jamk.fi

Lab 02. Port scan

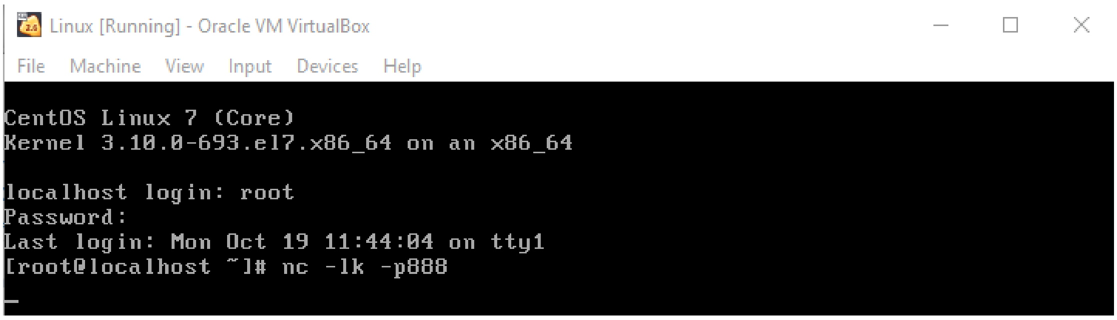
Teacher: Markku Vajaranta
Autor of Assignment: Adam Pawełek
Group: TTKS0700-3001
Jamk number: AA4917

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

1 Understanding NMAP

1.1 start netcat on Linux (terminal, nc -lk –p888, starts netcat listener on port 888)

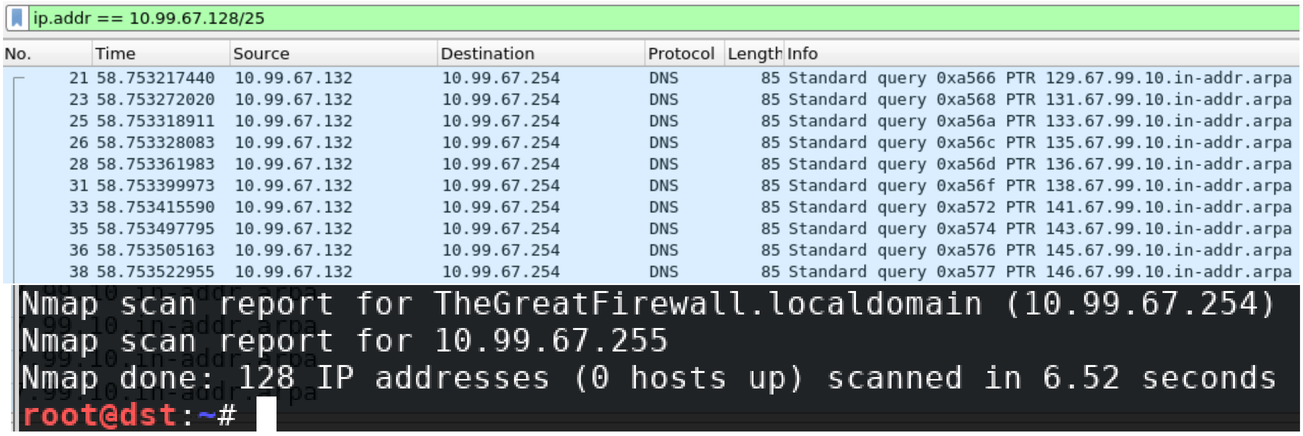


Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

```
CentOS Linux 7 (Core)
Kernel 3.10.0-693.el7.x86_64 on an x86_64

localhost login: root
Password:
Last login: Mon Oct 19 11:44:04 on tty1
[root@localhost ~]# nc -lk -p888
_
```

1.2 nmap -sL

Lan 1

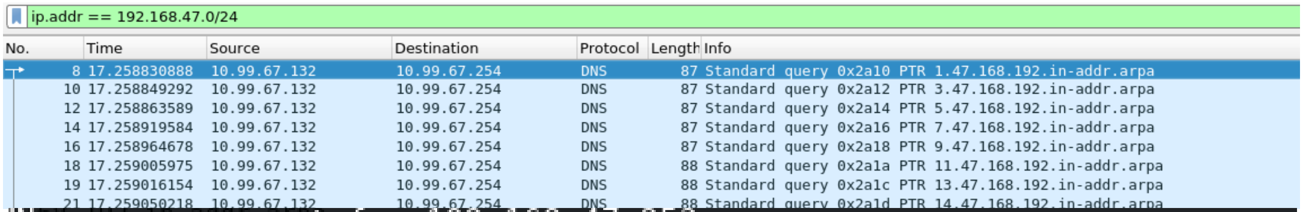


```
ip.addr == 10.99.67.128/25
No.  Time          Source        Destination   Protocol Length Info
  21 58.753217440  10.99.67.132  10.99.67.254  DNS      85 Standard query 0xa566 PTR 129.67.99.10.in-addr.arpa
  23 58.753272020  10.99.67.132  10.99.67.254  DNS      85 Standard query 0xa568 PTR 131.67.99.10.in-addr.arpa
  25 58.753318911  10.99.67.132  10.99.67.254  DNS      85 Standard query 0xa56a PTR 133.67.99.10.in-addr.arpa
  26 58.753328083  10.99.67.132  10.99.67.254  DNS      85 Standard query 0xa56c PTR 135.67.99.10.in-addr.arpa
  28 58.753361983  10.99.67.132  10.99.67.254  DNS      85 Standard query 0xa56d PTR 136.67.99.10.in-addr.arpa
  31 58.753399973  10.99.67.132  10.99.67.254  DNS      85 Standard query 0xa56f PTR 138.67.99.10.in-addr.arpa
  33 58.753415590  10.99.67.132  10.99.67.254  DNS      85 Standard query 0xa572 PTR 141.67.99.10.in-addr.arpa
  35 58.753497795  10.99.67.132  10.99.67.254  DNS      85 Standard query 0xa574 PTR 143.67.99.10.in-addr.arpa
  36 58.753505163  10.99.67.132  10.99.67.254  DNS      85 Standard query 0xa576 PTR 145.67.99.10.in-addr.arpa
  38 58.753522955  10.99.67.132  10.99.67.254  DNS      85 Standard query 0xa577 PTR 146.67.99.10.in-addr.arpa
```

```
Nmap scan report for TheGreatFirewall.localdomain (10.99.67.254)
Nmap scan report for 10.99.67.255
Nmap done: 128 IP addresses (0 hosts up) scanned in 6.52 seconds
root@dst:~#
```

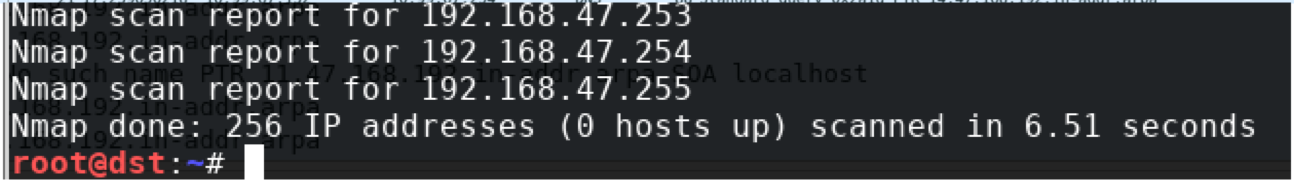
This scan doesn’t find any host up.

Lan2:



ip.addr == 192.168.47.0/24

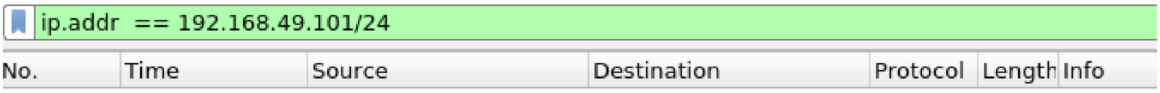
No.	Time	Source	Destination	Protocol	Length	Info
8	17.258830888	10.99.67.132	10.99.67.254	DNS	87	Standard query 0x2a10 PTR 1.47.168.192.in-addr.arpa
10	17.258849292	10.99.67.132	10.99.67.254	DNS	87	Standard query 0x2a12 PTR 3.47.168.192.in-addr.arpa
12	17.258863589	10.99.67.132	10.99.67.254	DNS	87	Standard query 0x2a14 PTR 5.47.168.192.in-addr.arpa
14	17.258919584	10.99.67.132	10.99.67.254	DNS	87	Standard query 0x2a16 PTR 7.47.168.192.in-addr.arpa
16	17.258964678	10.99.67.132	10.99.67.254	DNS	87	Standard query 0x2a18 PTR 9.47.168.192.in-addr.arpa
18	17.259005975	10.99.67.132	10.99.67.254	DNS	88	Standard query 0x2a1a PTR 11.47.168.192.in-addr.arpa
19	17.259016154	10.99.67.132	10.99.67.254	DNS	88	Standard query 0x2a1c PTR 13.47.168.192.in-addr.arpa
21	17.259050218	10.99.67.132	10.99.67.254	DNS	88	Standard query 0x2a1d PTR 14.47.168.192.in-addr.arpa



```
Nmap scan report for 192.168.47.253
Nmap scan report for 192.168.47.254
Nmap scan report for 192.168.47.255
Nmap done: 256 IP addresses (0 hosts up) scanned in 6.51 seconds
root@dst:~#
```

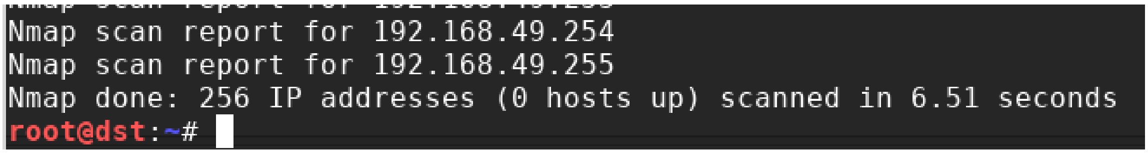
This scan doesn't find any host up.

