Step 0

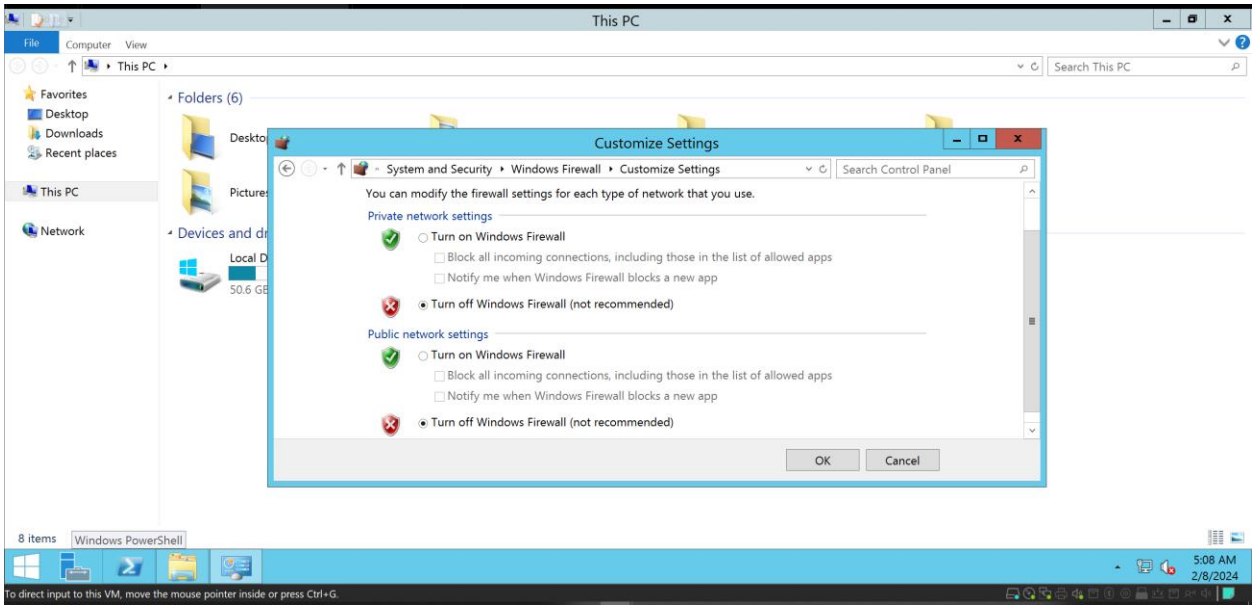
Preparation

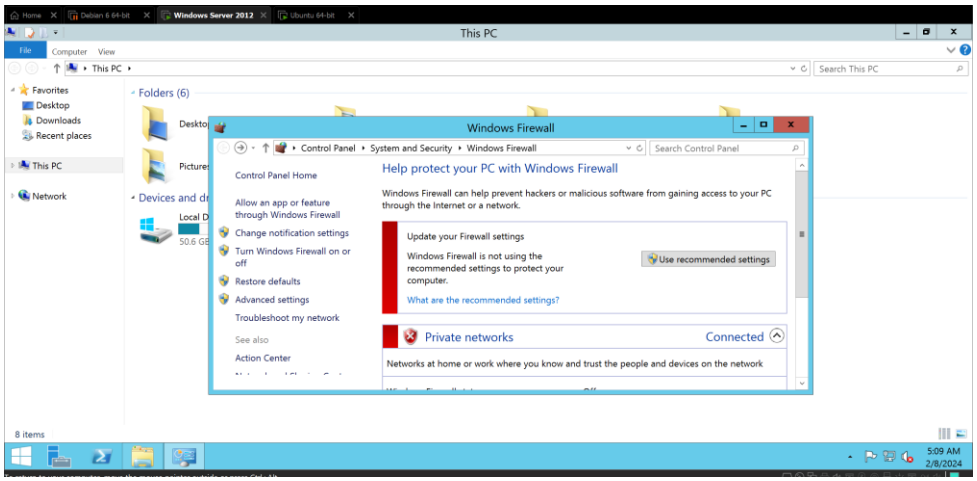
For this lab We need

1- Kali machine
2- Ubuntu Machine
3- Windows Server
4- Metasploitable 2

Making sure all machines are up and running we will first disable the antivirus of Windows server.

- Select Start > Control Panel > System and Security > Windows Firewall. ...
- Select Turn Windows Firewall on or off.
- Select Turn off Windows Firewall (not recommended) for both Home or work (private) network location settings and Public network location settings, and then click OK.

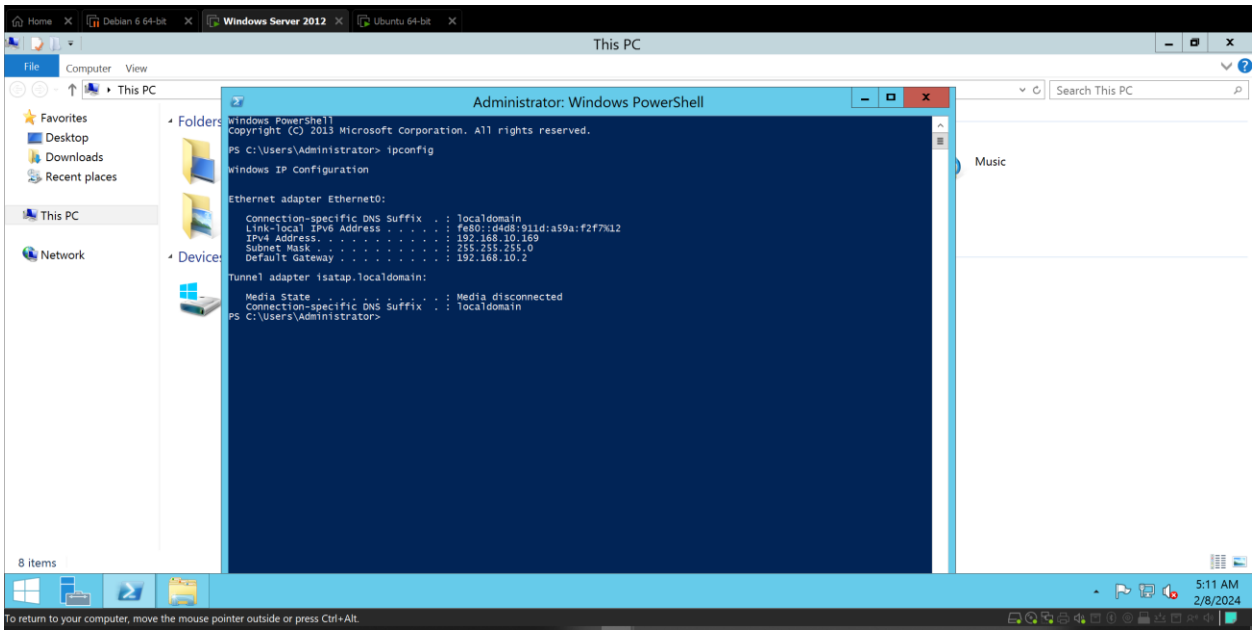




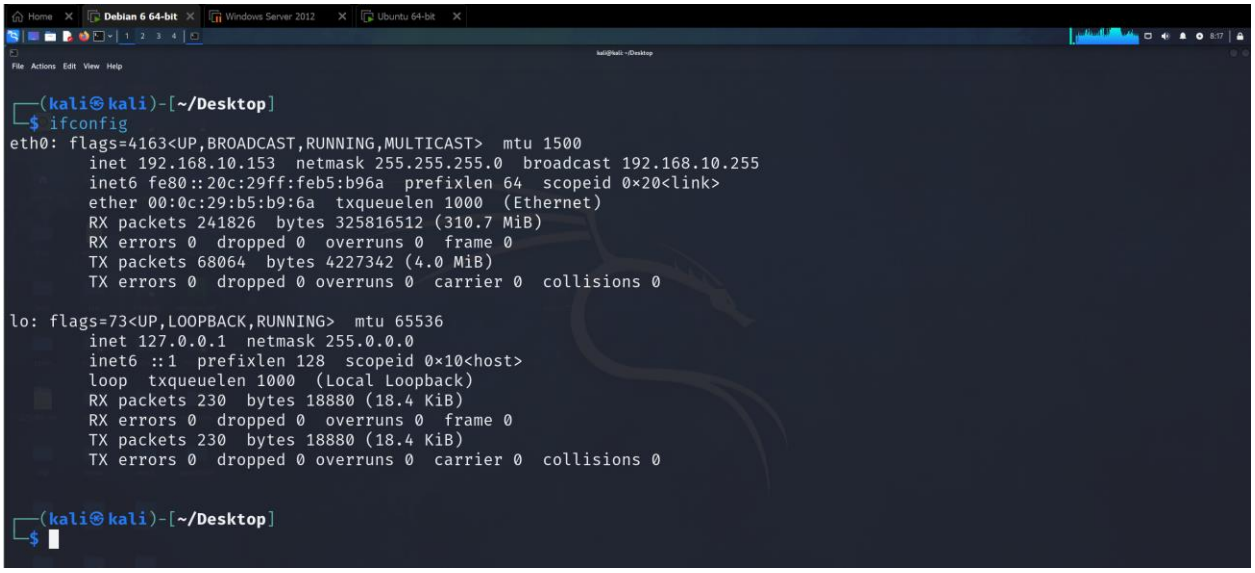
Step 1

We will first make sure that Metasploitable 2 is running and has IP address on the same network. Login to system and ifconfig to see the ip.

