OLD DOMINION UNIVERSITY

CYSE 301: Cybersecurity Technique and Operations

Assignment 3: Sword vs. Shield

Alan Schneider

Aschn014

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.

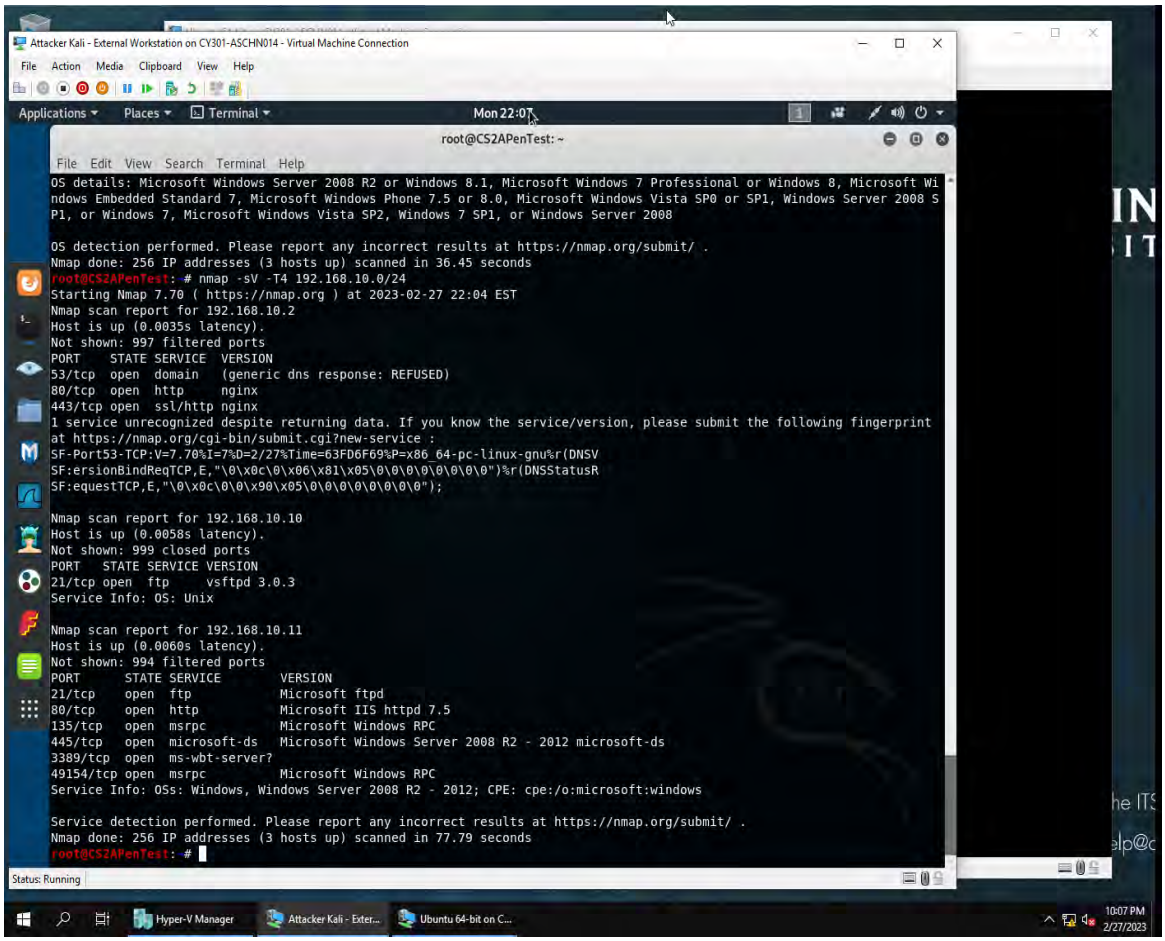
Task A: Sword - Network Scanning (20+ 20 = 40 points)

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.



I used the command nmap -sV -T4 192.168.10.0/24 to scan the network determining open ports, services and software version.

