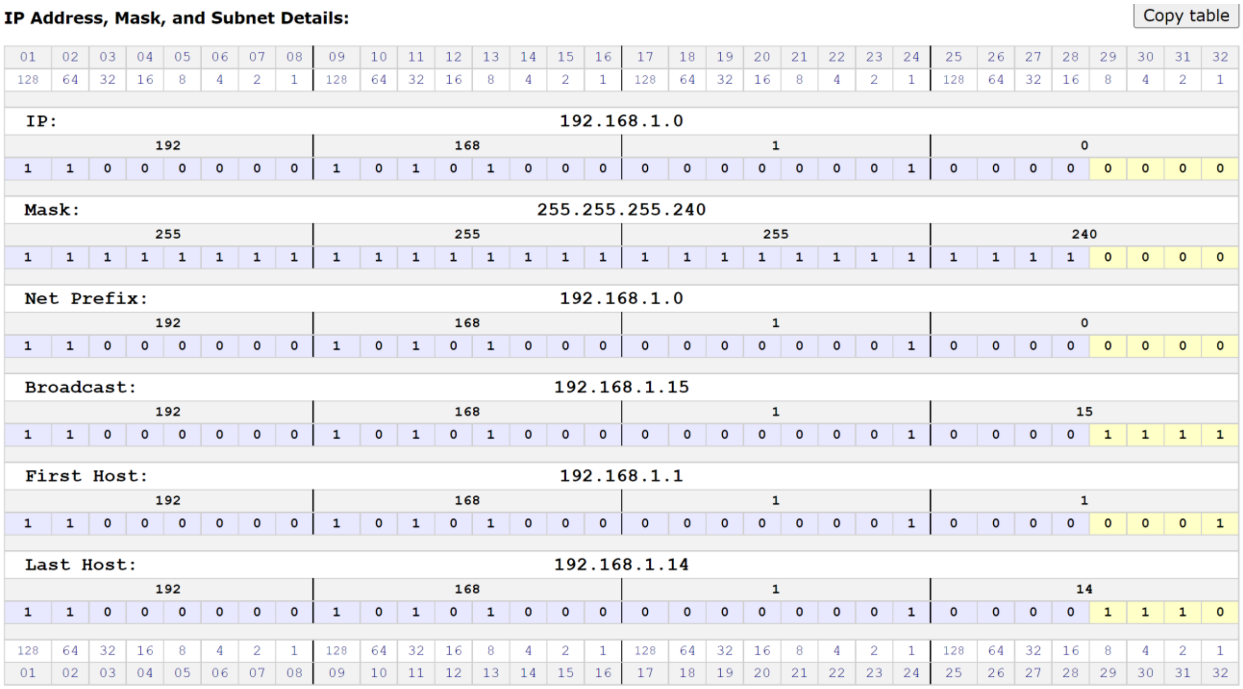
NETWORK SECURITY

Assignment 4

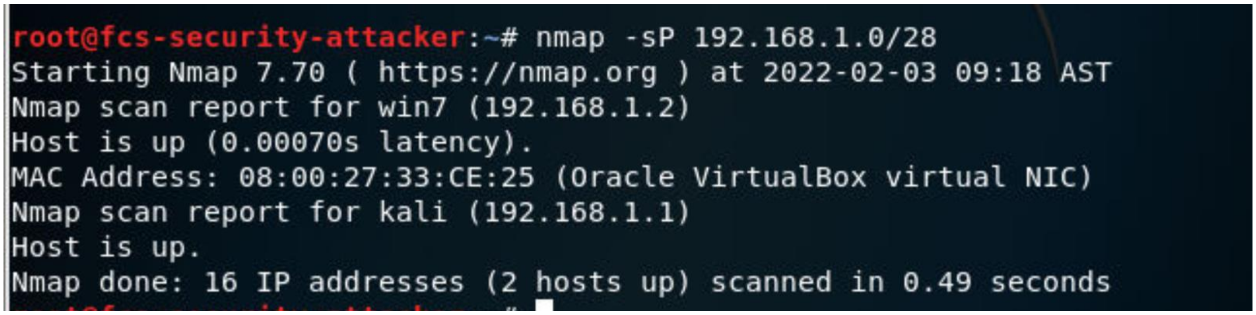
Soheil Shirvani 3720505

1) Find the IP range, number of valid host machines, and the subnet mask of a network 192.168.1.0/28



IP Address, Mask, and Subnet Details:

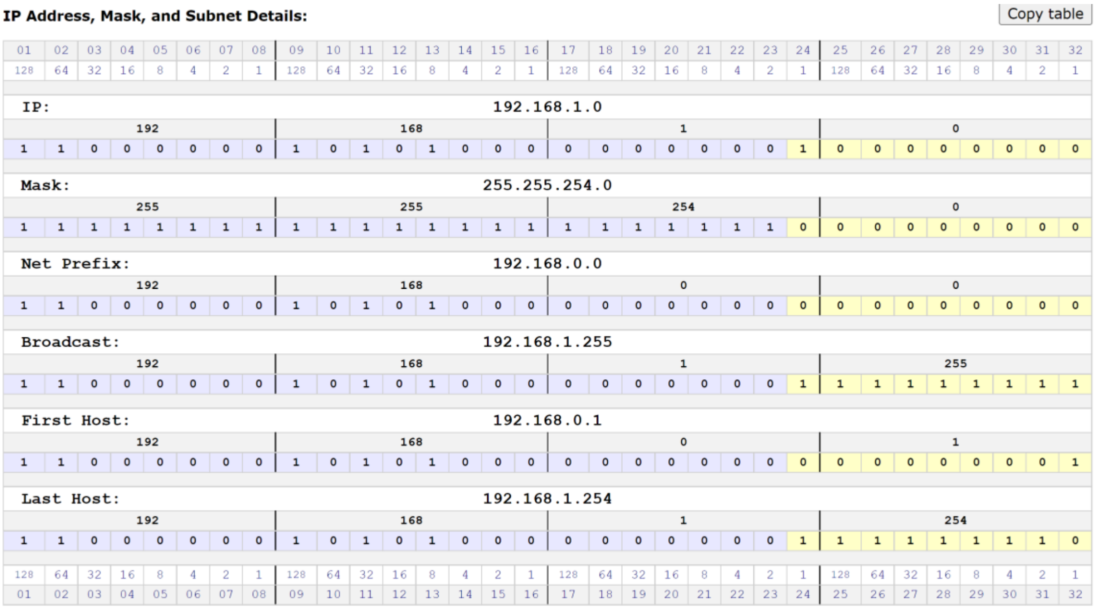
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1
IP:																192.168.1.0															
192								168								1								0							
1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
Mask:																255.255.255.240															
255								255								255								240							
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0
Net Prefix:																192.168.1.0															
192								168								1								0							
1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
Broadcast:																192.168.1.15															
192								168								1								15							
1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	1	1	1
First Host:																192.168.1.1															
192								168								1								1							
1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1
Last Host:																192.168.1.14															
192								168								1								14							
1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	1	1	0
128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32



```
root@fcs-security-attacker:~# nmap -sP 192.168.1.0/28
Starting Nmap 7.70 ( https://nmap.org ) at 2022-02-03 09:18 AST
Nmap scan report for win7 (192.168.1.2)
Host is up (0.00070s latency).
MAC Address: 08:00:27:33:CE:25 (Oracle VirtualBox virtual NIC)
Nmap scan report for kali (192.168.1.1)
Host is up.
Nmap done: 16 IP addresses (2 hosts up) scanned in 0.49 seconds
```

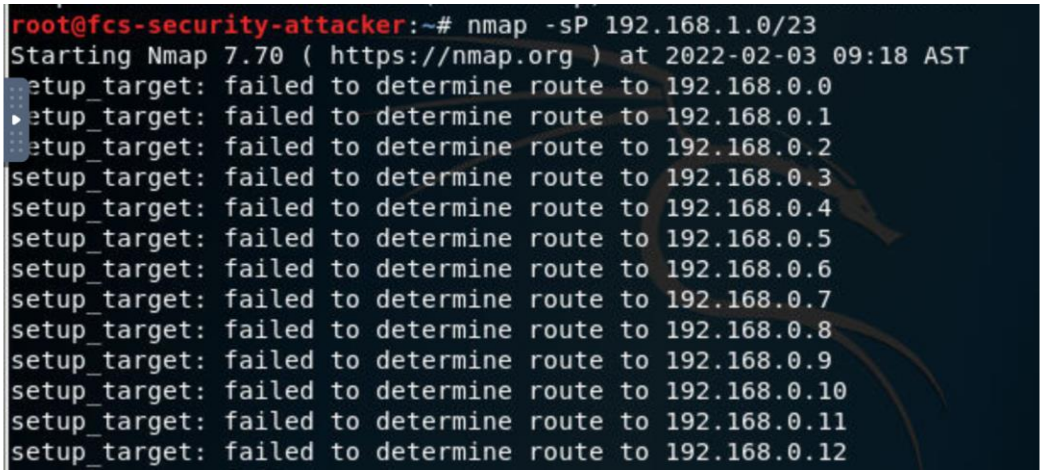
Found 16 IP addresses in which 2 hosts are up

2) 2) Find the IP range, number of valid host machines, and the subnet mask of a network 192.168.1.0/23

