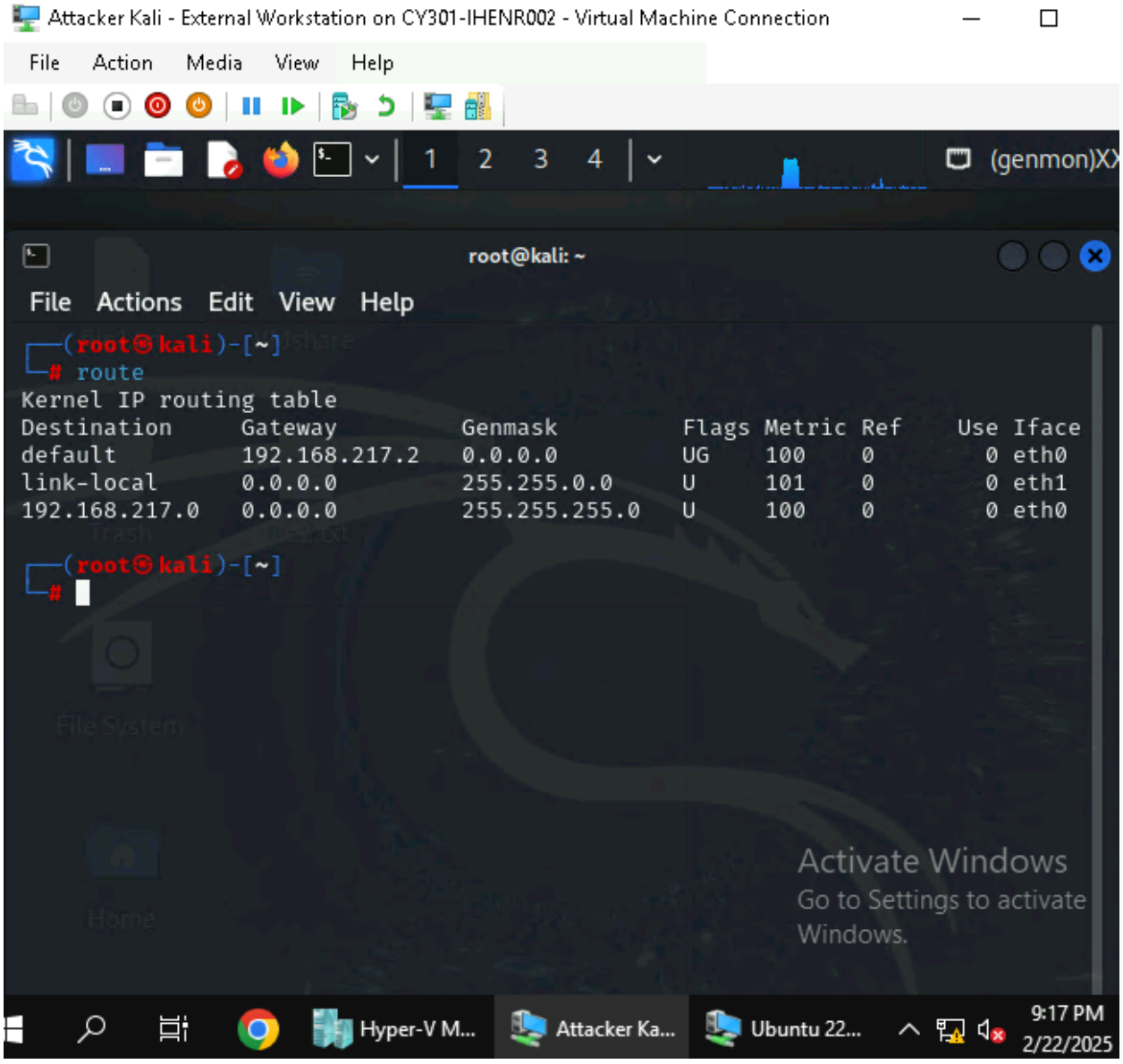
India Henry
CYSE 301 - 32781
Shideh Yavary Mehr
28 February 2025

