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.

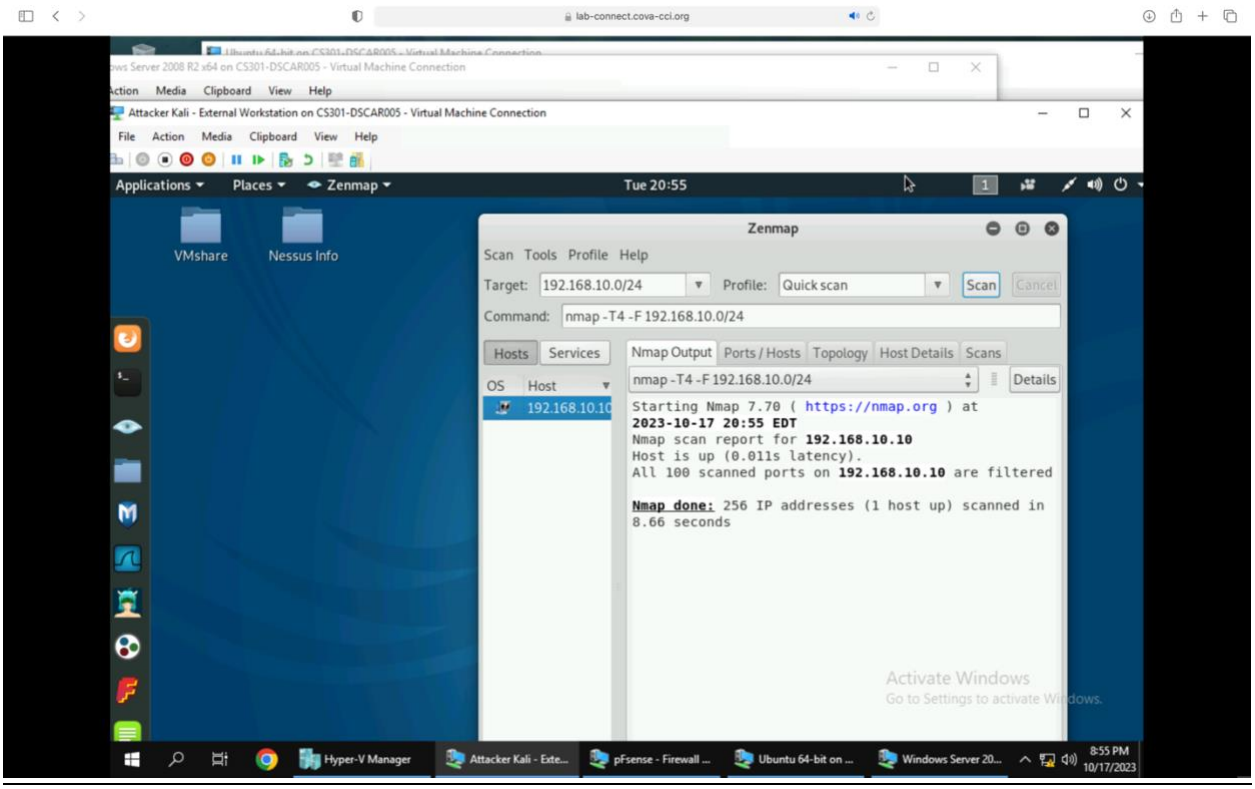
Task A: Sword - Network Scanning (20+ 20 = 40 points)

