CYSE 301: Cybersecurity Technique and Operations

Assignment 3: Sword vs. Shield

Michael Neuwirth

01235176

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 command in order to scan the network for any open ports and other information.

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.**

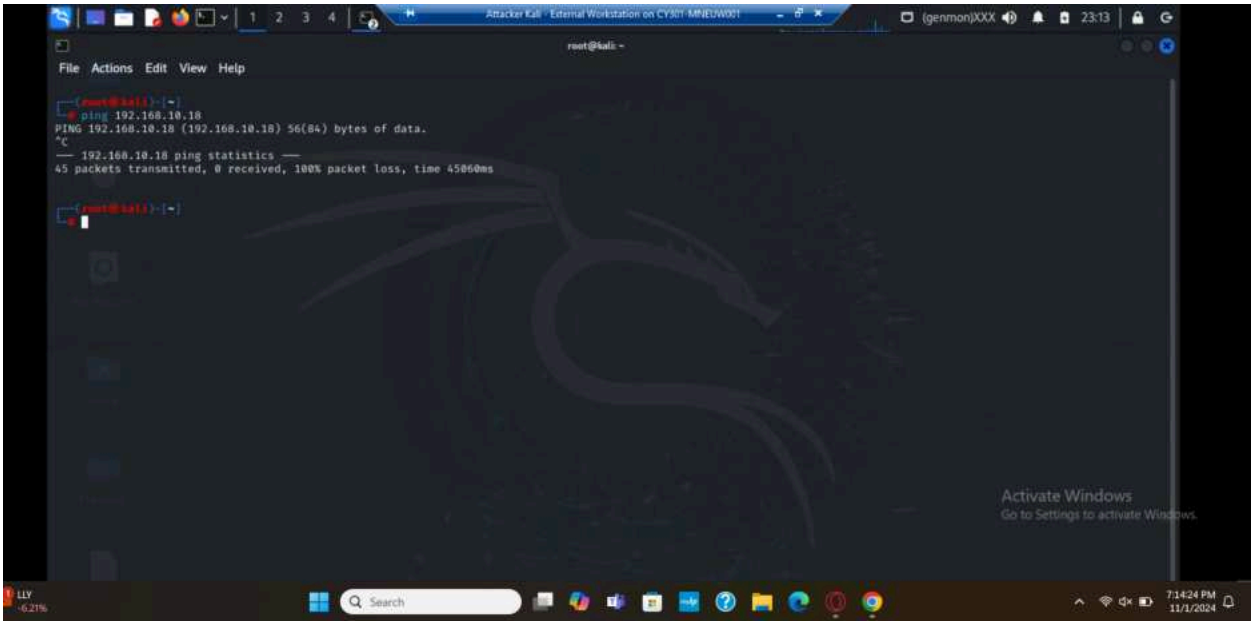
When running wireshark I noticed a lot of traffic at first as broadcast ARPs, all asking for different ips, originating from 192.168.10.2, I assume this is the first stage of NMAP as it tries to establish what ips are being used and listening on the network. After this large bevy of establishment there is a ton of syn and ack packages, between .10.13 (the internal kali I'm on) and .217.13 (the external attack kali) - each syn and ack is part of the three way handshake as the attack Kali attempts to scan and identify every single open port, there is about eight syn packages in a row, which are then met by 8 ack packages acknowledging the request. This goes on as nmap attempts to find information about all the open ports on the internal kali machine.