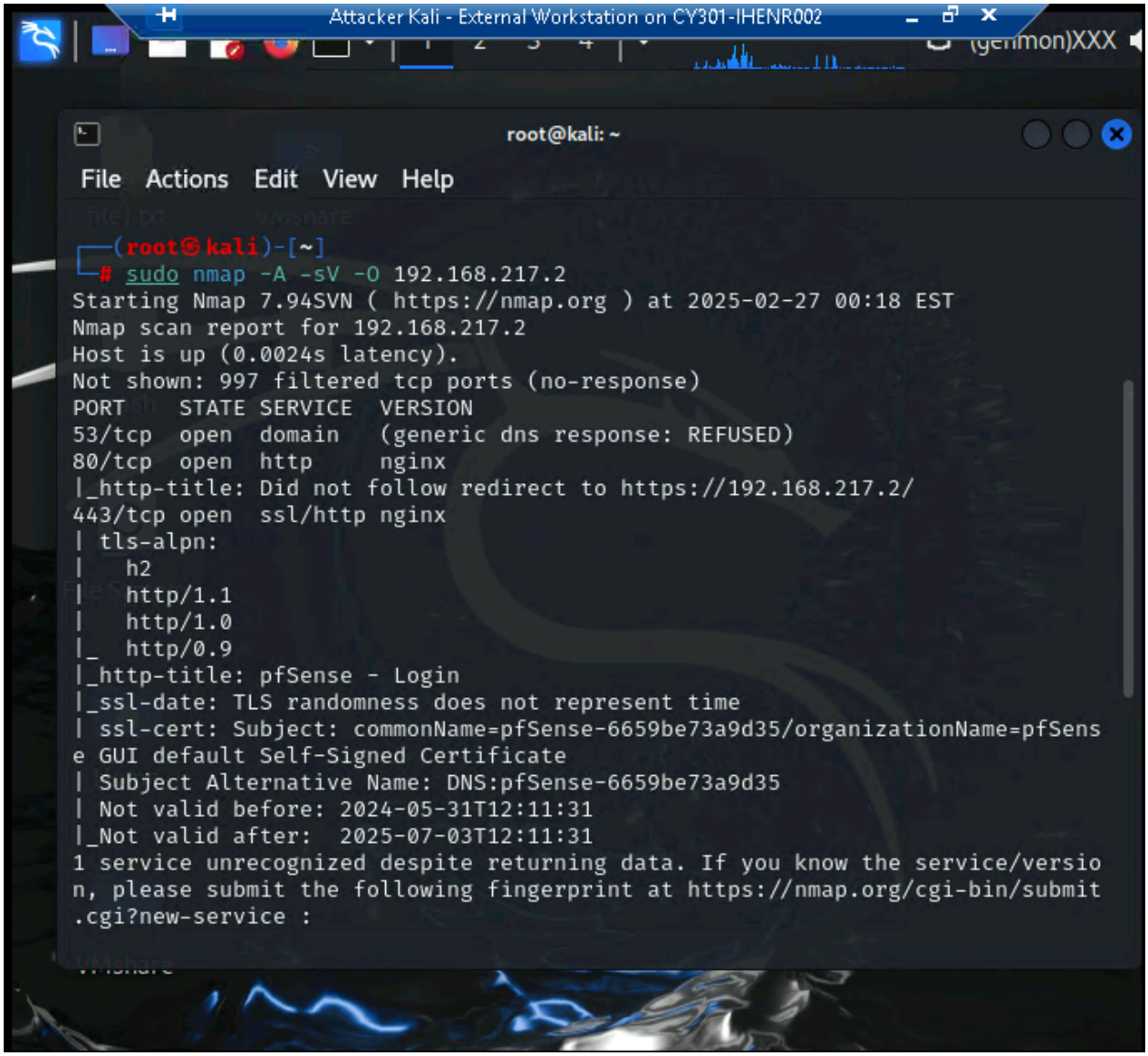
CYSE: Cybersecurity Techniques and Operations
Assignment: Lab 3 - Sword v Shield

