OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

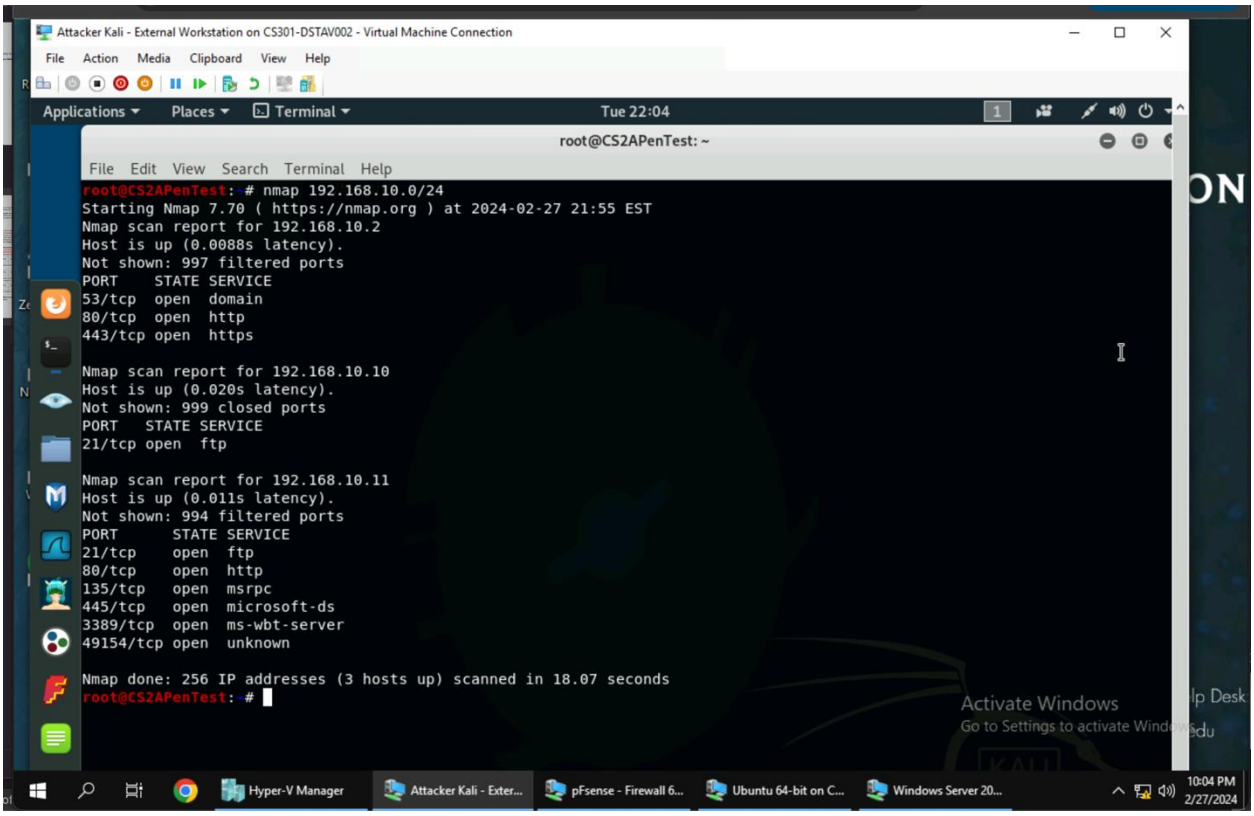
Assignment #3 Sword vs. Shield

Donte Staves

01171770

TASK A

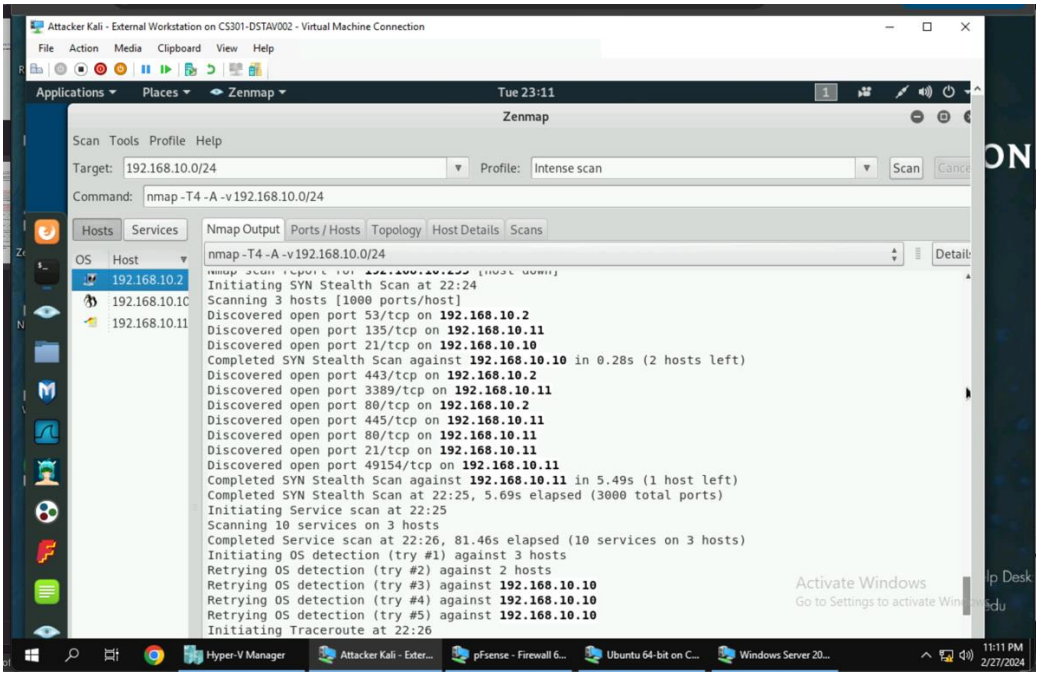
1. Use Nmap to profile the basic information about the subnet topology (including open ports information, operation systems, etc.) You need to get the service and backend software information associated with each opening port in each VM.