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.**

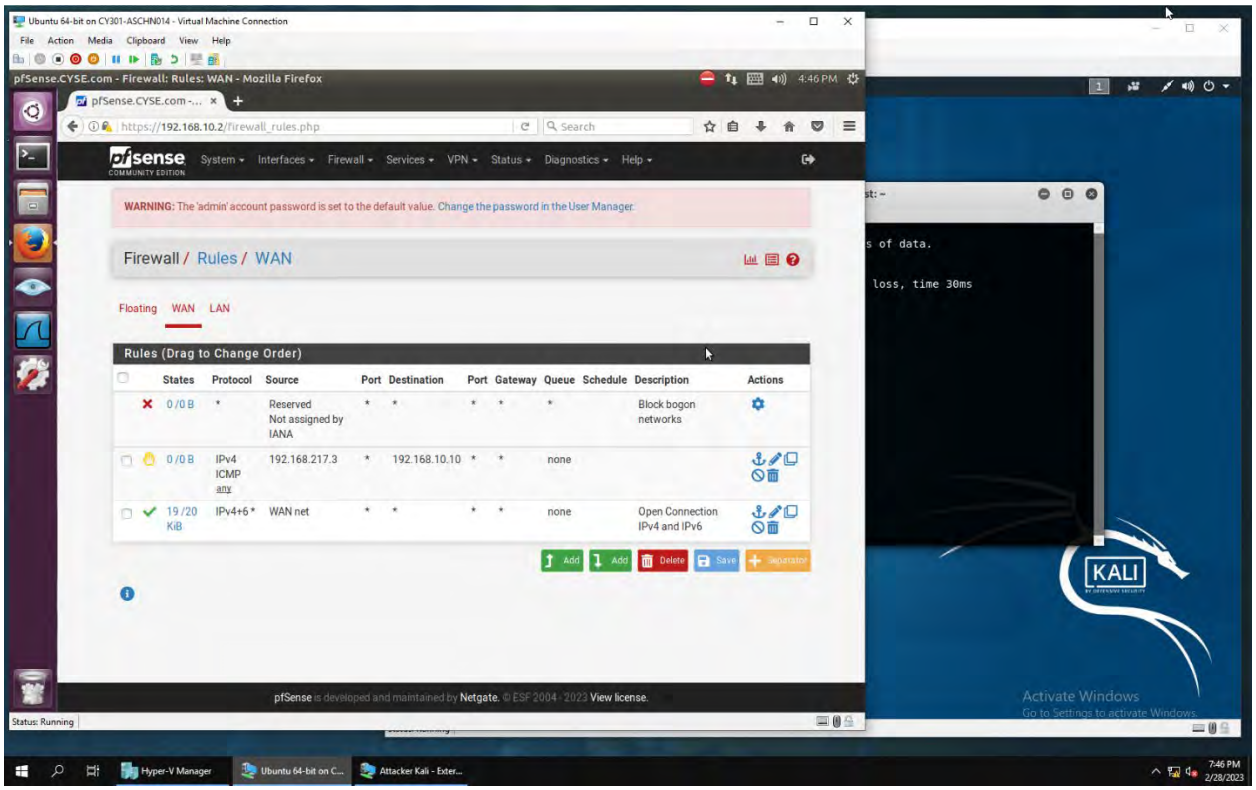
I ran a wireshark filter: ip addr==192.168.217.3 && ip.addr==192.168.10.11 to isolate the captured traffic between external kali and ubuntu during the scan. I observed external kali scanning for open ports through 3-way handshake connection between the source: 192.168.217.3 and destination: 192.168.10.11 port. When it found an open port then the source made a request with a SYN packet, a response destination sent SYN, ACK packet and then source sent ACK packets, at last source again sent RST, ACK packets. Open ports discovered were: 21, 80 135, 145 3389 and 49154. For the closed ports a 3-way handshake connection was not possible between source and destination. For example The source sent a Syn packet, to see if port 554 was open, it was not so a three way handshake was not possible. The destination send a response via RST, ACK.

