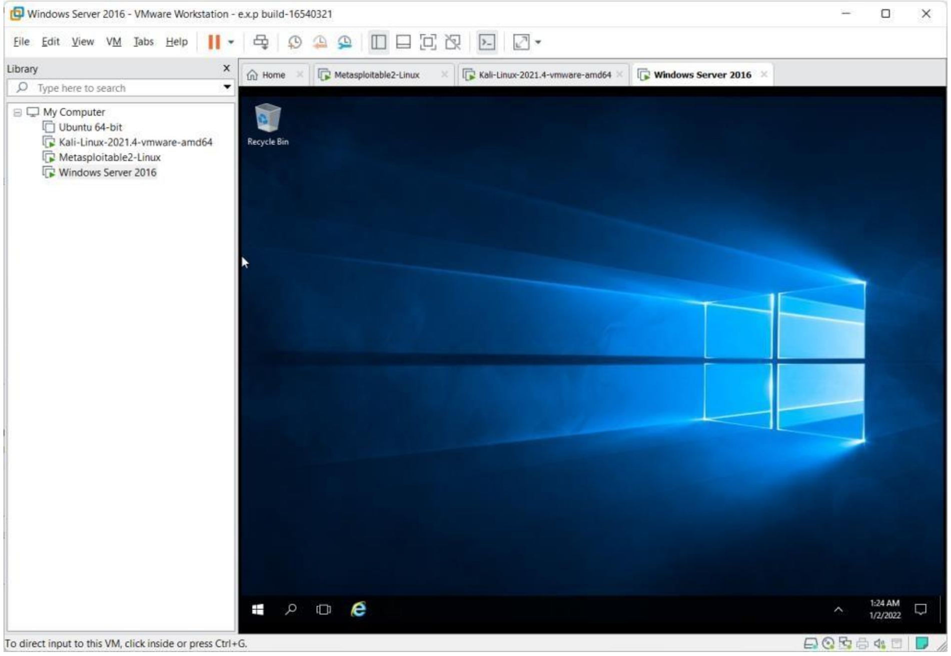
Lab 4 Report- Discovering the Network, Scan and Reconnaissance

Name : Hamza Abdellah Ahmed

ID:18P7231

Installing Required VMs

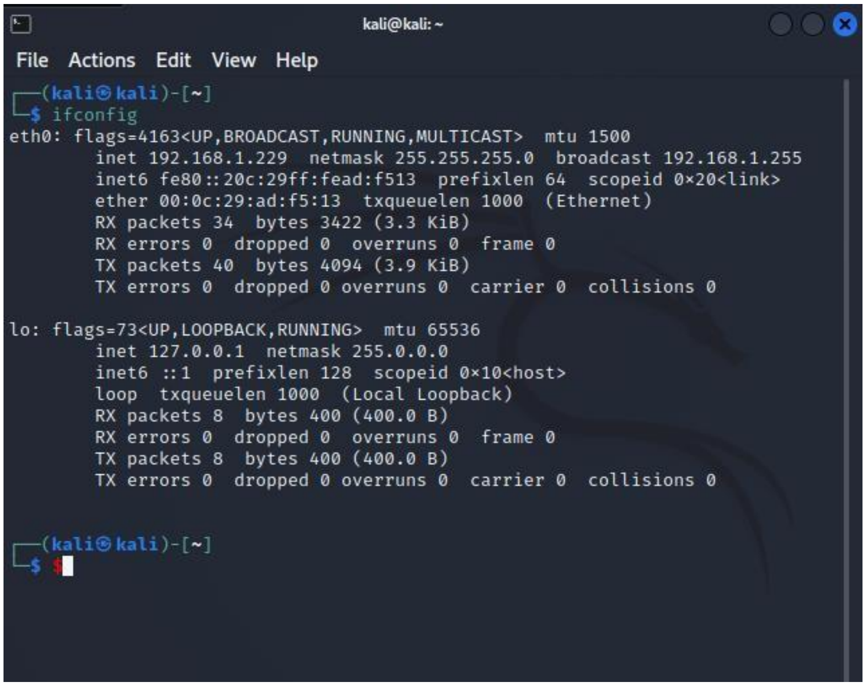
Shown are the VMs installed:



To direct input to this VM, click inside or press Ctrl+G.

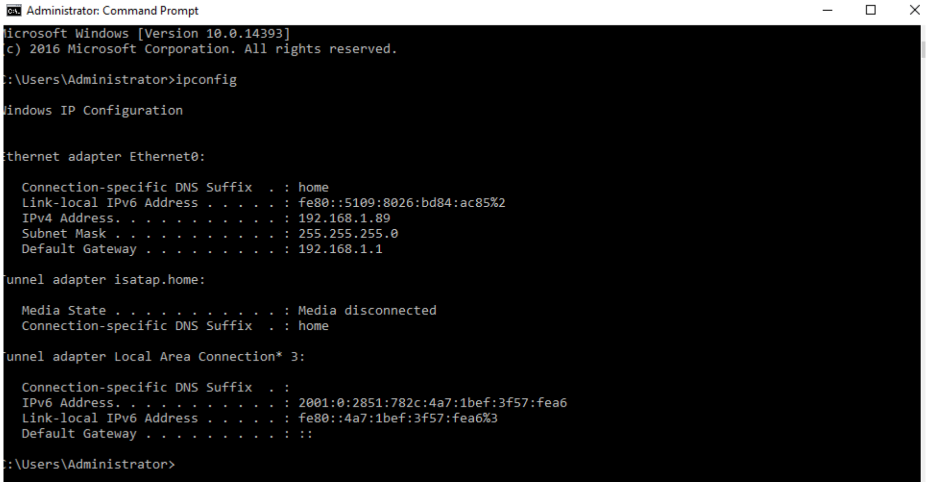
VMs IPs Table

Kali Linux:



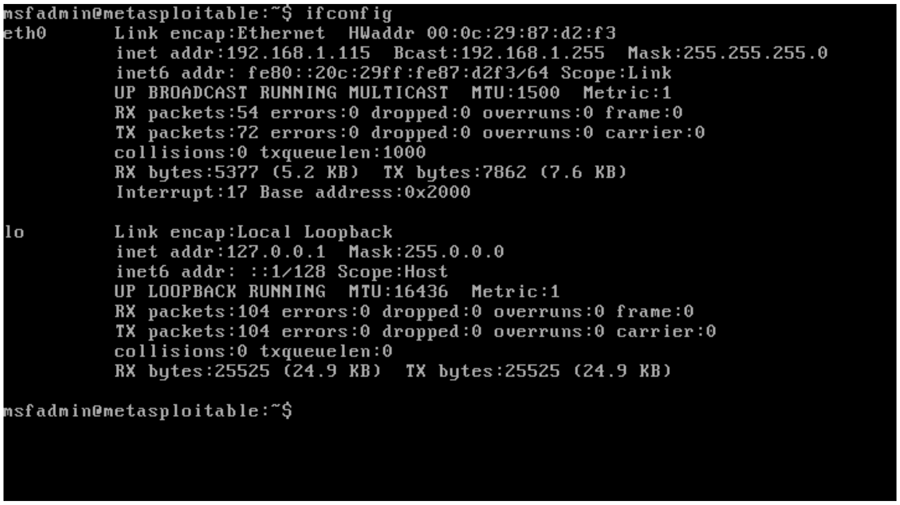
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.229  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::20c:29ff:fead:f513  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:ad:f5:13  txqueuelen 1000  (Ethernet)
        RX packets 34  bytes 3422 (3.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 40  bytes 4094 (3.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 400 (400.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 400 (400.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ $
```

Windows Server:



```
icrosoft Windows [Version 10.0.14393]
c) 2016 Microsoft Corporation. All rights reserved.

:\Users\Administrator>ipconfig

indows IP Configuration


thernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : home
   Link-local IPv6 Address . . . . . : fe80::5109:8026:bd84:ac85%2
   IPv4 Address. . . . . . . . . . . : 192.168.1.89
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

unnel adapter isatap.home:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : home

unnel adapter Local Area Connection* 3:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:0:2851:782c:4a7:1bef:3f57:fea6
   Link-local IPv6 Address . . . . . : fe80::4a7:1bef:3f57:fea6%3
   Default Gateway . . . . . . . . . : ::

:\Users\Administrator>
```

Metasploitable:

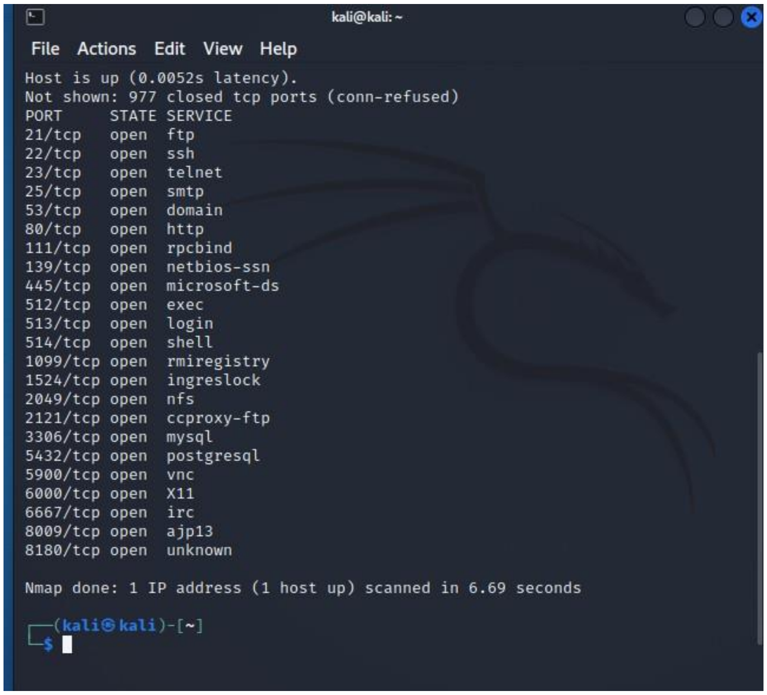