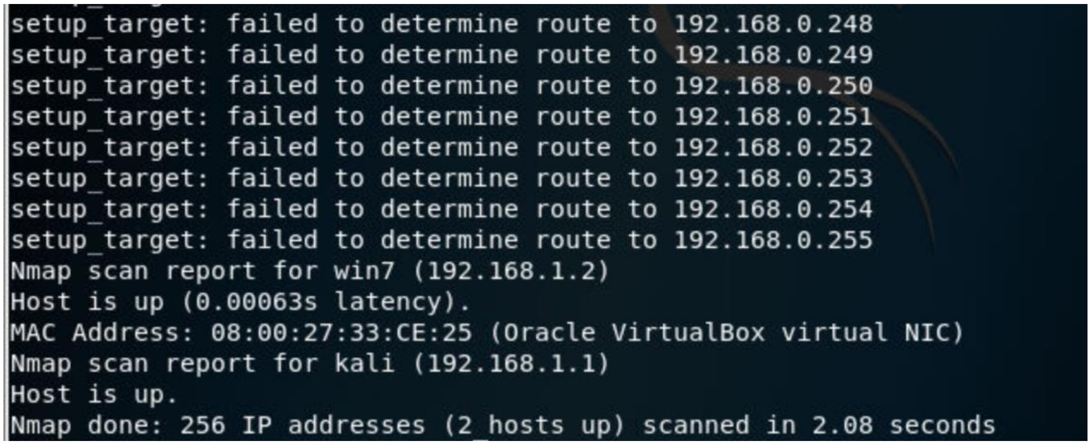


IP Address, Mask, and Subnet Details:

	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1
IP: 192.168.1.0																																
	192								168								1								0							
	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
Mask: 255.255.254.0																																
	255								255								254								0							
	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0
Net Prefix: 192.168.0.0																																
	192								168								0								0							
	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Broadcast: 192.168.1.255																																
	192								168								1								255							
	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1
First Host: 192.168.0.1																																
	192								168								0								1							
	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Last Host: 192.168.1.254																																
	192								168								1								254							
	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0
	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1
	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32



```
root@fcs-security-attacker:~# nmap -sP 192.168.1.0/23
Starting Nmap 7.70 ( https://nmap.org ) at 2022-02-03 09:18 AST
etup_target: failed to determine route to 192.168.0.0
etup_target: failed to determine route to 192.168.0.1
etup_target: failed to determine route to 192.168.0.2
setup_target: failed to determine route to 192.168.0.3
setup_target: failed to determine route to 192.168.0.4
setup_target: failed to determine route to 192.168.0.5
setup_target: failed to determine route to 192.168.0.6
setup_target: failed to determine route to 192.168.0.7
setup_target: failed to determine route to 192.168.0.8
setup_target: failed to determine route to 192.168.0.9
setup_target: failed to determine route to 192.168.0.10
setup_target: failed to determine route to 192.168.0.11
setup_target: failed to determine route to 192.168.0.12
```



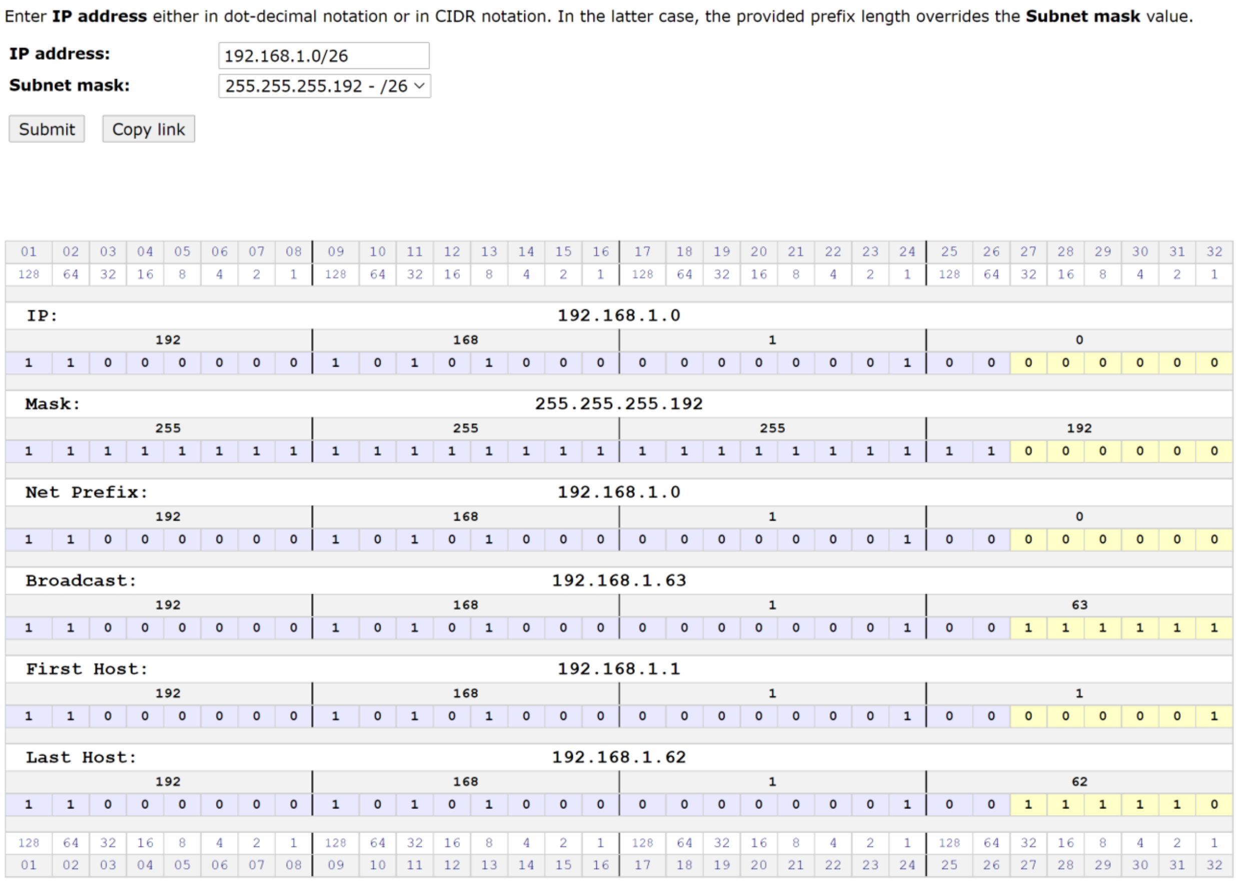
```
setup_target: failed to determine route to 192.168.0.248
setup_target: failed to determine route to 192.168.0.249
setup_target: failed to determine route to 192.168.0.250
setup_target: failed to determine route to 192.168.0.251
setup_target: failed to determine route to 192.168.0.252
setup_target: failed to determine route to 192.168.0.253
setup_target: failed to determine route to 192.168.0.254
setup_target: failed to determine route to 192.168.0.255
Nmap scan report for win7 (192.168.1.2)
Host is up (0.00063s latency).
MAC Address: 08:00:27:33:CE:25 (Oracle VirtualBox virtual NIC)
Nmap scan report for kali (192.168.1.1)
Host is up.
Nmap done: 256 IP addresses (2 hosts up) scanned in 2.08 seconds
```

