CYSE 301: Cybersecurity Technique and Operations

Assignment 3: Sword vs. Shield

Owin Ifill

01230552

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.

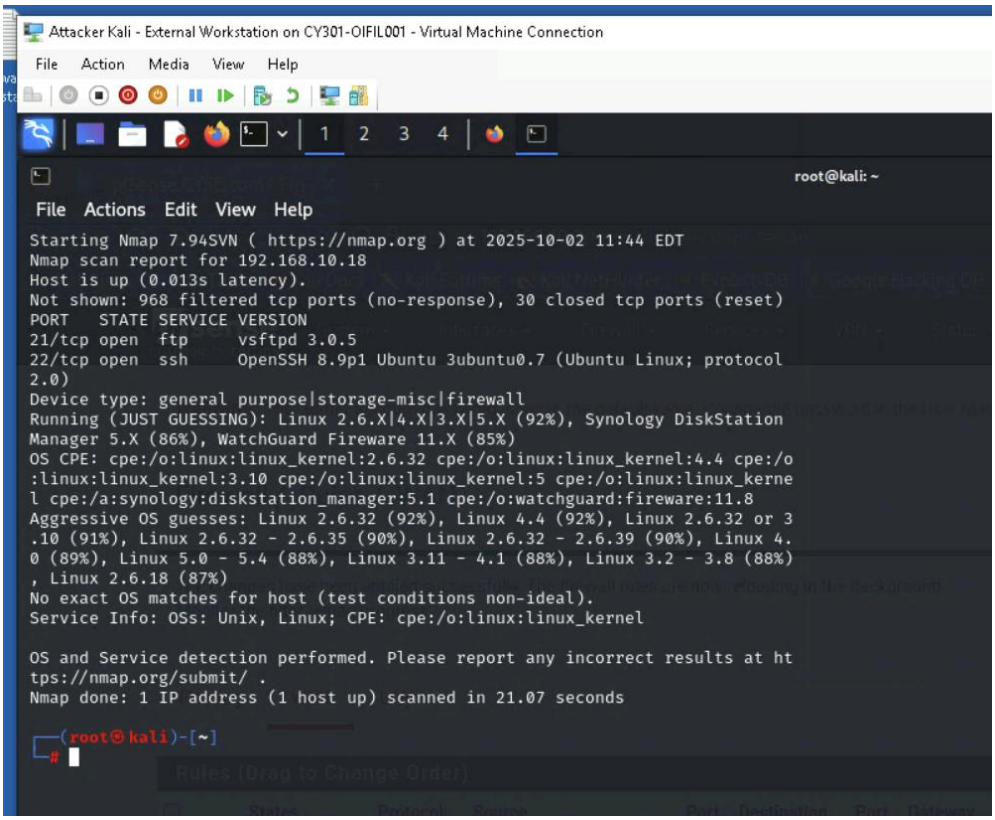
Task A: Sword - Network Scanning (20+ 20 = 40 points)

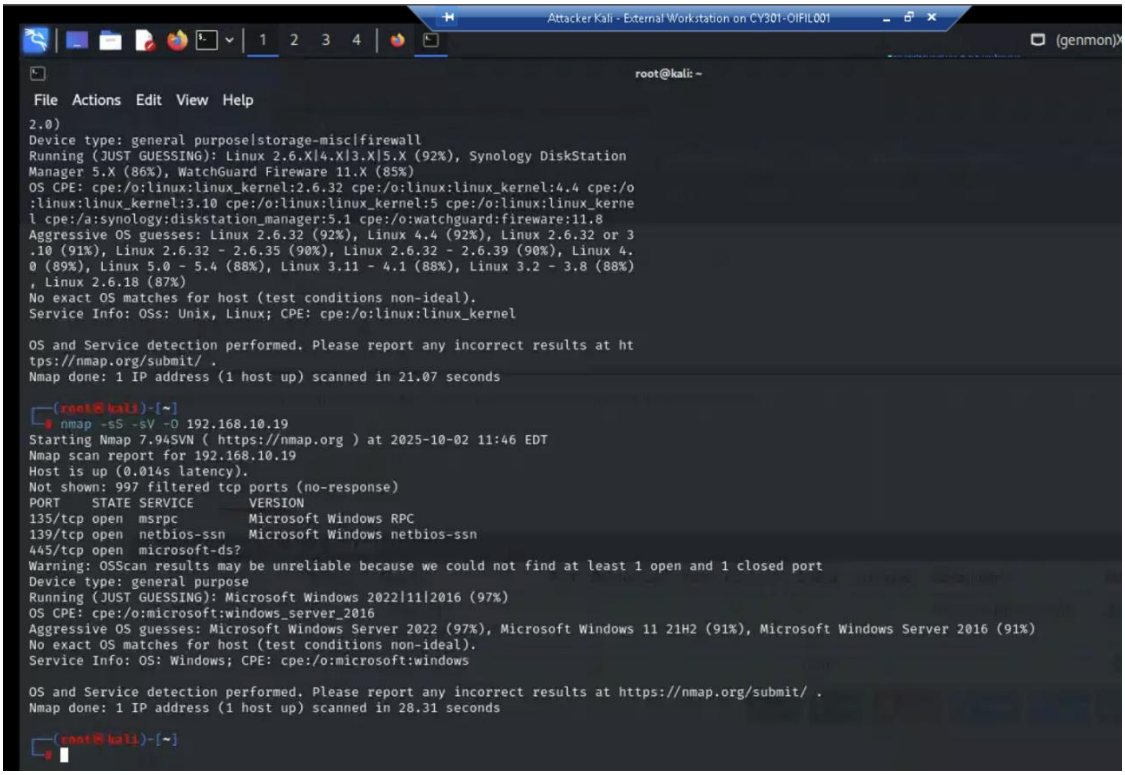
Power on the listed VMs and complete the following steps from the **External Kali** (you can use either nmap or zenmap to complete the assignment)

