CYSE 301: Cybersecurity Technique and Operations

Assignment 3: Sword vs. Shield

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.

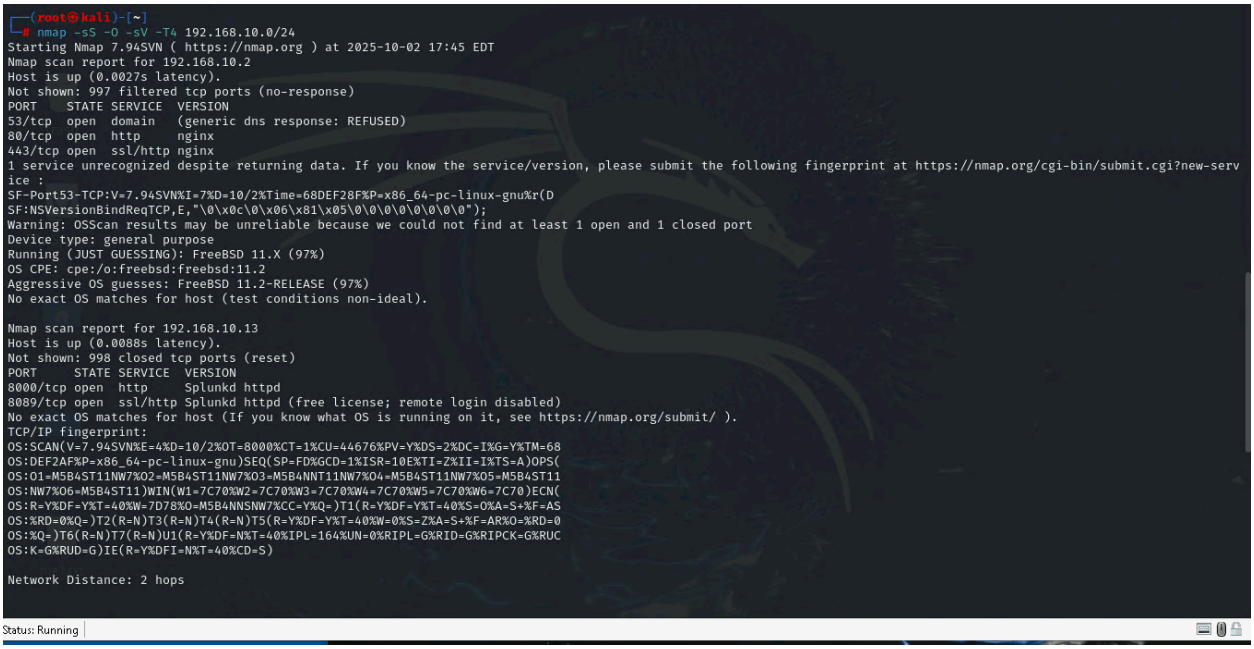
Task A: Sword - Network Scanning (20+ 20 = 40 points)