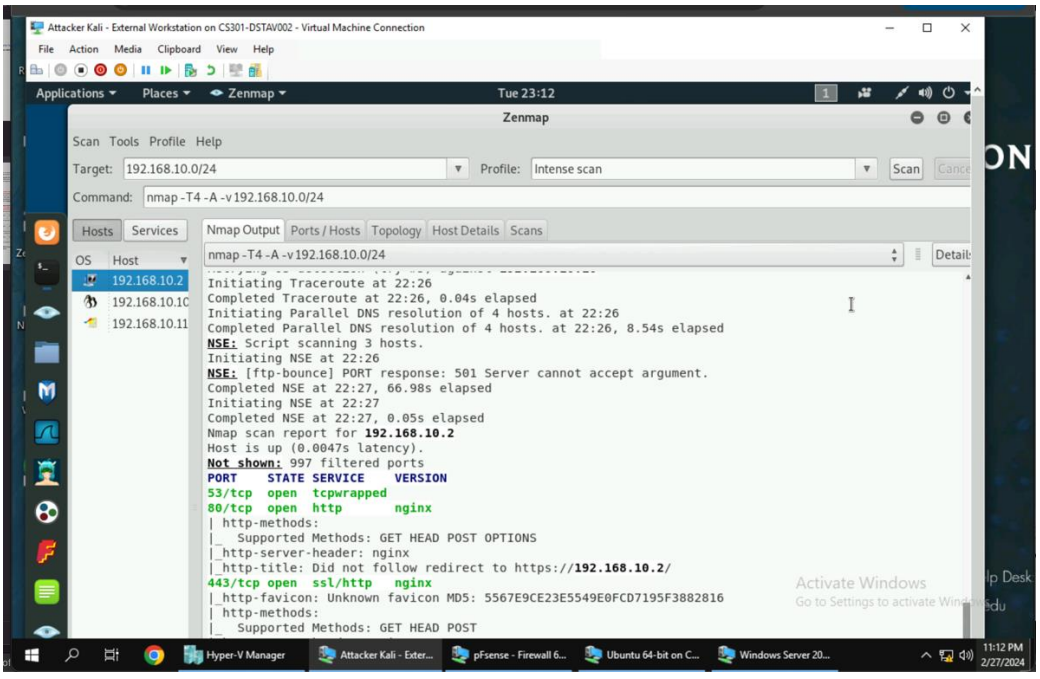


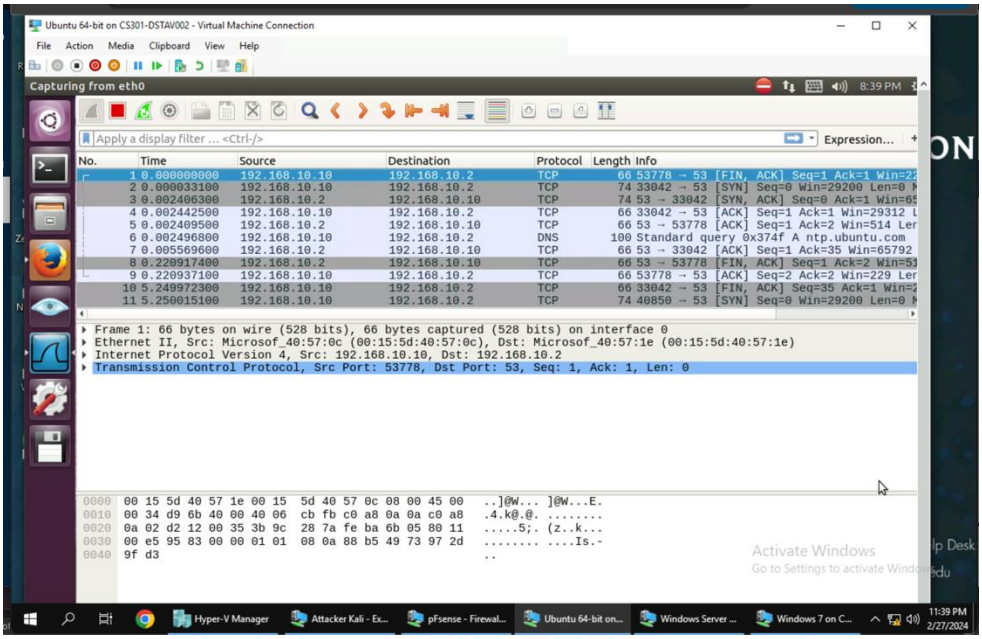
In this screenshot I used the command “nmap” followed by “192.168.10.0/24” to get the basic information about the about the subnet topology.