```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:87:d2:f3
          inet addr:192.168.1.115  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe87:d2f3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:54 errors:0 dropped:0 overruns:0 frame:0
          TX packets:72 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5377 (5.2 KB)  TX bytes:7862 (7.6 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:104 errors:0 dropped:0 overruns:0 frame:0
          TX packets:104 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:25525 (24.9 KB)  TX bytes:25525 (24.9 KB)

msfadmin@metasploitable:~$
```

Kali Linux	**192.168.1.229**
Windows Server	**192.168.1.89**
Metasploitable	**192.168.1.115**

Scanning the Target Using nmap

Command: nmap –T4 192.168.1.115



```
Host is up (0.0052s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 6.69 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

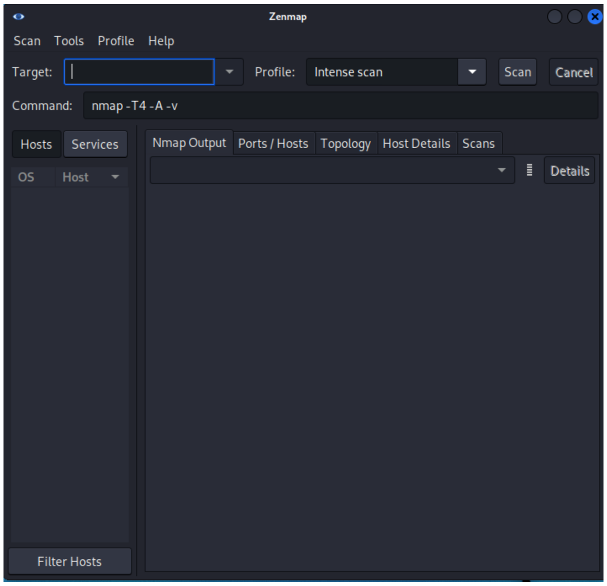
Zenmap

Commands to install (It wasn't installed by default for me):

sudo apt install nix-bin

sudo nix run -f channel:nixos-unstable nmap_graphical

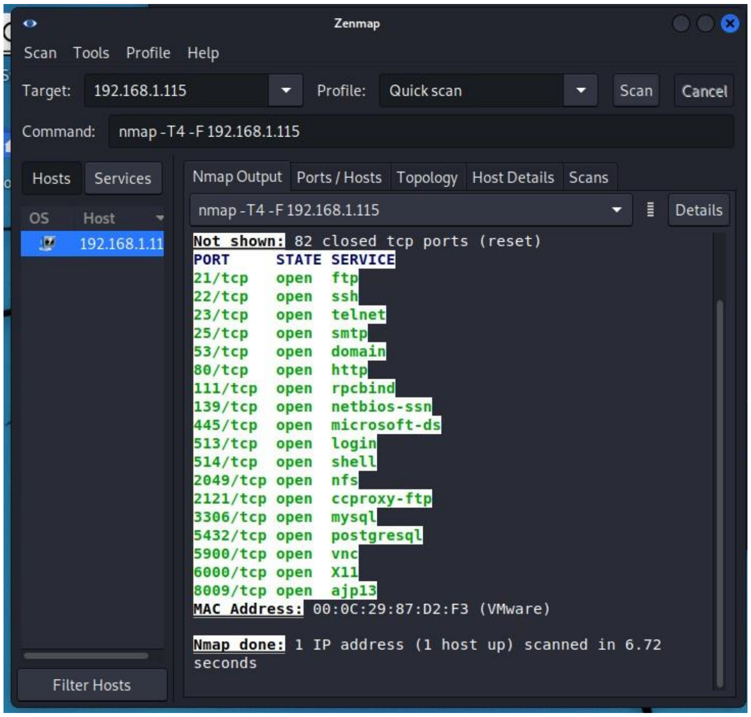
zenmap



Profile: Intense scan

Command: nmap -T4 -A -v

Results from Zenmap:



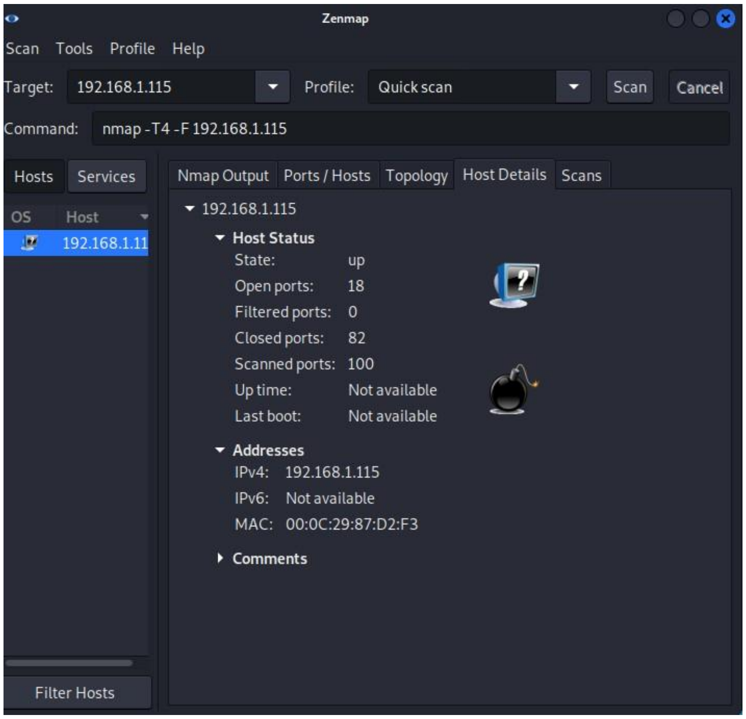
Target: 192.168.1.115

Profile: Quick scan

Command: nmap -T4 -F 192.168.1.115

nmap -T4 -F 192.168.1.115

```
Not shown: 82 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
513/tcp  open  login
514/tcp  open  shell
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
8009/tcp open  ajp13
MAC Address: 00:0C:29:87:D2:F3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 6.72
seconds
```



