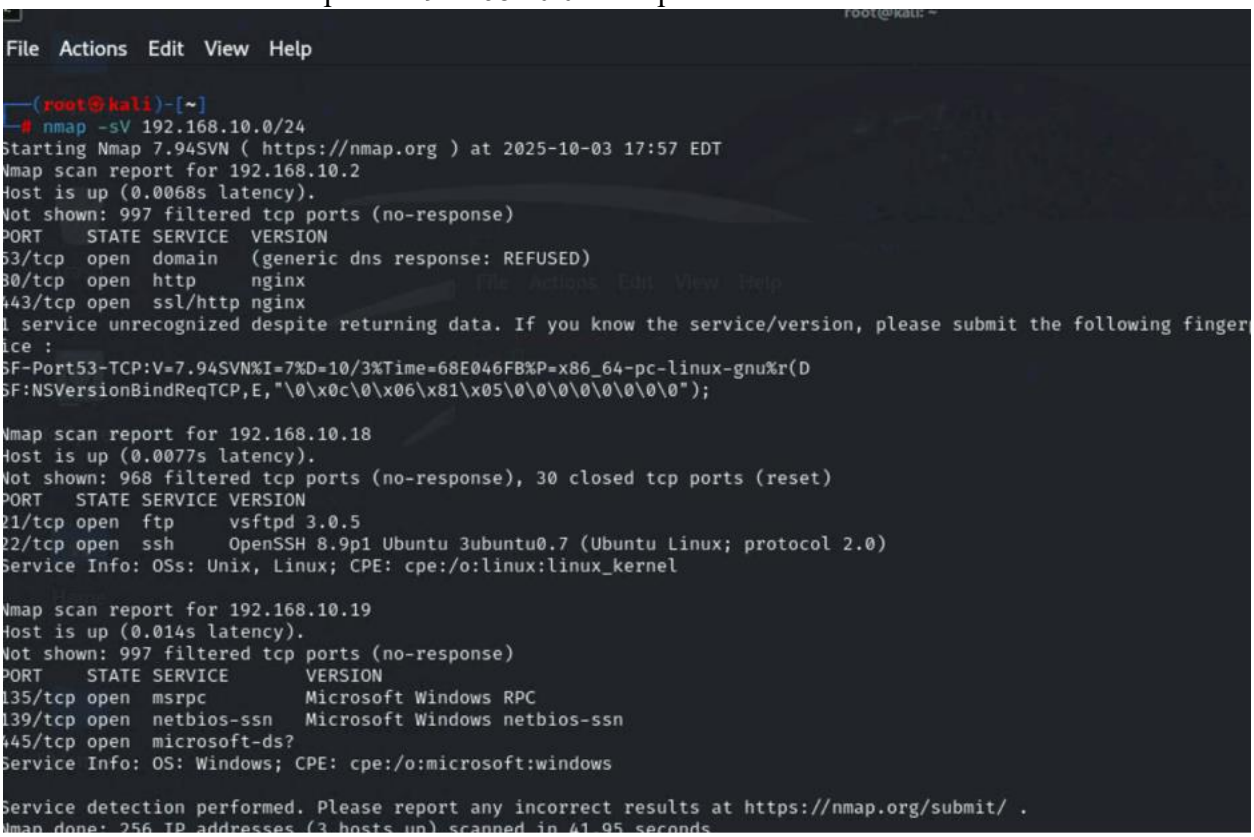
OLD DOMINION UNIVERSITY
CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS
Assignment #3 - Sword vs. Shield

Celeste Meraz-Luna
01302562

Task A: Sword - Network Scanning

Q1. 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 command nmap –sV 192.168.10.0/24 to profile basic information.



