Gerkeil Owens

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.

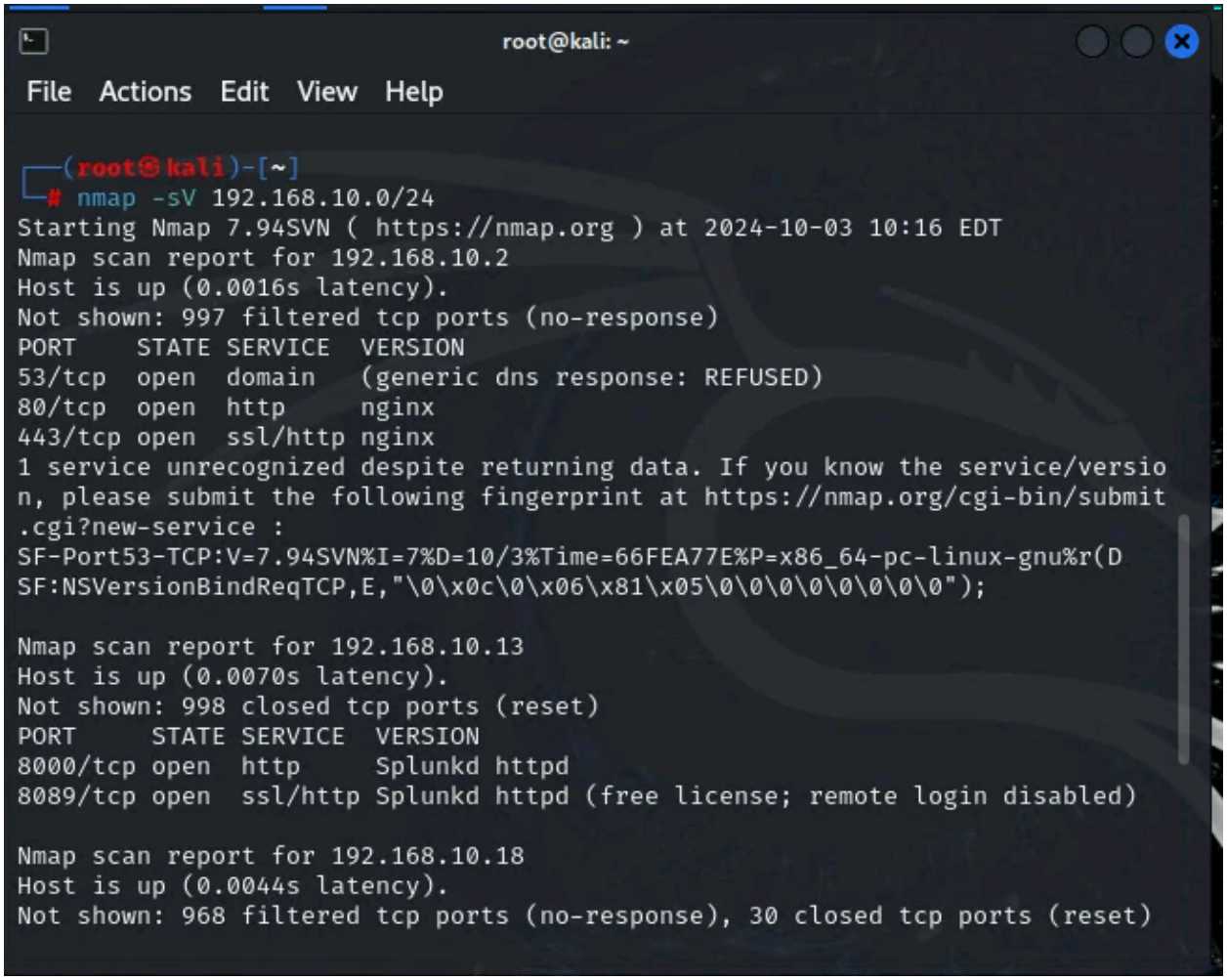
Task A: Sword - Network Scanning (20+ 20 = 40 points)

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)