Target: 192.168.1.115

Profile: Quick scan

Command: nmap -T4 -F 192.168.1.115

192.168.1.115

Host Status

State: up

Open ports: 18

Filtered ports: 0

Closed ports: 82

Scanned ports: 100

Up time: Not available

Last boot: Not available

Addresses

IPv4: 192.168.1.115

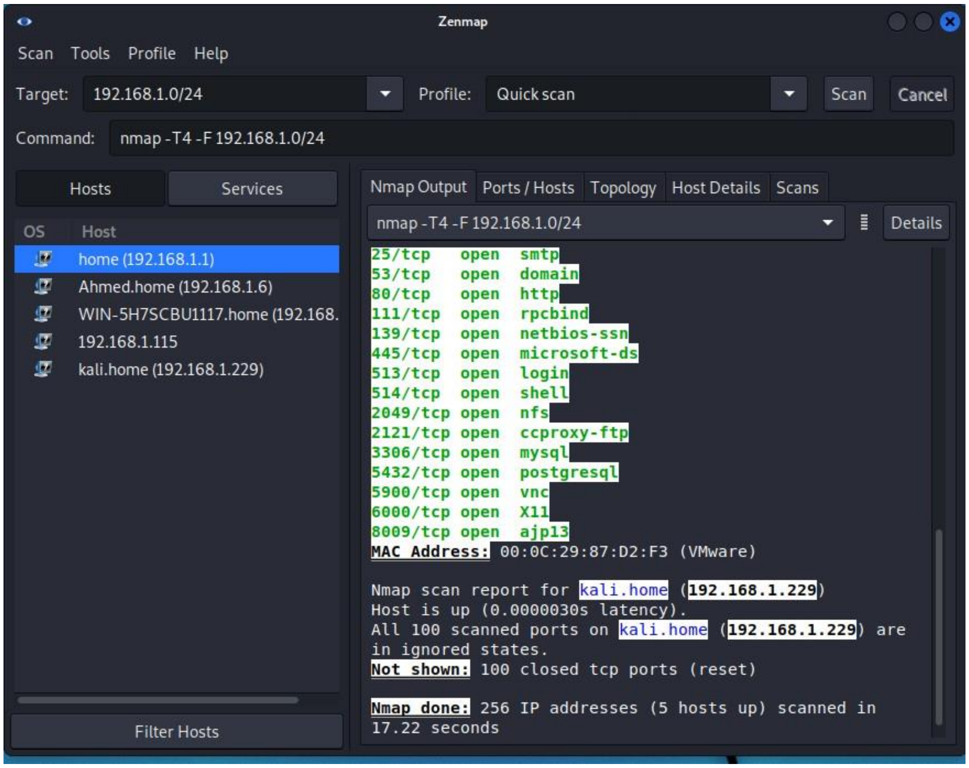
IPv6: Not available

MAC: 00:0C:29:87:D2:F3

Comments

Scanning the network for computers and host

Using slash notation for 192.168.1.0/24 as this is my subnet mask for my VMs



Target: 192.168.1.0/24

Profile: Quick scan

Command: nmap -T4 -F 192.168.1.0/24

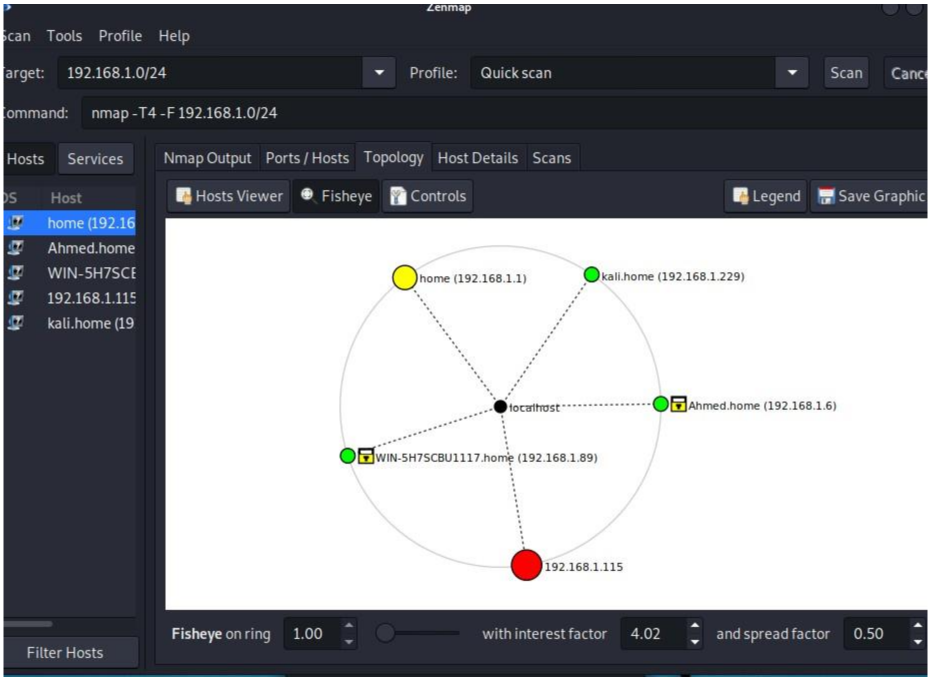
home (192.168.1.1)
Ahmed.home (192.168.1.6)
WIN-5H7SCBU1117.home (192.168.
192.168.1.115
kali.home (192.168.1.229)

```
nmap -T4 -F 192.168.1.0/24
```

```
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
513/tcp  open  login
514/tcp  open  shell
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
8009/tcp open  ajp13
MAC Address: 00:0C:29:87:D2:F3 (VMware)

Nmap scan report for kali.home (192.168.1.229)
Host is up (0.0000030s latency).
All 100 scanned ports on kali.home (192.168.1.229) are
in ignored states.
Not shown: 100 closed tcp ports (reset)

Nmap done: 256 IP addresses (5 hosts up) scanned in
17.22 seconds
```

The last IP in the lab report (x.x.x.254) is not present in my scan. My last address is just my Kali's IP.

Topology:



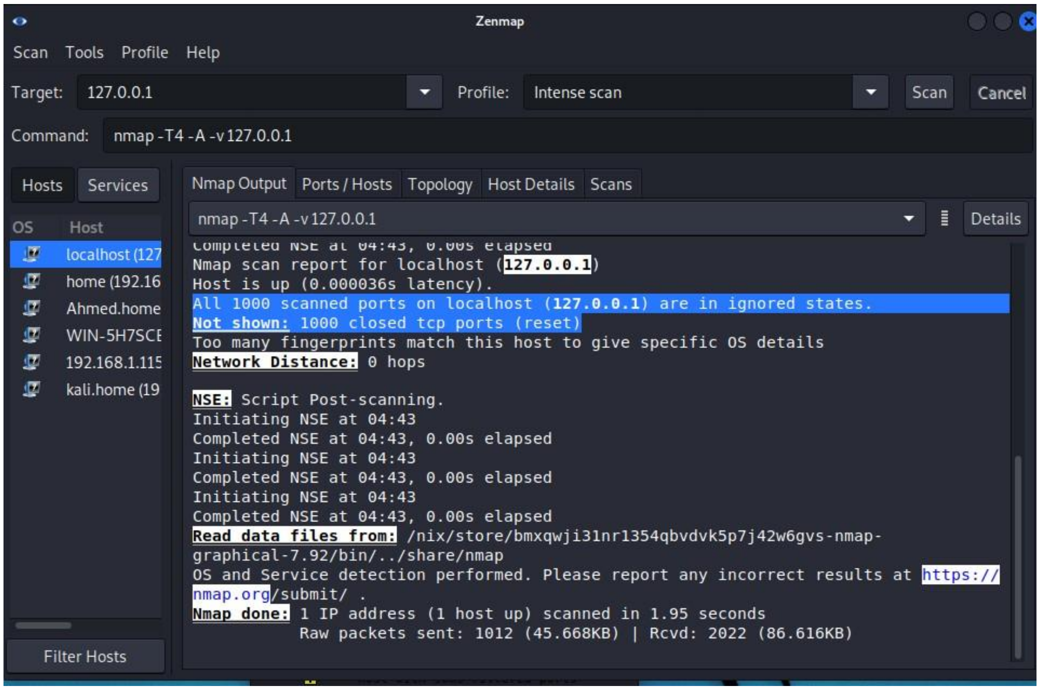
Target: 192.168.1.0/24

Profile: Quick scan

Command: nmap -T4 -F 192.168.1.0/24

Fisheye on ring 1.00 with interest factor 4.02 and spread factor 0.50

Intense scan of Kali machine



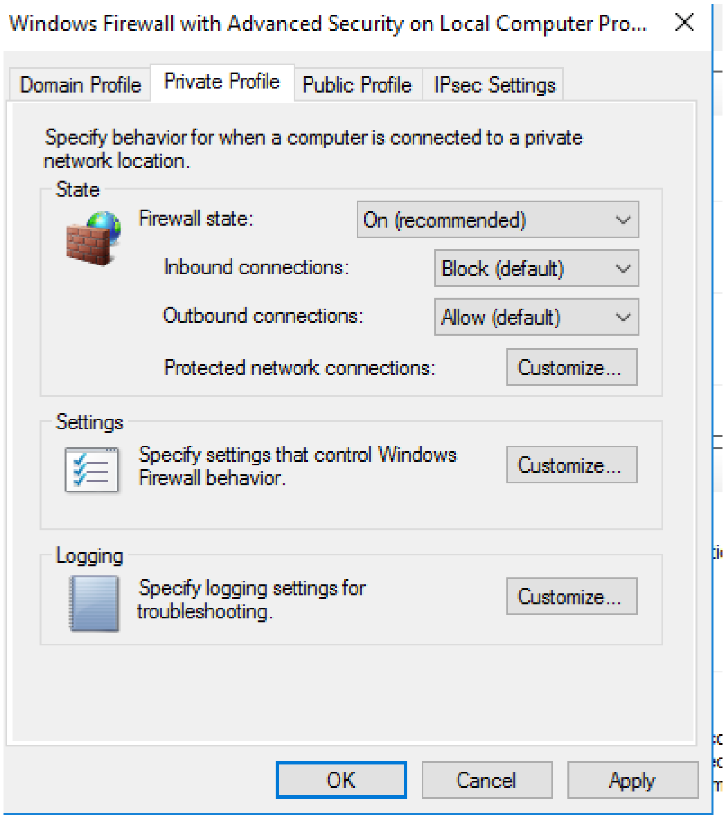
Target: 127.0.0.1

Profile: Intense scan

Command: nmap -T4 -A -v 127.0.0.1

```
Completed NSE at 04:43, 0.00s elapsed
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000036s latency).
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

NSE: Script Post-scanning.
Initiating NSE at 04:43
Completed NSE at 04:43, 0.00s elapsed
Initiating NSE at 04:43
Completed NSE at 04:43, 0.00s elapsed
Initiating NSE at 04:43
Completed NSE at 04:43, 0.00s elapsed
Read data files from: /nix/store/bmxqwji31nr1354qbvdvk5p7j42w6gvs-nmap-
graphical-7.92/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://
nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.95 seconds
           Raw packets sent: 1012 (45.668KB) | Rcvd: 2022 (86.616KB)
```

Intense scan of Windows server (Firewall on)



Specify behavior for when a computer is connected to a private network location.