WAN:



ip.addr == 192.168.49.101/24

No.	Time	Source	Destination	Protocol	Length	Info

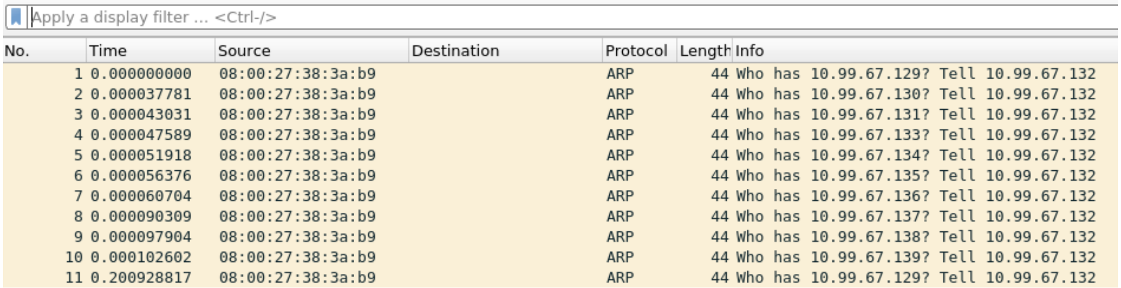


```
Nmap scan report for 192.168.49.253
Nmap scan report for 192.168.49.254
Nmap scan report for 192.168.49.255
Nmap done: 256 IP addresses (0 hosts up) scanned in 6.51 seconds
root@dst:~#
```

Firewall probably didn't allow scan WAN network. (Ss scan -> middle handshake scan works fine)

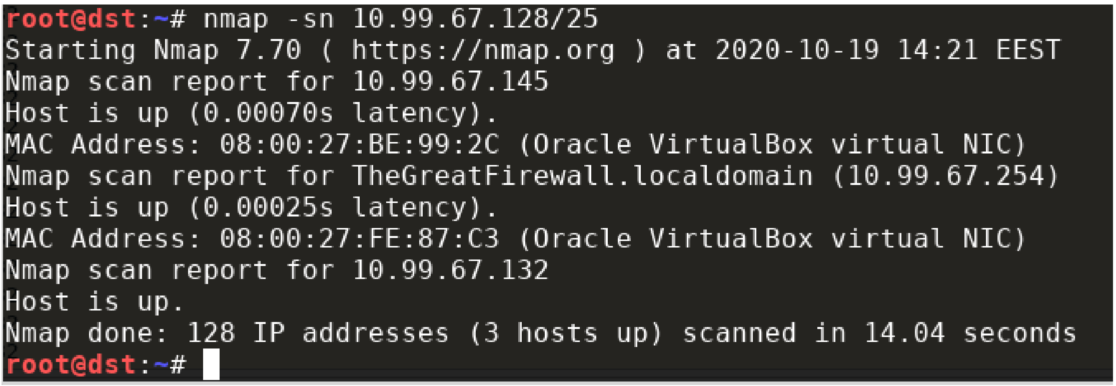
1.3 nmap -sn

Lan1:



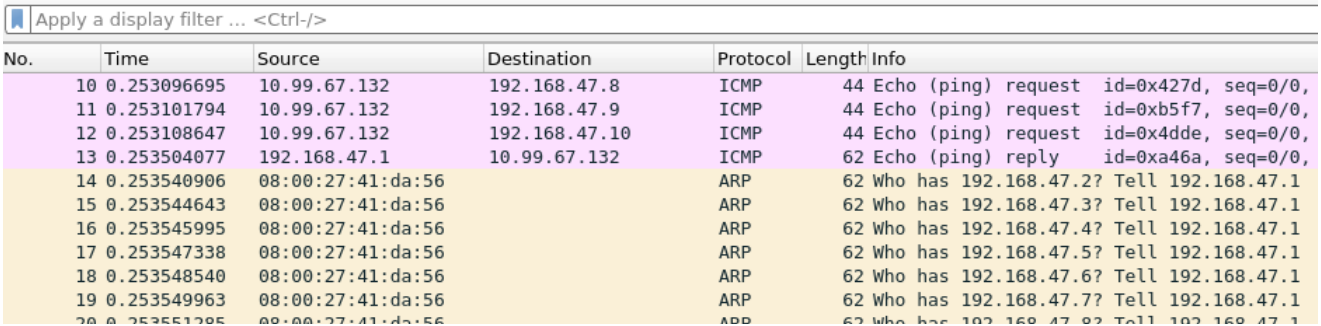
Apply a display filter … <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	08:00:27:38:3a:b9		ARP	44	Who has 10.99.67.129? Tell 10.99.67.132
2	0.000037781	08:00:27:38:3a:b9		ARP	44	Who has 10.99.67.130? Tell 10.99.67.132
3	0.000043031	08:00:27:38:3a:b9		ARP	44	Who has 10.99.67.131? Tell 10.99.67.132
4	0.000047589	08:00:27:38:3a:b9		ARP	44	Who has 10.99.67.133? Tell 10.99.67.132
5	0.000051918	08:00:27:38:3a:b9		ARP	44	Who has 10.99.67.134? Tell 10.99.67.132
6	0.000056376	08:00:27:38:3a:b9		ARP	44	Who has 10.99.67.135? Tell 10.99.67.132
7	0.000060704	08:00:27:38:3a:b9		ARP	44	Who has 10.99.67.136? Tell 10.99.67.132
8	0.000090309	08:00:27:38:3a:b9		ARP	44	Who has 10.99.67.137? Tell 10.99.67.132
9	0.000097904	08:00:27:38:3a:b9		ARP	44	Who has 10.99.67.138? Tell 10.99.67.132
10	0.000102602	08:00:27:38:3a:b9		ARP	44	Who has 10.99.67.139? Tell 10.99.67.132
11	0.200928817	08:00:27:38:3a:b9		ARP	44	Who has 10.99.67.129? Tell 10.99.67.132



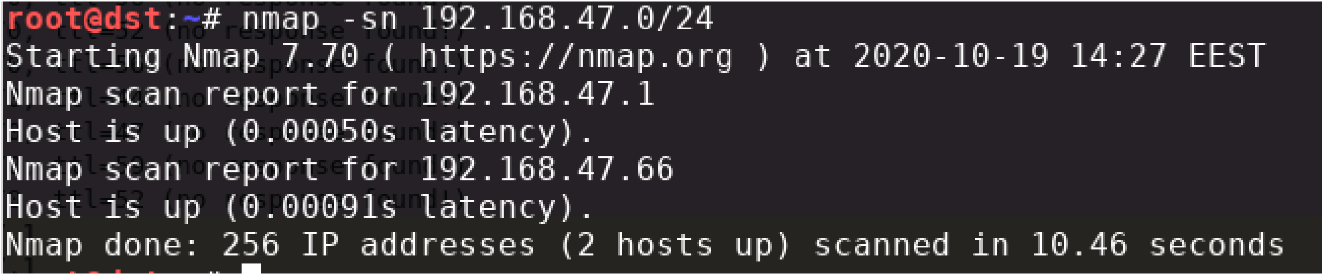
```
root@dst:~# nmap -sn 10.99.67.128/25
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-19 14:21 EEST
Nmap scan report for 10.99.67.145
Host is up (0.00070s latency).
MAC Address: 08:00:27:BE:99:2C (Oracle VirtualBox virtual NIC)
Nmap scan report for TheGreatFirewall.localdomain (10.99.67.254)
Host is up (0.00025s latency).
MAC Address: 08:00:27:FE:87:C3 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.99.67.132
Host is up.
Nmap done: 128 IP addresses (3 hosts up) scanned in 14.04 seconds
root@dst:~#
```

Lan2:



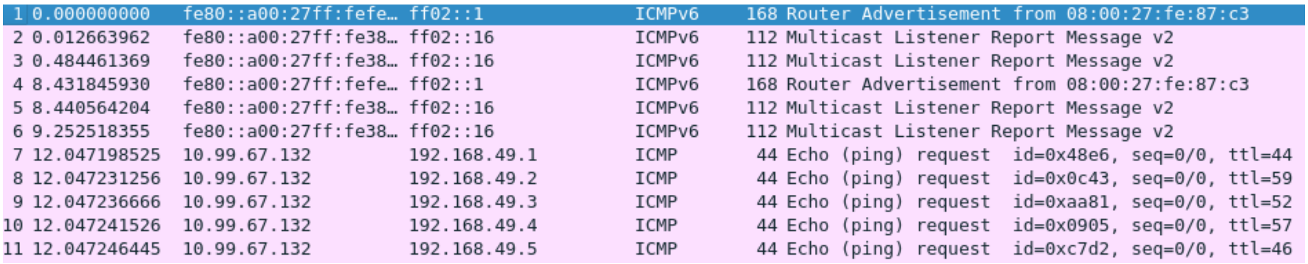
Apply a display filter … <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
10	0.253096695	10.99.67.132	192.168.47.8	ICMP	44	Echo (ping) request id=0x427d, seq=0/0,
11	0.253101794	10.99.67.132	192.168.47.9	ICMP	44	Echo (ping) request id=0xb5f7, seq=0/0,
12	0.253108647	10.99.67.132	192.168.47.10	ICMP	44	Echo (ping) request id=0x4dde, seq=0/0,
13	0.253504077	192.168.47.1	10.99.67.132	ICMP	62	Echo (ping) reply id=0xa46a, seq=0/0,
14	0.253540906	08:00:27:41:da:56		ARP	62	Who has 192.168.47.2? Tell 192.168.47.1
15	0.253544643	08:00:27:41:da:56		ARP	62	Who has 192.168.47.3? Tell 192.168.47.1
16	0.253545995	08:00:27:41:da:56		ARP	62	Who has 192.168.47.4? Tell 192.168.47.1
17	0.253547338	08:00:27:41:da:56		ARP	62	Who has 192.168.47.5? Tell 192.168.47.1
18	0.253548540	08:00:27:41:da:56		ARP	62	Who has 192.168.47.6? Tell 192.168.47.1
19	0.253549963	08:00:27:41:da:56		ARP	62	Who has 192.168.47.7? Tell 192.168.47.1
20	0.253551285	08:00:27:41:da:56		ARP	62	Who has 192.168.47.8? Tell 192.168.47.1