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

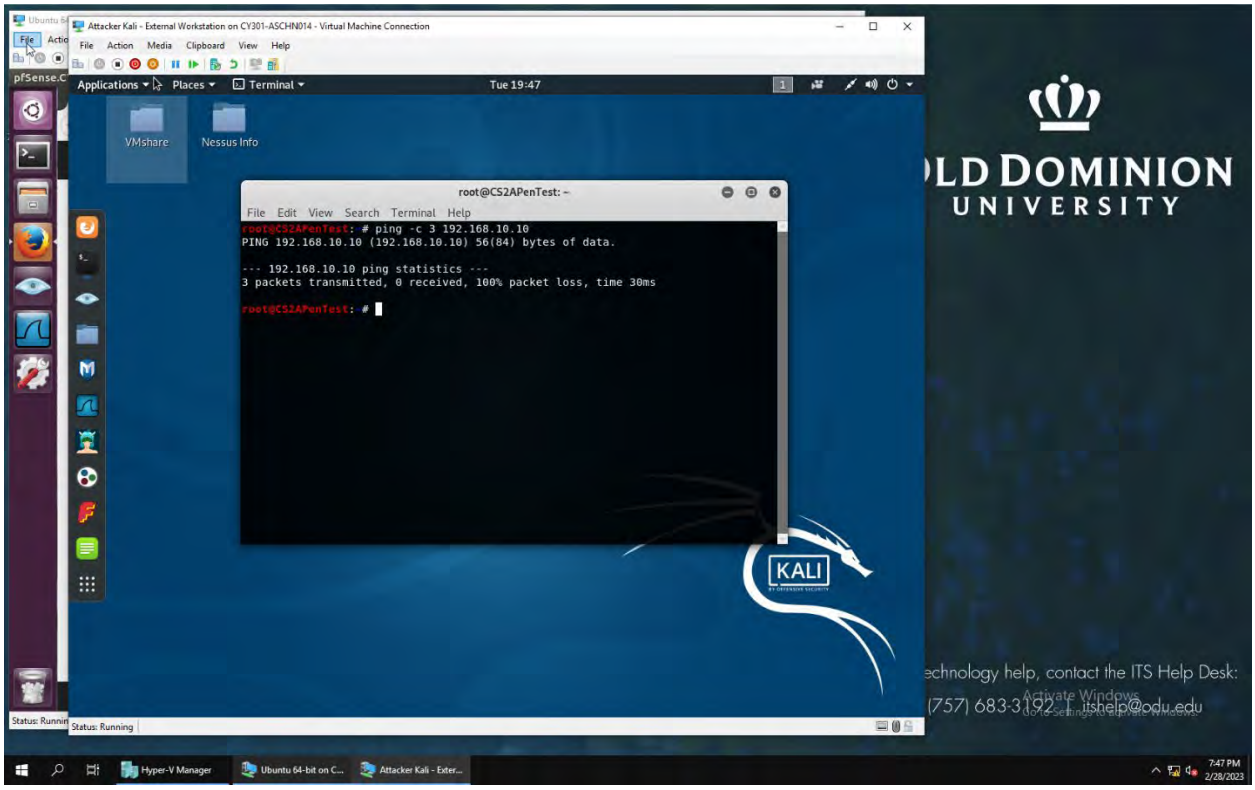
In order to receive full credits, you need to fill the table (add more rows if needed), implement the firewall rule(s), show me the screenshot of your firewall table, and verify the results.

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)
01	WAN	reject	192.168.217.3	192.168.10.10	ICMP



