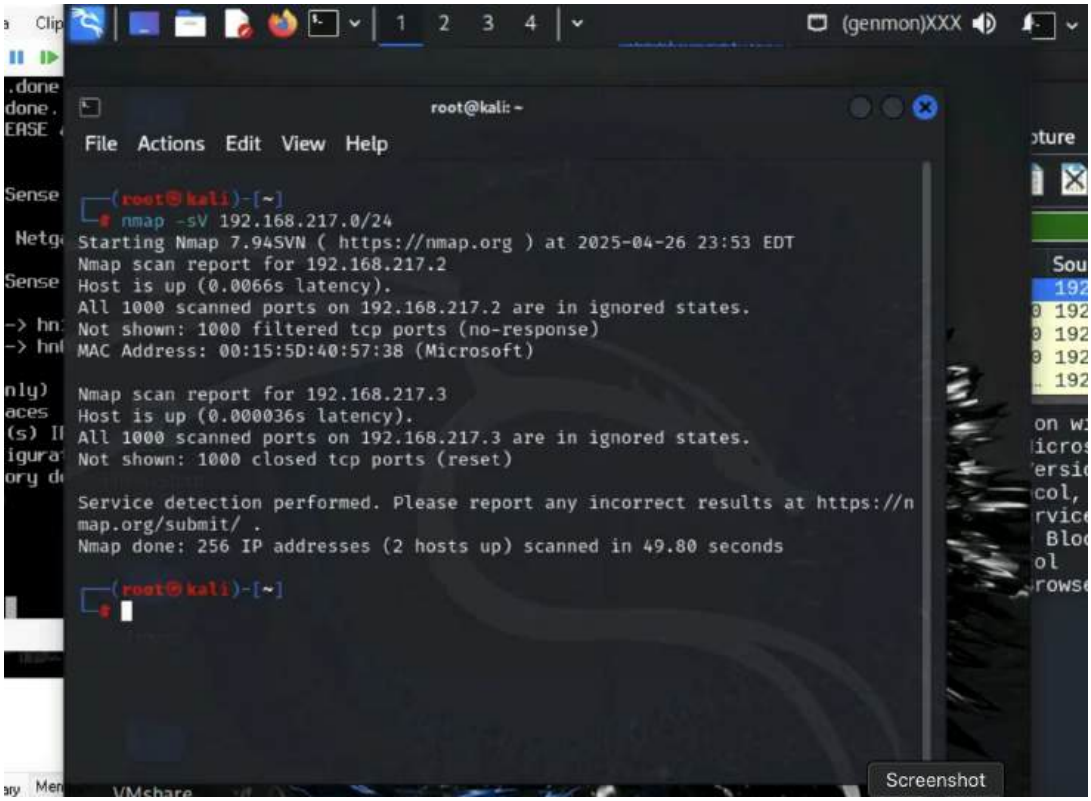
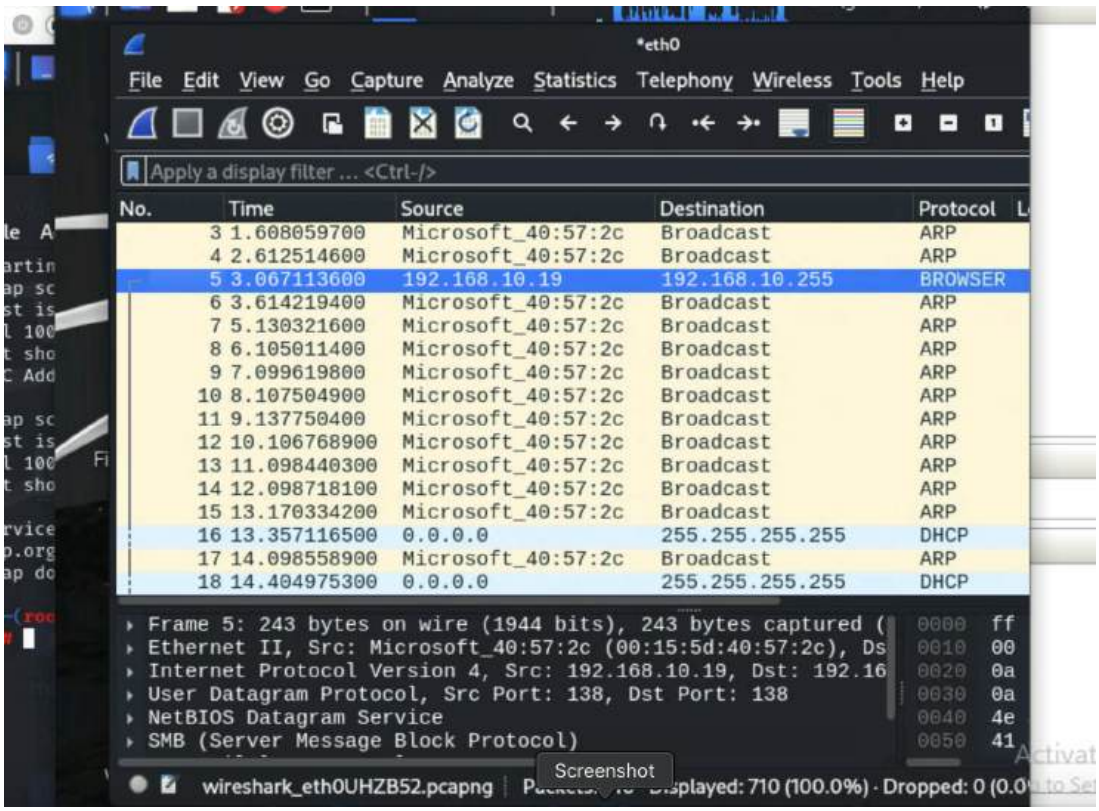
Task A