Task A: Sword - Network Scanning

1. **Use nmap to profile the basic information about the subnet topology (including open ports information, operating systems, etc). You need to get the service and backend software information associated with each opening port in each VM**



Ran route command to find external kali's ip and local ip

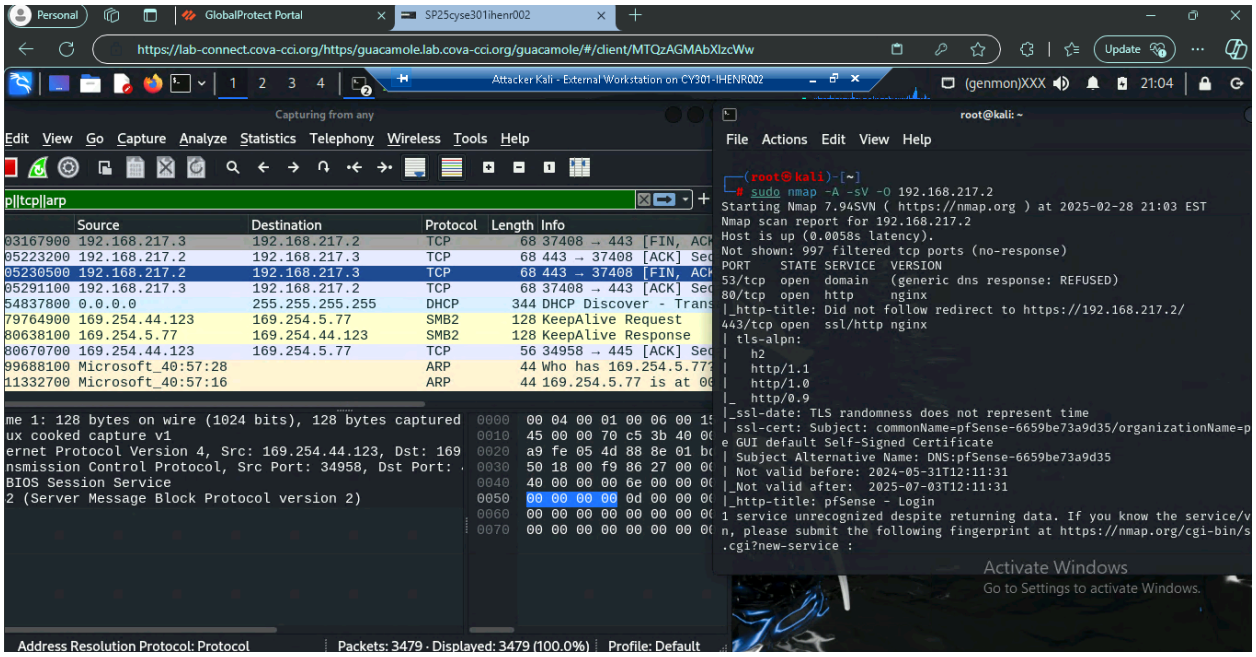


Ran nmap scan using ip from first step

2. **Run Wireshark in Ubuntu VM while External Kali is scanning the network. Discuss the traffic pattern you observed. What do you find?**

   During the scan, it seems that 100% of the packets that were transmitted were between ICMP, TCP, and ARP. After the scan was complete, I filtered out the packets to see exactly what percentage was ICMP, TCP, and ARP packers. ICMP had 0.2% of the packets, it was between the same two IP addresses, usually this is to see if there are any ports open. This process pings different ports on ubuntu to see if they are open to transmitting packets with external kali. 97% of the traffic was TCP traffic, this could be an attempt to establish connections between different ports. This traffic also confirms which ports are open and accepting packets from external kali, allowing packet transmission to occur between external kali and ubuntu. ARP packets held another 2.2% of the traffic

