technischen Hintergründe nicht, die ihre bevorzugten Hacker-Tools ausnützen. Daher wissen sich auch viele der Scriptkiddies nicht selber zu helfen, wenn die Standard-Vorgehensweise einmal nicht klappen würde. Aber das macht sie nicht weniger gefährlich. Diese Gruppe umfasst gut 90-95% der Personen, die Angriffe auf ein IT-System durchführen und in dieser Gruppe ist alles enthalten - von 14 Jährigen, der nur mal ausprobieren will was er im Internet gefunden hat - bis hin zum hauptberuflichen Cyberkriminellen, der an Ihre Konto- und Kreditkartendaten will.

In weiterer Folge des Buches werde ich den Begriff „Hacker“ als Überbegriff für alle hier genannten unterarten benutzen, wie es die meisten Leute aus dem üblichen Sprachgebrauch her gewohnt sind. Die Differenzierung um welche Art von „Hacker“ es sich in einem bestimmten Fall handelt, überlasse ich an der Stelle Ihnen als Leser.

Der Werkzeugkasten für den Angriff

Wer sich ernsthaft mit dem Hacken von Webseiten beschäftigen möchte, sollte sich ebenfalls mit Linux beschäftigen, denn der Großteil der Webserver wird auf dieser Plattform laufen.

Einige Grundlagen zum Thema Linux und das Setup von Kali-Linux habe ich sehr ausführlich in meinem ersten Buch "Hacken mit Kali-Linux" beschrieben. Daher erspare ich es uns an dieser Stelle diese Grundlagen nochmals aufzuführen. Ich will Ihnen stattdessen hier einige Alternativen vorstellen, damit interessierte Leser diese ausprobieren können falls sie es wünschen.

Auch in diesem Buch werde ich wieder meine bevorzugte Pentest-Distribution (*Kali-Linux*) verwenden. Dies ist aber bei Leibe nicht die einzige Distro mit einer fertigen Tool-Sammlung zum Hacken. Im Grunde kann man alle hier vorgestellen Tools in jeder beliebigen Linux-Distribution installieren und viele der Tools sind auch für Mac OSX oder Windows verfügbar! Der Vorteil einer Distribution, die alle diese Tools schon in den Paketquellen enthält, liegt aber auf der Hand:

Einerseits können so alle Tools mit der zentralen Paketverwaltung auf dem neuesten Stand gehalten werden und andererseits spart man sich viel Zeit diverse Tools von Hand zu suchen und zu installieren, die nicht von einer bestimmten Distribution angeboten werden.

Aber zurück zu den Alternativen - an dieser Stelle will ich Ihnen neben Kali auch noch folgende Pentest-Distros vorstellen:

Parrot Security OS
... ist eine auf Debian basierte Distrobution, die mit einem sehr umfangreichen Angebot an Hackertools. Darüber hinaus gibt es ebenfalls eine Parrot-Variante, die für den täglichen Gebrauch gedacht ist und als Standard-Desktop-Distro ausgelegt ist. Obgleich ich damit nur wenige Erfahrungen gemacht habe und Parrot nur kurz getestet habe halte ich es für einen ernstzunehmenden Konkurrenten für Kali und eine sehr gute Alternative. Darüber hinaus will ich die recht aktive Community erwähnen, die für Einsteiger durchaus sehr hilfreich sein kann.
(https://www.parrotsec.org/download.fx)

Fedora Security Spin
... ist eine auf Redhat basierte Distribution, die mit einer deutlich beschränkteren Anzahl an Tools bestückt ist. Dennoch will ich sie an dieser Stelle für all diejenigen nennen, die sich mit Redhat basierten Systemen besser auskennen und sich nicht unbedingt auf Debian oder Arch basierte Distributionen umgewöhnen wollen. Leider fehlen viele der Tools, die ich bevorzugt einsetze - in wieweit diese in den Repositories vorhanden und mit yum bzw. dnf nachinstallierbar sind, habe ich nicht getestet. Fedora zeichnet sich vor allem dadurch aus, dass viele Pakete in der aktuellsten Version verfügbar sind (*bleeding edge*), was allerdings nicht unbedingt für die bestmögliche Stabilität sorgt.
(https://labs.fedoraproject.org/de/security/)

Blackarch
... basiert, wie der Name vermuten lässt, auf Arch-Linux. Wie für Arch üblich, richtet sich das System an sehr erfahrene

