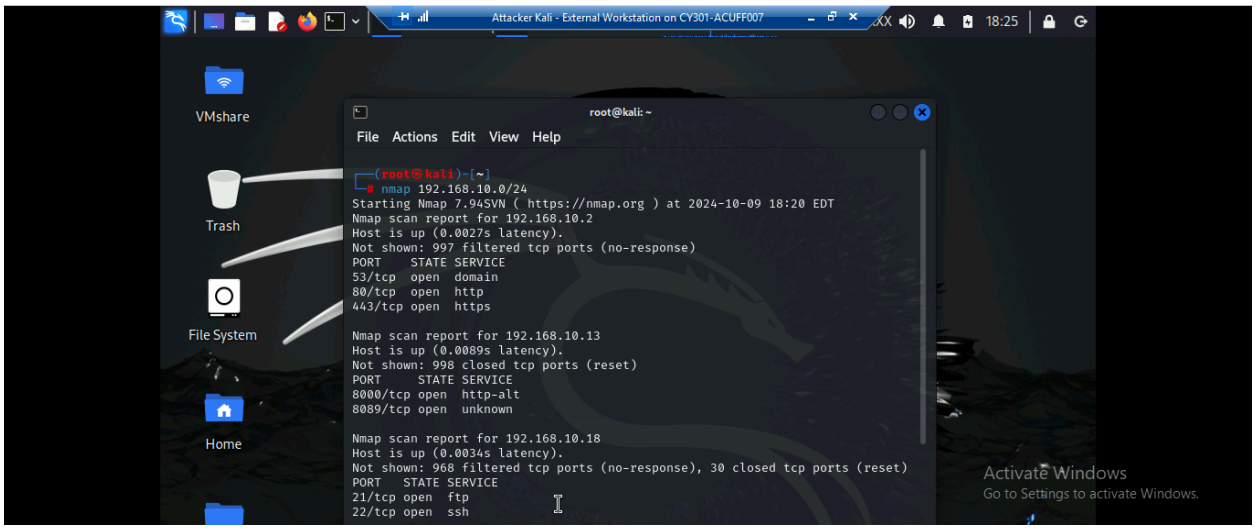
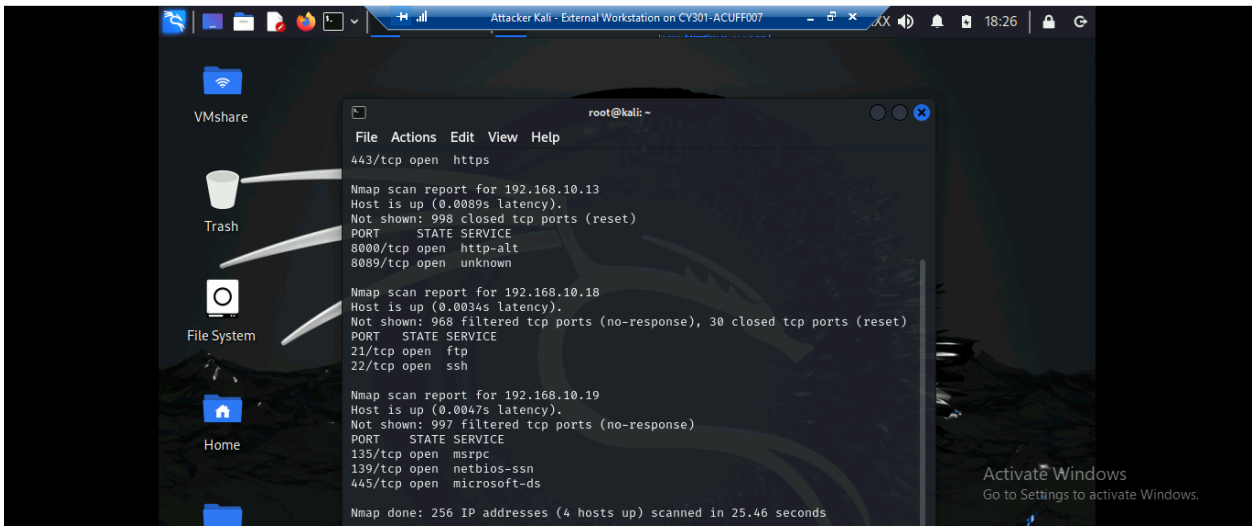
Task A: Sword - Network Scanning (20 + 20 = 40 points) Power on the listed VMs and complete the following steps from the External Kali (you can use either nmap or zenmap to complete the assignment) • External Kali • pfSense • Ubuntu • Windows Server 2022 Make sure you didn't add/delete any firewall policy 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.