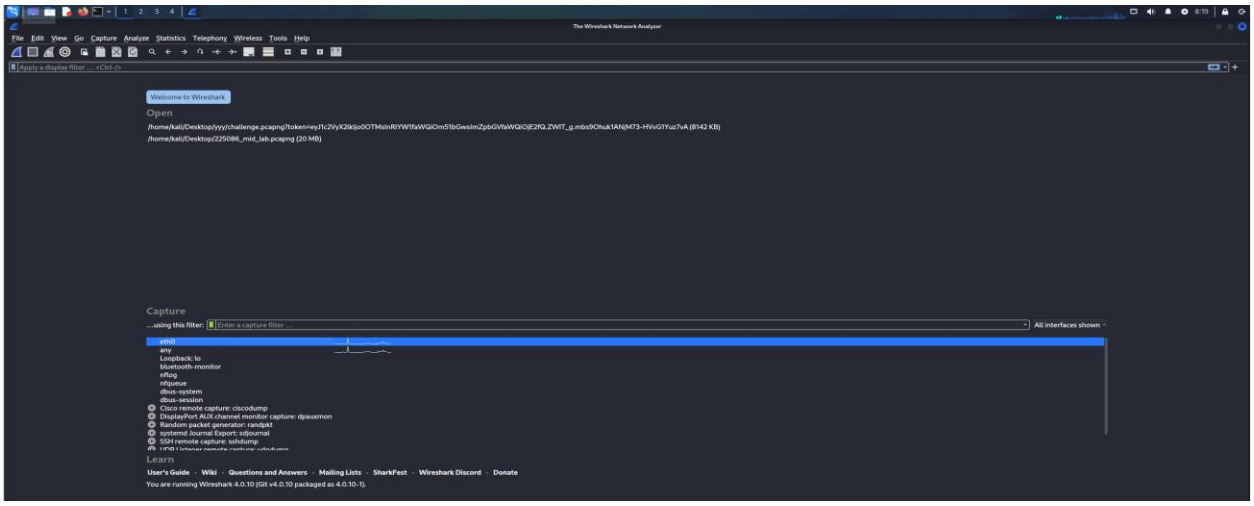
Same case with the Windows server

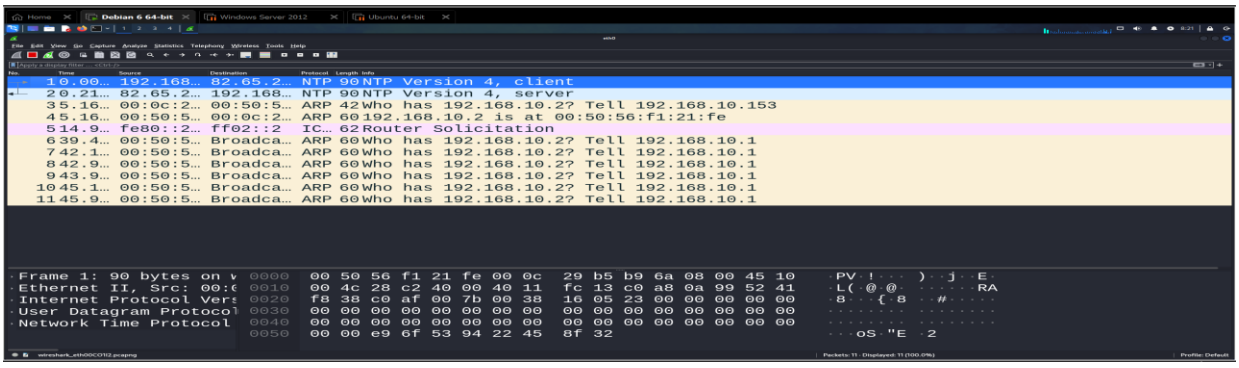


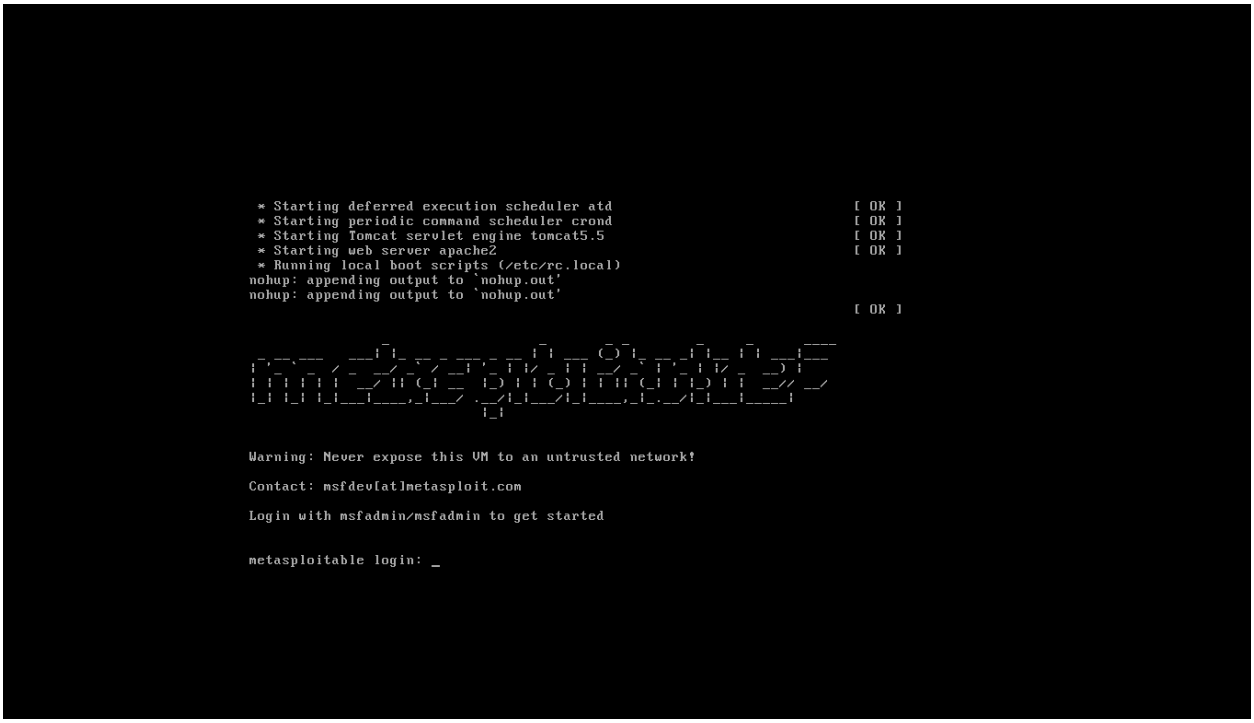
The Same goes with the Kali Machine.



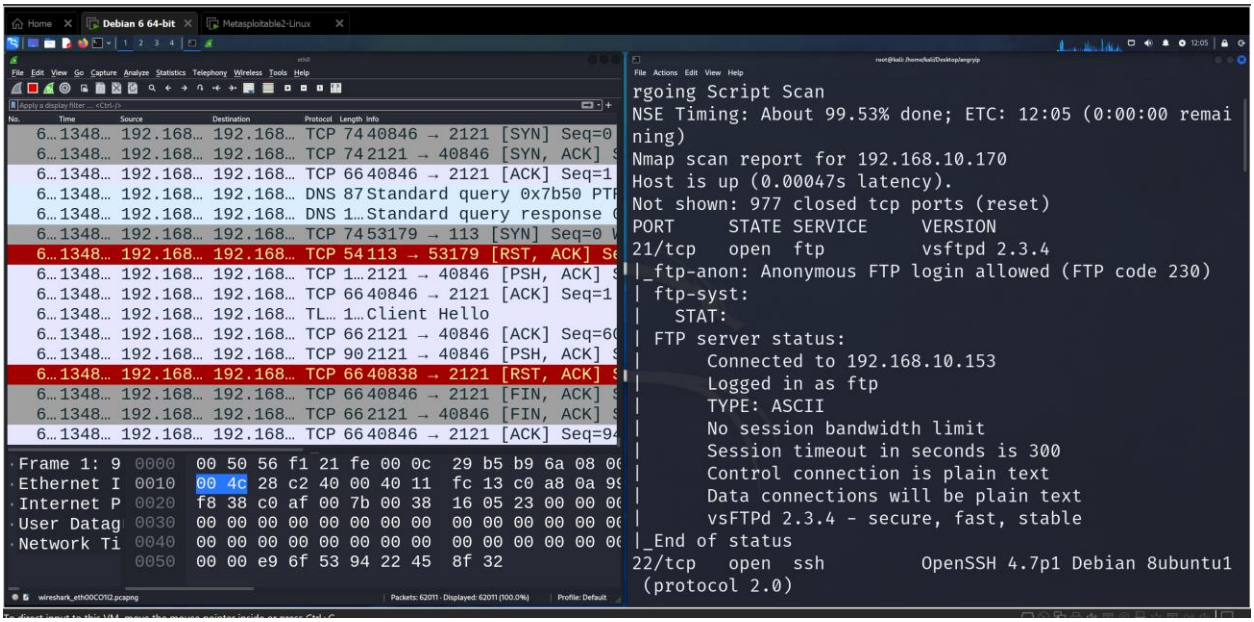
Then we will open the Wireshark and eavesdrop on eth0 network card