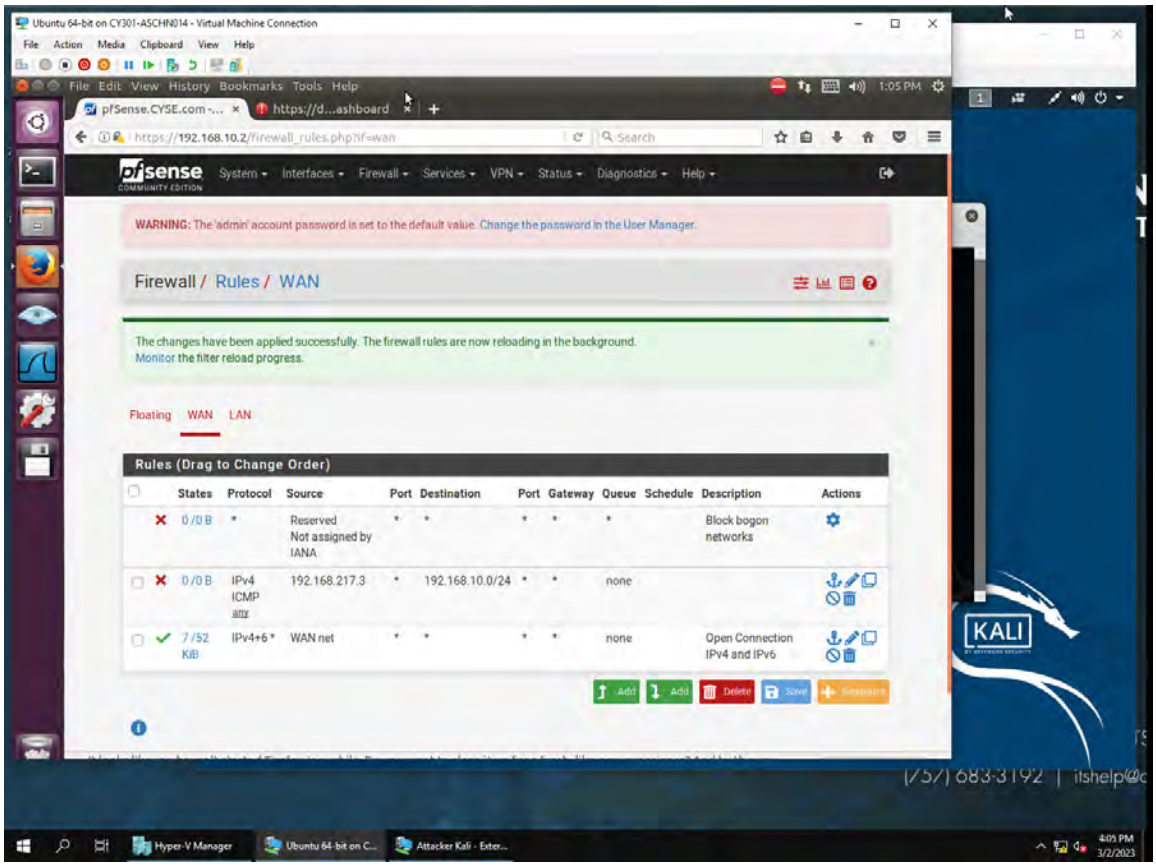
Below are the experiments I used to test the rule.



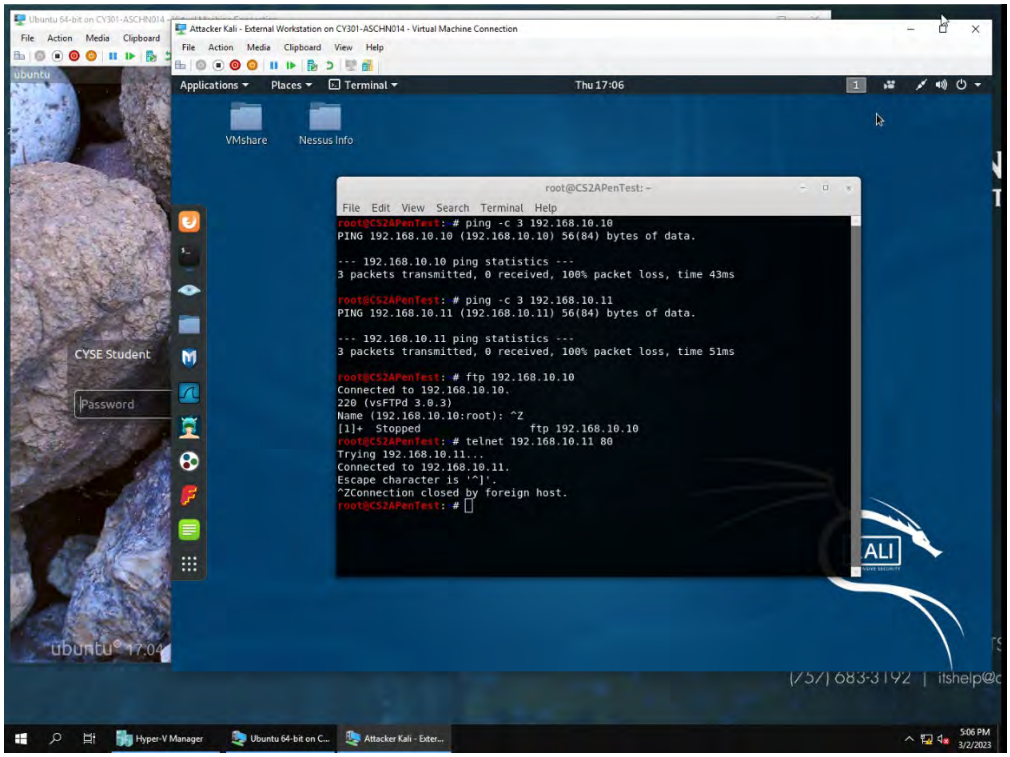
A. I used Ping -c 3 192.168.10.10 from 192.168.217.3. The result: 3 packets transmitted, 0 received 100% packet loss, time 36ms.