- 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.

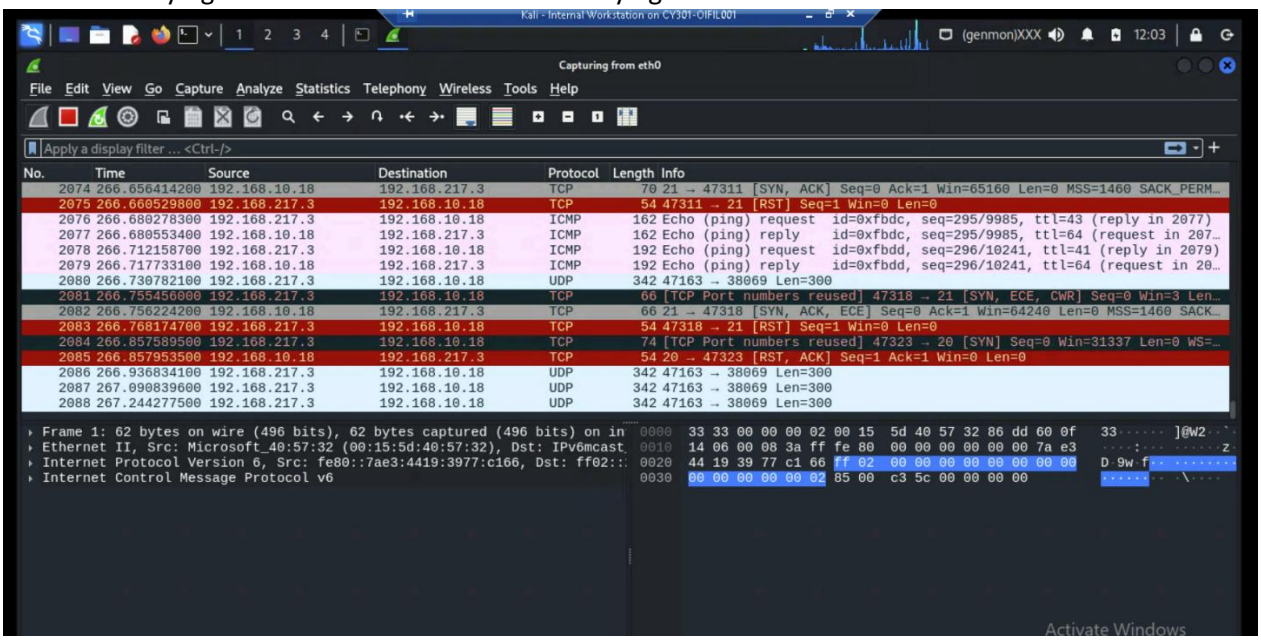




2. Run Wireshark in Internal Kali VM while External Kali is scanning the network. Discuss the traffic pattern you observed. What do you find? **Please write a 200-word essay to discuss your findings.**

When I scanned the network from the External Kali machine, I used Wireshark on the Internal Kali machine to watch the traffic. What I saw was a lot of small packets going to many different devices and ports very quickly. Most of these were TCP SYN packets, which are like the first “hello” a computer sends when trying to start a connection. The scanner sent these to many ports to check which ones would answer. I also noticed ICMP packets, which are used for things like “ping” to see if a device is online. When Nmap was checking for service versions, I saw packets with more data, like requests to web servers or SSH services. This is how Nmap learns what software and versions are running. The traffic looked different from normal network use because it was fast, repetitive, and touched many different devices and ports. This is a big clue that a scan is happening. As a defender, watching for this type of traffic can help you spot attackers early. If you see a pattern like this on your network, it likely means

someone is trying to discover weaknesses before trying to break in.