Q2. Run Wireshark in Internal Kali VM while External Kali is scanning the network. Discuss the traffic pattern you observed. What do you find? <u>Please write a 200-word essay to discuss your findings.</u>

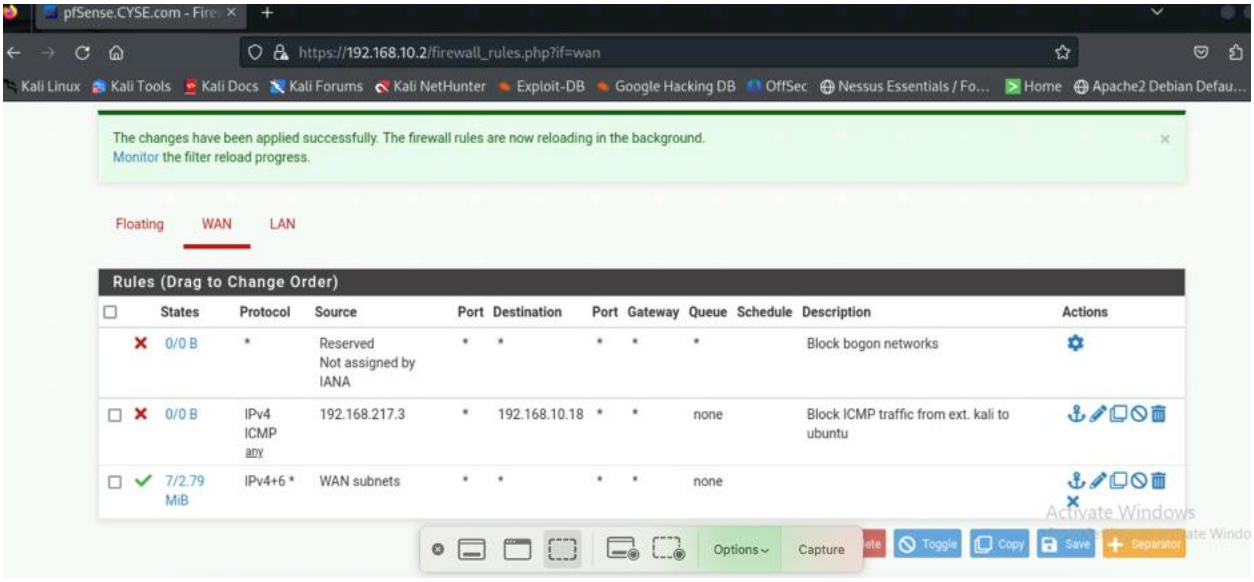
When running Wireshark on the Internal Kali VM while the External Kali conducted scanning, I observed distinct traffic patterns suggesting reconnaissance activity. The capture shows numerous TCP connections between 192.168.217.3 and 192.168.10.13, with a mix of SYN, ACK, RST, and HTTP requests. For open ports, the scan triggered partial TCP handshakes, indicating successful reachability. Conversely, closed or filtered ports responded with RST, ACK packets, signaling rejection of connections. I also noted HTTP requests such as GET and OPTIONS sent to the target host. This suggests service enumeration, where the scanning systems were not only identifying open ports but also attempting to probe web services for versioning or configuration details. The repetitive sequence of SYN and RST packets highlights how scans systematically sweep across port ranges. The clear pattern of rapid connection attempts across multiple ports is a strong indicator of network scanning,

easily identifiable by intrusion detection systems. These findings emphasize how noisy and detectable such scans can be, reinforcing the importance of network monitoring. Firewalls, IDS/IPS tools and strict access controls can help reduce exposure to this type of reconnaissance.

