CYSE 301: Cybersecurity Technique and Operations

Assignment 3: Sword vs. Shield

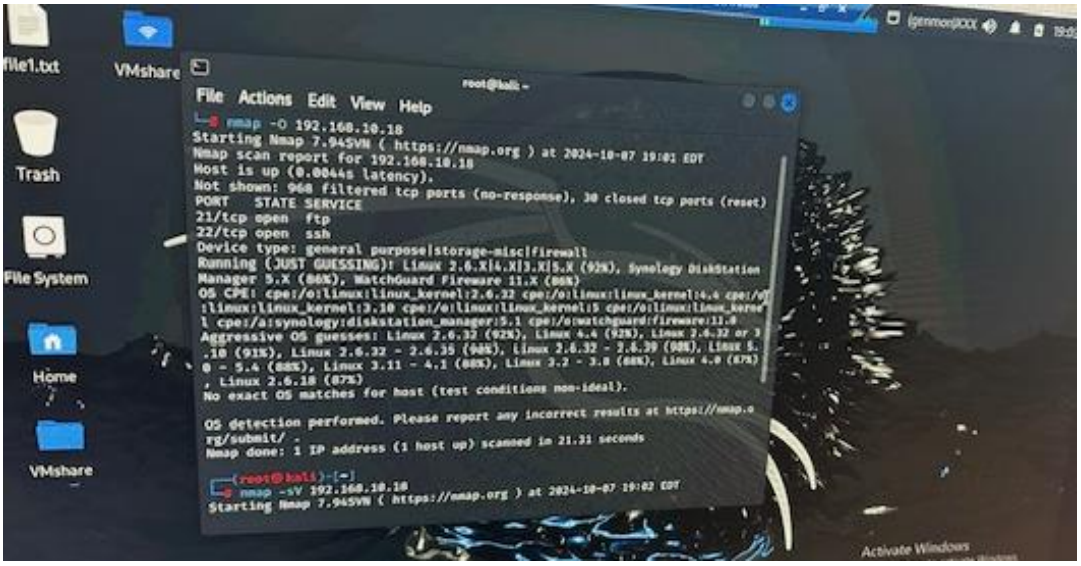
In this assignment, you will act as an attacker to identify the vulnerabilities in the LAN network and a defender to apply proper countermeasures. You need to provide a screenshot for each task below.

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.

I used the nmap -O 192.168.10.18 command to see that ftp and ssh packets were open on the Ubuntu network.



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 the Wireshark scan I saw a plethora of different packets from the network being sent a received. The Nmap command assisted with finding the packets very quickly. Some protocols found include TCP, SSH, ICMP, FTP, and ARP. I found that the TCP packets appeared the most while Arp packets were found the least. I also attempted to scan the Internal Kali VM Ip address, but the packets didn't appear. So, the network Ip I used was ubuntu, and that allowed the packets to appear. TCP packets, also known as Transmission Control Protocols, are packets that ensure data is successfully transmitted between devices