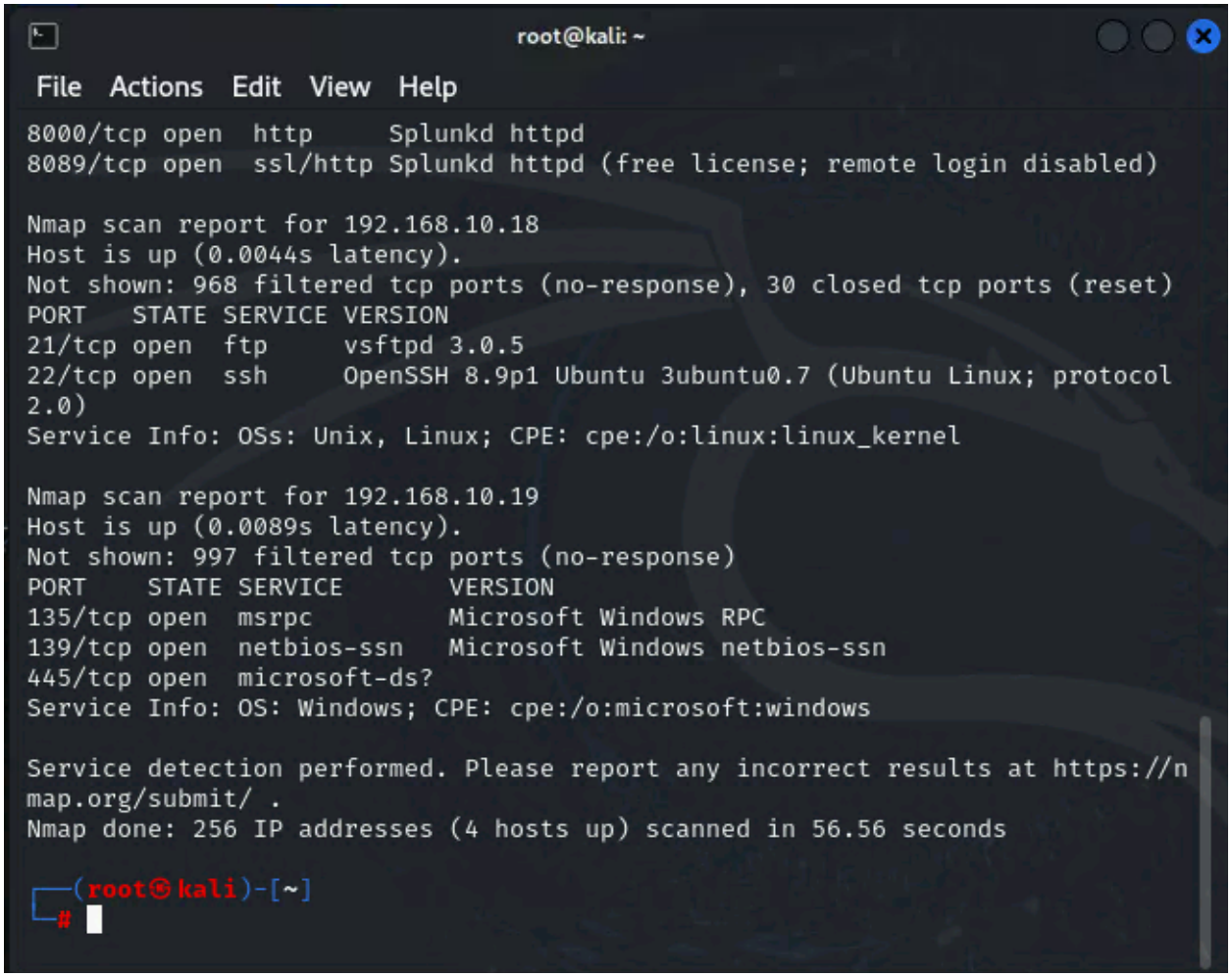
- External Kali
- pfSense
- Ubuntu
- Windows Server 2022

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.

