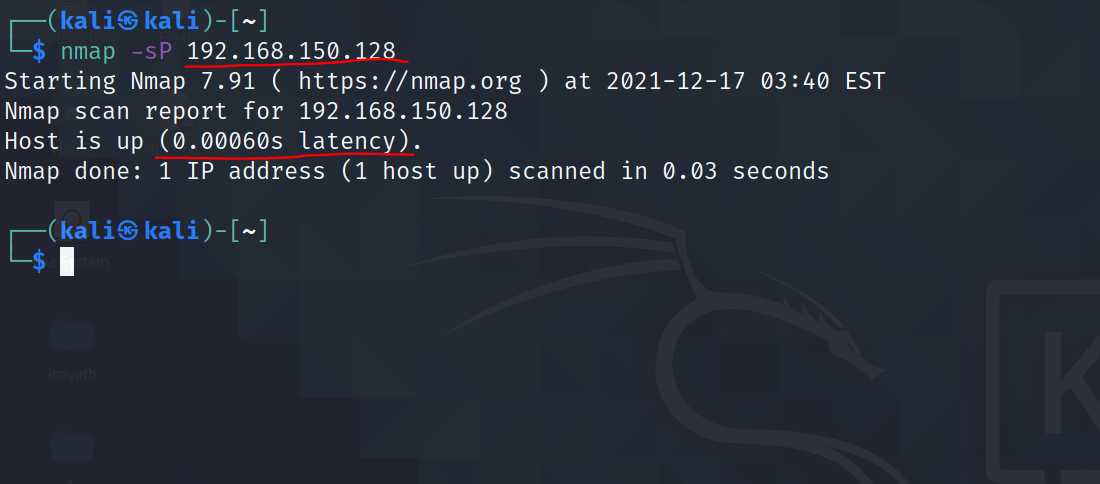
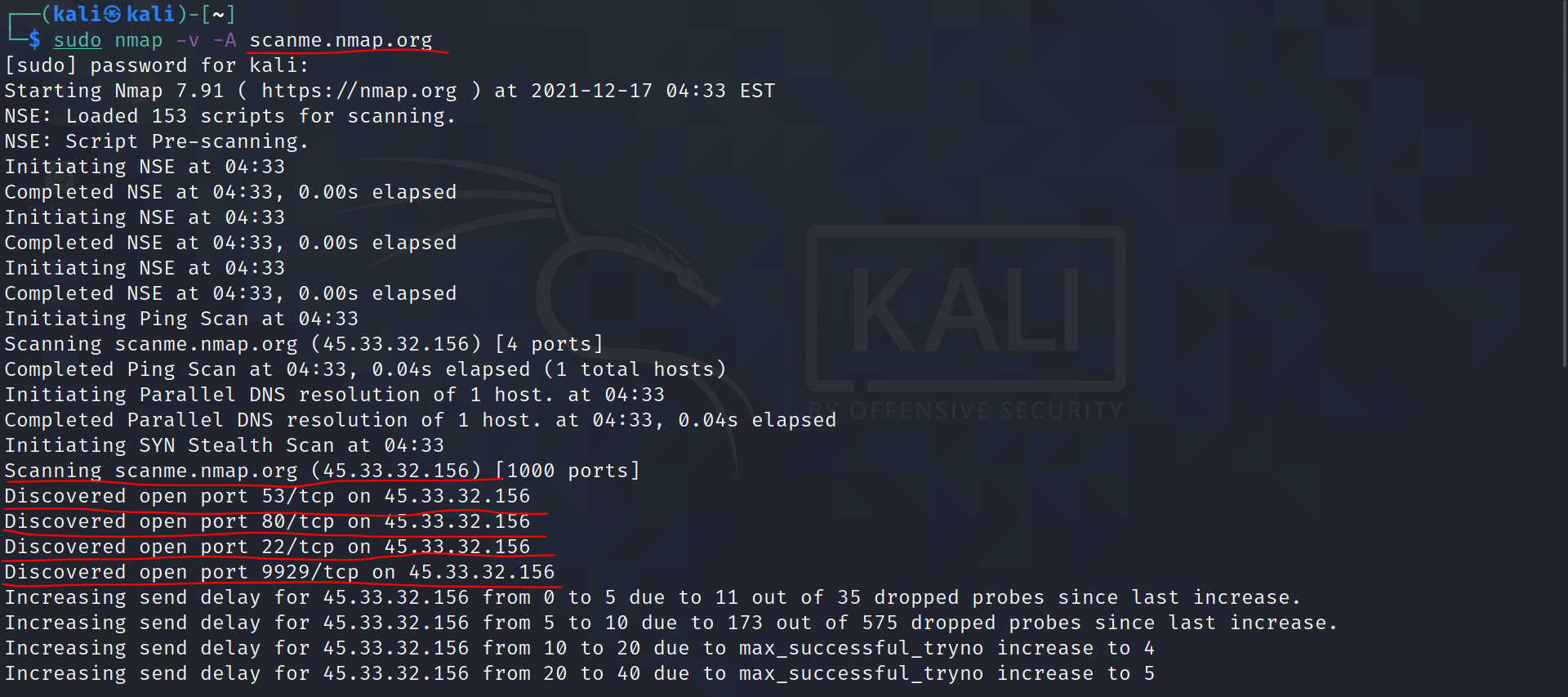
**Network security project**

