

Step 0

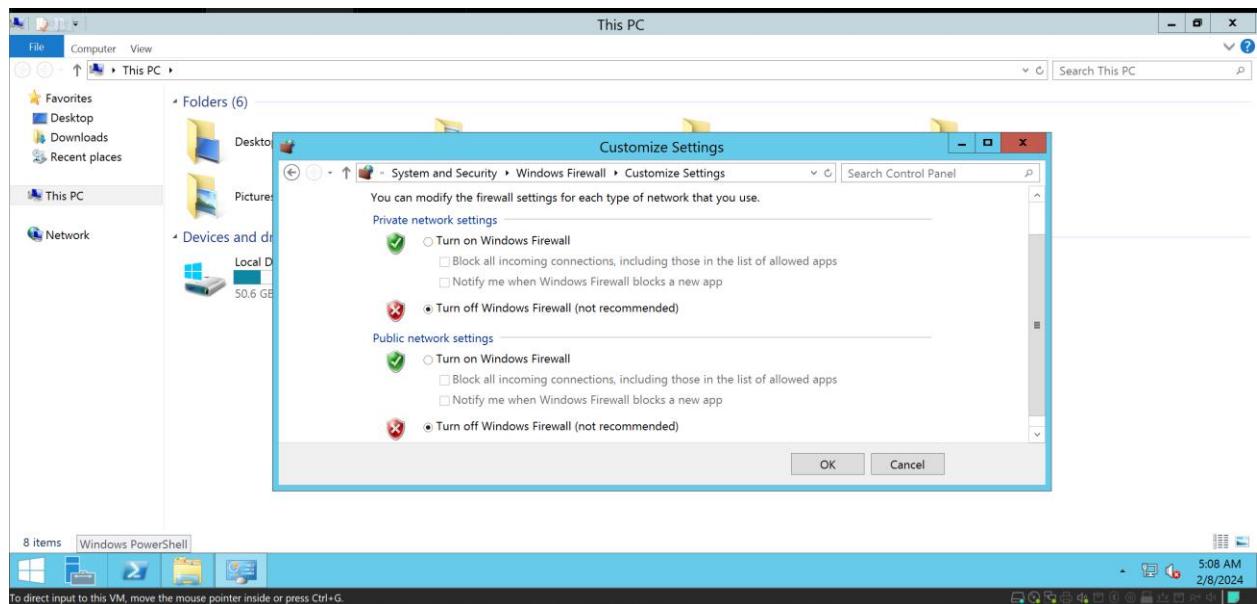
Preparation

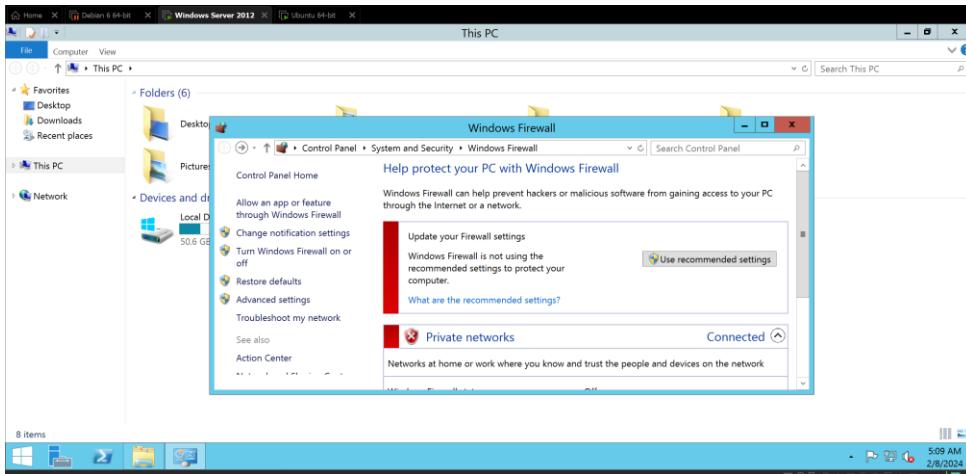
For this lab We need

- 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.