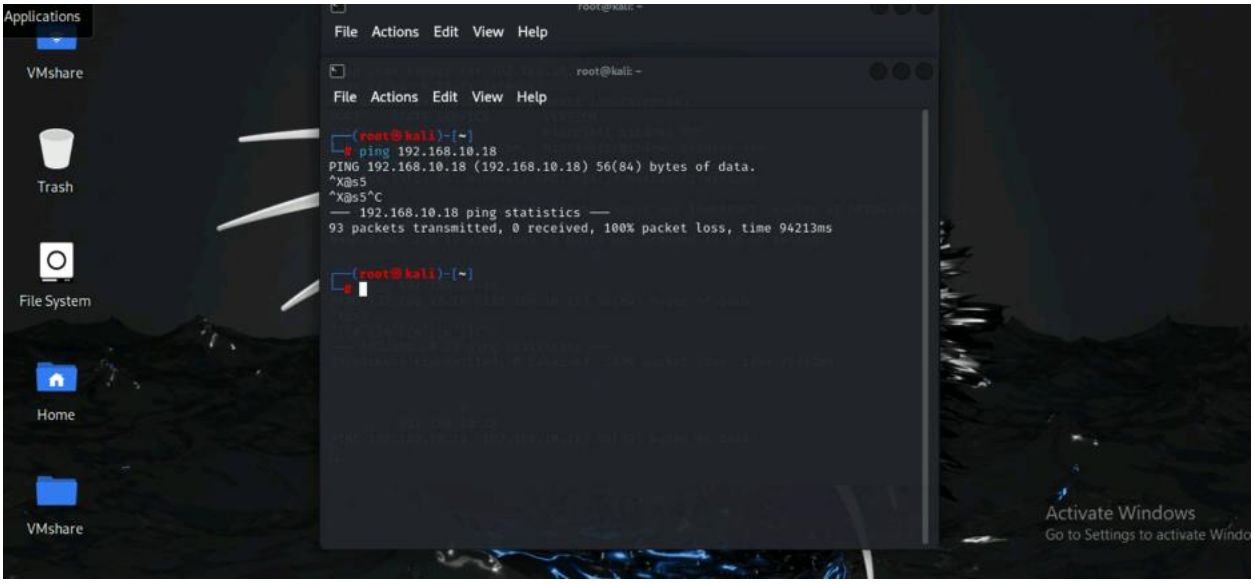
Task B: Shield – Protect your network with a firewall

Q1. 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

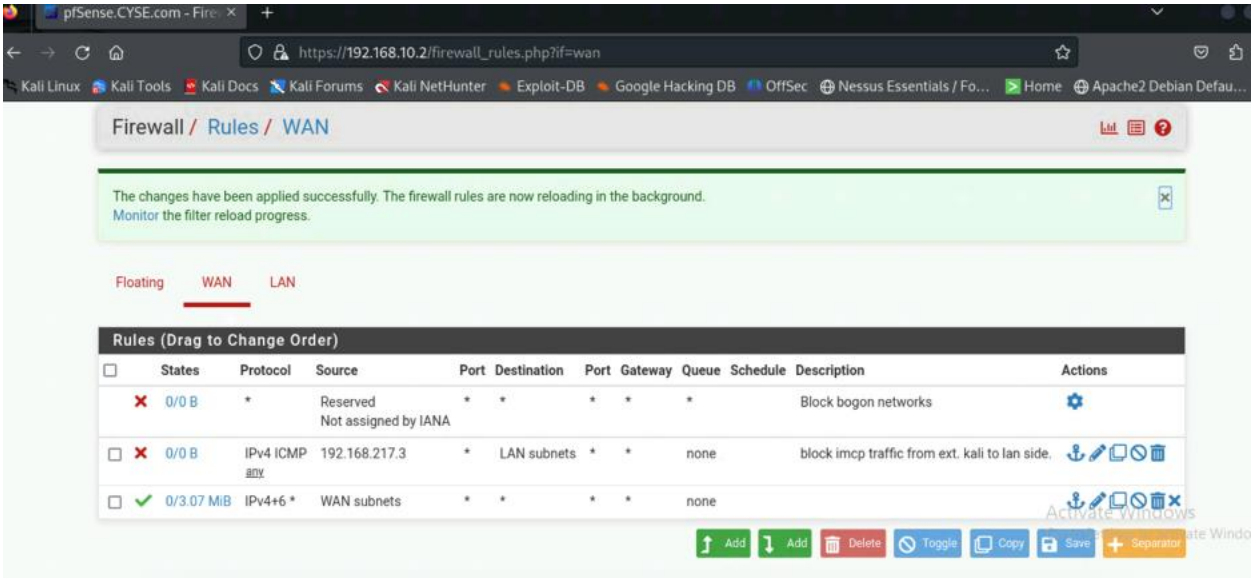


Pinging ubuntu from external Kali did not work.