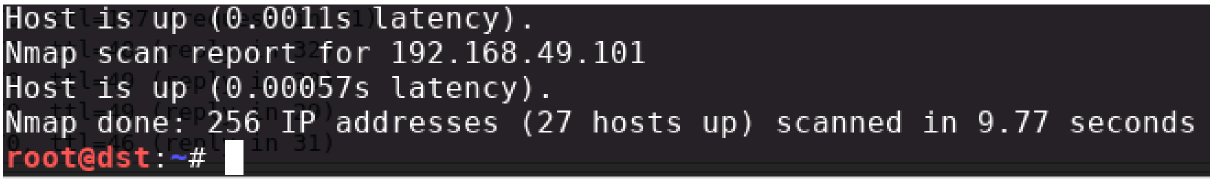


```
root@dst:~# nmap -sn 192.168.47.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-19 14:27 EEST
Nmap scan report for 192.168.47.1
Host is up (0.00050s latency).
Nmap scan report for 192.168.47.66
Host is up (0.00091s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 10.46 seconds
```

Wan:

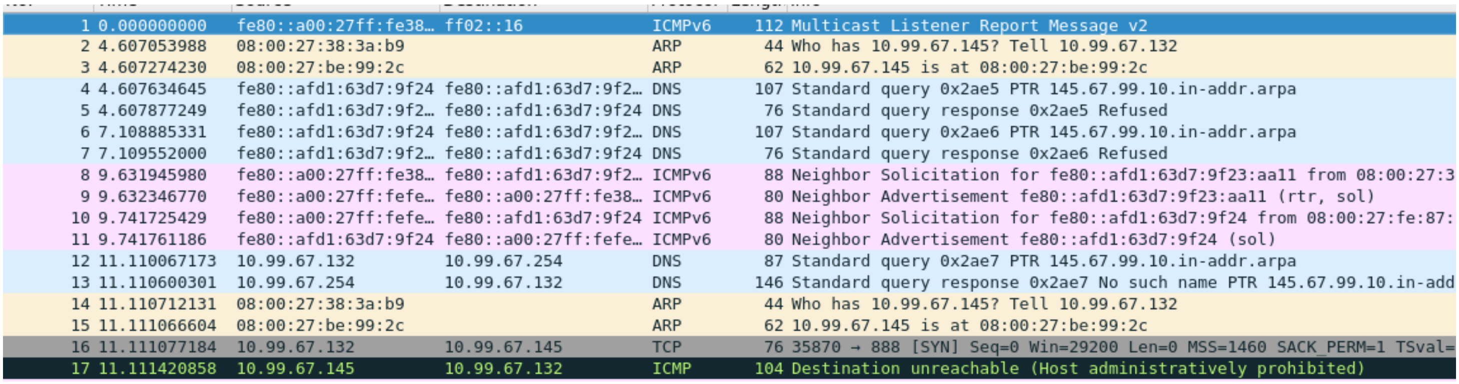


```
 1 0.000000000   fe80::a00:27ff:fefe… ff02::1            ICMPv6    168 Router Advertisement from 08:00:27:fe:87:c3
 2 0.012663962   fe80::a00:27ff:fe38… ff02::16           ICMPv6    112 Multicast Listener Report Message v2
 3 0.484461369   fe80::a00:27ff:fe38… ff02::16           ICMPv6    112 Multicast Listener Report Message v2
 4 8.431845930   fe80::a00:27ff:fefe… ff02::1            ICMPv6    168 Router Advertisement from 08:00:27:fe:87:c3
 5 8.440564204   fe80::a00:27ff:fe38… ff02::16           ICMPv6    112 Multicast Listener Report Message v2
 6 9.252518355   fe80::a00:27ff:fe38… ff02::16           ICMPv6    112 Multicast Listener Report Message v2
 7 12.047198525  10.99.67.132         192.168.49.1       ICMP       44 Echo (ping) request  id=0x48e6, seq=0/0, ttl=44
 8 12.047231256  10.99.67.132         192.168.49.2       ICMP       44 Echo (ping) request  id=0x0c43, seq=0/0, ttl=59
 9 12.047236666  10.99.67.132         192.168.49.3       ICMP       44 Echo (ping) request  id=0xaa81, seq=0/0, ttl=52
10 12.047241526  10.99.67.132         192.168.49.4       ICMP       44 Echo (ping) request  id=0x0905, seq=0/0, ttl=57
11 12.047246445  10.99.67.132         192.168.49.5       ICMP       44 Echo (ping) request  id=0xc7d2, seq=0/0, ttl=46
```

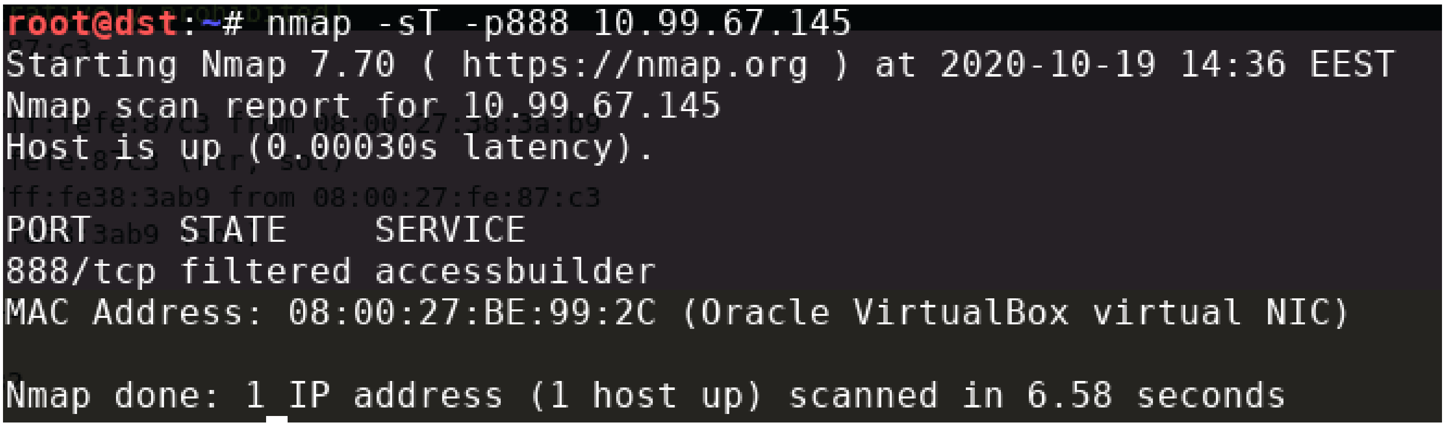


```
Host is up (0.0011s latency).
Nmap scan report for 192.168.49.101
Host is up (0.00057s latency).
Nmap done: 256 IP addresses (27 hosts up) scanned in 9.77 seconds
root@dst:~#
```