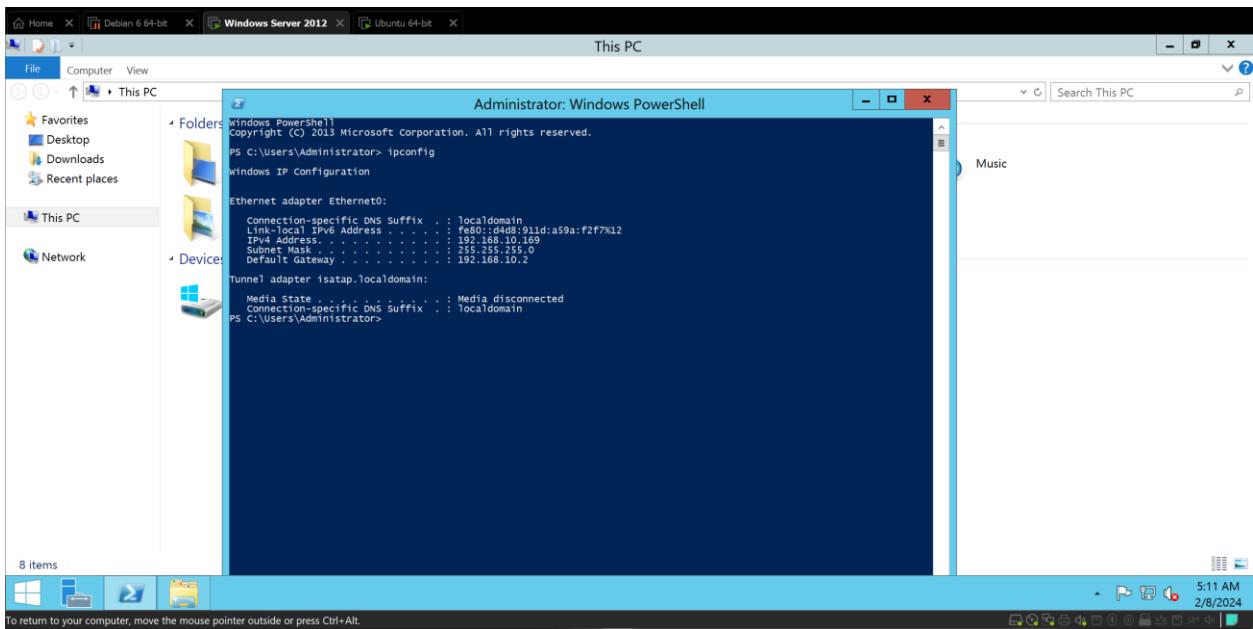




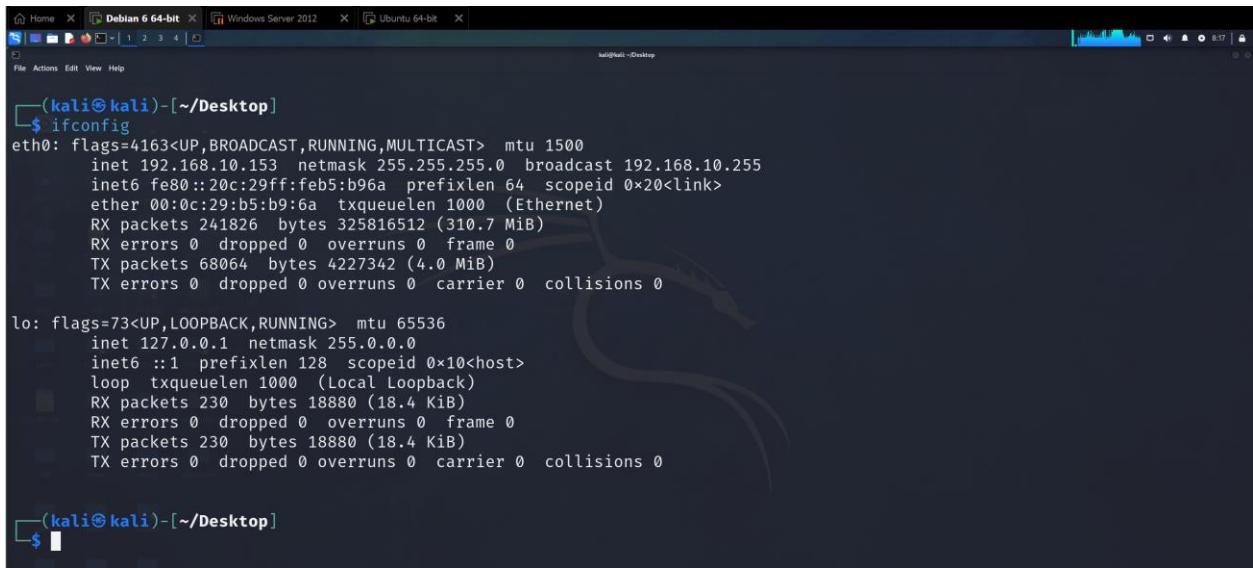
Step 1

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.

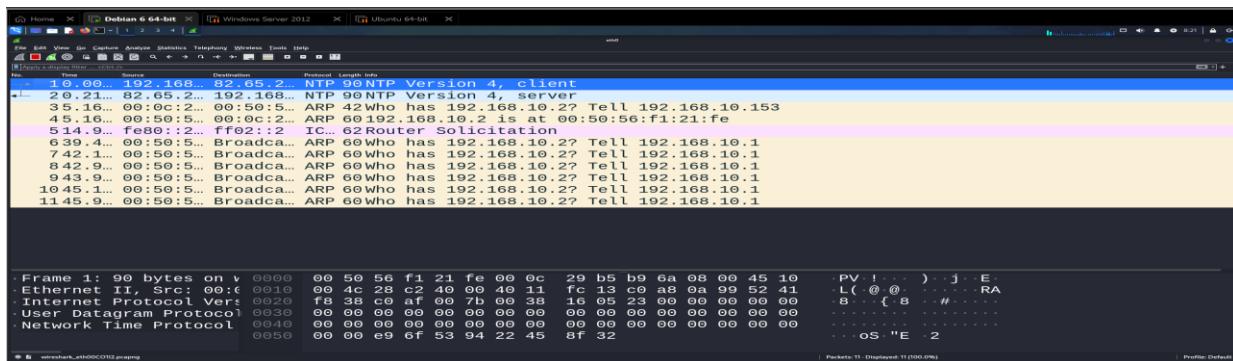
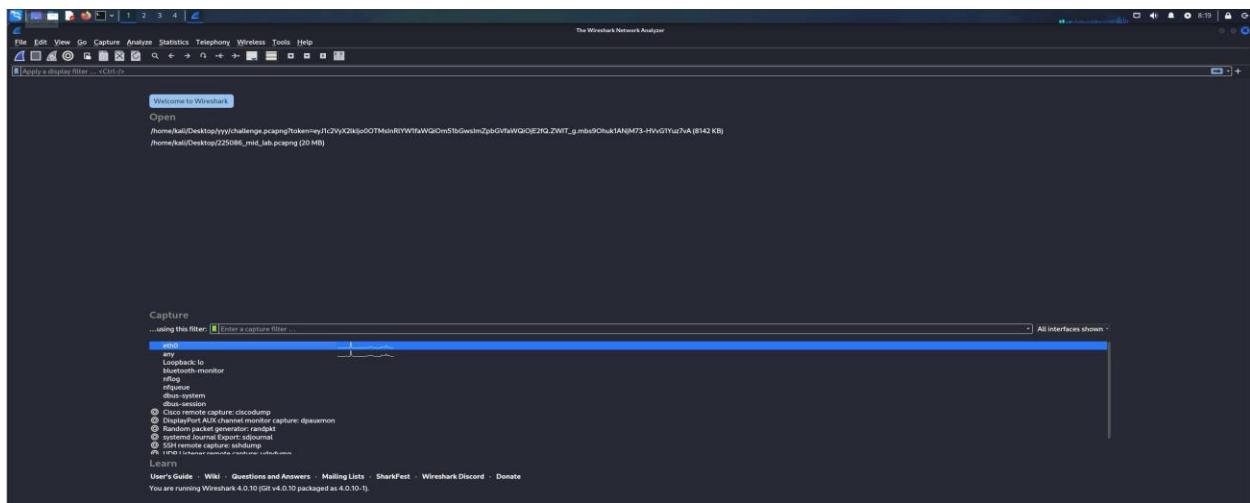


```
(kali㉿kali)-[~/Desktop]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 192.168.10.153  netmask 255.255.255.0  broadcast 192.168.10.255
      inet6 fe80::20c:29ff:feb5:b96a  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:b5:b9:6a  txqueuelen 1000  (Ethernet)
          RX packets 241826  bytes 325816512 (310.7 MiB)
          RX errors 0  dropped 0  overrun 0  frame 0
          TX packets 68064  bytes 4227342 (4.0 MiB)
          TX errors 0  dropped 0  overrun 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 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
          RX packets 230  bytes 18880 (18.4 KiB)
          RX errors 0  dropped 0  overrun 0  frame 0
          TX packets 230  bytes 18880 (18.4 KiB)
          TX errors 0  dropped 0  overrun 0  carrier 0  collisions 0

(kali㉿kali)-[~/Desktop]
$
```