Linux-User und so gibt es keine einfachen grafischen Installationstools und ähnliche Helfer. Auch der verwendete Window-Manager Namens Fluxbox ist sehr sporadisch. Obgleich ich nicht unerfahren im Umgang mit Linux bin, genieße ich einen gewissen Arbeitskonfort und daher ist Blackarch für mich persönlich keine Distribution mit der ich gern arbeite. Wer es allerdings ausprobieren möchte, kann dies mit dem Live-Image auch ohne vorherige Installation machen.
(https://blackarch.org/downloads.html)

Samurai Web Testing Framework
... ist keine eigenständige Linux-Distribustion, sondern ein Virtueller PC, der mit VMware oder VirtualBox gestartet werden kann. Samurai ist für Pentests von Webseiten gedacht und enthält ausschließlich die hierfür gedachten Tools. Dies vernachlässigt einige Angriffsvektoren, die direkt auf den Server abzielen. Außerdem bin ich persönlich kein Frund von virtuellen PCs zu diesem Zweck. Wer allendings eine fertige VM für Web-Pentesting sucht, wird hier fündig.
(https://sourceforge.net/projects/samurai/files/)

Diese Liste ist keinesfalls vollständig und es gibt noch dutzende weitere Distros, die für Pentesting oder Hacking optimiert sind bzw. die entsprechenden Tools in den Paketquellen anbieten. Allerdings will ich an dieser Stelle noch kurz ein paar Worte zur Auswahl der Distribution verlieren.

Oftmals dauert das Bruteforcen von Passwörtern oder diverse andere Aktivitäten im Rahmen eines Angriffs Stunden oder gar Tage. Daher ist mir die Stabilität des Systems essentiell wichtig! Sogar wichtiger als die neueste Version eines bestimmten Tools zu haben und ich nehme lieber in Kauf, ein einzelnes Tool ohne die Paketverwaltung händisch auf eine neuere Version upzudaten falls dies

unbedingt erforderlich ist, als 3 oder 4 Tage Cracking-Fortschritt zu verlieren weil das System abstürzt. Als Pentester ist man ohnehin oft genug genötigt sich mit schlecht dokumentierten und instabilen Exploit-Code herumzuschlagen, als dass man zusätzlich noch Beta-Tester für eine Distribution sein möchte oder eine Distribution verwenden möchte, für die wenig Unterstützung online zu finden ist. Außerdem möchte man nicht alle paar Monate auf eine andere Distro wechseln müssen weil die Macher der gewählten exotischen Distribution keine Lust mehr haben das Projekt fortzuführen.

Wer gerne alles selber bastelt und ohne Hilfe Fehler selbst debuggen will kann natürlich jede noch so kleine und exotische Distribution verwenden. Ich für meinen Teil setze aber nur auf die großen und etablierten Distributionen und ziehe wie bereits gesagt Stabilität der Aktualität vor und verlange vom System einen gewissen Arbeitskomfort und daher käme für mich abgesehen von Kali nur noch Parrot Security OS in Frage.

Kali-Linux

Kali wird von Offensive Security zusammengestellt und kann über die offizielle Homepage heruntergeladen werden: https://kali.org/downloads/

Zur Auswahl stehen hierbei ISO-Dateien, die Sie auf eine DVD brennen oder auf einen USB-Stick spielen können. Dabei ist es wichtig das ISO-Image nicht als Daten-DVD zu brennen oder einfach auf einen USB-Stick zu kopieren. Weiters haben Sie noch die Auswahl von Image-Dateien für ARM-Prozessoren *(zB Raspberry Pi*).

Bei den ISO-Dateien gibt es daüber hinaus teilweise die Auswahl zwischen einer 32-bit und 64-bit Variante. Sollten

Sie einen halbwegs aktuellen PC verwenden, nehmen Sie die 64-bit Variante. Falls Sie nicht sicher sind ob Ihre Hardware mit 64-bit klar kommt, dann wäre meine Empfehlung: Versuchen Sie sie 64-bit Variante und wenn es nicht klappt, dann erst nehmen Sie die 32-bit Variante. Ich entscheide mich hier für die 64-bit XFCE-Version, welche Ich Ihnen wärmstens empfehlen kann.

Nachdem Sie das Image heruntergeladen haben müssen Sie es auf eine DVD brennen. Hierzu können Sie unter Windows das Programm ImgBurn (http://imgburn.com) verwenden. Natürlich geht das ebenfalls mit vielen anderen Brennprogrammen. ImgBurn ist kostenlos, auf das Brennen von Image-Dateien spezialisiert und bietet daher kaum Spielraum für Fehler. Dennoch will ich Ihnen eine Schnellanleitung nicht vorenthalten.

