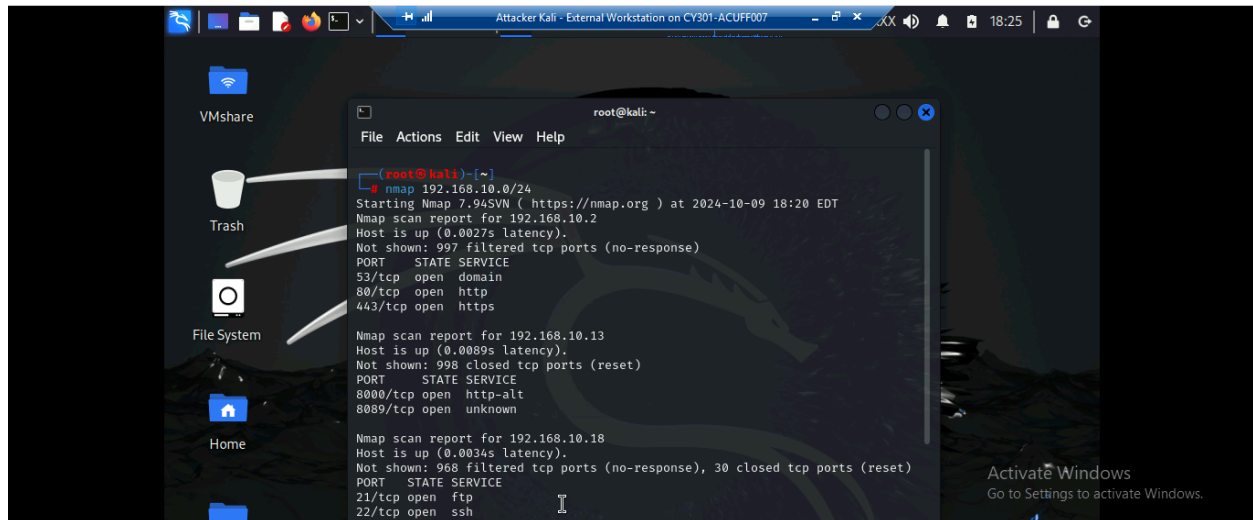
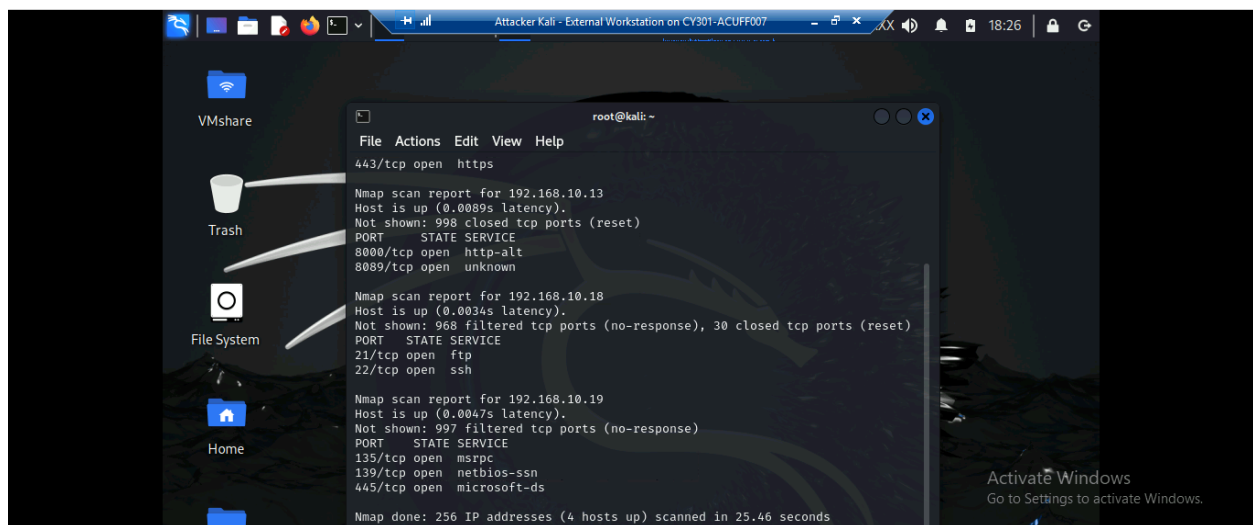