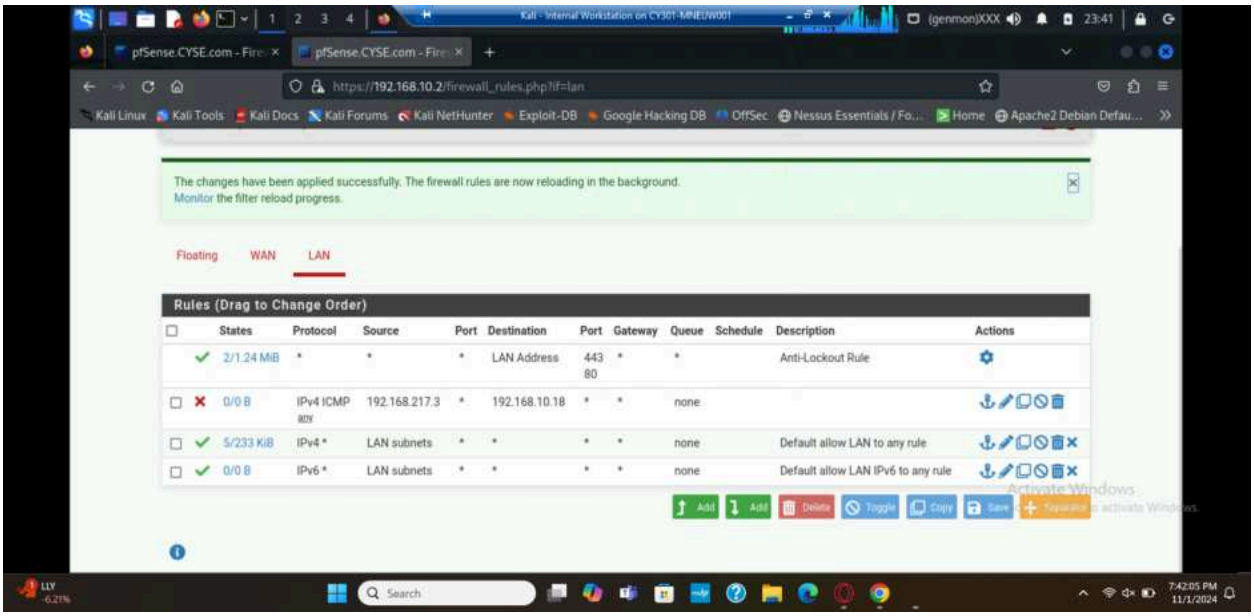
Task B: Shield – Protect your network with a firewall (10 + 10+ 20 + 20 = 60 points)

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)
1	LAN	BLOCK	192.168.217.3	192.168.10.18	ICMP