2. Run Wireshark in the 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.

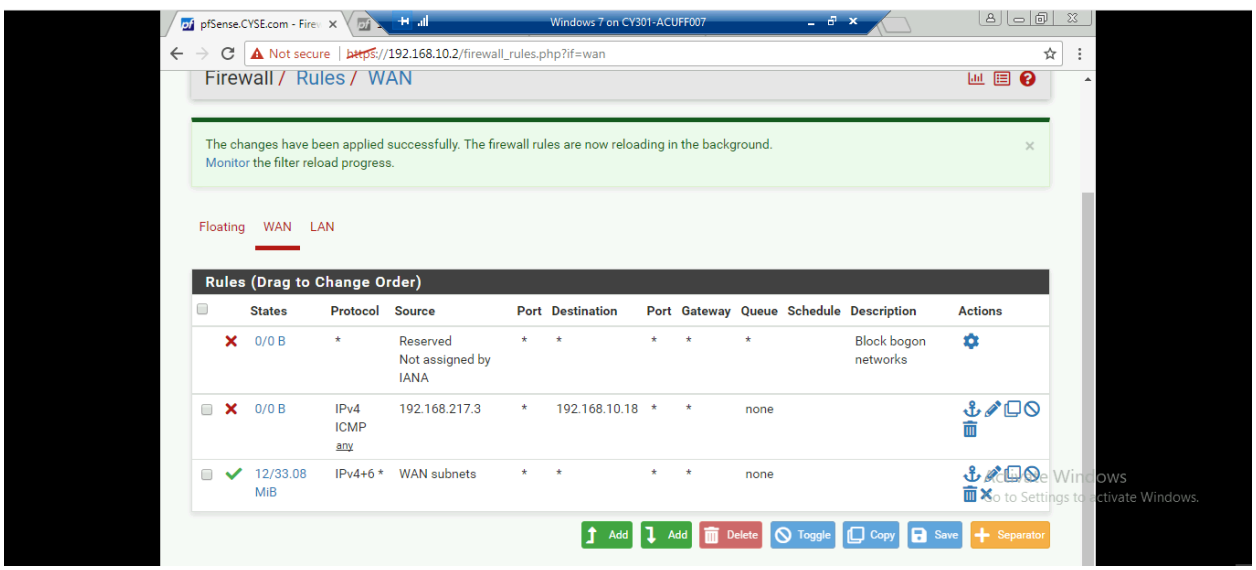
The first thing I examined while running wireshark is that the first 9 captures are ARP requests for 192.168.10.5 - 192.168.10.10. There are more ARP requests for some IP addresses that were not scanned through the External Kali. One thing that I noticed that was very interesting

