CYSE 301: Cybersecurity Technique and Operations

Assignment 3: Sword vs. Shield

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.

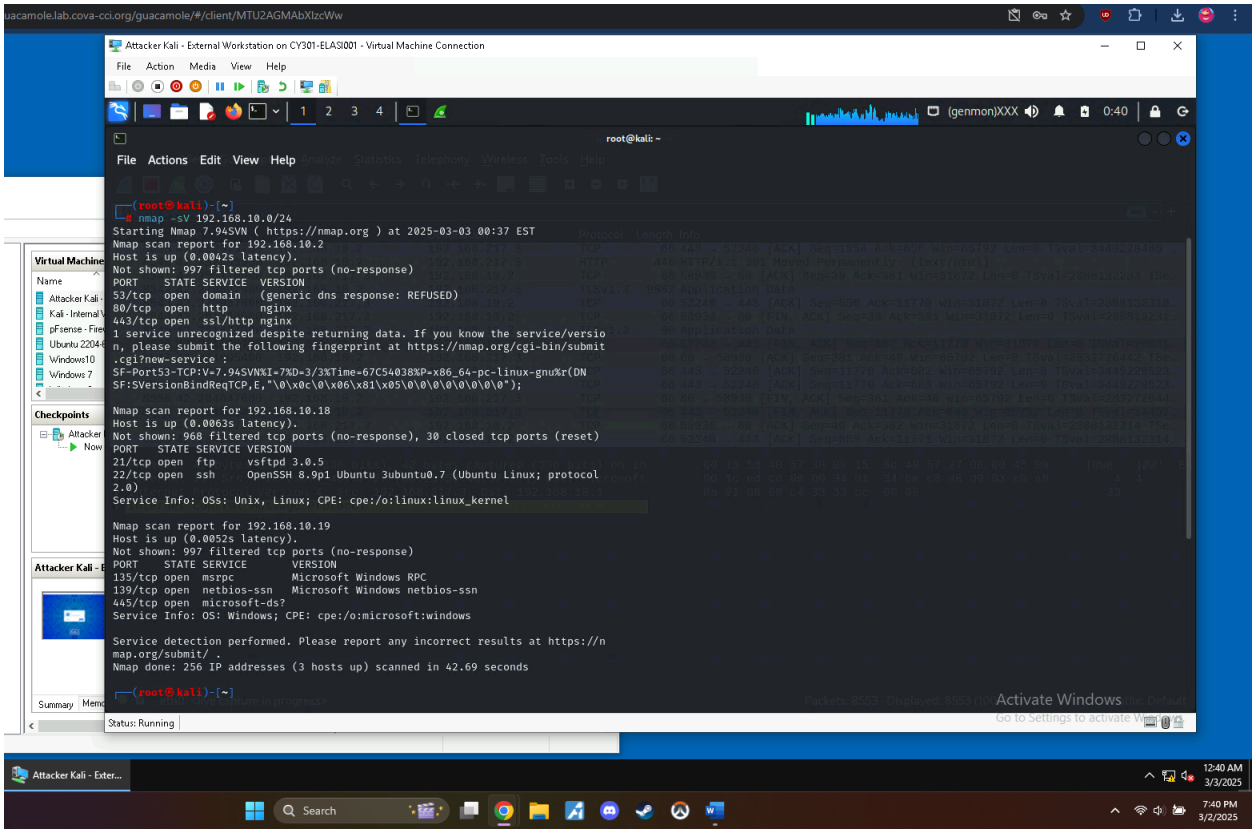
Task A: Sword - Network Scanning (20+ 20 = 40 points)

