

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)

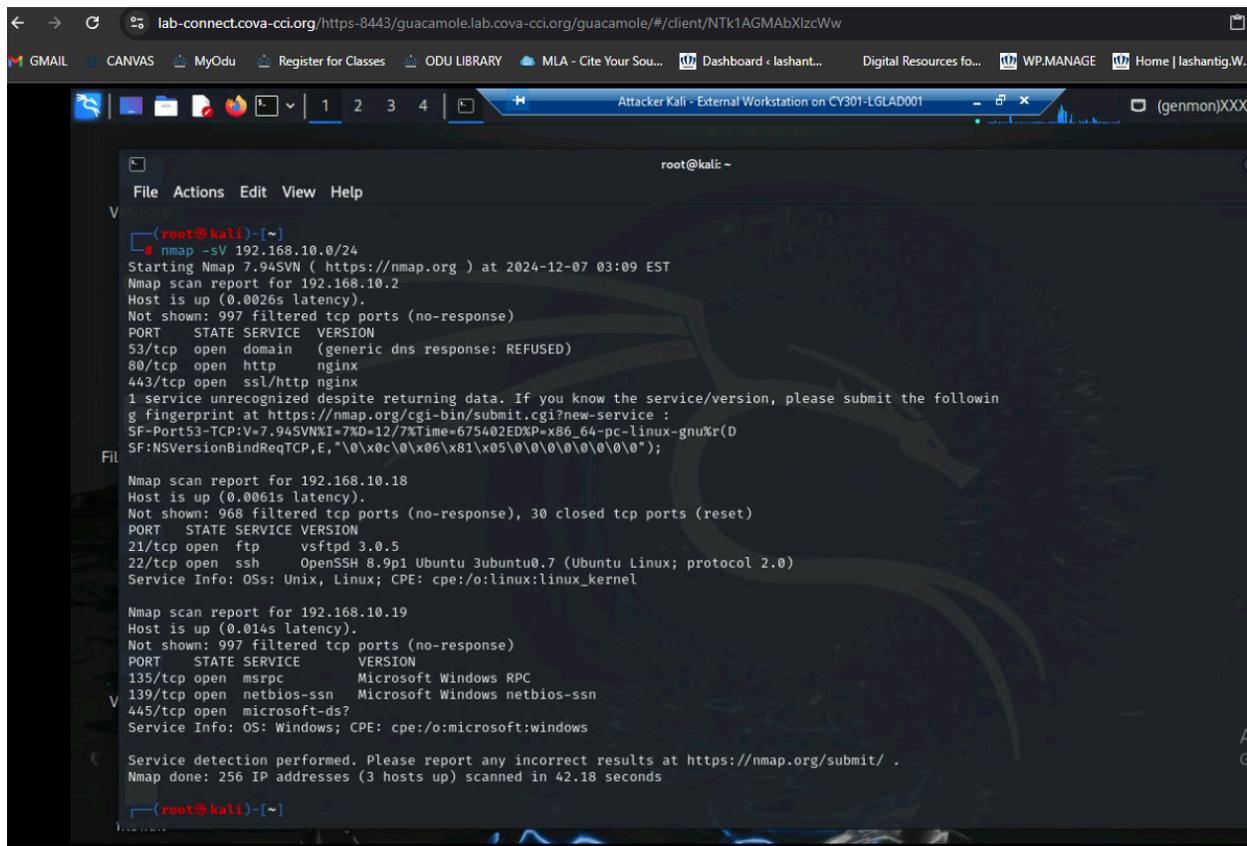
Power on the listed VMs and complete the following steps from the External Kali (you can use either

nmap or zenmap to complete the assignment)

- External Kali
- pfSense
- Ubuntu
- Windows Server 2022

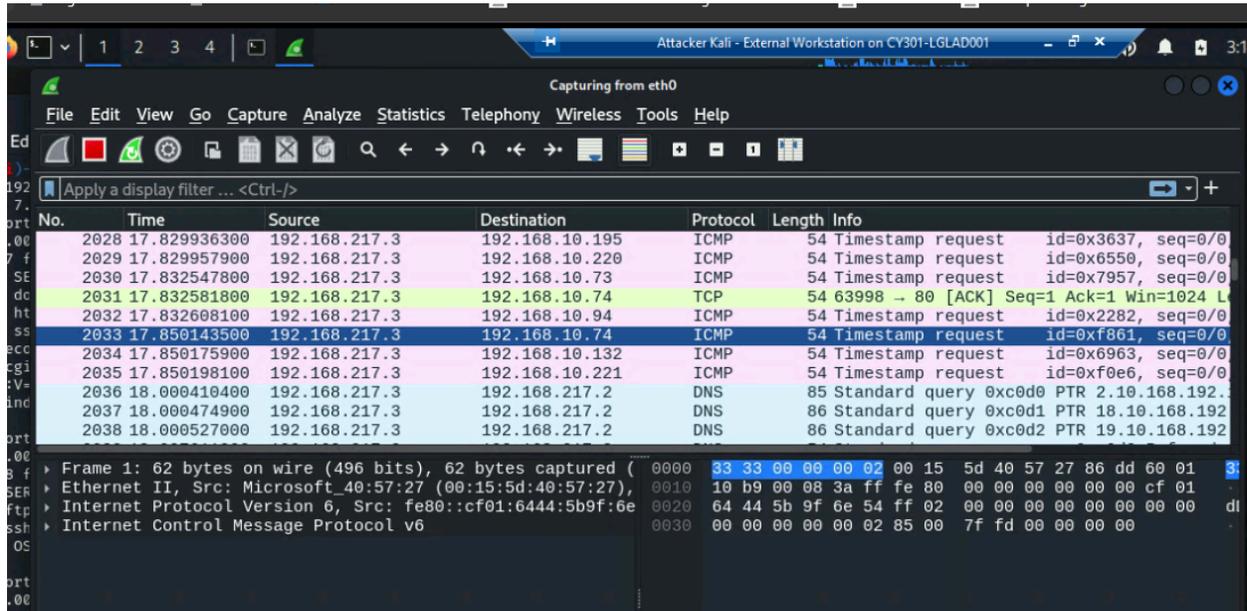
Make sure you didn't add/delete any firewall policy before continuing.