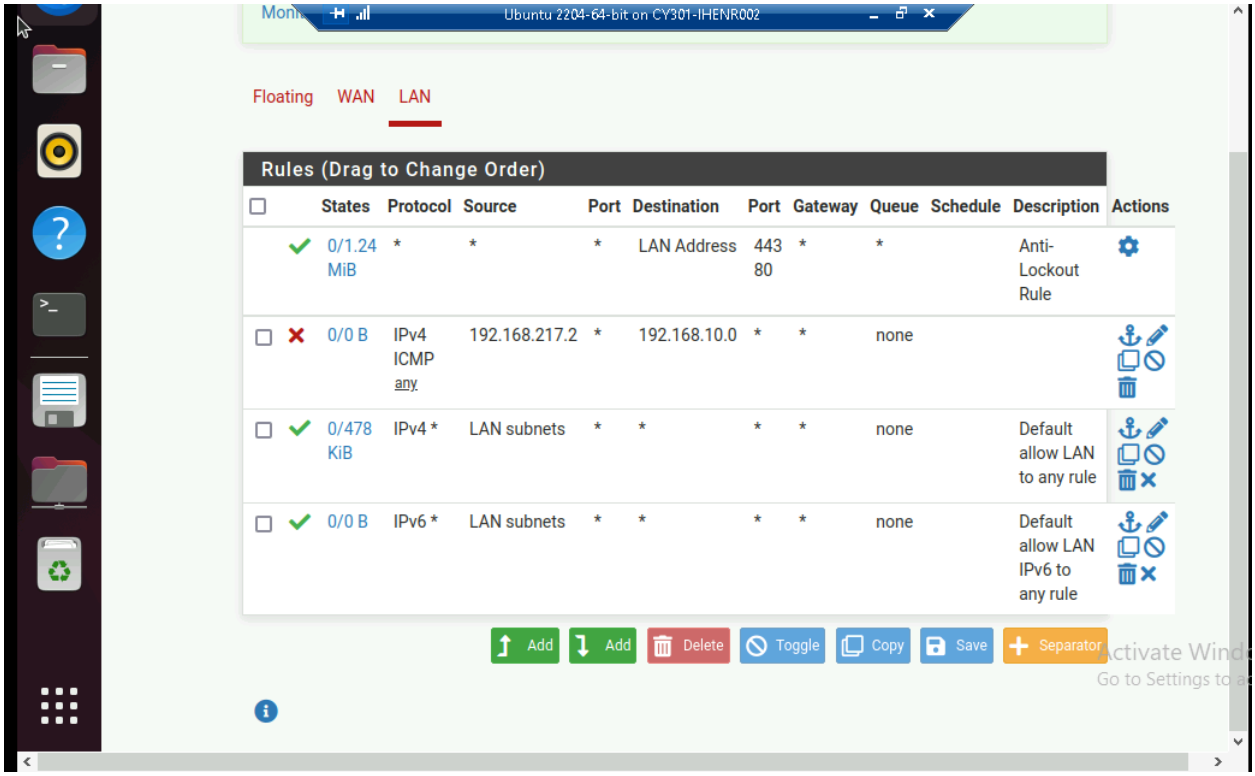
that happened during the nmap scan. ARP broadcasts a packet across the network to validate network IDs that are open to communicating with external kali. This is a process that goes through until it finds a destination IP with an open port to share the source IP with. These processes can be considered dangerous when using nmap nonconsensually because they share information about open ports which can be used to exploit a network.