**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

****

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**

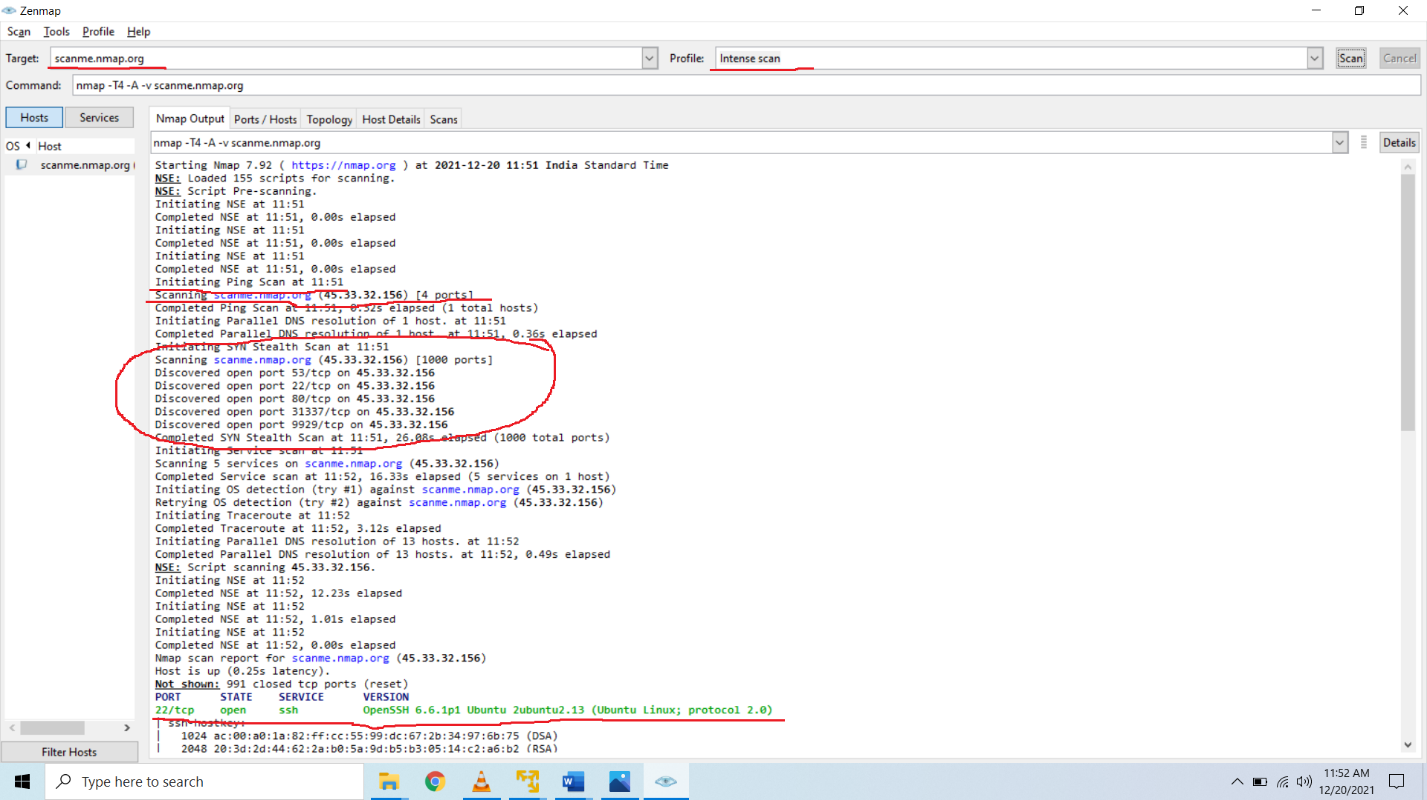
****

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.

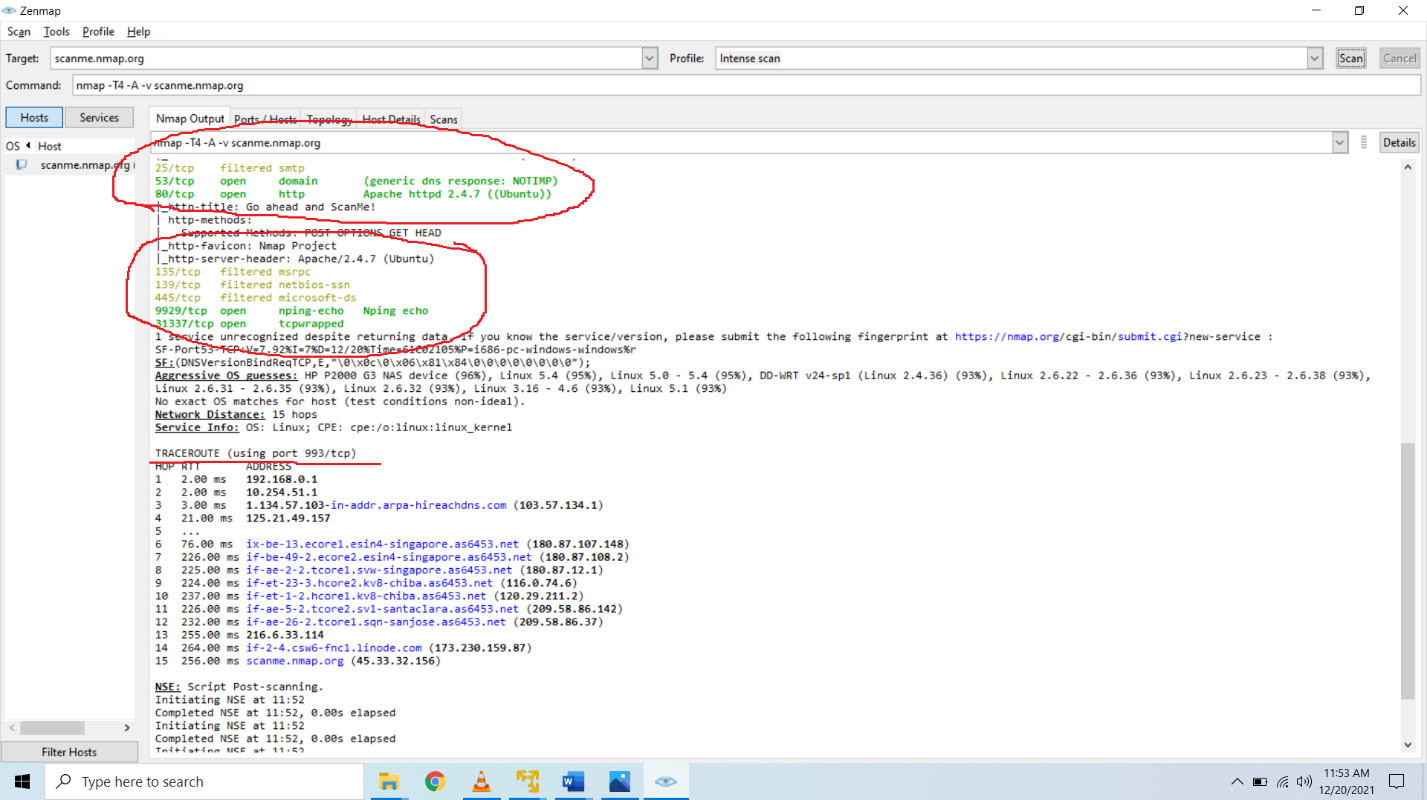
Port 22/tcp on server **45.33.32.156** is open.