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

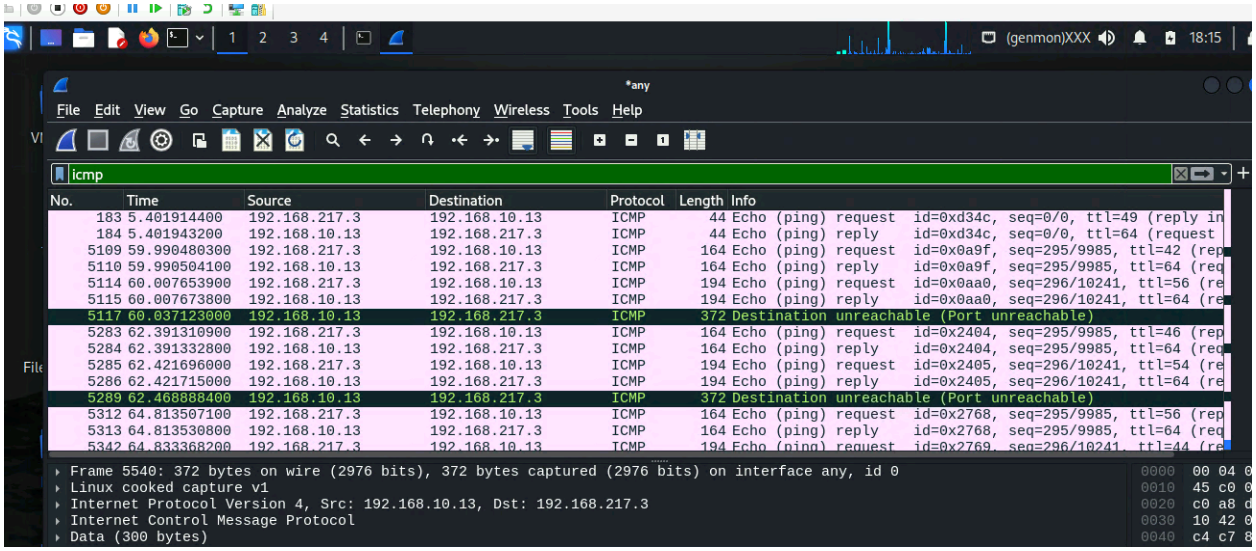
Make sure you didn't add/delete any firewall policy before continuing.

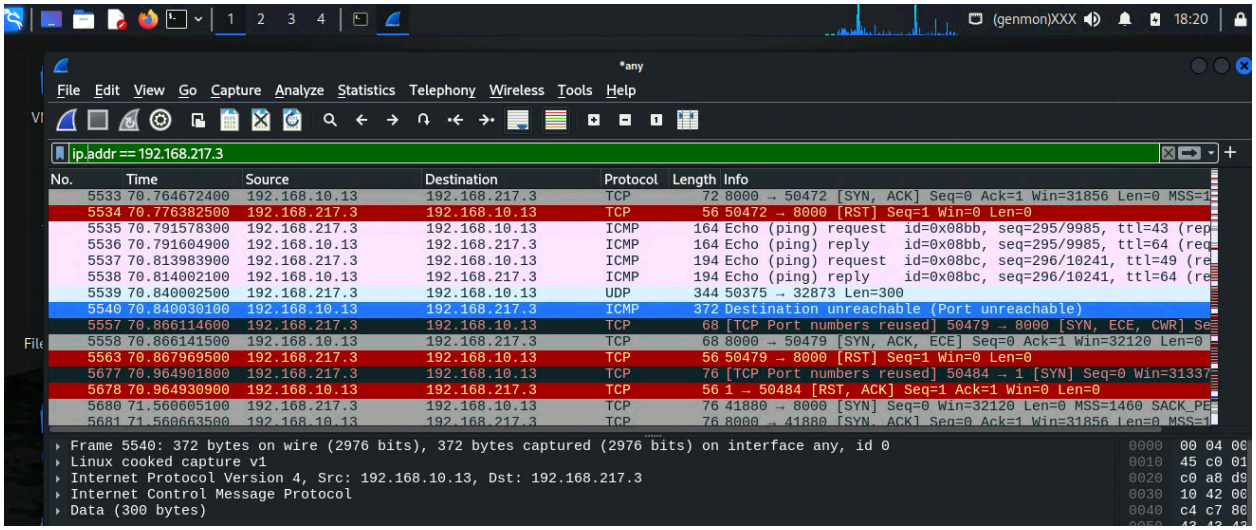
1. Use Nmap to profile the basic information about the **subnet** topology (including open ports information, operation systems, etc.) You need to get the **service** and **backend software** information associated with each opening port in each VM.



```
Network Distance: 2 hops

Nmap scan report for 192.168.10.18
Host is up (0.0039s 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)
Device type: general purpose|storage-misc|firewall
Running (JUST GUESSING): Linux 2.6.X|4.X|3.X|5.X (92%), Synology DiskStation Manager 5.X (86%), WatchGuard Fireware 11.X (85%)
OS CPE: cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:4.4 cpe:/o:linux:linux_kernel:3.10 cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel cpe:/a:sy
logy:diskstation_manager:5.1 cpe:/o:watchguard:fireware:11.8
Aggressive OS guesses: Linux 2.6.32 (92%), Linux 4.4 (92%), Linux 2.6.32 or 3.10 (91%), Linux 2.6.32 - 2.6.35 (90%), Linux 2.6.32 - 2.6.39 (90%), Linux 4.0 (89%), Li
x 5.0 - 5.4 (88%), Linux 3.11 - 4.1 (88%), Linux 3.2 - 3.8 (88%), Linux 2.6.18 (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.10.19
Host is up (0.0042s 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?
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2022|11|2016|10|2012 (94%)
OS CPE: cpe:/o:microsoft:windows_server_2016 cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_server_2012:r2
Aggressive OS guesses: Microsoft Windows Server 2022 (94%), Microsoft Windows 11 21H2 (90%), Microsoft Windows Server 2016 (89%), Microsoft Windows 10 (85%), Microso
 Windows Server 2012 or Windows Server 2012 R2 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 68.00 seconds
```