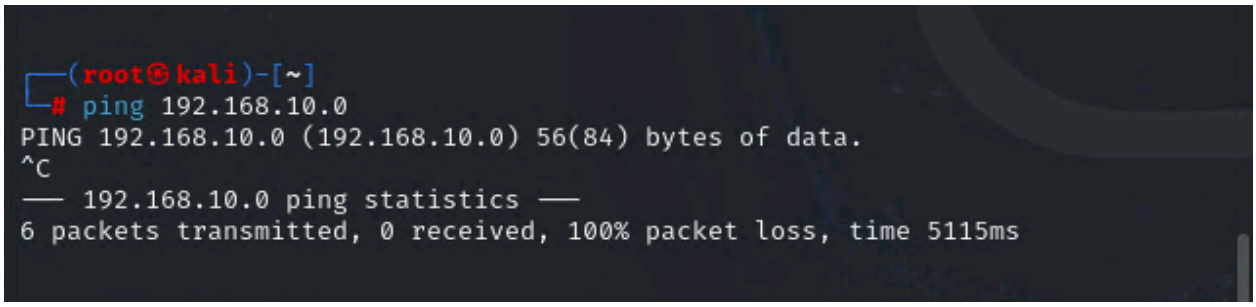
Task B: Shield - Protect your network with firewall

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)
1	LAN	Block	192.168.217.2	192.168.10.0	ICMP



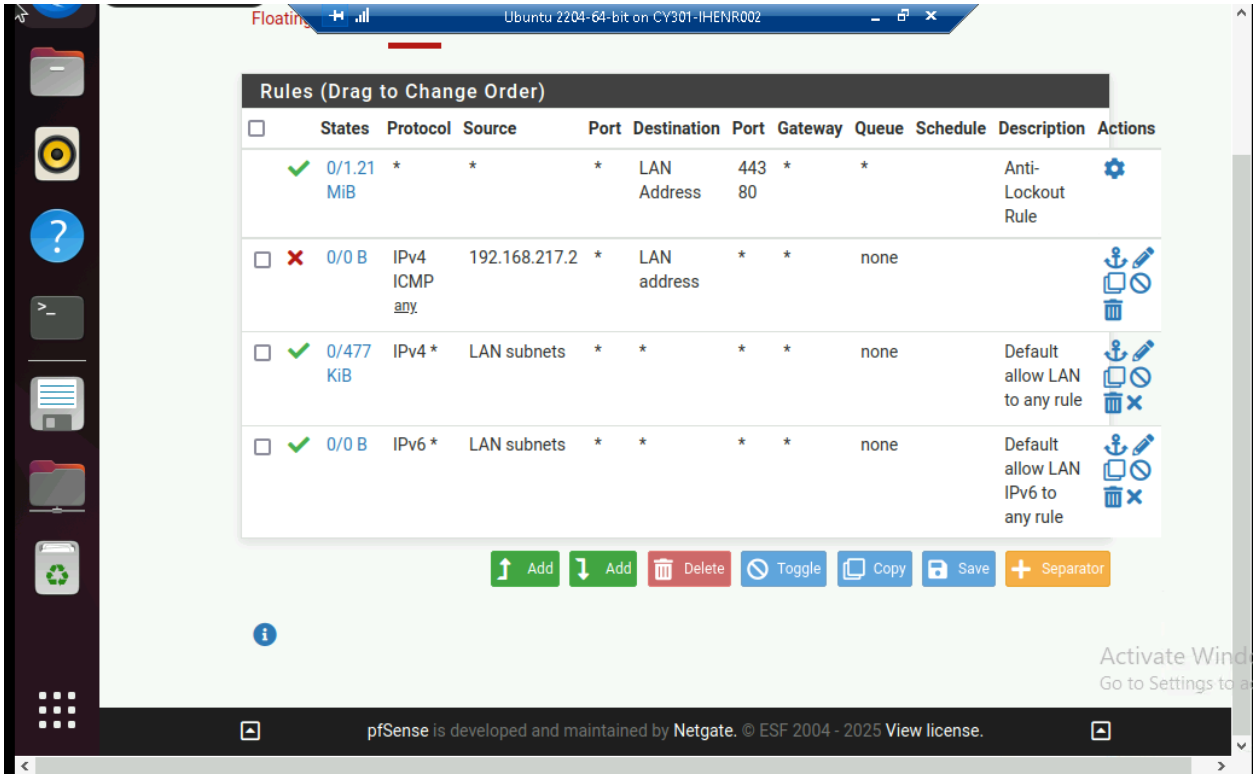
I added the above rule into the firewall. It should block any traffic going from external kali (192.168.217.2) to ubuntu (192.168.10.0).