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

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

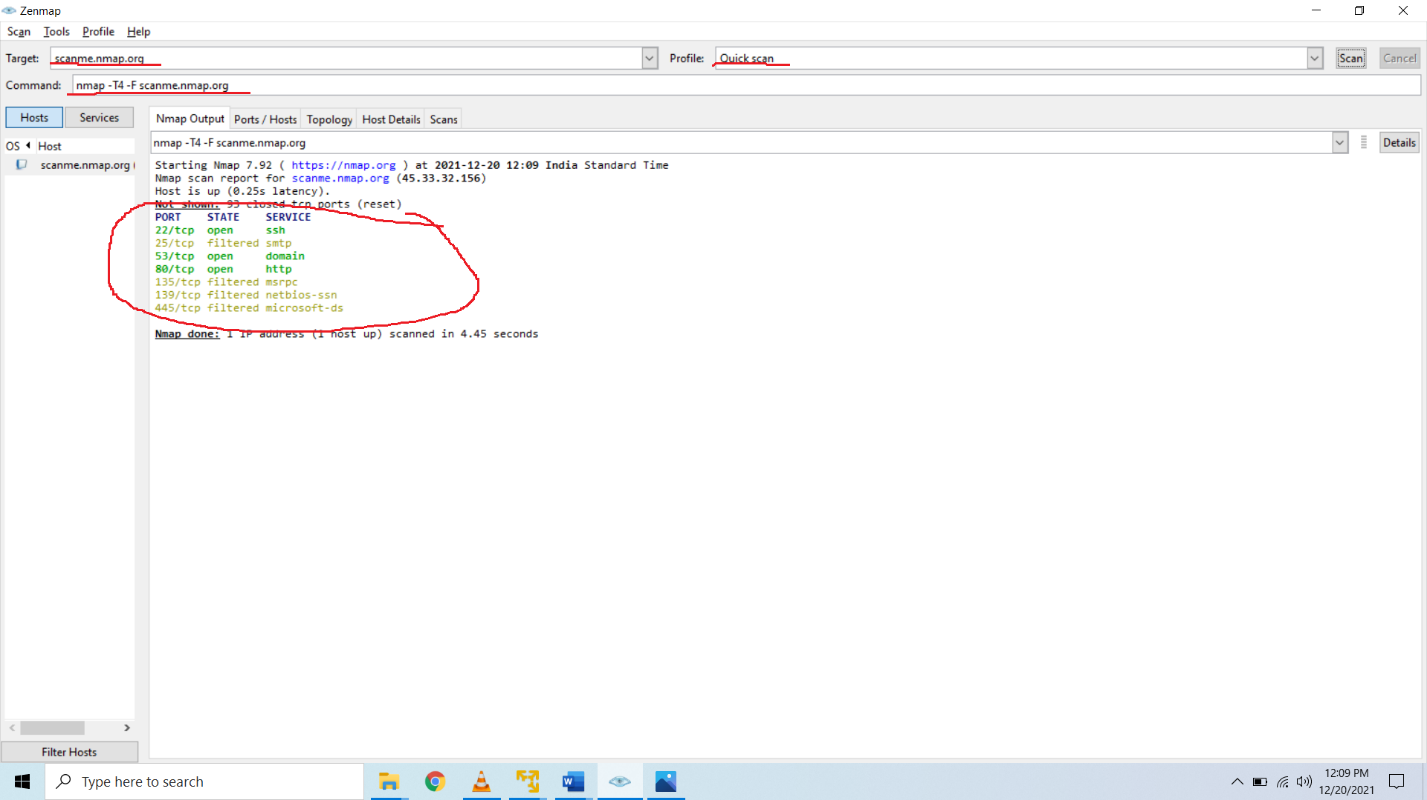
It did a ping scan. It also initiated traceroute. It shows there are not shown 991 filtered tcp ports (reset).

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.



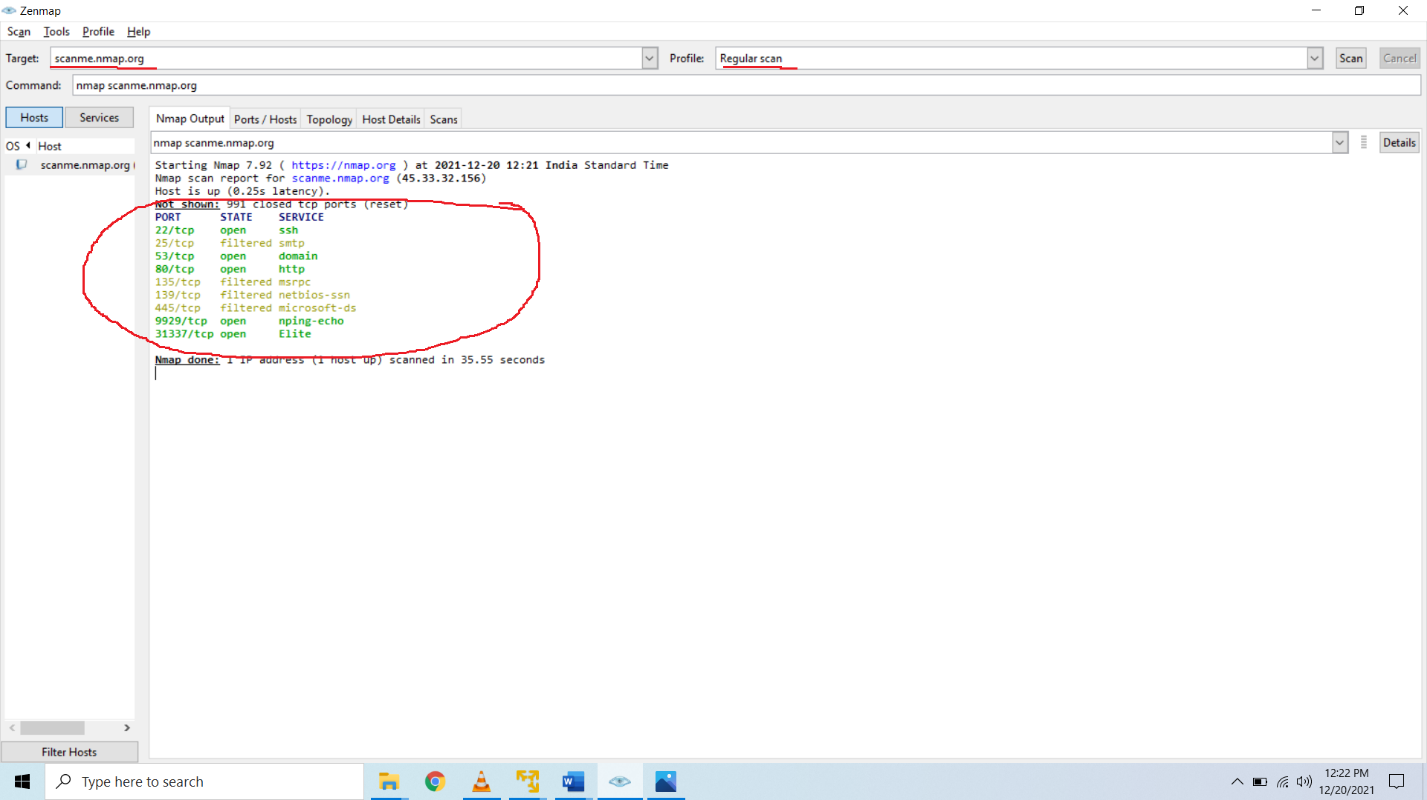
Scanning used here is quick scan. Highlights show name of the port, its state and service.