State

Firewall state: On (recommended)

Inbound connections: Block (default)

Outbound connections: Allow (default)

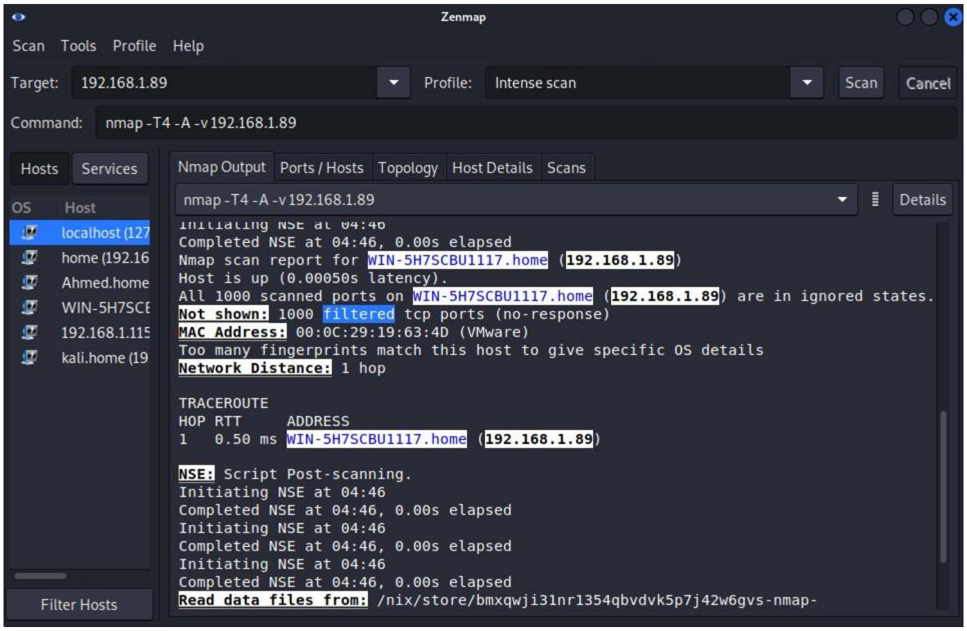
Protected network connections:

Settings

Specify settings that control Windows Firewall behavior.

Logging

Specify logging settings for troubleshooting.



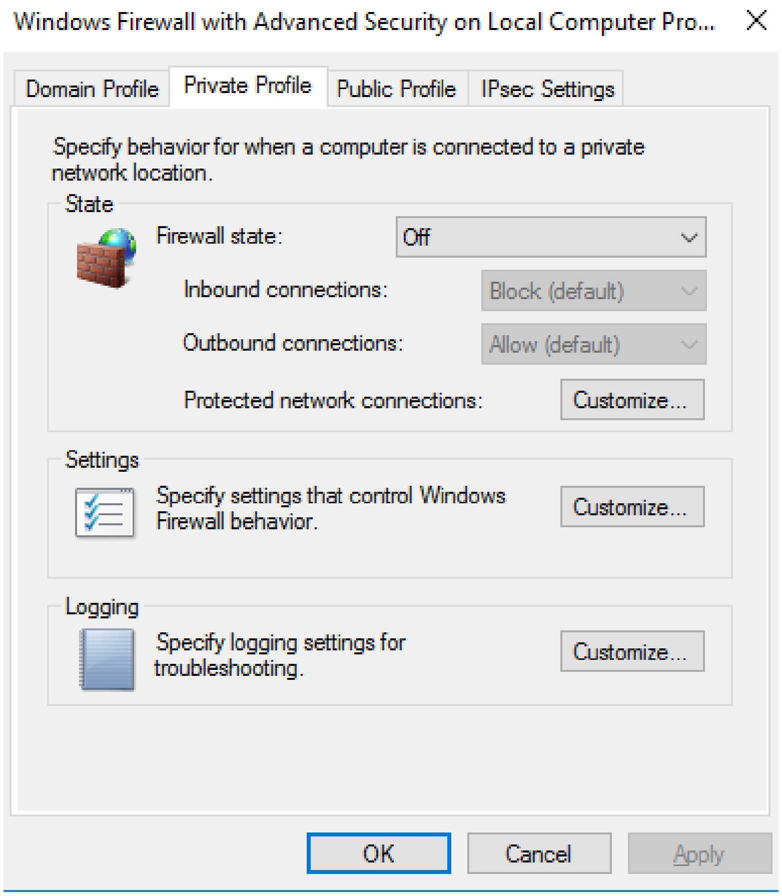
Target: 192.168.1.89

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.1.89

```
nmap -T4 -A -v 192.168.1.89
Initiating NSE at 04:46
Completed NSE at 04:46, 0.00s elapsed
Nmap scan report for WIN-5H7SCBU1117.home (192.168.1.89)
Host is up (0.00050s latency).
All 1000 scanned ports on WIN-5H7SCBU1117.home (192.168.1.89) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:0C:29:19:63:4D (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.50 ms WIN-5H7SCBU1117.home (192.168.1.89)

NSE: Script Post-scanning.
Initiating NSE at 04:46
Completed NSE at 04:46, 0.00s elapsed
Initiating NSE at 04:46
Completed NSE at 04:46, 0.00s elapsed
Initiating NSE at 04:46
Completed NSE at 04:46, 0.00s elapsed
Read data files from: /nix/store/bmxqwji31nr1354qbvdvk5p7j42w6gvs-nmap-
```

Intense scan of Windows server (Firewall off)



Specify behavior for when a computer is connected to a private network location.

State

Firewall state: Off

Inbound connections: Block (default)

Outbound connections: Allow (default)

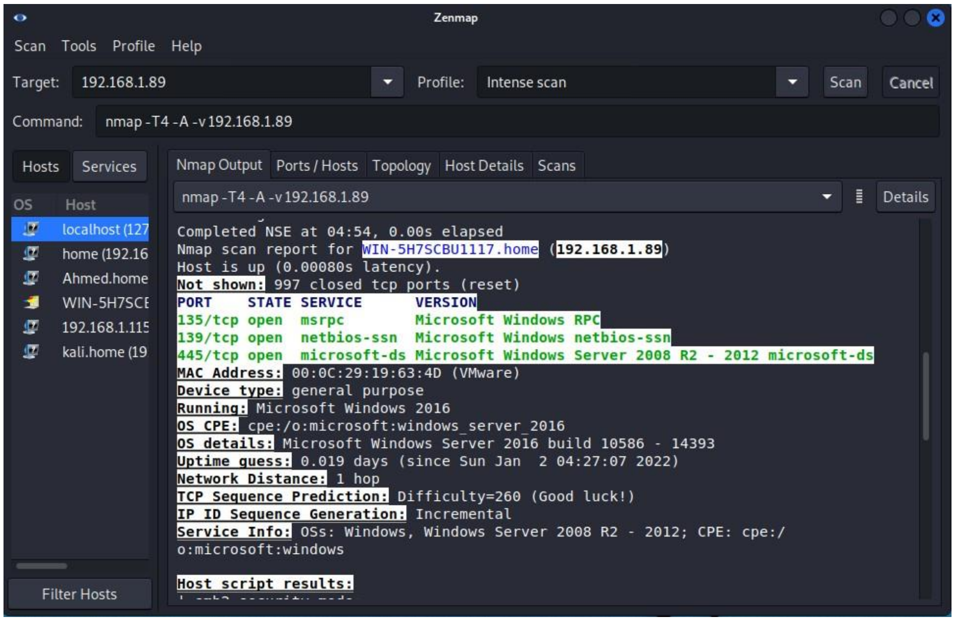
Protected network connections:

Settings

Specify settings that control Windows Firewall behavior.

Logging

Specify logging settings for troubleshooting.



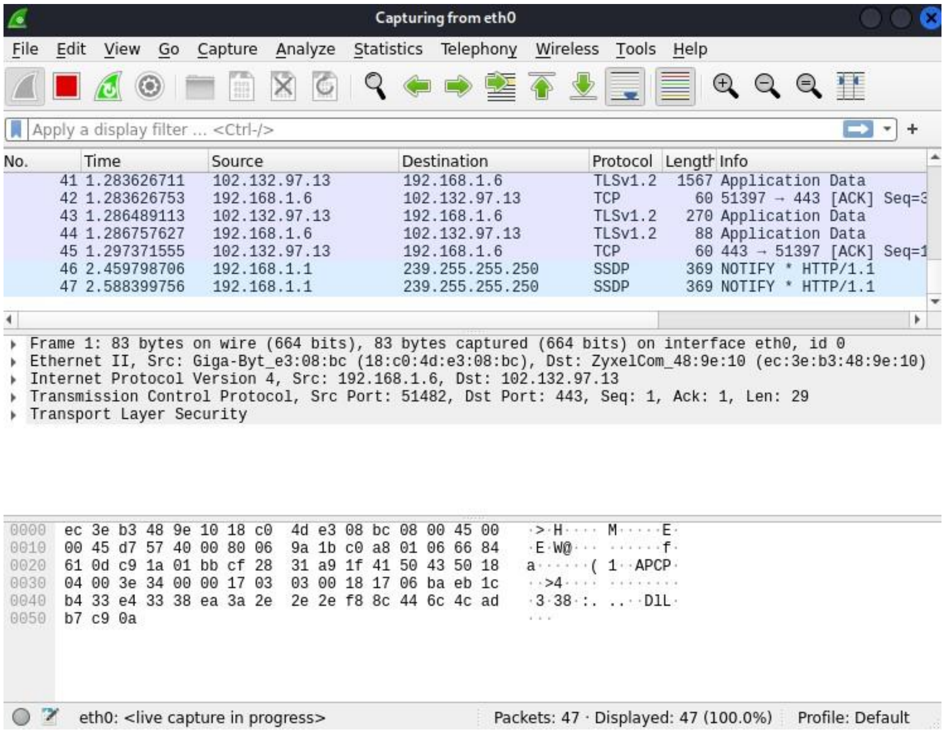
Target: 192.168.1.89 Profile: Intense scan