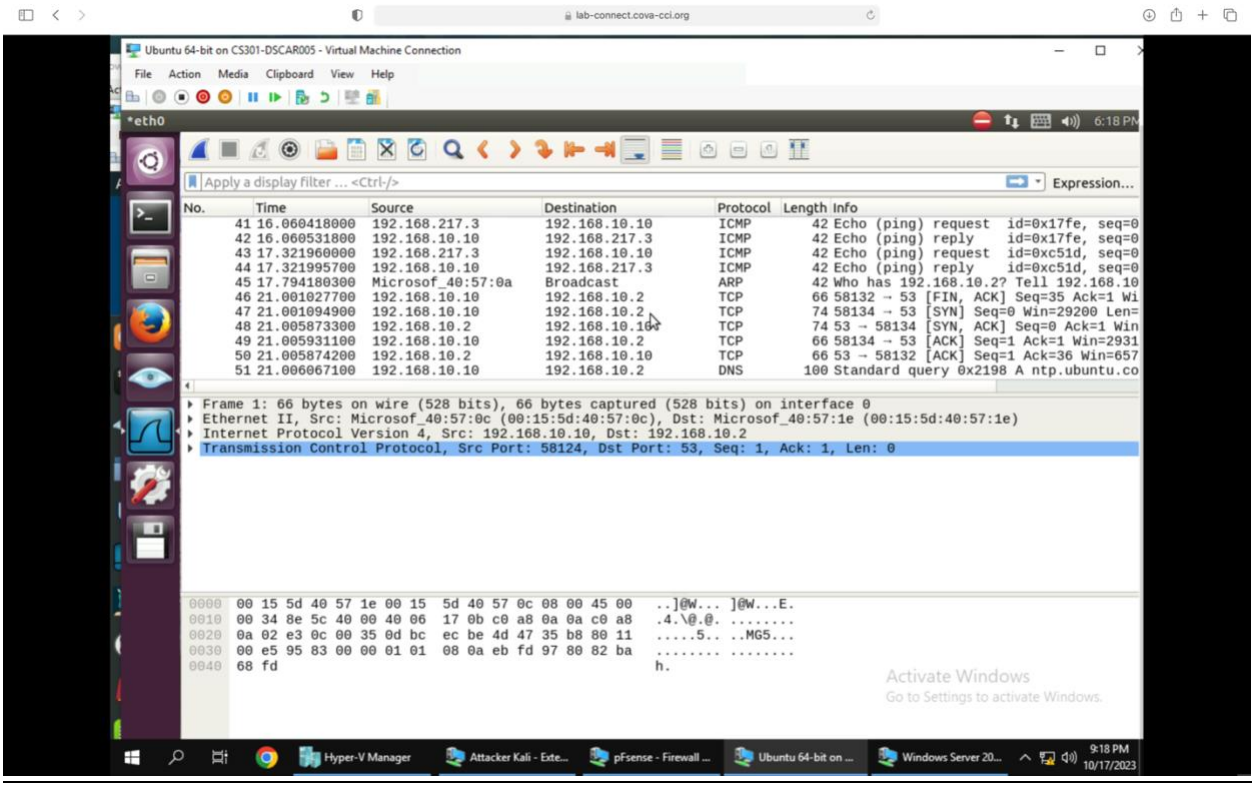
Power on the listed VMs and complete the following steps from the **External Kali** (you can use either nmap or zenmap to complete the assignment)

- External Kali
- pfSense
- Ubuntu
- Windows Server 2008

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 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.**



