CYSE 301: Cybersecurity Technique and Operations

Assignment 3: Sword vs. Shield

Tim Klein

10/14/2024

CYSE 301

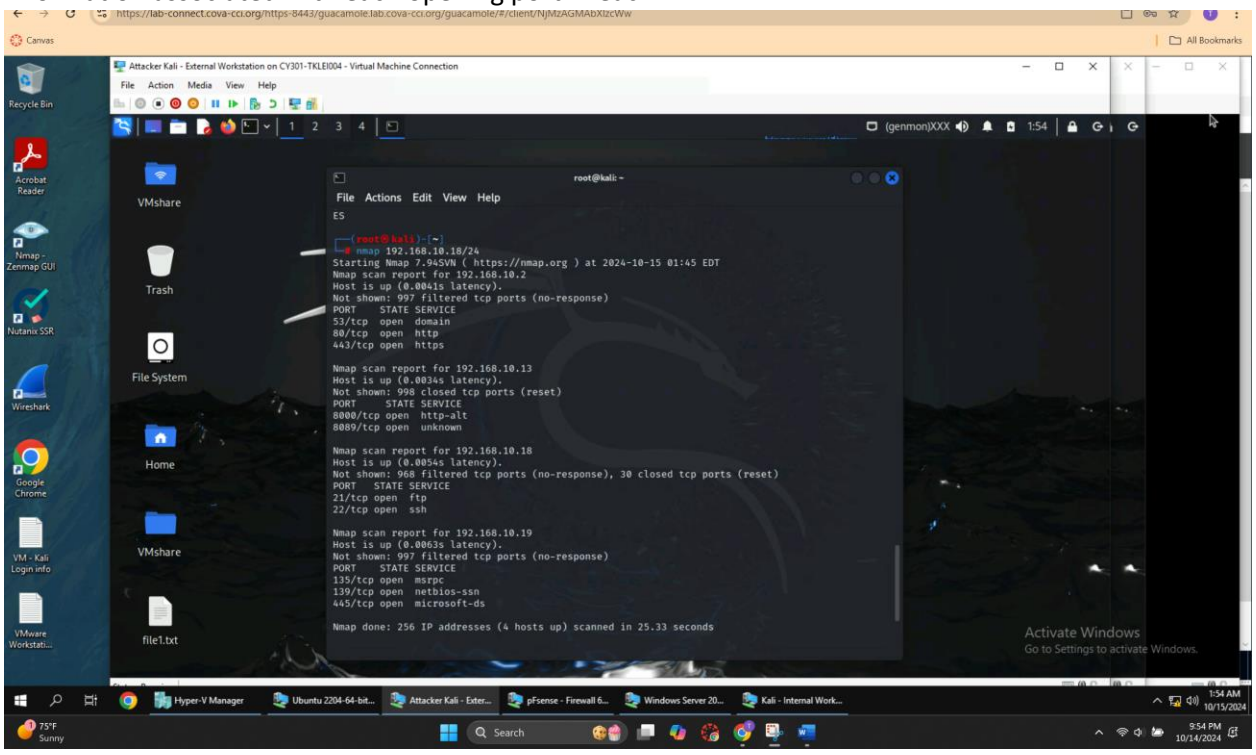
In this assignment, you will act as an attacker to identify the vulnerabilities in the LAN network and a defender to apply proper countermeasures. You need to provide a screenshot for each task below.