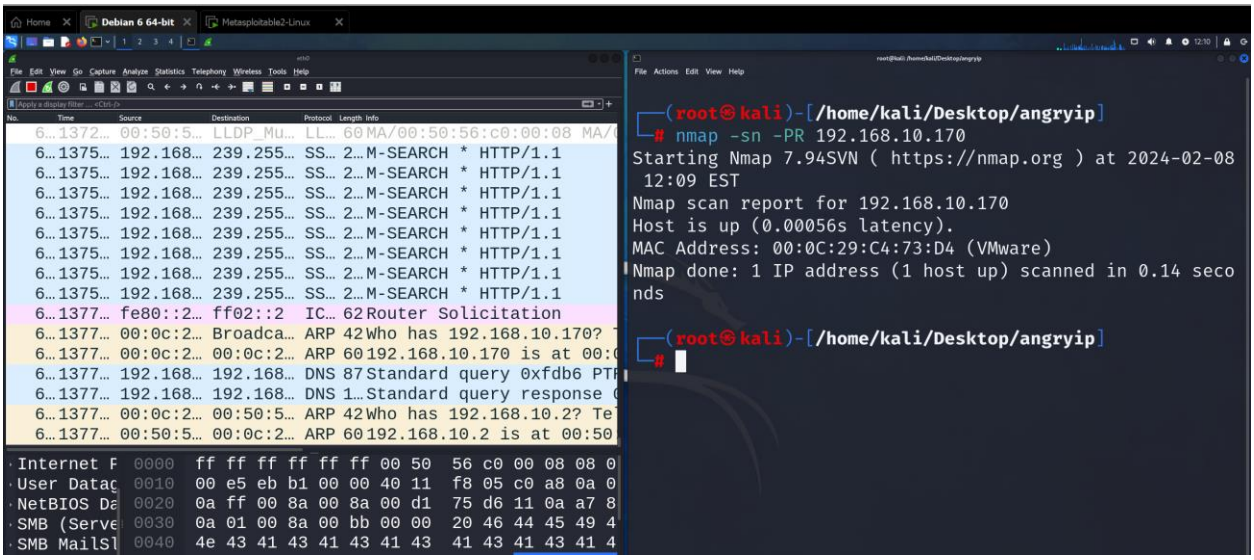


IP 192.168.10.170



Now Now let’s do the ARP scan with nmap on Metasploitable 2 (page 5)

$Nmap –sn –PR



On the Left side we can see the moment of ARP packets the target reply means it is connected.

Step 2

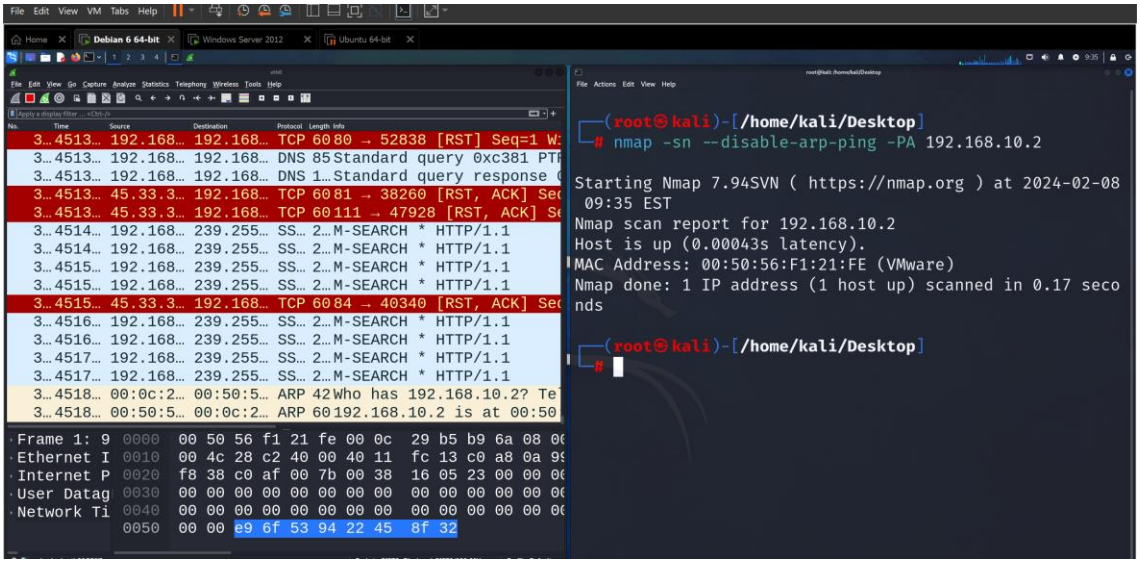
Let’s perform ICMP Echo scan using nmap

Command : nmap –sn –PE –disable-arp-ping <Metasploitable ip>

We notice on the left in Wireshark the traffic of ICMP Timestamp packets, the target ICMP Timestamp reply means it is connected.

TCP ACK Scan using nmap

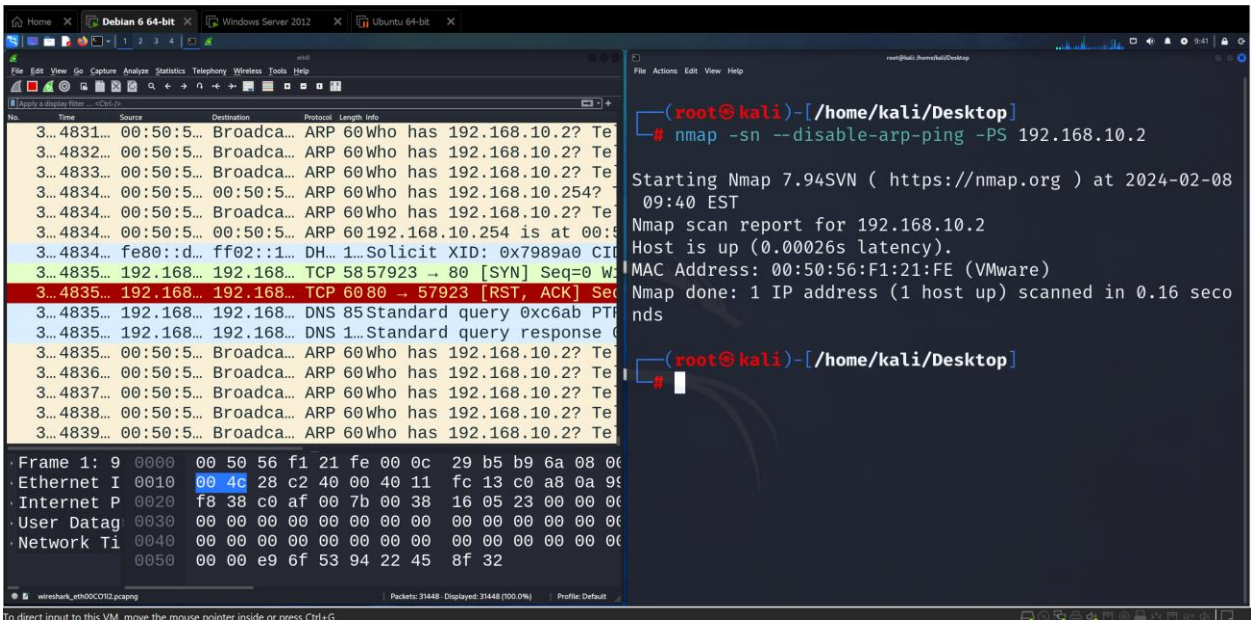
Command: nmap –sn –disable-arp-ping –PA 192.168.10.2



We notice on the left in Wireshark the movement of TCP ACK packets towards target to port 80. The target's TCP RST response means that is connected.

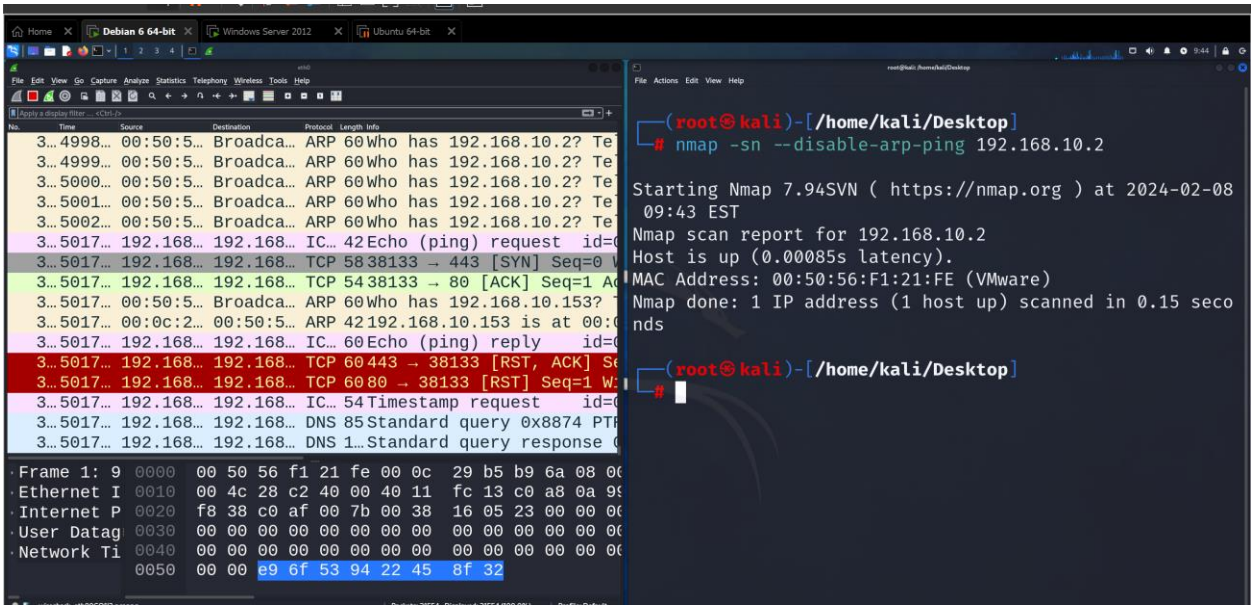
TCP SYN Scan using nmap

Command: nmap –sn –disable-arp-ping –PS 192.168.10.2



ICMP Echo sweep using nmap:

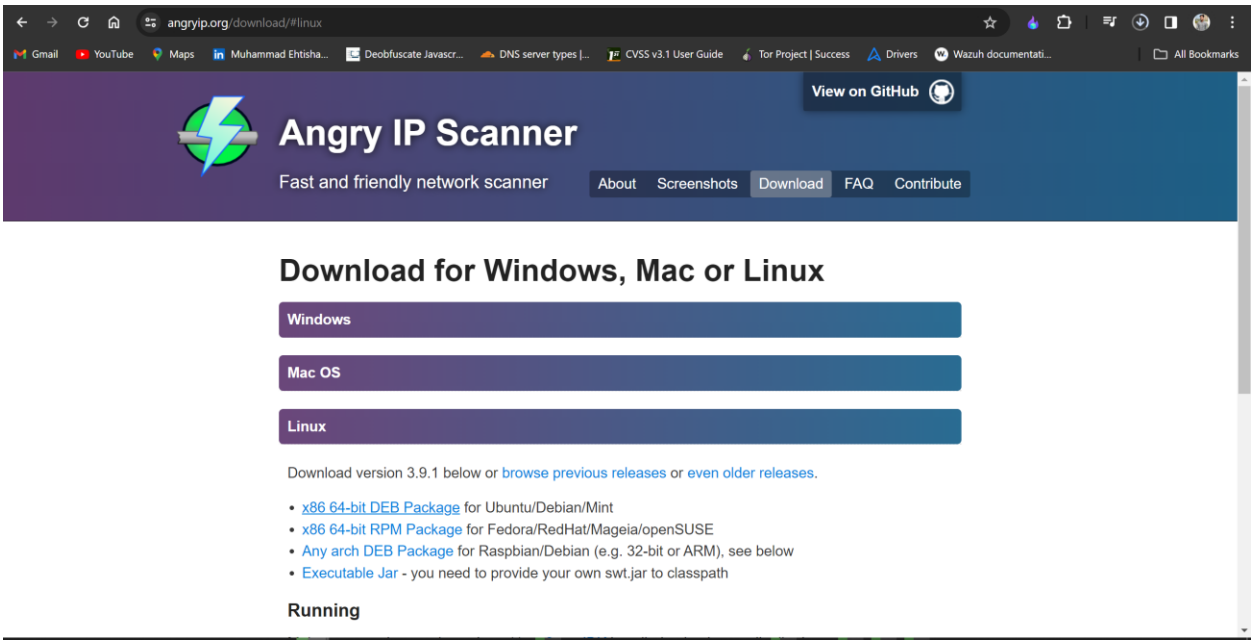
Command: nmap –sn –disable-arp-ping 192.168.10.2



Scan using Angry IP scanner:

First verify that all system is working and all are on same network we open angry scanner interface.

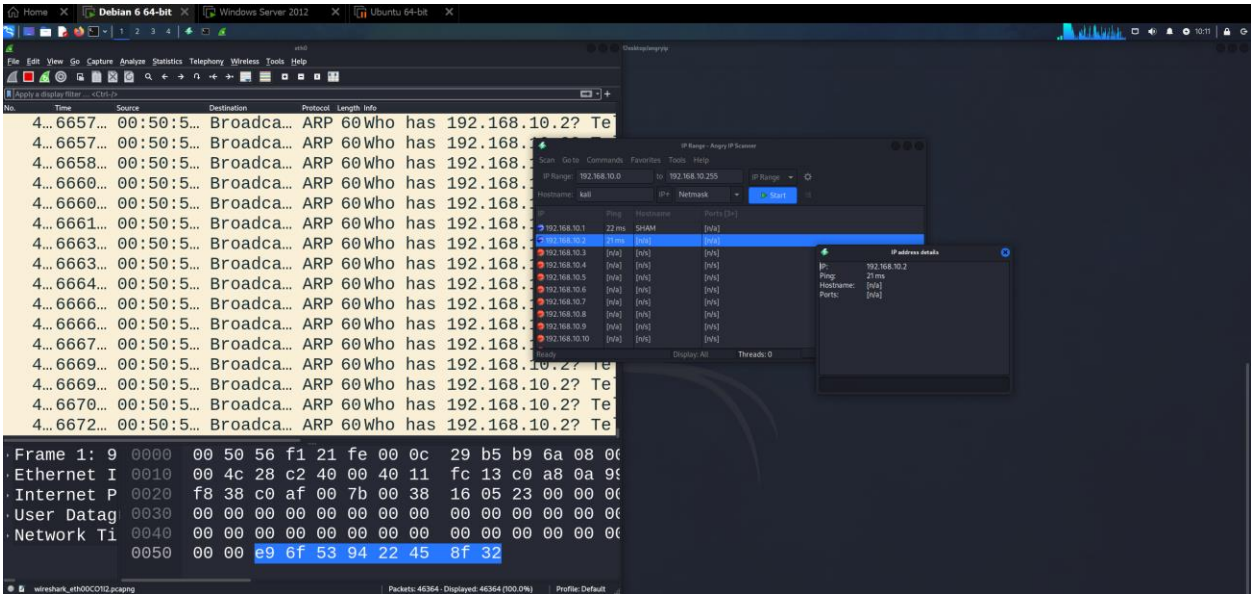
First download ipscan from official site.



Using wget tool to download

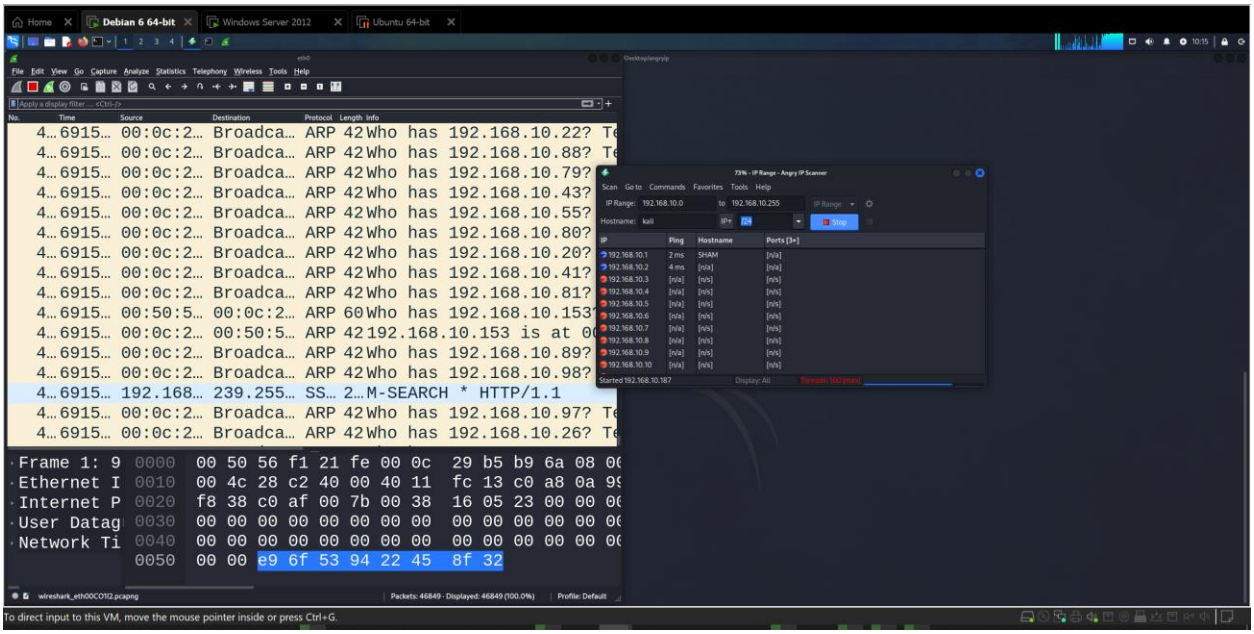
After downloading use dpkg –i ad the .deb file to install

After installing it will open.

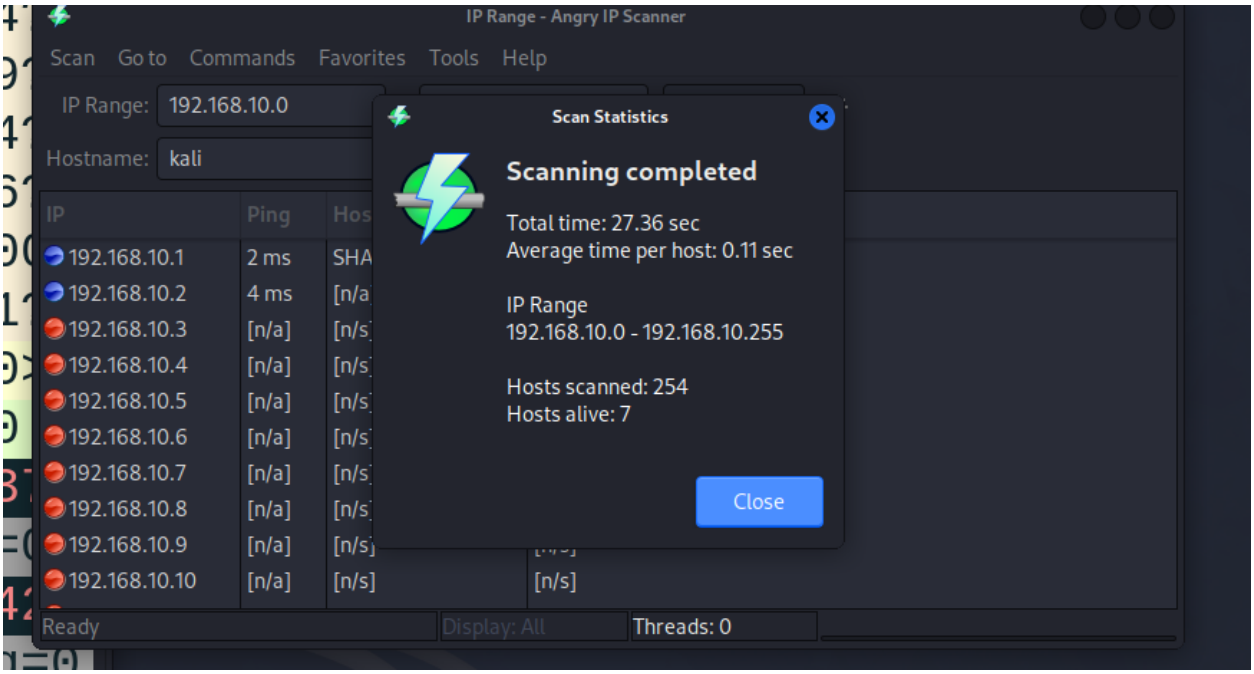


Make sure that alive host is selected which is kali.