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)
02	WAN	reject	192.168.217.3	192.168.10.0/24	ICMP



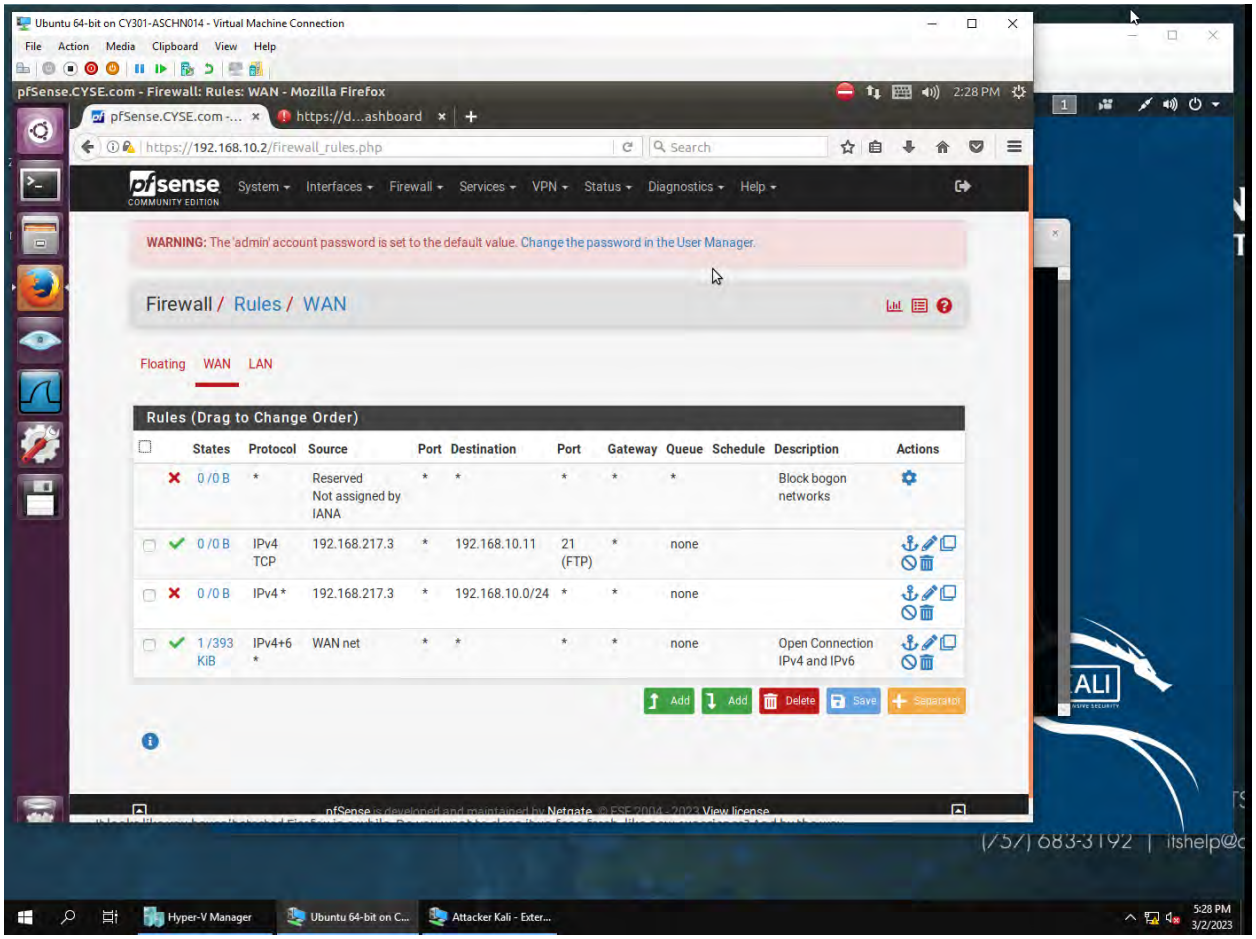
Below are the experiments I used to test the rule.