2. Run Wireshark in 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 started my examination by viewing the ICP packets. ICMP is the protocol used in the ping command, often used by attackers during the reconnaissance and enumeration phases of a cyber attack. After this, I filtered Wireshark for the External Kali's IP address and viewed a flood of TCP packets. I noticed that about half of these TCP packets were red, which means there was a critical error in the transmission, usually due to a packet malformation or a TCP retransmission. This makes sense because, to my knowledge, an nmap scan essentially sends a ton of packets to each port to see if it gets a response. It makes sense that it doesn't stop at one. Another thing that is important to note is that all of the red packets in Wireshark appear to actually be the responses of the tested ports that were closed. Another thing that I noticed was that all of the packets sent by external Kali were 60 bits long, while the responses by the closed ports were 56 bits. This makes me wonder if an Nmap scan could be configured to force longer replies from the ports to create a sort of DoS attack. I also found a yellow button on the corner that highlights where the issue in transmission occurred.

Task B: Shield – Protect your network with a firewall (10 + 10+ 20 + 20 = 60 points)

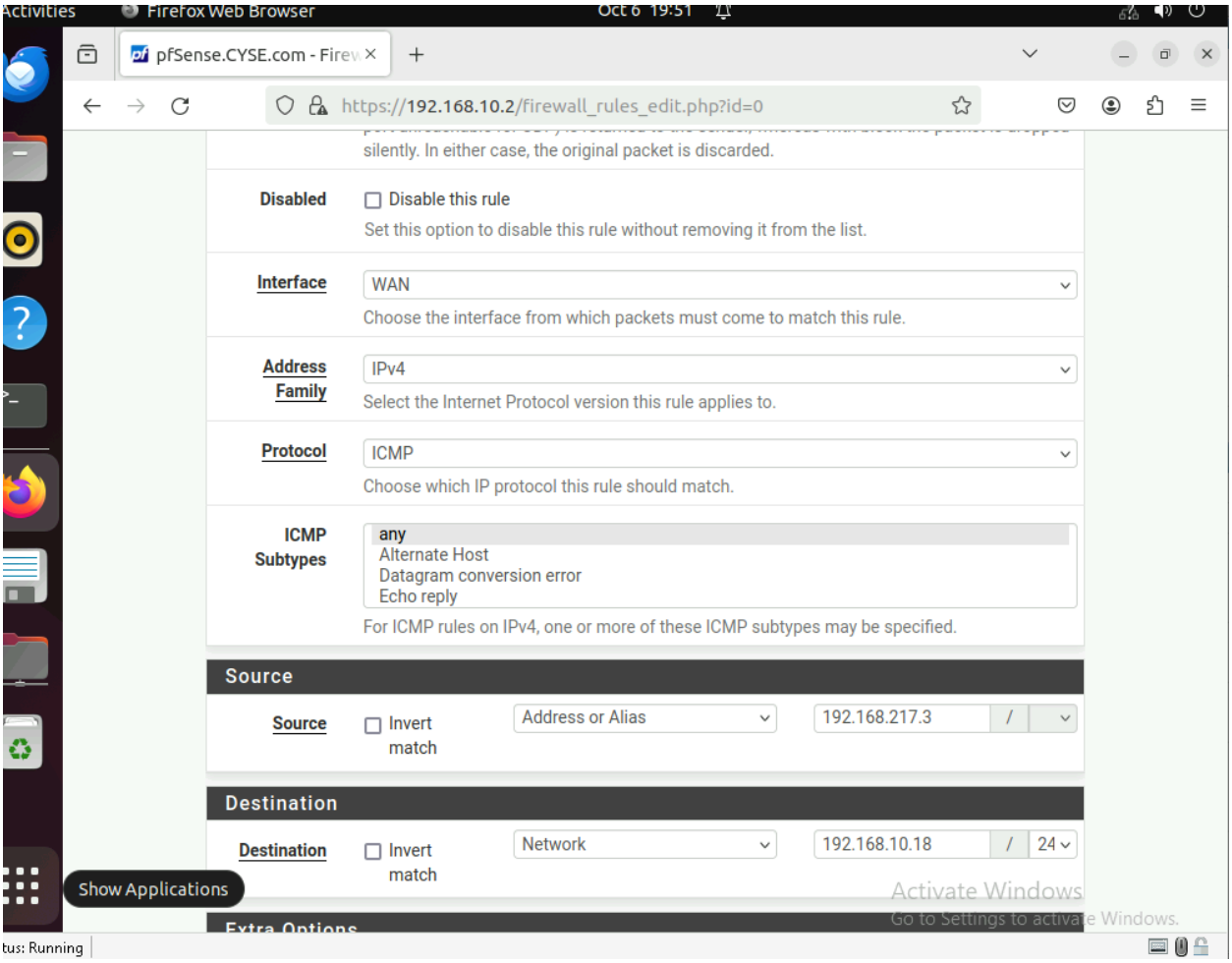
In order to receive full credits, you need to fill the table (add more rows if needed), implement the firewall rule(s), show me the screenshot of your firewall table, and verify the results.

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)
	Wan	block	192.168.217.3	192.168.10.18	ICMP

[Add the screenshot here]