1.4 nmap -sT -p888 10.99.67.145

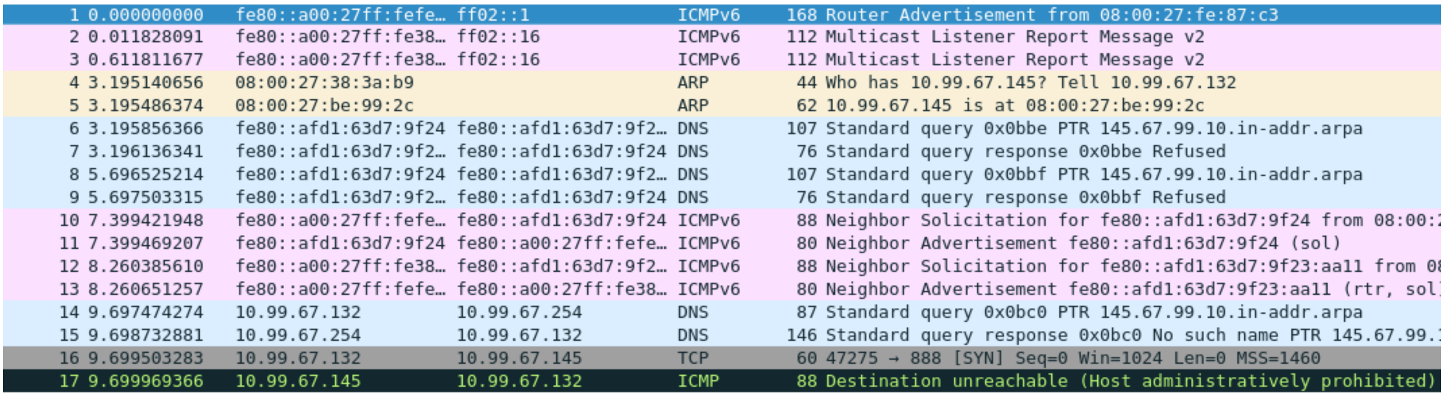


```
 1 0.000000000   fe80::a00:27ff:fe38… ff02::16             ICMPv6   112 Multicast Listener Report Message v2
 2 4.607053988   08:00:27:38:3a:b9                         ARP       44 Who has 10.99.67.145? Tell 10.99.67.132
 3 4.607274230   08:00:27:be:99:2c                         ARP       62 10.99.67.145 is at 08:00:27:be:99:2c
 4 4.607634645   fe80::afd1:63d7:9f24 fe80::afd1:63d7:9f2… DNS      107 Standard query 0x2ae5 PTR 145.67.99.10.in-addr.arpa
 5 4.607877249   fe80::afd1:63d7:9f2… fe80::afd1:63d7:9f24 DNS       76 Standard query response 0x2ae5 Refused
 6 7.108885331   fe80::afd1:63d7:9f24 fe80::afd1:63d7:9f2… DNS      107 Standard query 0x2ae6 PTR 145.67.99.10.in-addr.arpa
 7 7.109552000   fe80::afd1:63d7:9f2… fe80::afd1:63d7:9f24 DNS       76 Standard query response 0x2ae6 Refused
 8 9.631945980   fe80::a00:27ff:fe38… fe80::afd1:63d7:9f2… ICMPv6    88 Neighbor Solicitation for fe80::afd1:63d7:9f23:aa11 from 08:00:27:3
 9 9.632346770   fe80::a00:27ff:fefe… fe80::a00:27ff:fe38… ICMPv6    80 Neighbor Advertisement fe80::afd1:63d7:9f23:aa11 (rtr, sol)
10 9.741725429   fe80::a00:27ff:fefe… fe80::afd1:63d7:9f24 ICMPv6    88 Neighbor Solicitation for fe80::afd1:63d7:9f24 from 08:00:27:fe:87:
11 9.741761186   fe80::afd1:63d7:9f24 fe80::a00:27ff:fefe… ICMPv6    80 Neighbor Advertisement fe80::afd1:63d7:9f24 (sol)
12 11.110067173  10.99.67.132         10.99.67.254         DNS       87 Standard query 0x2ae7 PTR 145.67.99.10.in-addr.arpa
13 11.110600301  10.99.67.254         10.99.67.132         DNS      146 Standard query response 0x2ae7 No such name PTR 145.67.99.10.in-add
14 11.110712131  08:00:27:38:3a:b9                         ARP       44 Who has 10.99.67.145? Tell 10.99.67.132
15 11.111066604  08:00:27:be:99:2c                         ARP       62 10.99.67.145 is at 08:00:27:be:99:2c
16 11.111077184  10.99.67.132         10.99.67.145         TCP       76 35870 → 888 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=
17 11.111420858  10.99.67.145         10.99.67.132         ICMP     104 Destination unreachable (Host administratively prohibited)
```

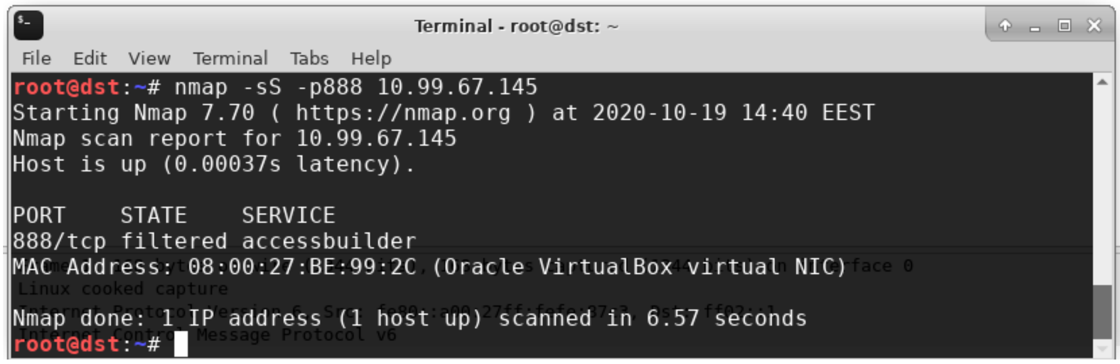


```
root@dst:~# nmap -sT -p888 10.99.67.145
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-19 14:36 EEST
Nmap scan report for 10.99.67.145
Host is up (0.00030s latency).

PORT    STATE    SERVICE
888/tcp filtered accessbuilder
MAC Address: 08:00:27:BE:99:2C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 6.58 seconds
```

1.5 nmap -sS -p888 10.99.67.145

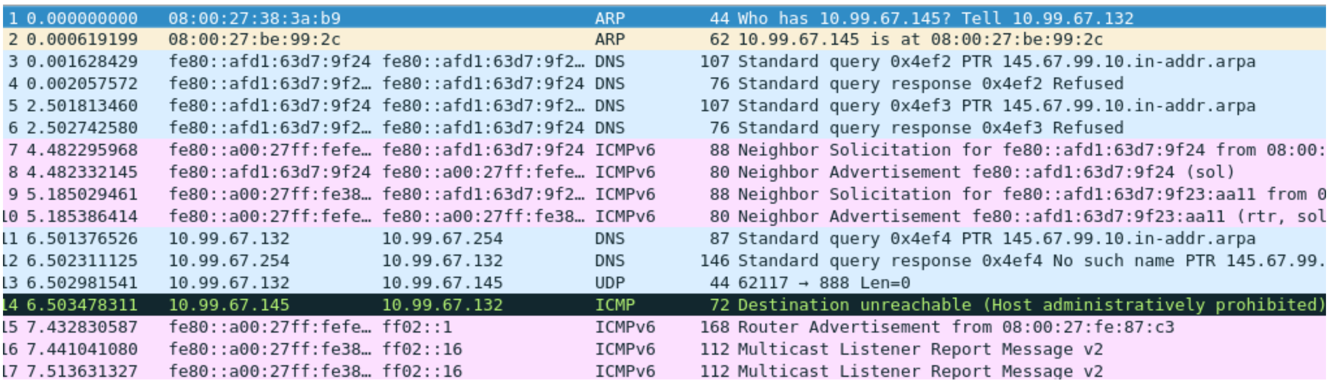


```
 1 0.000000000  fe80::a00:27ff:fefe… ff02::1              ICMPv6  168 Router Advertisement from 08:00:27:fe:87:c3
 2 0.011828091  fe80::a00:27ff:fe38… ff02::16             ICMPv6  112 Multicast Listener Report Message v2
 3 0.611811677  fe80::a00:27ff:fe38… ff02::16             ICMPv6  112 Multicast Listener Report Message v2
 4 3.195140656  08:00:27:38:3a:b9                         ARP      44 Who has 10.99.67.145? Tell 10.99.67.132
 5 3.195486374  08:00:27:be:99:2c                         ARP      62 10.99.67.145 is at 08:00:27:be:99:2c
 6 3.195856366  fe80::afd1:63d7:9f24 fe80::afd1:63d7:9f2… DNS     107 Standard query 0x0bbe PTR 145.67.99.10.in-addr.arpa
 7 3.196136341  fe80::afd1:63d7:9f2… fe80::afd1:63d7:9f24 DNS      76 Standard query response 0x0bbe Refused
 8 5.696525214  fe80::afd1:63d7:9f24 fe80::afd1:63d7:9f2… DNS     107 Standard query 0x0bbf PTR 145.67.99.10.in-addr.arpa
 9 5.697503315  fe80::afd1:63d7:9f2… fe80::afd1:63d7:9f24 DNS      76 Standard query response 0x0bbf Refused
10 7.399421948  fe80::a00:27ff:fefe… fe80::afd1:63d7:9f24 ICMPv6   88 Neighbor Solicitation for fe80::afd1:63d7:9f24 from 08:00::
11 7.399469207  fe80::afd1:63d7:9f24 fe80::a00:27ff:fefe… ICMPv6   80 Neighbor Advertisement fe80::afd1:63d7:9f24 (sol)
12 8.260385610  fe80::a00:27ff:fe38… fe80::afd1:63d7:9f2… ICMPv6   88 Neighbor Solicitation for fe80::afd1:63d7:9f23:aa11 from 08
13 8.260651257  fe80::a00:27ff:fefe… fe80::a00:27ff:fe38… ICMPv6   80 Neighbor Advertisement fe80::afd1:63d7:9f23:aa11 (rtr, sol
14 9.697474274  10.99.67.132         10.99.67.254         DNS      87 Standard query 0x0bc0 PTR 145.67.99.10.in-addr.arpa
15 9.698732881  10.99.67.254         10.99.67.132         DNS     146 Standard query response 0x0bc0 No such name PTR 145.67.99.1
16 9.699503283  10.99.67.132         10.99.67.145         TCP      60 47275 → 888 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17 9.699969366  10.99.67.145         10.99.67.132         ICMP     88 Destination unreachable (Host administratively prohibited)
```

