Nick Carpenter

CYSE 301: Cybersecurity Technique and Operations

Assignment 3: Sword vs. Shield

In this assignment, you will function 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.

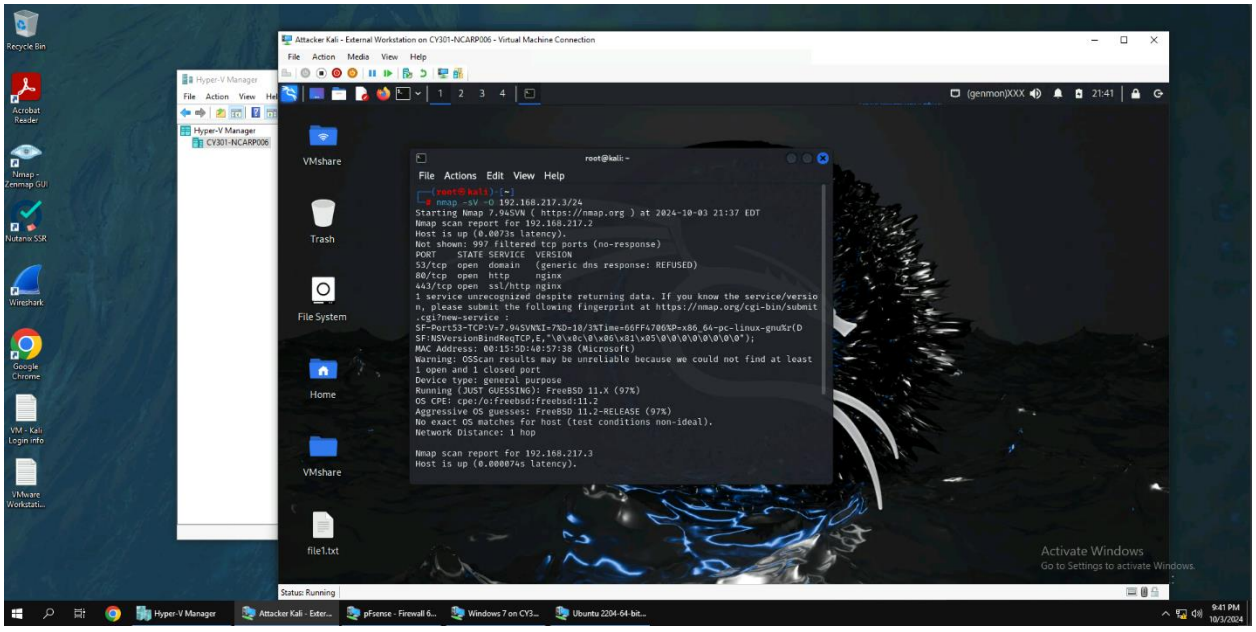
Task A: Sword - Network Scanning (20+ 20 = 40 points)