Found 256 IP addresses in which 2 hosts are up (Attacker and Victim VMs)

3) Suggest a CIDR block for IP address 192.168.1.0 to support up to 62 active nodes in the network.

To find 64 host:

https://wintelguy.com/ip-mask-visualizer.pl



Enter **IP address** either in dot-decimal notation or in CIDR notation. In the latter case, the provided prefix length overrides the **Subnet mask** value.

IP address: 192.168.1.0/26

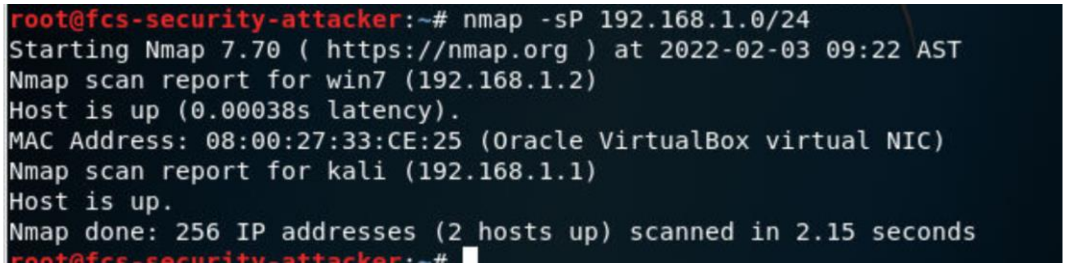
Subnet mask: 255.255.255.192 - /26

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1
IP:																192.168.1.0															
192								168								1								0							
1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
Mask:																255.255.255.192															
255								255								255								192							
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0
Net Prefix:																192.168.1.0															
192								168								1								0							
1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
Broadcast:																192.168.1.63															
192								168								1								63							
1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	1	1	1	1
First Host:																192.168.1.1															
192								168								1								1							
1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1
Last Host:																192.168.1.62															
192								168								1								62							
1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	1	1	1	0
128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

So by fixing 26 bit of an IP address we can search for 62 IP addresses.

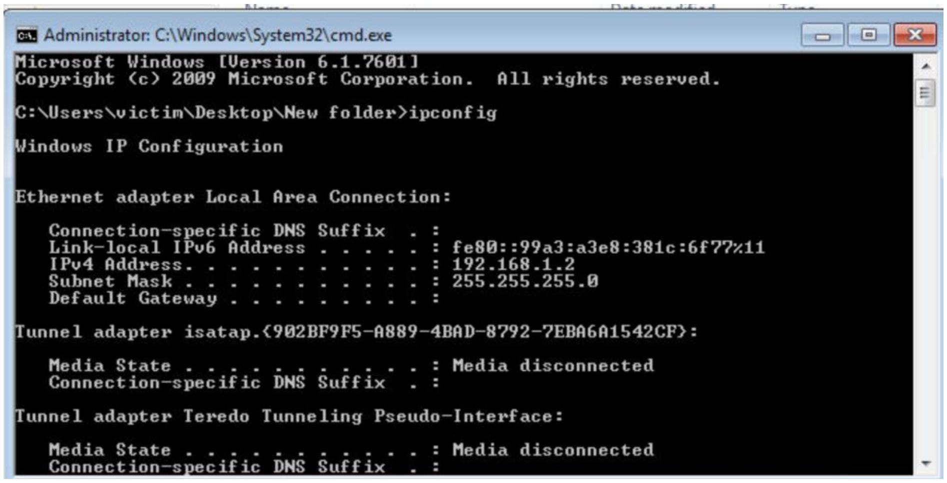
1) Find the list of up servers and devices in the victim network.