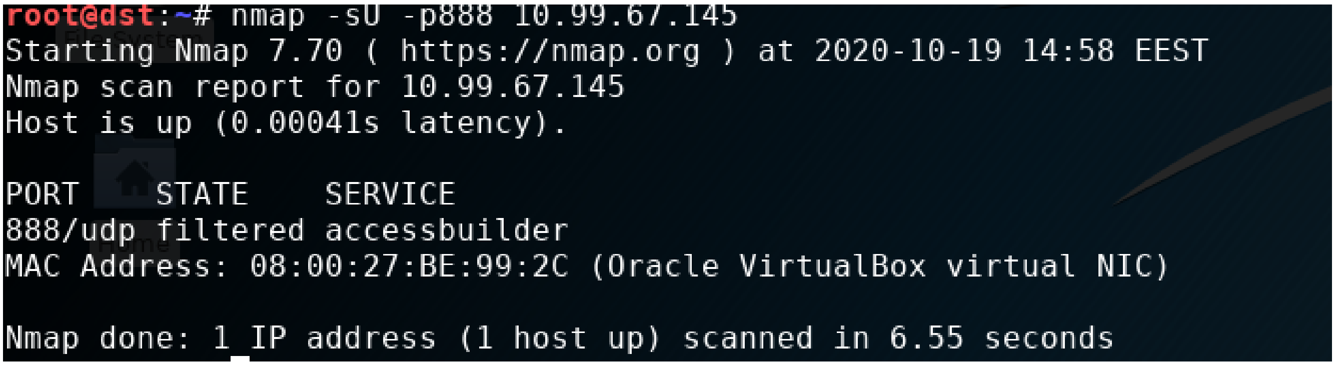


```
root@dst:~# nmap -sS -p888 10.99.67.145
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-19 14:40 EEST
Nmap scan report for 10.99.67.145
Host is up (0.00037s latency).

PORT     STATE    SERVICE
888/tcp filtered accessbuilder
MAC Address: 08:00:27:BE:99:2C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 6.57 seconds
root@dst:~#
```

1.6 nmap -SU -p888 10.99.67.145



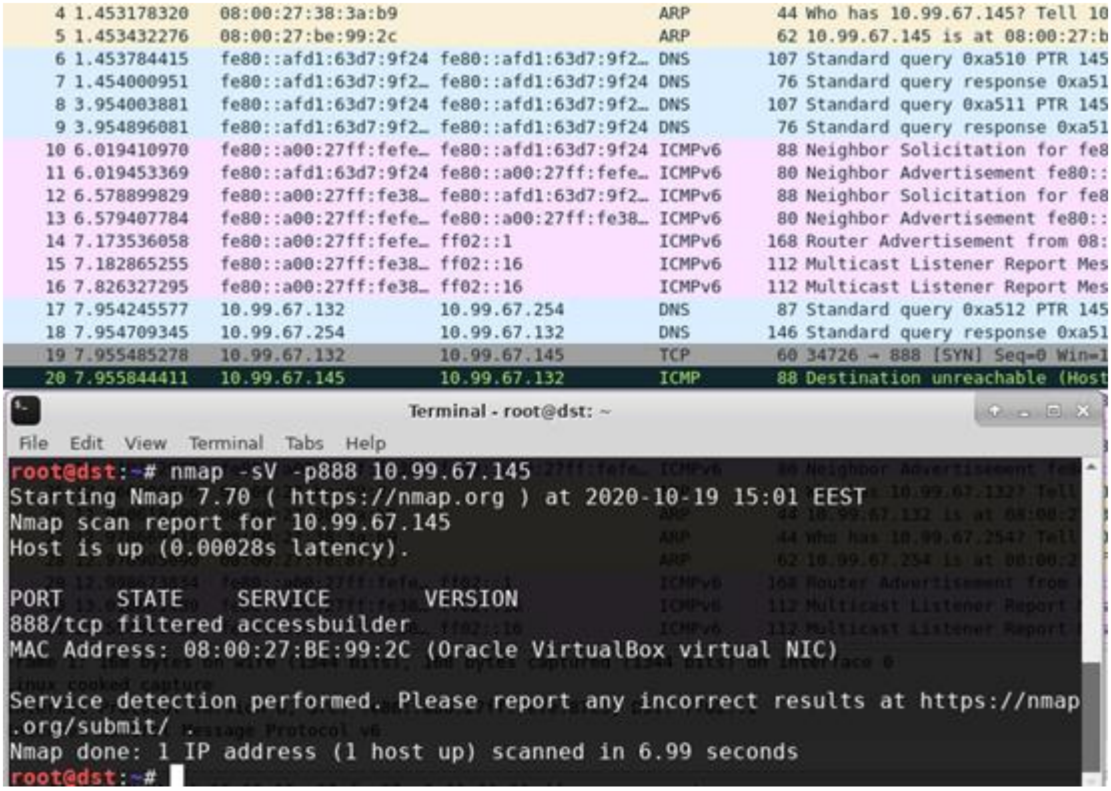
```
 1 0.000000000   08:00:27:38:3a:b9                               ARP        44 Who has 10.99.67.145? Tell 10.99.67.132
 2 0.000619199   08:00:27:be:99:2c                               ARP        62 10.99.67.145 is at 08:00:27:be:99:2c
 3 0.001628429   fe80::afd1:63d7:9f24 fe80::afd1:63d7:9f2… DNS       107 Standard query 0x4ef2 PTR 145.67.99.10.in-addr.arpa
 4 0.002057572   fe80::afd1:63d7:9f2… fe80::afd1:63d7:9f24 DNS        76 Standard query response 0x4ef2 Refused
 5 2.501813460   fe80::afd1:63d7:9f24 fe80::afd1:63d7:9f2… DNS       107 Standard query 0x4ef3 PTR 145.67.99.10.in-addr.arpa
 6 2.502742580   fe80::afd1:63d7:9f2… fe80::afd1:63d7:9f24 DNS        76 Standard query response 0x4ef3 Refused
 7 4.482295968   fe80::a00:27ff:fefe… fe80::afd1:63d7:9f24 ICMPv6     88 Neighbor Solicitation for fe80::afd1:63d7:9f24 from 08:00:
 8 4.482332145   fe80::afd1:63d7:9f24 fe80::a00:27ff:fefe… ICMPv6     80 Neighbor Advertisement fe80::afd1:63d7:9f24 (sol)
 9 5.185029461   fe80::a00:27ff:fe38… fe80::afd1:63d7:9f2… ICMPv6     88 Neighbor Solicitation for fe80::afd1:63d7:9f23:aa11 from 0
10 5.185386414   fe80::a00:27ff:fefe… fe80::a00:27ff:fe38… ICMPv6     80 Neighbor Advertisement fe80::afd1:63d7:9f23:aa11 (rtr, sol
11 6.501376526   10.99.67.132         10.99.67.254         DNS        87 Standard query 0x4ef4 PTR 145.67.99.10.in-addr.arpa
12 6.502311125   10.99.67.254         10.99.67.132         DNS       146 Standard query response 0x4ef4 No such name PTR 145.67.99.
13 6.502981541   10.99.67.132         10.99.67.145         UDP        44 62117 → 888 Len=0
14 6.503478311   10.99.67.145         10.99.67.132         ICMP       72 Destination unreachable (Host administratively prohibited)
15 7.432830587   fe80::a00:27ff:fefe… ff02::1              ICMPv6    168 Router Advertisement from 08:00:27:fe:87:c3
16 7.441041080   fe80::a00:27ff:fe38… ff02::16             ICMPv6    112 Multicast Listener Report Message v2
17 7.513631327   fe80::a00:27ff:fe38… ff02::16             ICMPv6    112 Multicast Listener Report Message v2
```



```
root@dst:~# nmap -sU -p888 10.99.67.145
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-19 14:58 EEST
Nmap scan report for 10.99.67.145
Host is up (0.00041s latency).

PORT    STATE    SERVICE
888/udp filtered accessbuilder
MAC Address: 08:00:27:BE:99:2C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 6.55 seconds
```

I ’ve got the same reult as all others scans. When I was scanning that target without -p888 it returns also ports that are open.

1.7 nmap -SV -p888 10.99.67.145



```
 4 1.453178320   08:00:27:38:3a:b9                          ARP       44 Who has 10.99.67.145? Tell 10
 5 1.453432276   08:00:27:be:99:2c                          ARP       62 10.99.67.145 is at 08:00:27:b
 6 1.453784415   fe80::afd1:63d7:9f24 fe80::afd1:63d7:9f2… DNS      107 Standard query 0xa510 PTR 145
 7 1.454000951   fe80::afd1:63d7:9f2… fe80::afd1:63d7:9f24 DNS       76 Standard query response 0xa51
 8 3.954003881   fe80::afd1:63d7:9f24 fe80::afd1:63d7:9f2… DNS      107 Standard query 0xa511 PTR 145
 9 3.954896081   fe80::afd1:63d7:9f2… fe80::afd1:63d7:9f24 DNS       76 Standard query response 0xa51
10 6.019410970   fe80::a00:27ff:fefe… fe80::afd1:63d7:9f24 ICMPv6    88 Neighbor Solicitation for fe8
11 6.019453369   fe80::afd1:63d7:9f24 fe80::a00:27ff:fefe… ICMPv6    80 Neighbor Advertisement fe80::
12 6.578899829   fe80::a00:27ff:fe38… fe80::afd1:63d7:9f2… ICMPv6    88 Neighbor Solicitation for fe8
13 6.579407784   fe80::a00:27ff:fefe… fe80::a00:27ff:fe38… ICMPv6    80 Neighbor Advertisement fe80::
14 7.173536058   fe80::a00:27ff:fefe… ff02::1              ICMPv6   168 Router Advertisement from 08:
15 7.182865255   fe80::a00:27ff:fe38… ff02::16             ICMPv6   112 Multicast Listener Report Mes
16 7.826327295   fe80::a00:27ff:fe38… ff02::16             ICMPv6   112 Multicast Listener Report Mes
17 7.954245577   10.99.67.132         10.99.67.254         DNS       87 Standard query 0xa512 PTR 145
18 7.954709345   10.99.67.254         10.99.67.132         DNS      146 Standard query response 0xa51
19 7.955485278   10.99.67.132         10.99.67.145         TCP       60 34726 → 888 [SYN] Seq=0 Win=1
20 7.955844411   10.99.67.145         10.99.67.132         ICMP      88 Destination unreachable (Host
```