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

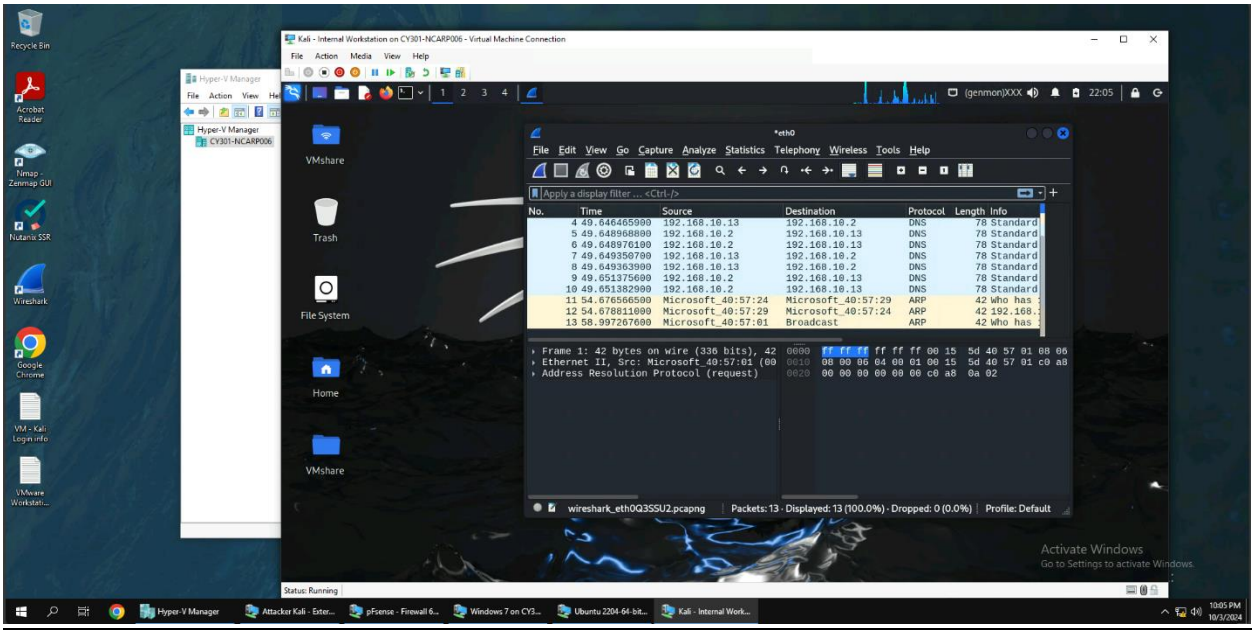
Make sure you didn't add/delete any firewall policy before continuing.

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.



Explanation for step 1: I used the nmap command follow by -sV (to get the version being used) followed by the -O command for the system. Then I used the subenet topology for external Kali (192.168.217.3/24)

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.**



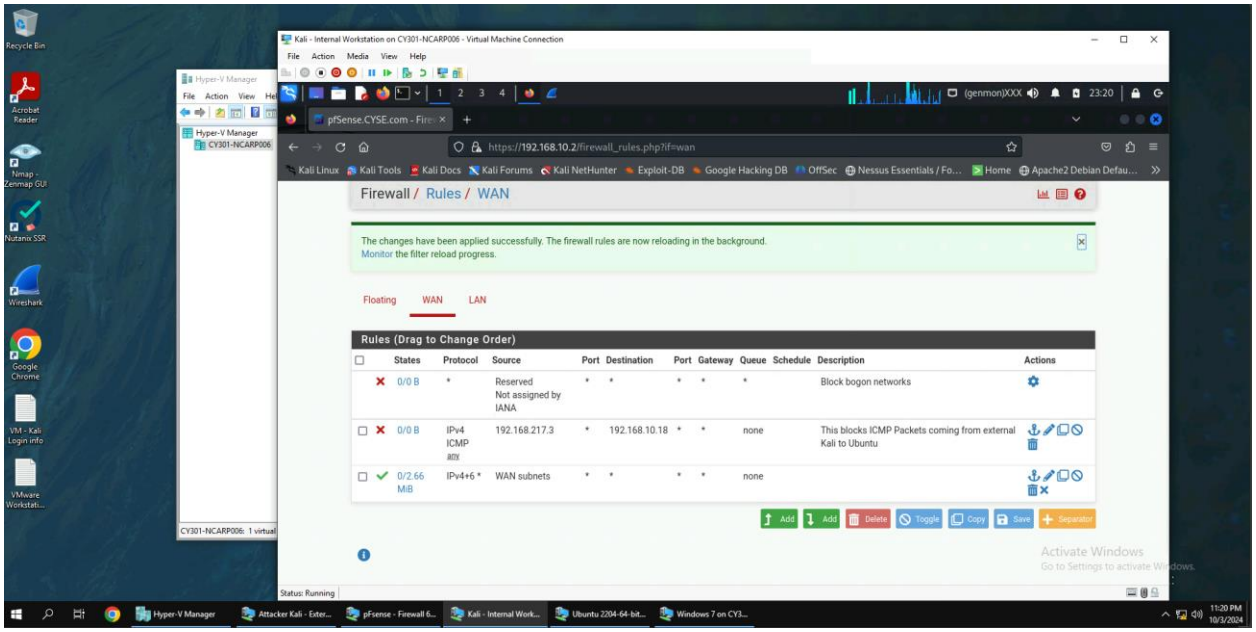
Explanation for part 2: When a system (in this case External Kali) attempts to send an ICMP request using NMAP, it needs to determine the IP addresses that it needs to send the packet to. Therefore, from internal Kali, we can see that there are various ARP requests that are happening across the subnet for the different IP addresses. These are initially established by using a TCP three-way handshake. This establishes a reliable connection between the client and the server. This process is performed in 3 steps including synchronization, synchronization and acknowledgement, and acknowledgement. After a reliable connection is established, the IP address, open ports, version, and operating system from the subnet are stored in the ARP cache. This cache is essential for the NMAP scan showing the results after pinging the system. Systems can be hardened from NMAP scan by closing the ports across a network. These ports can be blocked using the correct firewall rule (in our case through Pfsense). It is typically a good idea to block ICMP packets that are coming into the network. If ICMP packets are not blocked, the system can be at risk for denial-of-service-attacks. When ICMP packets are blocked, it restricts pinging the network in the traditional way.