Task A: Sword - Network Scanning (20 + 20 = 40 points) Power on the listed VMs and complete the following steps from the External Kali (you can use either nmap or zenmap to complete the assignment) • External Kali • pfSense • Ubuntu • Windows Server 2022 Make sure you didn't add/delete any firewall policy 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  
root@kali: ~  
# nmap 192.168.10.0/24  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-09 18:20 EDT  
Nmap scan report for 192.168.10.2  
Host is up (0.0027s latency).  
Not shown: 997 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
53/tcp    open  domain  
80/tcp    open  http  
443/tcp   open  https  
  
Nmap scan report for 192.168.10.13  
Host is up (0.0089s latency).  
Not shown: 998 closed tcp ports (reset)  
PORT      STATE SERVICE  
8000/tcp  open  http-alt  
8089/tcp  open  unknown  
  
Nmap scan report for 192.168.10.18  
Host is up (0.0034s latency).  
Not shown: 968 filtered tcp ports (no-response), 30 closed tcp ports (reset)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh
```



```
root@kali: ~  
File Actions Edit View Help  
443/tcp    open  https  
  
Nmap scan report for 192.168.10.13  
Host is up (0.0089s latency).  
Not shown: 998 closed tcp ports (reset)  
PORT      STATE SERVICE  
8000/tcp  open  http-alt  
8089/tcp  open  unknown  
  
Nmap scan report for 192.168.10.18  
Host is up (0.0034s latency).  
Not shown: 968 filtered tcp ports (no-response), 30 closed tcp ports (reset)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
  
Nmap scan report for 192.168.10.19  
Host is up (0.0047s latency).  
Not shown: 997 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
  
