jamk.fi

LAB 2 Port scan

Data security testing

Jere Pesonen TTV18S1
m3227@student.jamk.fi

LAB-02-Port scan
10-20
Tieto- ja viestintätekniikka
Tekniikan ja Liikenteen ala

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

1 NMAP

nmap -sL 10.99.67.128/25

sL- parameter sends reverse dns query with every ip address in the range

```
Nmap scan report for 10.99.67.144
Nmap scan report for 10.99.67.145
Nmap scan report for 10.99.67.146
```

it doesn't give anything on linux computer but for the firewall it does

```
Nmap scan report for TheGreatFirewall.localdomain (10.99.67.254)
Nmap scan report for 10.99.67.255
```

```
     5 0.079309877   fe80::afd1:63d7:9f25 fe80::afd1:63d7:9f2… DNS      105 Standard query 0x0921 PTR 128.67.99.10.in-addr.arpa
     6 0.079357965   10.99.67.131         10.99.67.254         DNS       85 Standard query 0x0922 PTR 129.67.99.10.in-addr.arpa
     7 0.079452286   fe80::afd1:63d7:9f25 fe80::afd1:63d7:9f2… DNS      105 Standard query 0x0923 PTR 130.67.99.10.in-addr.arpa
     8 0.079479517   10.99.67.131         10.99.67.254         DNS       85 Standard query 0x0924 PTR 131.67.99.10.in-addr.arpa
     9 0.079610311   fe80::afd1:63d7:9f25 fe80::afd1:63d7:9f2… DNS      105 Standard query 0x0925 PTR 132.67.99.10.in-addr.arpa
    10 0.079637624   10.99.67.131         10.99.67.254         DNS       85 Standard query 0x0926 PTR 133.67.99.10.in-addr.arpa
```

nmap -sn 10.99.67.128/25

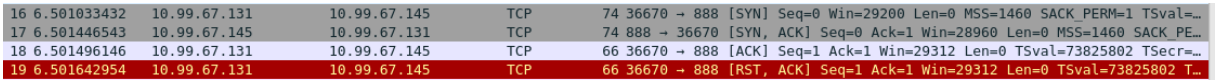
-sn parameter is ping scan. It sends arp query to every ip in the range, and gets their mac addressess if host is up. Now we see that linux host is up too.

```
root@dst:~# nmap -sn 10.99.67.128/25
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-22 20:55 EEST
Nmap scan report for 10.99.67.145
Host is up (0.00038s latency).
MAC Address: 08:00:27:9B:A6:06 (Oracle VirtualBox virtual NIC)
Nmap scan report for TheGreatFirewall.localdomain (10.99.67.254)
Host is up (0.00046s latency).
MAC Address: 08:00:27:48:41:EA (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.99.67.131
Host is up.
Nmap done: 128 IP addresses (3 hosts up) scanned in 16.55 seconds
```

```
22 0.401119809   08:00:27:d9:02:fc   ff:ff:ff:ff:ff:ff   ARP      42 Who has 10.99.67.145? Tell 10.99.67.131
23 0.401132977   08:00:27:d9:02:fc   ff:ff:ff:ff:ff:ff   ARP      42 Who has 10.99.67.146? Tell 10.99.67.131
24 0.401145835   08:00:27:d9:02:fc   ff:ff:ff:ff:ff:ff   ARP      42 Who has 10.99.67.147? Tell 10.99.67.131
25 0.401158464   08:00:27:d9:02:fc   ff:ff:ff:ff:ff:ff   ARP      42 Who has 10.99.67.148? Tell 10.99.67.131
26 0.401488596   08:00:27:9b:a6:06   08:00:27:d9:02:fc   ARP      60 10.99.67.145 is at 08:00:27:9b:a6:06
27 0.403886299   08:00:27:d9:02:fc   ff:ff:ff:ff:ff:ff   ARP      42 Who has 10.99.67.151? Tell 10.99.67.131
28 0.403911886   08:00:27:d9:02:fc   ff:ff:ff:ff:ff:ff   ARP      42 Who has 10.99.67.152? Tell 10.99.67.131
```