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



```

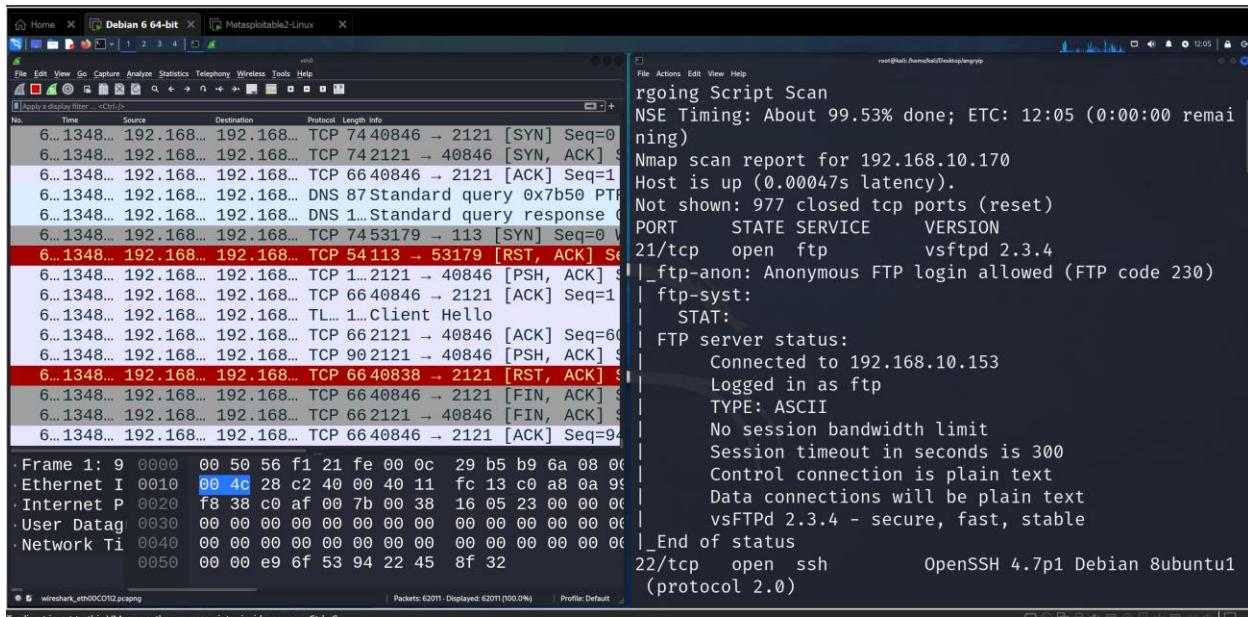
* Starting deferred execution scheduler atd [ OK ]
* Starting periodic command scheduler crond [ OK ]
* Starting Tomcat servlet engine tomcat5.5 [ OK ]
* Starting web server apache2 [ OK ]
* Running local boot scripts (/etc/rc.local)
nohup: appending output to 'nohup.out'
nohup: appending output to 'nohup.out' [ OK ]

Warning: Never expose this VM to an untrusted network!
Contact: msfdev@metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: _

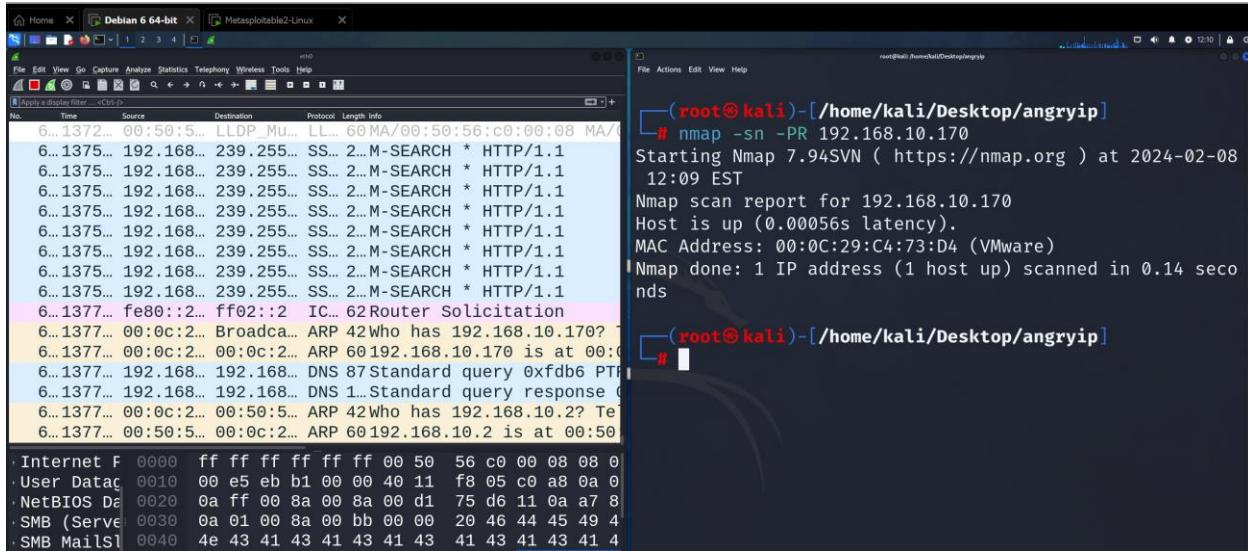
```

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

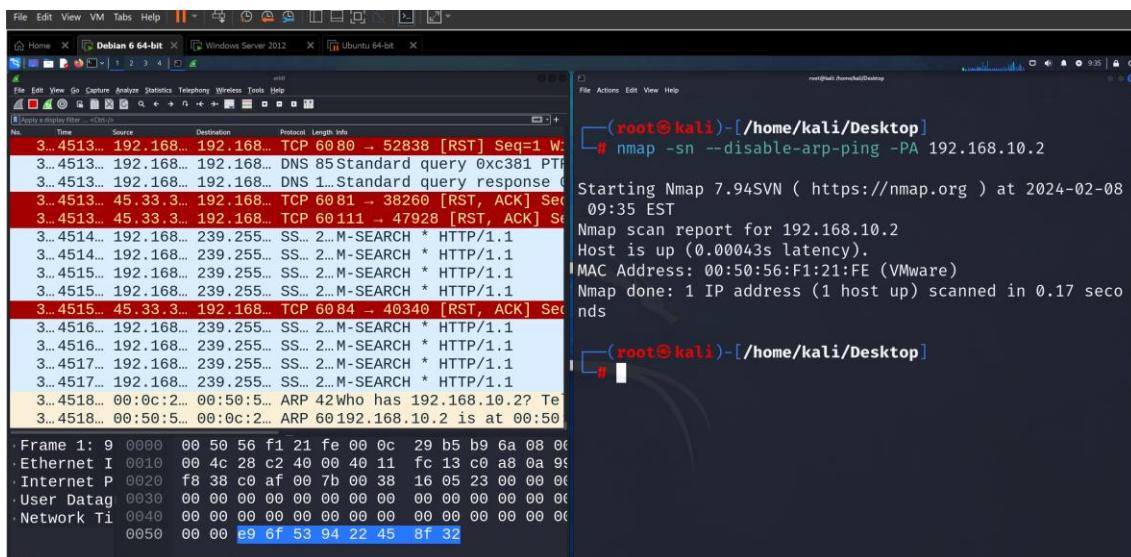
Let's perform ICMP Echo scan using nmap

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

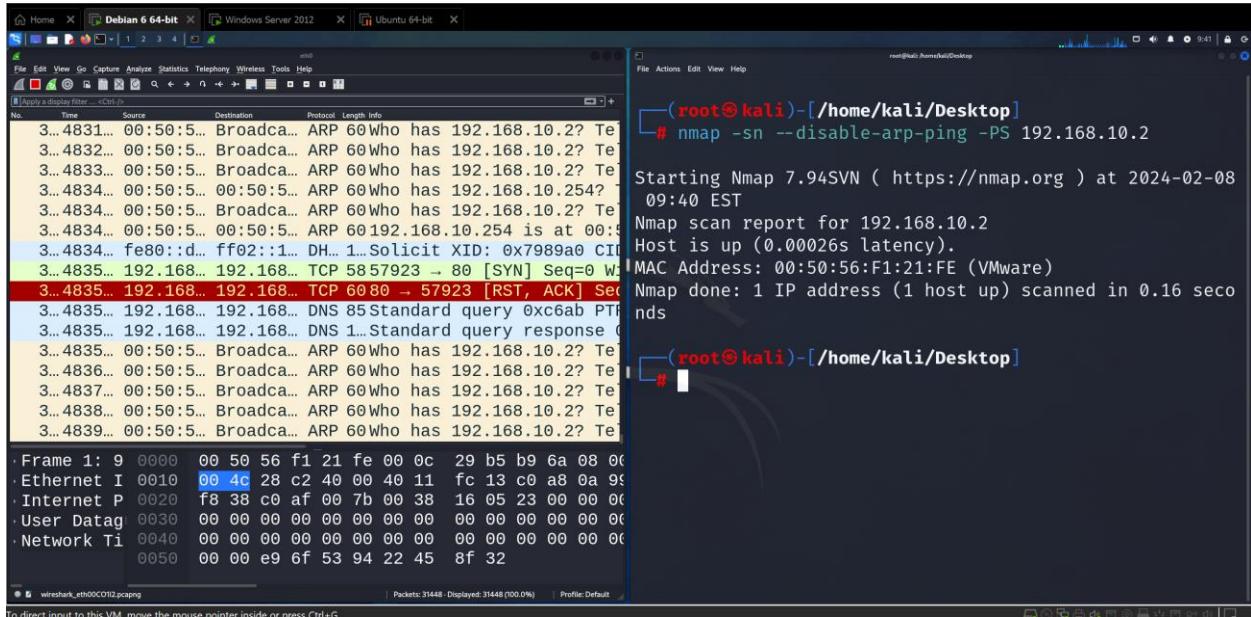
Command: nmap -sn --disable-arp-ping -PA 192.168.10.2