Select the range and press start

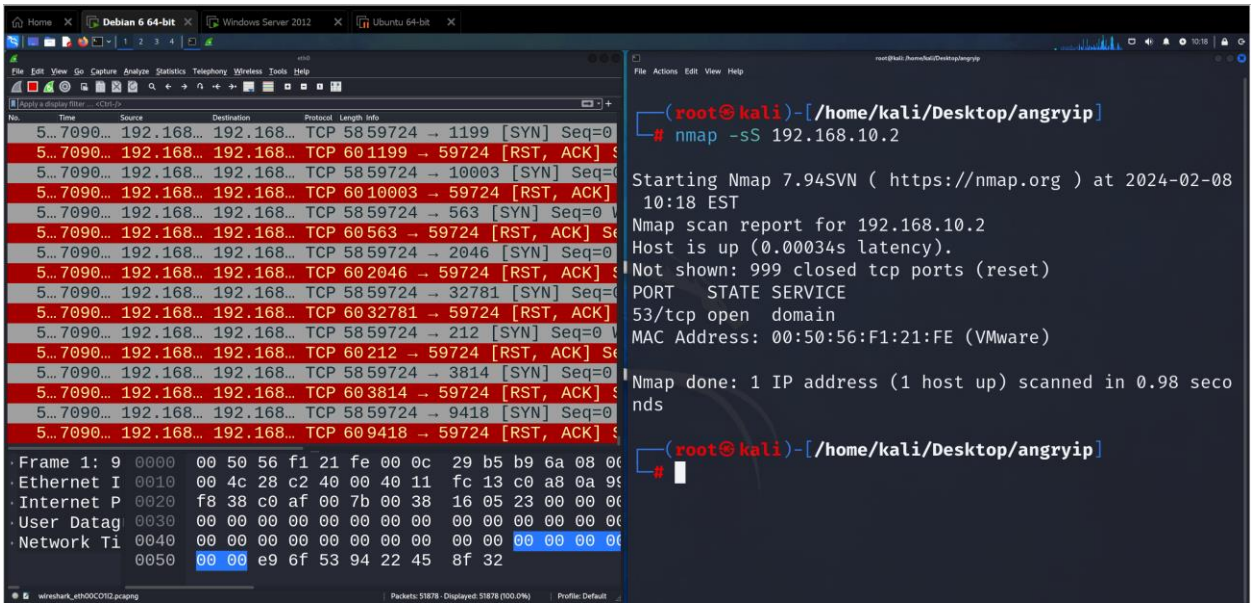


And the Result:



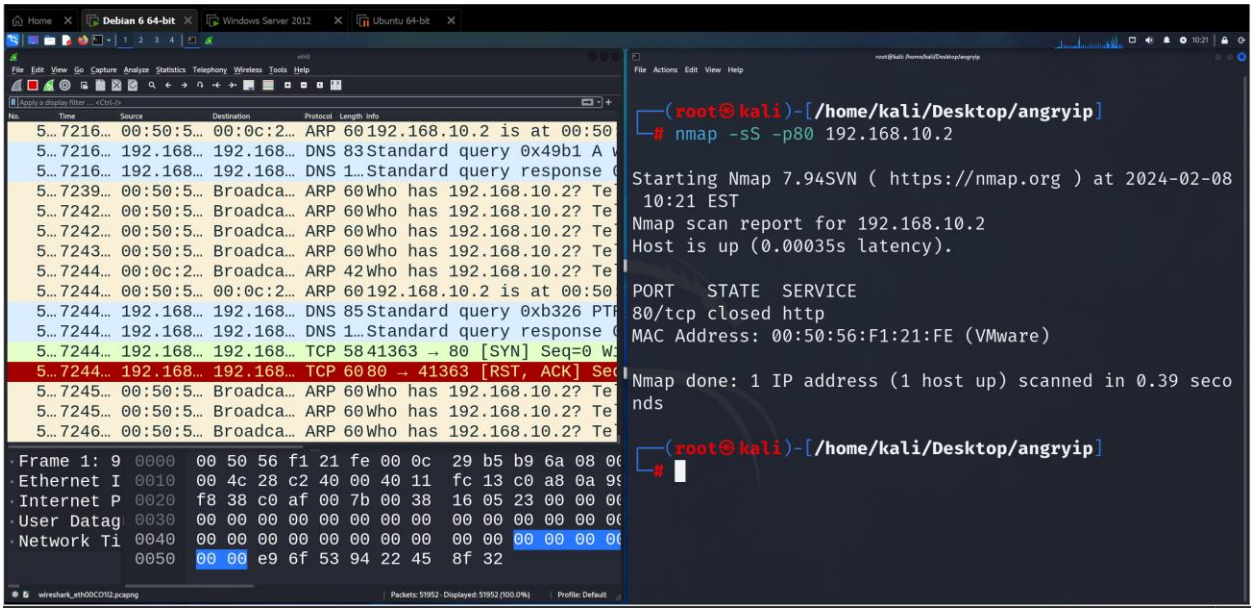
TCP Stealth Scan

Command: nmap –sS 192.168.10.2



Open port can be specified instead of famous 1000 as follow:

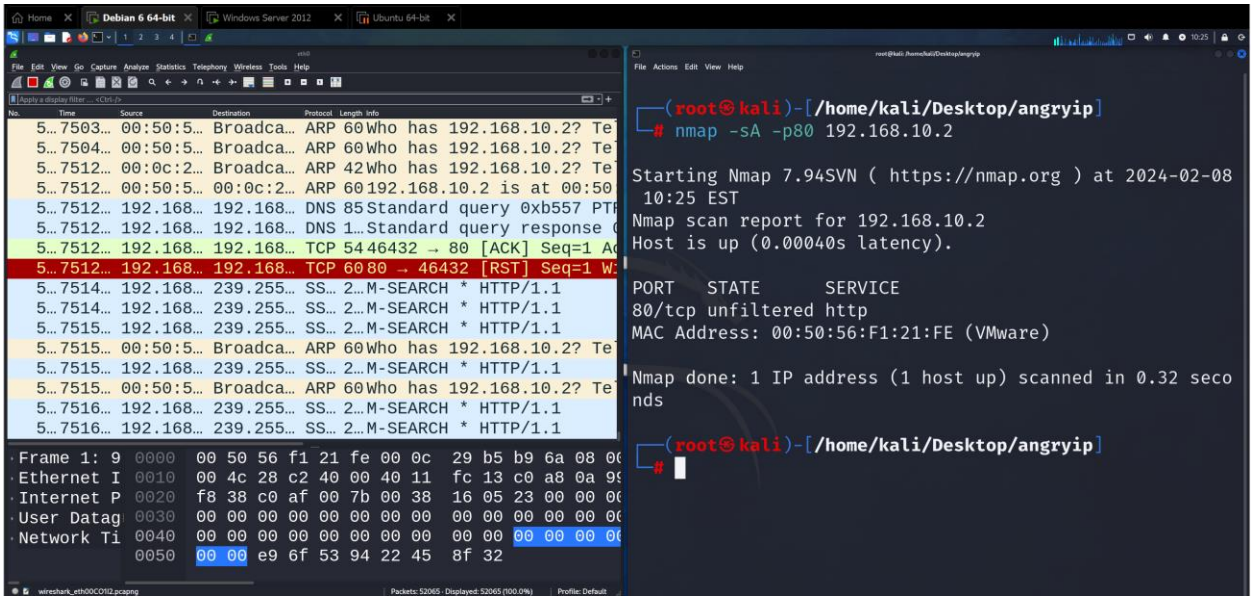
Command: nmap –sS –p80 192.168.10.2 http