nmap -sT -p888 10.99.67.145

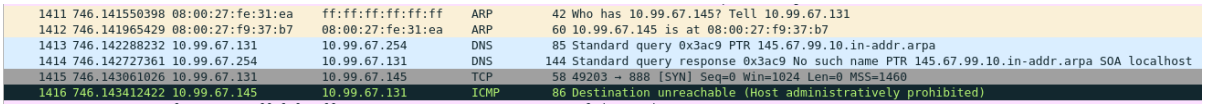
-sT is type of a TCP connect scan, where it uses complete three way handshake



16	6.501033432	10.99.67.131	10.99.67.145	TCP	74 36670 → 888 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=…
17	6.501446543	10.99.67.145	10.99.67.131	TCP	74 888 → 36670 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PE…
18	6.501496146	10.99.67.131	10.99.67.145	TCP	66 36670 → 888 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=73825802 TSecr=…
19	6.501642954	10.99.67.131	10.99.67.145	TCP	66 36670 → 888 [RST, ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=73825802 T…

nmap -sS -p888 10.99.67.145

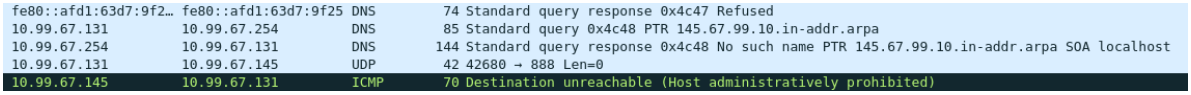
-sS is similar to previous one since it also uses three way handshake, but it terminate after target send syn/ack packet.



1411	746.141550398	08:00:27:fe:31:ea	ff:ff:ff:ff:ff:ff	ARP	42 Who has 10.99.67.145? Tell 10.99.67.131
1412	746.141965429	08:00:27:f9:37:b7	08:00:27:fe:31:ea	ARP	60 10.99.67.145 is at 08:00:27:f9:37:b7
1413	746.142288232	10.99.67.131	10.99.67.254	DNS	85 Standard query 0x3ac9 PTR 145.67.99.10.in-addr.arpa
1414	746.142727361	10.99.67.254	10.99.67.131	DNS	144 Standard query response 0x3ac9 No such name PTR 145.67.99.10.in-addr.arpa SOA localhost
1415	746.143061026	10.99.67.131	10.99.67.145	TCP	58 49203 → 888 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1416	746.143412422	10.99.67.145	10.99.67.131	ICMP	86 Destination unreachable (Host administratively prohibited)

