OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #3: Sword Vs. Shield

RANEEM ALARIAN

UIN: 01199741

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.

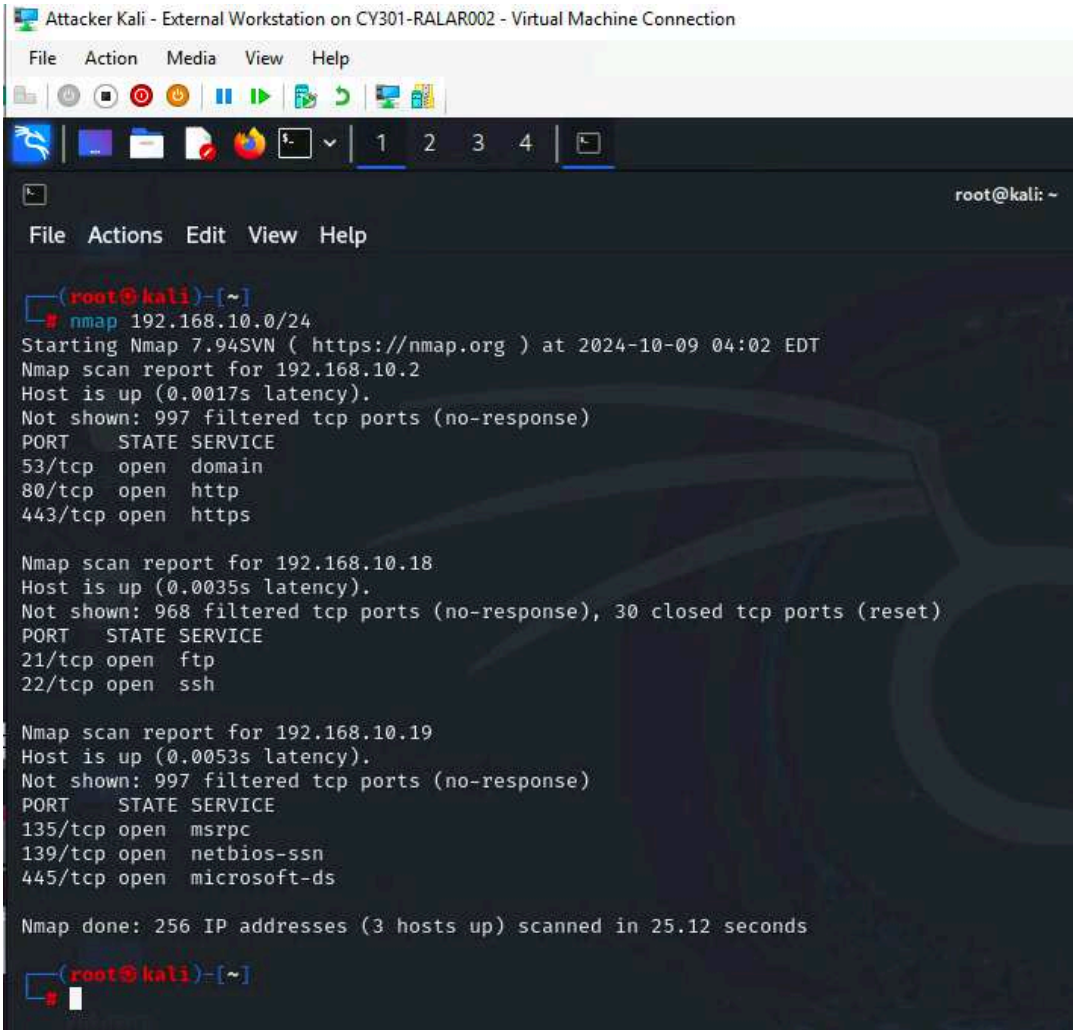
Task A: Sword- Network Scanning

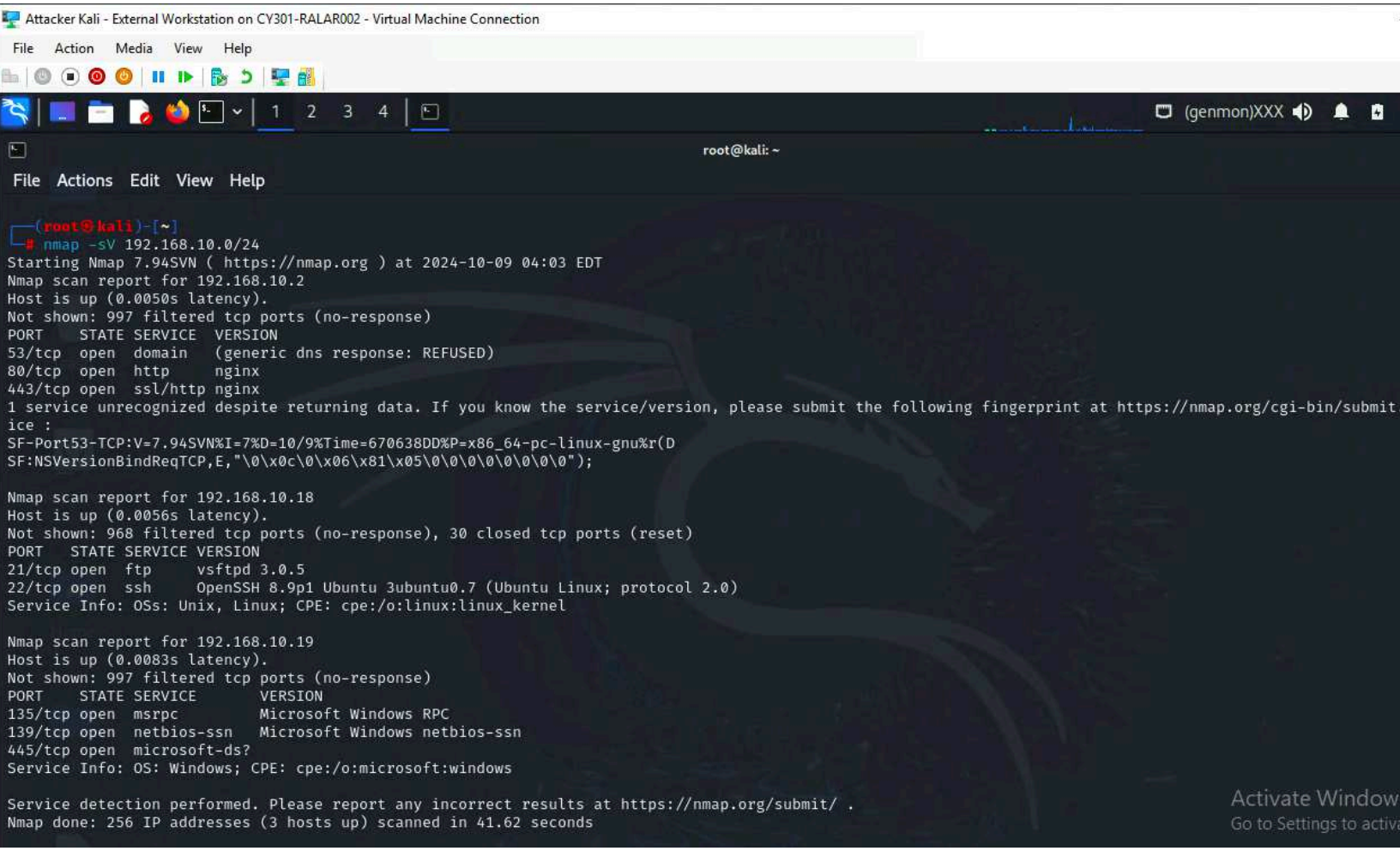
Power on the listed VMs and complete the following steps from the **External Kali** (you can use either nmap or zenmap to complete the assignment)

- 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**

My findings:

I found several results while running Wireshark in Internal Kali VM while External Kali scanned the network. First, ARP requests were frequently seen as External Kali tried to discover active devices. Alongside ARP, ICMP packets were also common. External Kali sent echo requests to check which hosts are active, and the responses provided feedback on their status.

