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.

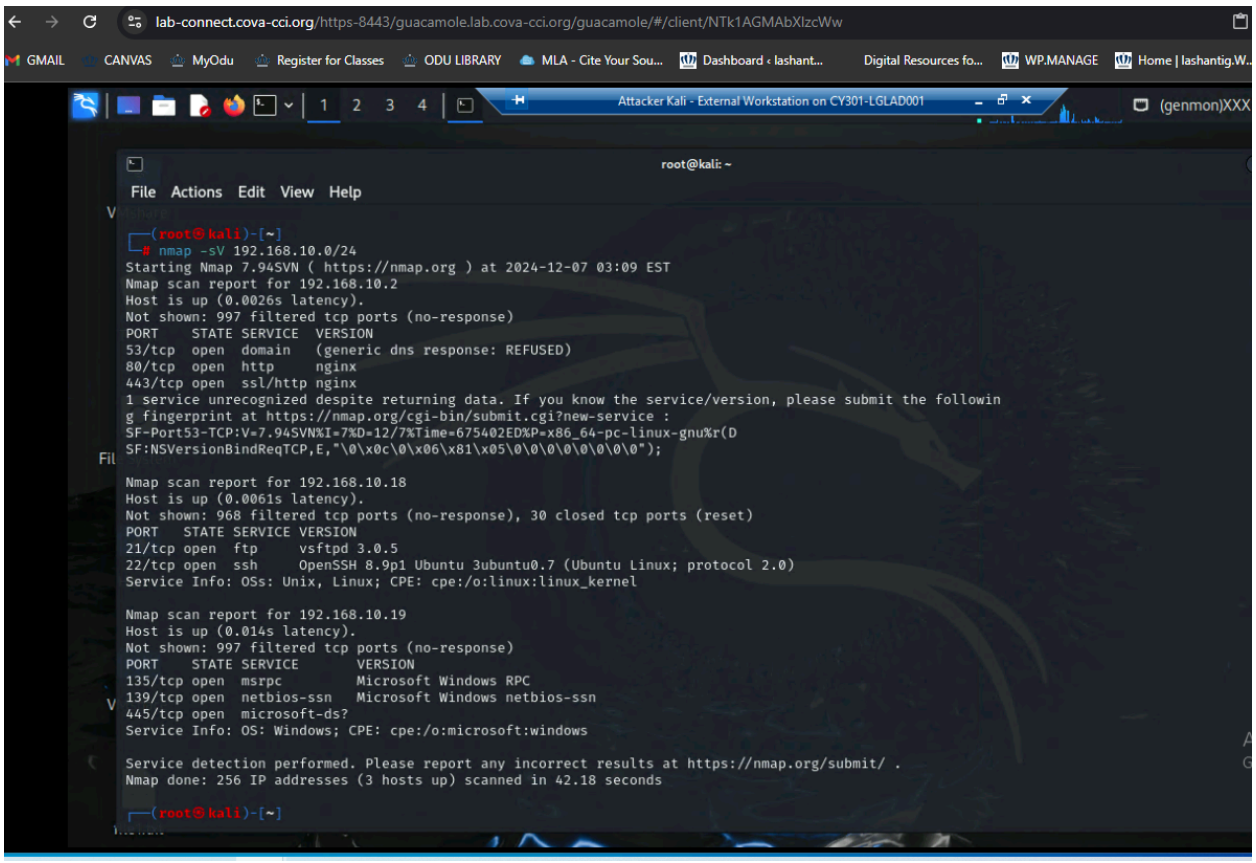
Task A: Sword - Network Scanning (20+ 20 = 40 points)

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)

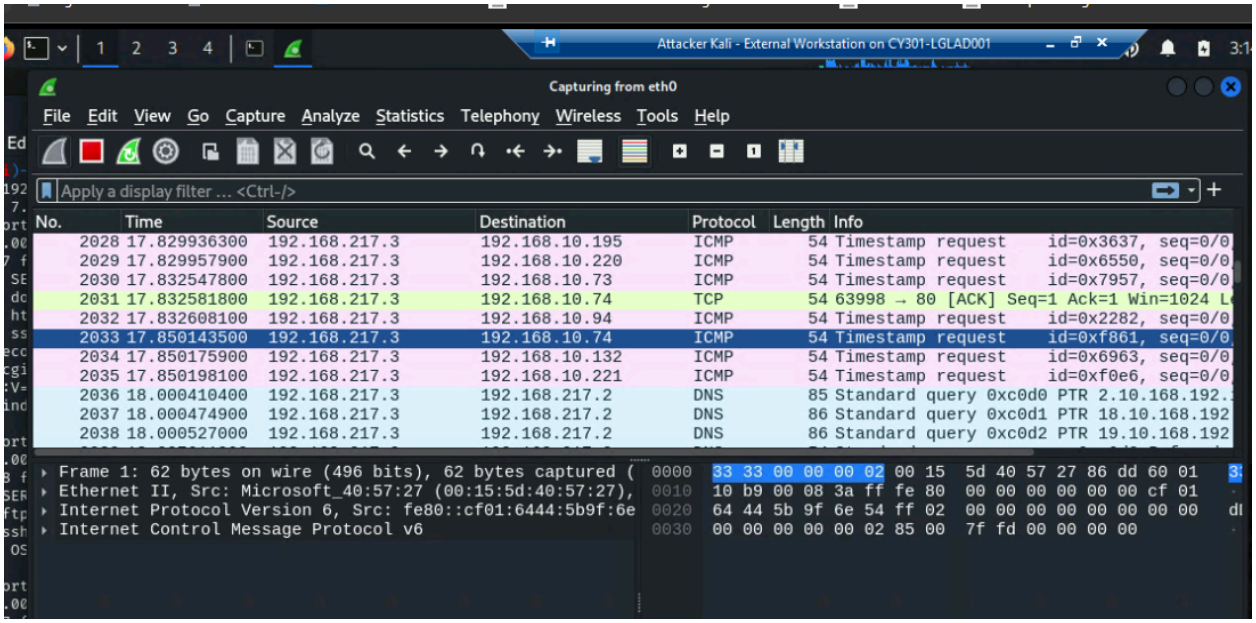
- External Kali
- pfSense
- Ubuntu
- Windows Server 2022