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

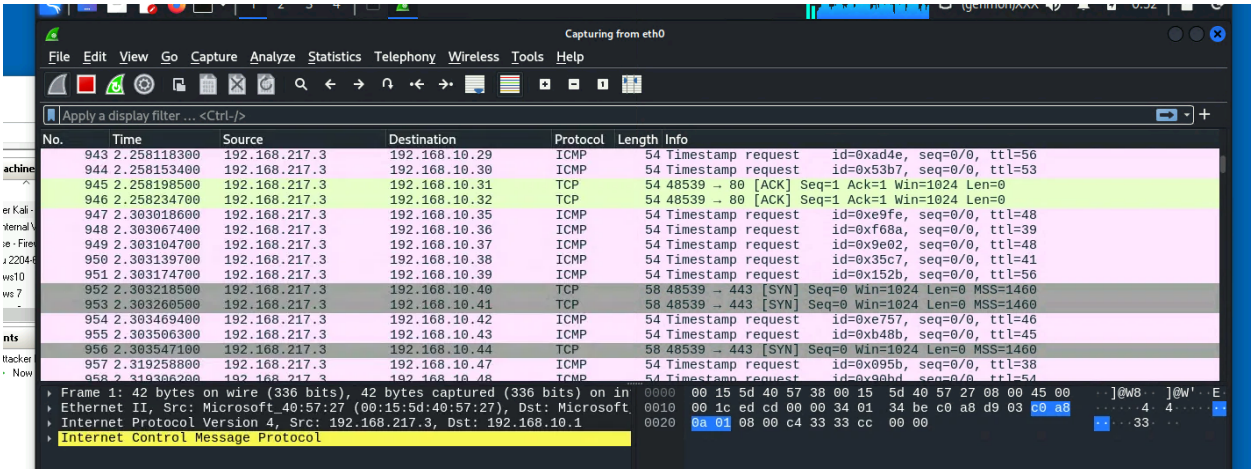
Make sure you didn't add/delete any firewall policy before continuing.

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.



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.**

Wireshark captured about 8,500 packets, most of which seems to be ICMP and TCP data. In the later packets, it was showing that common port numbers like port 445 and port 80 were being scanned, which I'm assuming was to gather the data of what services were running on those ports.



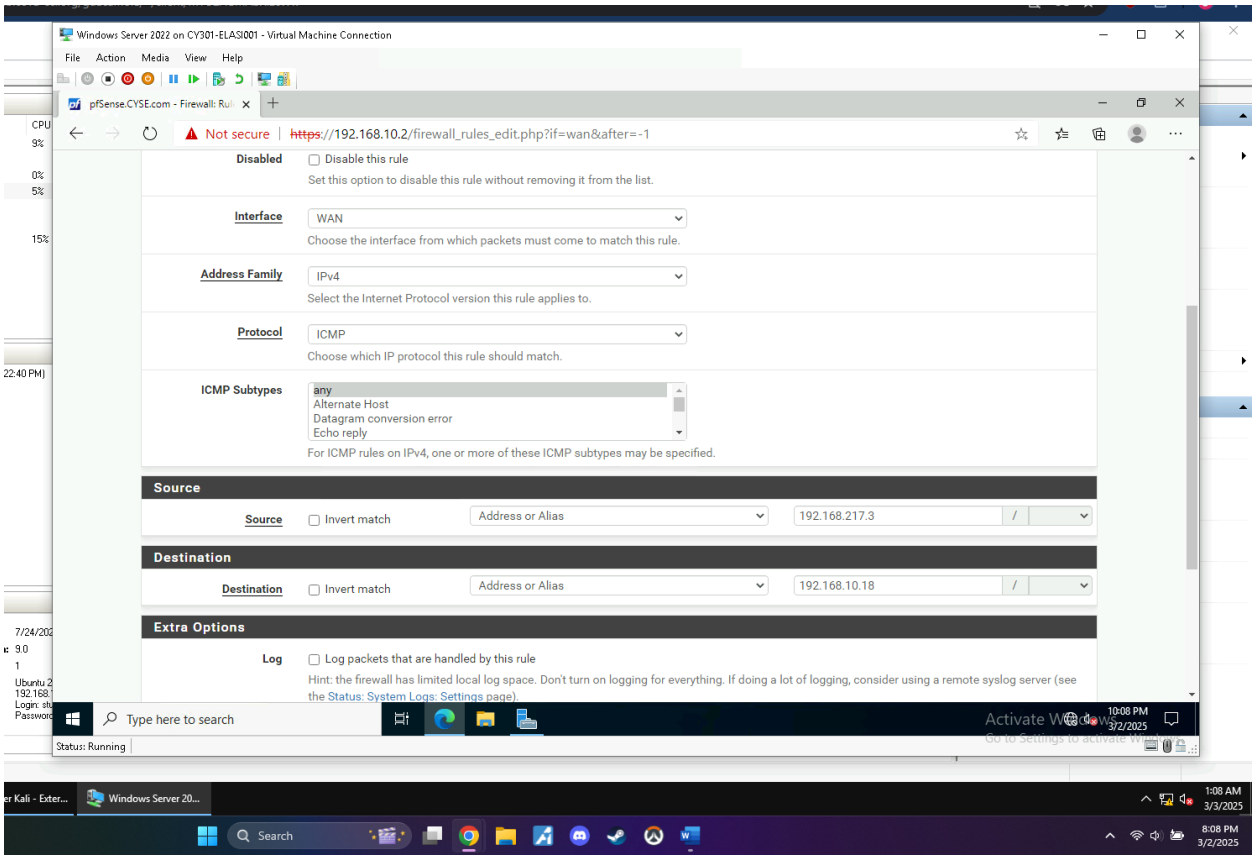
Task B: Shield – Protect your network with a firewall (10 + 10+ 20 + 20 = 60 points)