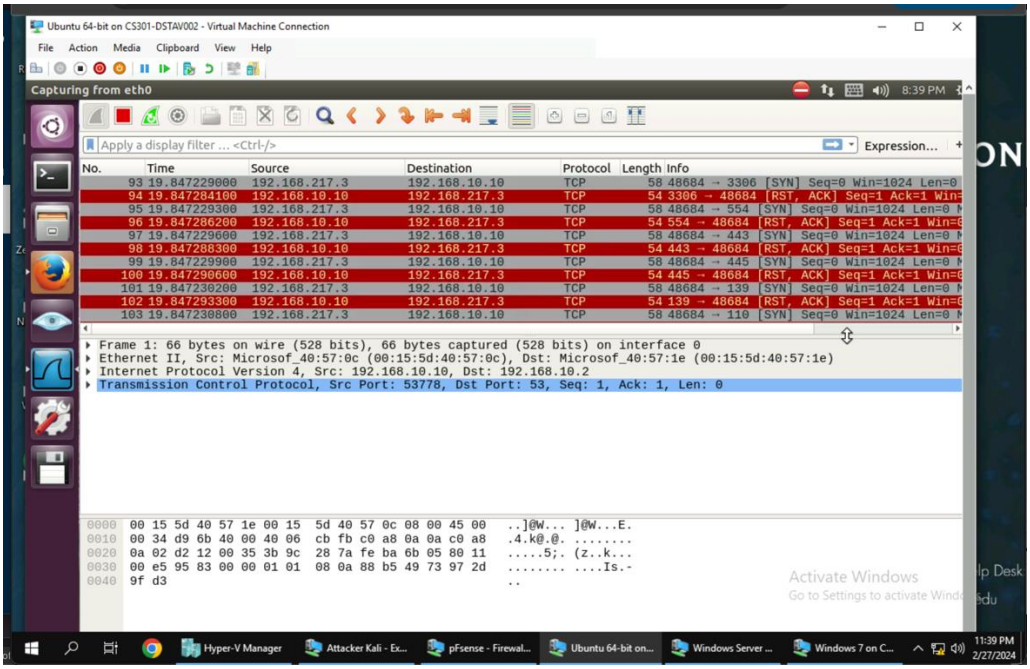
2. Run Wireshark in Ubuntu VM while External Kali is scanning the network. Discuss the traffic pattern

you observed. What do you find? Please write a 200-word essay to discuss your findings.