root@kali: ~
File Actions Edit View Help
nmap -sV 192.168.217.0/24
Starting Nmap 7.94SVN (https://nmap.org) at 2025-04-26 23:53 EDT
Nmap scan report for 192.168.217.2
Host is up (0.0066s latency).
All 1000 scanned ports on 192.168.217.2 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:15:5D:40:57:38 (Microsoft)
Nmap scan report for 192.168.217.3
Host is up (0.000036s latency).
All 1000 scanned ports on 192.168.217.3 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (2 hosts up) scanned in 49.80 seconds
Screenshot


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol
3 1.608059700 Microsoft_40:57:2c Broadcast ARP
4 2.612514600 Microsoft_40:57:2c Broadcast ARP
5 3.067113600 192.168.10.19 192.168.10.255 BROWSER
6 3.614219400 Microsoft_40:57:2c Broadcast ARP
7 5.130321600 Microsoft_40:57:2c Broadcast ARP
8 6.105011400 Microsoft_40:57:2c Broadcast ARP
9 7.099619800 Microsoft_40:57:2c Broadcast ARP
10 8.107504900 Microsoft_40:57:2c Broadcast ARP
11 9.137750400 Microsoft_40:57:2c Broadcast ARP
12 10.106768900 Microsoft_40:57:2c Broadcast ARP
13 11.098440300 Microsoft_40:57:2c Broadcast ARP
14 12.098718100 Microsoft_40:57:2c Broadcast ARP
15 13.170334200 Microsoft_40:57:2c Broadcast ARP
16 13.357116500 0.0.0.0 255.255.255.255 DHCP
17 14.098558900 Microsoft_40:57:2c Broadcast ARP
18 14.404975300 0.0.0.0 255.255.255.255 DHCP
Frame 5: 243 bytes on wire (1944 bits), 243 bytes captured (
Ethernet II, Src: Microsoft_40:57:2c (00:15:5d:40:57:2c), Ds
Internet Protocol Version 4, Src: 192.168.10.19, Dst: 192.16
User Datagram Protocol, Src Port: 138, Dst Port: 138
NetBIOS Datagram Service
SMB (Server Message Block Protocol)
0000 ff
0010 00
0020 0a
0030 0a
0040 4e
0050 41
Screenshot
wireshark_eth0UHZB52.pcapng