Wenn Sie das Programm öffnen wählen Sie „Write Image to Disk“ in der Übersicht aus, die Sie nach dem Programmstart erhalten. Im folgenden Dialog finden Sie oben links einen Eintrag „Source“ und daneben einen Button mit einem Öffnen-Symbol. Klicken Sie auf das Symbol und wählen Sie die ISO-Datei aus, die sie heruntergeladen haben. Nehmen Sie die Häkchen bei „Test“ und „Verify“ am unteren Ende des Brenn-Fensters heraus und stellen Sie die Brenngeschwindigkeit möglichst niedrig ein. Danach können Sie auf den Brennen-Knopf direkt unter diesen Checkboxen klicken.

Mac-User können das Festplatten-Dienstprogramm verwenden. Sie finden es im Ordner „Dienstprogramme“ innerhalb des „Programme“-Ordners. Das dritte Symbol an der Oberseite des Programmes ist ein gelb-schwarz gestreifter Kreis. Wenn Sie auf dieses Brennen-Symbol klicken, sehen sie den Öffnen-Dialog. Wählen Sie die ISO-Datei aus und klicken Sie auf brennen. Danach kommt eine

Bestätigung, die Ihnen sagt, dass Ihr Mac bereit ist zum Brennen. Bestätigen Sie diese nochmals mit brennen.

Linux-User können die ISO-Datei einfach von der Konsole aus brennen. Verwenden Sie dazu diesen Befehl:

```
wodim -v -dao --eject speed=4 /pfad/zur/datei.iso
```

Sollten Sie keinen DVD-Brenner zur Verfügung haben oder ihr Kali-Linux-PC, so wie mein Subnotebook, über kein DVD-Laufwerk verfügen, dann können Sie die ISO-Datei auf einen USB-Stick extrahieren lassen.

Verwenden Sie dazu das Programm Unetbootin (https://unetbootin.github.io). Wählen Sie dazu die ISO-Datei aus indem Sie den Punkt „Diskimage“ markieren, ISO im Dropdown-Feld auswählen und auf den „...“-Button klicken, um die ISO-Datei zu öffnen. Danach wählen Sie direkt darunter in dem Dropdown-Feld den USB-Stick aus und klicken auf OK. Wichtig ist, dass der USB-Stick mindestens 4GB freien Speicher braucht.

Linux-Nutzer können das auch mit einem einfachen Konsolenbefehl lösen:

```
dd if=/pfad/zur/datei.iso of=/dev/sd[X] bs=512k
```

Hierbei muss das `[X]` durch den passenden Laufwerksbuchstaben für den USB-Stick ersetzt werden. Wenn sie nicht sicher sind was Sie machen, dann lassen Sie die Finger von `dd`! Dieser Befehl ist unerbitterlich und kann Ihre gesamte Festplatte mit all Ihren Daten und den Betriebssystem unbrauchbar machen. Mit entsprechender Software können einige Daten sicherlich danach immer noch gerettet werden, aber lustig ist so eine Sache nicht.

Falls Sie dd einsetzen und auch sicher sind welches Laufwerk Sie überschreiben dann werden sie nicht ungeduldig, dd braucht seine Zeit und meldet auch keinen Fortschritt!

