OLD DOMINION UNIVERSITY

CYSE 301: Cybersecurity Technique and Operations

Assignment: Lab 3 – Sword vs. Shield

Ammar Shamsher

01223879

In this assignment, you will act as an attacker to identify the vulnerabilities in the LAN network and a defender to apply proper countermeasures. You need to provide a screenshot for each task below.

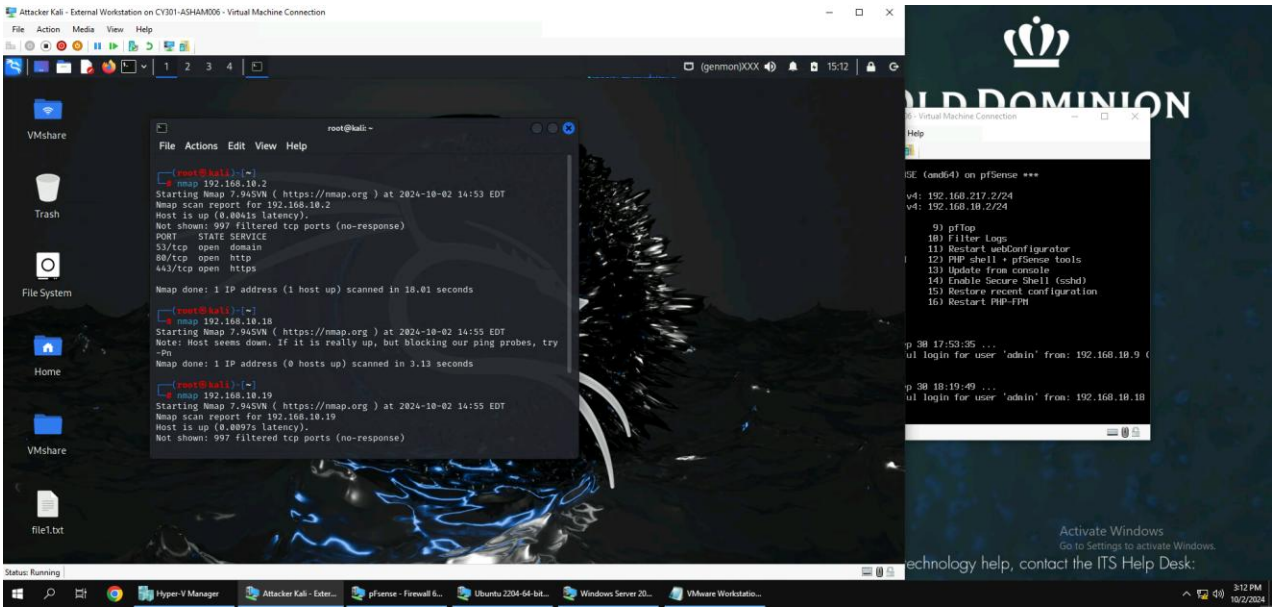
Task A: Sword - Network Scanning (20+ 20 = 40 points)

Power on the listed VMs and complete the following steps from the **External Kali** (you can use either nmap or zenmap to complete the assignment)