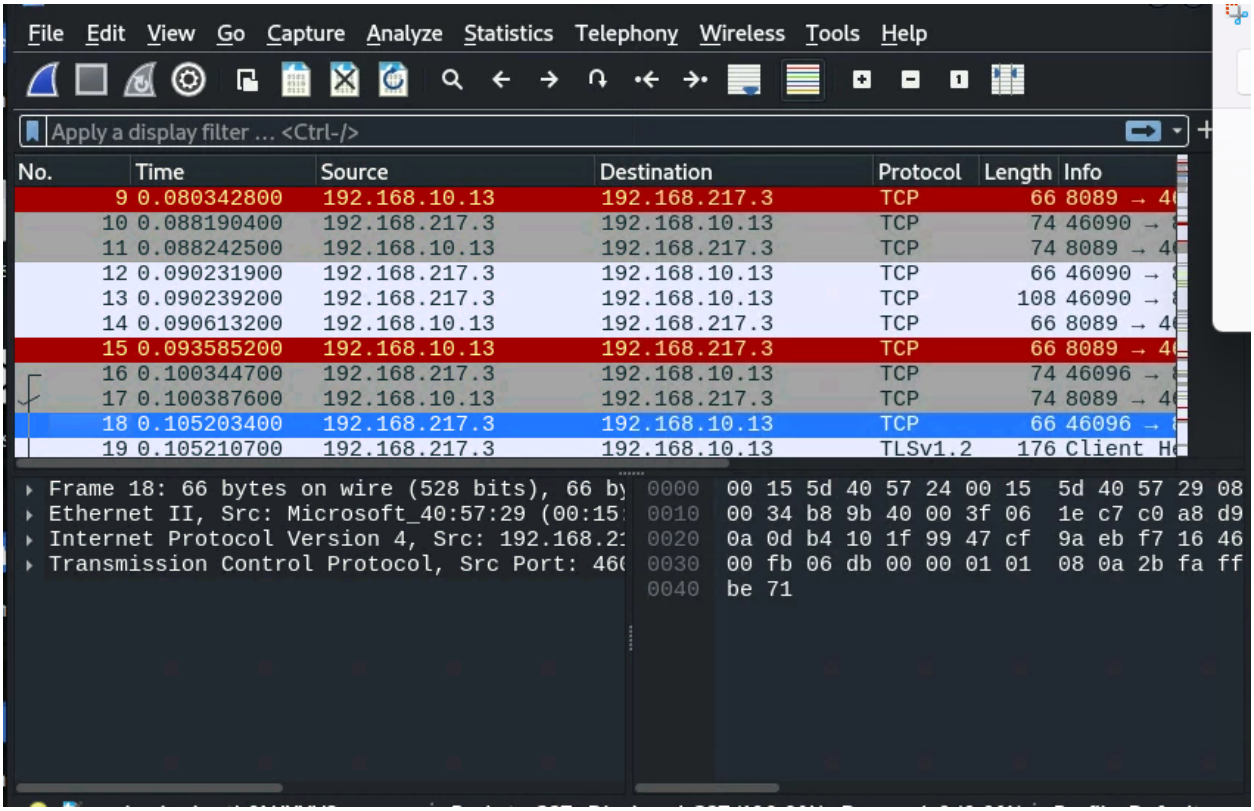


- Entering the "nmap -Sv 192.168.10.0/24" command to profile the basic information about the subnet.



- Entering the “nmap -Sv 192.168.10.0/24” command to profile the basic information about the subnet continued.

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.**



- In analyzing the traffic captured during the Nmap scan using Wireshark, several patterns emerged that provided insight into the network's behavior. A significant number of requests were observed as the scanning tool attempted to identify active hosts within the subnet. This is normal behavior as requests are necessary for resolving IP addresses to MAC addresses. The majority of the traffic consisted of TCP scans, which aims to identify open ports without establishing a full TCP connection. This stealth approach minimizes detection, making it a preferred method. Also, there were a few ICMP echo requests and replies, suggesting that ping sweeps were occurring, though this depends on the specific Nmap options chosen.