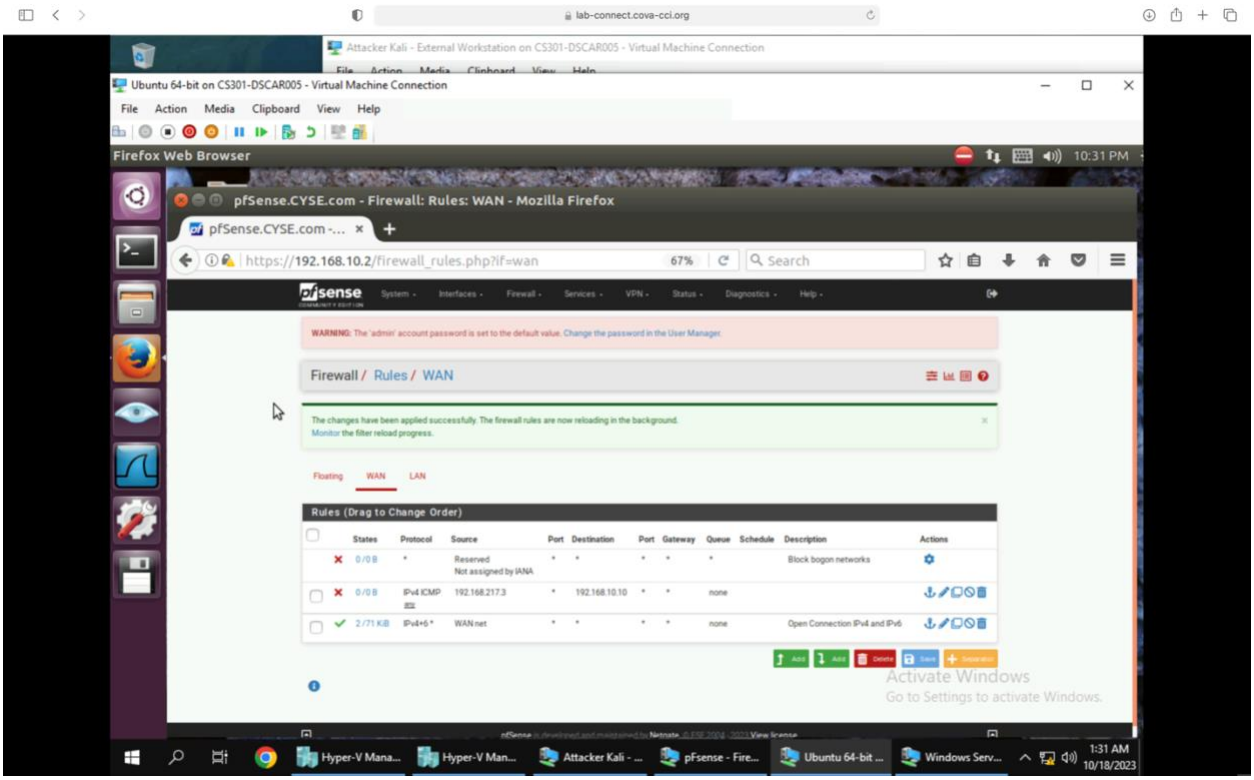


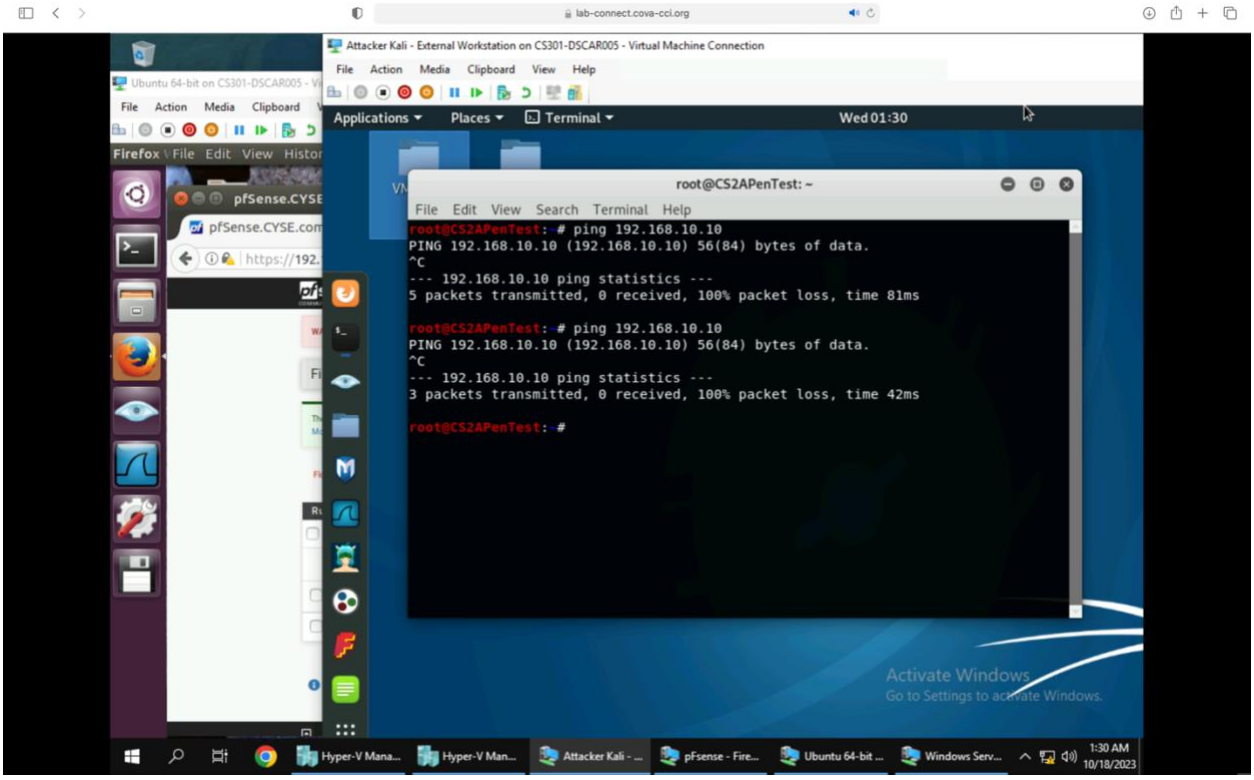
Several unusual traffic patterns were observed in the simulated scenario where Wireshark was operating in an Ubuntu Virtual Machine (VM) while an external Kali system was scanning the network. A network protocol analyzer called Wireshark provided an informative look at the dynamics of communication during the scanning process. A spike in ARP (Address Resolution Protocol) requests was instantly apparent after starting the Kali scan. The scanning system was making queries to map IP addresses to MAC addresses in an effort to find active hosts on the network. Then, a string of ICMP (Internet Control Message Protocol) echo requests—often indicative of a host scanning for live hosts—were noticed. In the reconnaissance stage of a network assault, this step is crucial. Port scanning activity were visible while the scan went on. There were a lot of TCP SYN packets, indicating an effort to connect to a variety of target machines' ports. A network's vulnerabilities or active services may be indicated by unusual or unexpected ports that are being probed. The Wireshark logs also showed an increase in HTTP requests, indicating that the scanning system was attempting to learn more about the web services available on the discovered hosts. This might entail determining web servers, versions, or even potential vulnerabilities in web applications.

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.