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



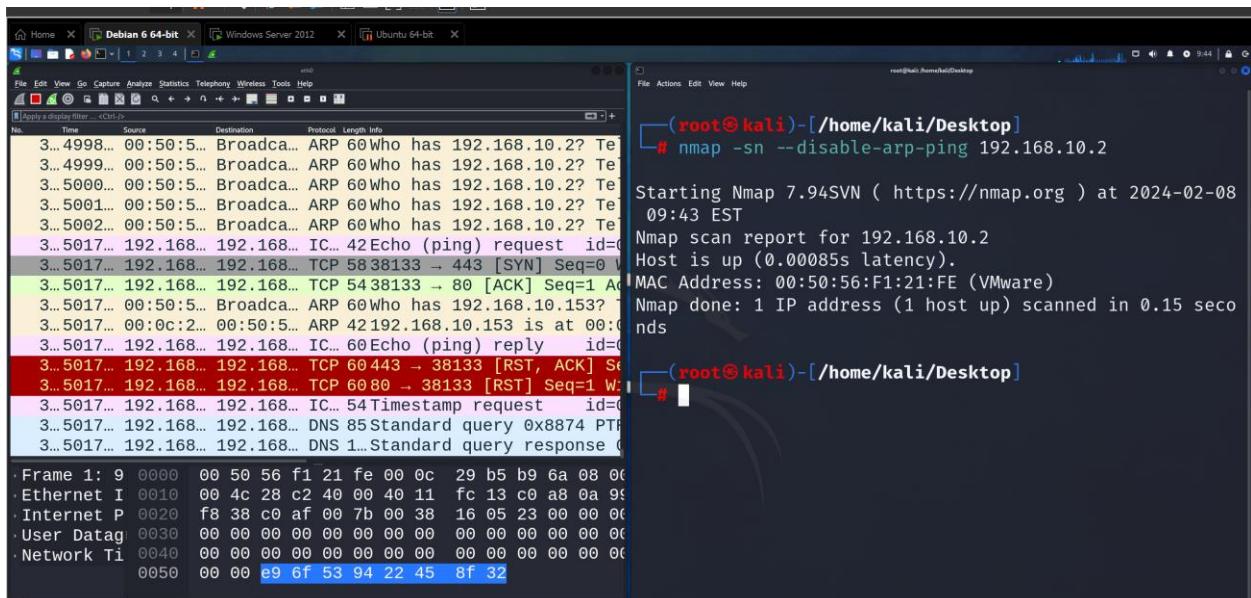
```
(root㉿kali)-[~/home/kali/Desktop]
# nmap -sn --disable-arp-ping -PS 192.168.10.2

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-08
09:40 EST
Nmap scan report for 192.168.10.2
Host is up (0.00026s latency).
MAC Address: 00:50:56:F1:21:FE (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds

#
```

ICMP Echo sweep using nmap:

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



```
(root㉿kali)-[~/home/kali/Desktop]
# nmap -sn --disable-arp-ping 192.168.10.2

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-08
09:43 EST
Nmap scan report for 192.168.10.2
Host is up (0.00085s latency).
MAC Address: 00:50:56:F1:21:FE (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds

#
```

Scan using Angry IP scanner:

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

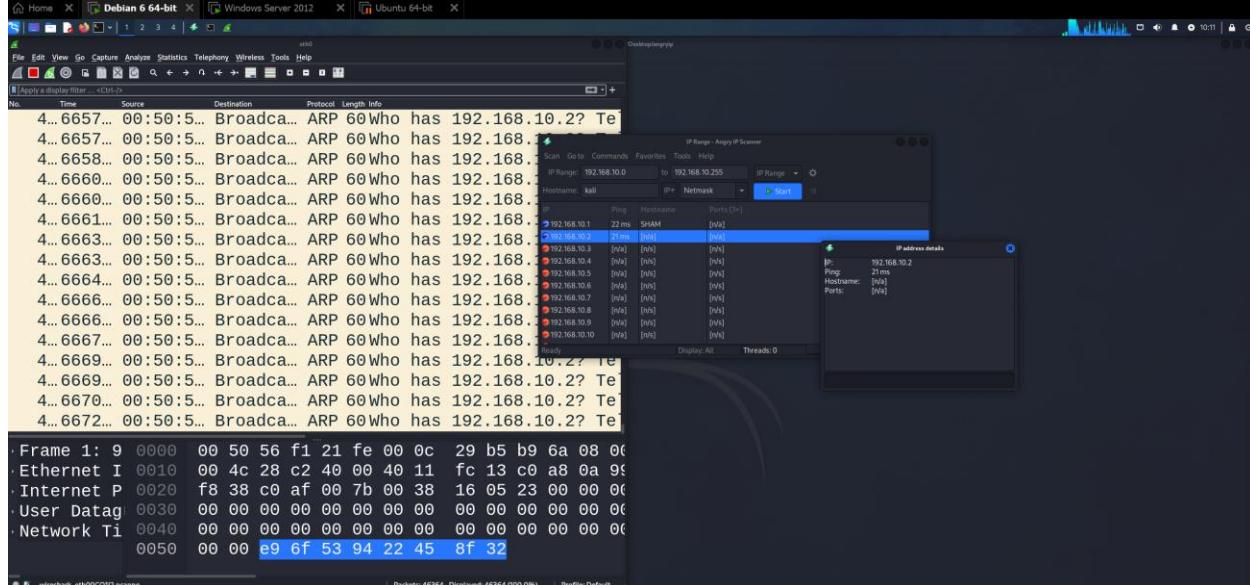
First download ipscan from official site.

The screenshot shows the official website for Angry IP Scanner (angryip.org/download/#linux). The page has a dark blue header with the Angry IP Scanner logo and the text "Fast and friendly network scanner". Below the header are buttons for "About", "Screenshots", "Download" (which is highlighted), "FAQ", and "Contribute". The main content area is titled "Download for Windows, Mac or Linux" and features three large buttons: "Windows", "Mac OS", and "Linux". Below these buttons, there is a note about downloading version 3.9.1 or previous releases, followed by a list of download links for various operating systems and architectures. A "Running" section is visible at the bottom.