- External Kali
- pfSense
- Ubuntu
- Windows Server 2022

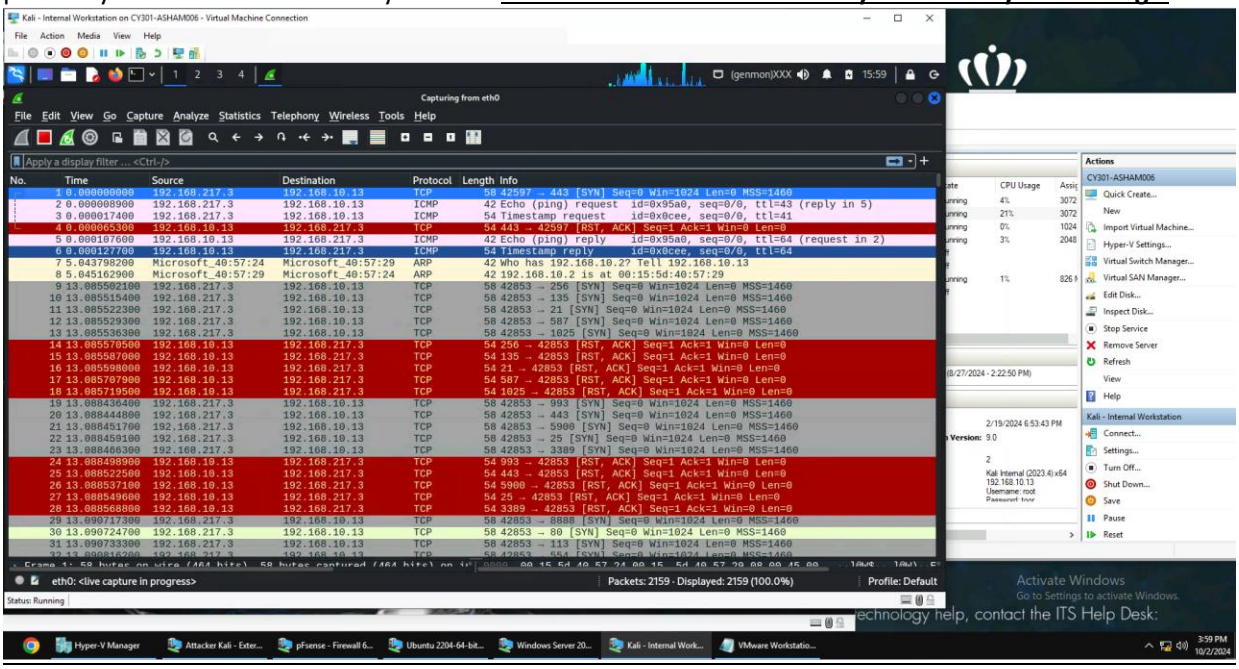
Make sure you didn't add/delete any firewall policy before continuing.

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.



I nmaped the Ubuntu, Windows Server 2022, pfSense, External Kali

2. Run Wireshark in Internal Kali 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.**



No.	Time	Source	Destination	Protocol	Length	Info
32	13.090816200	192.168.217.3	192.168.10.13	TCP	58	42853 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
33	13.090823300	192.168.217.3	192.168.10.13	TCP	58	42853 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
34	13.090830300	192.168.217.3	192.168.10.13	TCP	58	42853 → 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
35	13.090854400	192.168.10.13	192.168.217.3	TCP	54	8888 → 42853 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
36	13.090868700	192.168.10.13	192.168.217.3	TCP	54	80 → 42853 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
37	13.090879700	192.168.10.13	192.168.217.3	TCP	54	113 → 42853 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
38	13.090891300	192.168.10.13	192.168.217.3	TCP	54	554 → 42853 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
39	13.090902400	192.168.10.13	192.168.217.3	TCP	54	139 → 42853 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
40	13.090914300	192.168.10.13	192.168.217.3	TCP	54	143 → 42853 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
41	13.094683700	192.168.217.3	192.168.10.13	TCP	58	42853 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
42	13.094691100	192.168.217.3	192.168.10.13	TCP	58	42853 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
43	13.094698200	192.168.217.3	192.168.10.13	TCP	58	42853 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
44	13.094705400	192.168.217.3	192.168.10.13	TCP	58	42853 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
45	13.094727200	192.168.10.13	192.168.217.3	TCP	54	23 → 42853 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
46	13.094739600	192.168.10.13	192.168.217.3	TCP	54	1720 → 42853 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
47	13.094750400	192.168.10.13	192.168.217.3	TCP	54	8080 → 42853 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
48	13.094761800	192.168.10.13	192.168.217.3	TCP	54	22 → 42853 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
49	13.107220400	192.168.217.3	192.168.10.13	TCP	58	42853 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
50	13.107228000	192.168.217.3	192.168.10.13	TCP	58	42853 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
51	13.107235000	192.168.217.3	192.168.10.13	TCP	58	42853 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
52	13.107242200	192.168.217.3	192.168.10.13	TCP	58	42853 → 1043 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
53	13.107249200	192.168.217.3	192.168.10.13	TCP	58	42853 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
54	13.107256300	192.168.217.3	192.168.10.13	TCP	58	42853 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
55	13.107263400	192.168.217.3	192.168.10.13	TCP	58	42853 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
56	13.107270500	192.168.217.3	192.168.10.13	TCP	58	42853 → 33 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
57	13.107307200	192.168.10.13	192.168.217.3	TCP	54	199 → 42853 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
58	13.107324200	192.168.10.13	192.168.217.3	TCP	54	3306 → 42853 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
59	13.107335900	192.168.10.13	192.168.217.3	TCP	54	110 → 42853 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
60	13.107351900	192.168.10.13	192.168.217.3	TCP	54	1043 → 42853 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
61	13.107378000	192.168.10.13	192.168.217.3	TCP	54	995 → 42853 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
62	13.107388700	192.168.10.13	192.168.217.3	TCP	54	445 → 42853 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Within the two screenshots, it can be seen that there are many different sources, destinations, protocols, and the length of the info. As it can be seen there are many different protocols. There are TCP protocols which stands for Transmission Control Protocol, this is a set of rules that computers follow to send data to each other over the internet in a reliable way. This also helps break down large amounts of data into smaller pieces and send them one by one. The next one is ICMP protocols which stands for Internet Control Message Protocol. This is a network messenger that helps computers communicate with one another when something goes wrong or check if other devices are online. They can also send error messages when there are problems. The last one is ARP protocols which stand for Address Resolution Protocol. When a computer wants to send data to