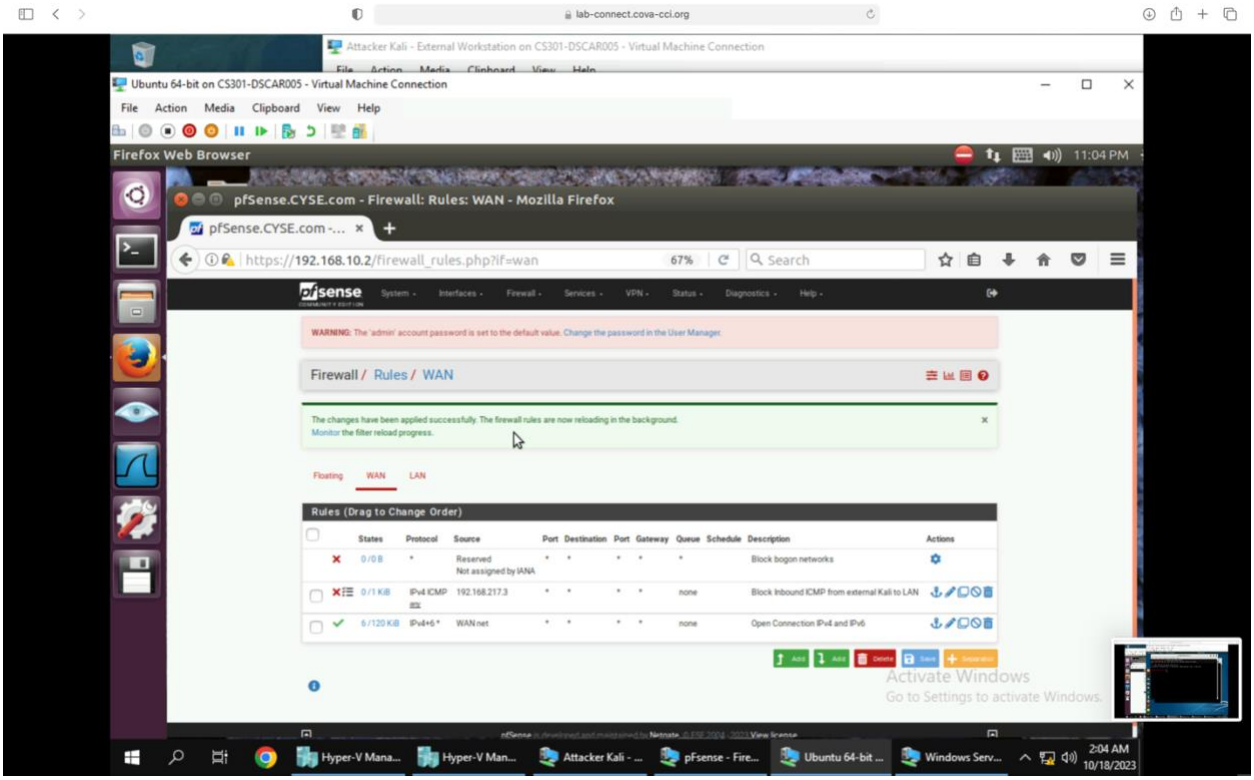


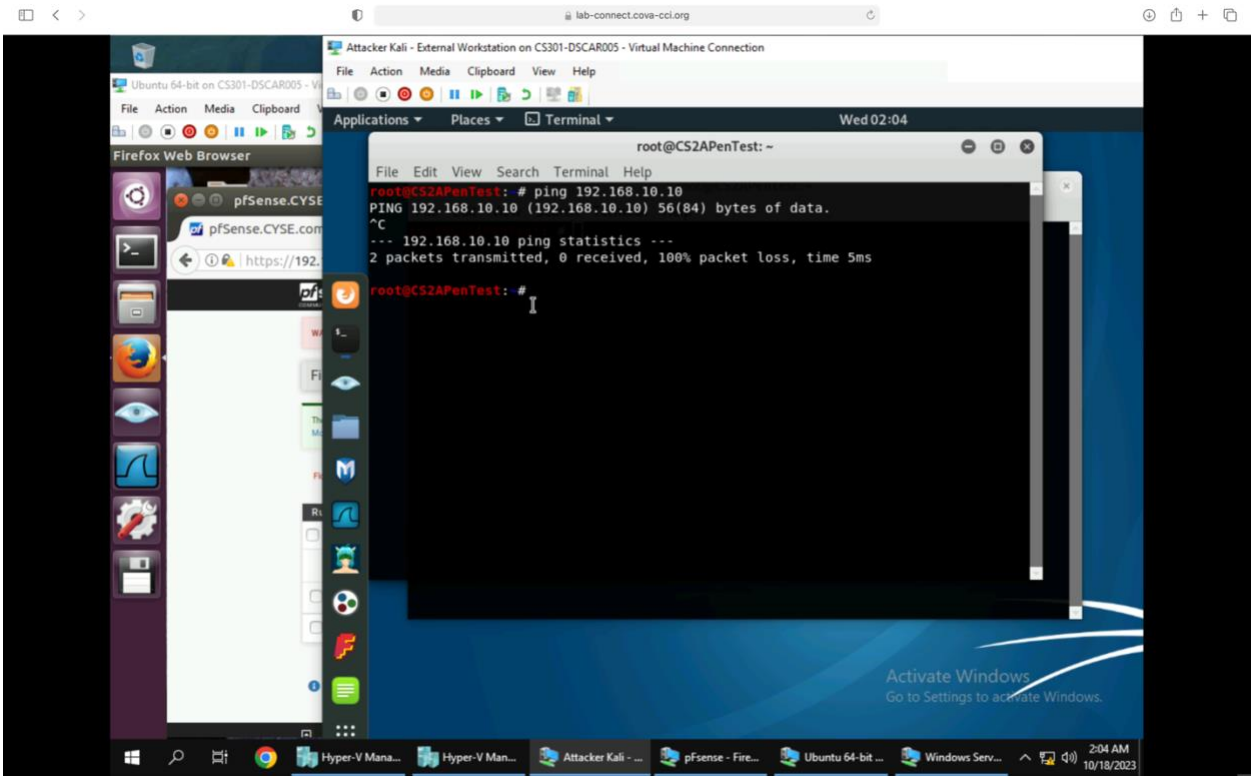


Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)