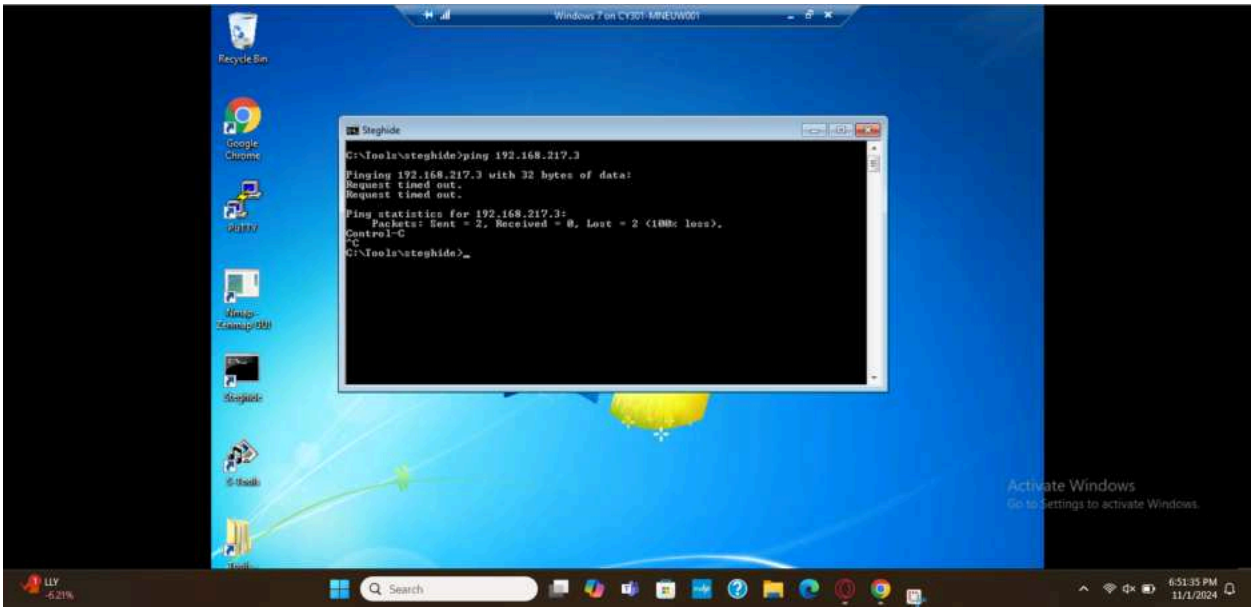


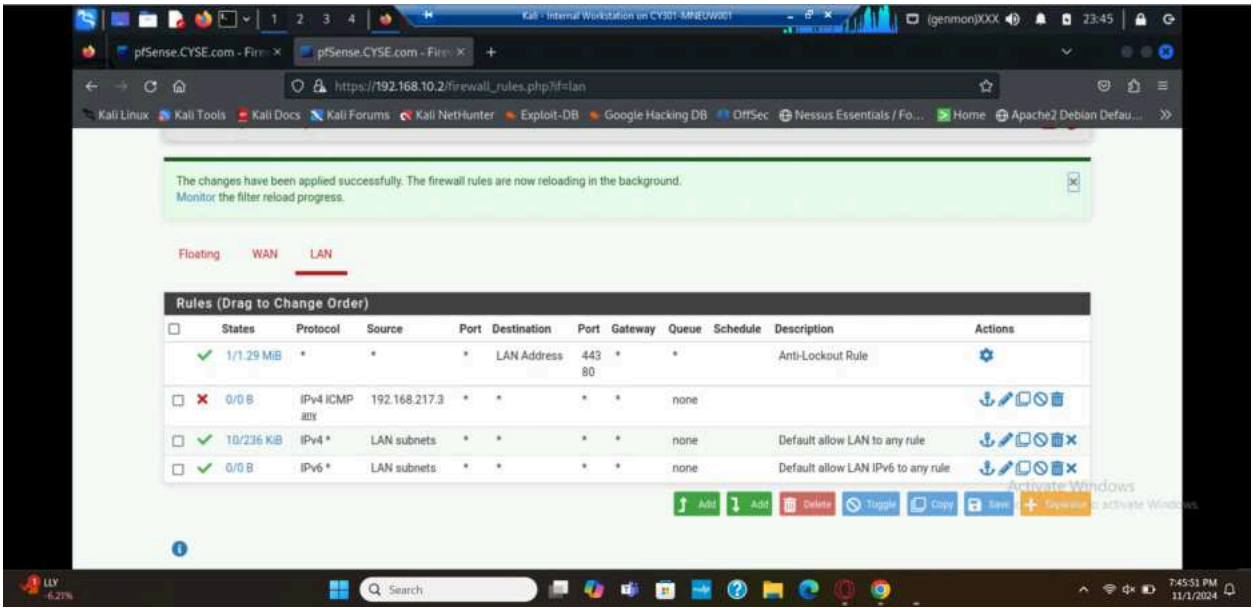


After setting up the firewall rule I logged into external kali which is under the firewall and attempted to ping the ubuntu in order to use icmp and it wouldn't ping, proving the firewall worked.

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)
1	LAN	BLOCK	192.168.217.3	*	ICMP





After setting up the firewall rule I logged into windows 7 which is under the firewall and attempted to ping the external kali in order to use icmp and it wouldn't ping, proving the firewall worked.

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)
1	LAN	PASS	192.168.217.3	192.168.10.18	FTP
2	LAN	BLOCK	192.168.217.3	*	*

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

Now when I attempt to use nmap the external kali is unable to get the information for all of the computers on the network as its traffic is blocked by the firewall.