Command: nmap -T4 -A -v 192.168.1.89

```
Completed NSE at 04:54, 0.00s elapsed
Nmap scan report for WIN-5H7SCBU1117.home (192.168.1.89)
Host is up (0.00080s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
MAC Address: 00:0C:29:19:63:4D (VMware)
Device type: general purpose
Running: Microsoft Windows 2016
OS CPE: cpe:/o:microsoft:windows_server_2016
OS details: Microsoft Windows Server 2016 build 10586 - 14393
Uptime guess: 0.019 days (since Sun Jan  2 04:27:07 2022)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/
o:microsoft:windows

Host script results:
```

Analyzing Port Scan

Starting Wireshark and start to capture packets:


Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

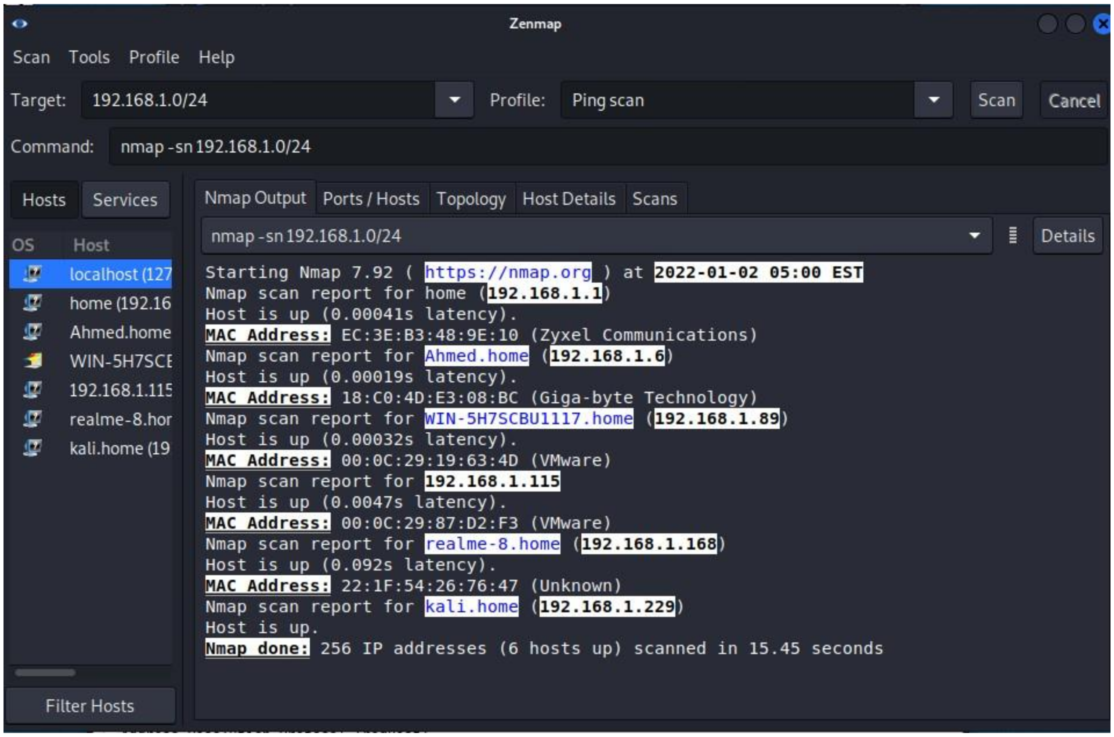
```
No.   Time         Source          Destination      Protocol Length Info
   41 1.283626711 102.132.97.13   192.168.1.6      TLSv1.2  1567 Application Data
   42 1.283626753 192.168.1.6     102.132.97.13    TCP        60 51397 → 443 [ACK] Seq=3
   43 1.286489113 102.132.97.13   192.168.1.6      TLSv1.2   270 Application Data
   44 1.286757627 192.168.1.6     102.132.97.13    TLSv1.2    88 Application Data
   45 1.297371555 102.132.97.13   192.168.1.6      TCP        60 443 → 51397 [ACK] Seq=1
   46 2.459798706 192.168.1.1     239.255.255.250  SSDP      369 NOTIFY * HTTP/1.1
   47 2.588399756 192.168.1.1     239.255.255.250  SSDP      369 NOTIFY * HTTP/1.1
```

```
▸ Frame 1: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface eth0, id 0
▸ Ethernet II, Src: Giga-Byt_e3:08:bc (18:c0:4d:e3:08:bc), Dst: ZyxelCom_48:9e:10 (ec:3e:b3:48:9e:10)
▸ Internet Protocol Version 4, Src: 192.168.1.6, Dst: 102.132.97.13
▸ Transmission Control Protocol, Src Port: 51482, Dst Port: 443, Seq: 1, Ack: 1, Len: 29
▸ Transport Layer Security
```

```
0000  ec 3e b3 48 9e 10 18 c0  4d e3 08 bc 08 00 45 00   ·>·H····M·····E·
0010  00 45 d7 57 40 00 80 06  9a 1b c0 a8 01 06 66 84   ·E·W@·········f·
0020  61 0d c9 1a 01 bb cf 28  31 a9 1f 41 50 43 50 18   a······(1··APCP·
0030  04 00 3e 34 00 00 17 03  03 00 18 17 06 ba eb 1c   ··>4············
0040  b4 33 e4 33 38 ea 3a 2e  2e 2e f8 8c 44 6c 4c ad   ·3·38·:.....DlL·
0050  b7 c9 0a                                           ···
```

eth0: <live capture in progress> Packets: 47 · Displayed: 47 (100.0%) Profile: Default

Then go to zenmap and ping all devices



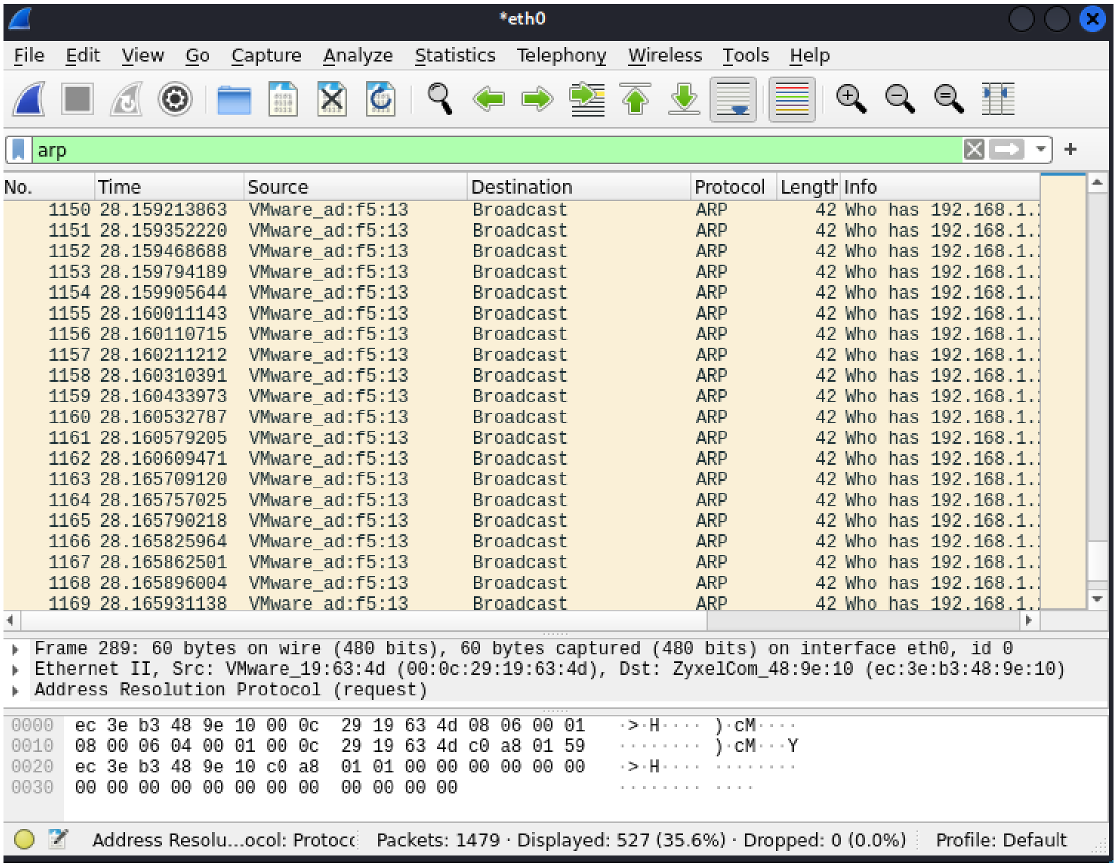
Target: 192.168.1.0/24

Profile: Ping scan

Command: nmap -sn 192.168.1.0/24

```
localhost (127
home (192.16
Ahmed.home
WIN-5H7SCE
192.168.1.115
realme-8.hor
kali.home (19
```

```
nmap -sn 192.168.1.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-02 05:00 EST
Nmap scan report for home (192.168.1.1)
Host is up (0.00041s latency).
MAC Address: EC:3E:B3:48:9E:10 (Zyxel Communications)
Nmap scan report for Ahmed.home (192.168.1.6)
Host is up (0.00019s latency).
MAC Address: 18:C0:4D:E3:08:BC (Giga-byte Technology)
Nmap scan report for WIN-5H7SCBU1117.home (192.168.1.89)
Host is up (0.00032s latency).
MAC Address: 00:0C:29:19:63:4D (VMware)
Nmap scan report for 192.168.1.115
Host is up (0.0047s latency).
MAC Address: 00:0C:29:87:D2:F3 (VMware)
Nmap scan report for realme-8.home (192.168.1.168)
Host is up (0.092s latency).
MAC Address: 22:1F:54:26:76:47 (Unknown)
Nmap scan report for kali.home (192.168.1.229)
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 15.45 seconds
```