Die Testumgebung für unsere Reise einrichten

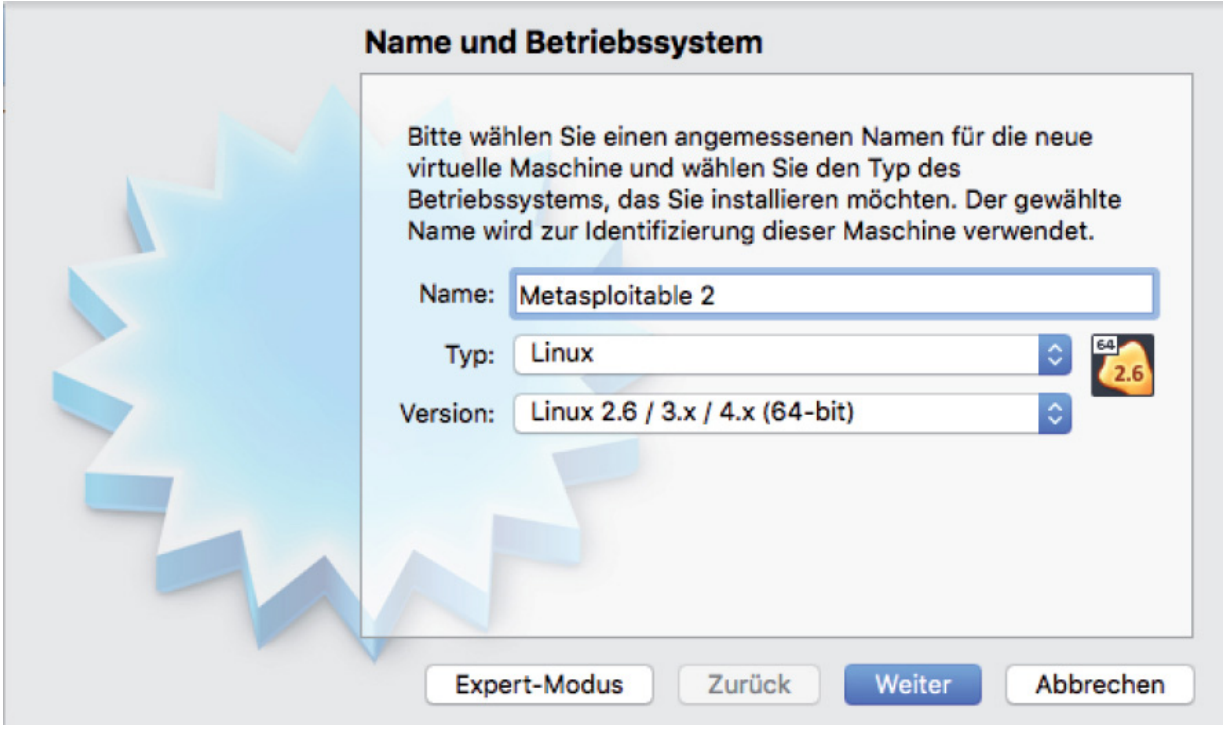
Einerseits ist es - wie eingangs schon erwähnt - illegal irgendwelche fremden Seiten anzugreifen und andererseits ist es auch höchstwahrscheinlich, dass sich an einer Seite die ich angreifen würde schon etwas geändert hat, bis Sie das Buch lesen. Daher sollten wir für unsere Reise eine einheitliche Labor-Umgebung einrichten in der wir arbeiten können und in der Sie vor allem, die gezeigten Beispiele auch genau nachvollziehen können.

Zu diesem Zweck werden wir einen virtuellen PC Namens `Metasploitable 2` verwenden. Diesen können Sie unter: https://sourceforge.net/projects/metasploitable/files/Metasploitable2/ herunterladen. In der ZIP-Datei sind dann folgende Dateien enhalten:

```
Metasploitable.nvram
Metasploitable.vmdk
Metasploitable.vmsd
Metasploitable.vmx
Metasploitable.vmxf
```

Die `vmdk`-Datei können wir als Festplatte in Virtualbox laden. Sie können auch gern den VMware Player verwenden um den VPC zu starten. Da dieser aber nicht für alle Plattformen verfügbar ist zeige ich die Vorgehensweise anhand von Virtualbox. Dieses Programm können Sie unter: https://www.virtualbox.org/wiki/Downloads herunterladen.

Nachdem Sie das Programm installiert und gestartet haben klicken Sie auf den Neu-Button und führen Sie folgende Schritte aus:



Den Namen können Sie beliebig wählen. Als Typ verwenden Sie `Linux` und als Version `Linux 2.6 / 3.x / 4.x (64-bit)`.

