

Basic Pentesting 1

Diese VM ist speziell für Anfänger im Bereich Penetrationstests gedacht. Das Ziel ist es, die VM aus der Ferne anzugreifen und Root-Rechte zu erlangen. Wenn du das geschafft hast, kannst du versuchen Sie, andere Angriffsvektoren zu finden zu finden, die du möglicherweise übersehen hast.

Die [virtuelle Maschine](#) kannst du auf [Vulnhub](#) herunterladen.

Die virtuelle Maschine hat verschiedene Sicherheitslücken, die es ermöglichen, administrative Rechte zu erlangen.

Variante 1: ProFTPD

Informationsbeschaffung Runde 1

Zunächst verschafft man sich einen Überblick über die Netzwerkeinstellungen und Adressen, der Befehl `ip a s` zeigt die Netzwerkschnittstellen und ihre aktuelle Konfiguration an:

```
(kali㉿kali)-[~]
$ ip a s
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether 08:00:27:b4:a1:05 brd ff:ff:ff:ff:ff:ff
   inet 192.168.56.104/24 brd 192.168.56.255 scope global dynamic noprefixroute eth0
       valid_lft 473sec preferred_lft 473sec
   inet6 fe80::3352:7719:3cdc:c0e7/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether 08:00:27:3f:85:80 brd ff:ff:ff:ff:ff:ff
   inet6 fd:c7:3c9d:ff31:e:a417:2389:abf:asb6/64 scope global dynamic noprefixroute
       valid_lft 86398sec preferred_lft 14398sec
   inet6 fe80::2ffa:a065:90ab:abc4/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

(kali㉿kali)-[~]
$
```

Das ist die Schnittstelle für den Internetzugang von Kali - hier keine Hacking Tools verwenden!

Das ist die Netzwerkschnittstelle, in der sich unsere verwundbaren Maschinen befinden.
Netzwerk: 192.168.56.1/24

Hier im Beispiel ist die interne Schnittstelle also `eth0` mit der Adresse `192.168.56.104/24`.

Jetzt können wir das Zielnetzwerk scannen, um zu sehen, welche Geräte sich dort befinden: `netdiscover -i eth0 192.168.56.1/24` liefert folgendes Ergebnis:

```
Currently scanning: Finished! | Screen View: Unique Hosts
5 Captured ARP Req/Rep packets, from 5 hosts. Total size: 300

IP           At MAC Address      Count  Len  MAC Vendor / Hostname
-----
192.168.56.1  0a:00:27:00:00:00    1     60  Unknown vendor
192.168.56.100 08:00:27:35:ed:79    1     60  PCS Systemtechnik GmbH
192.168.56.101 08:00:27:93:05:02    1     60  PCS Systemtechnik GmbH
192.168.56.102 08:00:27:ba:c6:57    1     60  PCS Systemtechnik GmbH
192.168.56.103 08:00:27:20:58:bc    1     60  PCS Systemtechnik GmbH

(root@kali)-[~]
# netdiscover -i eth0 -r 192.168.56.1/24
```

Es gibgt also poentiell 4 Angriffsziele in unserem Netz - um INformationen zu den einzelnen Hosts zu erhalten untersucht man sie einzeln mit nmap <IP-Adresse>. Die Pentesting 1 Maschine bietet folgende Dienste an:

- Port 21 - FTP
- Port 22 - SSH
- Port 80 - http

Es gibt nur ein Maschine, die genau diese Kombination aus Ports geöffnet hat, die mit der IP-Adresse **192.168.66.102**. Im Weiteren werden wir also mit dieser IP Adresse "arbeiten".

```
# nmap 192.168.56.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-05 03:42 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00018s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 08:00:27:BA:C6:57 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 6.77 seconds

(root@kali)-[~]
# nmap 192.168.56.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-05 03:42 EDT
Nmap scan report for 192.168.56.103
Host is up (0.00046s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    closed ssh
80/tcp    open  http
443/tcp   open  https
MAC Address: 08:00:27:20:58:BC (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 11.34 seconds
```

Nun versuchen wir, mehr Informationen über die eingesetzte Software auf dem Server zu erhalten, dazu verwenden wir erneut nmap, jetzt aber mit Optionen, die versucht, die Software und deren Versionen zu ermitteln:

```
nmap -sV -A 192.168.56.102
```

- Die Option -sV scannt nach den Versionen
- Die Option -A schält "Aggressive Scanning" ein, damit bekommt man einige zusätzliche Infos

Das Ergebnis sieht so aus:

```
└─# nmap -sV -A 192.168.56.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-05 03:59 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00027s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD 1.3.3c
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 d6:01:90:39:2d:8f:46:fb:03:86:73:b3:3c:54:7e:54 (RSA)
|   256 f1:f3:c0:dd:ba:a4:85:f7:13:9a:da:3a:bb:4d:93:04 (ECDSA)
|_  256 12:e2:98:d2:a3:e7:36:4f:be:6b:ce:36:6b:7e:0d:9e (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: Apache/2.4.18 (Ubuntu)
MAC Address: 08:00:27:BA:C6:57 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.14, Linux 3.8 - 3.16
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   0.27 ms  192.168.56.102

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 15.23 seconds
```

Wir sehen jetzt zu den offenen Ports jeweils, welches Programm in welcher Version für den entsprechenden Dienste eingesetzt wird und einige weitere Informationen, z.B. zum verwendeten Linux Kernel.

Diese Informationen ermöglicht es uns, zu überprüfen, ob irgendeine der eingesetzten Software ungepatchte Sicherheitslücken hat, wie wir ausnutzen können.

Angriff

<https://infosecwriteups.com/basic-pentesting-1-walkthrough-vulnhub-4dac91b416ff>

From:
<https://info-bw.de/> -

Permanent link:
https://info-bw.de/faeher:informatik:oberstufe:netzwerke:basic_pentesting1:start

Last update: **05.06.2025 08:06**