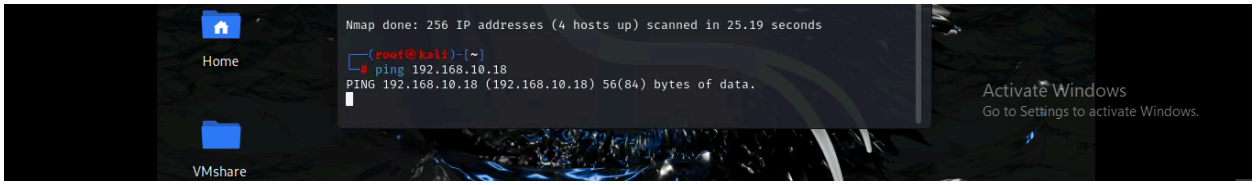
were the TCPs highlighted in red. It happens when the IP address 192.168.10.13 (Internal Kali) communicates with 192.168.217.3 (External Kali). Another observation is that External Kali mostly communicates with Ubnutu throughout the capturing process but never has network communication with Windows Server 2022. It is strange that the Internal Kali never once captured anything that was for the IP address of Windows Server 2022, but managed to capture itself talking with External Kali and Ubnutu. There were some flags captured from TCP which either stated something about ACK and RST or SYN. The ACK means acknowledgement and the RST means reset. As for SYN, that means that the client wants to establish a connection with the server or “synchronize”. One more thing I saw in the wireshark capture is that almost all of the protocols were TCP throughout. Some of the protocols were ARP and a small number of them were ICMP.

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.

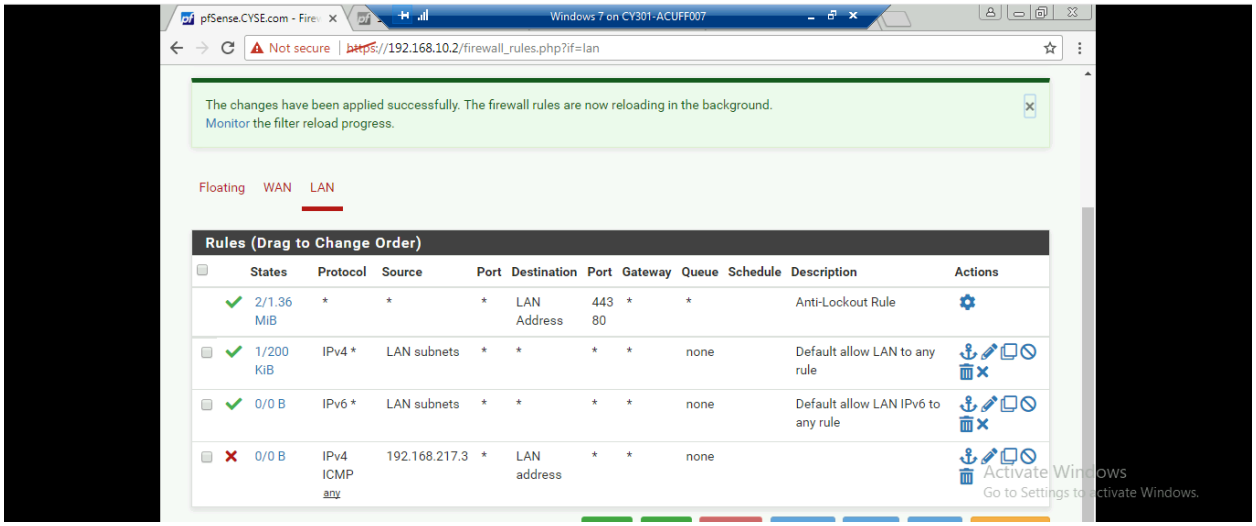
Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if applicable)
1	WAN	Block	192.168.217.3	192.168.10.18	ICMP