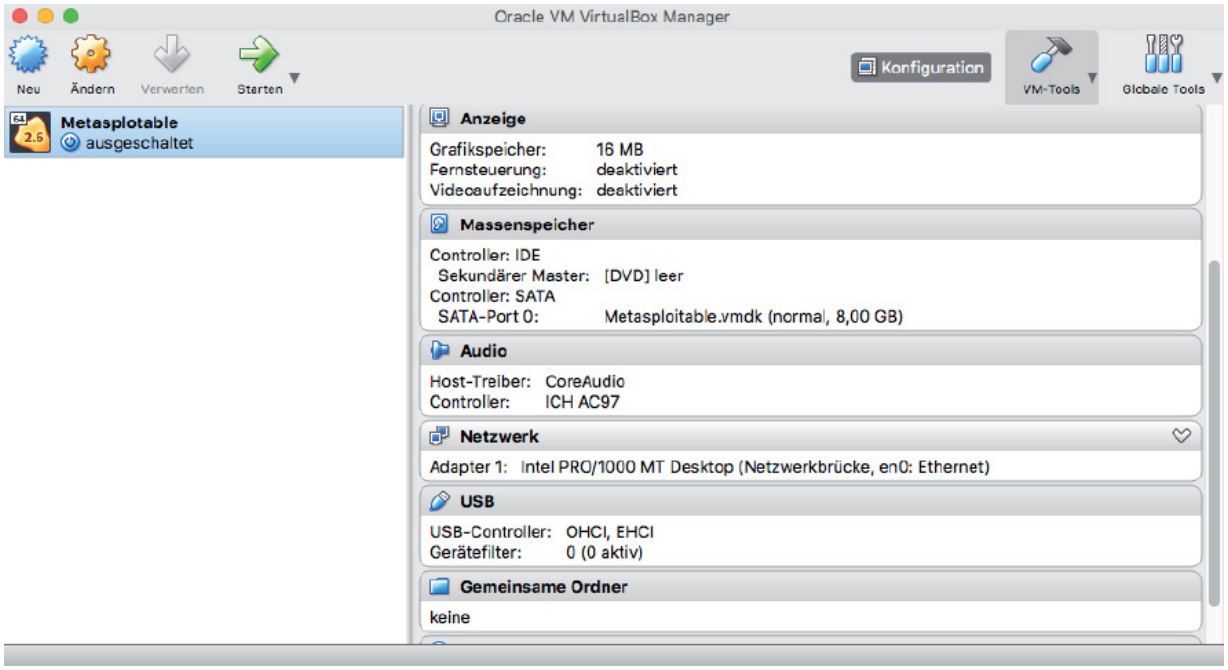
Danach klicken Sie auf Weiter.

Als RAM-Speicher reichen in unserem Fall 1024 MB aus. Bestätigen Sie dies mit einem Klick auf Weiter.

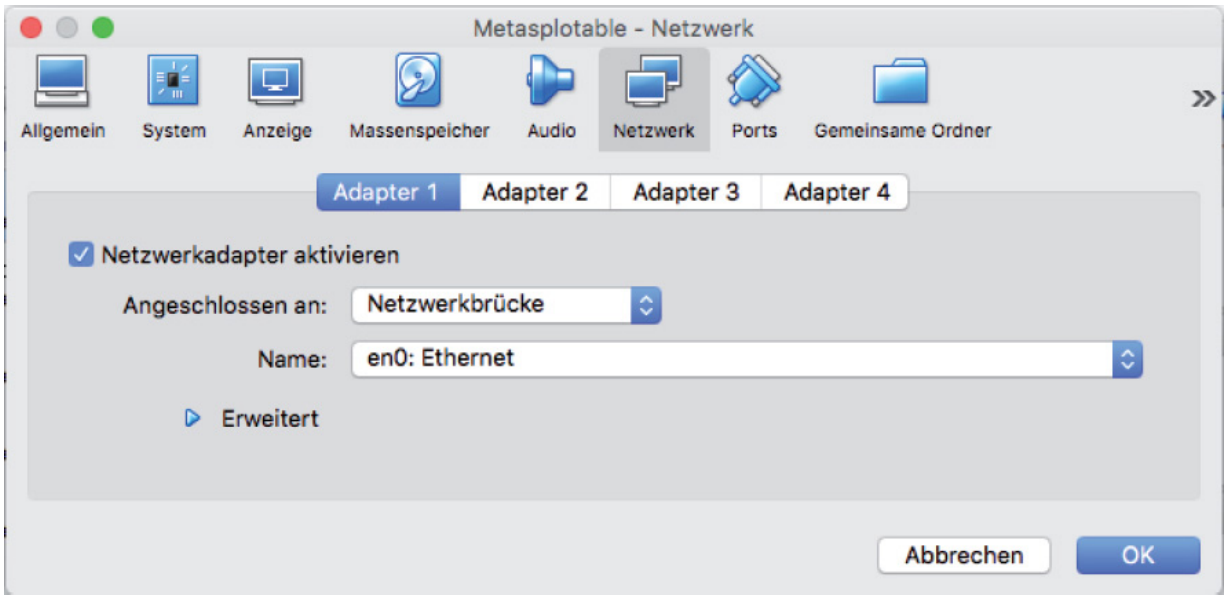
Hier wählen Sie "Vorhandene Festplatte verwenden" aus und danach klicken Sie auf das - Symbol rechts neben der Drowpdown-Leiste.