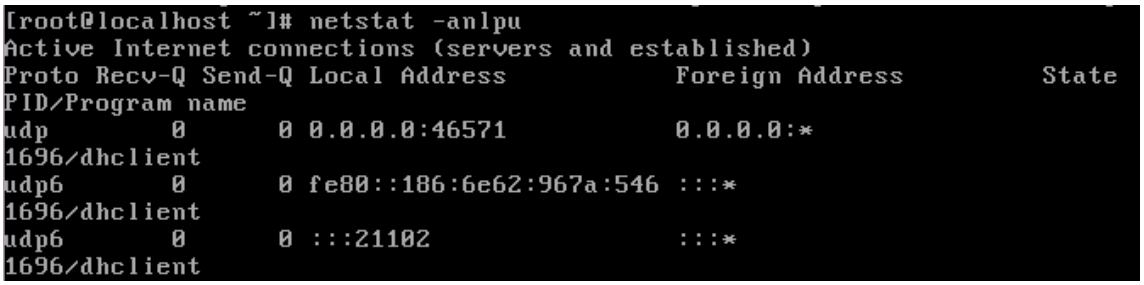
nmap -sU -p888 10.99.67.145

-sU parameter performs udp scan, target is unreachable



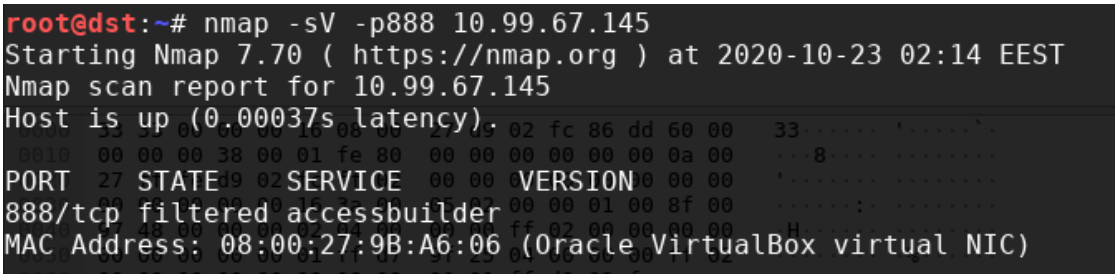
fe80::afd1:63d7:9f2…	fe80::afd1:63d7:9f25	DNS	74	Standard query response 0x4c47 Refused
10.99.67.131	10.99.67.254	DNS	85	Standard query 0x4c48 PTR 145.67.99.10.in-addr.arpa
10.99.67.254	10.99.67.131	DNS	144	Standard query response 0x4c48 No such name PTR 145.67.99.10.in-addr.arpa SOA localhost
10.99.67.131	10.99.67.145	UDP	42	42680 → 888 Len=0
10.99.67.145	10.99.67.131	ICMP	70	Destination unreachable (Host administratively prohibited)

Im not sure why its unreachable, but with command ”netstat -anlpu” it show all ports listening UDP, and 888 is not there.



```
[root@localhost ~]# netstat -anlpu
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
udp        0      0 0.0.0.0:46571           0.0.0.0:*
1696/dhclient
udp6       0      0 fe80::186:6e62:967a:546 :::*
1696/dhclient
udp6       0      0 :::21102                :::*
1696/dhclient
```

nmap -sV -p888 10.99.67.145



-sV parameter is service and version detection. The netcat listener i think captures, and shows whole tcp stream between nmap and target system. Nmap has a lot of querys when detecting the os:s and versions.

2 Task

```
root@dst:~# nmap -PE -n -Pn -oN icmp_scan.txt 10.99.67.128/25
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-22 23:40 EEST
Nmap scan report for 10.99.67.145
Host is up (0.00055s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
888/tcp open  accessbuilder
MAC Address: 08:00:27:9B:A6:06 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.99.67.254
Host is up (0.00052s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http
MAC Address: 08:00:27:48:41:EA (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.99.67.131
Host is up (0.000011s latency).
All 1000 scanned ports on 10.99.67.131 are closed

Nmap done: 128 IP addresses (3 hosts up) scanned in 8.47 seconds
```

-PE parameter is used to send icmp echo requests

```
root@dst:~# nmap -sS -n -Pn -oN tcp_scan.txt 10.99.67.145
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-22 23:43 EEST
Nmap scan report for 10.99.67.145
Host is up (0.00050s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
888/tcp open  accessbuilder
MAC Address: 08:00:27:9B:A6:06 (Oracle VirtualBox virtual NIC)
```

-sS is parameter for tcp syn scan

```
root@dst:~# nmap -sU -n -F -Pn -oN udp_scan.txt 10.99.67.254
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-22 23:49 EEST
Nmap scan report for 10.99.67.254
Host is up (0.00034s latency).
Not shown: 98 open|filtered ports
PORT    STATE SERVICE
53/udp  open  domain
123/udp open  ntp
MAC Address: 08:00:27:48:41:EA (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 3.13 seconds
```

-sU is parameter for udp scan. Linux didnt have any udp ports open, but firewall had.