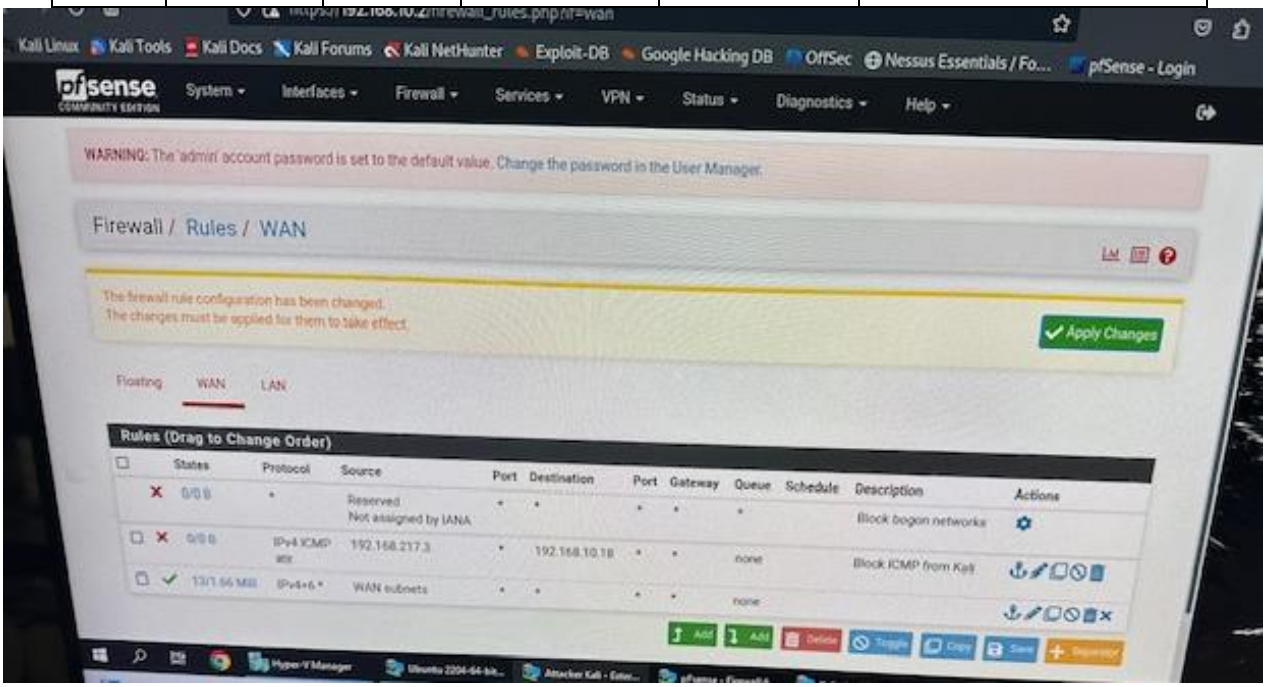
that are connected on a network. ARP packets, or Address Resolution Protocol and this is used to connect IP address to MAC address of the devices on the network. Even though those were the most, and least displayed packets on the Wireshark, there was a total of 2049 packets found. The was 100% packets received and zero packets lost for a clean transfer.

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.

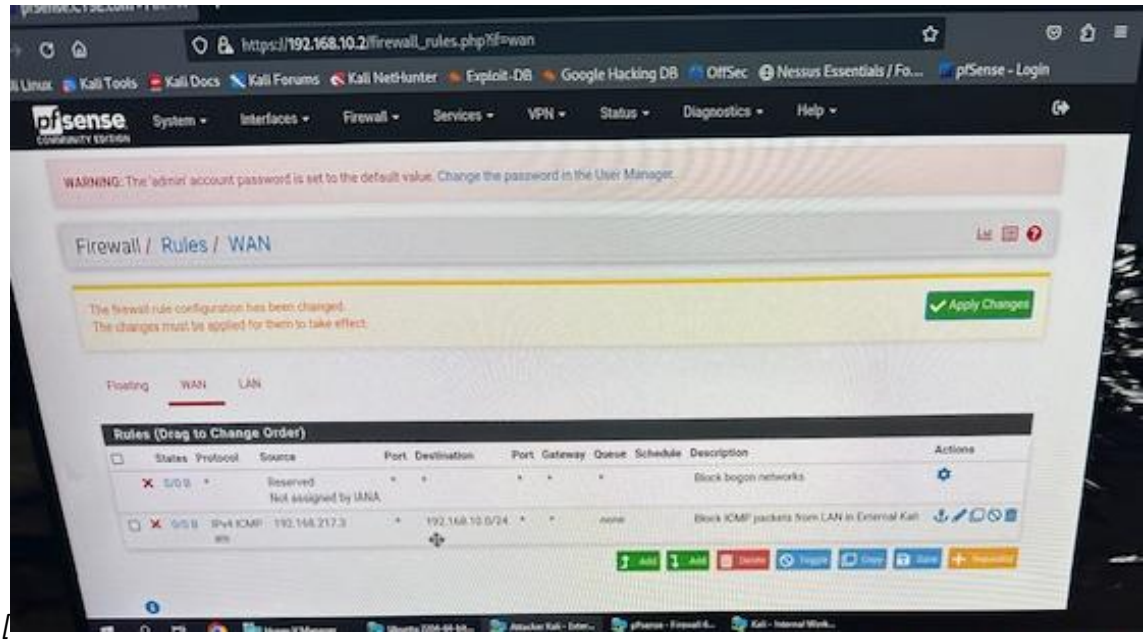
Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
1	WAN	Block	192.168.217.3	192.168.10.18	ICMP



I went to the pfsense bookmark on firefox and added the following rule.