Dadurch öffnet sich der Dateiauswahl-Dialog und Sie können die `vmdk`-Datei auswählen, die Sie zuvor aus der Zip-Datei entpackt haben.

Schließlich können Sie die Anlage des VPC mit einen Klick auf Erzeugen abschließen.



Bevor wir den VPC starten, sollten wir noch die Netzwerkeinstellungen überprüfen. Dazu scrollen Sie die Liste auf der rechten Seite nach unten bis Sie das Wort Netzwerk sehen und dann öffnen Sie den folgenden Dialog mit einem Doppelklick auf das Wort Netzwerk.



Hier bei muss zumindest Adapter 1 aktiviert sein. Weiters muss im Feld "Angeschlossen an" der Eintrag "Netzwerkbrücke" ausgewählt sein.

Unter Name wählen Sie die Netzwerkkarte aus mit der der Host-Computer an ihr Netzwerk angeschlossen ist. Danach bestätigen Sie das Ganze mit dem OK-Button.

Dadurch wird sichergestellt, dass der soeben erstellte virtuelle PC in Ihrem Heimnetzwerk wie ein weiterer PC auftaucht und Sie von jedem Rechner in Ihrem Netzwerk darauf zugreifen können.

Jetzt können Sie den VPC einfach mit einem Klick auf den Start-Button booten.

Wordpress & Joomla auf Metasploitable einrichten

Nachdem unser Test-Opfer nun gebootet wurde können wir uns mit dem Usernamen `msfadmin` und dem Passwort `msfadmin`

anmelden. Mit DVWA (*Damn Vulnerable Web Application*) haben wir schon eine Test-Webseite, die wir auf vielfältige Weise hacken können. Allerdings will ich Ihnen auch noch einige weitere Techniken für beliebte Content-Management-Systeme zeigen.

Darum werden wir noch folgende zwei Scripts installieren. Dazu fangen wir mit Wordpress an:

```
msfadmin@metasploitable:~$ cd /var/www/

msfadmin@metasploitable:/var/www$ sudo wget https://wordpress.org/wordpress-4.6.zip
--17:42:40-- https://wordpress.org/wordpress-4.6.zip
          => `wordpress-4.6.zip'
Resolving wordpress.org... 66.155.40.250, 66.155.40.249
Connecting to wordpress.org|66.155.40.250|:443... connected.
ERROR: Certificate verification error for wordpress.org: unable to get local issuer certificate
ERROR: certificate common name `*.wordpress.org' doesn't match requested host name `wordpress.org'.
To connect to wordpress.org insecurely, use `--no-check-certificate'.
Unable to establish SSL connection.
```

Wenn Sie das erste mal `sudo` verwenden werden Sie nach dem `root`-Passwort gefragt. Tippen Sie das Passwort einfach ein und lassen Sie sich nicht beirren! Linux zeigt ihnen nicht an, dass Sie tippen und es scheint so als würde nichts geschehen. Sobald Sie die Eingabe mit der Enter-Taste bestätigen wird Ihre Eingabe überprüft und der Befehl ausgeführt, wenn das Passwort korrekt war oder eine Fehlermeldung ausgegeben.

Scheinbar kann `wget` das Certifikat nicht überprüfen. Falls Sie den gleichen Fehler erhalten drücken Sie die Pfeil aufwärts - Taste um den letzten Befehl wieder aufzurufen und fügen am Ende `--no-check-certificate` hinzu.

```
msfadmin@metasploitable:/var/www$ sudo wget https://wordpress.org/wordpress-4.6.zip --no-check-certificate
--17:44:01-- https://wordpress.org/wordpress-4.6.zip
          => `wordpress-4.6.zip'
Resolving wordpress.org... 66.155.40.250, 66.155.40.249
Connecting to wordpress.org|66.155.40.250|:443... connected.
WARNING: Certificate verification error for wordpress.org: unable to get local issuer certificate
WARNING: certificate common name `*.wordpress.org' doesn't match requested host name `wordpress.org'.
HTTP request sent, awaiting response... 200 OK

Length: 8,648,124 (8.2M) [application/zip]

100% [=====================================================================>] 8,648,124 3.21M/s

17:44:04 (3.20 MB/s) - `wordpress-4.6.zip' saved [8648124/8648124]
```