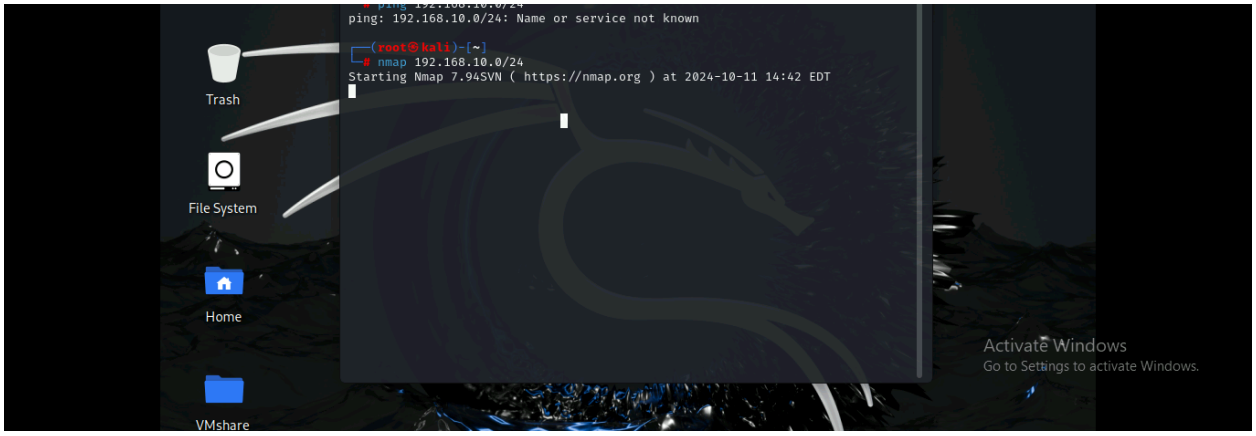




2. Clear the previous firewall policies and configure the pfSense firewall to block all ICMP traffic from External Kali to the LAN side.

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if applicable)
2	LAN	Block	192.168.217.3	LAN address?	ICMP