  Overall, the captured traffic illustrated typical patterns associated with network scanning, characterized by a high volume of TCP packets and requests. This data emphasizes the importance of monitoring network traffic to detect potential activities, which can serve as a precursor to more malicious actions. Also, I noticed the color pattern of red and grey. This might be a security feature to highlight suspicious activity in a network's traffic so cybersecurity engineers working within the network can filter through traffic more easily.

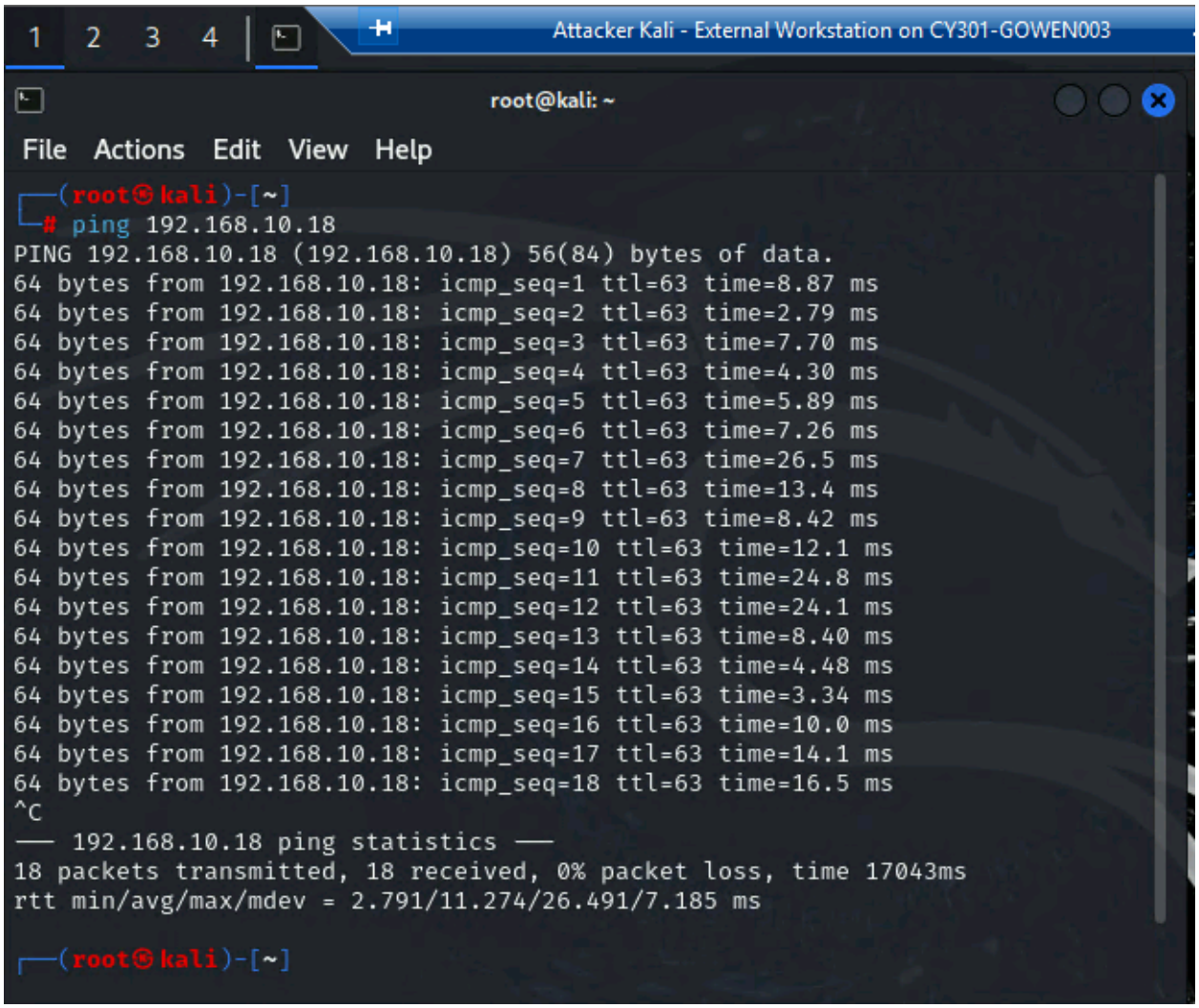
Task B: Shield – Protect your network with firewall (10 + 10+ 20 + 20 = 60 points)

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.