Danach sollte der Download auf jeden Fall klappen und wir können die ZIP-Datei auspacken.

```
msfadmin@metasploitable:/var/www$ sudo unzip wordpress-4.6.zip
```

Danach müssen wir eine Datenbank anlegen. Dazu verwenden wir den MySQL CLI-Client und führen damit den Befehl `CREATE DATABASE wordpress;` aus. Da wir gerade dabei sind, können wir auch gleich die Datenbank für Joomla anlegen:

```
msfadmin@metasploitable:/var/www$ mysql -u root
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 8
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> CREATE DATABASE wordpress;
Query OK, 1 row affected (0.03 sec)
```

```
mysql> CREATE DATABASE joomla;
Query OK, 1 row affected (0.03 sec)

mysql> exit
Bye
```

Beim Extrahieren der Dateien ist der Ordner `wordpress` erstellt worden in dem sich das Script befindet. Daher wechseln wir nun in diesen Ordner.

```
msfadmin@metasploitable:/var/www$ cd wordpress
```

Danach kopieren wir die `wp-config-sample.php` und speichern diese als `wp-config.php` ab. In dieser Datei werden wir dann die DB-Einstellungen vornehmen. Wichtig ist hierbei, dass Sie darauf achten müssen, den Dateinamen mit Kleinbuchstaben zu schreiben und keine Tippfehler einbauen. Andernfalls kann Wordpress die Datei nicht finden und wird eine Fehlermeldung ausgeben.

```
msfadmin@metasploitable:/var/www/wordpress$ sudo cp wp-config-sample.php wp-config.php
```

Jetzt müssen wir die soeben erstellt Datei mit `vim` bearbeiten. `vim` ist ein sehr mächtiger aber äußerst gewöhnungsbedürftiger Editor. Ich kann Ihnen nur raten sich mit diesem Programm zu beschäftigen, da Sie es auf sehr vielen Servern antreffen werden und über kurz oder lang damit arbeiten müssen.

Wenn Sie `vim` starten befinden Sie sich im Normalmodus. In diesem Modus können Sie den Text nur lesen und einige Aktionen über Tasten ausführen. Sie können allerdings Text NICHT normal eingeben oder bearbeiten. Dazu müssen Sie mit einem Druck auf die `i`-Taste in den Editor-Modus wechseln. Danach erscheint in der letzten Zeile am Bildschirm -- `INSERT` --.

Jetzt sind Sie in der Lage die nebenstehenden Ändrungen vorzunehmen.

```
msfadmin@metasploitable:/var/www/wordpress$ sudo vim wp-config.php

<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config. php creation script uses this file during the
 installation. You don't have to use the web site, you can copy
 this file to "wp-config.php" and fill in the values.
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://codex.wordpress.org/Editing_wp-config.php
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host
** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', '');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8');
```

```
/** The Database Collate type. Don't change this if in doubt.
*/
"wp-config.php" [dos] 89L, 2822C written
```

Sie können mit den Pfeiltasten im Dokument navigieren, Texte eingeben und löschen wie in einem herkömmlichen Editor. Sie müssen wie oben gezeigt den Datenbank-Namen (`define('DB_NAME', ...)` auf `wordpress` und den DB-User (`define('DB_USER', ...)` auf `root` ändern. Das Passwort (`define('DB_PASSWORD', ...)` muss leer sein - also löschen Sie den Platzhalter-Text bis auf die einfachen Anführungszeichen heraus. Um diese Änderungen zu speichern müssen Sie durch Drücken der `ESC`-Taste wieder zurück in den Normal-Modus wechseln. Dadurch verschwindet auch wieder das -- `INSERT` -- in der letzten Zeile.

Jetzt schreiben Sie auf Ihrer Tastatur einfach `:wq` - diese Eingabe wird Ihnen dann ebenfalls in der untersten Zeile angezeigt und bedeutet so viel wie "Befehl *`(:)`* Schreiben *(write)* Beenden *(quit)"*

Danach bestätigen Sie den Befehl mit Enter und `vim` wird geschlossen. Wenn Ihnen das jetzt zu schnell war dann gibt es einige sehr gute Anleitungen zu `vim` im Internet. Machen Sie eine kurze Pause und arbeiten Sie sich ein wenig ein.