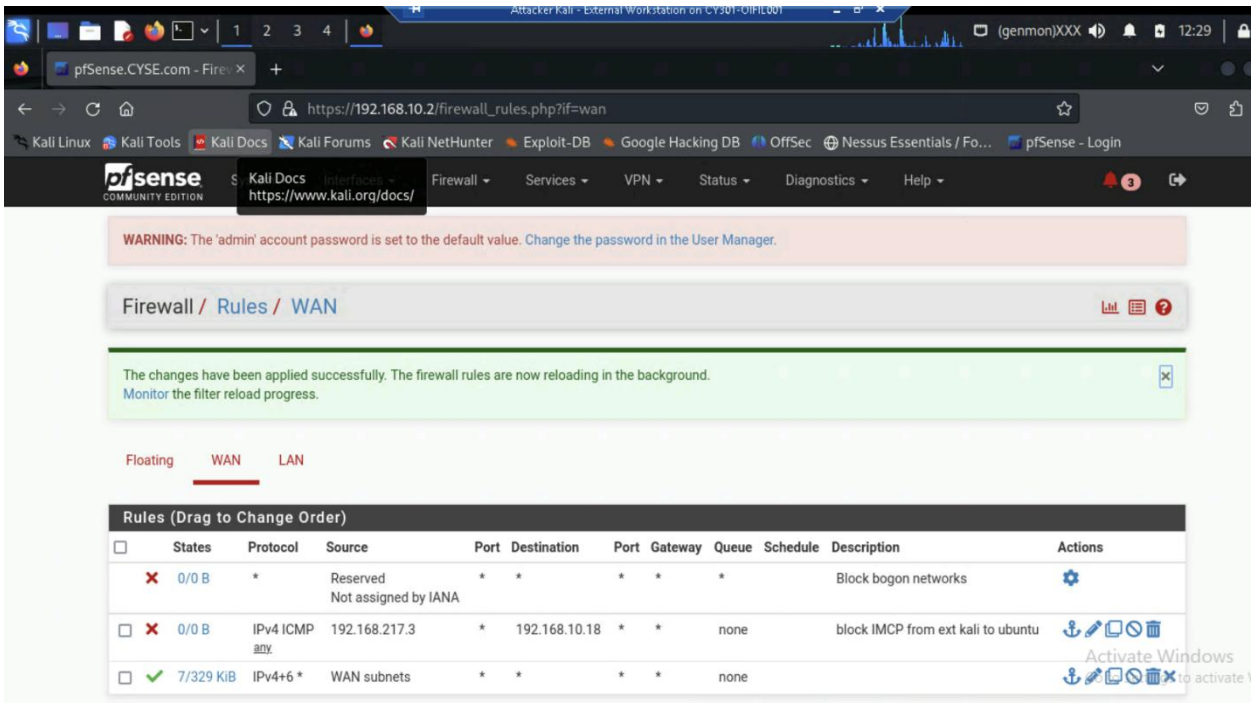


Task B: Shield – Protect your network with a firewall (10 + 10+ 20 + 20 = 60 points)

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.

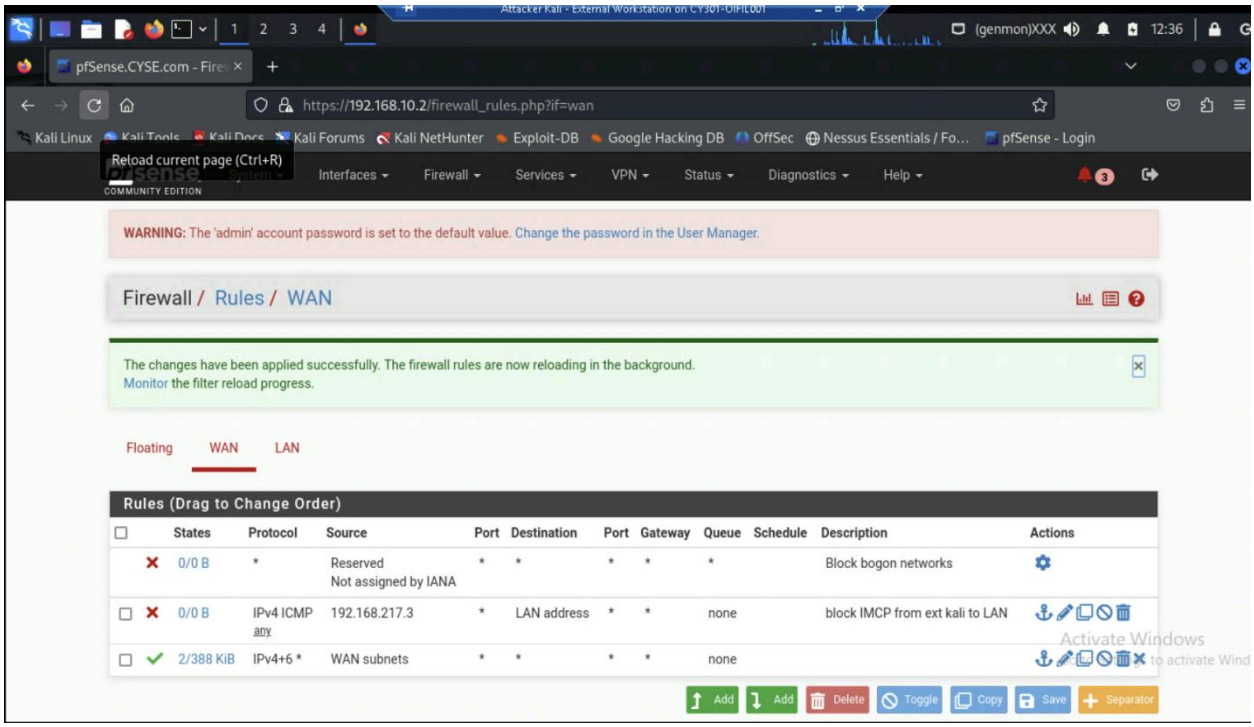
1. Configure the pfSense firewall rule to block the ICMP traffic from External Kali to Ubuntu VM.