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

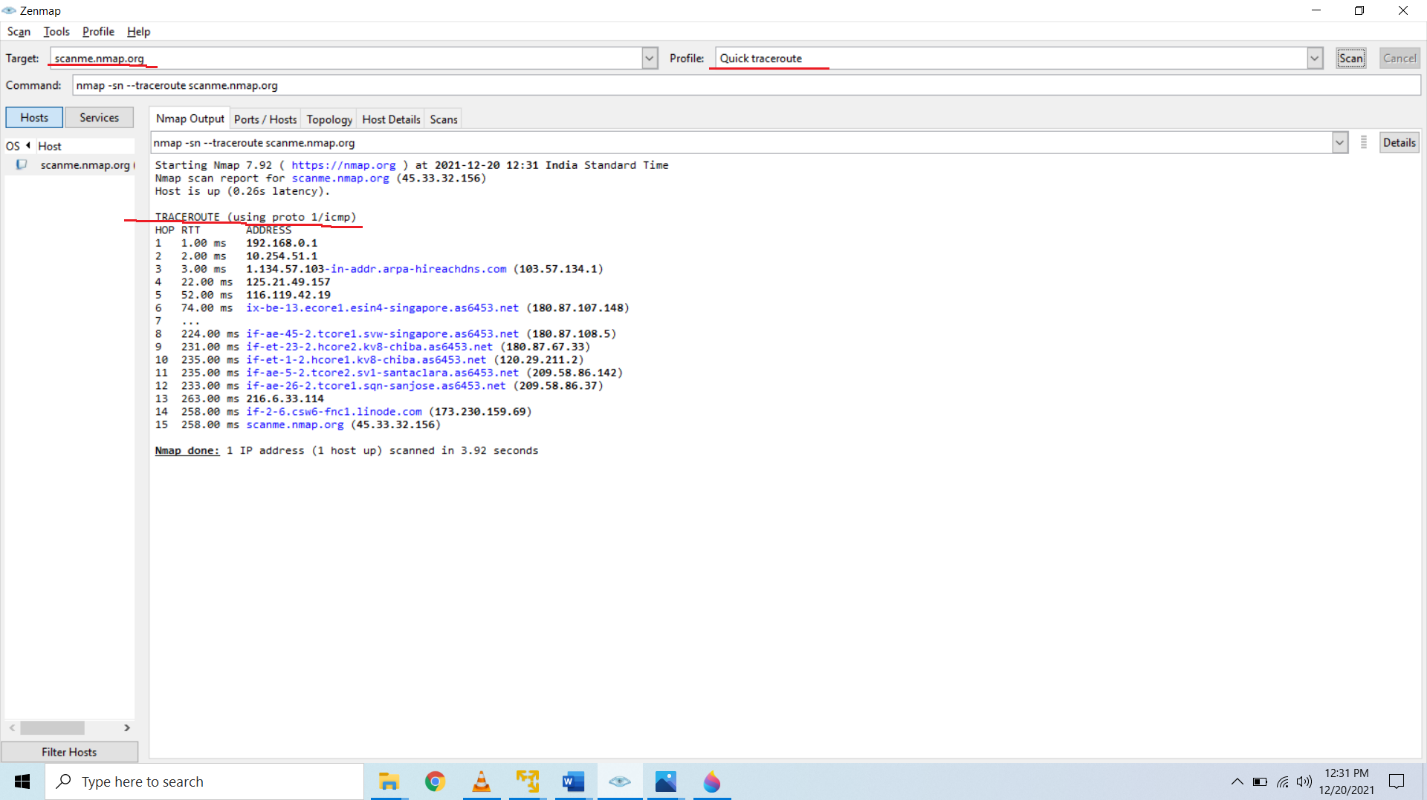
Port 25/tcp is in filtered state with smtp service.

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.

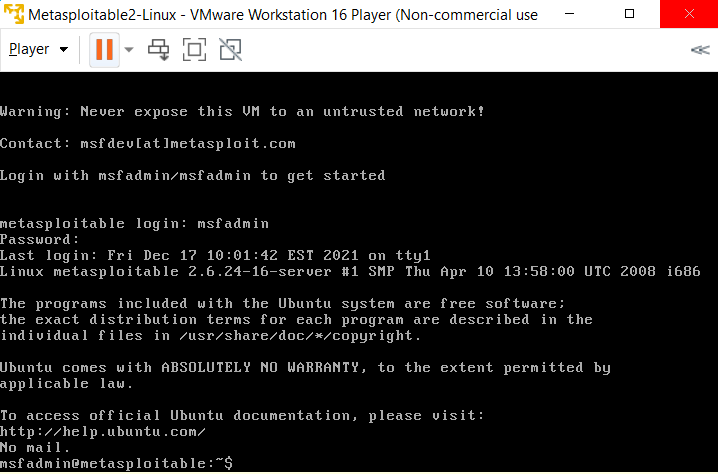


Scanning used here is regular scan. Highlights show name of the port, its state and service. The difference between quick scan and regular scan is it shows not shown tcp closed ports are 991 whereas in regular scan it shows not shown ports are 91 only.

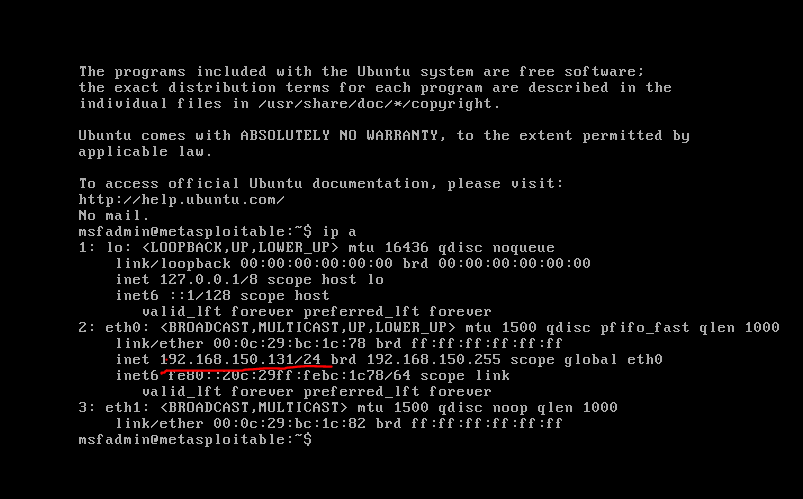


Scanning used here is quick traceroute. In this scan it did only a quick traceroute when compared to intense, quick and regular scan.

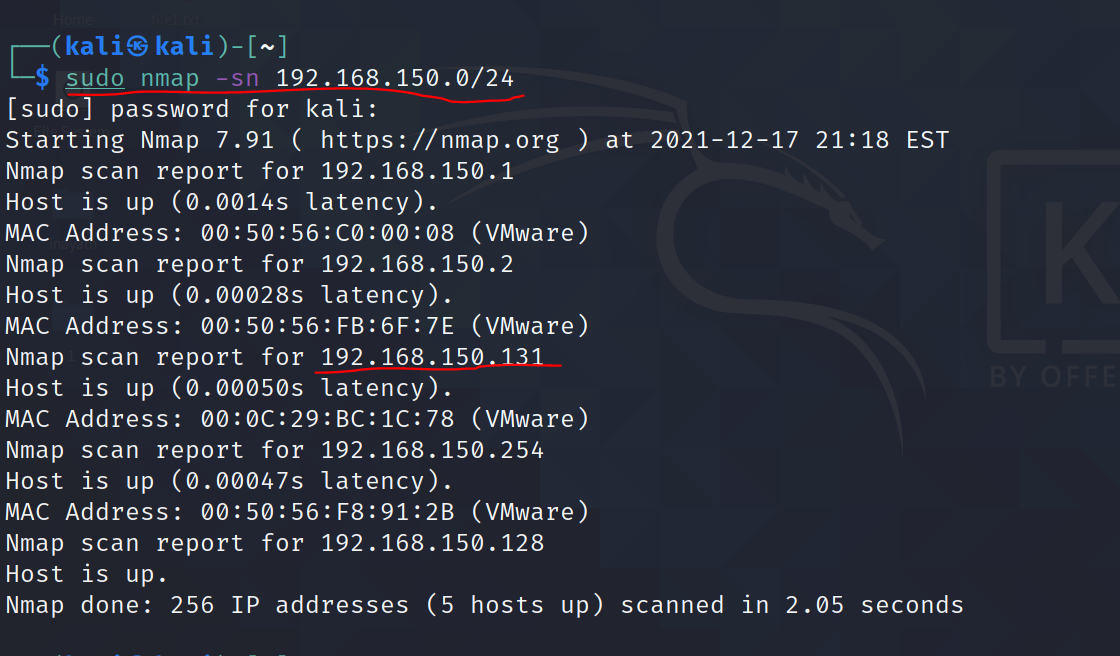
**Task 3 :** Download metasploitable 2 from Metasploitable - Browse /Metasploitable2 at SourceForge.net (If already not done) and install it in the virtual machine