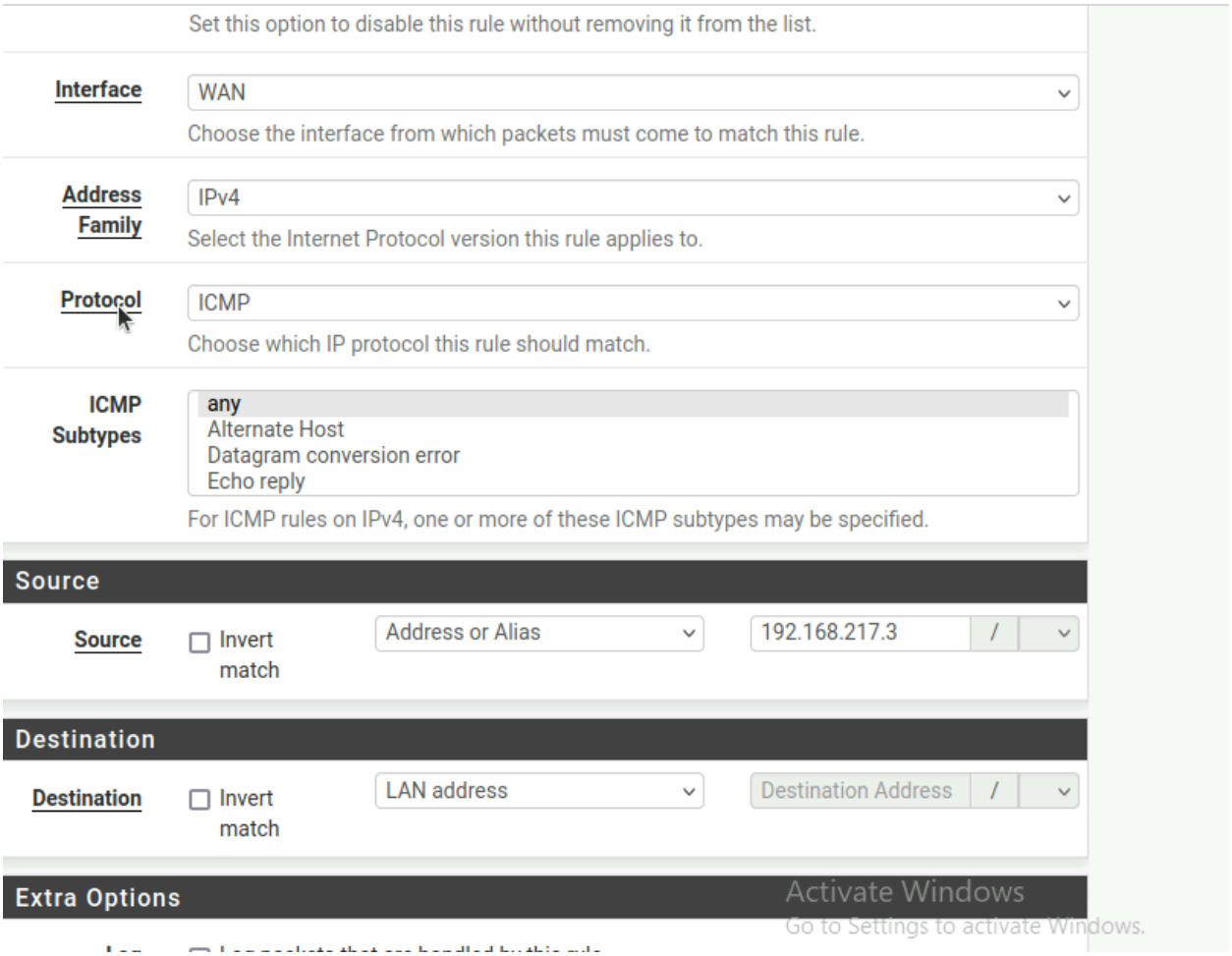
```
┌──(root㉿kali)-[~]
└─# ping 182.168.10.18
PING 182.168.10.18 (182.168.10.18) 56(84) bytes of data.
From 192.168.217.2 icmp_seq=1 Time to live exceeded
From 192.168.217.2 icmp_seq=2 Time to live exceeded
From 192.168.217.2 icmp_seq=3 Time to live exceeded
From 192.168.217.2 icmp_seq=4 Time to live exceeded
From 192.168.217.2 icmp_seq=5 Time to live exceeded
From 192.168.217.2 icmp_seq=6 Time to live exceeded
From 192.168.217.2 icmp_seq=7 Time to live exceeded
From 192.168.217.2 icmp_seq=8 Time to live exceeded
From 192.168.217.2 icmp_seq=9 Time to live exceeded
From 192.168.217.2 icmp_seq=10 Time to live exceeded
From 192.168.217.2 icmp_seq=11 Time to live exceeded
From 192.168.217.2 icmp_seq=12 Time to live exceeded
From 192.168.217.2 icmp_seq=13 Time to live exceeded
From 192.168.217.2 icmp_seq=14 Time to live exceeded
From 192.168.217.2 icmp_seq=15 Time to live exceeded
From 192.168.217.2 icmp_seq=16 Time to live exceeded
From 192.168.217.2 icmp_seq=17 Time to live exceeded
From 192.168.217.2 icmp_seq=18 Time to live exceeded
From 192.168.217.2 icmp_seq=19 Time to live exceeded
From 192.168.217.2 icmp_seq=20 Time to live exceeded
^CFrom 192.168.217.2 icmp_seq=21 Time to live exceeded
From 192.168.217.2 icmp_seq=22 Time to live exceeded
^C
── 182.168.10.18 ping statistics ──
22 packets transmitted, 0 received, +22 errors, 100% packet loss, time 21033ms
```