Ubuntu 64-bit on CS301-DSTAV002 - Virtual Machine Connection
File Action Media Clipboard View Help
Capturing from eth0
8:39 PM
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
1 0.000000000 192.168.10.10 192.168.10.2 TCP 66 53778 → 53 [FIN, ACK] Seq=1 Ack=1 Win=22
2 0.000033100 192.168.10.10 192.168.10.2 TCP 74 33042 → 53 [SYN] Seq=0 Win=29200 Len=0 M
3 0.002406300 192.168.10.2 192.168.10.10 TCP 74 53 → 33042 [SYN, ACK] Seq=0 Ack=1 Win=65
4 0.002442500 192.168.10.10 192.168.10.2 TCP 66 33042 → 53 [ACK] Seq=1 Ack=1 Win=29312 L
5 0.002409500 192.168.10.2 192.168.10.10 TCP 66 53 → 53778 [ACK] Seq=1 Ack=2 Win=514 Len
6 0.002496800 192.168.10.10 192.168.10.2 DNS 100 Standard query 0x374f A ntp.ubuntu.com
7 0.005569600 192.168.10.2 192.168.10.10 TCP 66 53 → 33042 [ACK] Seq=1 Ack=35 Win=65792
8 0.220917400 192.168.10.2 192.168.10.10 TCP 66 53 → 53778 [FIN, ACK] Seq=1 Ack=2 Win=51
9 0.220937100 192.168.10.10 192.168.10.2 TCP 66 53778 → 53 [ACK] Seq=2 Ack=2 Win=229 Len
10 5.249972300 192.168.10.10 192.168.10.2 TCP 66 33042 → 53 [FIN, ACK] Seq=35 Ack=1 Win=2
11 5.250015100 192.168.10.10 192.168.10.2 TCP 74 40850 → 53 [SYN] Seq=0 Win=29200 Len=0 M
Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: Microsof_40:57:0c (00:15:5d:40:57:0c), Dst: Microsof_40:57:1e (00:15:5d:40:57:1e)
Internet Protocol Version 4, Src: 192.168.10.10, Dst: 192.168.10.2
Transmission Control Protocol, Src Port: 53778, Dst Port: 53, Seq: 1, Ack: 1, Len: 0
0000 00 15 5d 40 57 1e 00 15 5d 40 57 0c 08 00 45 00 ..]@W...]@W...E.
0010 00 34 d9 6b 40 00 40 06 cb fb c0 a8 0a 0a c0 a8 .4.k@.@. ....
0020 0a 02 d2 12 00 35 3b 9c 28 7a fe ba 6b 05 80 11 .....5;. (z..k...
0030 00 e5 95 83 00 00 01 01 08 0a 88 b5 49 73 97 2d ....Is.-
0040 9f d3 ..
Activate Windows
Go to Settings to activate Windows.
Hyper-V Manager
Attacker Kali - Ex...
pFsense - Firewal...
Ubuntu 64-bit on...
Windows Server ...
Windows 7 on C...
11:39 PM
2/27/2024