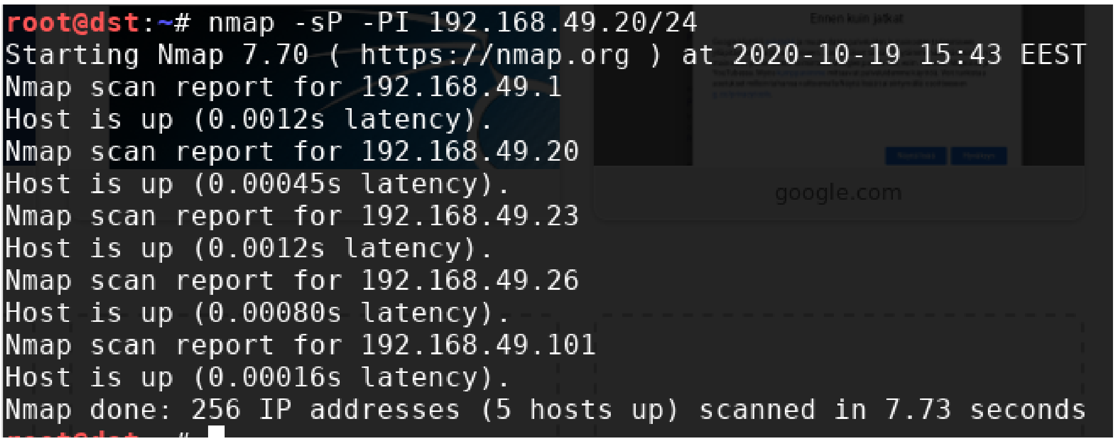
```
root@dst:~# nmap -sV -p888 10.99.67.145
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-19 15:01 EEST
Nmap scan report for 10.99.67.145
Host is up (0.00028s latency).

PORT     STATE    SERVICE       VERSION
888/tcp filtered accessbuilder
MAC Address: 08:00:27:BE:99:2C (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.99 seconds
root@dst:~#
```

Netcat listener when I started this scan did not show enything.

I was doing scan on my linux, windows and computers in dynamo campus laboratory and everyware I've got the same results.

2 Run NMAP from KALI terminal

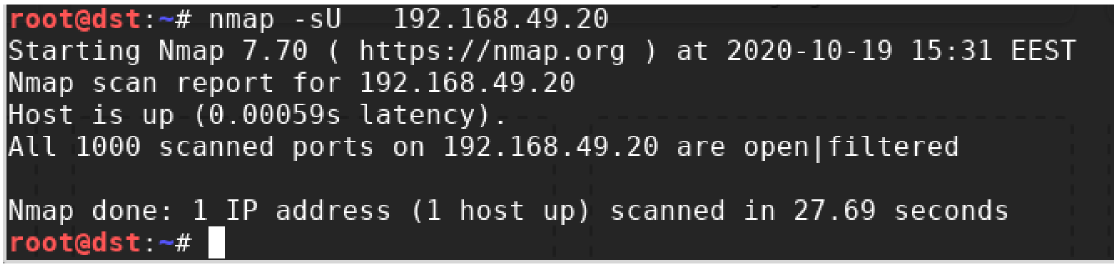
2.1 Run ICMP –scan against target network



```
root@dst:~# nmap -sP -PI 192.168.49.20/24
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-19 15:43 EEST
Nmap scan report for 192.168.49.1
Host is up (0.0012s latency).
Nmap scan report for 192.168.49.20
Host is up (0.00045s latency).
Nmap scan report for 192.168.49.23
Host is up (0.0012s latency).
Nmap scan report for 192.168.49.26
Host is up (0.00080s latency).
Nmap scan report for 192.168.49.101
Host is up (0.00016s latency).
Nmap done: 256 IP addresses (5 hosts up) scanned in 7.73 seconds
```

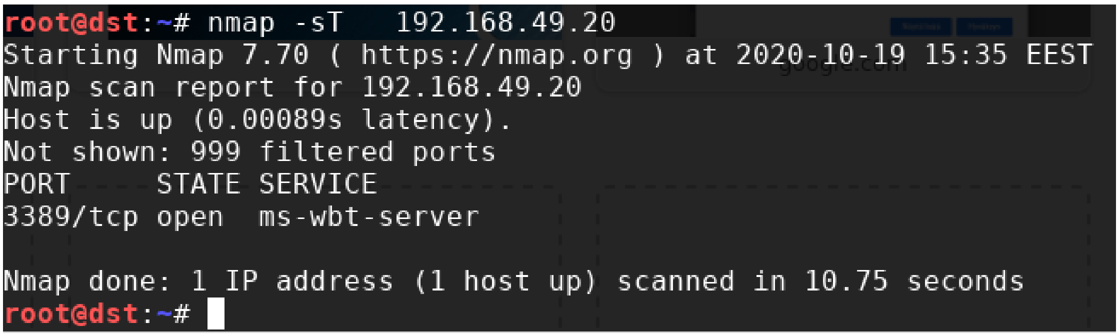
2.2 Run TCP and UDP scans against target(s)

UDP Scan:



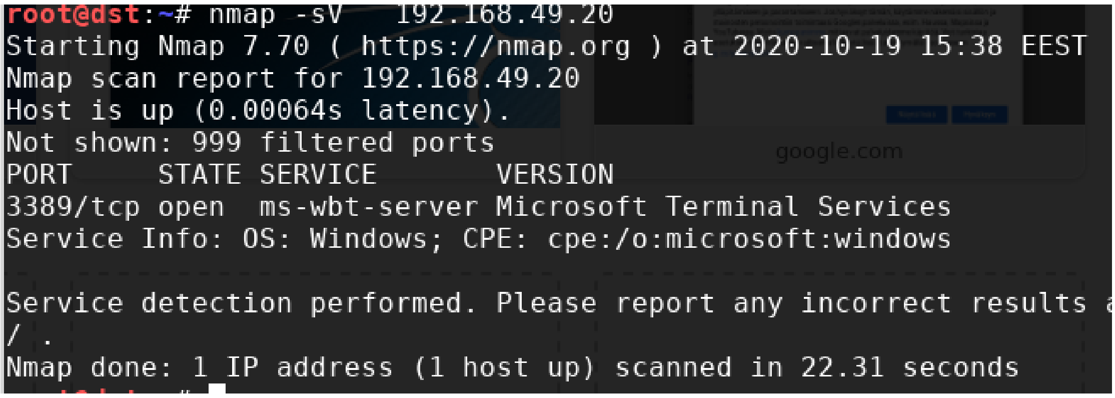
```
root@dst:~# nmap -sU   192.168.49.20
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-19 15:31 EEST
Nmap scan report for 192.168.49.20
Host is up (0.00059s latency).
All 1000 scanned ports on 192.168.49.20 are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 27.69 seconds
root@dst:~# 
```

TCP Scan:



```
root@dst:~# nmap -sT   192.168.49.20
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-19 15:35 EEST
Nmap scan report for 192.168.49.20
Host is up (0.00089s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 10.75 seconds
root@dst:~# 
```

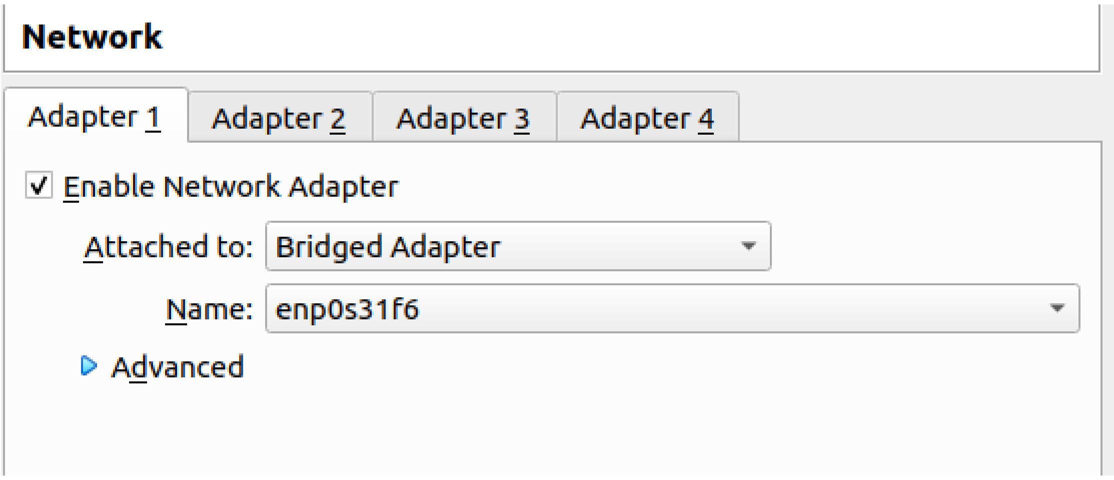
2.3 Run Service detection scan against target(s)



```
root@dst:~# nmap -sV   192.168.49.20
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-19 15:38 EEST
Nmap scan report for 192.168.49.20
Host is up (0.00064s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE       VERSION
3389/tcp open  ms-wbt-server Microsoft Terminal Services
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results a
/ .
Nmap done: 1 IP address (1 host up) scanned in 22.31 seconds
```