Using wget tool to download

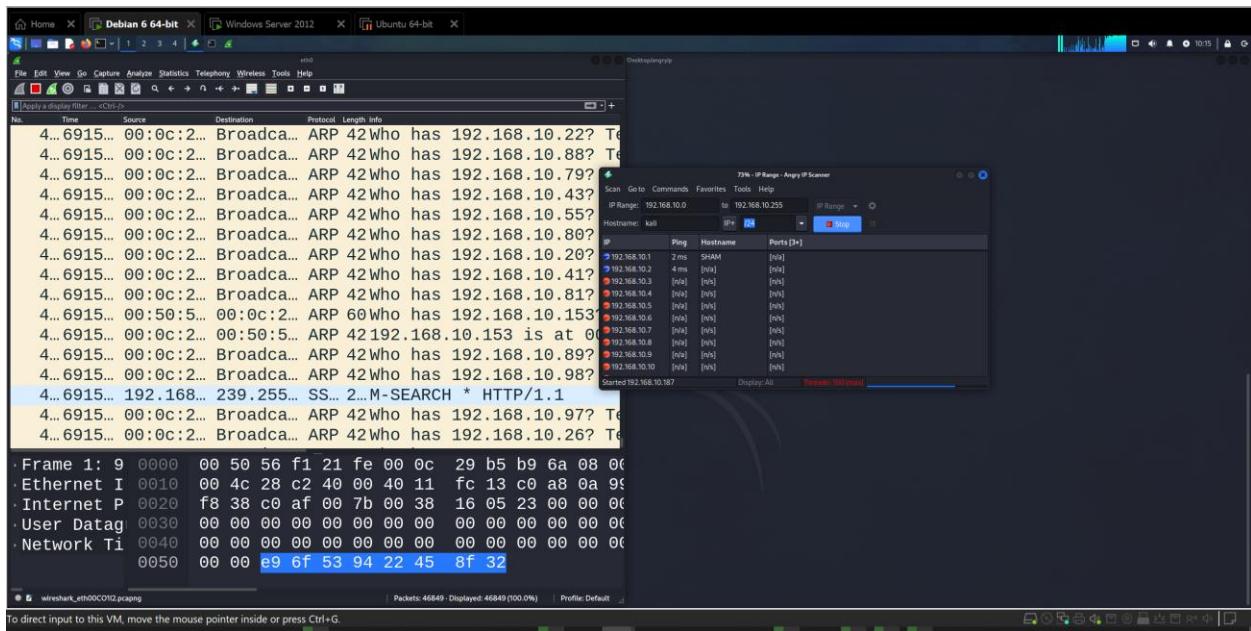
After downloading use dpkg –i ad the .deb file to install

After installing it will open.

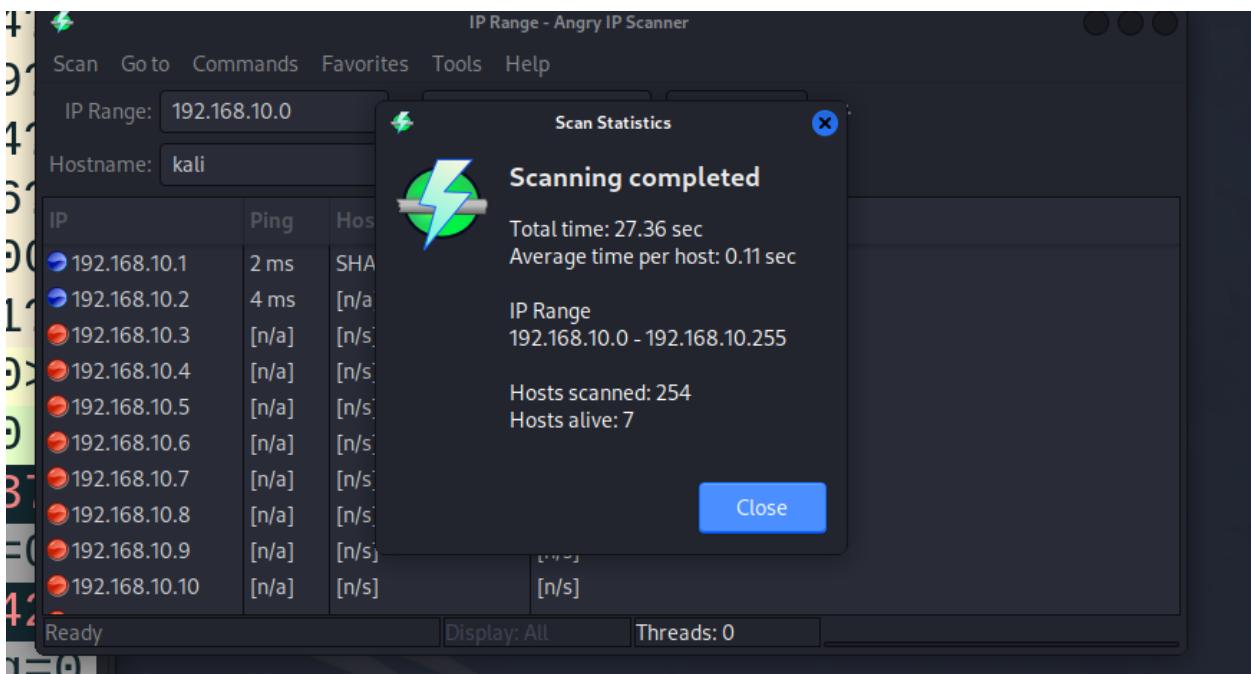


Make sure that alive host is selected which is kali.

Select the range and press start



And the Result:



TCP Stealth Scan

Command: nmap -sS 192.168.10.2

The screenshot shows a dual-pane interface. On the left is Wireshark displaying network traffic on interface eth0, with a captured file named 'wireshark_eth00C012.pcapng'. The list view shows several SYN and RST/ACK packets exchanged between the local host (192.168.1.10) and the target host (192.168.10.2). On the right is a terminal window running on Kali Linux, showing the command 'nmap -sS 192.168.10.2' and its output. The output indicates that the port 192.168.10.2 is open, with a domain service. It also lists 999 closed ports.

```
(root㉿kali)-[~/home/kali/Desktop/angryip]
# nmap -sS 192.168.10.2

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-08
10:18 EST
Nmap scan report for 192.168.10.2
Host is up (0.00034s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 00:50:56:F1:21:FE (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.98 seconds

(root㉿kali)-[~/home/kali/Desktop/angryip]
#
```

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

Command: nmap -sS -p80 192.168.10.2 http

The screenshot shows a dual-pane interface. On the left is Wireshark displaying network traffic on interface eth0, with a captured file named 'wireshark_eth00C012.pcapng'. The list view shows several DNS queries and a single TCP SYN packet from the target host to port 80. On the right is a terminal window running on Kali Linux, showing the command 'nmap -sS -p80 192.168.10.2 http' and its output. The output indicates that port 80 is closed, with the HTTP service. It also lists 999 closed ports.

```
(root㉿kali)-[~/home/kali/Desktop/angryip]
# nmap -sS -p80 192.168.10.2 http

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-08
10:21 EST
Nmap scan report for 192.168.10.2
Host is up (0.00035s latency).

PORT      STATE SERVICE
80/tcp    closed http
MAC Address: 00:50:56:F1:21:FE (VMware)

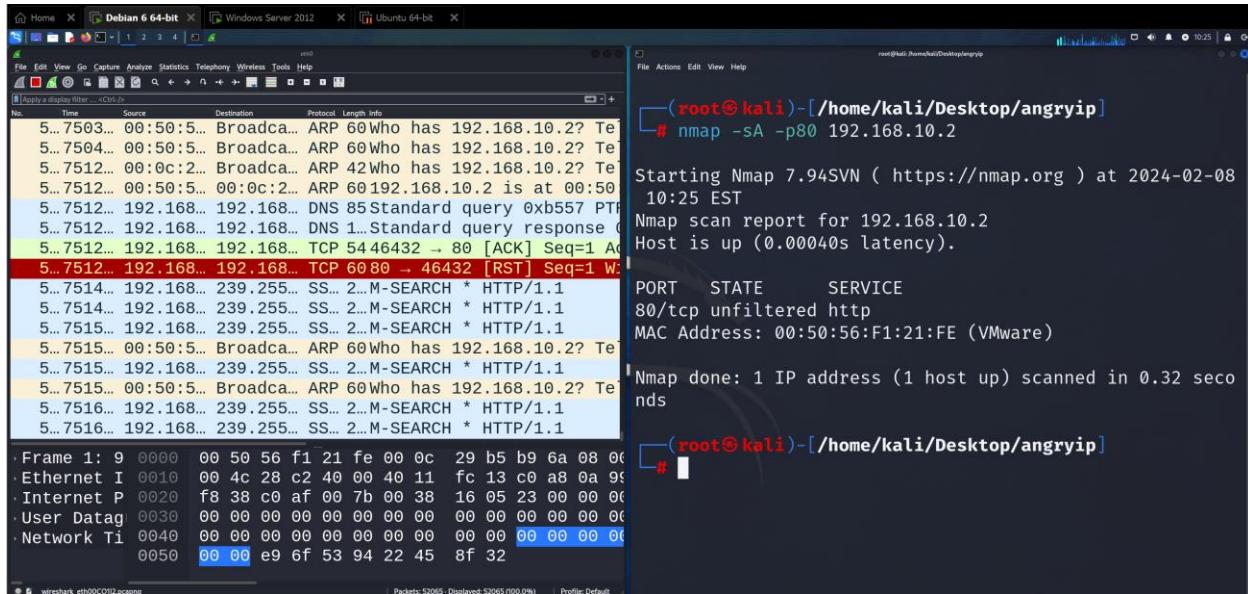
Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds

(root㉿kali)-[~/home/kali/Desktop/angryip]
#
```