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.**

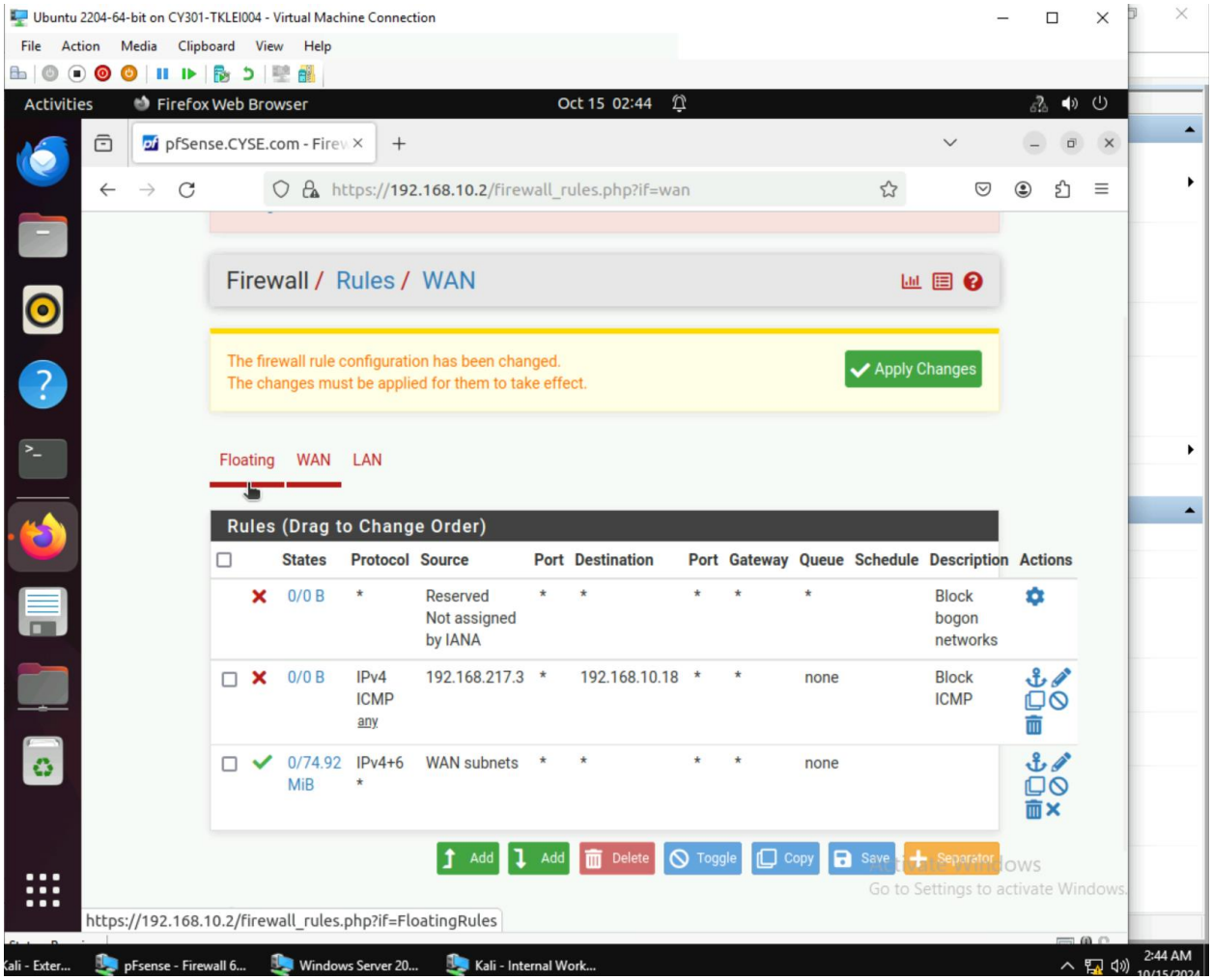
When running the Nmap scan I picked up on wireshark (on internal kali) I noticed a lot of ICMP requests coming through or basically its that the Nmap scan was pinging the network. It was trying to identify which hosts were active based on whether a response was received or not. There was also TCP SYN traffic found being done during the scan. This would be used to tell if a port was active or not based on the response, SYN ACK packets for open, RST for closed.

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.