Wenn alles geklappt hat, dann können Sie Wordpress über `http://IP-Adresse/wordpress` erreichen und fertig einrichten. Die IP-Adresse bekommen Sie wie folgt heraus:

```
msfadmin@metasploitable:/var/www$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:a6:bd:c5
          inet addr:192.168.1.52 Bcast: 192.168.1.255
          Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fea6:bdc5/64
          Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
```

```
          RX packets: 121604 errors:0 dropped:0 overruns:0
          frame:0
          TX packets: 71761 errors:0 dropped:0 overruns:0
          carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:56292884 (53.6 MB) TX bytes:21013683
          (20.0 MB)
          Base address:0xd010 Memory:f0000000-f0020000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:1373 errors:0 dropped:0 overruns:0
          frame:0
          TX packets:1373 errors:0 dropped:0 overruns:0
          carrier:0
          collisions:0 txqueuelen:0
          RX bytes:124002 (121.0 KB) TX bytes:124002 (121.0
          KB)
```

Der Block `eth0` steht für die erste Netzwerkkarte und der Eintrag `inet addr:192.168.1.52` gibt die IP-Adresse an.

Da wir gerade bei so gut wie jedem Befehl Superuser-Rechte benötigten, ich persönlich sehr Tippfauel bin und nicht andauernd `sudo` *(Superuser Do)* eingeben will, zeige ich Ihnen wie wir dauerhaft zu Superuser-Rechten kommen:

```
msfadmin@metasploitable:/var/www/wordpress$ sudo su
```

Nachdem wir nun zum User `root` gewechselt haben, können wir mit der Einrichtung von Joomla beginnen. Dazu müssen wir wiederum in das Haupt-Verzeichnis des Webservers wechseln:

```
root@metasploitable:/var/www/wordpress# cd /var/www/
```

Und das Script als ZIP-Datei herunterladen:

```
root@metasploitable:/var/www/joomla# wget https://downloads.joomla.org/de/cms/joomla25/2-5-15/joomla_2-5-15-stable-full_package-zip?format=zip --no-check-certificate
```

Einen Ordner Namens `joomla` erstellen:

```
root@metasploitable:/var/www# mkdir joomla
```

Die ZIP-Datei in diesen Ordner verschieben:

```
root@metasploitable:/var/www# mv joomla_2-5-15-stable-full_package.zip joomla/
```

In den Ordner joomla wechseln:

```
root@metasploitable:/var/www# cd joomla/
```

Und die ZIP-Datei auspacken:

```
root@metasploitable:/var/www/joomla# unzip joomla_2-5-15-stable-full_package.zip
```

Danach erstellen wir eine leere Datei mit dem Namen `configuration.php`:

```
root@metasploitable:/var/www/joomla# touch configuration.php
```

Und machen diese Datei für alle beschreibbar damit das Setup-Script die noch leere Datei befüllen kann.

```
root@metasploitable:/var/www/joomla# chmod 666 configuration.php
```

Nun können wir den Installations-Assistenten von Joomla mit `http://IP-Adddresse/joomla` aufrufen. Folgen Sie einfach den Anweisungen auf der Seite und in wenigen Klicks ist die Installation fertig.

Zum Abschluss müssen wir noch den Installations-Ordner aus dem `joomla`-Ordner löschen:

```
root@metasploitable:/var/www/joomla# rm -r installation/
```

Jetzt ist unser zweites CMS ebenfalls einsatzbereit.

Vorbereitungen für einen Angriff

Bevor man einen Angriff auf einen Server beginnt, ist es unerlässlich verschiedenste Informationen zu sammeln und mögliche Angriffsvektoren zu identifizieren.

Passive Informationsbeschaffung

... heißt so weil der Angreifer hierbei noch nicht einmal eine Verbindung zum Opfer-Server aufbaut. Man verwendet also Informationen, die in öffentlich zugänglichen Datenbanken über das Opfer gespeichert wurden.

In Kali-Linux verwende ich dazu einfach den folgenden Befehl in einem Terminal:

```
user@kali:~$ whois einedomain.at
% Copyright (c)2017 by NIC.AT (1)
%
% Restricted rights.
%
% Except for agreed Internet operational purposes, no part of
this information may be reproduced, stored in a retrieval
system, or transmitted, in any form or by any means,
electronic, mechanical, recording, or otherwise, without prior
permission of NIC.AT on behalf of itself and/or the copyright
holders. Any use of this material to target advertising or
similar activities is explicitly forbidden and can be
prosecuted.
%
% It is furthermore strictly forbidden to use the Whois-
Database in such a way that jeopardizes or could jeopardize the
stability of the technical systems of NIC.AT under any
circumstances. In particular, this includes any misuse of the
```