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.

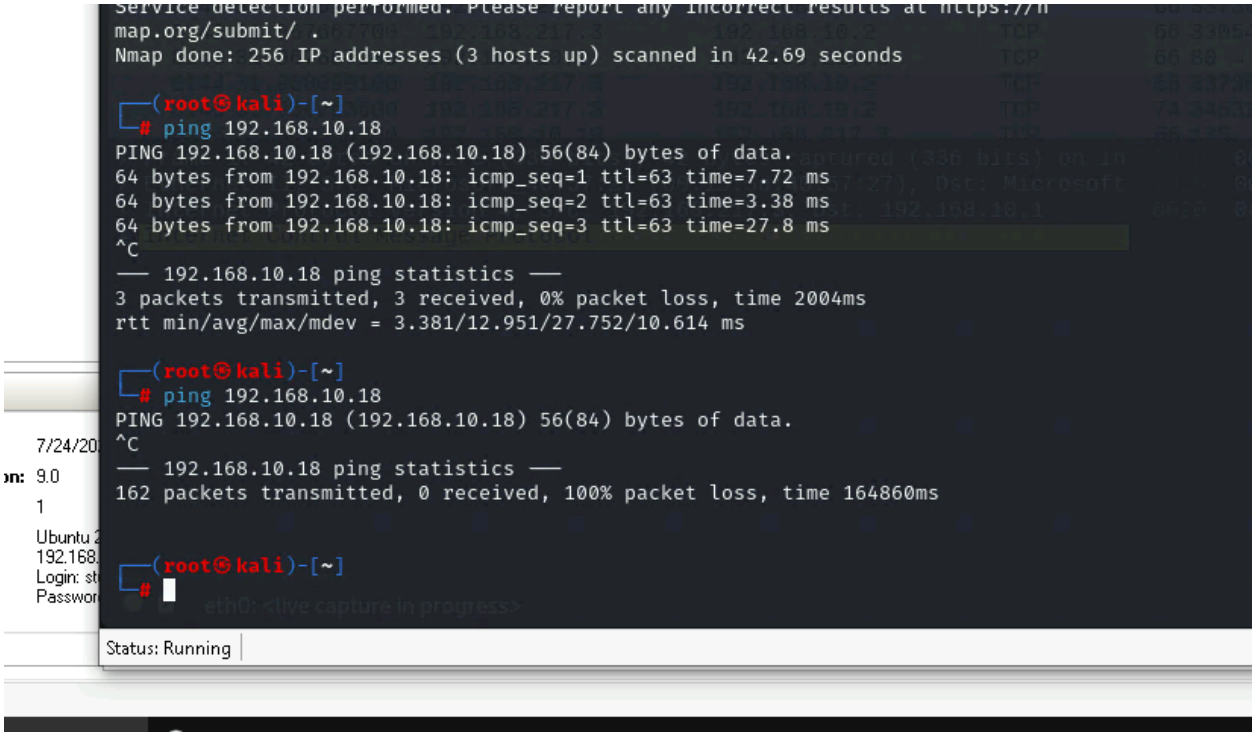
1. Configure the pfSense firewall rule to block the ICMP traffic from External Kali to Ubuntu VM.