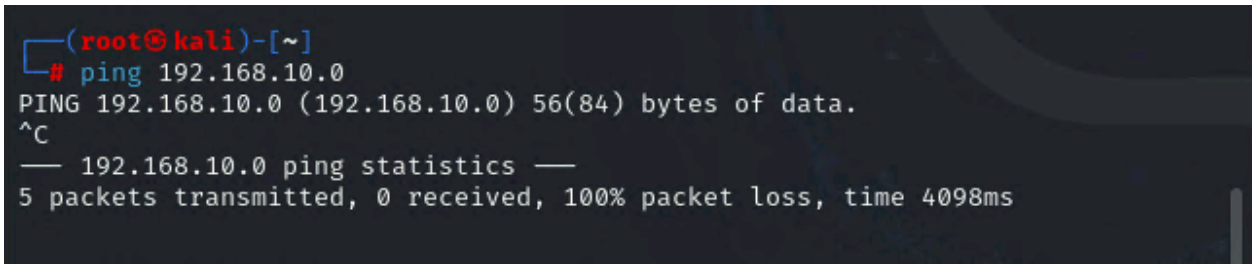
To check if the rule worked, on external kali I pinged the IP for ubuntu, the rule was successful because the firewall prevented the traffic from going through.

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	LAN	Block	192.168.217.2	LAN	ICMP



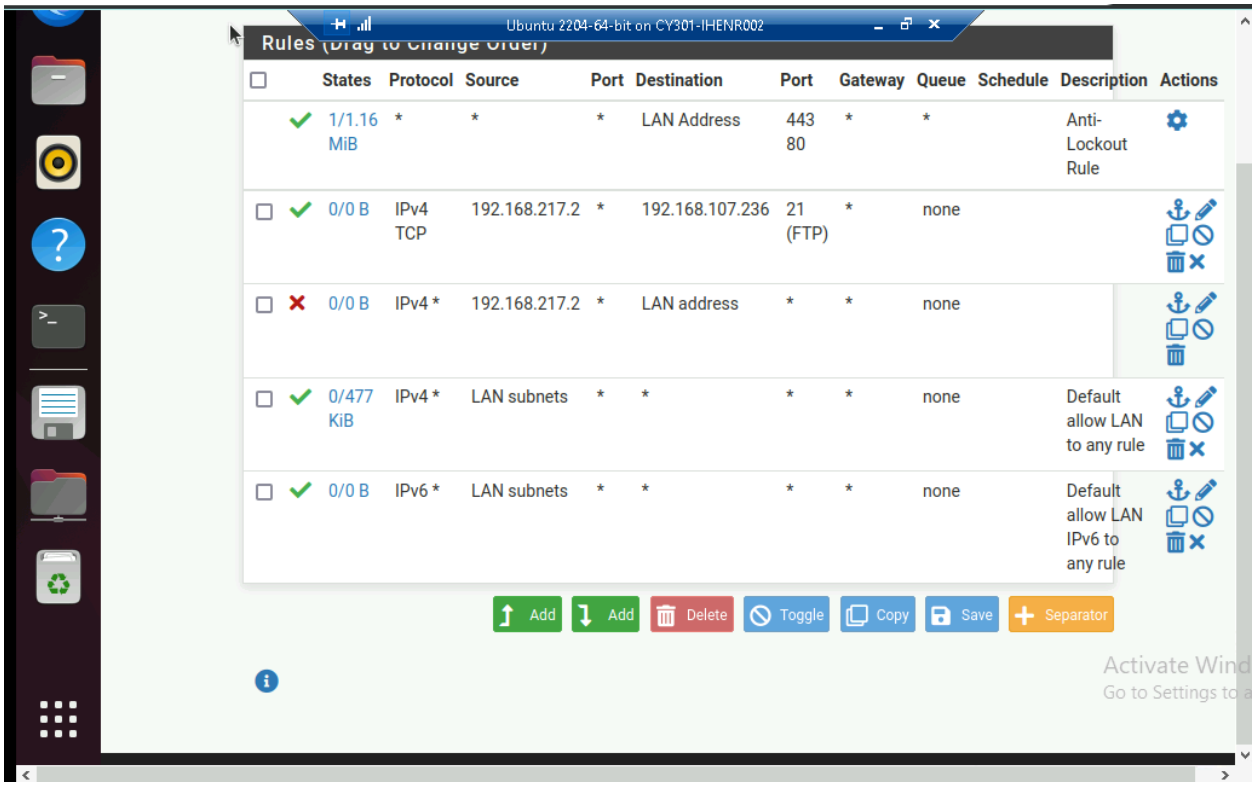
I added the above rule which would block any traffic from external kali to the LAN address.