3 Use NMAP to validate Firewall rules

3.1 Connect one interface to WAN and another to LAN

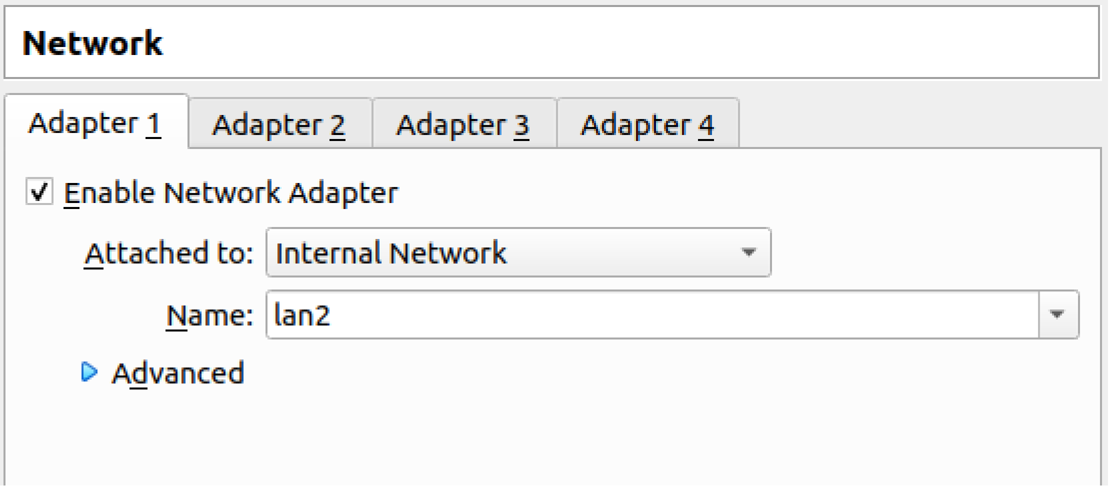


Network

☑ Enable Network Adapter

Attached to: Bridged Adapter

Name: enp0s31f6



Network

☑ Enable Network Adapter

Attached to: Internal Network

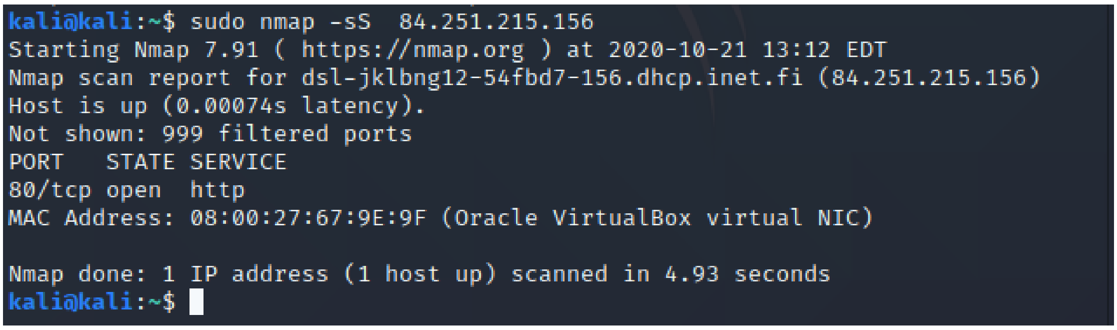
Name: lan2

I used 2 kali virtual machines for this exercise.

3.2 Start wireshark on LAN interface

I started Wireshark on lan2 interface.

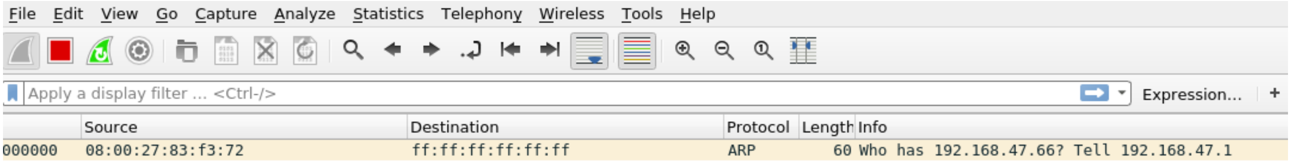
3.3 Generate full scan from WAN to firewall interface



```
kali@kali:~$ sudo nmap -sS  84.251.215.156
Starting Nmap 7.91 ( https://nmap.org ) at 2020-10-21 13:12 EDT
Nmap scan report for dsl-jklbng12-54fbd7-156.dhcp.inet.fi (84.251.215.156)
Host is up (0.00074s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 08:00:27:67:9E:9F (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 4.93 seconds
kali@kali:~$ 
```

I used scans -sL, -sn, -sT, -sS, -sU but only in -sS scan I saw the trophic in Wireshark.

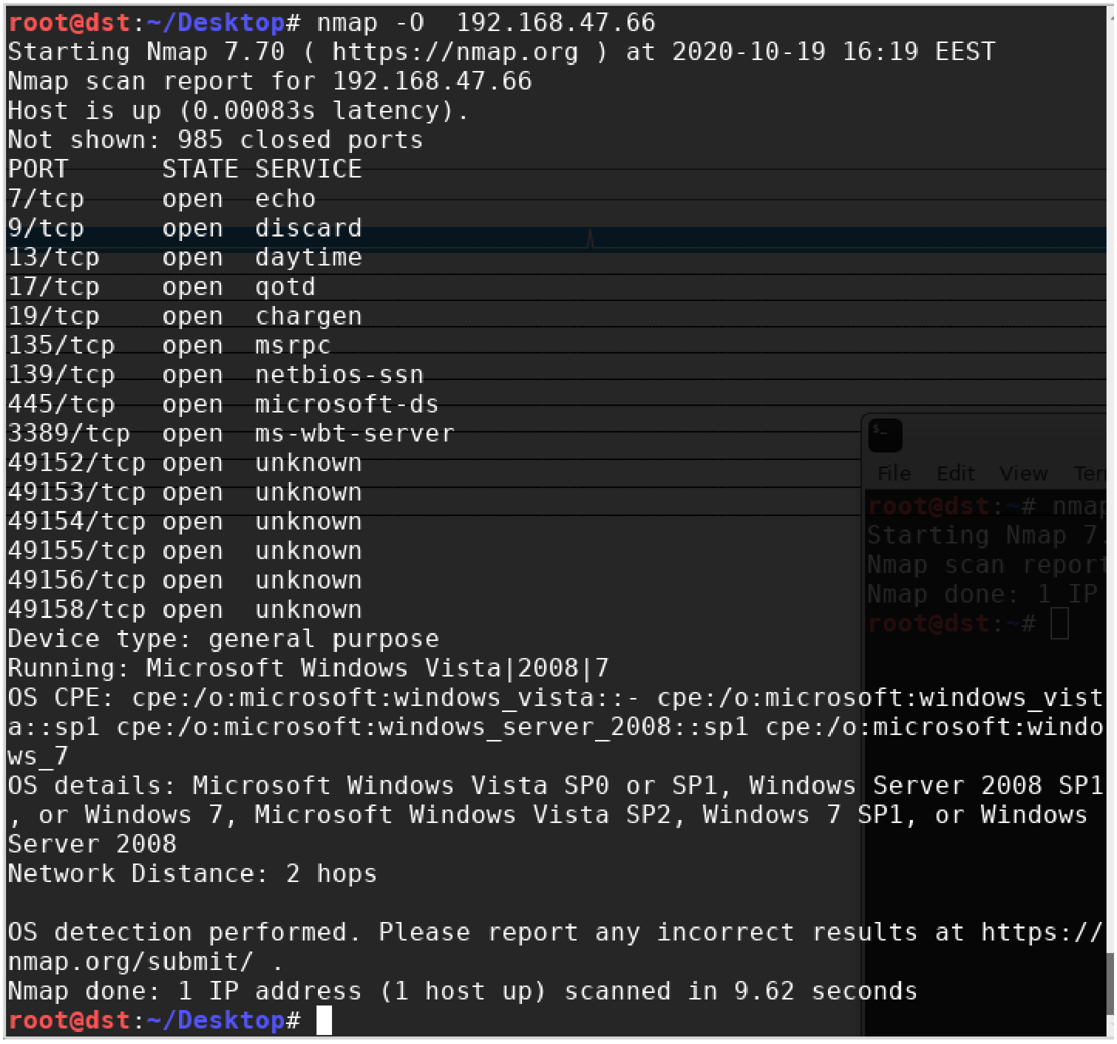
3.4 Look from the Wireshark if you see any traffic from your KALI machine WANnetwork ip-address



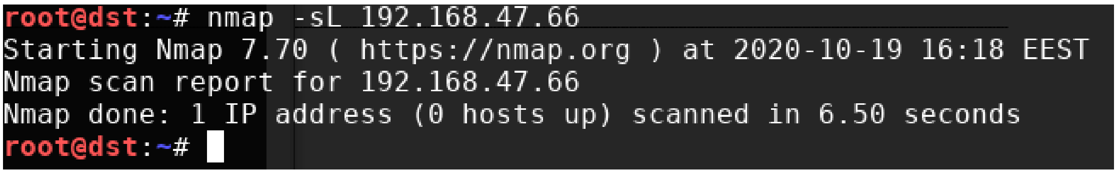
	Source	Destination	Protocol	Length	Info
000000	08:00:27:83:f3:72	ff:ff:ff:ff:ff:ff	ARP	60	Who has 192.168.47.66? Tell 192.168.47.1

4 More scans!

4.1 (Windows)