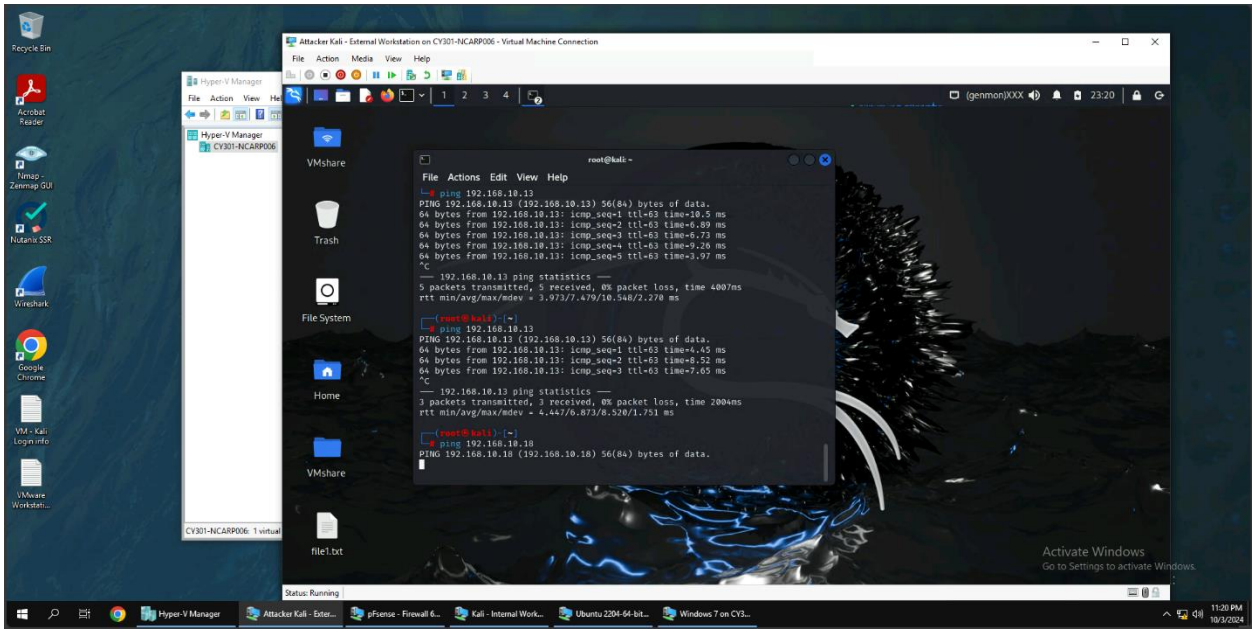
Task B: Shield – Protect your network with a firewall (10 + 10+ 20 + 20 = 60 points)