Wireshark Traffic Analysis Discussion

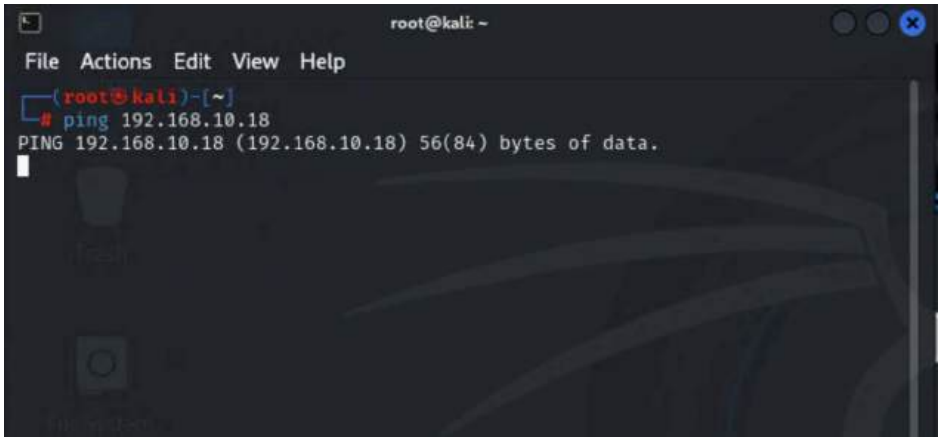
During the network scan from External Kali, I captured the traffic using Wireshark on the Internal Kali VM. In total, there were 710 packets recorded. Out of these, 417 packets were ARP traffic, which is common when devices are trying to map IP addresses to MAC addresses across the local network. Additionally, there were 264 DHCP packets, showing that devices were communicating with the DHCP server to obtain IP address leases or renew them. I also observed 21 DHCPv6 packets and 2 ICMPv6 packets, which indicate that IPv6 communication is active, even though my main focus was IPv4. There were also 6 "browser" packets, typically related to network services advertisements (such as NetBIOS or service discovery in Windows networks).

Interestingly, while scanning, I noticed that most of the traffic was background network noise, not direct responses to my Nmap probe. This matches the network design, where External Kali is on a different subnet (192.168.217.x) than the internal machines (192.168.10.x). Because pfSense separates the networks, the scan from External Kali did not trigger much direct traffic from Ubuntu or Windows Server 2022. Overall, Wireshark helped visualize how active background protocols like ARP and DHCP are during normal network operations.