	WAN	Block/reject	192.168.10.10	192.168.217.3	ICMP

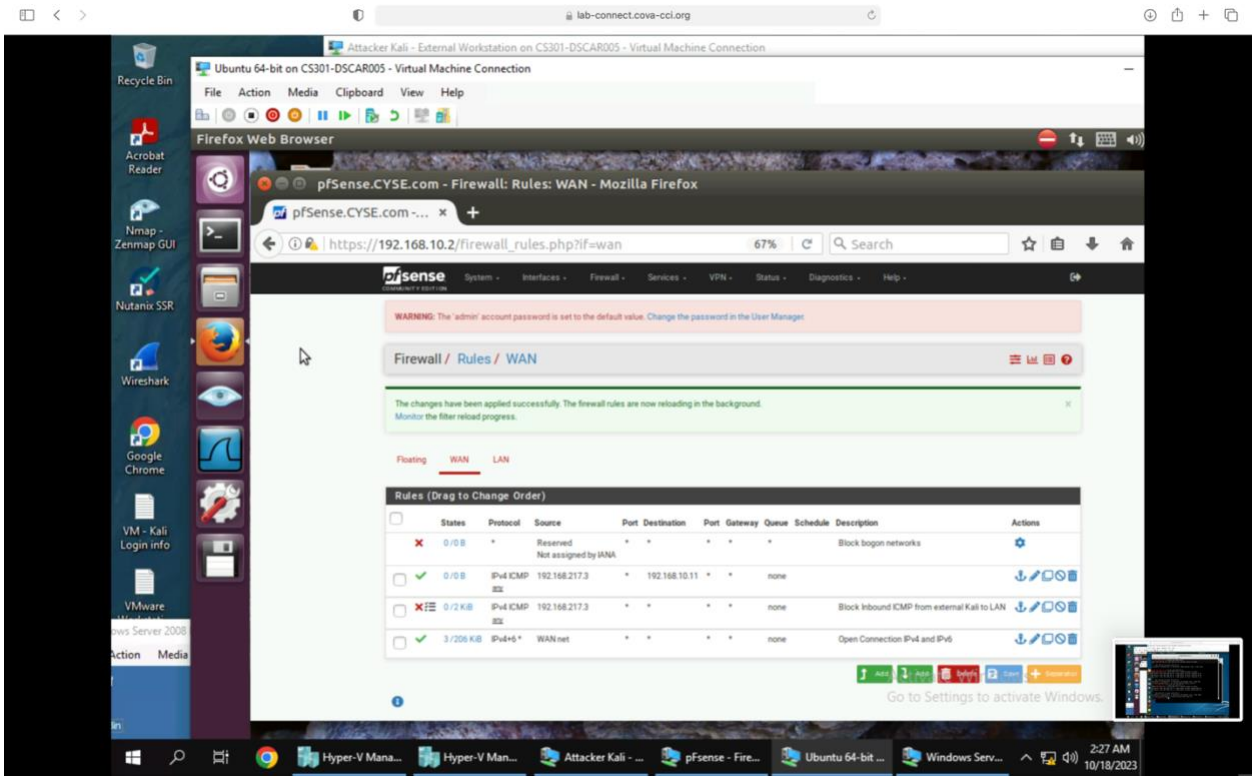
2. Clear the previous firewall policies and configure the pfSense firewall to block all ICMP traffic from External Kali to the LAN side.