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
1	WAN	BLOCK	192.168.217.3	192.168.10.18	ICMP

[Add the screenshot here]



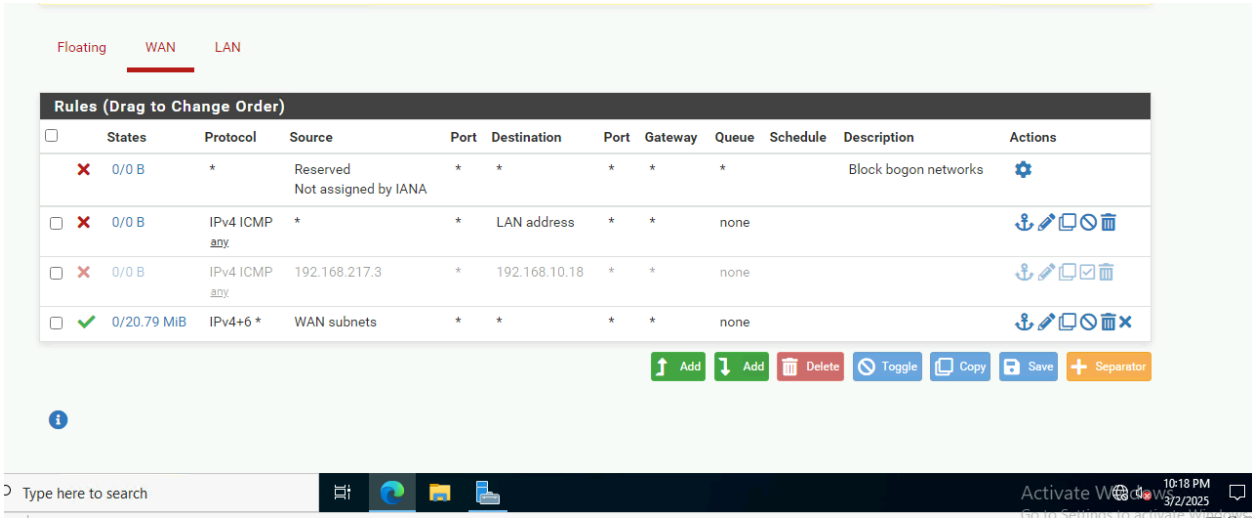
This is the before and after of applying the ICMP firewall rule:



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)
2	WAN	Block	ANY	LAN Address	

[Add the screenshot here]