arp

```
No.   Time         Source          Destination  Protocol  Length Info
 1150 28.159213863 VMware_ad:f5:13 Broadcast    ARP       42 Who has 192.168.1.:
 1151 28.159352220 VMware_ad:f5:13 Broadcast    ARP       42 Who has 192.168.1.:
 1152 28.159468688 VMware_ad:f5:13 Broadcast    ARP       42 Who has 192.168.1.:
 1153 28.159794189 VMware_ad:f5:13 Broadcast    ARP       42 Who has 192.168.1.:
 1154 28.159905644 VMware_ad:f5:13 Broadcast    ARP       42 Who has 192.168.1.:
 1155 28.160011143 VMware_ad:f5:13 Broadcast    ARP       42 Who has 192.168.1.:
 1156 28.160110715 VMware_ad:f5:13 Broadcast    ARP       42 Who has 192.168.1.:
 1157 28.160211212 VMware_ad:f5:13 Broadcast    ARP       42 Who has 192.168.1.:
 1158 28.160310391 VMware_ad:f5:13 Broadcast    ARP       42 Who has 192.168.1.:
 1159 28.160433973 VMware_ad:f5:13 Broadcast    ARP       42 Who has 192.168.1.:
 1160 28.160532787 VMware_ad:f5:13 Broadcast    ARP       42 Who has 192.168.1.:
 1161 28.160579205 VMware_ad:f5:13 Broadcast    ARP       42 Who has 192.168.1.:
 1162 28.160609471 VMware_ad:f5:13 Broadcast    ARP       42 Who has 192.168.1.:
 1163 28.165709120 VMware_ad:f5:13 Broadcast    ARP       42 Who has 192.168.1.:
 1164 28.165757025 VMware_ad:f5:13 Broadcast    ARP       42 Who has 192.168.1.:
 1165 28.165790218 VMware_ad:f5:13 Broadcast    ARP       42 Who has 192.168.1.:
 1166 28.165825964 VMware_ad:f5:13 Broadcast    ARP       42 Who has 192.168.1.:
 1167 28.165862501 VMware_ad:f5:13 Broadcast    ARP       42 Who has 192.168.1.:
 1168 28.165896004 VMware_ad:f5:13 Broadcast    ARP       42 Who has 192.168.1.:
 1169 28.165931138 VMware_ad:f5:13 Broadcast    ARP       42 Who has 192.168.1.:
```

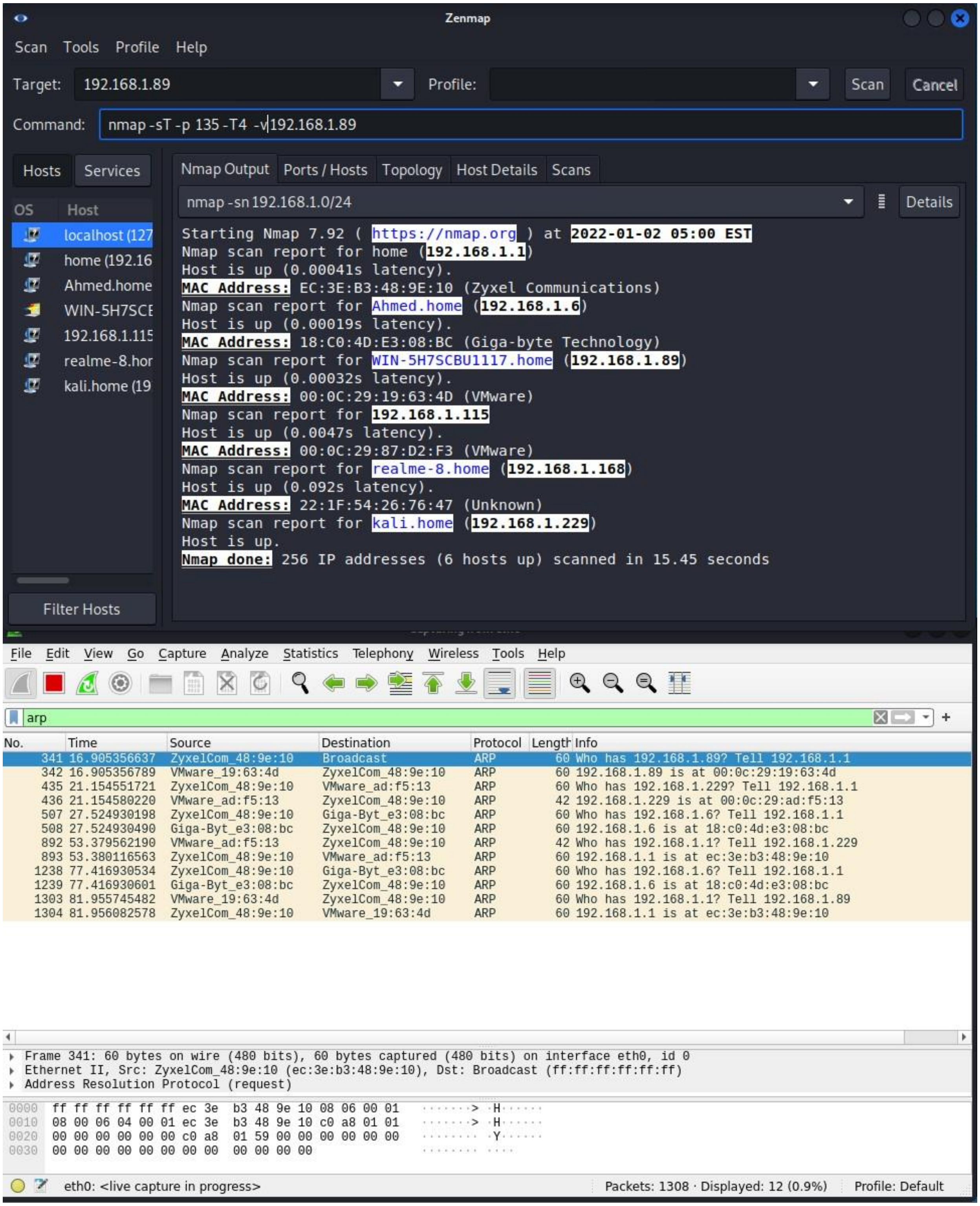
```
▸ Frame 289: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
▸ Ethernet II, Src: VMware_19:63:4d (00:0c:29:19:63:4d), Dst: ZyxelCom_48:9e:10 (ec:3e:b3:48:9e:10)
▸ Address Resolution Protocol (request)
```

```
0000  ec 3e b3 48 9e 10 00 0c  29 19 63 4d 08 06 00 01   ·>·H····  )·cM····
0010  08 00 06 04 00 01 00 0c  29 19 63 4d c0 a8 01 59   ········  )·cM···Y
0020  ec 3e b3 48 9e 10 c0 a8  01 01 00 00 00 00 00 00   ·>·H····  ········
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········  ····
```

Address Resolu...ocol: Protocc   Packets: 1479 · Displayed: 527 (35.6%) · Dropped: 0 (0.0%)   Profile: Default

Targeting a specific machine and port

Settings for Zenmap before scanning



Target: 192.168.1.89

Profile:

Command: nmap -sT -p 135 -T4 -v 192.168.1.89

nmap -sn 192.168.1.0/24

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-02 05:00 EST
Nmap scan report for home (192.168.1.1)
Host is up (0.00041s latency).
MAC Address: EC:3E:B3:48:9E:10 (Zyxel Communications)
Nmap scan report for Ahmed.home (192.168.1.6)
Host is up (0.00019s latency).
MAC Address: 18:C0:4D:E3:08:BC (Giga-byte Technology)
Nmap scan report for WIN-5H7SCBU1117.home (192.168.1.89)
Host is up (0.00032s latency).
MAC Address: 00:0C:29:19:63:4D (VMware)
Nmap scan report for 192.168.1.115
Host is up (0.0047s latency).
MAC Address: 00:0C:29:87:D2:F3 (VMware)
Nmap scan report for realme-8.home (192.168.1.168)
Host is up (0.092s latency).
MAC Address: 22:1F:54:26:76:47 (Unknown)
Nmap scan report for kali.home (192.168.1.229)
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 15.45 seconds
```

arp

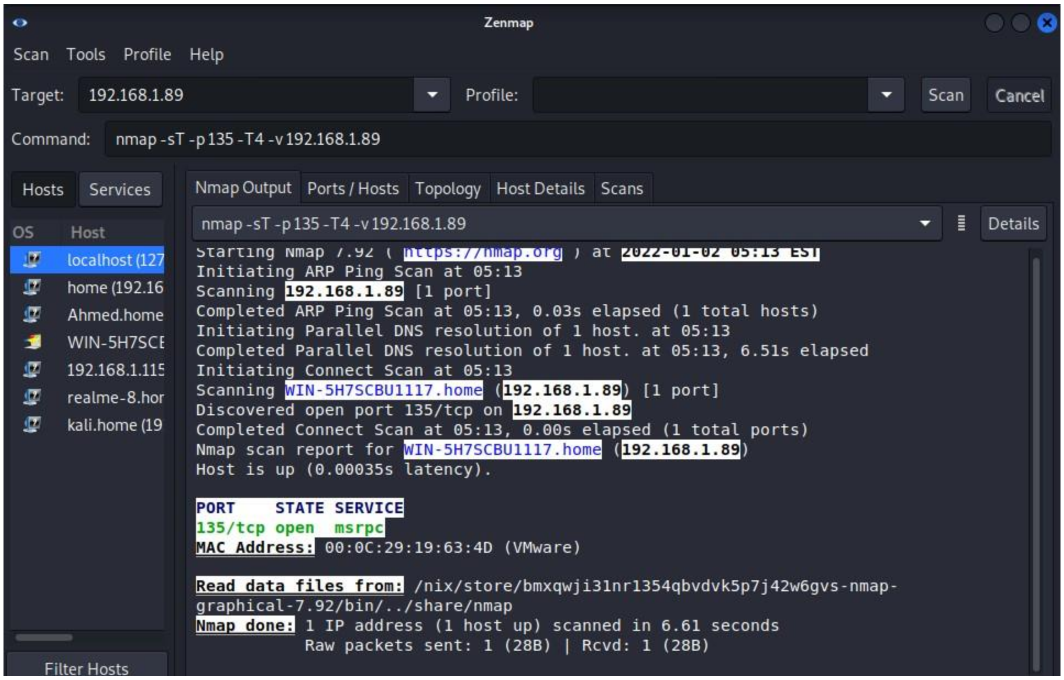
```
No.     Time          Source               Destination          Protocol Length Info
    341 16.905356637  ZyxelCom_48:9e:10    Broadcast            ARP         60 Who has 192.168.1.89? Tell 192.168.1.1
    342 16.905356789  VMware_19:63:4d      ZyxelCom_48:9e:10    ARP         60 192.168.1.89 is at 00:0c:29:19:63:4d
    435 21.154551721  ZyxelCom_48:9e:10    VMware_ad:f5:13      ARP         60 Who has 192.168.1.229? Tell 192.168.1.1
    436 21.154580220  VMware_ad:f5:13      ZyxelCom_48:9e:10    ARP         42 192.168.1.229 is at 00:0c:29:ad:f5:13
    507 27.524930198  ZyxelCom_48:9e:10    Giga-Byt_e3:08:bc    ARP         60 Who has 192.168.1.6? Tell 192.168.1.1
    508 27.524930490  Giga-Byt_e3:08:bc    ZyxelCom_48:9e:10    ARP         60 192.168.1.6 is at 18:c0:4d:e3:08:bc
    892 53.379562190  VMware_ad:f5:13      ZyxelCom_48:9e:10    ARP         42 Who has 192.168.1.1? Tell 192.168.1.229
    893 53.380116563  ZyxelCom_48:9e:10    VMware_ad:f5:13      ARP         60 192.168.1.1 is at ec:3e:b3:48:9e:10
   1238 77.416930534  ZyxelCom_48:9e:10    Giga-Byt_e3:08:bc    ARP         60 Who has 192.168.1.6? Tell 192.168.1.1
   1239 77.416930601  Giga-Byt_e3:08:bc    ZyxelCom_48:9e:10    ARP         60 192.168.1.6 is at 18:c0:4d:e3:08:bc
   1303 81.955745482  VMware_19:63:4d      ZyxelCom_48:9e:10    ARP         60 Who has 192.168.1.1? Tell 192.168.1.89
   1304 81.956082578  ZyxelCom_48:9e:10    VMware_19:63:4d      ARP         60 192.168.1.1 is at ec:3e:b3:48:9e:10
```

```
Frame 341: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
Ethernet II, Src: ZyxelCom_48:9e:10 (ec:3e:b3:48:9e:10), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff ec 3e  b3 48 9e 10 08 06 00 01   ·······> ·H······
0010  08 00 06 04 00 01 ec 3e  b3 48 9e 10 c0 a8 01 01   ·······> ·H······
0020  00 00 00 00 00 00 c0 a8  01 59 00 00 00 00 00 00   ········ ·Y······
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

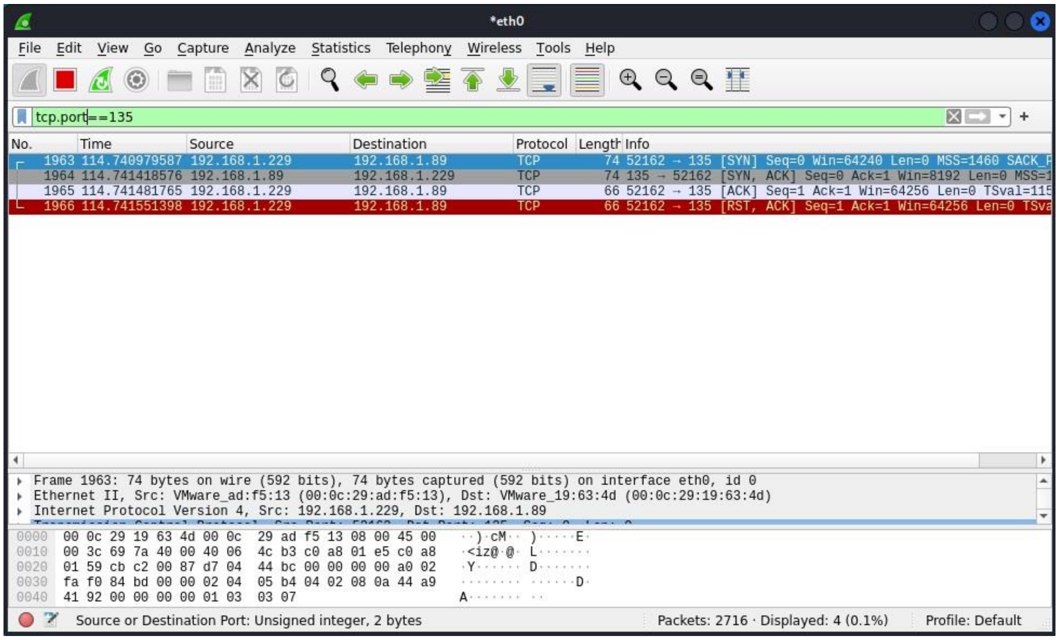
eth0: <live capture in progress> Packets: 1308 · Displayed: 12 (0.9%) Profile: Default

Scan Results in Zenmap:



```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-02 05:13 EST
Initiating ARP Ping Scan at 05:13
Scanning 192.168.1.89 [1 port]
Completed ARP Ping Scan at 05:13, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 05:13
Completed Parallel DNS resolution of 1 host. at 05:13, 6.51s elapsed
Initiating Connect Scan at 05:13
Scanning WIN-5H7SCBU1117.home (192.168.1.89) [1 port]
Discovered open port 135/tcp on 192.168.1.89
Completed Connect Scan at 05:13, 0.00s elapsed (1 total ports)
Nmap scan report for WIN-5H7SCBU1117.home (192.168.1.89)
Host is up (0.00035s latency).

PORT    STATE SERVICE
135/tcp open  msrpc
MAC Address: 00:0C:29:19:63:4D (VMware)

Read data files from: /nix/store/bmxqwji31nr1354qbvdvk5p7j42w6gvs-nmap-
graphical-7.92/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 6.61 seconds
           Raw packets sent: 1 (28B) | Rcvd: 1 (28B)
```

Scan Results in Wireshark:


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port==135

```
No.     Time           Source          Destination     Protocol Length Info
   1963 114.740979587 192.168.1.229   192.168.1.89    TCP        74 52162 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_P
   1964 114.741418576 192.168.1.89    192.168.1.229   TCP        74 135 → 52162 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1
   1965 114.741481765 192.168.1.229   192.168.1.89    TCP        66 52162 → 135 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=115
   1966 114.741551398 192.168.1.229   192.168.1.89    TCP        66 52162 → 135 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSva
```

```
▸ Frame 1963: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0
▸ Ethernet II, Src: VMware_ad:f5:13 (00:0c:29:ad:f5:13), Dst: VMware_19:63:4d (00:0c:29:19:63:4d)
▸ Internet Protocol Version 4, Src: 192.168.1.229, Dst: 192.168.1.89
```

```
0000  00 0c 29 19 63 4d 00 0c  29 ad f5 13 08 00 45 00   ··)·cM·· )·····E·
0010  00 3c 69 7a 40 00 40 06  4c b3 c0 a8 01 e5 c0 a8   ·<iz@·@· L·······
0020  01 59 cb c2 00 87 d7 04  44 bc 00 00 00 00 a0 02   ·Y······ D·······
0030  fa f0 84 bd 00 00 02 04  05 b4 04 02 08 0a 44 a9   ········ ······D·
0040  41 92 00 00 00 00 01 03  03 07                     A······· ··
```

Source or Destination Port: Unsigned integer, 2 bytes · Packets: 2716 · Displayed: 4 (0.1%) · Profile: Default

Questions and Discussion

1. **What is Host Discovery?**

   Identifying hosts on a network. For example, listing the hosts which respond to pings or have a particular port open.