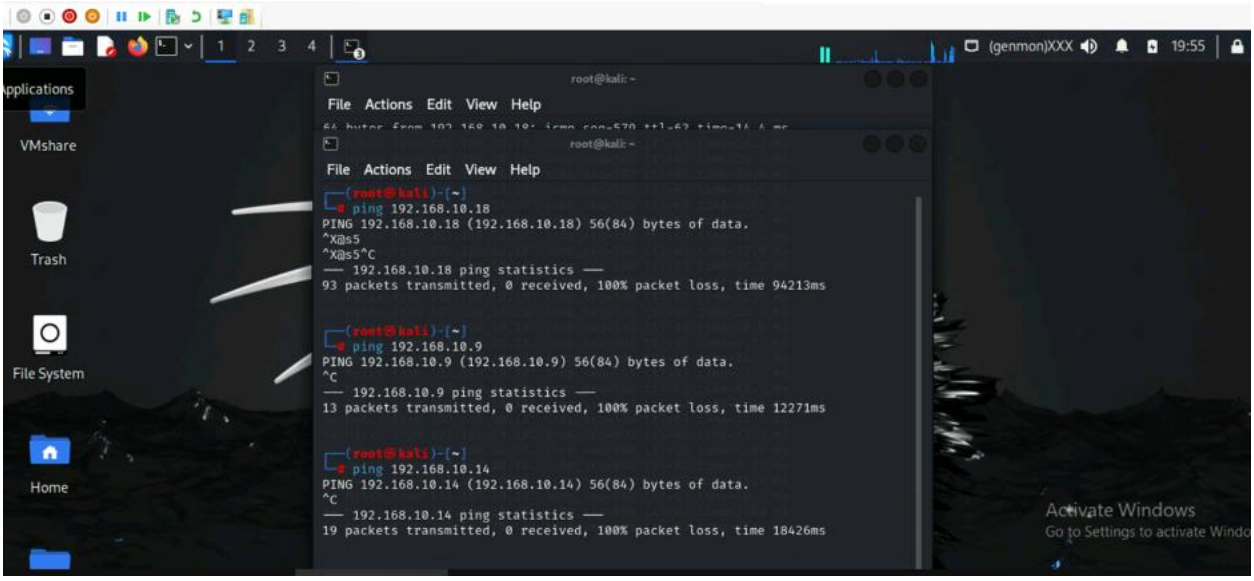


Q2. Clear the previous firewall policies and configure the pfSense firewall to block all ICMP traffic from External Kali to the LAN side.