First we can see the hosts which are up and running by running nmap -sp of the attacker VM address:



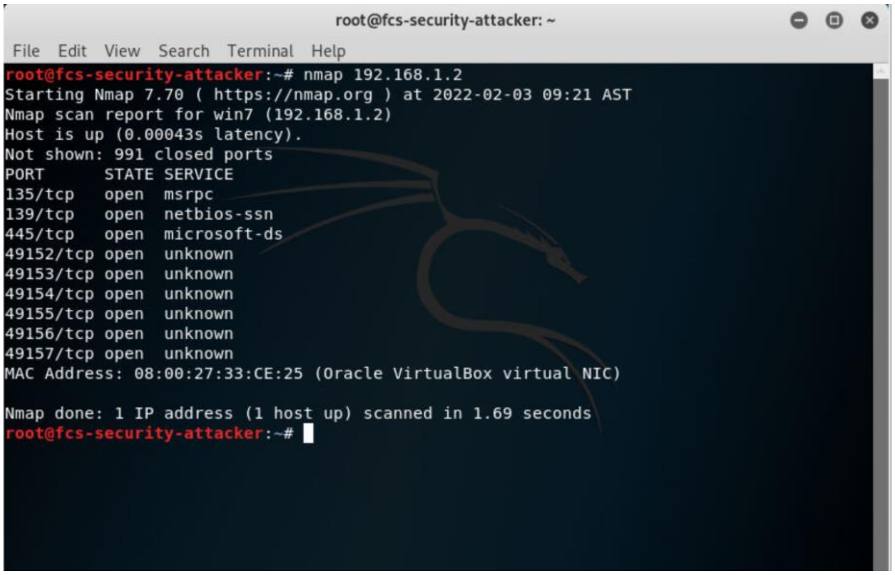
```
root@fcs-security-attacker:~# nmap -sP 192.168.1.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2022-02-03 09:22 AST
Nmap scan report for win7 (192.168.1.2)
Host is up (0.00038s latency).
MAC Address: 08:00:27:33:CE:25 (Oracle VirtualBox virtual NIC)
Nmap scan report for kali (192.168.1.1)
Host is up.
Nmap done: 256 IP addresses (2 hosts up) scanned in 2.15 seconds
root@fcs-security-attacker:~#
```

We see that 192.168.1.2 is up This is actually the IP address of the windows victim.



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

C:\Users\victim\Desktop\New folder>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::99a3:a3e8:381c:6f77%11
   IPv4 Address. . . . . . . . . . . : 192.168.1.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Tunnel adapter isatap.{902BF9F5-A889-4BAD-8792-7EBA6A1542CF}:

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

Tunnel adapter Teredo Tunneling Pseudo-Interface:

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

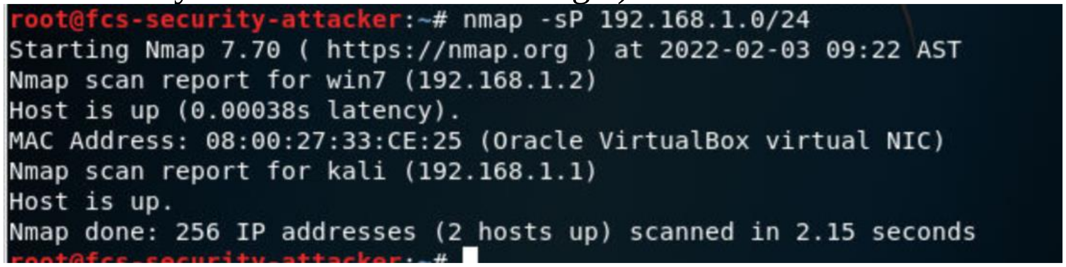
By running nmap for Windows Victim in attacker terminal we can see all the services that are up in victims machine



root@fcs-security-attacker: ~
File Edit View Search Terminal Help

```
root@fcs-security-attacker:~# nmap 192.168.1.2
Starting Nmap 7.70 ( https://nmap.org ) at 2022-02-03 09:21 AST
Nmap scan report for win7 (192.168.1.2)
Host is up (0.00043s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 08:00:27:33:CE:25 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.69 seconds
root@fcs-security-attacker:~#
```