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



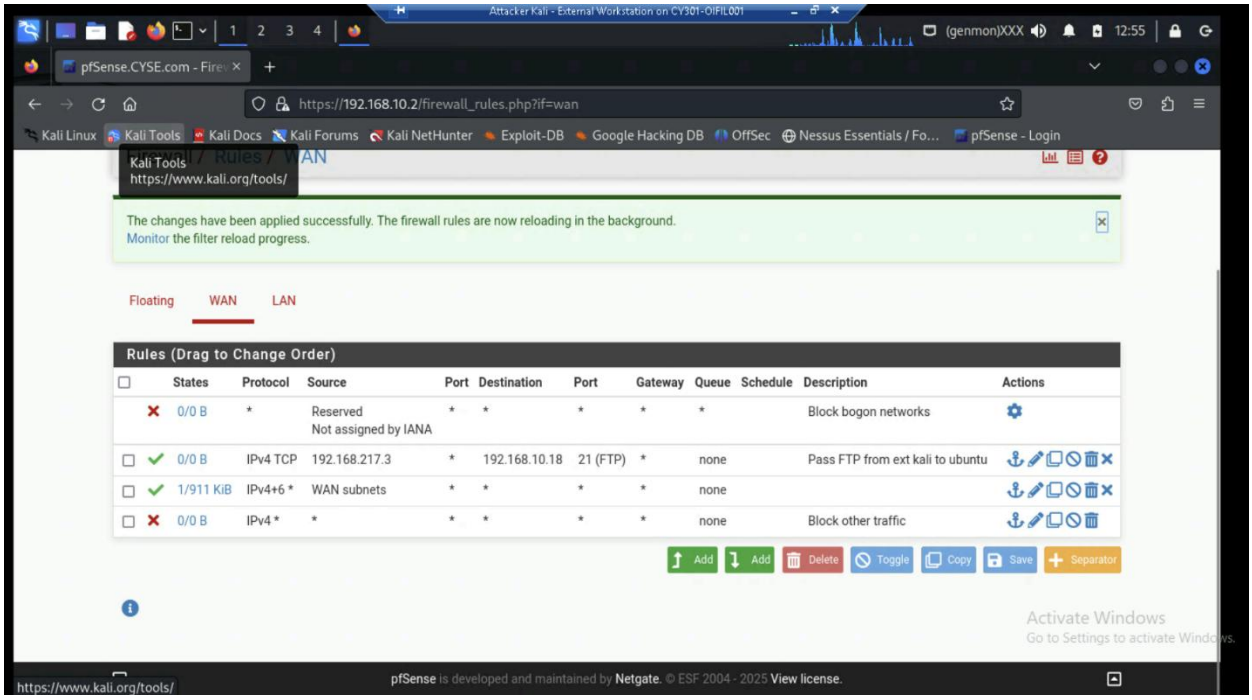
2. Clear the previous firewall policies and configure the pfSense firewall to block all ICMP traffic from External Kali to the LAN side.

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
2	WAN	Block	192.168.217.3	LAN Adress	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 Ubuntu.

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
2	WAN	Pass	192.168.217.3	192.168.10.18	21
Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
4	WAN	Block	any	any	any



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

After making the firewall rules, the results of the Nmap scan changed a lot. Previously, multiple hosts and open ports were visible, and Nmap was able to retrieve detailed service and version information. Now, with the firewall in place, the scan results were mostly empty. Only the FTP service on the Ubuntu server responded, while all other traffic from the External Kali machine was blocked. ICMP echo requests no longer received replies, so Nmap was unable to map the subnet accurately.

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