Nmap done: 256 IP addresses (4 hosts up) scanned in 25.46 seconds
```

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 Ubuntu 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 Ubuntu. 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

The screenshot displays the pfSense Firewall Rules configuration for the WAN interface. A green notification bar at the top indicates that changes have been applied successfully and the firewall rules are reloading in the background. The 'Rules (Drag to Change Order)' table shows three rules:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*	*	Block bogus networks	Settings
0/0 B	IPv4 ICMP	192.168.217.3	*	192.168.10.18	*	*	none			Block, Log, Toggle, Copy, Save, Separator
12/33.08 MiB	IPv4+6 *	WAN subnets	*	*	*	*	none			Block, Log, Toggle, Copy, Save, Separator

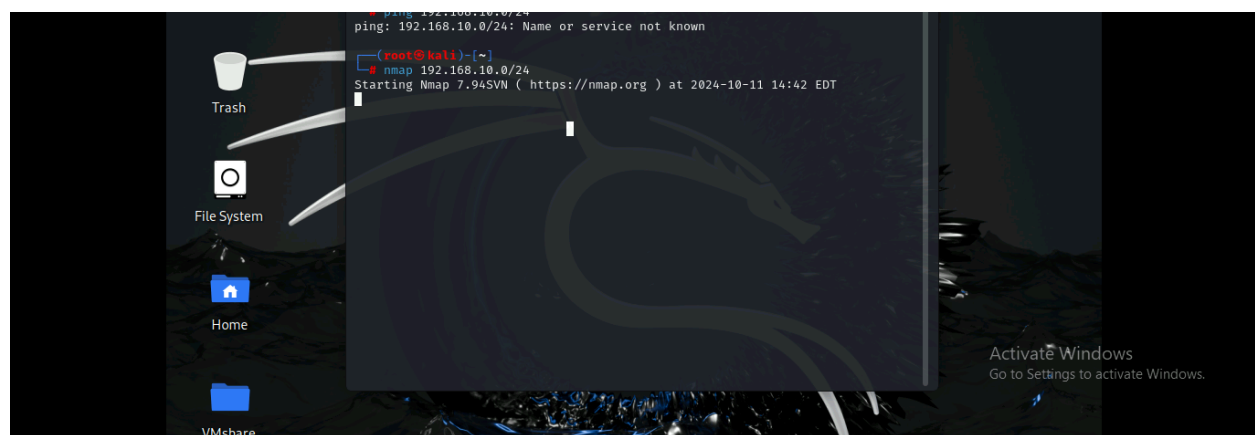
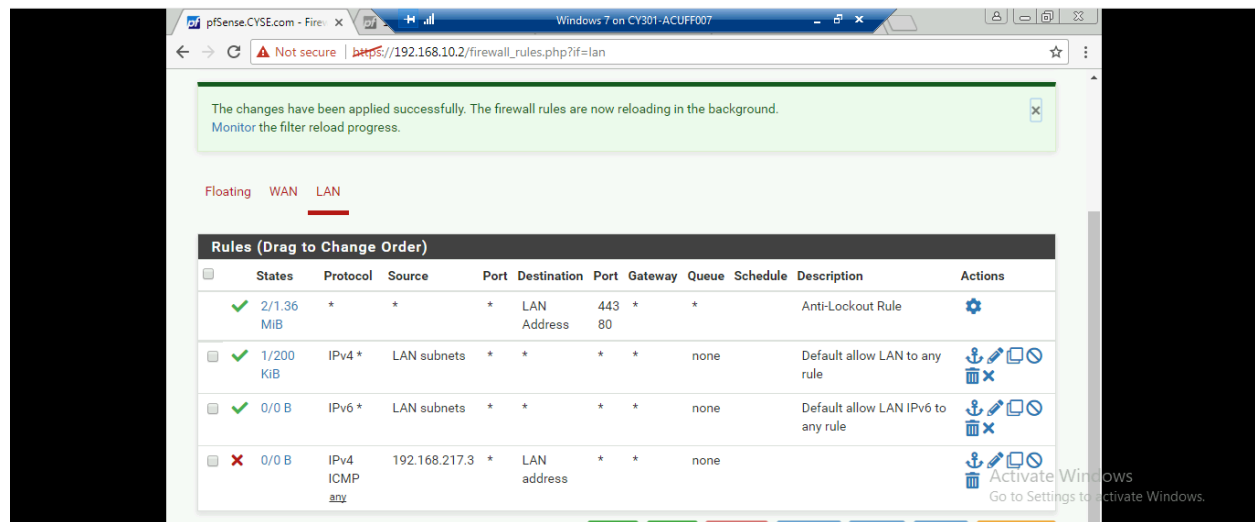
Below the configuration, a terminal window shows the results of a network scan and a ping test:

```

Nmap done: 256 IP addresses (4 hosts up) scanned in 25.19 seconds
root@kali:~# ping 192.168.10.18
PING 192.168.10.18 (192.168.10.18) 56(84) bytes of data:
  
```

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

pfSense.CYSE.com - Fire X

Not secure | https://192.168.10.2/firewall_rules_edit.php?if=lan&after=-1

Protocol TCP
Choose which IP protocol this rule should match.

Source

Source ☐ Invert match Address or Alias 192.168.217.3 /

[Display Advanced](#)

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination ☐ Invert match Address or Alias 192.168.10.18 /

Destination Port Range **FTP (21)** From Custom **FTP (21)** To Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

pfSense.CYSE.com - Fire X

Not secure | https://192.168.10.2/firewall_rules_edit.php?if=lan&after=-1

Firewall / Rules / Edit

Edit Firewall Rule

Action Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface LAN
Choose the interface from which packets must come to match this rule.

Address Family IPv4
Select the Internet Protocol version this rule applies to.

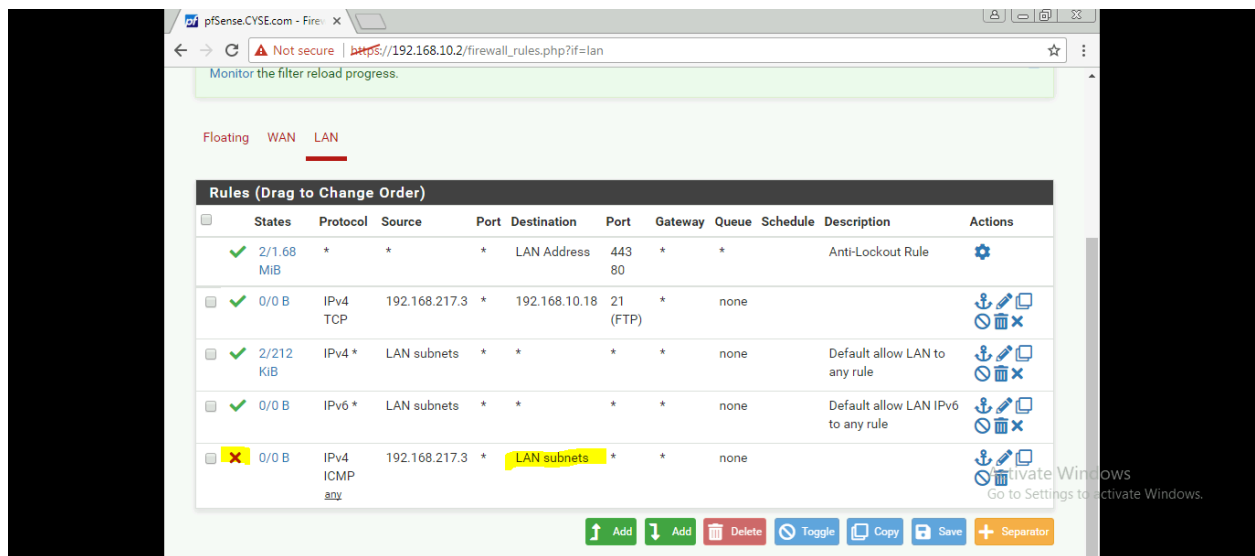
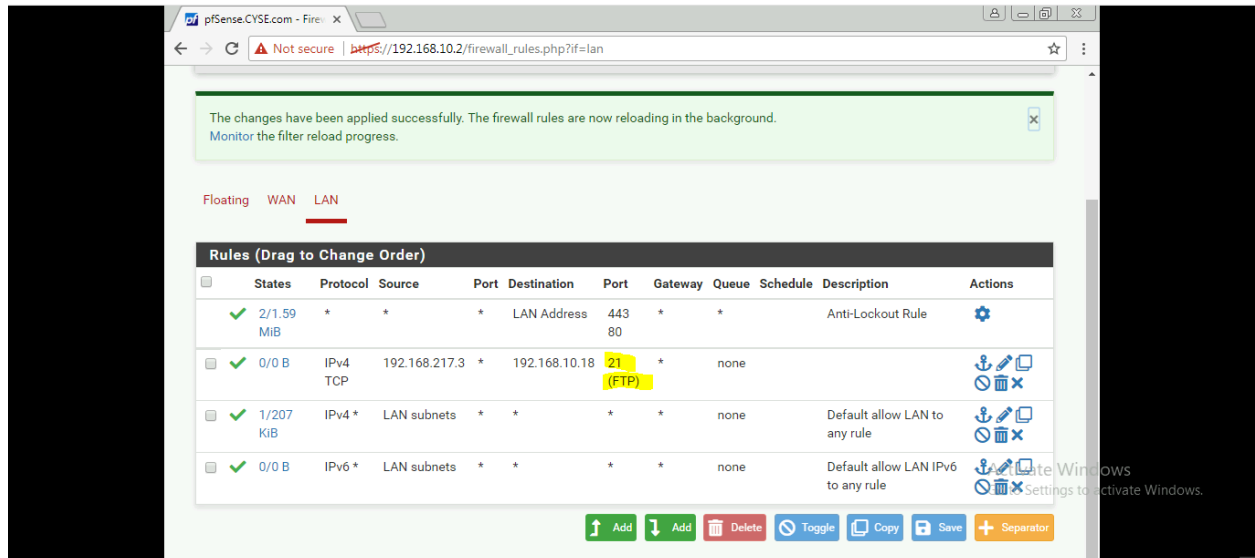
Protocol TCP
Choose which IP protocol this rule should match.

Activate Windows
Go to Settings to activate Windows

Attacker Kali - External Workstation on CY301-ACUFF007

root@kali: ~

```
(root@kali) ~  
# ftp 192.168.10.18  
Connected to 192.168.10.18.  
220 (vsFTPD 3.0.5)  
Name (192.168.10.18:root): student  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp>
```



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.