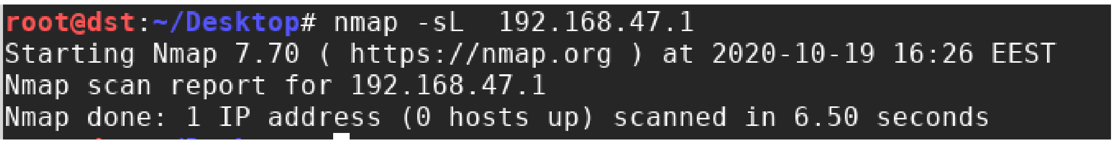


```
root@dst:~/Desktop# nmap -O  192.168.47.66
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-19 16:19 EEST
Nmap scan report for 192.168.47.66
Host is up (0.00083s latency).
Not shown: 985 closed ports
PORT      STATE SERVICE
7/tcp     open  echo
9/tcp     open  discard
13/tcp    open  daytime
17/tcp    open  qotd
19/tcp    open  chargen
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49158/tcp open  unknown
Device type: general purpose
Running: Microsoft Windows Vista|2008|7
OS CPE: cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vist
a::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windo
ws_7
OS details: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1
, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows
Server 2008
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://
nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.62 seconds
root@dst:~/Desktop#
```

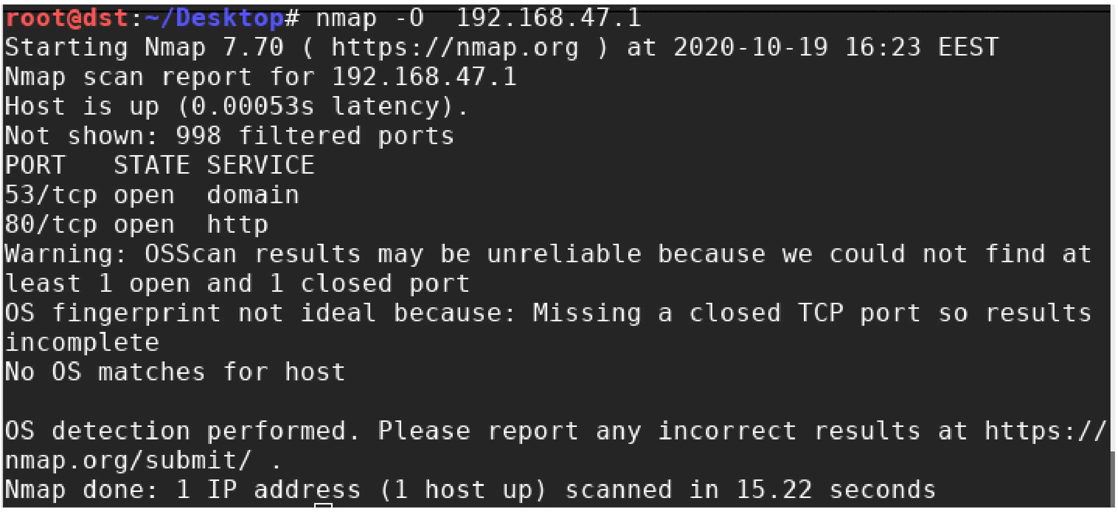


```
root@dst:~# nmap -sL 192.168.47.66
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-19 16:18 EEST
Nmap scan report for 192.168.47.66
Nmap done: 1 IP address (0 hosts up) scanned in 6.50 seconds
root@dst:~#
```

4.2 Firewall:



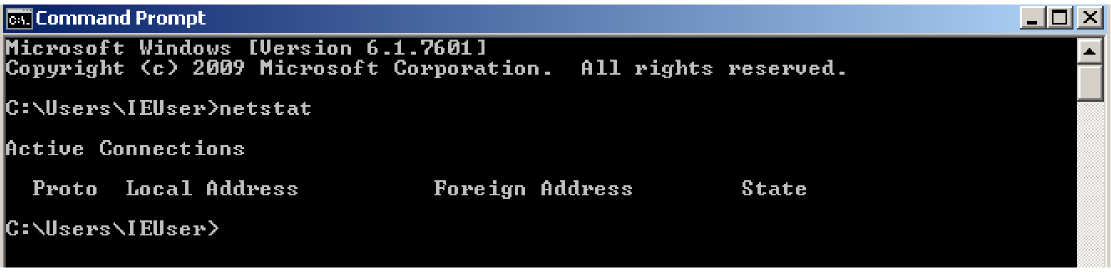
```
root@dst:~/Desktop# nmap -sL  192.168.47.1
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-19 16:26 EEST
Nmap scan report for 192.168.47.1
Nmap done: 1 IP address (0 hosts up) scanned in 6.50 seconds
```



```
root@dst:~/Desktop# nmap -O  192.168.47.1
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-19 16:23 EEST
Nmap scan report for 192.168.47.1
Host is up (0.00053s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http
Warning: OSScan results may be unreliable because we could not find at
least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results
incomplete
No OS matches for host

OS detection performed. Please report any incorrect results at https://
nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.22 seconds
```

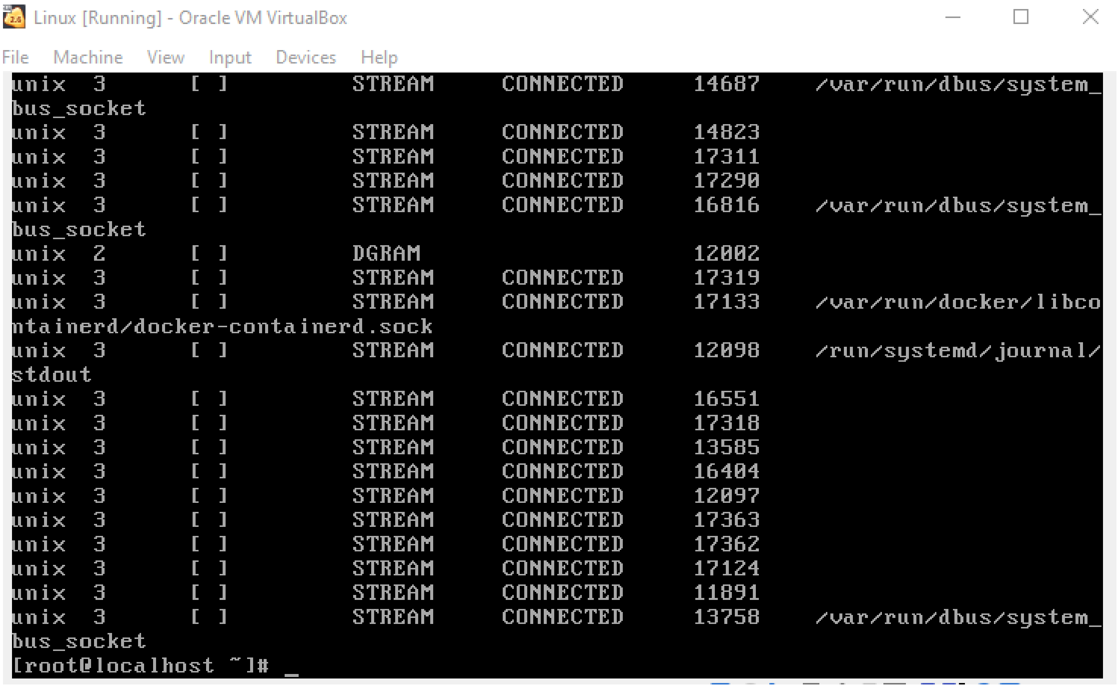
5 NETSTAT

5.1 Windows:



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\IEUser>netstat

Active Connections

  Proto  Local Address          Foreign Address        State

C:\Users\IEUser>
```

5.2 Linux:



```
unix  3      [ ]         STREAM     CONNECTED     14687    /var/run/dbus/system_
bus_socket
unix  3      [ ]         STREAM     CONNECTED     14823
unix  3      [ ]         STREAM     CONNECTED     17311
unix  3      [ ]         STREAM     CONNECTED     17290
unix  3      [ ]         STREAM     CONNECTED     16816    /var/run/dbus/system_
bus_socket
unix  2      [ ]         DGRAM                    12002
unix  3      [ ]         STREAM     CONNECTED     17319
unix  3      [ ]         STREAM     CONNECTED     17133    /var/run/docker/libco
ntainerd/docker-containerd.sock
unix  3      [ ]         STREAM     CONNECTED     12098    /run/systemd/journal/
stdout
unix  3      [ ]         STREAM     CONNECTED     16551
unix  3      [ ]         STREAM     CONNECTED     17318
unix  3      [ ]         STREAM     CONNECTED     13585
unix  3      [ ]         STREAM     CONNECTED     16404
unix  3      [ ]         STREAM     CONNECTED     12097
unix  3      [ ]         STREAM     CONNECTED     17363
unix  3      [ ]         STREAM     CONNECTED     17362
unix  3      [ ]         STREAM     CONNECTED     17124
unix  3      [ ]         STREAM     CONNECTED     11891
unix  3      [ ]         STREAM     CONNECTED     13758    /var/run/dbus/system_
bus_socket
[root@localhost ~]# _
```

Linux showed a lot of active connections but windows didn’t show anything.

6 Conclusion

6.1 Do you feel you understood methods to do External and Internal SCANS?

I think I understand methods and idea of External and Internal Scans.

6.2 How much time did you spend? Was it enough to get reliable results?

I spend a lot of time doing this exercises, the most demanding one was set up virtual machine correctly (for example wan network doens’t work with wifi on my computer). I had also problems with seting kali to lan and wan network I manage to do this with 2 kali linux virtual machines.

I didn’t know what complite scan means in the exercise 3.3.

SU and SV scnas returns the same result as the rest of the scans.

I don’t know if results in exercise 1.6 and 1.7 are as they should be, but I was doing scan on my linux, windows and computers in dynamo campus laboratory and everyware I’ve got the same results.