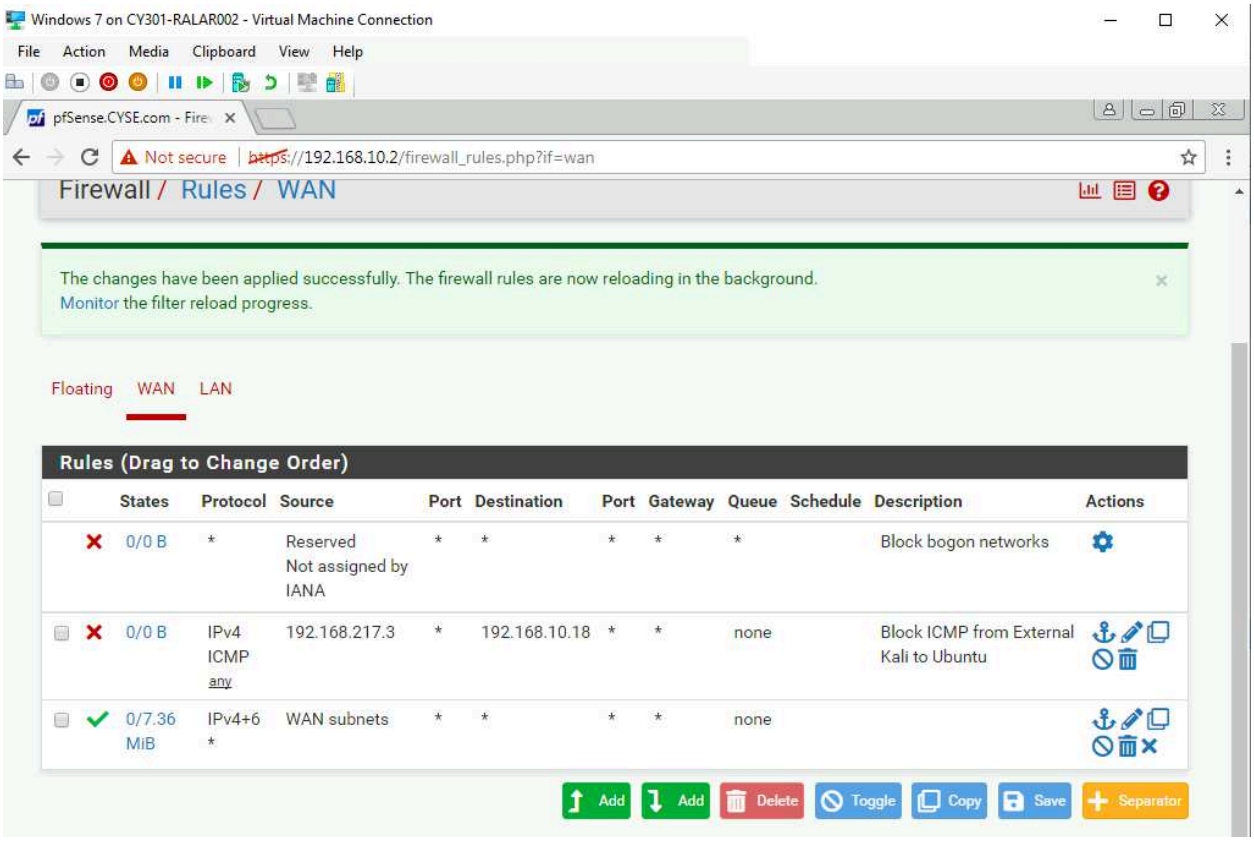
Another critical aspect was the observation of TCP SYN packets, especially when checking for open ports. External Kali sent SYN packets to various ports, and the responses indicated which ports were open and what services might be running.

Overall, the traffic patterns observed provide valuable insights into the network's layout and security. Active devices and their responsiveness can indicate how well-protected the network is. A network that shows minimal responses may have strong security measures in place, while responsive devices could point to potential vulnerabilities.