I also used -F parameter to make scan quicker

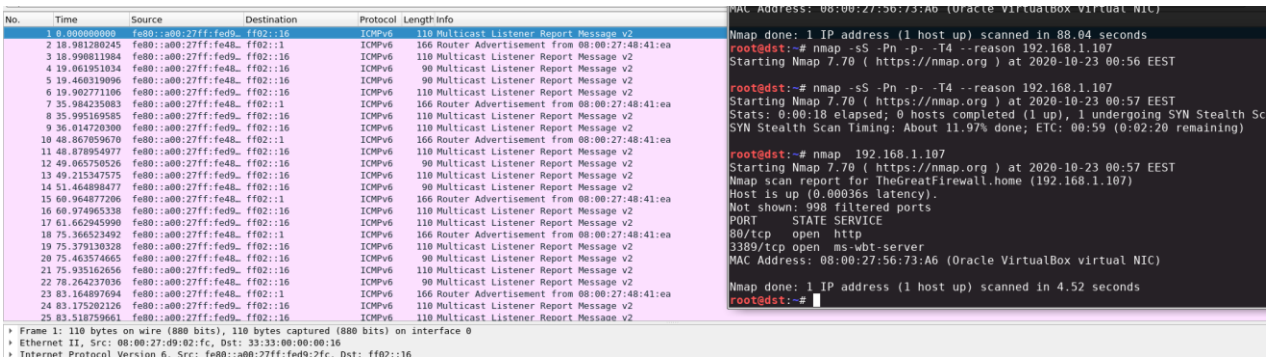
```
root@dst:~# nmap -sV -n -F -Pn -oN version_scan.txt 10.99.67.254 10.99.67.145
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-22 23:57 EEST
Stats: 0:00:02 elapsed; 0 hosts completed (2 up), 2 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 11.00% done; ETC: 23:57 (0:00:08 remaining)
Nmap scan report for 10.99.67.254
Host is up (0.00036s latency).
Not shown: 98 filtered ports
PORT   STATE SERVICE VERSION
53/tcp open  domain  (generic dns response: NOTIMP)
80/tcp open  http    nginx
1 service unrecognized despite returning data. If you know the service/version, please sub
mit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.70%I=7%D=10/22%Time=5F91F258%P=x86_64-pc-linux-gnu%r(DNS
SF:VersionBindReqTCP,20,"\0\x1e\0\x06\x81\x85\0\x01\0\0\0\0\0\0\x07version
SF:\x04bind\0\0\x10\0\x03")%r(DNSStatusRequestTCP,E,"\0\x0c\0\0\x90\x04\0\
SF:0\0\0\0\0\0\0");
MAC Address: 08:00:27:48:41:EA (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.99.67.145
Host is up (0.00036s latency).
Not shown: 98 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.4 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
MAC Address: 08:00:27:9B:A6:06 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submi
t/ .
Nmap done: 2 IP addresses (2 hosts up) scanned in 24.93 seconds
```

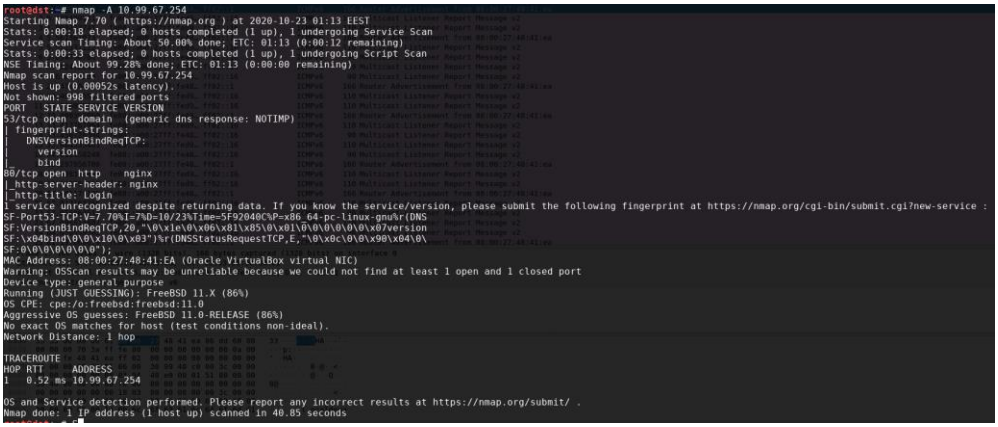
-sV is version detecting parameter. I scanned both ip:s at same time.