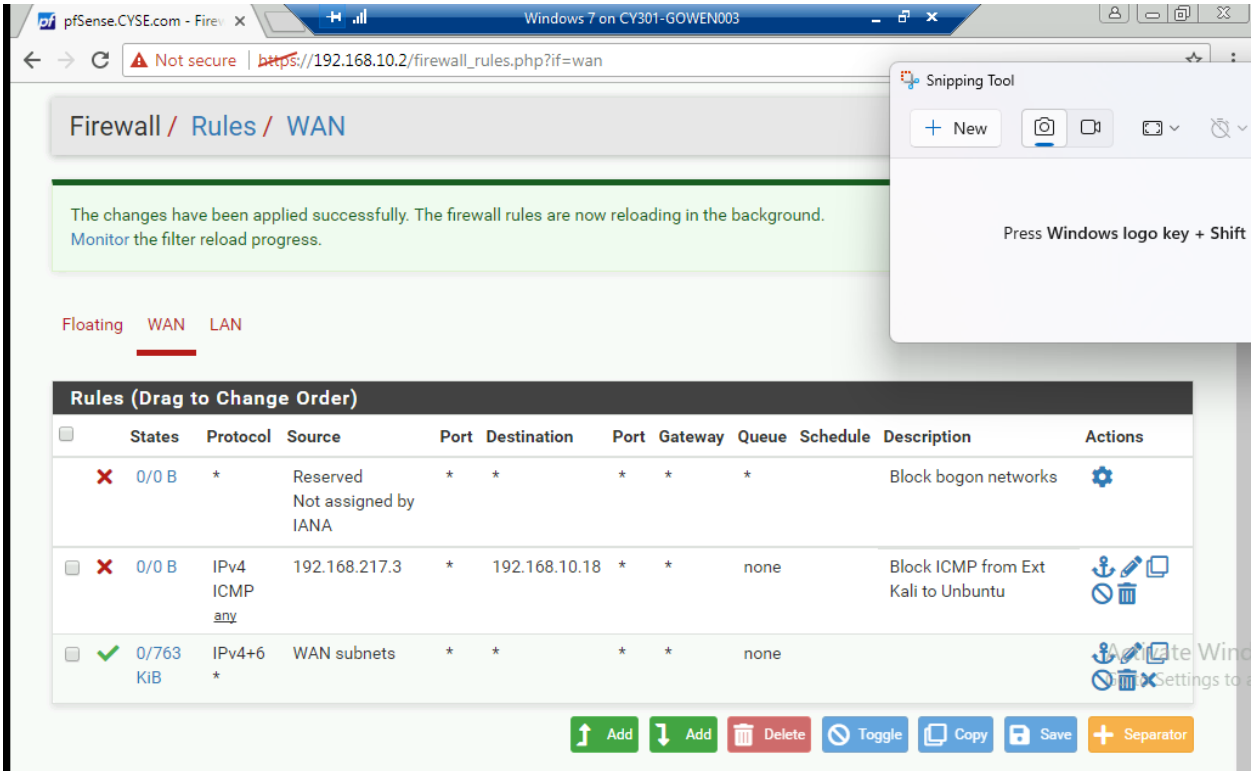
1. Configure the pfSense firewall rule to block the ICMP traffic from External Kali to Ubuntu VM.

