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.

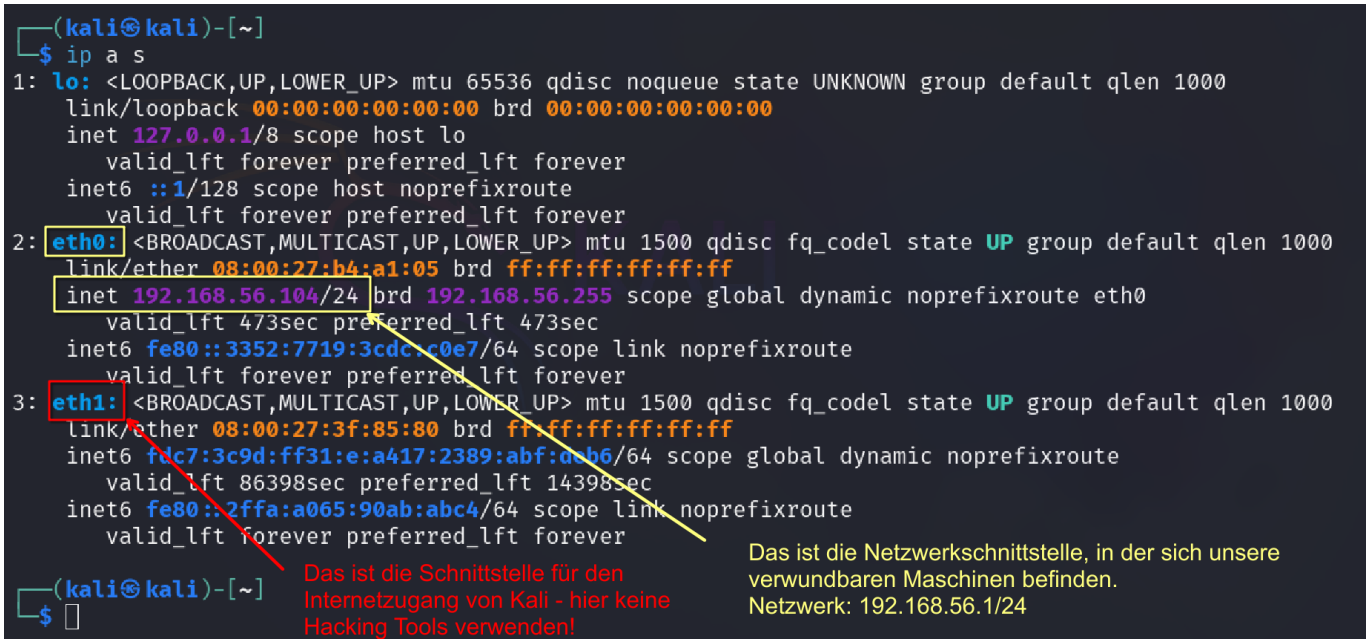
Die virtuelle Maschine kannst du auf Vulnhub herunterladen.

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` zeihgt die Negtzwerkschnittstellen und ihre aktuelle Konfiguration an:



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
```

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=1749109229

Last update: **05.06.2025 07:40**