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

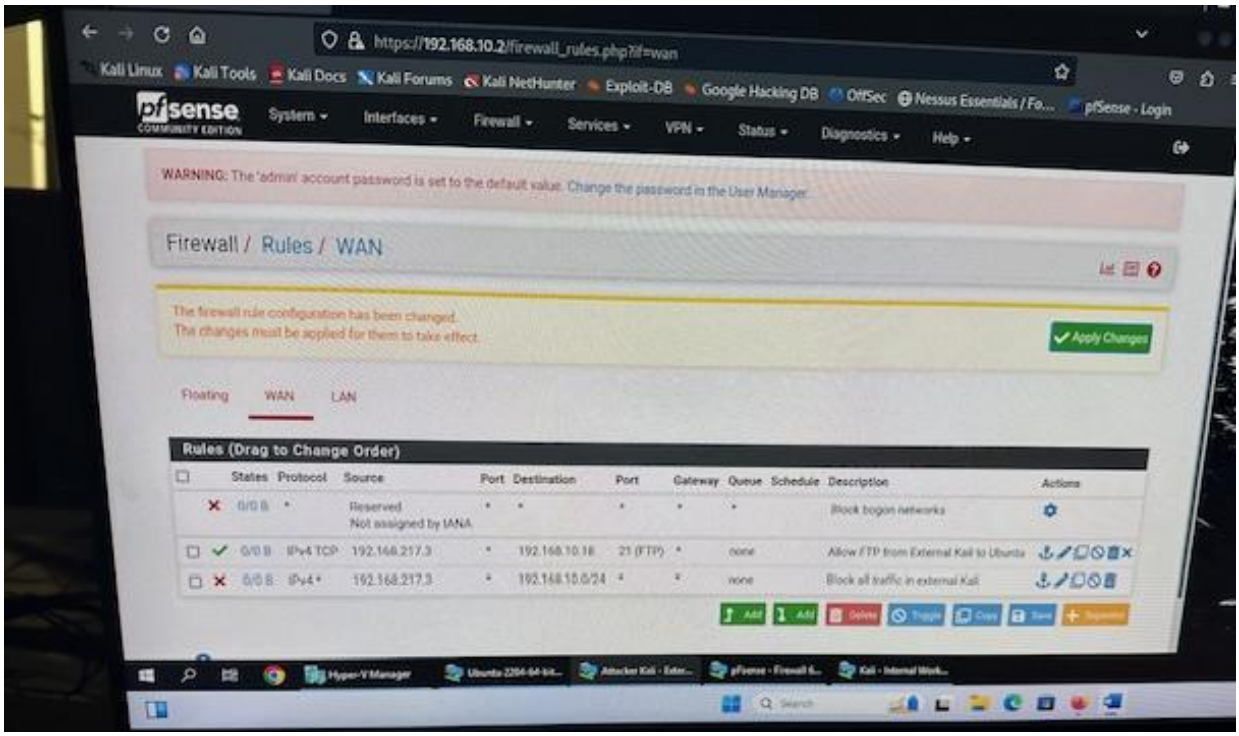
Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
2	WAN	Block	192.168.217.3	192.168.10.0/24	ICMP



I went to the pfsense bookmark on firefox and added the following rule after deleting the previous rules.

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)
3	WAN	Allow	192.168.217.3	192.168.10.18	TCP/FTP
4	WAN	Block	192.168.217.3	192.168.10.0/24	ANY



I went to the pfsense bookmark on firefox and added the following rule after deleting the previous rules. I added two rules this time, one to allow FTP/TCP packets and the other to block any other packets from coming through.

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

The traffic in B3 is all blocked.

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