Ubuntu 64-bit on CS301-DSTAV002 - Virtual Machine Connection
File Action Media Clipboard View Help
Capturing from eth0
8:39 PM
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
93 19.847229000 192.168.217.3 192.168.10.10 TCP 58 48684 → 3306 [SYN] Seq=0 Win=1024 Len=0
94 19.847284100 192.168.10.10 192.168.217.3 TCP 54 3306 → 48684 [RST, ACK] Seq=1 Ack=1 Win=
95 19.847229300 192.168.217.3 192.168.10.10 TCP 58 48684 → 554 [SYN] Seq=0 Win=1024 Len=0 M
96 19.847286200 192.168.10.10 192.168.217.3 TCP 54 554 → 48684 [RST, ACK] Seq=1 Ack=1 Win=0
97 19.847229600 192.168.217.3 192.168.10.10 TCP 58 48684 → 443 [SYN] Seq=0 Win=1024 Len=0 M
98 19.847288300 192.168.10.10 192.168.217.3 TCP 54 443 → 48684 [RST, ACK] Seq=1 Ack=1 Win=0
99 19.847229900 192.168.217.3 192.168.10.10 TCP 58 48684 → 445 [SYN] Seq=0 Win=1024 Len=0 M
100 19.847290600 192.168.10.10 192.168.217.3 TCP 54 445 → 48684 [RST, ACK] Seq=1 Ack=1 Win=0
101 19.847230200 192.168.217.3 192.168.10.10 TCP 58 48684 → 139 [SYN] Seq=0 Win=1024 Len=0 M
102 19.847293300 192.168.10.10 192.168.217.3 TCP 54 139 → 48684 [RST, ACK] Seq=1 Ack=1 Win=0
103 19.847230800 192.168.217.3 192.168.10.10 TCP 58 48684 → 110 [SYN] Seq=0 Win=1024 Len=0 M
Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: Microsof_40:57:0c (00:15:5d:40:57:0c), Dst: Microsof_40:57:1e (00:15:5d:40:57:1e)
Internet Protocol Version 4, Src: 192.168.10.10, Dst: 192.168.10.2
Transmission Control Protocol, Src Port: 53778, Dst Port: 53, Seq: 1, Ack: 1, Len: 0
0000 00 15 5d 40 57 1e 00 15 5d 40 57 0c 08 00 45 00 ..]@W...]@W...E.
0010 00 34 d9 6b 40 00 40 06 cb fb c0 a8 0a 0a c0 a8 .4.k@.@. ....
0020 0a 02 d2 12 00 35 3b 9c 28 7a fe ba 6b 05 80 11 .....5;. (z..k...
0030 00 e5 95 83 00 00 01 01 08 0a 88 b5 49 73 97 2d ....Is.-
0040 9f d3 ..
Activate Windows
Go to Settings to activate Windows.
Hyper-V Manager
Attacker Kali - Ex...
pFsense - Firewal...
Ubuntu 64-bit on...
Windows Server ...
Windows 7 on C...
11:39 PM
2/27/2024

In my findings of the traffic pattern, you can see many requests occurring in the scan. The scan goes on for some time and gathers a long list of information. This information covers various things. There are two different scans occurring such as SYN Stealth scan and a service scan. You also see multiple IPs being scanned and reported. Many different ports or are being reported along with its host. There is also a traceroute present that shows 4 hosts. The scan becomes a lot more closely as it shows more TCP ports and where they are coming from. When you go to eth0 on Wireshark your standard information going through. However, when you scan Ubuntu on External Kali and go back to Wireshark you begin to see a pattern in the information where every other one is highlighted in red. This is an indication that someone is trying to scan your network. Making it so that your network is now vulnerable for information to be taken. You can also see form this information the protocol which is TCP and the length which is 54. This pattern keeps going continuously indicating that whoever it may that is scanning your network is scanning it.