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	No ICMP Port Number

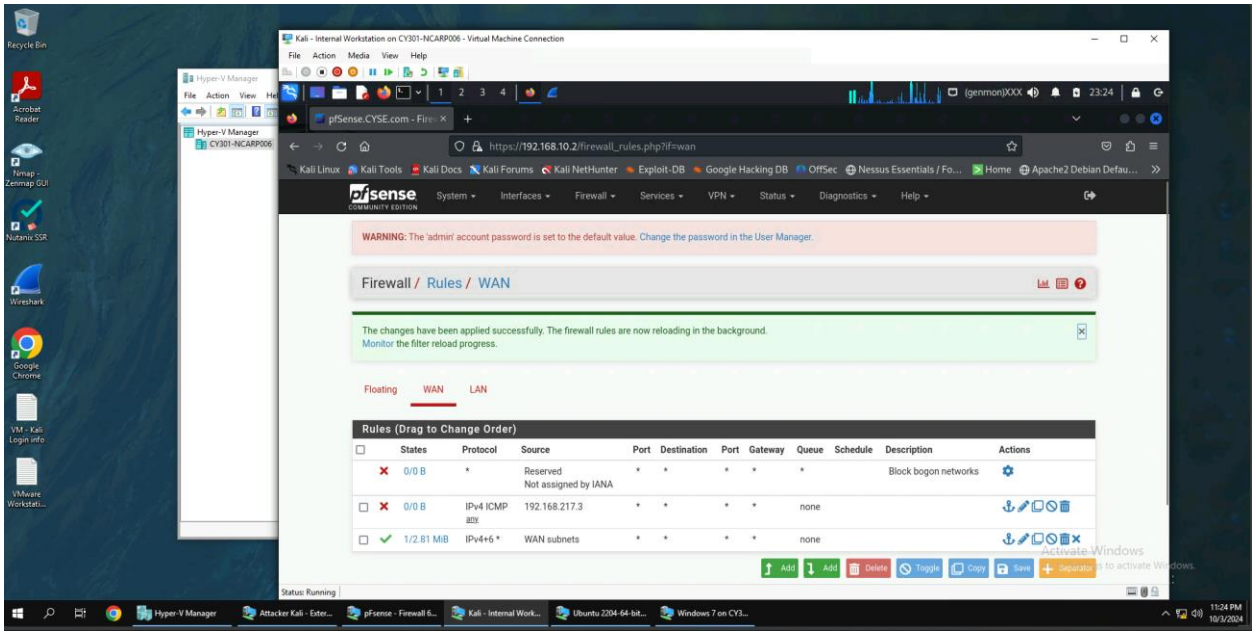


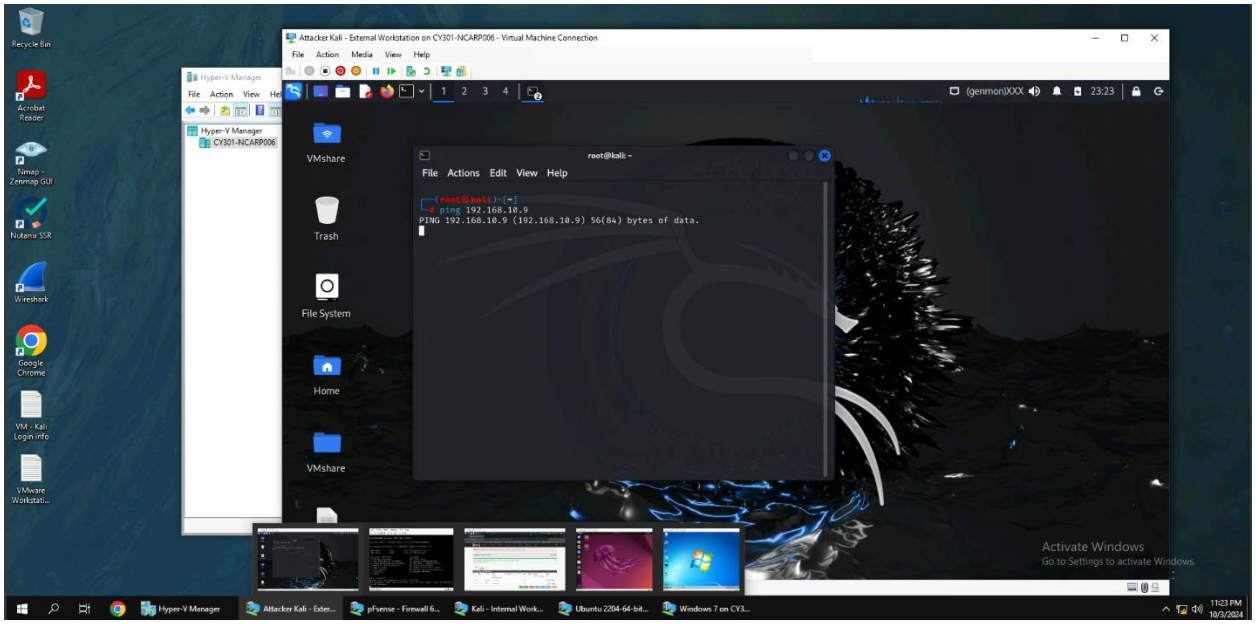


Explanation for step 1: Since we want to block incoming traffic, we need to use the WAN interface with the correct IP addresses. Then I attempted to ping Ubuntu to make sure my firewall rule was correct.