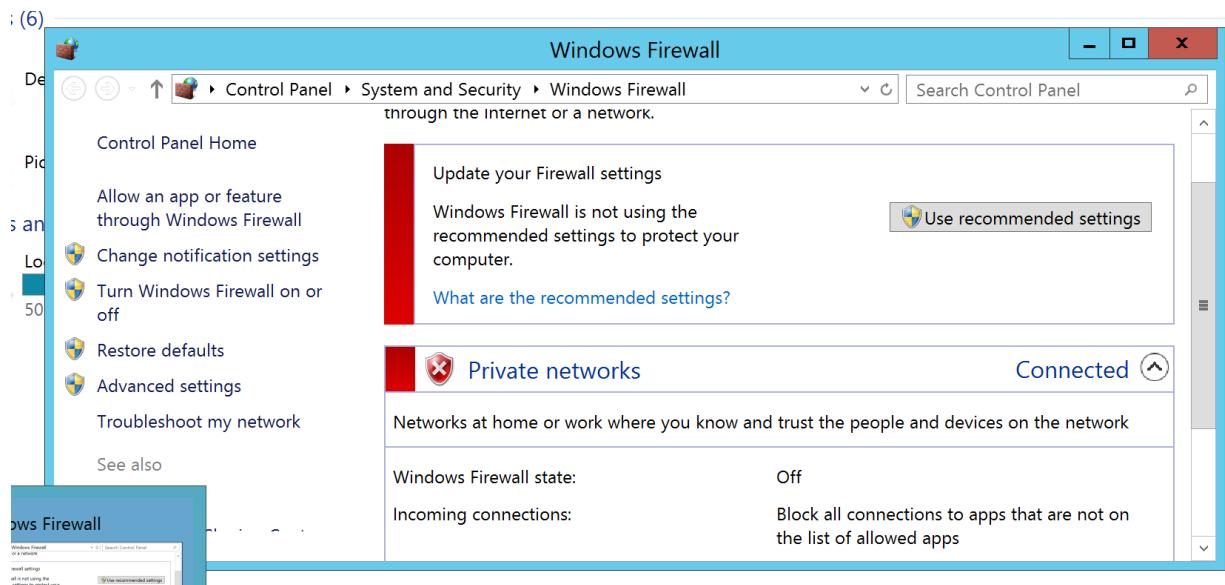
Nmap sends TCP FIN PSH URG packets to the port to be tested. The target responds with TCP RST if the port is closed, and does not respond if the port is open. Nmap considers the port as open | filtered because a firewall can block reply packet if the port is closed.

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

```
(root㉿kali)-[/home/kali/Desktop/angryip]
# nmap -sU 192.168.10.2

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-08
10:29 EST
Stats: 0:00:08 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 34.00% done; ETC: 10:29 (0:00:16 remaining)
Nmap scan report for 192.168.10.2
Host is up (0.001s latency).
Not shown: 999 open|filtered udp ports (no-response)
PORT      STATE SERVICE
53/udp    open  domain
MAC Address: 00:50:56:F1:21:FE (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.28 seconds
```

Step 3

Service Version Discovery

Command: nmap -sV 192.168.10.2

```
(root㉿kali)-[/home/kali/Desktop/angryip]
# nmap -sV 192.168.10.2

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-08
10:31 EST
Stats: 0:00:12 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Nmap scan report for 192.168.10.2
Host is up (0.00051s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
53/tcp    open  domain (generic dns response: FORMERR)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.94SVN%I=7%D=2/8%Time=65C4F3CD%P=x86_64
-pc-linux-gnu%r(DN
SF:ServiceBindReqTCP,6B,"\0i\0\x06\x81\x83\0\x01\0\0\0\x01\0\x07version
SF:\x04bind\0\0\x10\0\x03\0\0\x06\0\x01\0\x01Q\x06\0\0\x01\0\x0croot-servers

Frame 1: 9 0000 00 50 56 f1 21 fe 00 0c 29 b5 b9 6a 08 0e
Ethernet I 0010 00 4c 28 c2 40 00 40 11 fc 13 c0 a8 0a 95
Internet P 0020 f8 38 c0 af 00 7b 00 38 16 05 23 00 00 00
User Data: 0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Network Ti 0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0050 00 00 e9 6f 53 94 22 45 8f 32

Packets: 56408 - Displayed: 56408 (100.0%) | Profile: Default
```

Operating System Discovery

Command: nmap -sO 192.168.10.2

```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
File Actions Edit View Help
[+] (root@kali)-[/home/kali/Desktop/angryip]
# nmap -sO 192.168.10.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-08
10:34 EST
Nmap scan report for 192.168.10.2
Host is up (0.00034s latency).
Not shown: 252 closed n/a protocols (proto-unreach)
PROTOCOL STATE SERVICE
1 open icmp
6 open tcp
17 open|filtered udp
47 open|filtered gre
MAC Address: 00:50:56:F1:21:FE (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.69 seconds

[+] (root@kali)-[/home/kali/Desktop/angryip]
# 

```

Wireshark capture details:

- Frame 1: 9 0000 00 50 56 f1 21 fe 00 0c 29 b5 b9 6a 08 00
- Ethernet I 0010 00 4c 28 c2 40 00 40 11 fc 13 c0 a8 0a 95
- Internet P 0020 f8 38 c0 af 00 7b 00 38 16 05 23 00 00 00
- User Data: 0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
- Network Ti 0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
- 0050 00 00 e9 6f 53 94 22 45 8f 32

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

Command nmap -sV -O 192.168.10.2

```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
File Actions Edit View Help
[+] (root@kali)-[/home/kali/Desktop/angryip]
# nmap -sV -O 192.168.10.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-08
10:34 EST
OS CPE: cpe:/a:vmware:player cpe:/o:microsoft:windows_xp_sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012 cpe:/o:linux:linux_kernel:2.4.37 cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel cpe:/o:linux:linux_kernel:3.2
Aggressive OS guesses: VMware Player virtual NAT device (99%), Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012 (93%), DD-WRT v24-sp2 (Linux 2.4.37) (91%), Microsoft Windows XP SP3 (91%), Actiontec MI424WR-GEN3I WAP (91%), Linux 3.2 (90%), DVTEL DVT-9540DW network camera (89%)
No exact OS matches for host (test conditions non-ideal)
.
Network Distance: 1 hop

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 26.32 seconds

[+] (root@kali)-[/home/kali/Desktop]
# 