another device, it knows the other device's Ip address, but it needs the device's MAC address to send the data. Something that I recognized that I haven't seen before within WireShark are the different colors in the screenshot, the red shows a malformed packet, this could be an error, such as a corrupted or incomplete packet, which means a problem in the network. And then light yellow, which is broadcast/multicast traffic packets that are sent to multiple devices in the network.

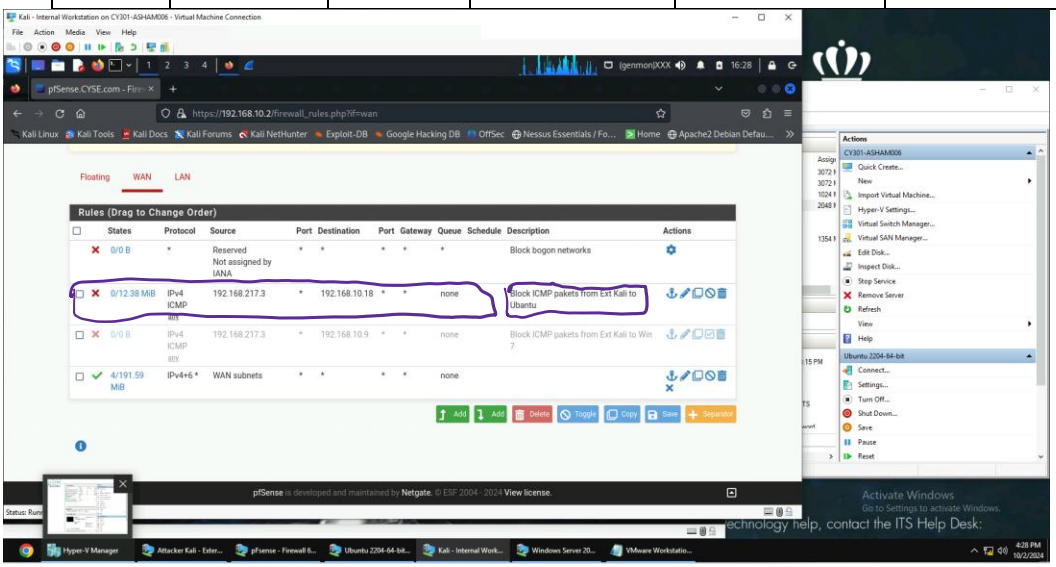
References:

***How to analyze Wireshark data*. Shure. (2022, May 20). https://service.shure.com/s/article/How-to-analyze-Wireshark-data?language=en_US#:~:text=Wireshark%20uses%20colors%20to%20help,Filtering%20Packets**

Task B: Shield – Protect your network with firewall (10 + 10+ 20 + 20 = 60 points) In order to receive full credits, you need to fill the table (add more rows if needed), implement the firewall rule(s), show me the screenshot of your firewall table, and verify the results.

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 appliable)
Rule #1	WAN	Block	192.168.217.3	192.168.10.18	ICMP

