

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.

Walkthrough

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

Variante 1: ProFTPD

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:usb6/64 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 gibt also potentiell 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 192.168.66.101

```
# 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
```

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

From:

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

Permanent link:

https://www.info-bw.de/faecher:informatik:oberstufe:netzwerke:basic_pentesting1:start?rev=1749109734

Last update: **05.06.2025 07:48**