Task B

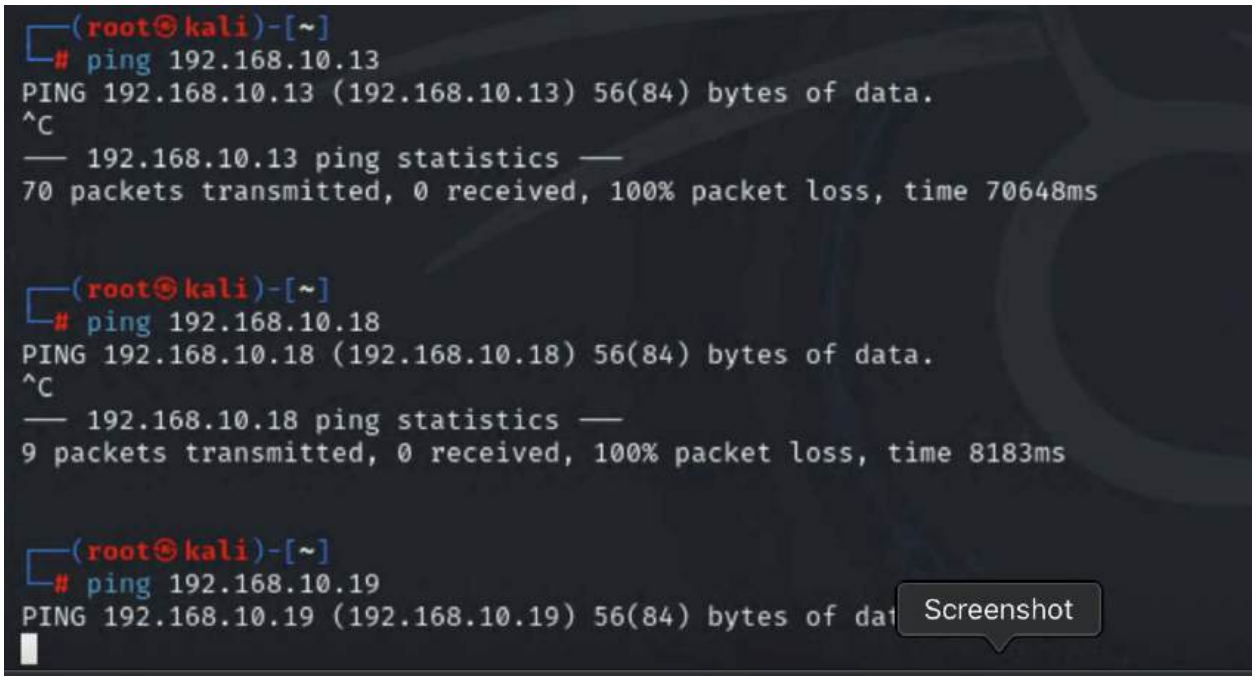
1.

Rule#	Interface	Action	Source IP	Destination IP	Protocol
1	WAN	Block	192.168.217.3	192.168.10.18	ICMP



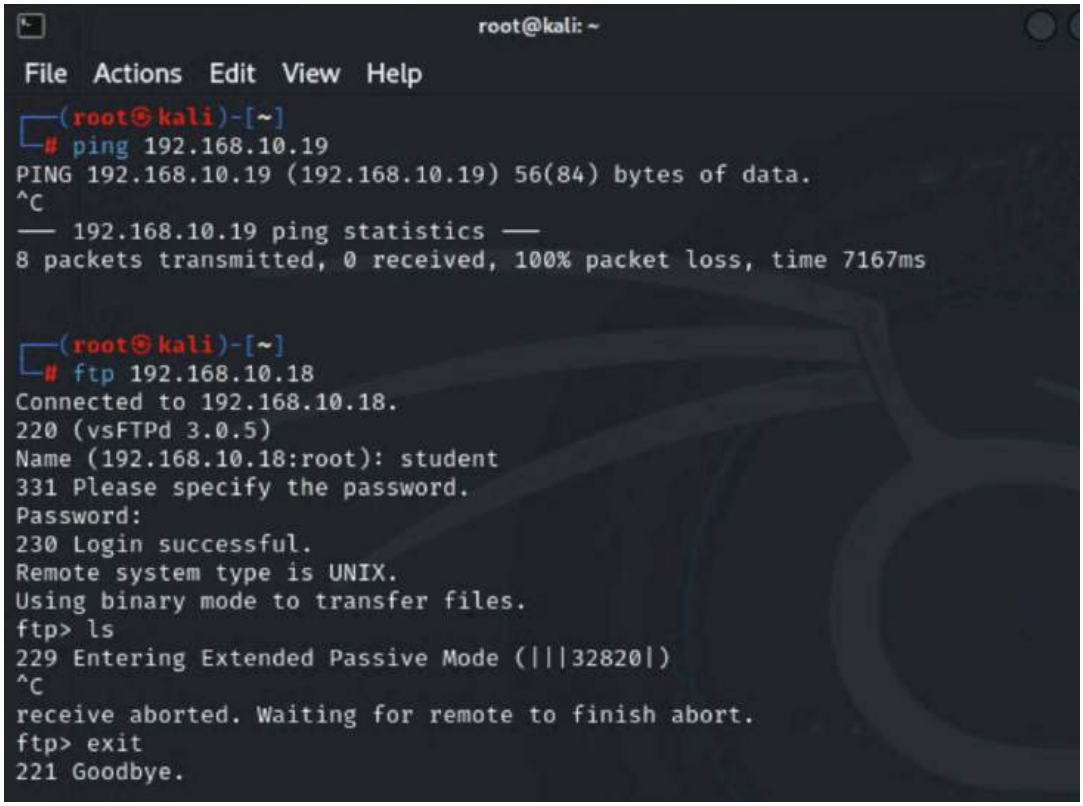
2.