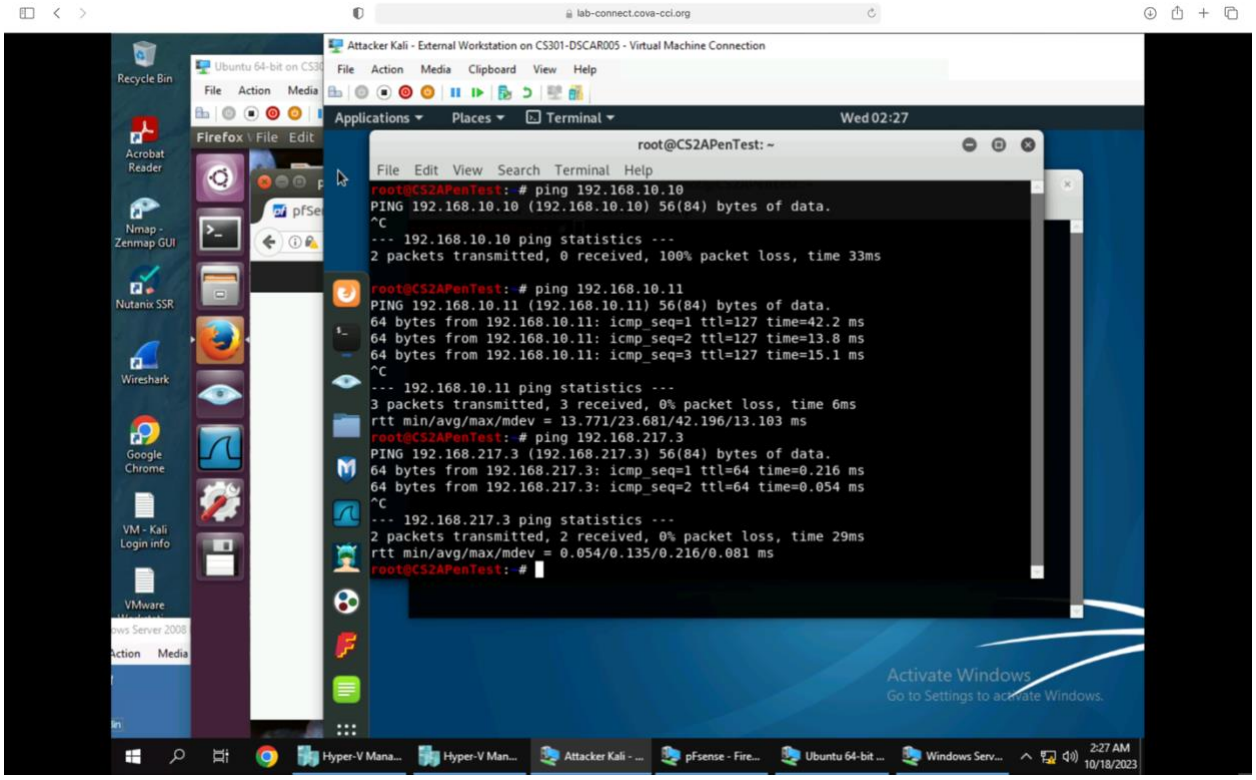




Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
	WAN	Block	192.168.217.3	LAN net/ any	ICMP

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 appliable)

	WAN	Block	192.168.217.3	Any	Any
	WAN	Pass	192.168.217.3	192.168.10.11	TCP

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

The main goal of this project was to use pfSense firewall to develop appropriate countermeasures while acting as both an attacker and a defender to find vulnerabilities in a LAN network. Network scanning, Wireshark traffic pattern capture, and firewall rule configuration were among the duties.

Task A involved profiling the fundamental details of the subnet topology, including open ports, operating systems, and services connected to each VM in the LAN network, using Nmap or Zenmap from the External Kali VM. The Ubuntu VM was also used to run Wireshark in order to record network activity while scanning was being done.

Task B concentrated on configuring pfSense's firewall rules to secure the network. The four sub-tasks were to block all ICMP traffic to the LAN side, all ICMP communication from External Kali to Ubuntu VM, all LAN side traffic except for FTP to Windows Server 2008, and finally to rerun the network scan after configuring the firewall rules.

Extra credit (15 points): Use NESSUS to enumerate the security vulnerabilities of Microsoft Windows Server 2008 VM in the CCIA network.