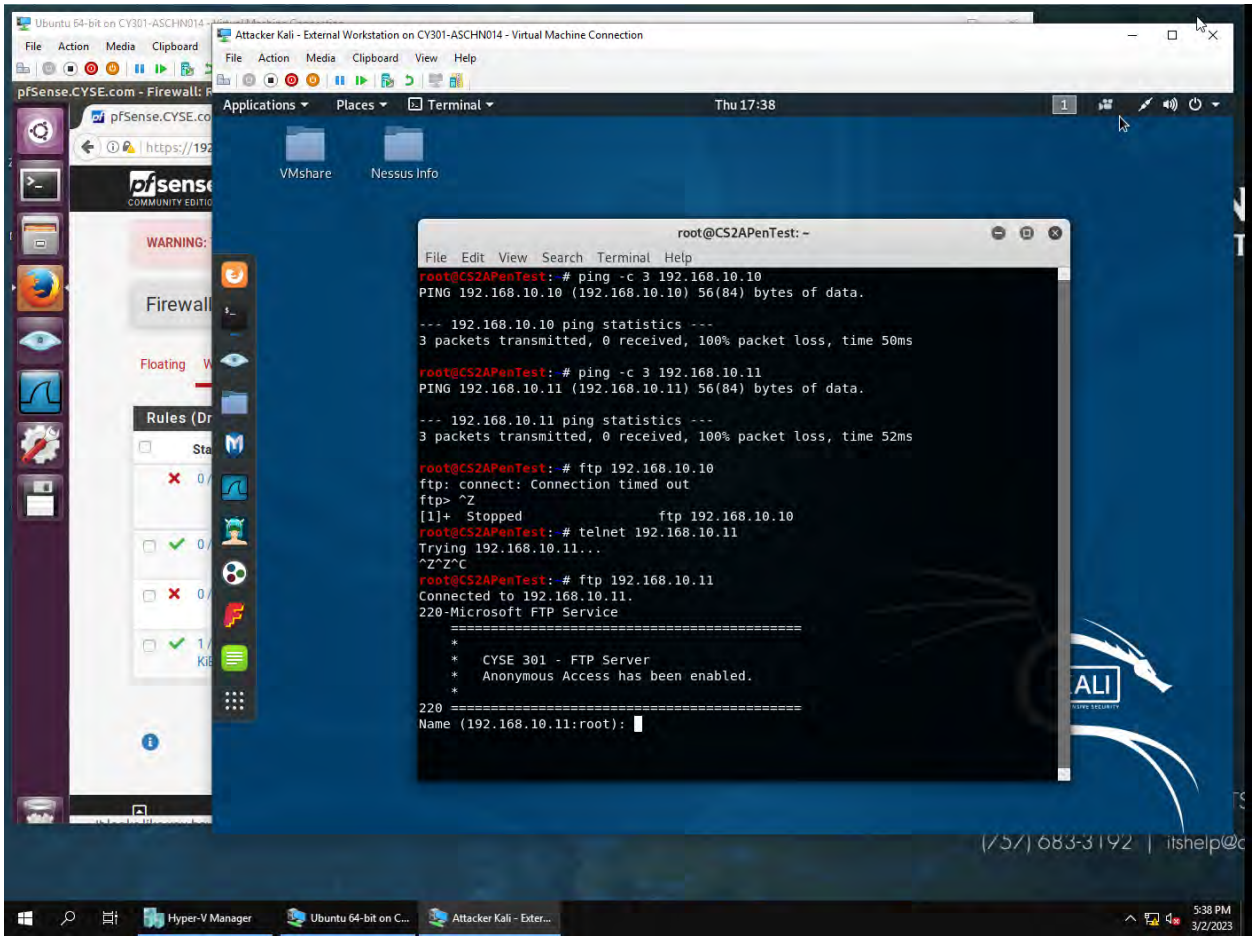
A. I used Ping -c 3 192.168.10.10 command and then ping -c 3 192.168.10.11 from 192.168.217.3. The result for both: 3 packets transmitted, 0 received 100% packet loss, time 36ms and 56ms.ftp
B. I was able to connect to ubuntu 192.168.10.10 via ftp from 192.168.217.3
C. I was able to connect to window 8 server 192.168.10.11 via over port 80 http from 192.168.217.3

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)
01	WAN	Block	192.168.217.3	192.168.10.0/24	All
02	WAN	Pass	192.168.217.3	192.168.10.11	FTP