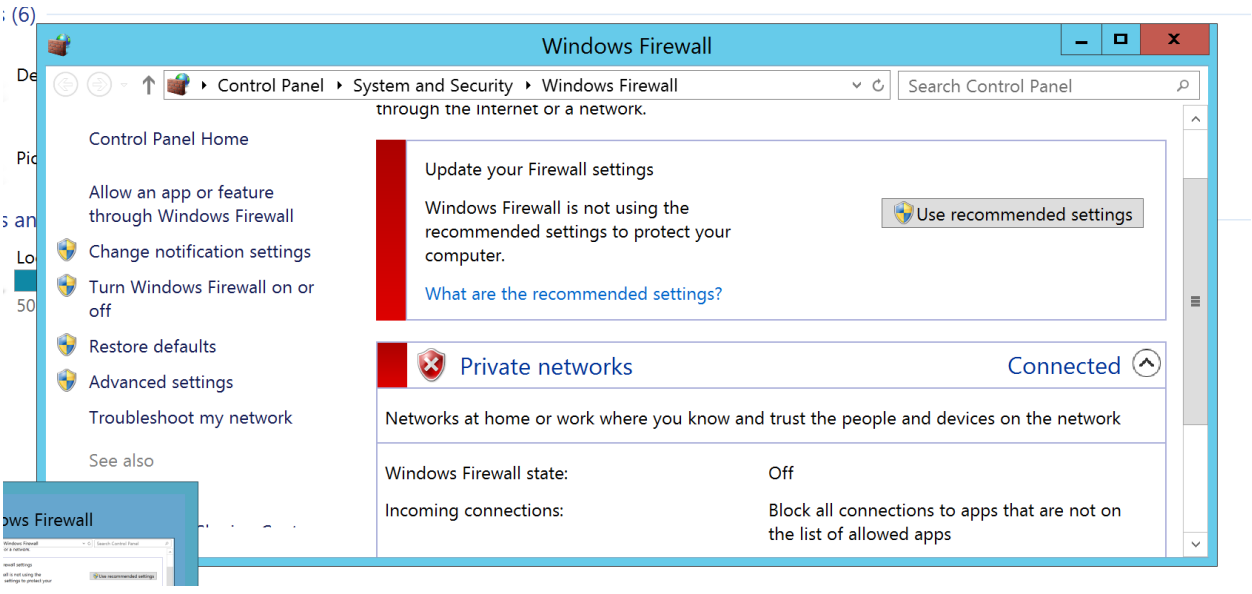
Nmap sends TCP FIN PSH URG packets to the port to be tested. The target responds with TCP RST if the port is closed, and does not respond if the port is open. Nmap consider the port as open | filtered because a firewall can block reply packet is the port is closed.

TCP Ack Probe scan:

Nmap –sA –p80 192.168.10.2

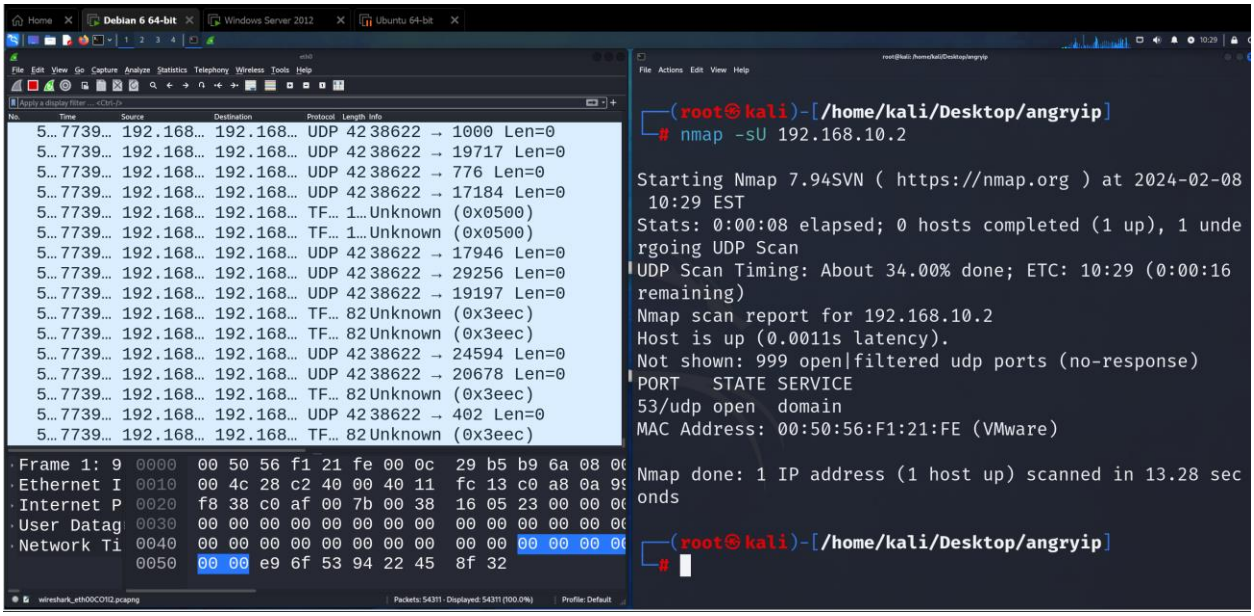


Let’s try without a firewall:



UDP Scan:

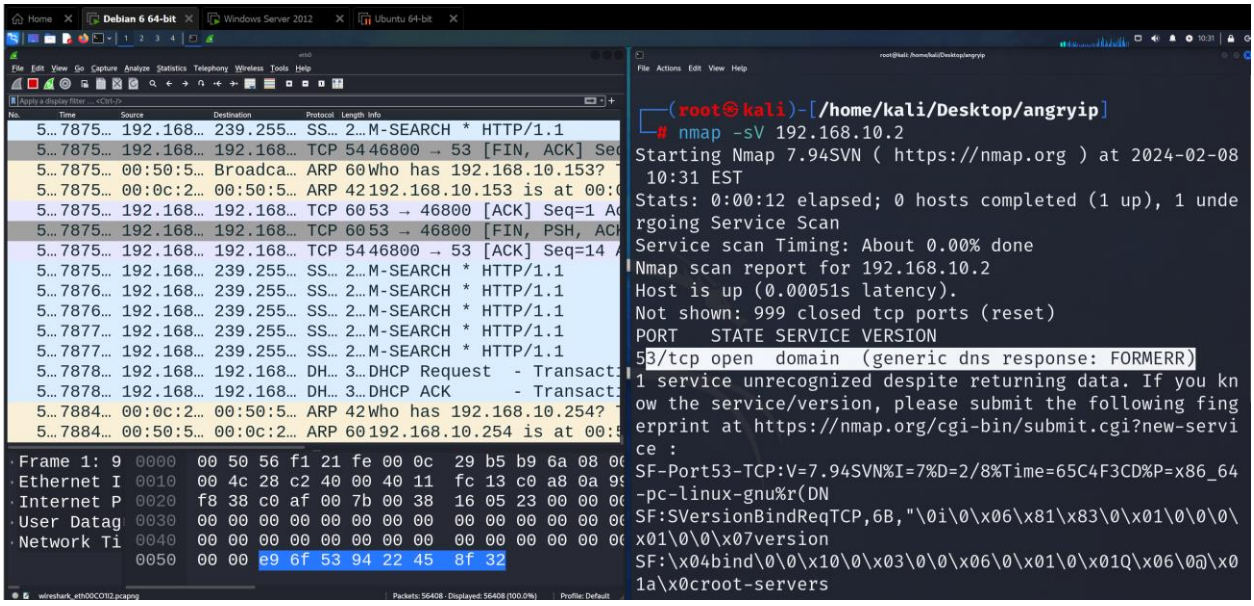
nmap –sU 192.168.10.2



Step 3

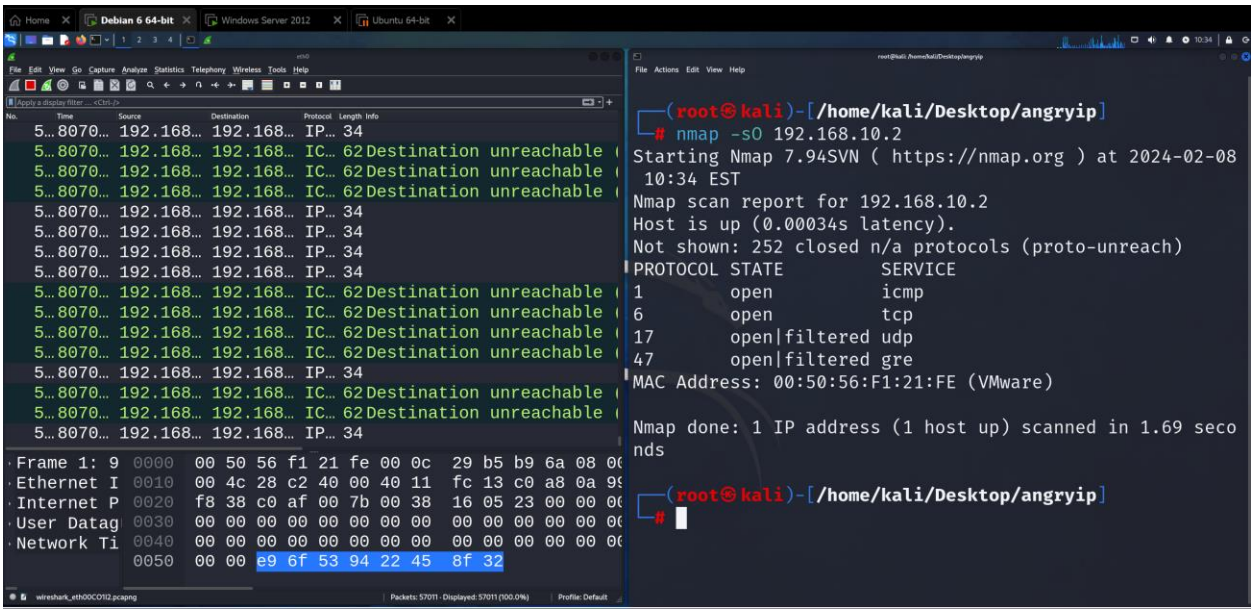
Service Version Discovery

Command: nmap –sV 192.168.10.2



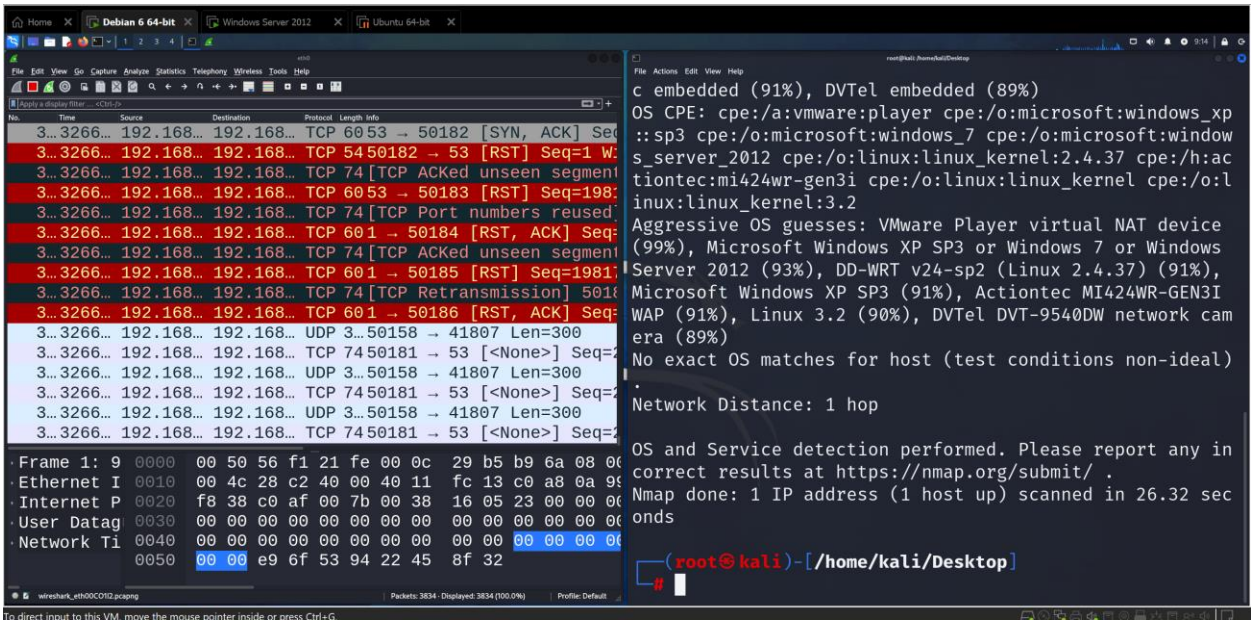
Operating System Discovery

Command: nmap –sO 192.168.10.2



Discover Nmap scan to detect Operating system type, but it's not 100% correct

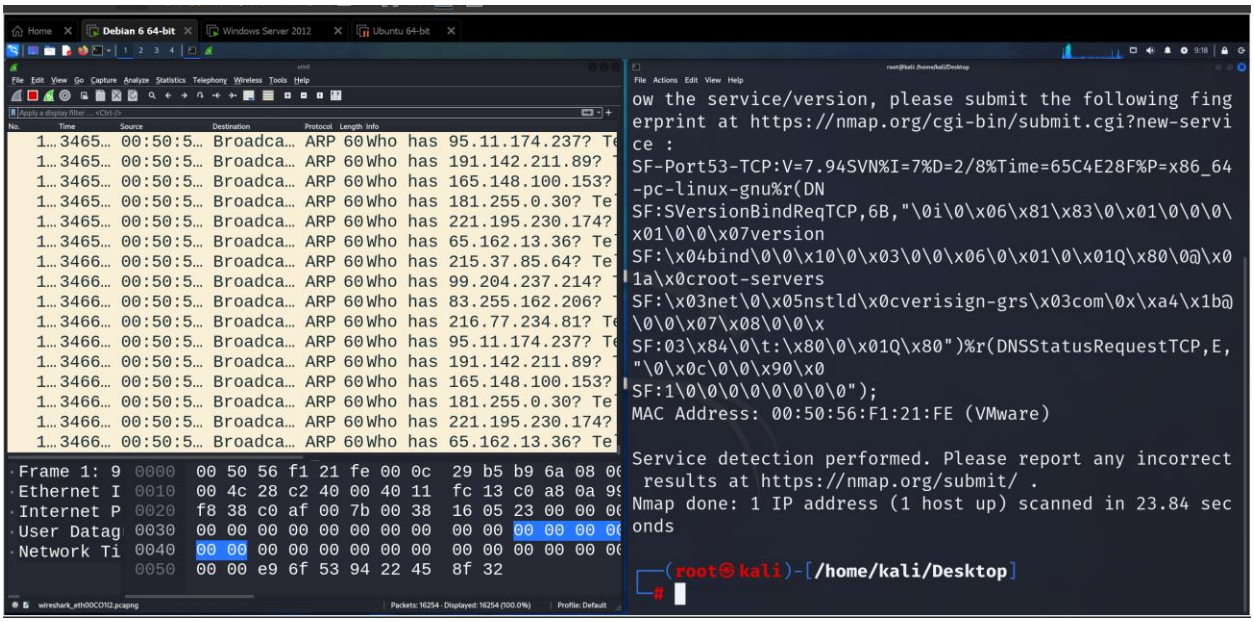
Command nmap –sV -O 192.168.10.2



Scan operation decoy

Nmap can be used to camouflage the scanning process, nmap spoofs the set of all IPS can send the scanning packets from them

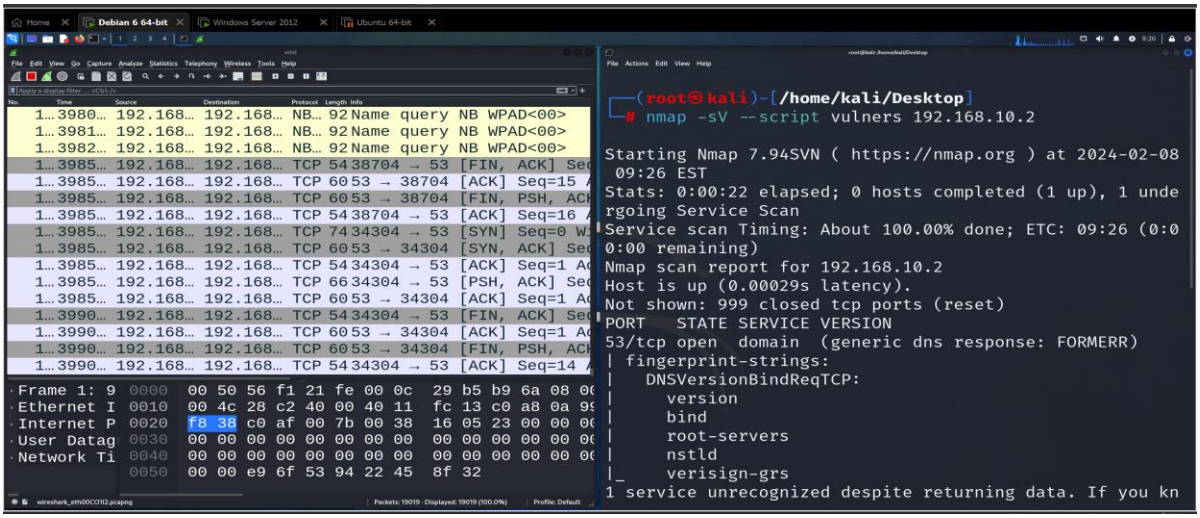
Command: nmap –D RND:10 –sV 192.168.10.2



Nmap for vulnerability scanning

Nmap script engine can be used to find the vulnerability by matching the software versions of the software behind the ports this feature required internet on Linux

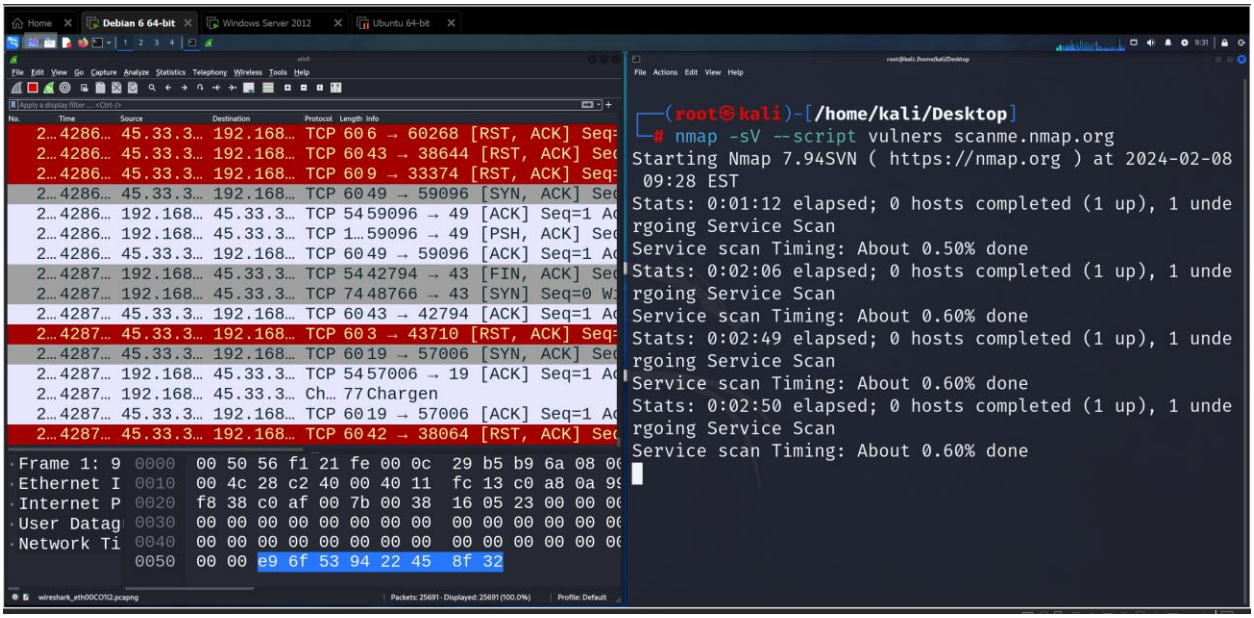
Command**: nmap –sV –script vulners 192.168.10.2**