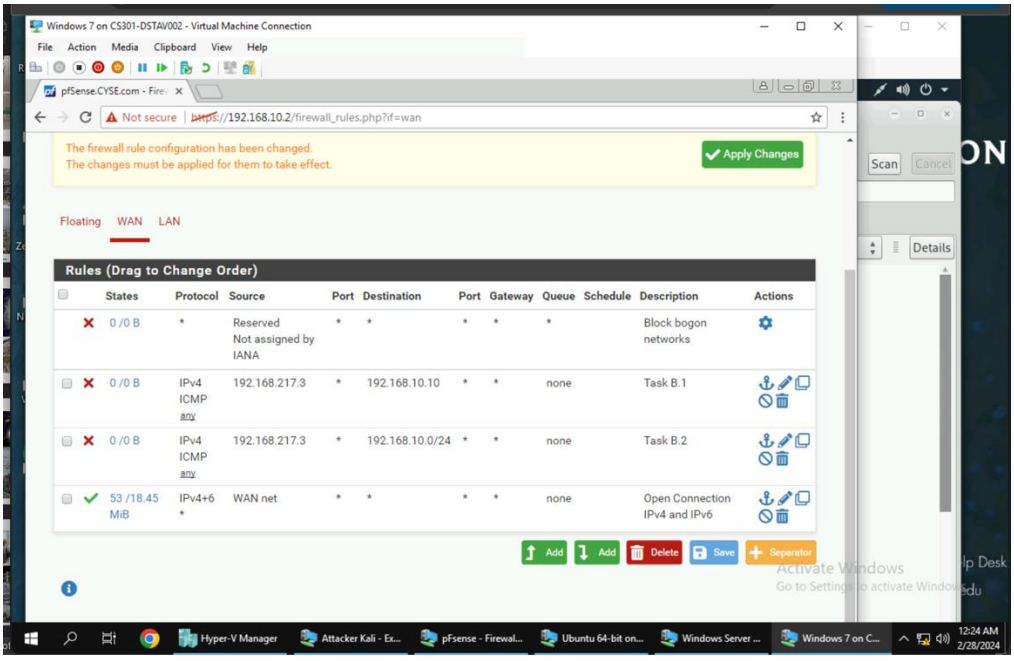
Task B

1. Configure the pfSense firewall rule to block the ICMP traffic from External Kali to Ubuntu VM.

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if applicable
1	WAN	Block	192.168.217.3	192.168.10.10	ICMP

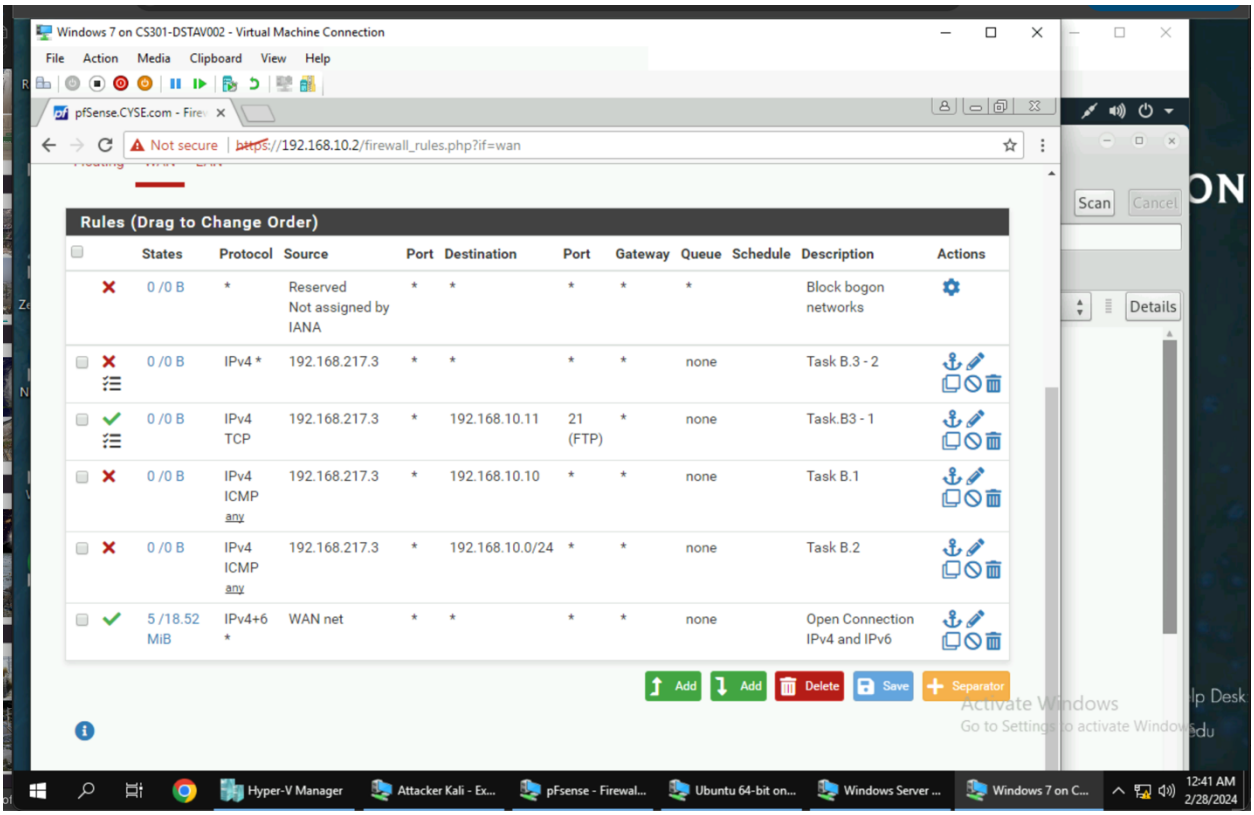
2. Clear the previous firewall policies and configure the pfSense firewall to block all ICMP traffic from External Kali to the LAN side.