```

Wireshark capture details:

- Frame 1: 9 0000 00 50 56 f1 21 fe 00 0c 29 b5 b9 6a 08 00
- Ethernet I 0010 00 4c 28 c2 40 00 40 11 fc 13 c0 a8 0a 95
- Internet P 0020 f8 38 c0 af 00 7b 00 38 16 05 23 00 00 00
- User Data: 0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
- Network Ti 0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
- 0050 00 00 e9 6f 53 94 22 45 8f 32

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

```
File Actions Edit View Help
ow the service/version, please submit the following fing
erprint at https://nmap.org/cgi-bin/submit.cgi?new-servi
ce :
SF-Port53-TCP:V=7.94SVN%I=7%D=2%/8%Time=65C4E28F%P=x86_64
-pc-linux-gnu%r(DN
SF:SVersionBindReqTCP,6B,"\0i\0\x06\x81\x83\0\x01\0\0\0\x01\0\0\x07version
SF:\x04bind\0\0\x10\0\x03\0\0\x06\0\x01\0\x01Q\x80\0a\0\x01a\x0croot-servers
SF:\x03net\0\x05nstld\x0cverisign-grs\x03com\0x\x0xa4\x1b\0\0\x07\x08\0\x
SF:\x84\0\t:\x80\0\x01Q\x80"\%)r(DNSStatusRequestTCP,E,
"\0\x0c\0\0\x90\0\x0
SF:1\0\0\0\0\0\0\0\0";
MAC Address: 00:50:56:F1:21:FE (VMware)

Service detection performed. Please report any incorrect
results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.84 seconds

[root@kali]~[~/home/kali/Desktop]
#
```

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

```
File Actions Edit View Help
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-08 09:26 EST
Stats: 0:00:22 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 100.00% done; ETC: 09:26 (0:00:00 remaining)
Nmap scan report for 192.168.10.2
Host is up (0.00029s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
53/tcp    open  domain (generic dns response: FORMERR)
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|     bind
|     root-servers
|     nstld
|     verisign-grs
1 service unrecognized despite returning data. If you kn

[root@kali]~[~/home/kali/Desktop]
# nmap -sV --script vulners 192.168.10.2

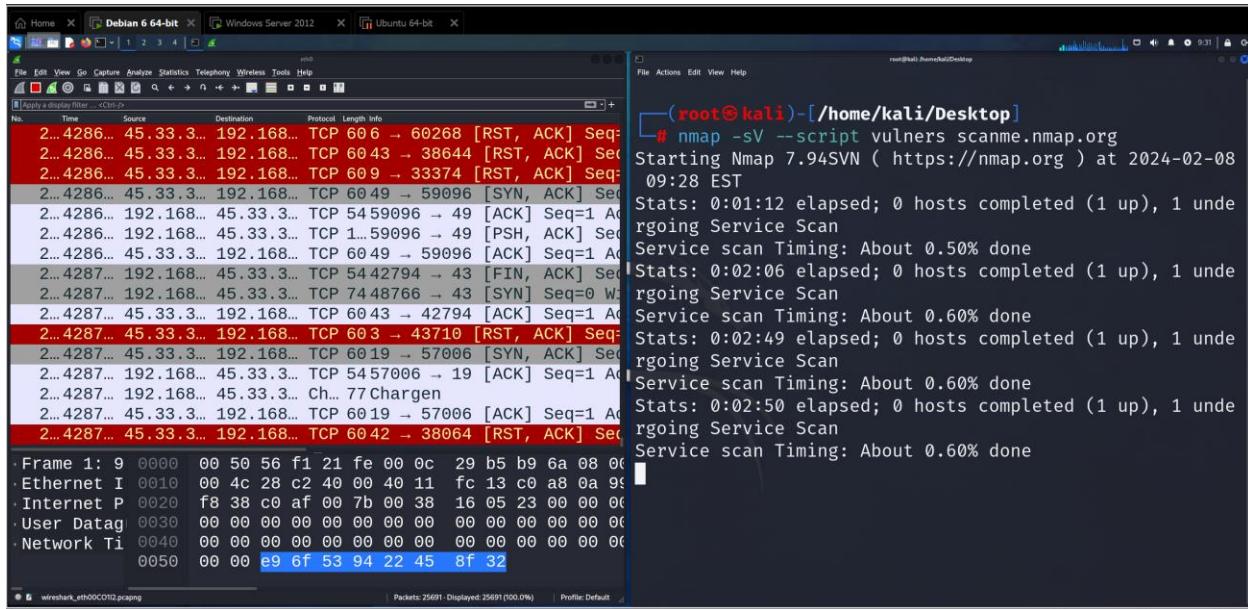
Frame 1: 9 0000 00 50 56 f1 21 fe 00 0c 29 b5 b9 6a 08 00
· Ethernet I 0010 00 4c 28 c2 40 00 40 11 fc 13 c0 a8 0a 95
· Internet P 0020 f8 38 c0 af 00 7b 00 38 16 05 23 00 00 00
· User Datag 0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
· Network Ti 0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0050 00 00 e9 6f 53 94 22 45 8f 32

[root@kali]~[~/home/kali/Desktop]
#
```

Exercise:

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

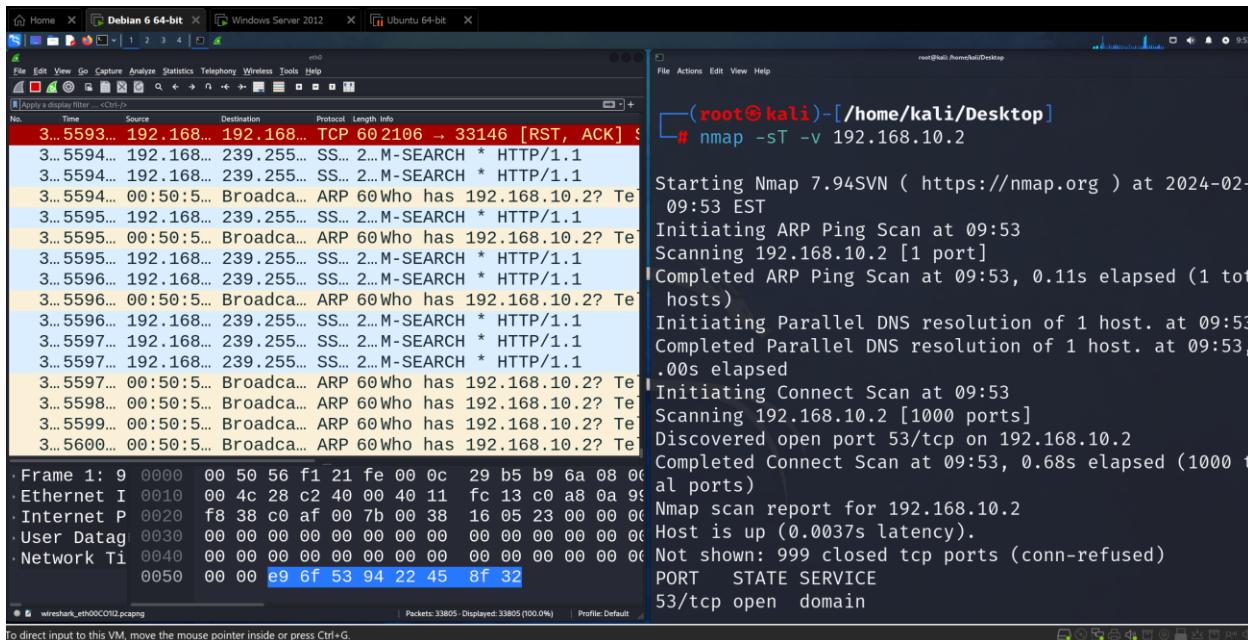
Command: nmap -sV --script vulners scanme.nmap.org



```
# nmap -sV --script vulners scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-08
09:28 EST
Stats: 0:01:12 elapsed; 0 hosts completed (1 up), 1 unde
rongoing Service Scan
Service scan Timing: About 0.50% done
Stats: 0:02:06 elapsed; 0 hosts completed (1 up), 1 unde
rongoing Service Scan
Service scan Timing: About 0.60% done
Stats: 0:02:49 elapsed; 0 hosts completed (1 up), 1 unde
rongoing Service Scan
Service scan Timing: About 0.60% done
Stats: 0:02:50 elapsed; 0 hosts completed (1 up), 1 unde
rongoing Service Scan
Service scan Timing: About 0.60% done
Stats: 0:02:50 elapsed; 0 hosts completed (1 up), 1 unde
rongoing Service Scan
Service scan Timing: About 0.60% done
```