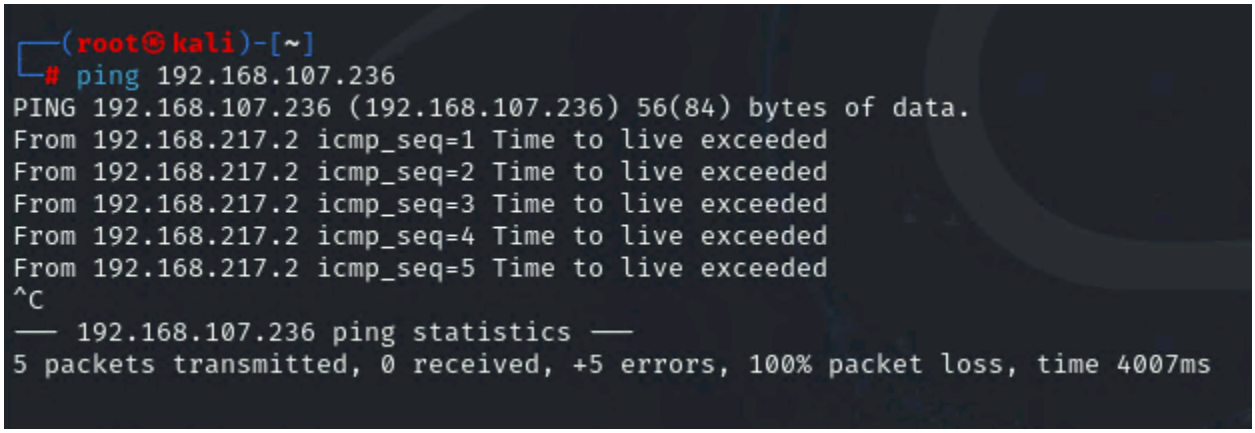
To check if the rule worked, I pinged ubuntu and the rule blocked traffic from getting through.

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 2008.**

Rule #	Interface	Action	Source IP	Destination IP	Protocol (Port # if applicable)
3	LAN	Allow	192.168.217.2	192.168.107.236	FTP (21)
4	LAN	Block	192.168.217.2	LAN	Any