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.



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.

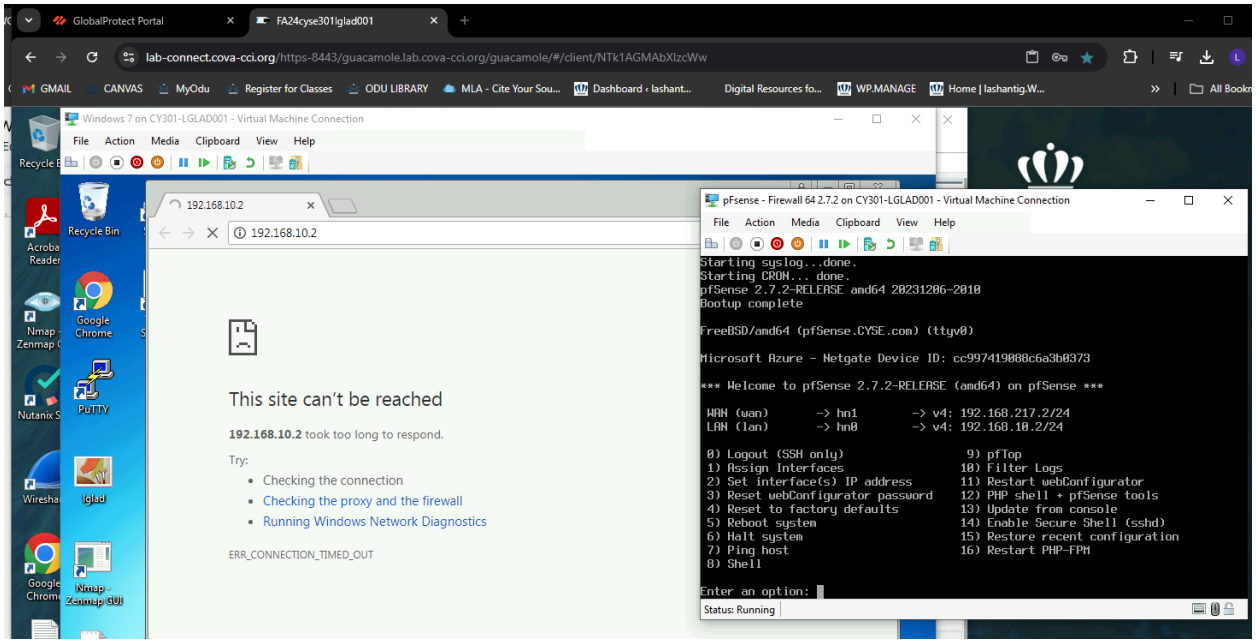


I found quite a bif of different types of information from my wireshark scan. One such thing I found was the destination which was ipv6mcast_02 while my source was microsoft 40:57:27. Overall wireshark captured 8557 packets from the scan all of which were displayed. Of those captured packets 1022 or 11.9% of them were icmp packets. Whereas 87.7% or 7504 packets were tcp packets. The dns packets I captured made up only 0.3% of the total packets with only 28. I also noticed a ICMPv6 protocol categorized as router solicitation.

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 applicable)
[Add the screenshot here]

rule	interface	action	sourceip	desip	protocol
1	wan	block	192.168.217.3	198.168.10.18	icmp

2. Clear the previous firewall policies and configure the pfSense firewall to block all ICMP traffic from
External Kali to the LAN side.
[Add the screenshot here]
Rule # Interface Action Source IP Destination IP Protocol
(port # if applicable)
[Add the screenshot here]



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**.
[Add the screenshot here]

4. Keep the firewall policies you created in Task B.3 and repeat Task A.1. What's the difference?
Extra credit (15 points): Use NESSUS to enumerate the security vulnerabilities of Microsoft Windows

Server 2022 VM in the CCIA network