Rule#	Interface	Action	Source IP	Destination IP	Protocol
2	WAN	Block	192.168.217.3	LAN Subnet	ICMP

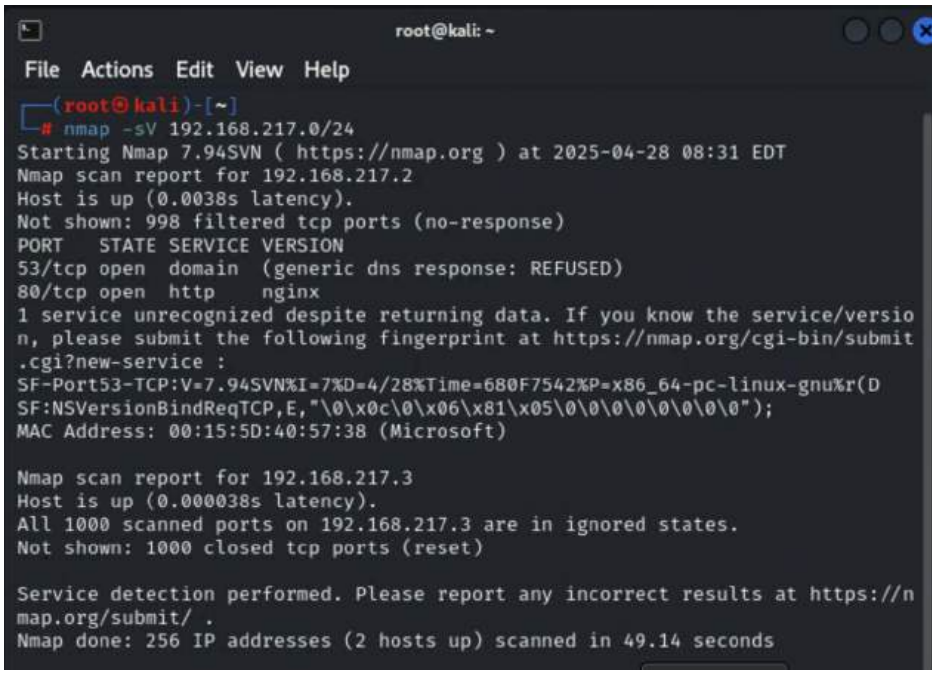


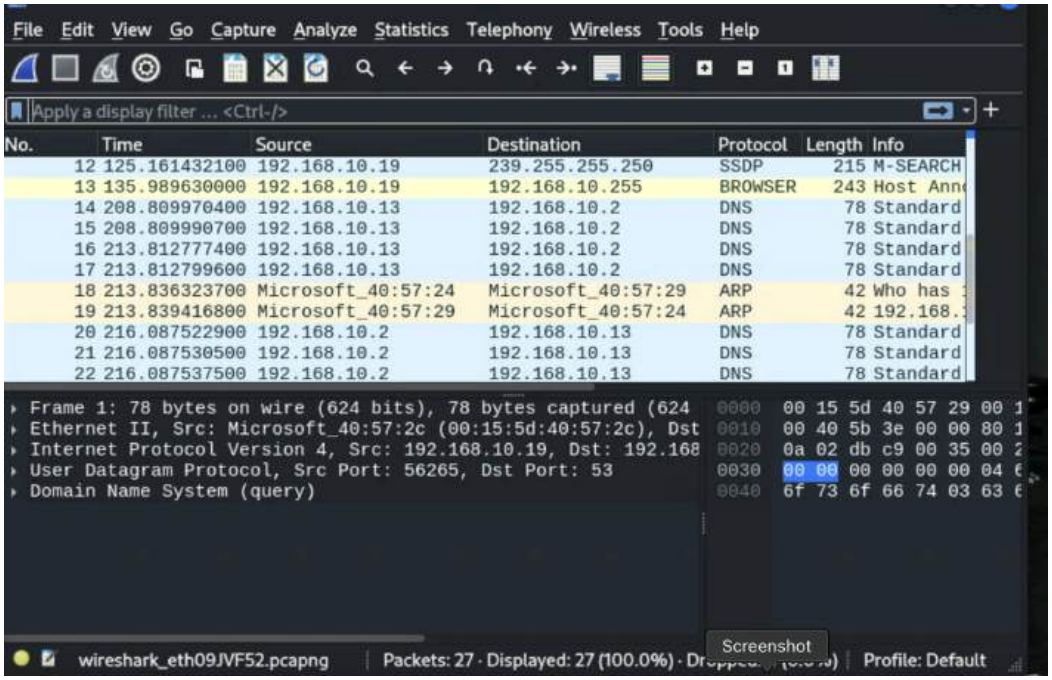
3.

Rule#	Interface	Action	Source IP	Destination IP	Protocol
3	WAN	Allow	192.168.217.3	192.168.10.18	FTP(21)
4	WAN	Block	192.168.217.3	LAN Subnet	Any


root@kali: ~
File Actions Edit View Help
(root㉿kali)-[~]
ping 192.168.10.19
PING 192.168.10.19 (192.168.10.19) 56(84) bytes of data.
^C
— 192.168.10.19 ping statistics —
8 packets transmitted, 0 received, 100% packet loss, time 7167ms
(root㉿kali)-[~]
ftp 192.168.10.18
Connected to 192.168.10.18.
220 (vsFTPd 3.0.5)
Name (192.168.10.18:root): student
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||32820|)
^C
receive aborted. Waiting for remote to finish abort.
ftp> exit
221 Goodbye.

4.


root@kali: ~
File Actions Edit View Help
(root㉿kali)-[~]
nmap -sV 192.168.217.0/24
Starting Nmap 7.94SVN (https://nmap.org) at 2025-04-28 08:31 EDT
Nmap scan report for 192.168.217.2
Host is up (0.0038s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
53/tcp open domain (generic dns response: REFUSED)
80/tcp open http nginx
1 service unrecognized despite returning data. If you know the service/versio
n, please submit the following fingerprint at https://nmap.org/cgi-bin/submit
.cgi?new-service :
SF-Port53-TCP:V=7.94SVN%I=7%D=4/28%Time=680F7542%P=x86_64-pc-linux-gnu%r(D
SF:NSVersionBindReqTCP,E,"\0\x0c\0\x06\x81\x05\0\0\0\0\0\0\0");
MAC Address: 00:15:5D:40:57:38 (Microsoft)
Nmap scan report for 192.168.217.3
Host is up (0.000038s latency).
All 1000 scanned ports on 192.168.217.3 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 256 IP addresses (2 hosts up) scanned in 49.14 seconds



After applying the firewall rules, I repeated the network scan while monitoring traffic in Wireshark. Compared to the first scan, the traffic volume was much lower. In five minutes, I captured only about 27 packets, while the first scan had hundreds of packets including ARP, DHCP, DNS, and browser traffic. This time, I also observed SSDP (Simple Service Discovery Protocol) traffic, which was not as noticeable before. The network scan ran much slower because most of the ports were being filtered or blocked by pfSense, causing long timeouts and minimal packet exchange.