Below are the experiments I used to test the rule



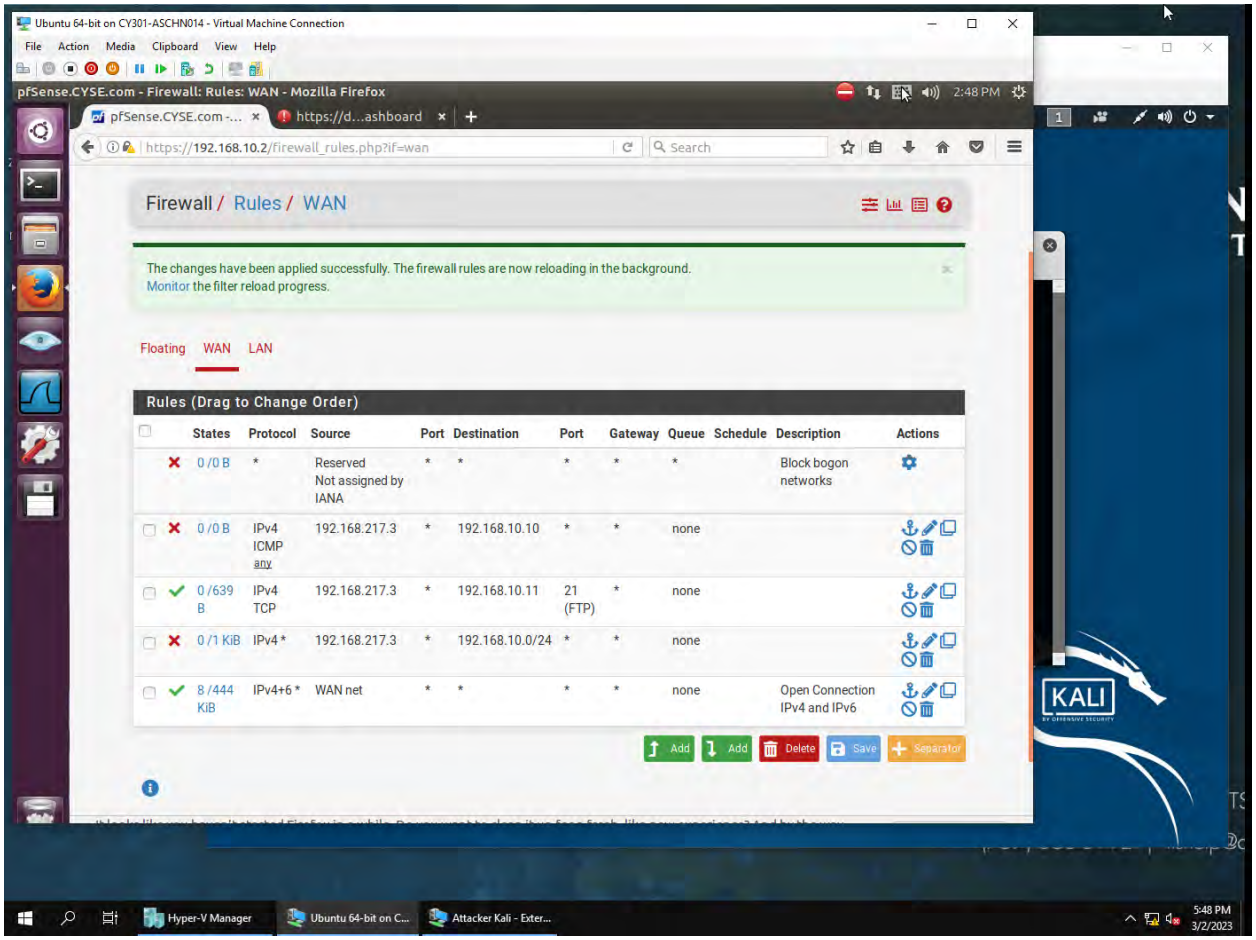
A. I used Ping -c 3 192.168.10.10 command and then ping -c 3 192.168.10.11 from 192.168.217.3. As I used a block action. The result for both: 3 packets transmitted, 0 received 100% packet loss, time 36ms and 56ms