2. **How to use nmap to detect remote OS?**

   Using the command:

   ```
   sudo nmap -O <target>
   ```

   or

   ```
   sudo nmap -A <target> // Aggressive scan
   ```

   or

   via Zenmap > Quick or Intensive Scan > Host Details > Operation System Section.

3. **How to check whether NMAP already installed or not?**

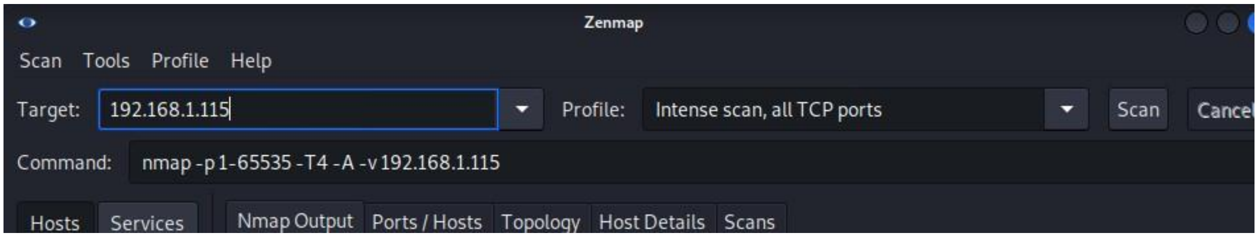
   By the command “sudo nmap” in the terminal. If we got an error, then it’s not installed. To install it we use the command: “sudo apt-get install nmap”

4. **what are the phases of NMAP scanning?**
   a. Script pre-scanning.
   b. Target enumeration
   c. Host discovery
   d. Reverse-DNS resolution
   e. Port scanning
   f. Version detection
   g. OS detection
   h. Traceroute
   i. Script scanning
   j. Output

5. **Describe the technique behind nmap work principles**
   Nmap sends specially crafted packets to the target host and then analyzes the responses, hence we can detect several criteria, like users, operating system of the targets, names and versions of the listening services, estimated uptime, type of device, and presence of a firewall.

6. **Find out all the message sent in a TCP scan for the metasploitable Linux machine, put those in a .pcap file and add it to your report. Take a screen shot of the Wireshark program.**

   Scan criteria: Testing all TCP ports on the IP 192.168.1.115 (Metasploitable)

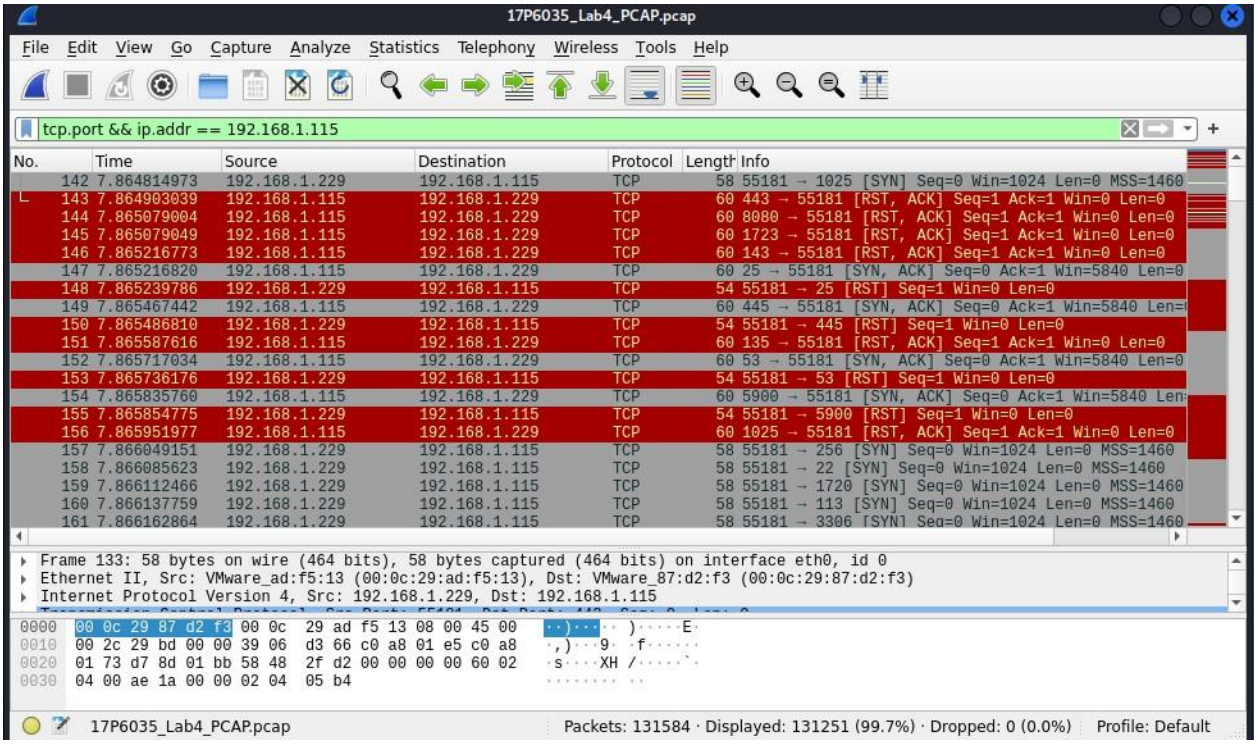


Target: 192.168.1.115

Profile: Intense scan, all TCP ports

Command: nmap -p 1-65535 -T4 -A -v 192.168.1.115

Results in Wireshark:



tcp.port && ip.addr == 192.168.1.115

```
No.   Time          Source          Destination     Protocol  Length Info
  142 7.864814973   192.168.1.229   192.168.1.115   TCP       58 55181 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  143 7.864903039   192.168.1.115   192.168.1.229   TCP       60 443 → 55181 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  144 7.865079004   192.168.1.115   192.168.1.229   TCP       60 8080 → 55181 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  145 7.865079049   192.168.1.115   192.168.1.229   TCP       60 1723 → 55181 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  146 7.865216773   192.168.1.115   192.168.1.229   TCP       60 143 → 55181 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  147 7.865216820   192.168.1.115   192.168.1.229   TCP       60 25 → 55181 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
  148 7.865239786   192.168.1.229   192.168.1.115   TCP       54 55181 → 25 [RST] Seq=1 Win=0 Len=0
  149 7.865467442   192.168.1.115   192.168.1.229   TCP       60 445 → 55181 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=
  150 7.865486810   192.168.1.229   192.168.1.115   TCP       54 55181 → 445 [RST] Seq=1 Win=0 Len=0
  151 7.865587616   192.168.1.115   192.168.1.229   TCP       60 135 → 55181 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  152 7.865717034   192.168.1.115   192.168.1.229   TCP       60 53 → 55181 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
  153 7.865736176   192.168.1.229   192.168.1.115   TCP       54 55181 → 53 [RST] Seq=1 Win=0 Len=0
  154 7.865835760   192.168.1.115   192.168.1.229   TCP       60 5900 → 55181 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len
  155 7.865854775   192.168.1.229   192.168.1.115   TCP       54 55181 → 5900 [RST] Seq=1 Win=0 Len=0
  156 7.865951977   192.168.1.115   192.168.1.229   TCP       60 1025 → 55181 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  157 7.866049151   192.168.1.229   192.168.1.115   TCP       58 55181 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  158 7.866085623   192.168.1.229   192.168.1.115   TCP       58 55181 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  159 7.866112466   192.168.1.229   192.168.1.115   TCP       58 55181 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  160 7.866137759   192.168.1.229   192.168.1.115   TCP       58 55181 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  161 7.866162864   192.168.1.229   192.168.1.115   TCP       58 55181 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
```

```
▸ Frame 133: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface eth0, id 0
▸ Ethernet II, Src: VMware_ad:f5:13 (00:0c:29:ad:f5:13), Dst: VMware_87:d2:f3 (00:0c:29:87:d2:f3)
▸ Internet Protocol Version 4, Src: 192.168.1.229, Dst: 192.168.1.115
```

```
0000  00 0c 29 87 d2 f3 00 0c  29 ad f5 13 08 00 45 00   ··)···· )·····E·
0010  00 2c 29 bd 00 00 39 06  d3 66 c0 a8 01 e5 c0 a8   ·,)···9· ·f······
0020  01 73 d7 8d 01 bb 58 48  2f d2 00 00 00 00 60 02   ·s····XH /·····`·
0030  04 00 ae 1a 00 00 02 04  05 b4                     ········ ··
```

17P6035_Lab4_PCAP.pcap   Packets: 131584 · Displayed: 131251 (99.7%) · Dropped: 0 (0.0%)   Profile: Default

Result file (.pcab) is attached with the report.

7. **Take a screen shot of your own work for all of the above steps and put them all together in your report, you must order them as the flow of the experiments go, label each screen shot with a suitable title**

   Done in previous steps.