**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.



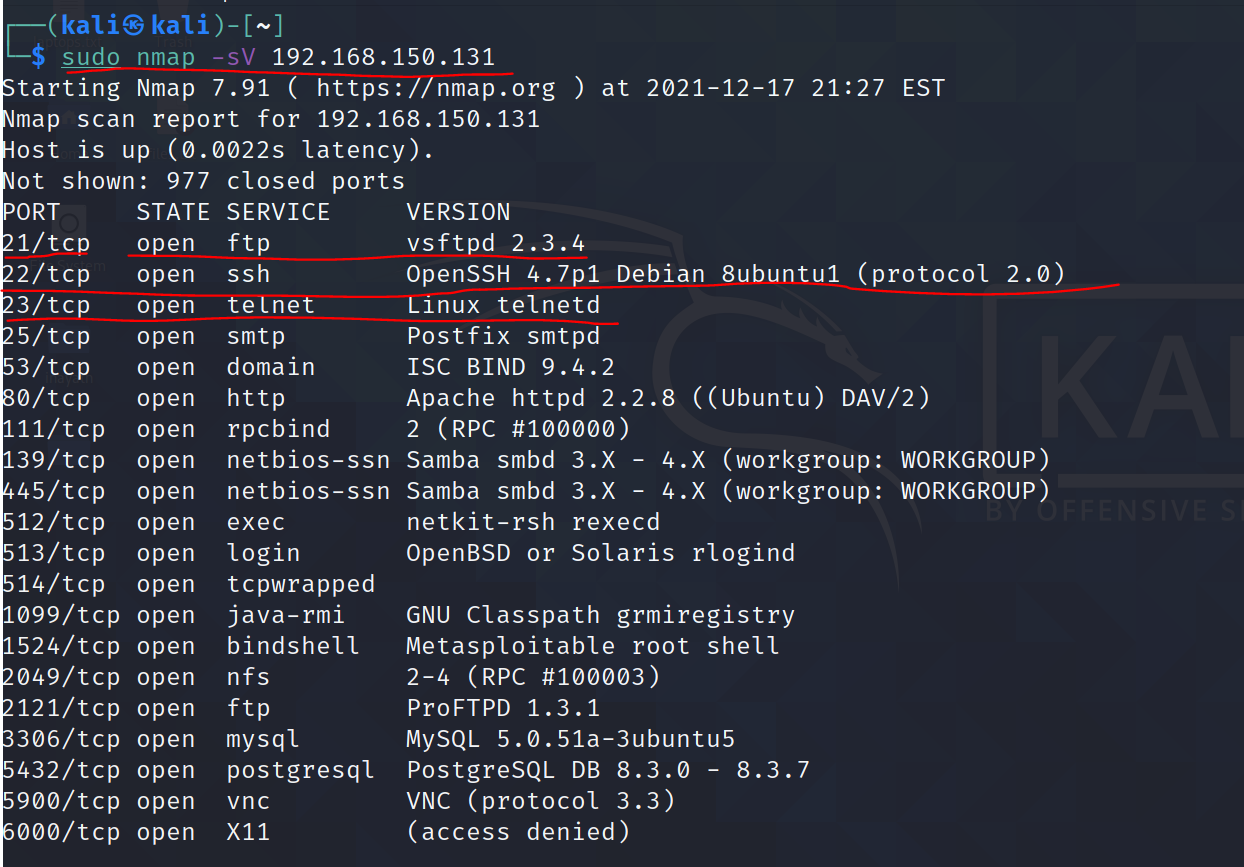
Highlights show that the IP address of my vulnerable machine is **192.168.150.131/24**

****

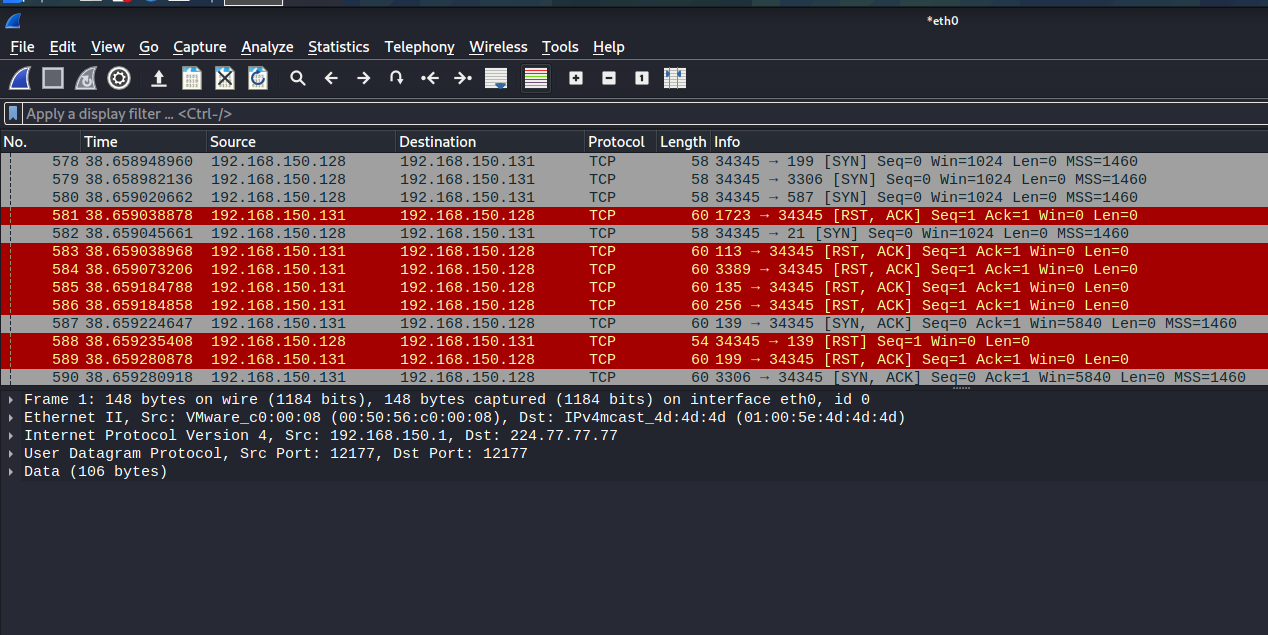
The command I have used for scanning different IP’s in this Network is **sudo nmap -sn 192.168.150.0/24**