3 Firewall rules

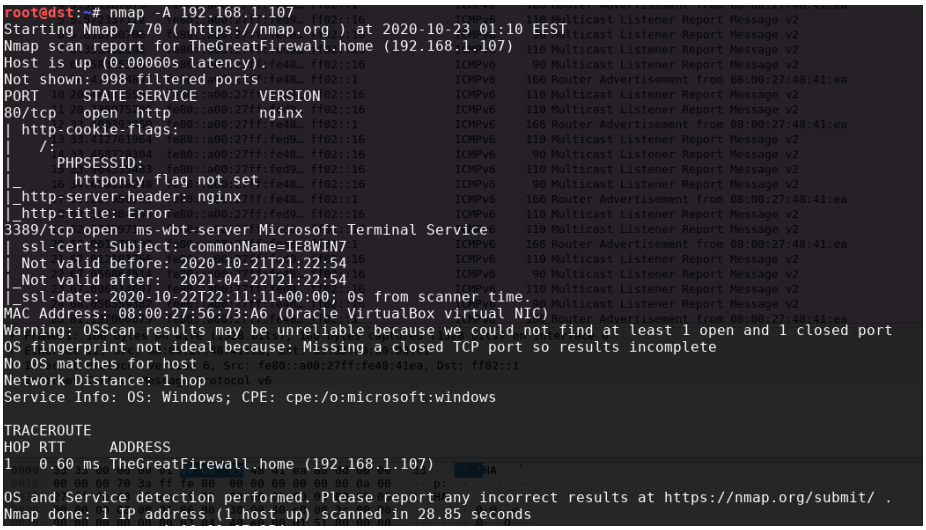
I dont know if i got the task right, but when scanning firewall through WAN, i get absolutely nothing to wireshark input. Makes sense to me.



LAN Scan:



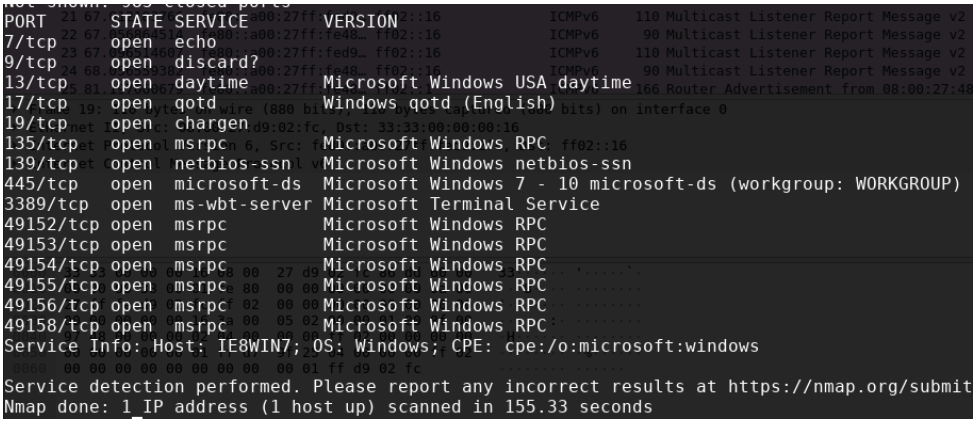
WAN Scan:



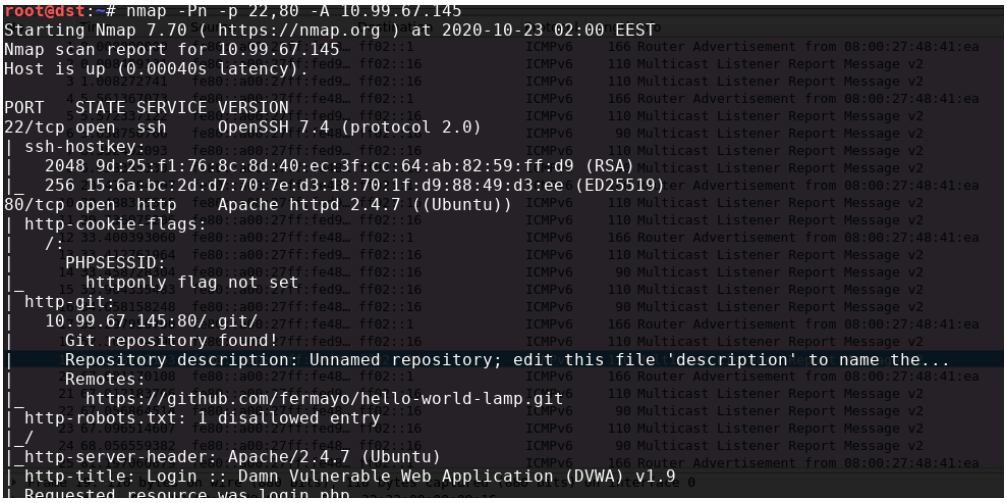
Both scans found one open port which other on didnt. WAN has 3389 and LAN has 53: HTTP: 80 available through both.

4 More scans

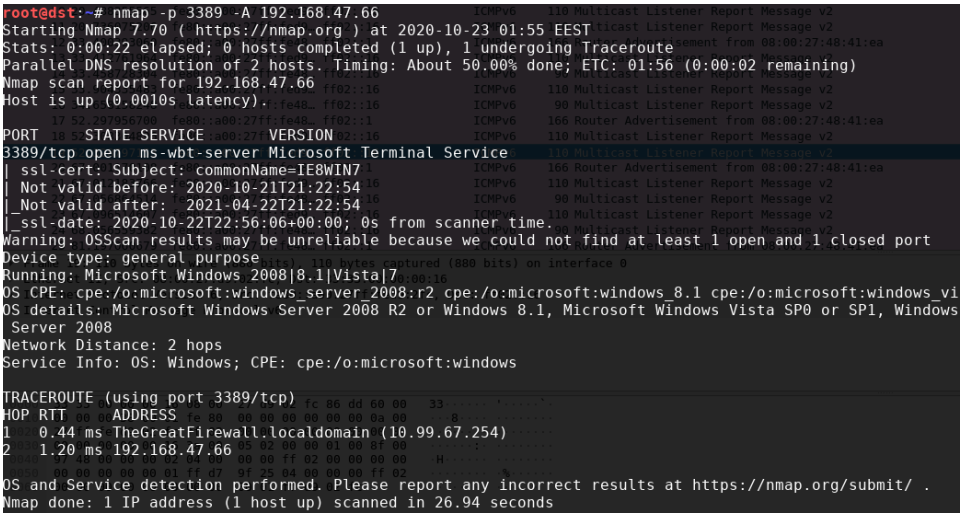
Windows has lot more ports open than linux



Both ssh and http ports are open in linux, so, as far as i know windows should be able to get into linux system through those ports



rdp port is found in windows and it is open, but i have no idea if connection is allowed



5 Conclusion

This lab was kinda hard to keep up with. I wish there were simple guide for tasks, what you want me to do or find out about. It took way too much time for me to figure out the tasks, and i dont think result is exactly like it was meant. In any case i learned a lot from nmap and its parameters. Also im starting to get more familiar with wireshark.