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	Any	No ICMP Port Number

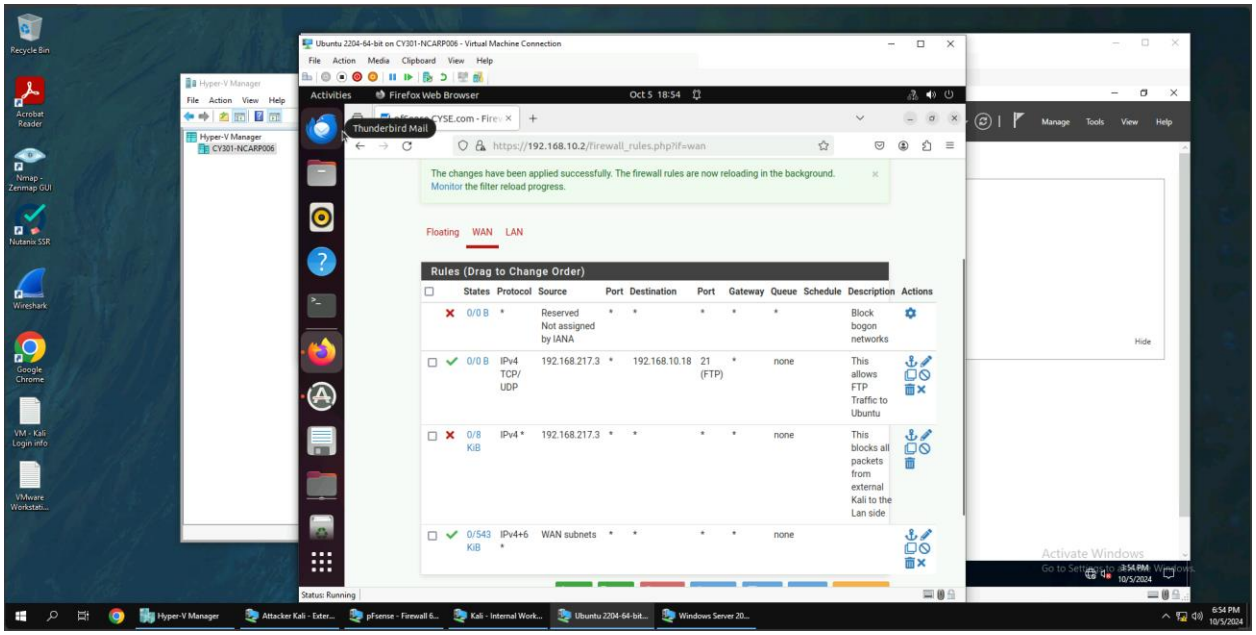


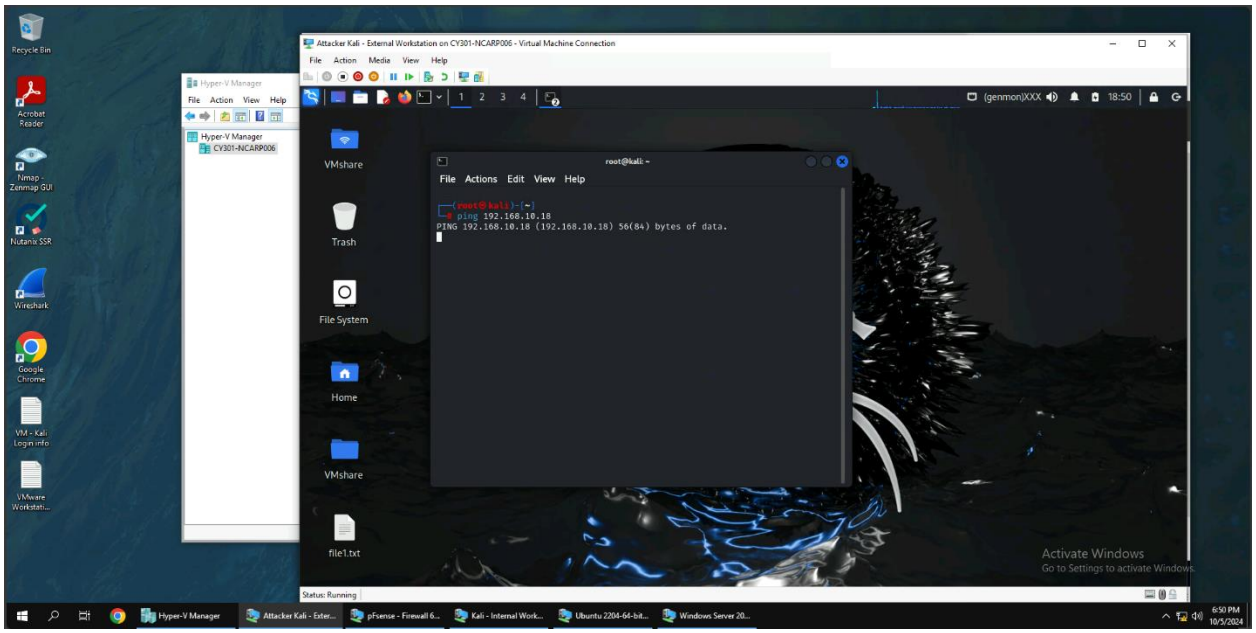


Explanation for step 2: We want to block incoming traffic, therefore need to use the WAN interface with the correct IP address for external Kali. Since we want to block any traffic to the LAN side, we need to set the destination to any. Then I attempted to ping the LAN side to make sure my firewall rule was correct.

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.