Task B: Protect Your Network With A Firewall

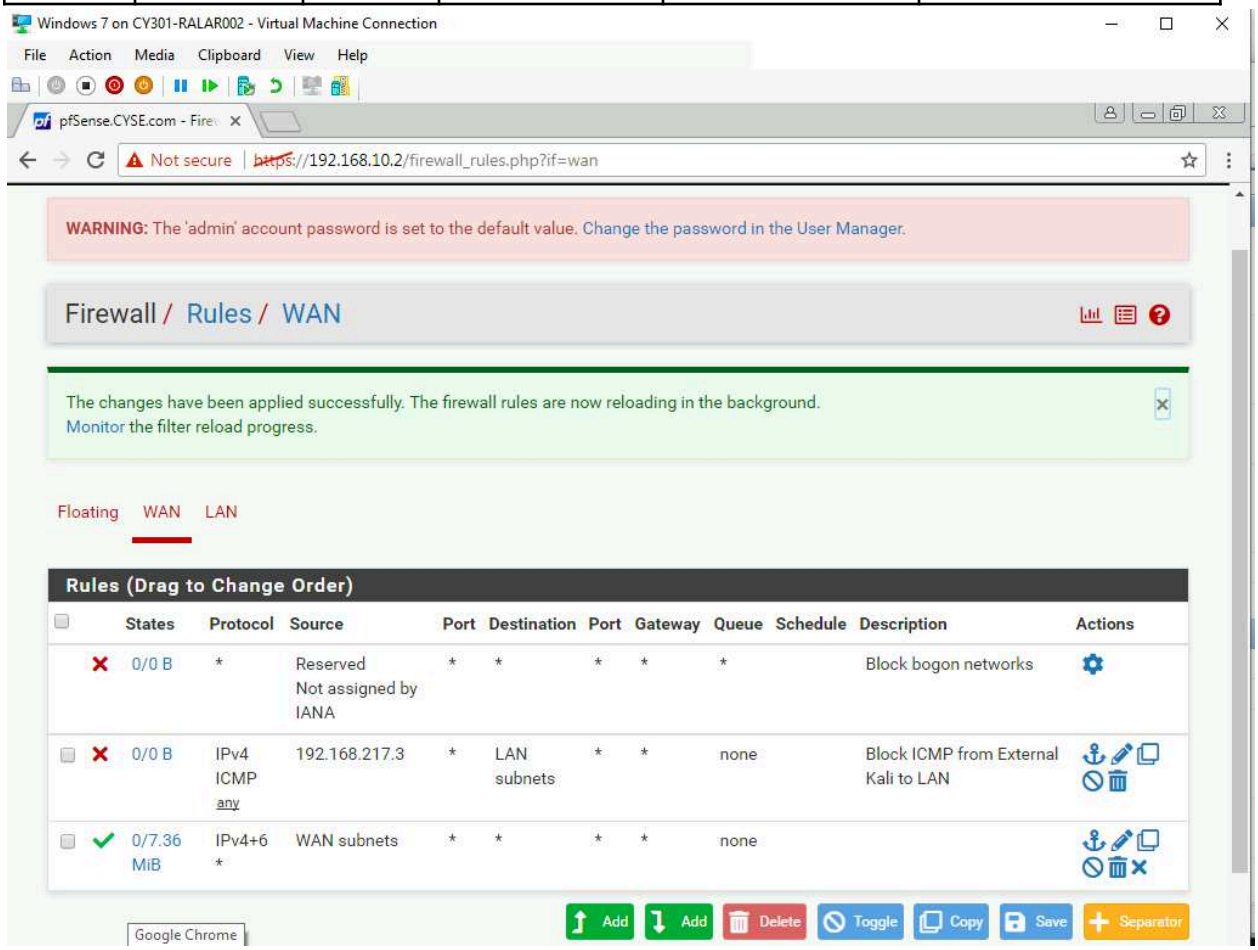
1. Configure the pfSense firewall rule to block the ICMP traffic from External Kali to Ubuntu VM