TCP Connect scan:

nmap -sT -v 192.168.10.2

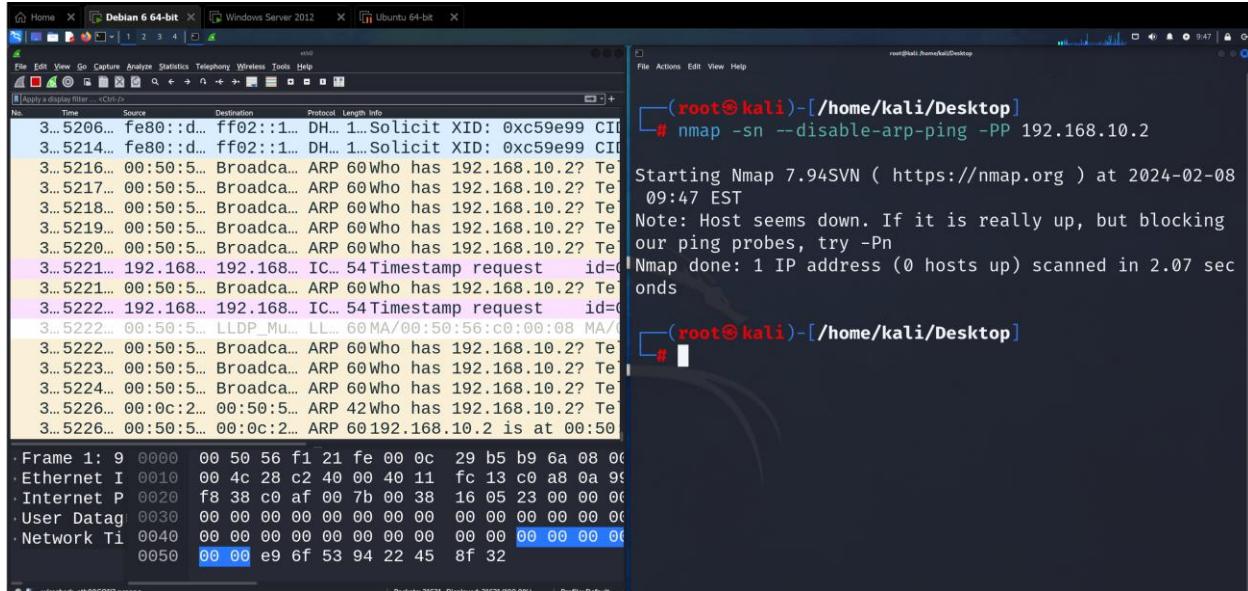


```
# nmap -sT -v 192.168.10.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-09:53 EST
Initiating ARP Ping Scan at 09:53
Scanning 192.168.10.2 [1 port]
Completed ARP Ping Scan at 09:53, 0.11s elapsed (1 tot
hosts)
Initiating Parallel DNS resolution of 1 host. at 09:53
Completed Parallel DNS resolution of 1 host. at 09:53,
.00s elapsed
Initiating Connect Scan at 09:53
Scanning 192.168.10.2 [1000 ports]
Discovered open port 53/tcp on 192.168.10.2
Completed Connect Scan at 09:53, 0.68s elapsed (1000 t
al ports)
Nmap scan report for 192.168.10.2
Host is up (0.0037s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE     SERVICE
53/tcp    open      domain
```

We see on the left the Wireshark the movement of ICMP Echo packets towards address 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



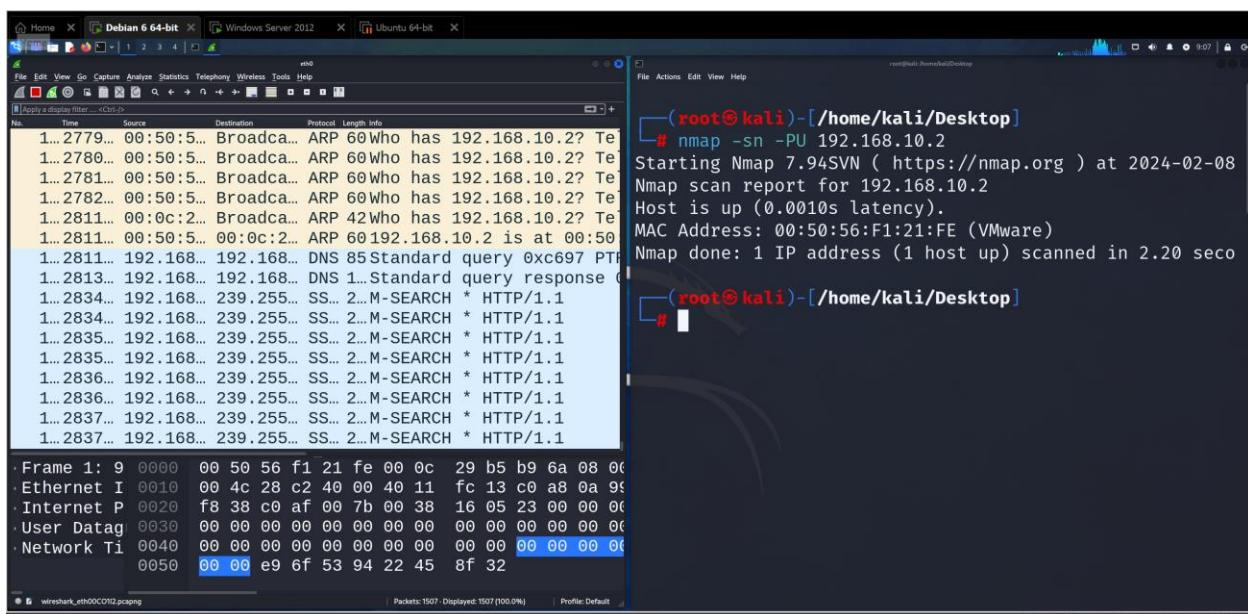
```
(root㉿kali)-[~/home/kali/Desktop]
# nmap -sn --disable-arp-ping -PP 192.168.10.2

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-08
09:47 EST
Note: Host seems down. If it is really up, but blocking
our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.07 seconds

#
```

Let's do a UDP host scan with nmap

Command: nmap -sn -PU 192.168.10.2



```
(root㉿kali)-[~/home/kali/Desktop]
# nmap -sn -PU 192.168.10.2

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-08
Nmap scan report for 192.168.10.2
Host is up (0.0010s latency).
MAC Address: 00:50:56:F1:21:FE (VMware)
Nmap done: 1 IP address (1 host up) scanned in 2.20 seconds

#
```

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.