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if applicable
1	WAN	Block	192.168.217.3	ALL (192.168.10.0/24)	ICMP

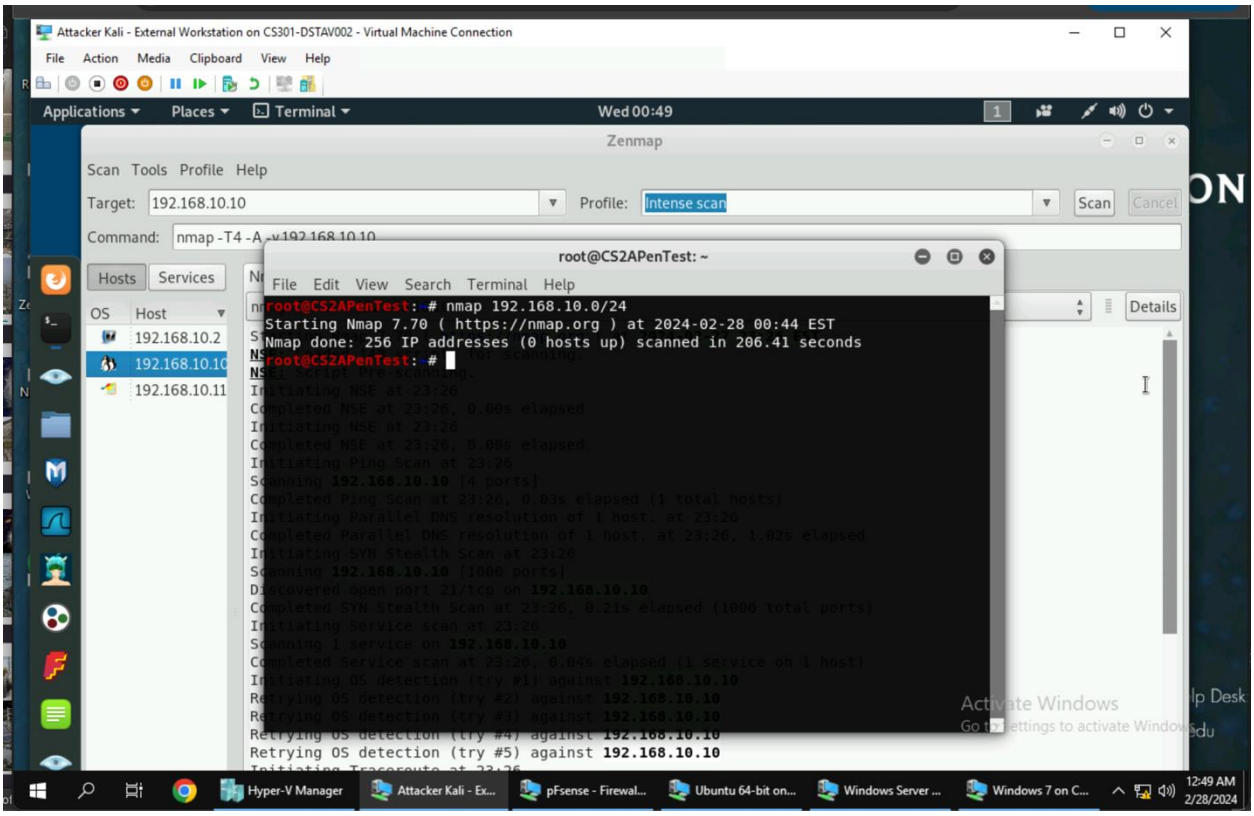


3. Clear the previous firewall policies and configure the pfSense firewall to block ALL traffic from External Kali to the LAN side, except for the FTP protocol towards Windows Server 2008.

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if applicable
1	WAN	Pass	192.168.217.3	192.168.10.11	FTP (TCP:21)
2	WAN	Block	192.168.217.3	(ALL) 192.168.10.0/24	ALL



4. Keep the firewall policies you created in Task B.3 and repeat Task A.1. What's the difference?



In this screenshot I used the command "nmap" followed by "192.168.10.0/24" as used in Task A.1, the difference is that there was no information provided about the subnet topology.