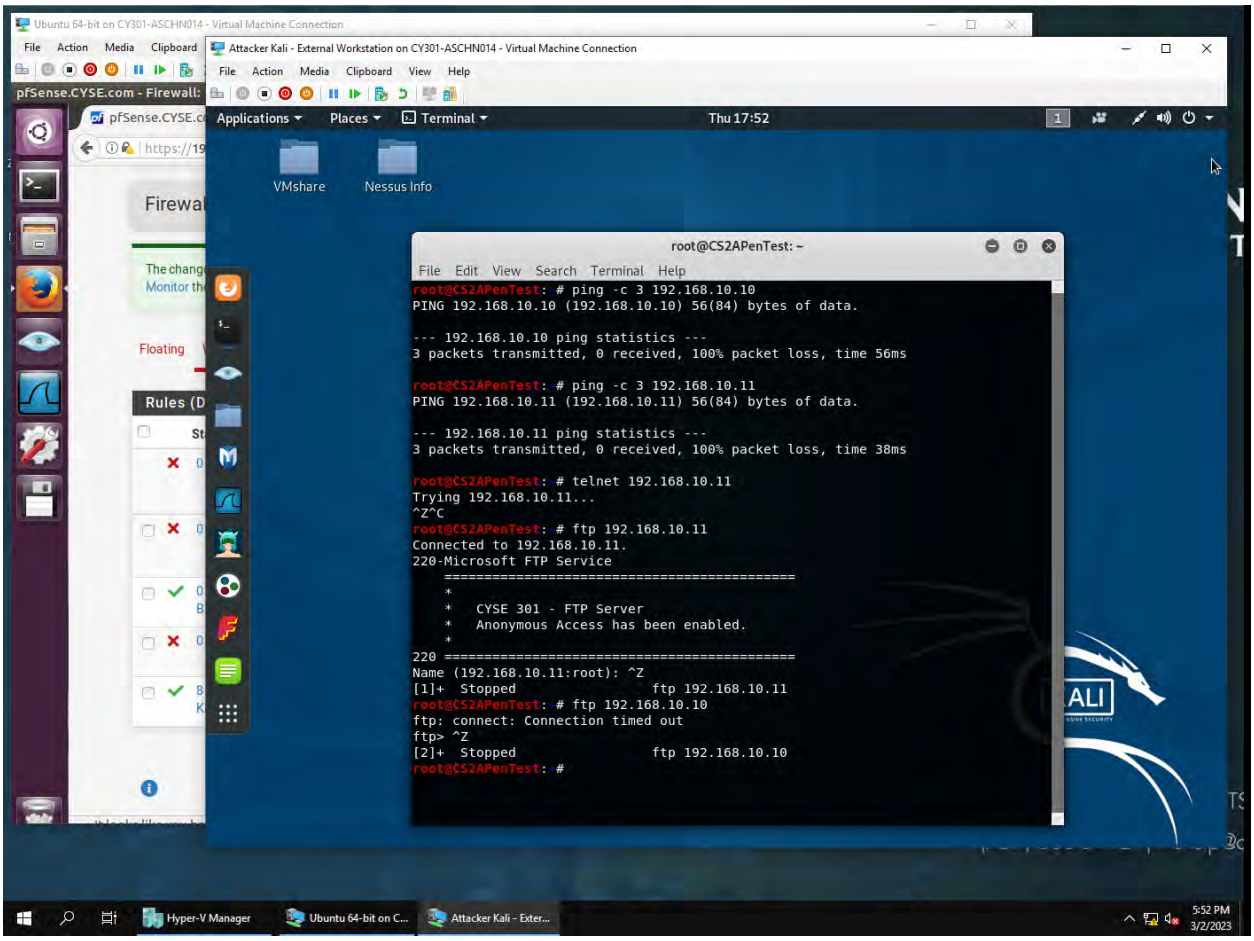
B. I was unable to connect to ubuntu 192.168.10.10 via ftp from 192.168.217.3

C. I was unable to connect to window 8 server 192.168.10.11 via over port 80 http from 192.168.217.3

D. I was able to connect to Windows 8 server 192.168.10.11 via ftp port 21 from 192.168.217.3

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





Although the new firewall rule specifically blocks icmp traffic from external kali 192.168.217.3 to ubuntu 192.168.10.10. The previous firewall rule is applied first and already blocks any traffic to include ICMP from external kali 192.168.217.3 to the 192.168.10.0/24 network. Then the firewall rule to pass ftp port 21 from 192.168.217.3 to 192.168.10.11 only.

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