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



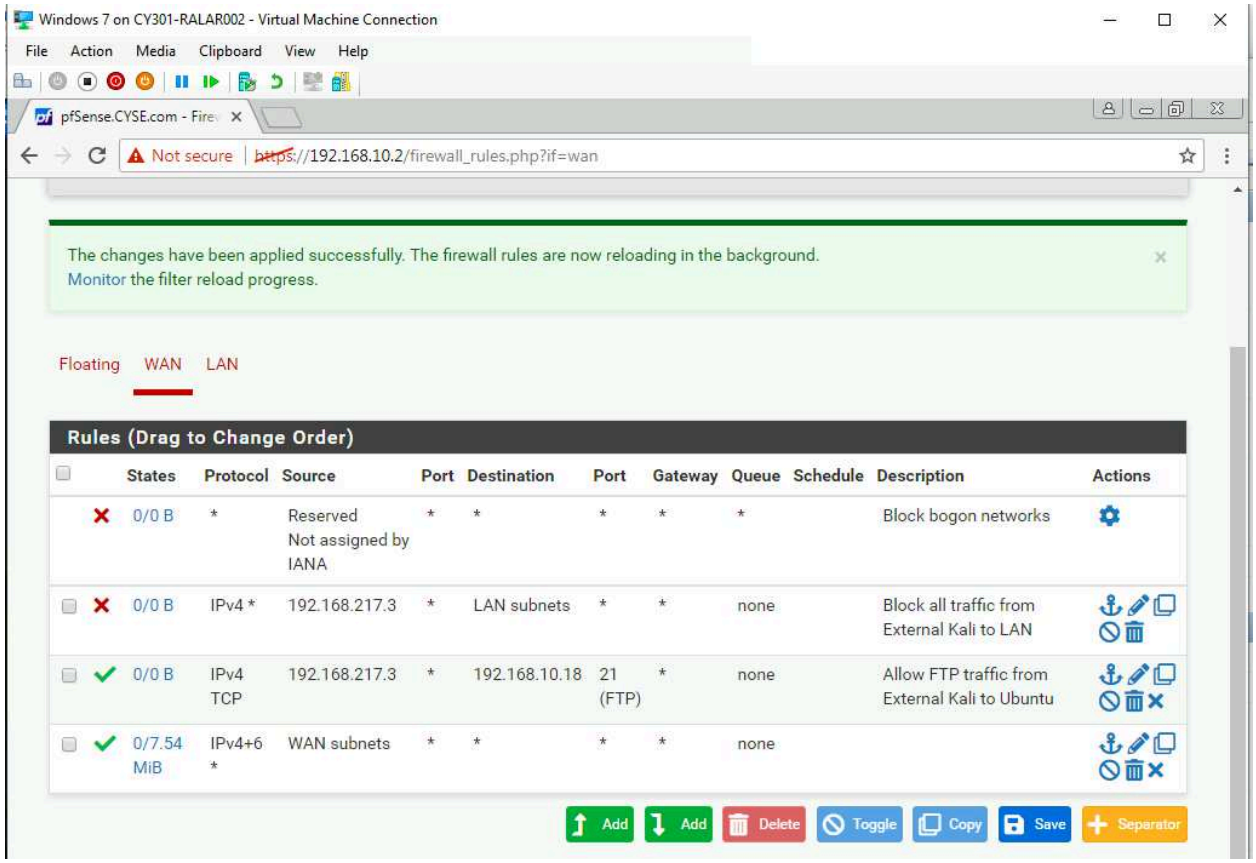
2. Clear the previous firewall policies and configure the pfSense firewall to block all ICMP traffic from External Kali to the LAN side

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if applicable)
2	WAN	Block	192.168.217.3	192.168.10.0/24	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 applicable)
2, 3	WAN	Block then allow	192.168.217.3	Block: 192.168.10.0/24 Allow: 192.168.10.18	TCP



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

   The difference now is that External Kali is no longer able to probe the hosts on the LAN network due to the block rules I configured. I am no longer able to get any information about the open ports on the LAN. If I attempt to scan Ubuntu on port 21, basic FTP information is given, but not much else.