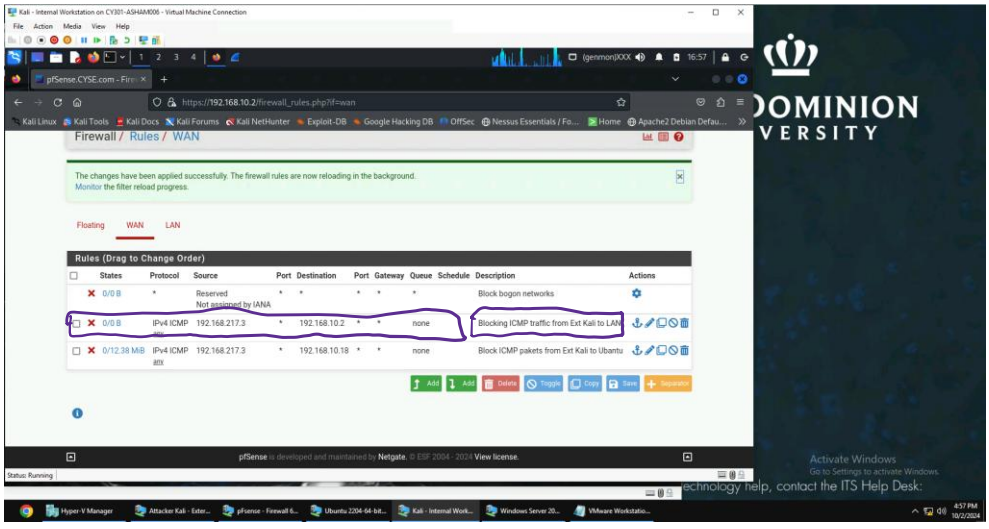


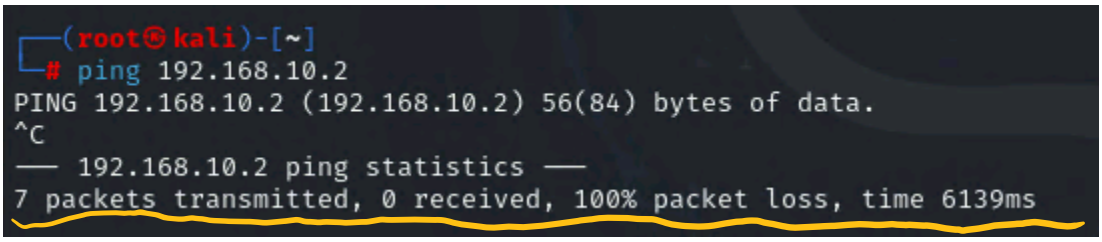
```
┌──(root㉿kali)-[~]
└─# ping 192.168.10.18
PING 192.168.10.18 (192.168.10.18) 56(84) bytes of data.
^C
── 192.168.10.18 ping statistics ──
12 packets transmitted, 0 received, 100% packet loss, time 11244ms
```

Opened a separate web browser within the VM then typed pfSense in the search, this then allows me to configure and edit the firewall rules as shown in the first screenshot. Plugging in all the information within the table above, it can be seen that we have to block ICMP traffic from External Kali to Ubuntu VM. Once that is done, the second screenshot shows that we pinged Ubuntu and that 100% (12 packets) were lost.

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 appliable)
Rule #2	WAN	Block	192.168.217.3	192.168.10.2(LAN)	ICMP