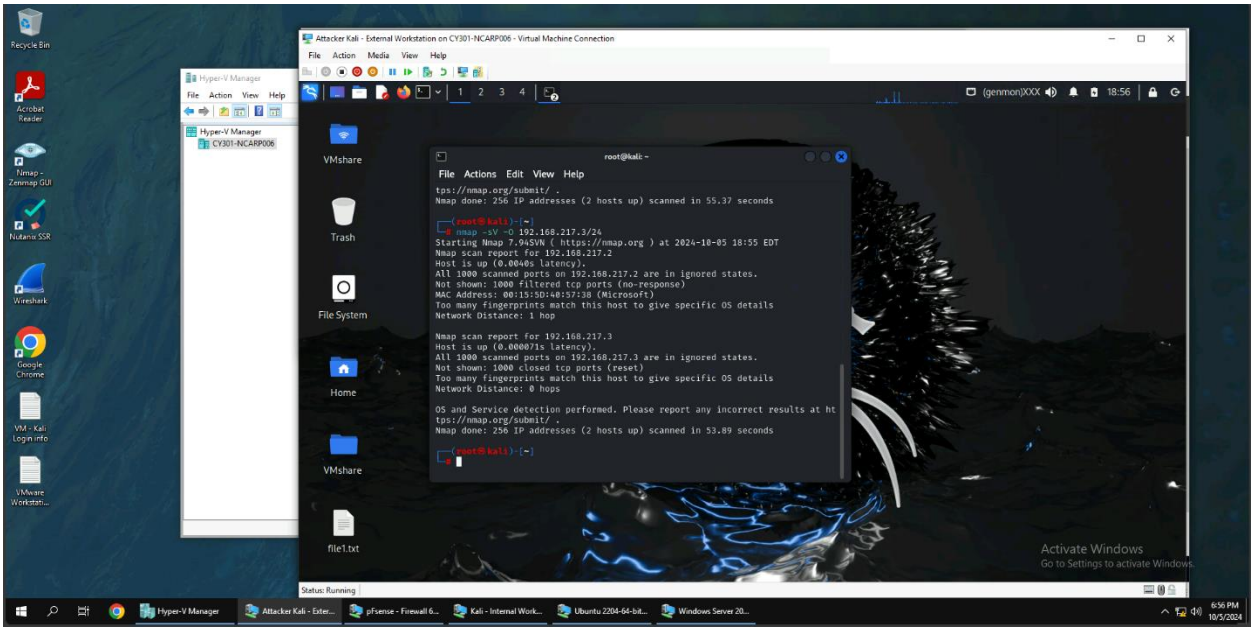
Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
2	WAN	PASS	192.168.217.3	192.168.10.18	21
3	WAN	Block	192.168.217.3	Any	No port number





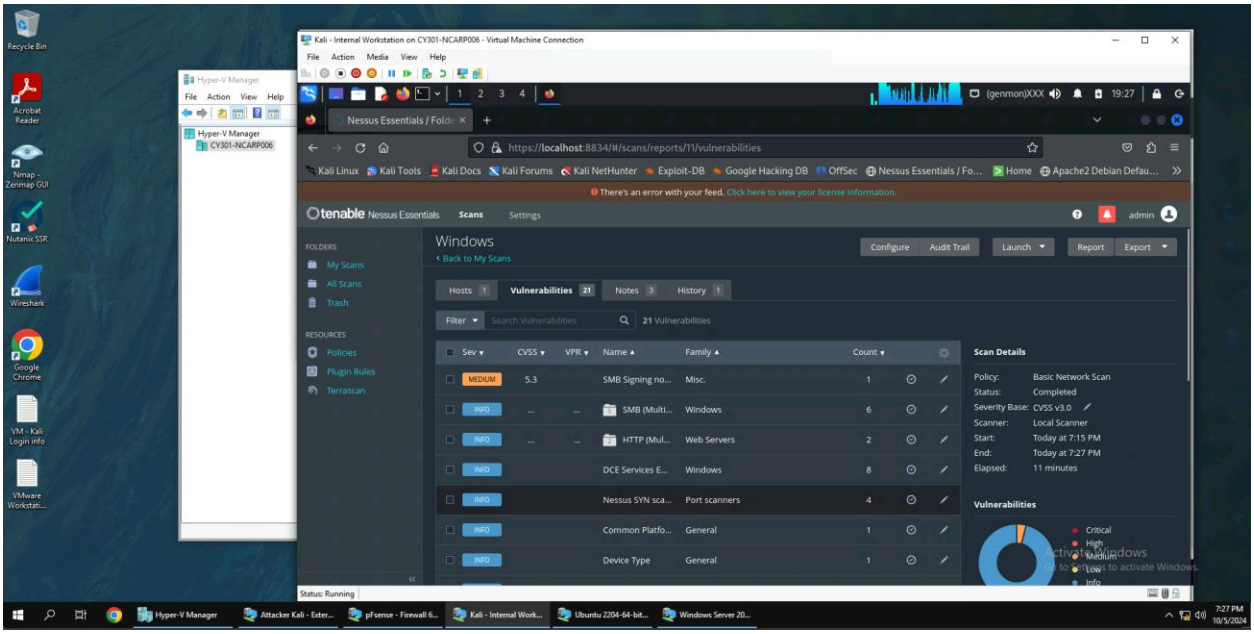
Explanation for step 3: Since we are still dealing with incoming traffic, therefore need to use the WAN interface for both rules with the correct IP addresses. The first rule needs to allow traffic for port 21. The second rule should block the rest of the incoming traffic.