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

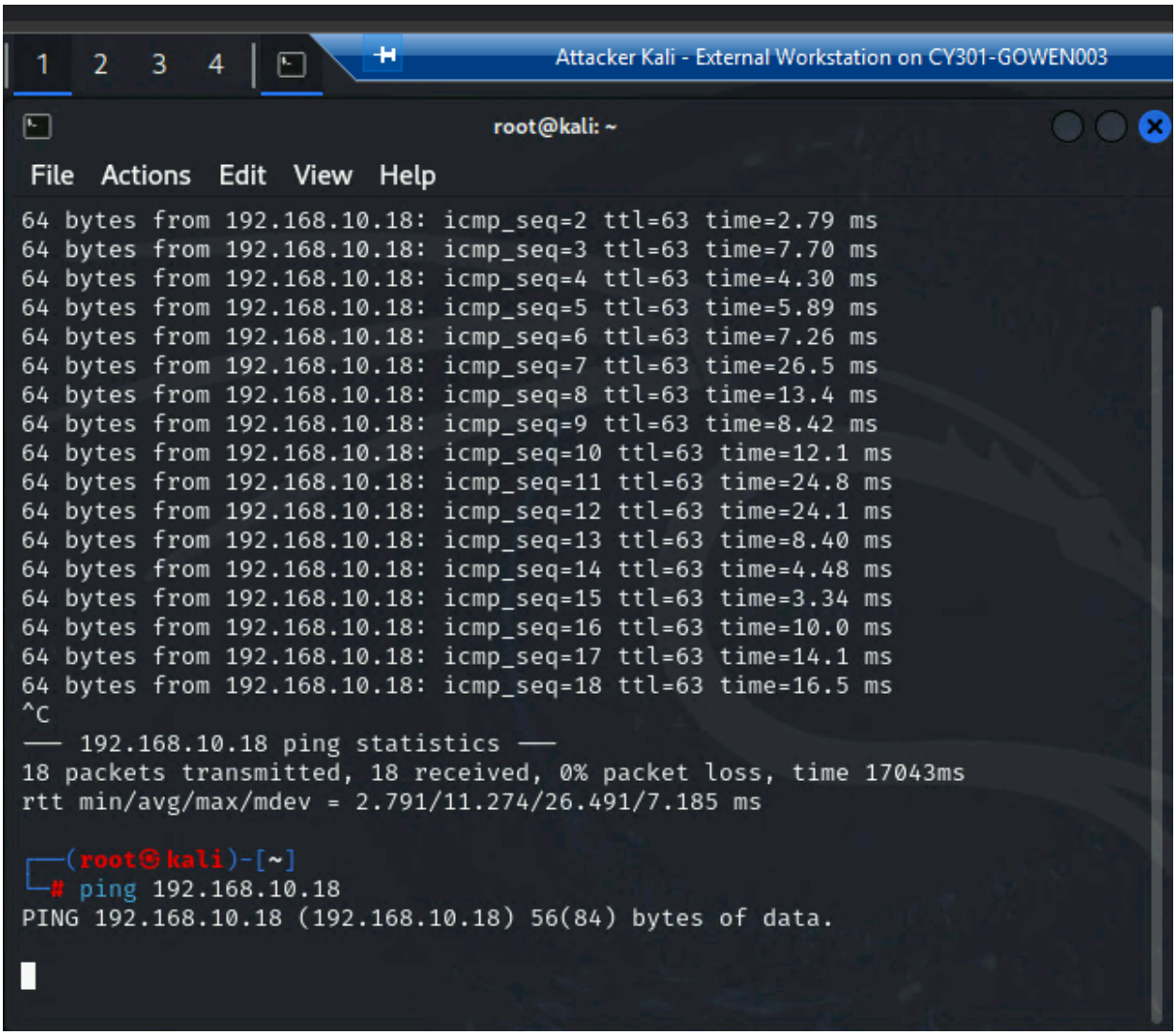
[Add the screenshot here]



- Pinging Unbuntu before put the rules in place to block access



- The rules changes being applied to block ICMP from external Kali to Unbuntu



- Trying to ping Unbuntu after the rules changes were applied and after waiting a few minutes this is all that happened show not being able to access Unbuntu.

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	192.168.10.0/24; all	

[Add the screenshot here]

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 2022.

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?

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