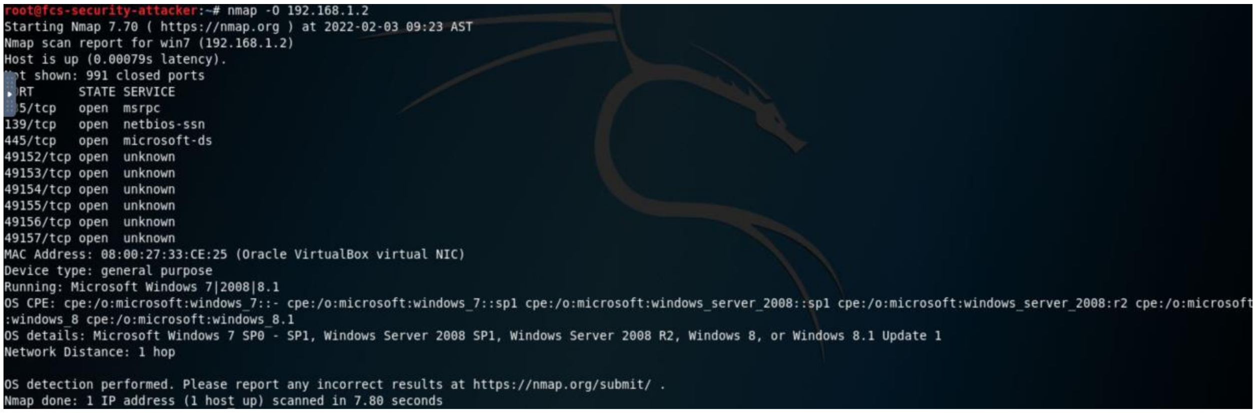
2) Find the OS of the first up computer in the victim network (from now this machine is your victim machine or target).



```
root@fcs-security-attacker:~# nmap -sP 192.168.1.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2022-02-03 09:22 AST
Nmap scan report for win7 (192.168.1.2)
Host is up (0.00038s latency).
MAC Address: 08:00:27:33:CE:25 (Oracle VirtualBox virtual NIC)
Nmap scan report for kali (192.168.1.1)
Host is up.
Nmap done: 256 IP addresses (2 hosts up) scanned in 2.15 seconds
root@fcs-security-attacker:~#
```

First Up Machine is Windows 192.168.1.2

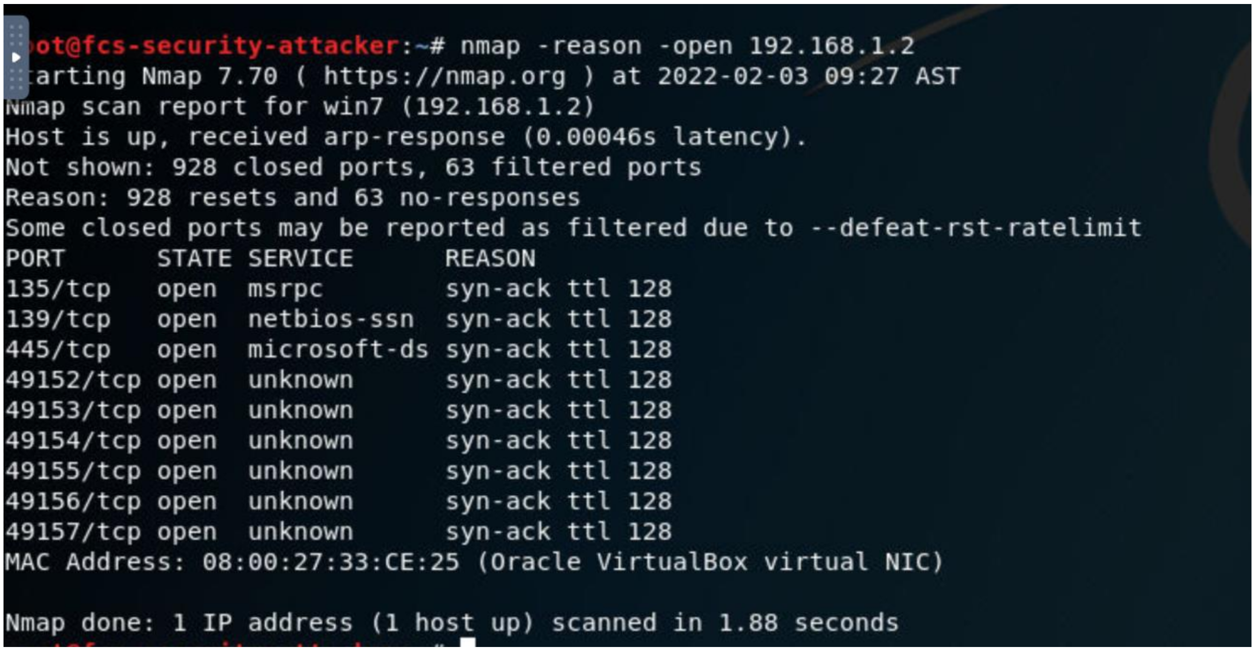
Then by running nmap -o we can find the operating system of the victim



```
root@fcs-security-attacker:~# nmap -O 192.168.1.2
Starting Nmap 7.70 ( https://nmap.org ) at 2022-02-03 09:23 AST
Nmap scan report for win7 (192.168.1.2)
Host is up (0.00079s latency).
t shown: 991 closed ports
RT      STATE SERVICE
5/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 08:00:27:33:CE:25 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft
:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.80 seconds
```

3) Find all open ports and the reason that are in the particular states on the victim machine