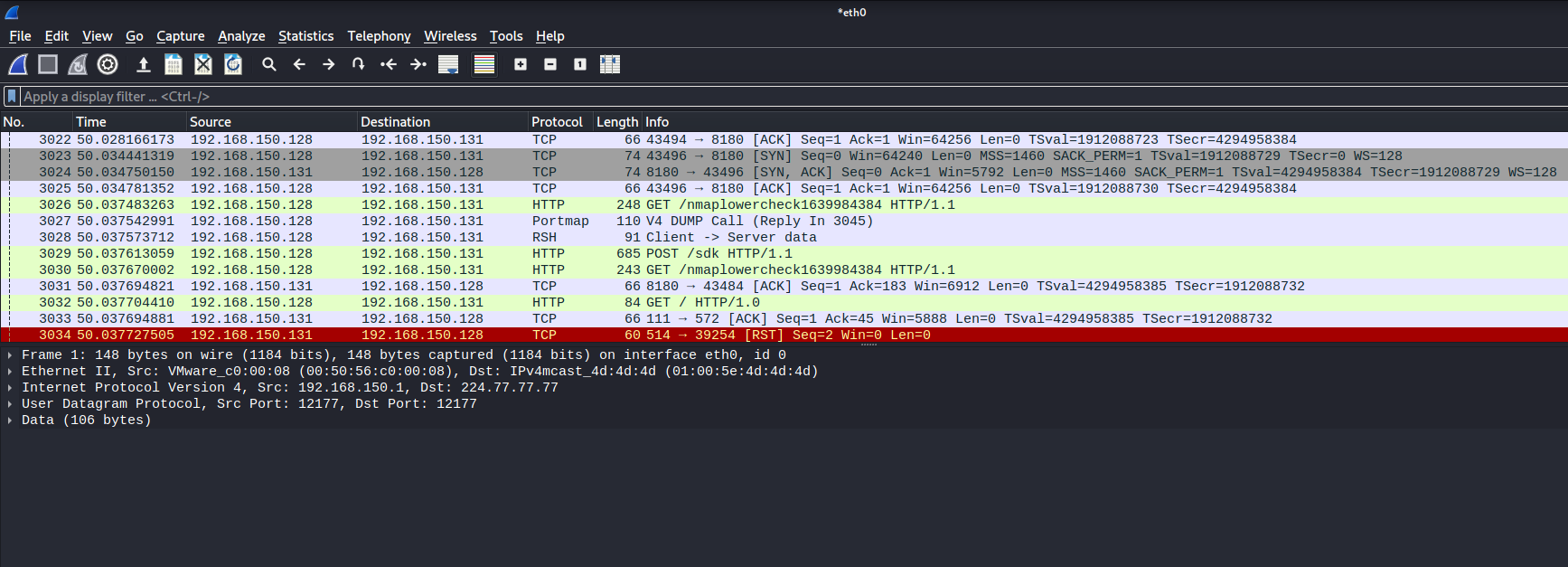


While using ping sweep, we see the packets its using is address resolution protocol (ARP) telling the network who has this particular IP inform to the system.

****

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.