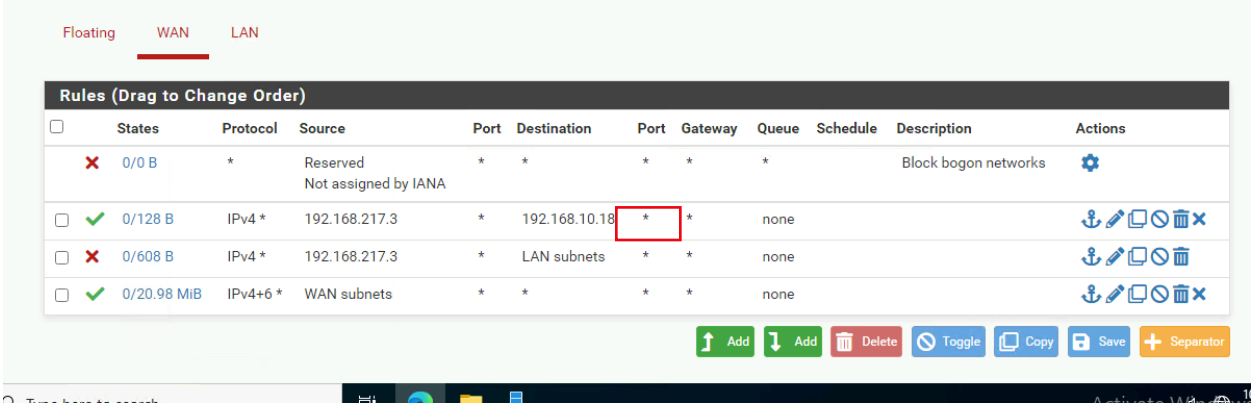


3. Clear the previous firewall policies and configure the pfSense firewall to block ALL traffic from External Kali to the LAN side, except for the FTP protocol towards Ubuntu.

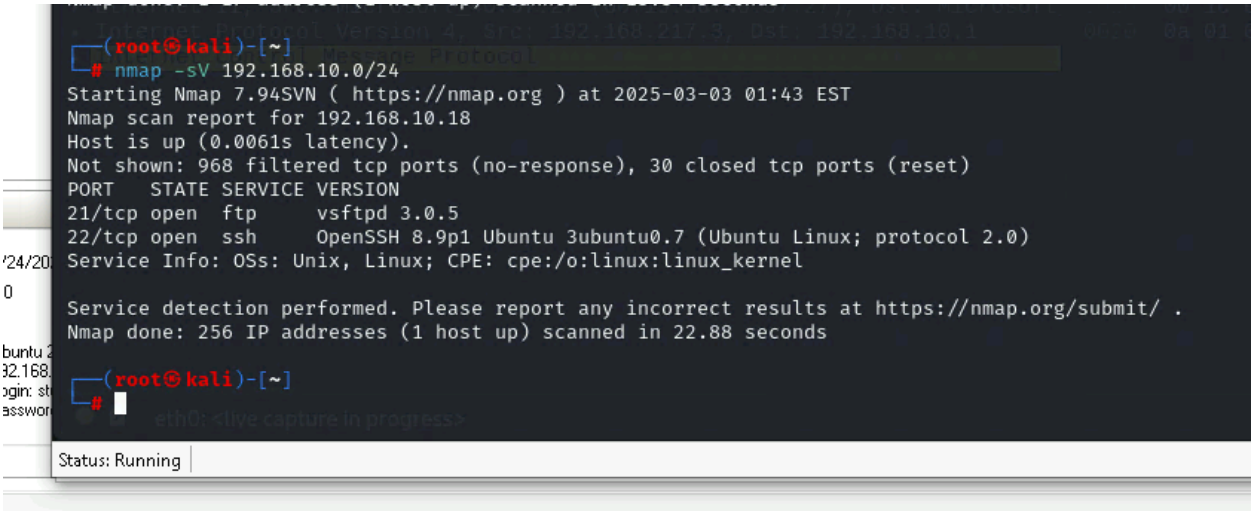
Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
1	WAN	Pass	192.168.217.3	192.168.10.18	Any, port 21
2	WAN	Block	192.168.217.3	LAN subnets	Any

[Add the screenshot here]

I made two rules, one to block all traffic, and another to specifically allow the FTP to Ubuntu.



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



With the new firewall rules, nmap couldn't find any hosts on the network except for Ubuntu, but for that one it was only able to see port 21, and for some reason port 22. I wasn't able to find out why port 22 wasn't getting blocked.

Extra credit (15 points): Use NESSUS to enumerate the security vulnerabilities of Microsoft Windows Server 2022 VM in the CCIA network.