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.



```
root@kali: ~  
File Actions Edit View Help  
V  
root@kali:~# nmap -sV 192.168.10.0/24  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-07 03:09 EST  
Nmap scan report for 192.168.10.2  
Host is up (0.0026s latency).  
Not shown: 997 filtered tcp ports (no-response)  
PORT      STATE SERVICE VERSION  
53/tcp    open  domain (generic dns response: REFUSED)  
80/tcp    open  http  nginx  
443/tcp   open  ssl/http nginx  
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :  
SF-Port53-TCP:V=7.94SVN&I=7&D=12/7&Time=675402ED&P=x86_64-pc-linux-gnu&R(D  
SF:NSVersionBindReqTCP,E,"\\0\\x0c\\0\\x06\\x81\\x05\\0\\0\\0\\0\\0\\0");  
File  
Nmap scan report for 192.168.10.18  
Host is up (0.0061s latency).  
Not shown: 968 filtered tcp ports (no-response), 30 closed tcp ports (reset)  
PORT      STATE SERVICE VERSION  
21/tcp    open  ftp    vsftpd 3.0.5  
22/tcp    open  ssh    OpenSSH 8.9p1 Ubuntu 3ubuntu0.7 (Ubuntu Linux; protocol 2.0)  
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
Nmap scan report for 192.168.10.19  
Host is up (0.014s latency).  
Not shown: 997 filtered tcp ports (no-response)  
PORT      STATE SERVICE VERSION  
135/tcp   open  msrpc  Microsoft Windows RPC  
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn  
445/tcp   open  microsoft-ds?   
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 256 IP addresses (3 hosts up) scanned in 42.18 seconds  
root@kali:~#
```

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 bit 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 an 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	198.168.10.1 8	icmp

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

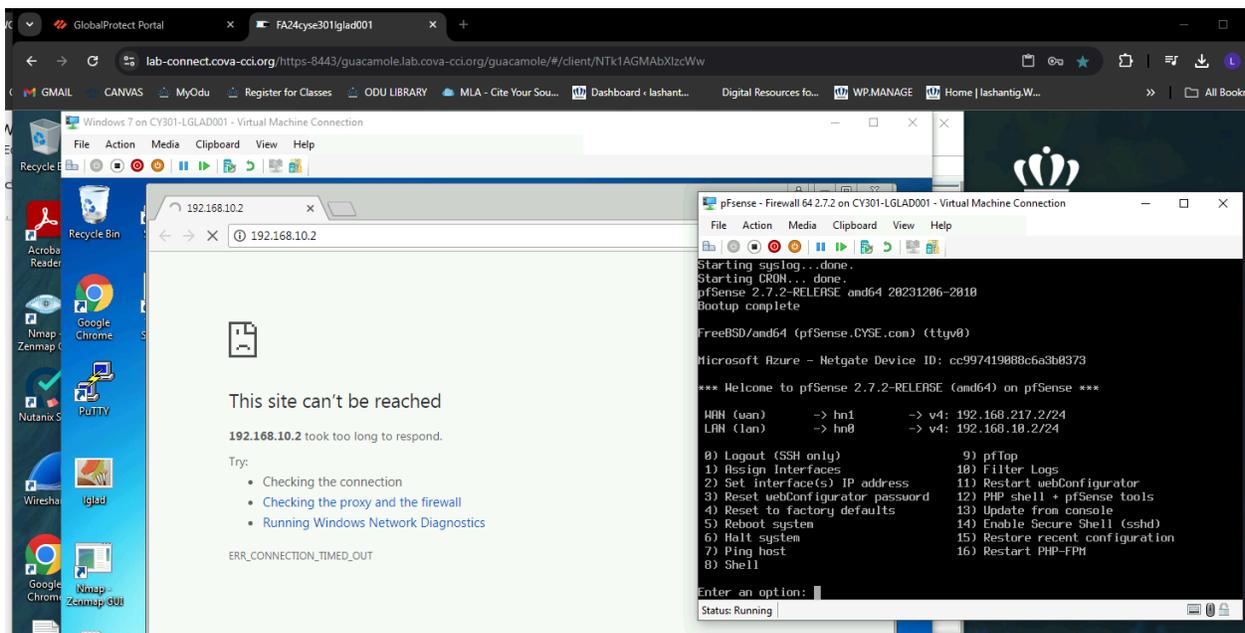
External Kali to the LAN side.

[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