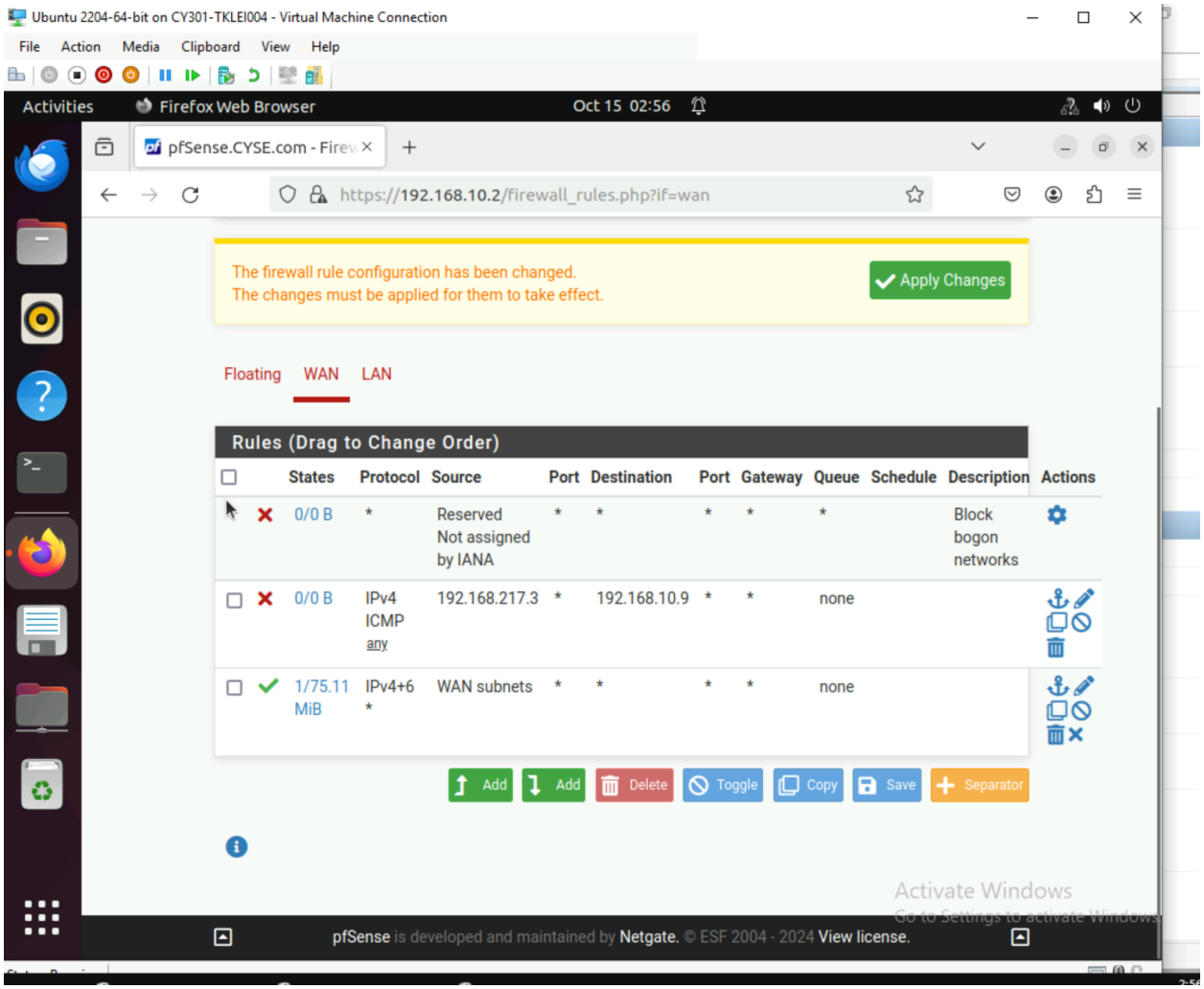
1. Configure the pfSense firewall rule to block the ICMP traffic from External Kali to Ubuntu VM.

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



2.