Exercise:

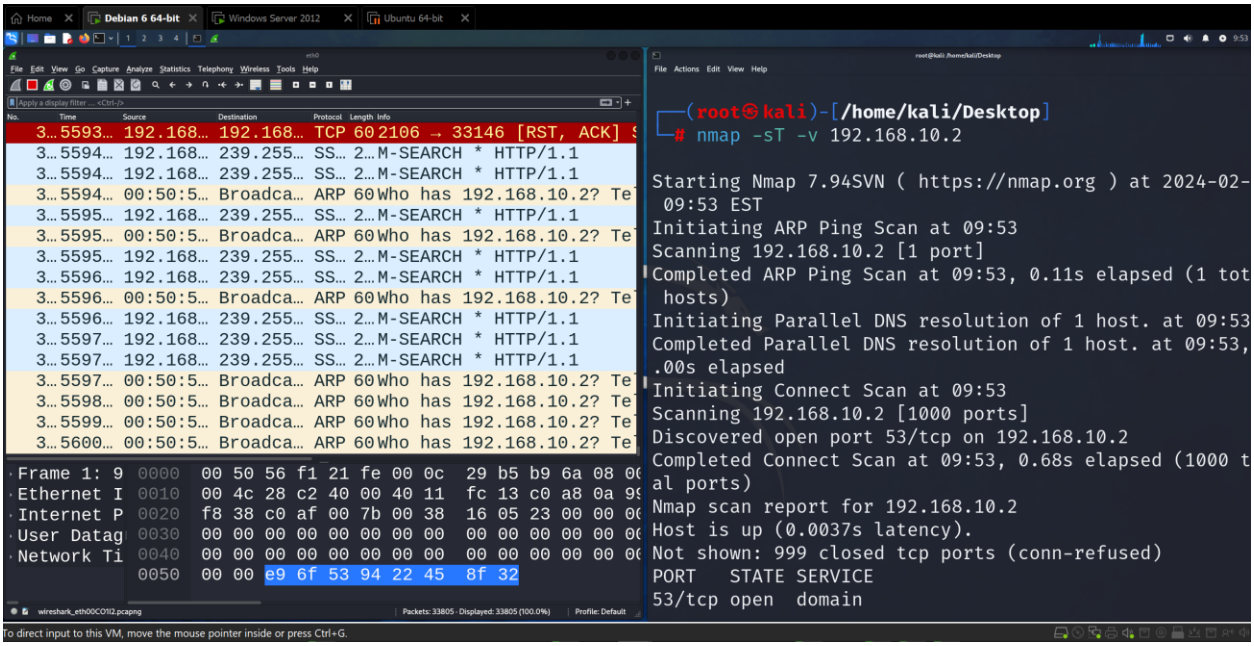
Scan the scanme.nmap.org and find any vulnerabilities.

Command: nmap -sV --script vulners scanme.nmap.org



TCP Connect scan:

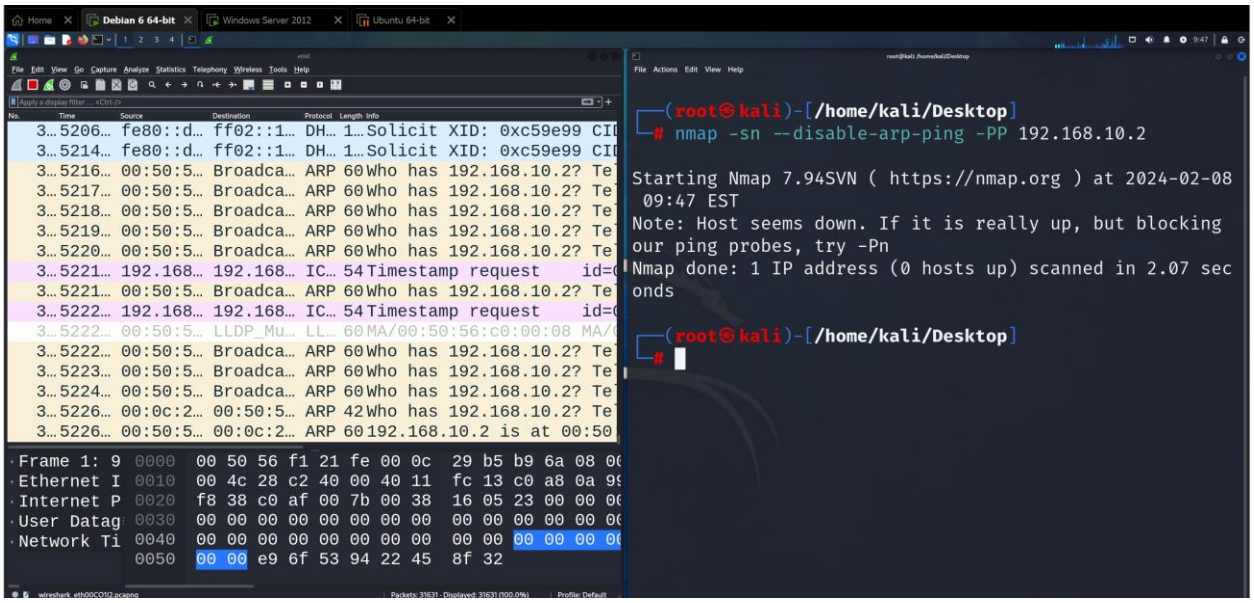
nmap –sT –v 192.168.10.2



We see on the left the Wireshark the movement of ICMP Echo packets towards address 192.168.10.132 to 192.168.10.2 which is the victim machine.

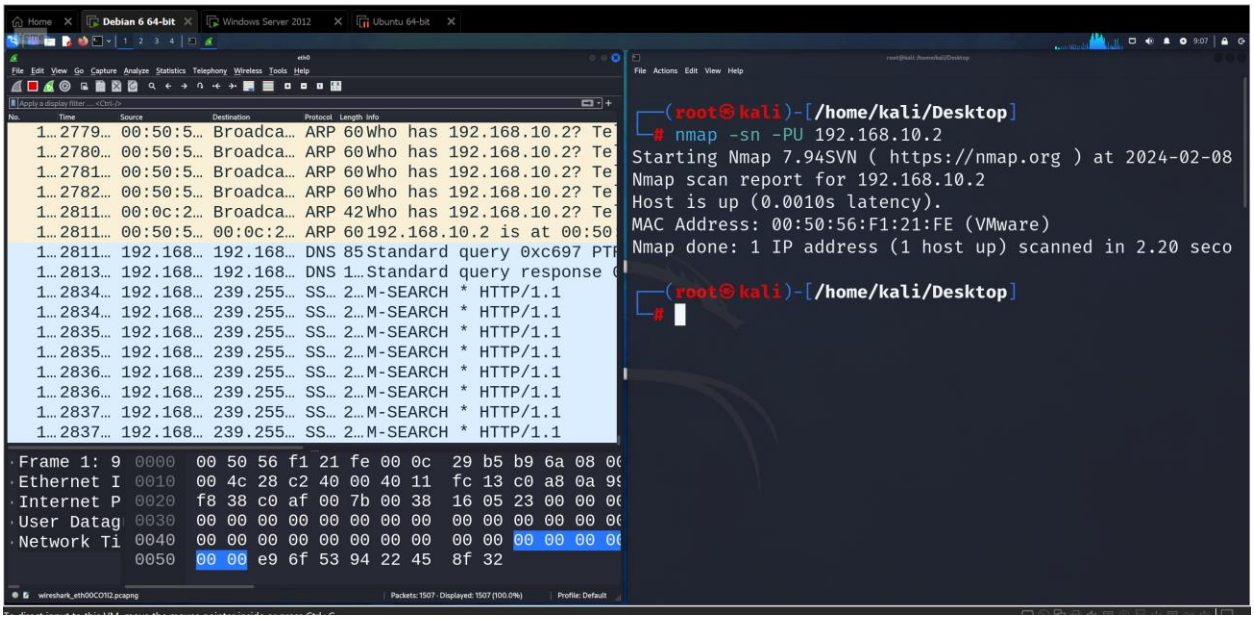
ICMP Timestamps scan using nmap

Command: nmap –sn - -disable-arp-ping –PP 192.168.10.2



Let’s do a UDP host scan with nmap

Command: nmap –sn –PU 192.168.10.2



When the scanning in local network (LAN), nmap is satisfied with scanning ARP because computer need a MAC address before sending TCP and UDP packets. To force NMAP to perform TCP and UDP scanning in local network.

Conclusions:

This lab provided hands-on experience in network reconnaissance and vulnerability scanning using tools like Nmap and Wireshark, enabling thorough exploration of networked systems' vulnerabilities and service versions.

References:

1. Mazurczyk, W., & Caviglione, L. (2021). Cyber reconnaissance techniques. Communications of the ACM, 64(3), 86-95.
2. Calderon, P. (2021). Nmap Network Exploration and Security Auditing Cookbook: Network discovery and security scanning at your fingertips. Packt Publishing Ltd.
3. Ndatinya, V., Xiao, Z., Manepalli, V. R., Meng, K., & Xiao, Y. (2015). Network forensics analysis using Wireshark. International Journal of Security and Networks, 10(2), 91-106.