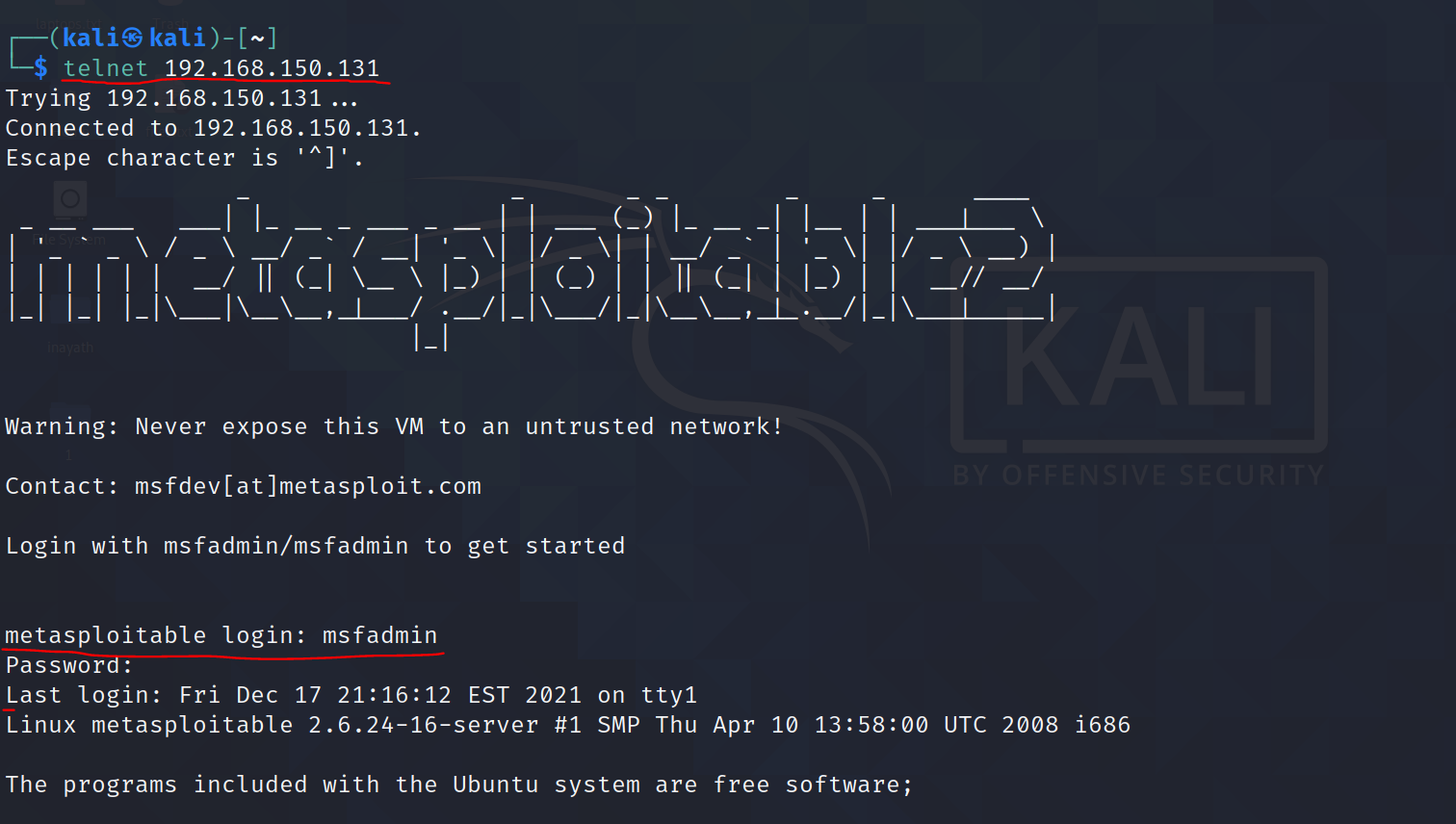


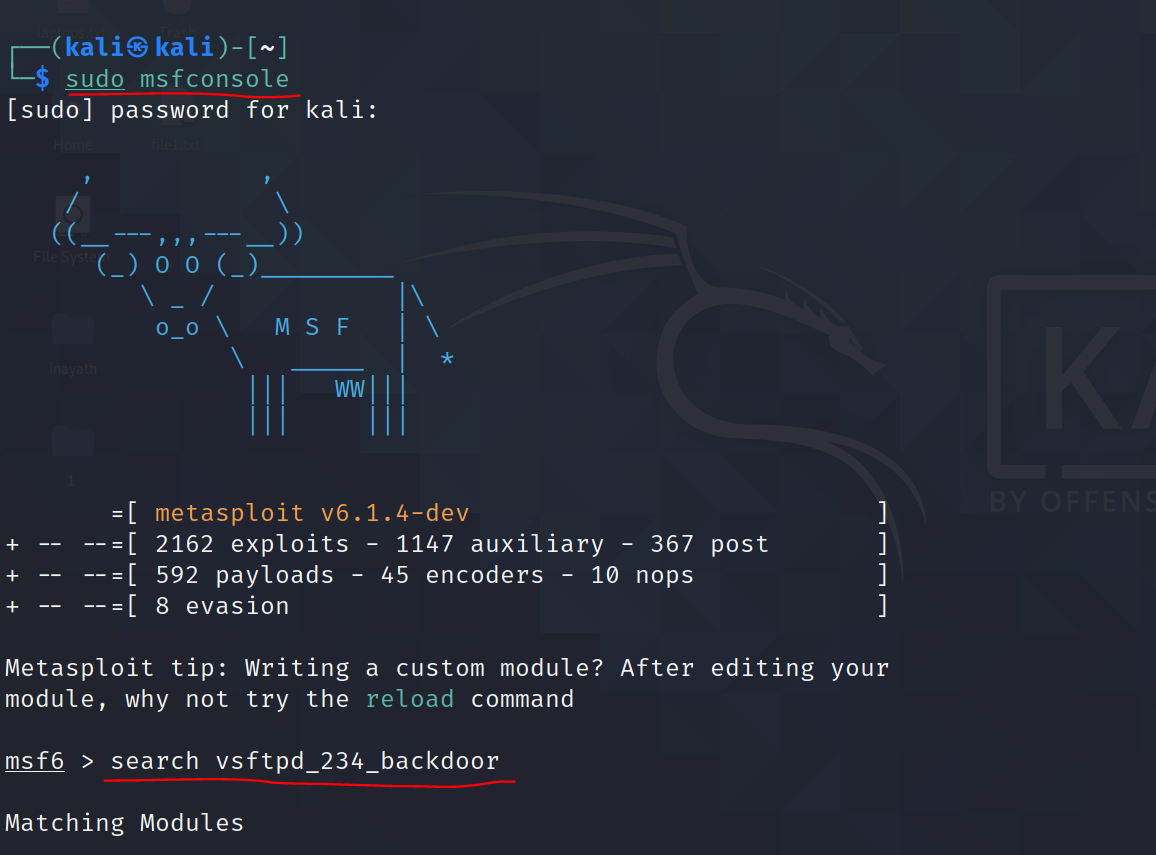


Nmap has scanned these ports.it tried to do a handshake.it had tried scanning many ports. At port nymber 84 it asked for HTTP whose version is 1.0

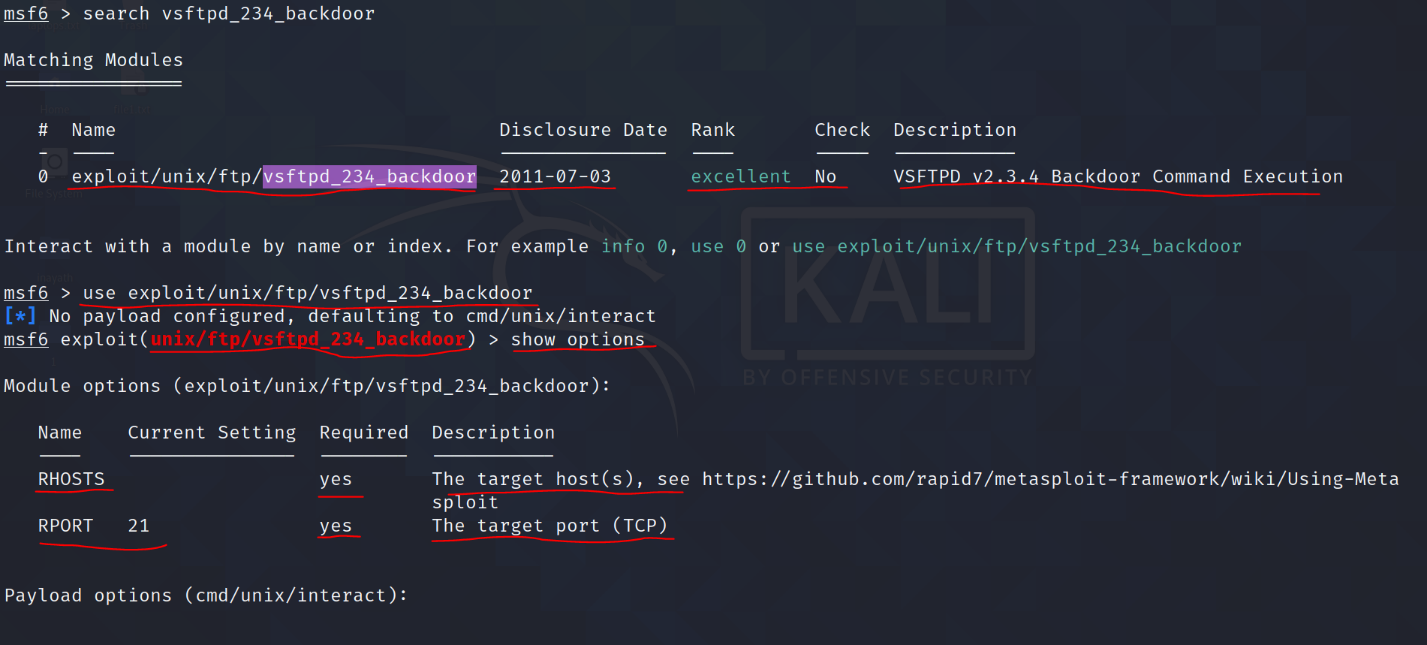
**Task 5:** Metasploitable 2 has multiple vulnerability you can exploit, You have full freedom to choice any. Pick any one vulnerable ports and Attack it. Use Metasploit framework (MSF) from msfconsole to exploit the vulnerable service.

There is a service telnet on port 23.