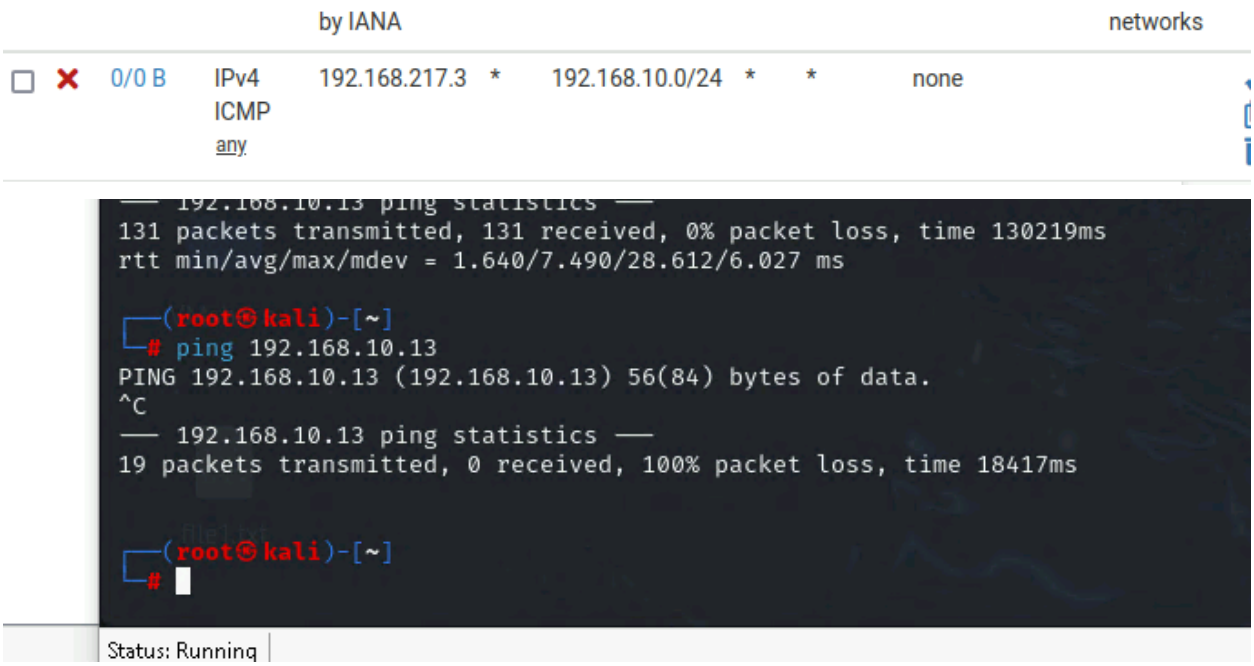


2. Clear the previous firewall policies and configure the pfSense firewall to block all ICMP traffic from External Kali to the LAN side.

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
	WAN	Block	192.168.217.3	192.168.10.0/24	ICMP

[Add the screenshot here]