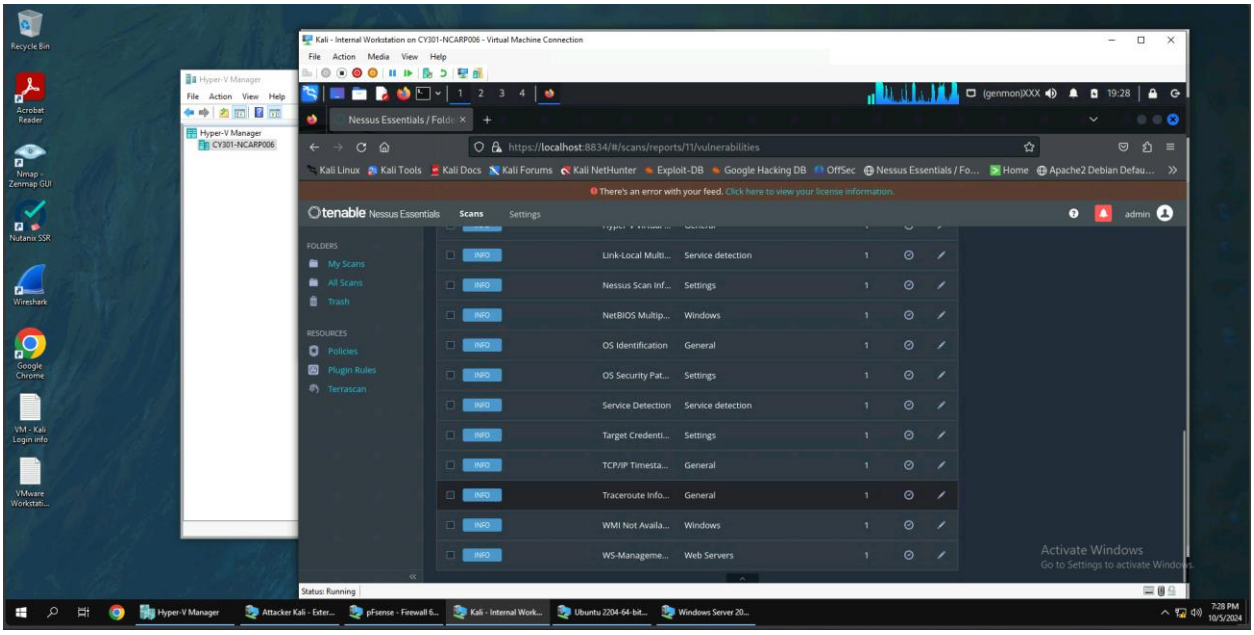
4. Keep the firewall policies you created in Task B.3 and repeat Task A.1. What's the difference?



The ports that were shown as open are now closed. In the first screenshot, there were 997 ports open with information present for the 3 open ports. After implementing the firewall rules, there are now 1000 closed ports with no subnet information present.

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





Explanation: I created a network scan for the windows IP address. After the scan completed, I clicked on the vulnerabilities tab which outlines the current vulnerabilities for this system.