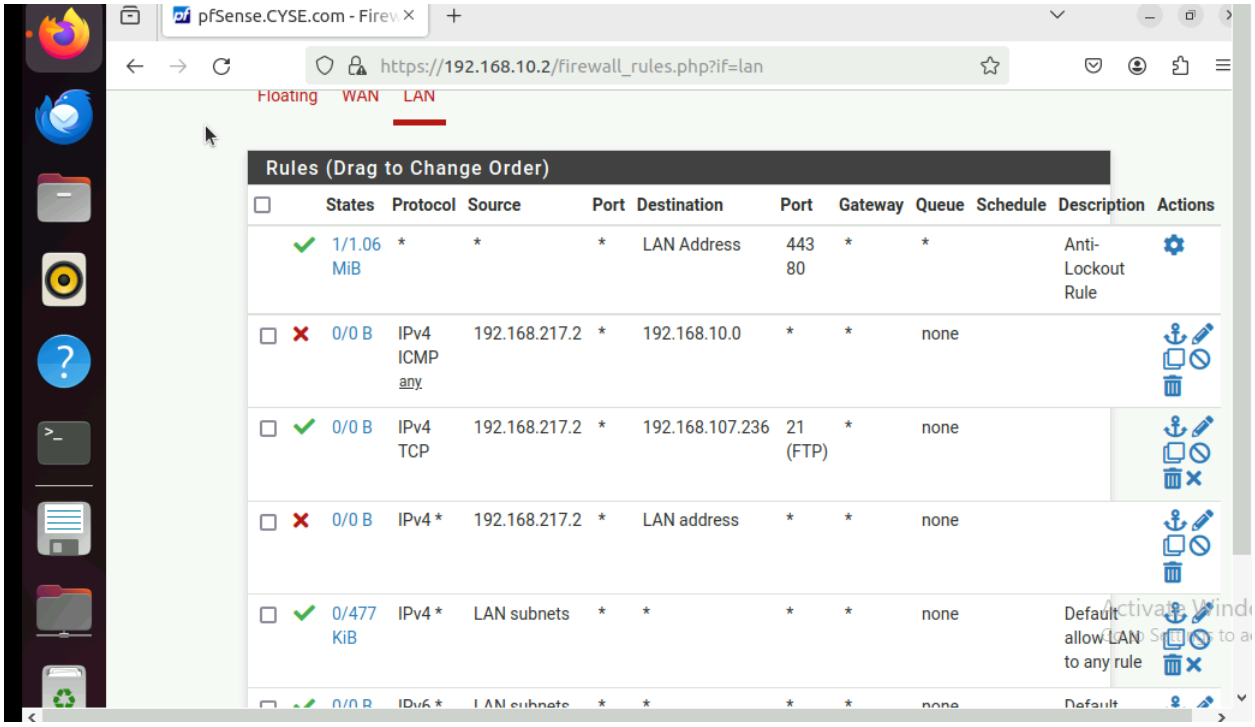


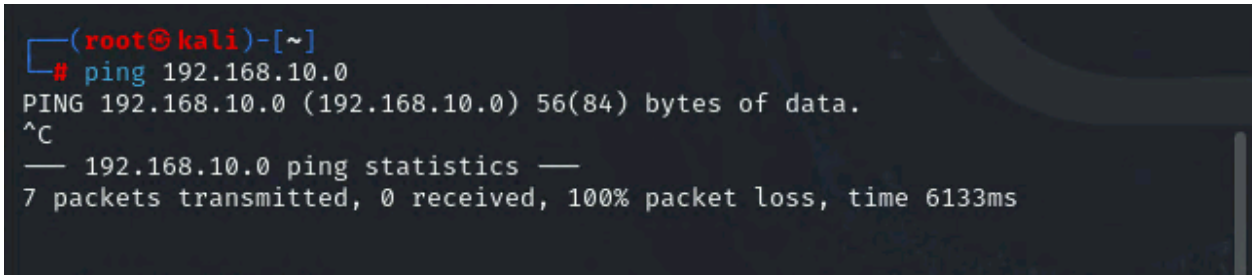
I added two rules: the first rule allows for FTP traffic from external kali to reach windows 2008, the second rule blocks all other traffic.



To see if the rule worked, I pinged the windows IP and while the packets were sent, they exceeded the time to be received.

4. **Keep the firewall policies you created in Task B3 and repeat Task A1. What's the difference?**





I kept the rules from the previous step, then added back the rule from the first step. Doing this I tried to ping Ubuntu and all packets were dropped.