ITSI EK - PENTESTING

Kural Deniz Sinan

3DHIT

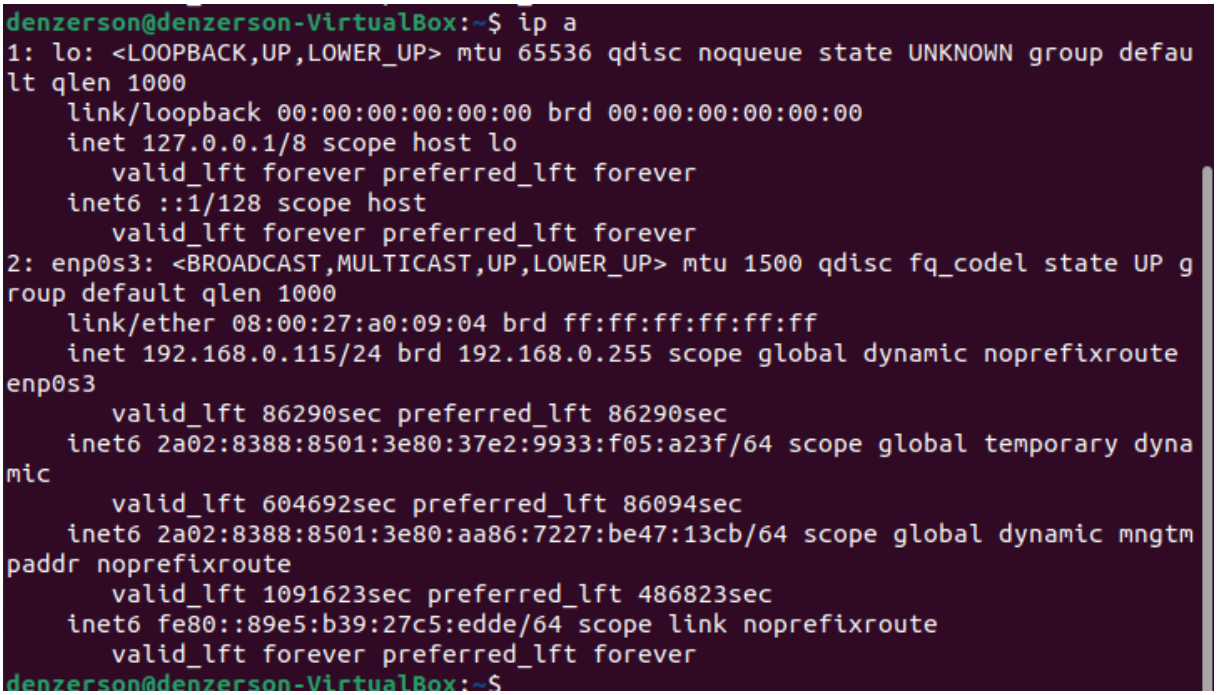
Contents

Netzwerkstruktur 2
Angeschlossene Geräte 3
Offene Ports 5
WLAN 6
Bedrohungsanalyse 7

Netzwerkstruktur

Der Befehl „ip addr“ oder auch „ip a“ zeigt IP-Adressen dieser Schnittstellen an:

- Name der Netzwerkschnittstelle (z.B. eth0, wlan0, etc.)
- IP-Adresse(n) der Schnittstelle (z.B. 192.168.0.100)
- Netzmaske(n) der Schnittstelle (z.B. 255.255.255.0)
- MTU (Maximum Transmission Unit) der Schnittstelle
- Status der Schnittstelle (z.B. ob die Schnittstelle aktiv ist oder nicht)
- MAC-Adresse der Schnittstelle
- andere informationen wie z.B. Broadcast-Adresse, multicast-Adresse



Angeschlossene Geräte

Mit dem Befehl nmap kann man herausfinden, welche Geräte im Netzwerk sind.

1) nmap -sL <Network> (sL: simple list)

```
denzerson@denzerson-VirtualBox:~$ nmap -sL 192.168.0.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-01-25 20:15 C
Nmap scan report for 192.168.0.0
Nmap scan report for compalhub.home (192.168.0.1)
Nmap scan report for 192.168.0.2
Nmap scan report for 192.168.0.3
Nmap scan report for 192.168.0.4
Nmap scan report for 192.168.0.5
Nmap scan report for 192.168.0.6
Nmap scan report for 192.168.0.7
Nmap scan report for 192.168.0.8
Nmap scan report for 192.168.0.9
Nmap scan report for 192.168.0.10
Nmap scan report for 192.168.0.11
Nmap scan report for 192.168.0.12
Nmap scan report for 192.168.0.13
Nmap scan report for 192.168.0.14
N                  192.168.0.15
Anwendungen anzeigen  192.168.0.16
Nmap scan report for 192.168.0.17
```

Hier ist zB meine VM:

```
Nmap scan report for 192.168.0.114
Nmap scan report for denzerson-VirtualBox (192.168.0.115)
Nmap scan report for 192.168.0.116
```

2) nmap -sn <Network>

Zeigt aktive Geräte im Netzwerk

```
denzerson@denzerson-VirtualBox:~$ nmap -sn 192.168.0.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-01-25 20:22 C
Nmap scan report for compalhub.home (192.168.0.1)
Host is up (0.0077s latency).
Nmap scan report for 192.168.0.10
Host is up (0.051s latency).
Nmap scan report for 192.168.0.38
Host is up (0.026s latency).
Nmap scan report for 192.168.0.53
Host is up (0.020s latency).
Nmap scan report for denzerson-VirtualBox (192.168.0.115)
Host is up (0.0021s latency).
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.53 seco
```