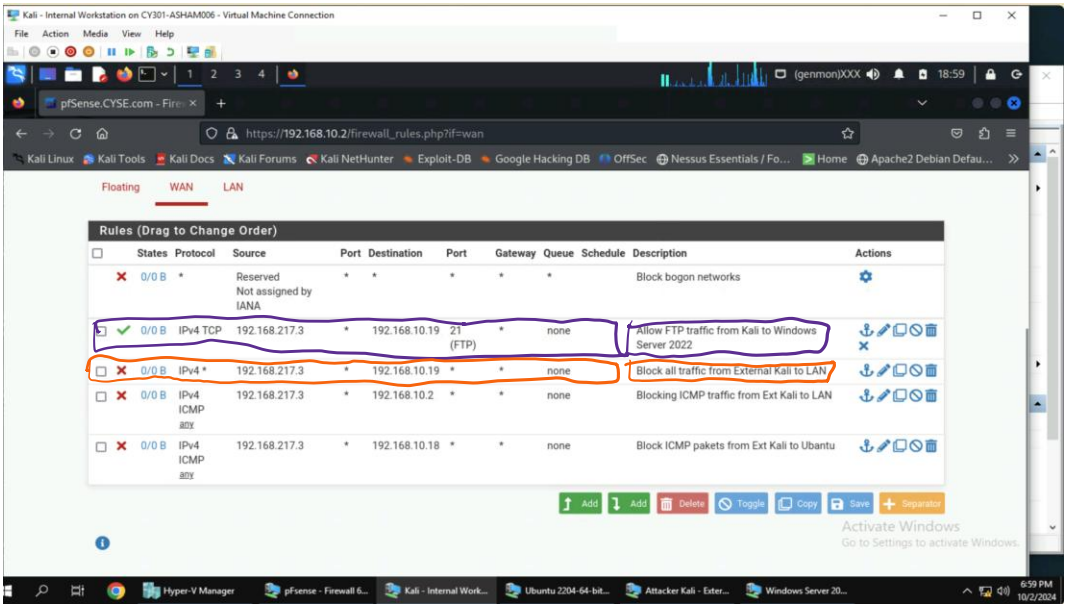




Opened a separate web browser within the VM then typed pfSense in the search, this then allows me to configure and edit the firewall rules as shown in the first screenshot. Plugging in all the information within the table above, it can be seen that we have to block ICMP traffic from External Kali to the LAN side. Once that is done, the second screenshot shows that we pinged LAN and that 100%(7 packets) were lost.

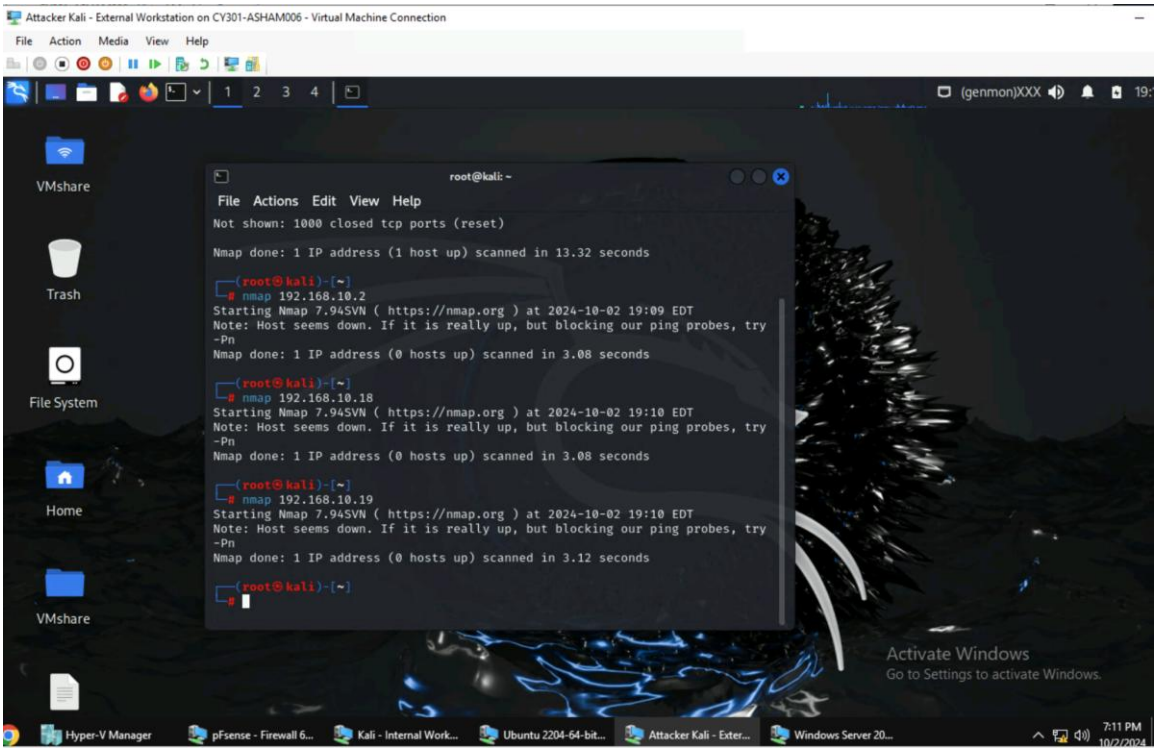
3. Clear the previous firewall policies and configure the pfSense firewall to block ALL traffic from External Kali to the LAN side, except for the FTP protocol towards Windows Server 2022.

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
Rule #1	WAN	Pass	192.168.217.3	192.168.10.19	FTP
Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
Rule #2	WAN	Block	192.168.217.3	192.168.10.19	Any



Opened a separate web browser within the VM then typed pfSense in the search, this then allows me to configure and edit the firewall rules as shown in the first screenshot. Plugging in all the information within the table above, it can be seen that we are asked to block all traffic from External Kali to the LAN side, except for FTP towards Windows Server 2022.

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



The difference is that it's blocking off all traffic coming and going.