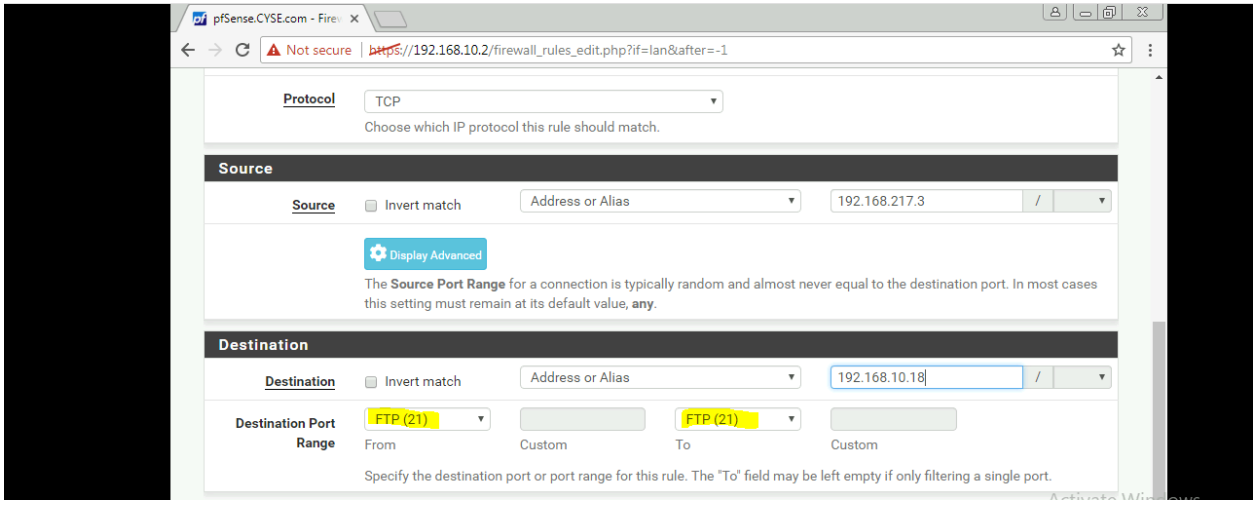


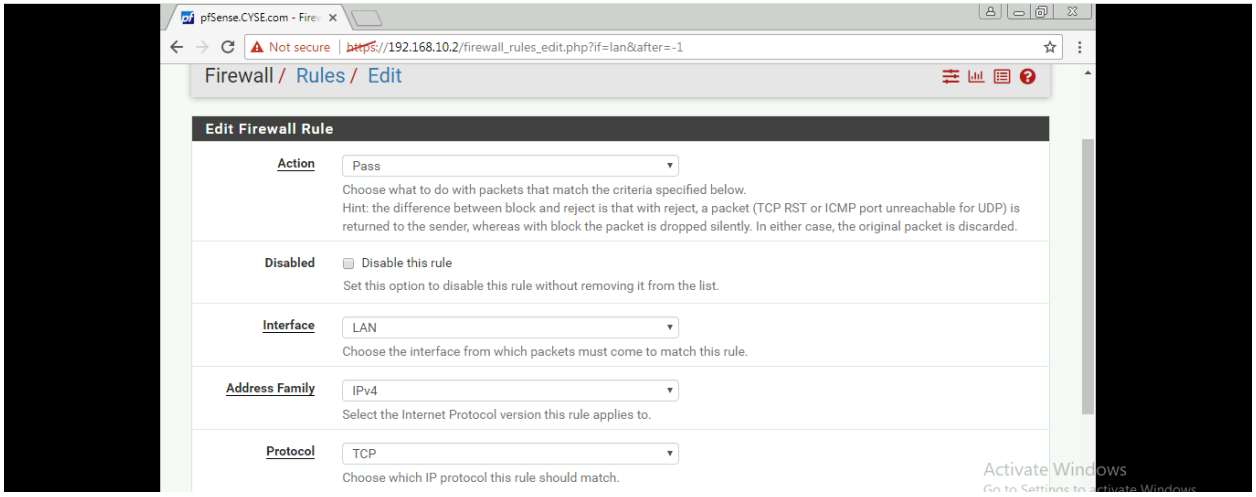


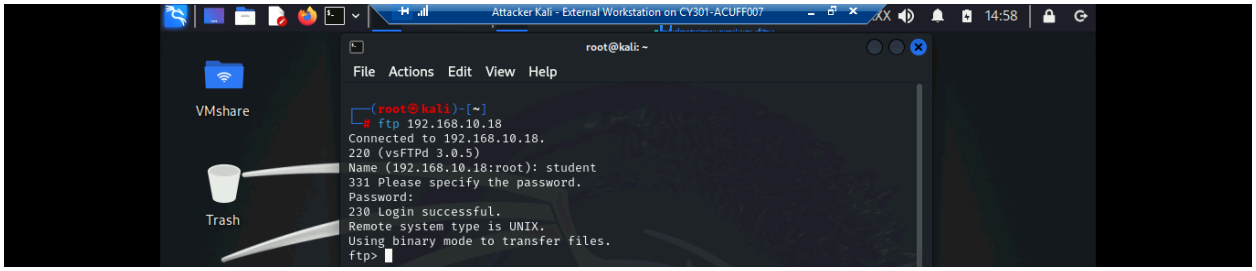
3. Clear the previous firewall policies and configure the pfSense firewall to block ALL traffic from External Kali to the LAN side, except for the FTP protocol towards Windows Server 2022 (actually Ubuntu, not Windows Server 2022).