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

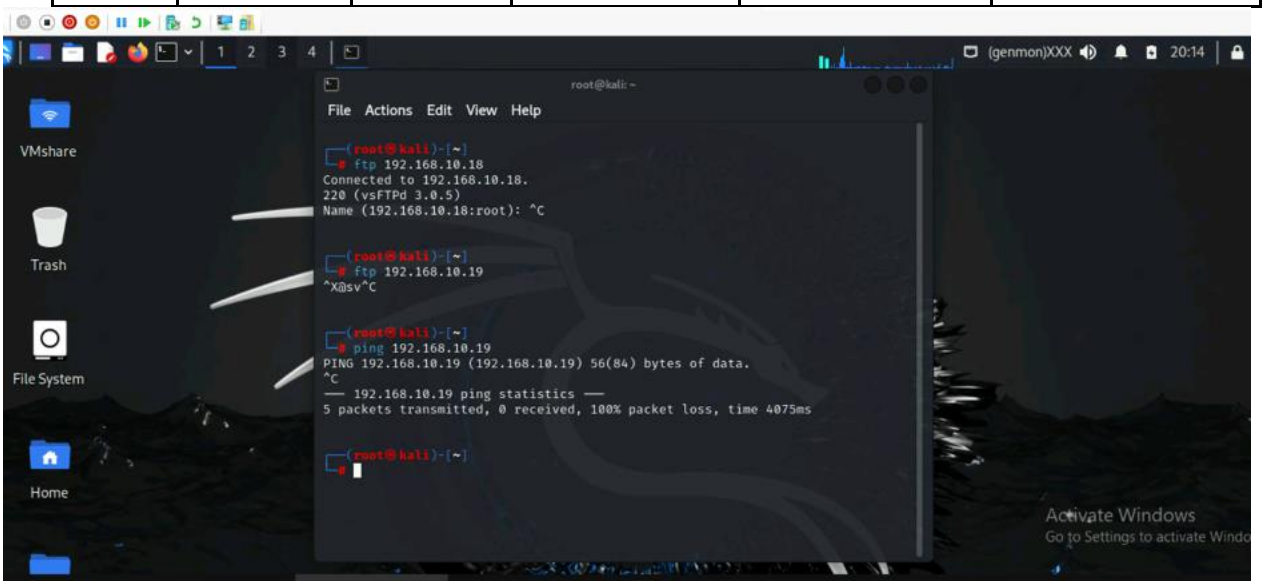


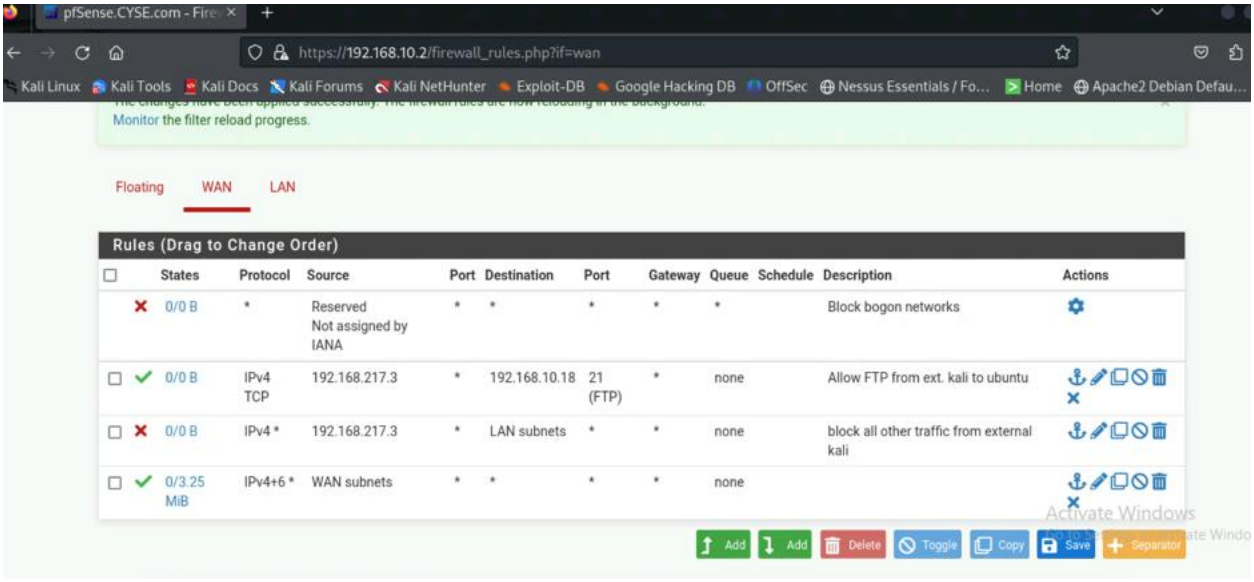
After I tried to ping some LAN addresses and it did not work.



Q3. 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	Block except for FTP protocol towards Ubuntu	192.168.217.3	192.168.10.0/24 192.168.10.18	FTP





Q4. Keep the firewall policies you created in Task B.3 and repeat Task A.1. What's the difference?

In the first Task A.1, Nmap was able to detect multiple hosts and open services within the 192.168.10.0/24 network. However, after the firewall rules, the second scan had fewer hosts and open ports. Some systems that were available before the rule are no longer effective. This difference demonstrates that firewall policies effectively filtered or blocked Nmap's probes, limited network visibility and reduced the exposure of internal services to scanning attempts.