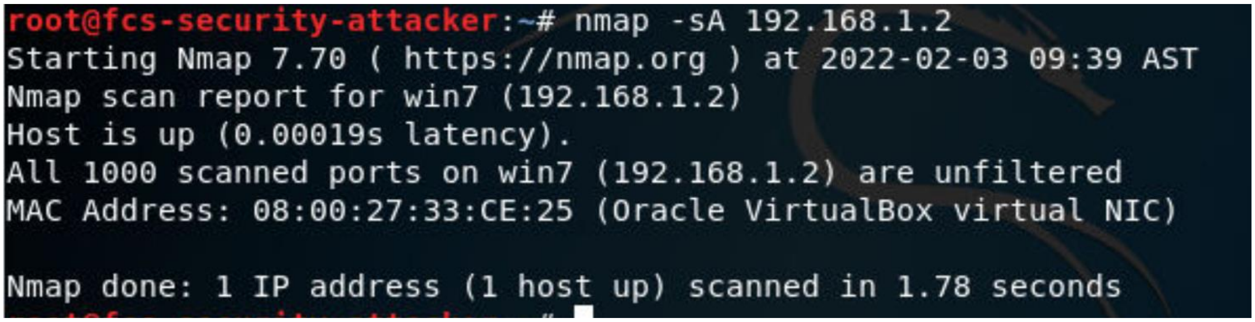
Using nmap -reason -open we can find all open ports and the reason of the open service



```
ot@fcs-security-attacker:~# nmap -reason -open 192.168.1.2
arting Nmap 7.70 ( https://nmap.org ) at 2022-02-03 09:27 AST
Nmap scan report for win7 (192.168.1.2)
Host is up, received arp-response (0.00046s latency).
Not shown: 928 closed ports, 63 filtered ports
Reason: 928 resets and 63 no-responses
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      REASON
135/tcp   open  msrpc        syn-ack ttl 128
139/tcp   open  netbios-ssn  syn-ack ttl 128
445/tcp   open  microsoft-ds syn-ack ttl 128
49152/tcp open  unknown      syn-ack ttl 128
49153/tcp open  unknown      syn-ack ttl 128
49154/tcp open  unknown      syn-ack ttl 128
49155/tcp open  unknown      syn-ack ttl 128
49156/tcp open  unknown      syn-ack ttl 128
49157/tcp open  unknown      syn-ack ttl 128
MAC Address: 08:00:27:33:CE:25 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.88 seconds
```

4) Find out if the host is protected by a firewall.

By using nmap -sA we can find if the targe machine is filtered or unfiltered (with firewall or without firewall)

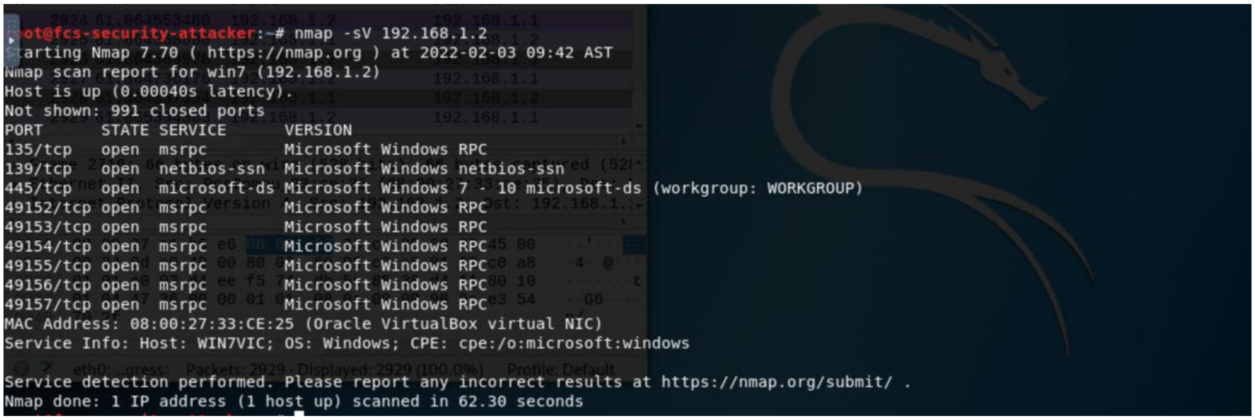


```
root@fcs-security-attacker:~# nmap -sA 192.168.1.2
Starting Nmap 7.70 ( https://nmap.org ) at 2022-02-03 09:39 AST
Nmap scan report for win7 (192.168.1.2)
Host is up (0.00019s latency).
All 1000 scanned ports on win7 (192.168.1.2) are unfiltered
MAC Address: 08:00:27:33:CE:25 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.78 seconds
```

The firewall is off on Windows Victim

5) Find the common vulnerabilities on the victim machine.