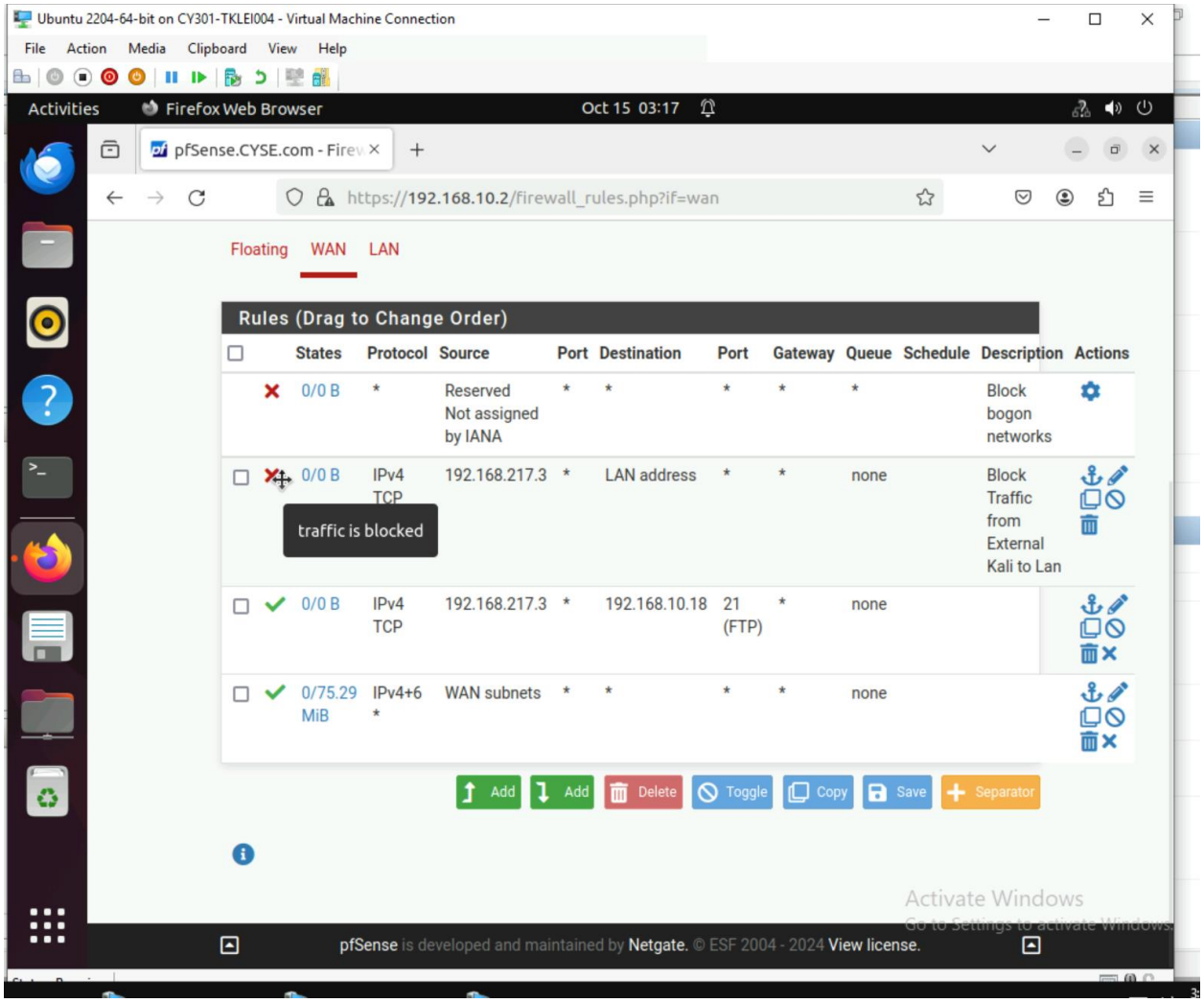
Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
Block	WAN	ICMP	192.168.217.3	192.168.10.9	Block ICMP



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)

[Add the screenshot here]



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

Only the External Kali is visible in the scan/ping.

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