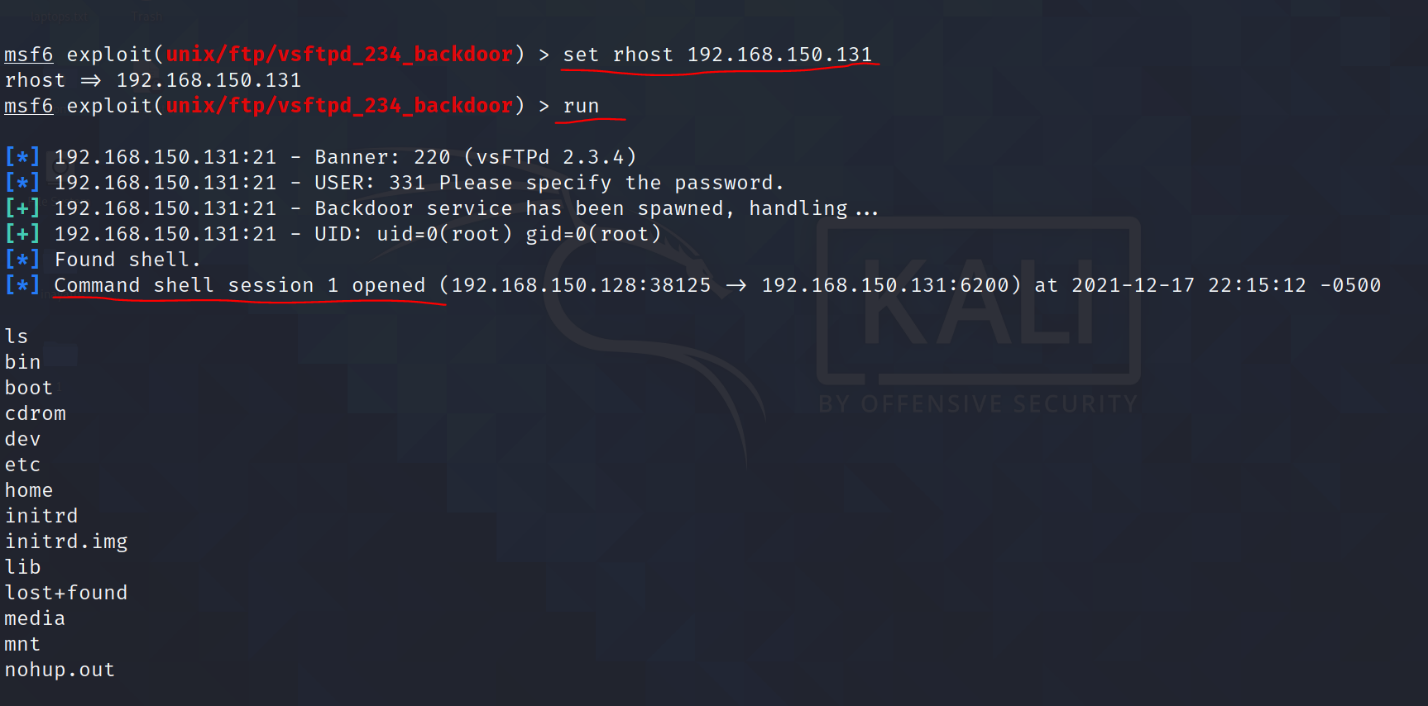


The command I have used for attacking telnet port is **telnet 192.168.150.131.**

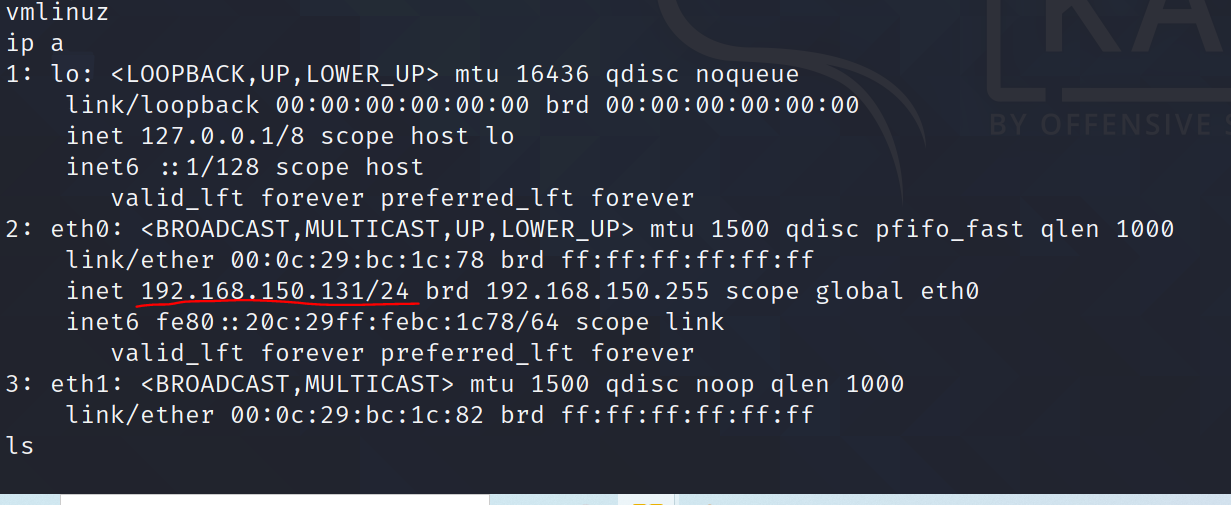
msfconsole is a metasploitable framework which comes with kali. The command I have used is **sudo msfconsole**. Choosing server ftp whose version is vsftpd 2.3.4.



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.



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



Im into target machine.



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.

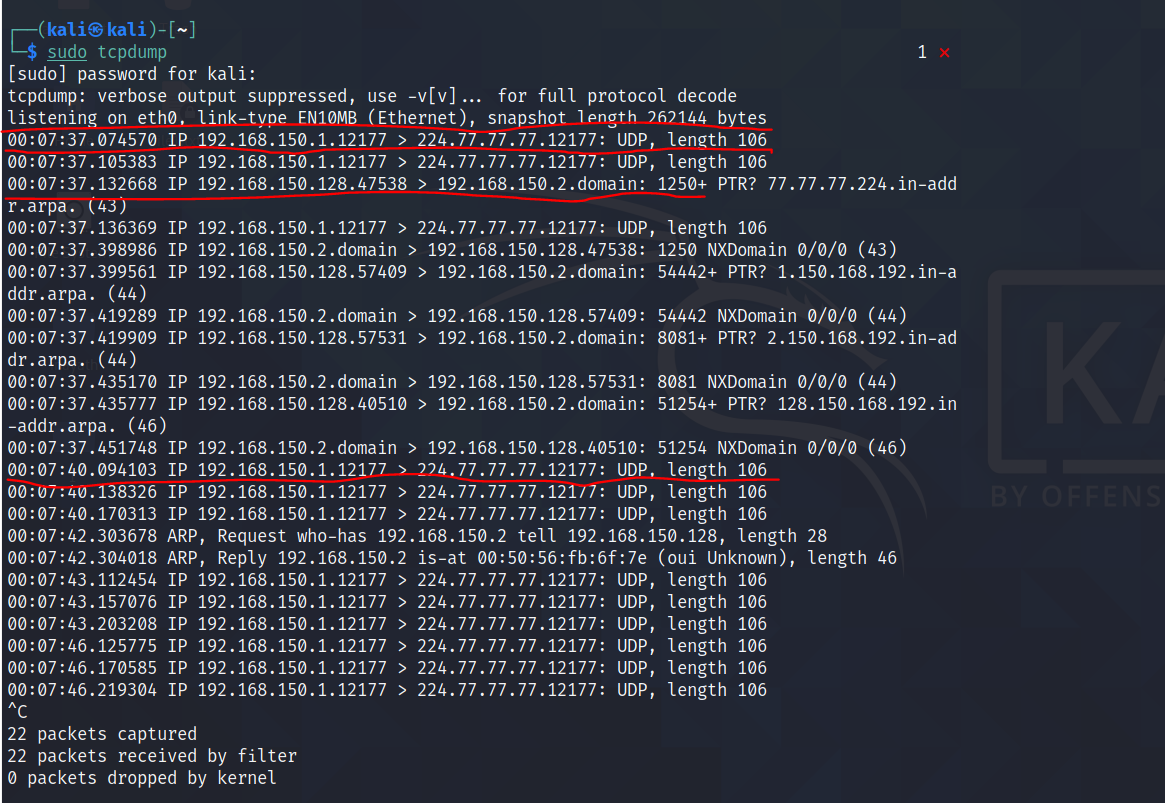
C. Vulnerable service

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.



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.