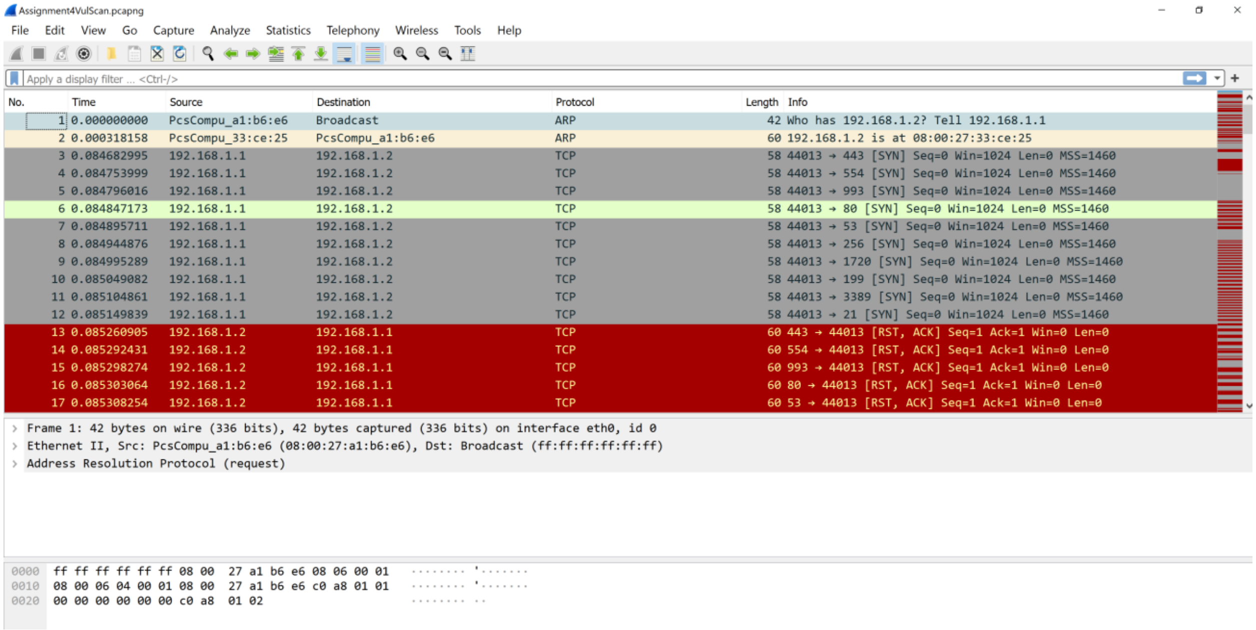
By Using nmap -sV we can find all the vulnerabilities on Victim machine for each service



```
ot@fcs-security-attacker:~# nmap -sV 192.168.1.2
arting Nmap 7.70 ( https://nmap.org ) at 2022-02-03 09:42 AST
Nmap scan report for win7 (192.168.1.2)
Host is up (0.00040s latency).
Not shown: 991 closed ports
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 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:33:CE:25 (Oracle VirtualBox virtual NIC)
Service Info: Host: WIN7VIC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 62.30 seconds
```

Captured Packets Available

Sample Packets are:



Assignment4VulScan.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time         Source             Destination        Protocol  Length Info
   1 0.000000000  PcsCompu_a1:b6:e6  Broadcast          ARP       42 Who has 192.168.1.2? Tell 192.168.1.1
   2 0.000318158  PcsCompu_33:ce:25  PcsCompu_a1:b6:e6  ARP       60 192.168.1.2 is at 08:00:27:33:ce:25
   3 0.084682995  192.168.1.1        192.168.1.2        TCP       58 44013 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
   4 0.084753999  192.168.1.1        192.168.1.2        TCP       58 44013 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
   5 0.084796016  192.168.1.1        192.168.1.2        TCP       58 44013 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
   6 0.084847173  192.168.1.1        192.168.1.2        TCP       58 44013 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
   7 0.084895711  192.168.1.1        192.168.1.2        TCP       58 44013 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
   8 0.084944876  192.168.1.1        192.168.1.2        TCP       58 44013 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
   9 0.084995289  192.168.1.1        192.168.1.2        TCP       58 44013 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  10 0.085049082  192.168.1.1        192.168.1.2        TCP       58 44013 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  11 0.085104861  192.168.1.1        192.168.1.2        TCP       58 44013 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  12 0.085149839  192.168.1.1        192.168.1.2        TCP       58 44013 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  13 0.085260905  192.168.1.2        192.168.1.1        TCP       60 443 → 44013 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  14 0.085292431  192.168.1.2        192.168.1.1        TCP       60 554 → 44013 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  15 0.085298274  192.168.1.2        192.168.1.1        TCP       60 993 → 44013 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  16 0.085303064  192.168.1.2        192.168.1.1        TCP       60 80 → 44013 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  17 0.085308254  192.168.1.2        192.168.1.1        TCP       60 53 → 44013 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
> Ethernet II, Src: PcsCompu_a1:b6:e6 (08:00:27:a1:b6:e6), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 08 00  27 a1 b6 e6 08 06 00 01   ........ '.......
0010  08 00 06 04 00 01 08 00  27 a1 b6 e6 c0 a8 01 01   ........ '.......
0020  00 00 00 00 00 00 c0 a8  01 02                     ........ ..
```

All the packets are available in the pcap attached file. The -sV tries to communicate to all ports of the victim machine to fin out the services and vulnerabilities. There are a lot of packets since in tries with many ports. Not all the ports are working so most of the communications didn’t get a respond and that’s why they are in red in pcap file.