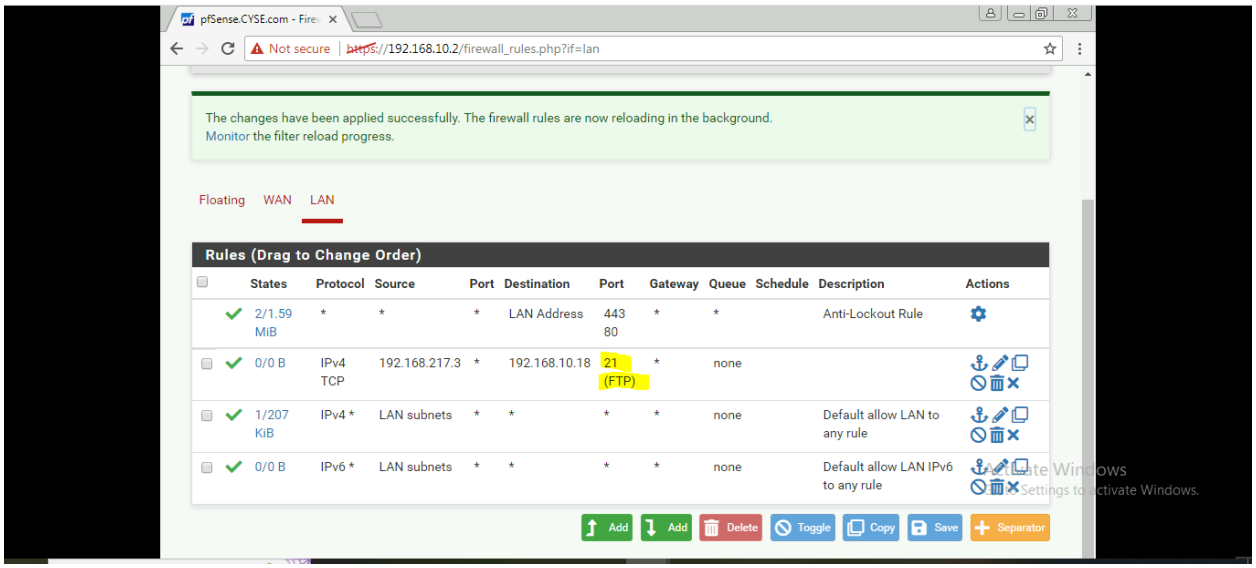
Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if applicable)
3	LAN	Pass	192.168.217.	192.168.10.1	FTP (port 21)

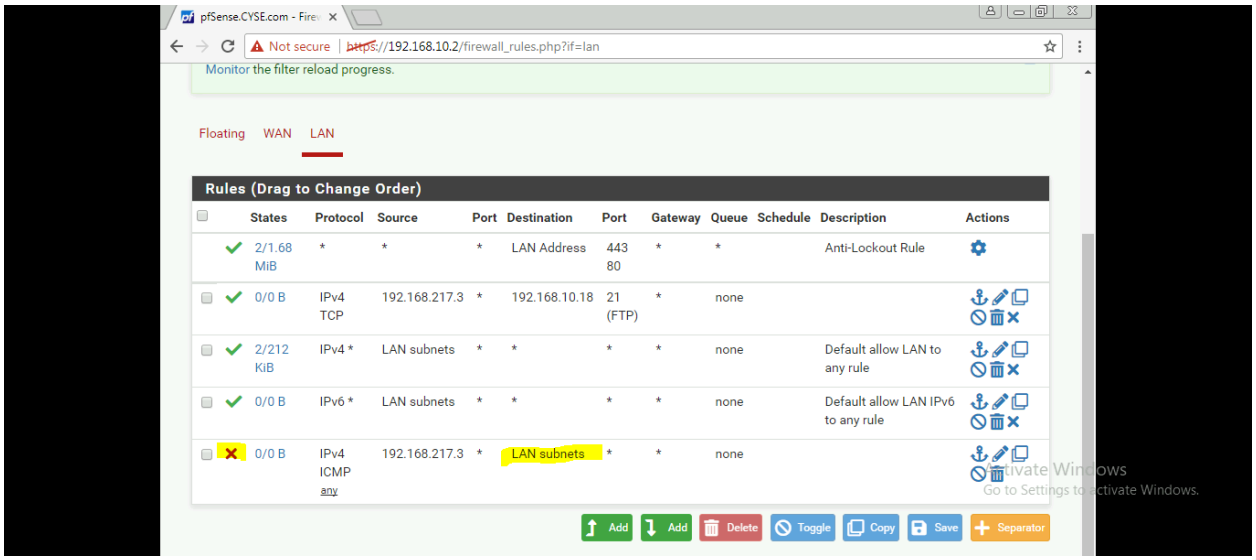
			3	8	
4	LAN	Block	192.168.217.3	LAN subnets	All traffic











4. Keep the firewall policies you created in Task B.3 and repeat Task A.1. What's the difference?
The difference in the results of Task A.1 and the results with the firewall policies is that the nmap command was able to scan through the network of all VMs. However, now the traffic is blocked so External Kali is unable to scan the network of all VMs.

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