3) nmap -sS <Network>

Das ist ein TCP SYN-Scan: Es werden Anfragen an Ports des Geräts gesendet. Dabei muss das Gerät nicht darauf reagieren, und es wird Verfügbarkeit und Konfiguration des Gerätes ermittelt. Es ist die meist verwendete Scanmethode, wenn die Geräte auf Pings nicht reagieren. (Stealth Scan)

```
Nmap scan report for compalhub.home (192.168.0.1)
Host is up (0.0059s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
5000/tcp open  upnp
MAC Address: 38:43:7D:8F:87:22 (Compal Broadband Networks)

Nmap scan report for 192.168.0.10
Host is up (0.0044s latency).
All 1000 scanned ports on 192.168.0.10 are closed
MAC Address: 48:43:DD:B8:2B:94 (Amazon Technologies)

Nmap scan report for 192.168.0.38
Host is up (0.016s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
8008/tcp  open  http
8009/tcp  open  ajp13
8443/tcp  open  https-alt
9000/tcp  open  cslistener
10001/tcp open  scp-config
MAC Address: 48:D6:D5:0F:30:A4 (Google)

Nmap scan report for 192.168.0.52
Host is up (0.0015s latency).
All 1000 scanned ports on 192.168.0.52 are filtered
MAC Address: A4:97:B1:83:B3:D9 (Chongqing Fugui Electronics)
```

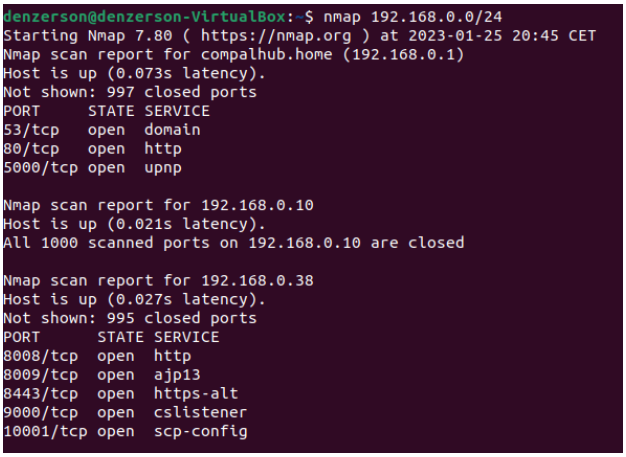
```
Nmap scan report for 192.168.0.52
Host is up (0.0015s latency).
All 1000 scanned ports on 192.168.0.52 are filtered
MAC Address: A4:97:B1:83:B3:D9 (Chongqing Fugui Electronics)

Nmap scan report for 192.168.0.53
Host is up (0.0084s latency).
All 1000 scanned ports on 192.168.0.53 are closed
MAC Address: 60:5B:B4:72:88:E3 (AzureWave Technology)

Nmap scan report for denzerson-VirtualBox (192.168.0.115)
Host is up (0.0000020s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
80/tcp open  http
81/tcp open  hosts2-ns

Nmap done: 256 IP addresses (6 hosts up) scanned in 12.11 seconds
```

Wie man sieht, kommen sehr viele Informationen raus, die sehr große Vorteile bringen könnten.

Offene Ports

`nmap <IP-Adresse>`

Scannt Ports 0-1000



`nmap -p- <IP-Adresse>`

Scannt alle Ports von 0 bis 65535

Das Ausführen dieses Befehls hat zu lange gebraucht.

`nmap -sV <IP-Adresse>`

Hier versucht das tool herauszufinden, welche Services und Versionen auf dem Port laufen. Es ist wichtig, dass diese Services aktuell sind, indem man nach CVEs sucht (bekannte Sicherheitslücken)

Das Ausführen dieses Befehls hat zu lange gebraucht.

`nmap -A <IP-Adresse>`

Dieser Befehl versucht soviele Informationen über den Host zu sammeln wie es möglich ist: das ist ein aggressiver Scan. Grundsätzlich sollte es in deinem Netzwerk wohl wenige offene Services geben, in der Praxis finden sich dennoch immer wieder einige, zum Beispiel am Router (zur Administration) oder 'smarten' Haushaltsgeraeten wie Fernseher

Das Ausführen dieses Befehls hat zu lange gebraucht.

WLAN

Das vom Hersteller erstellte Passwort wurde noch nicht verändert – weil ich zu faul war – und es wird WPA2 als Verschlüsselung eingesetzt. Ansich ist das Passwort als ziemlich sicher einstufbar: Groß-Kleinzeichen, länger als 12 Zeichen, Zahlen, aber keine Sonderzeichen. Das Admin Passwort hatte ich aber zuvor geändert.

Bedrohungsanalyse

Ich kann mir vorstellen, dass Eindringer mit bösen Absichten an unsere finanziellen Daten rankommen wollen. Meistens bekomme ich DDOS-Drohungen, und wenn mal eine Attacke passiert, mache ich den Router kurz aus und an, weil mein Provider mir einen eigenen DHCP Service eingerichtet hat. Jedoch ist es am wahrscheinlichsten, dass durch Malware unser Netzwerk beschädigt wird, da ich immer wieder verschiedene Programme von Fremden herunterlade. Wenn einmal ein Rat oder sonstiges eingebaut wird, könnte das zum Verderben führen.

Um sonstige Angriffe abzuwehren, nutze ich VPNs, Firewalls, Antivirusprogramme, stärkere Passwörter.