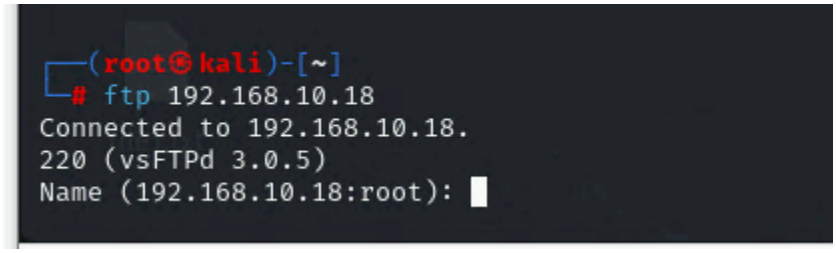




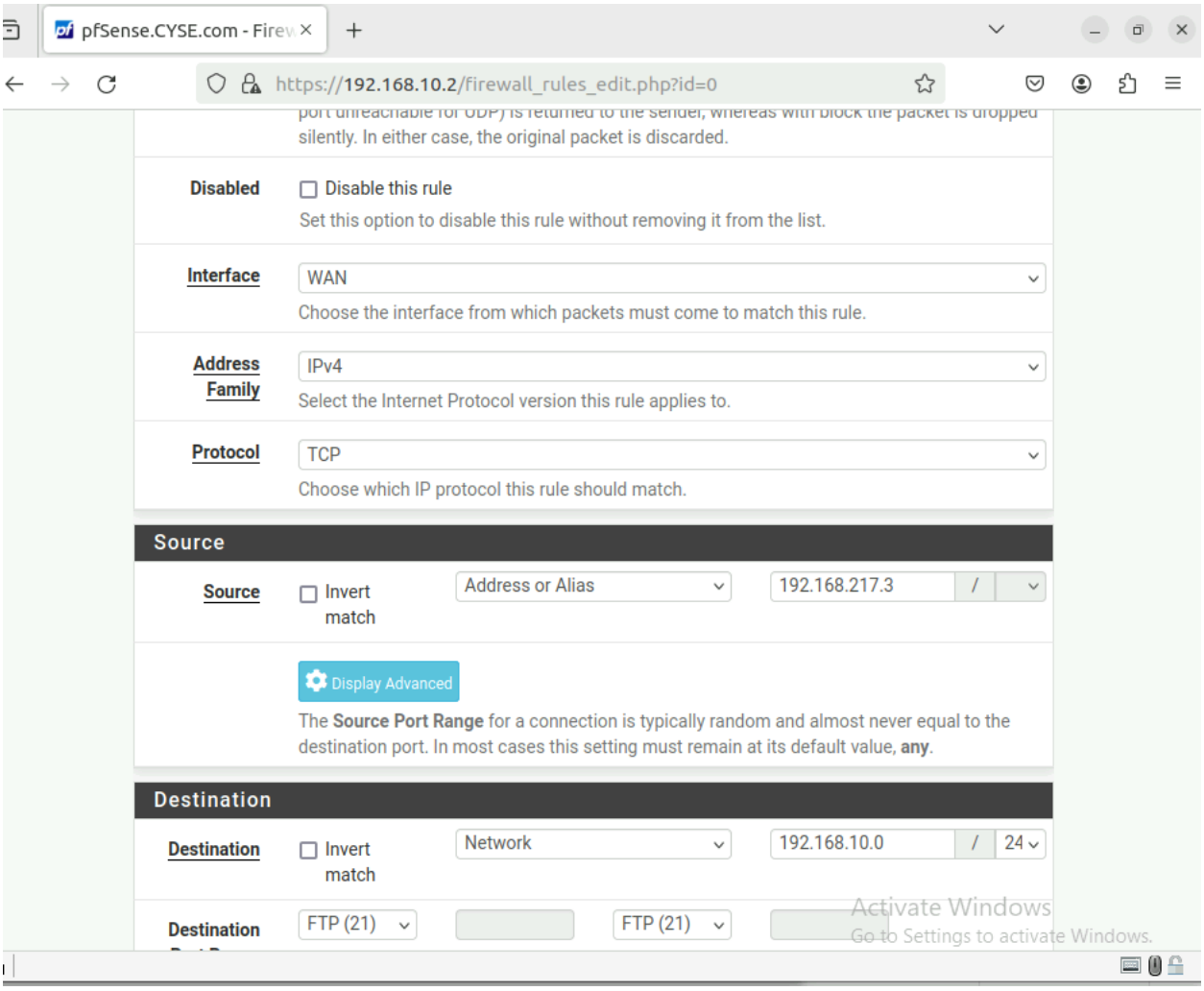
3. Clear the previous firewall policies and configure the pfSense firewall to block ALL traffic from External Kali to the LAN side, except for the FTP protocol towards Ubuntu.

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
1	WAN	Pass	192.168.217.3	192.168.10.18	TCP/21

[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.