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)

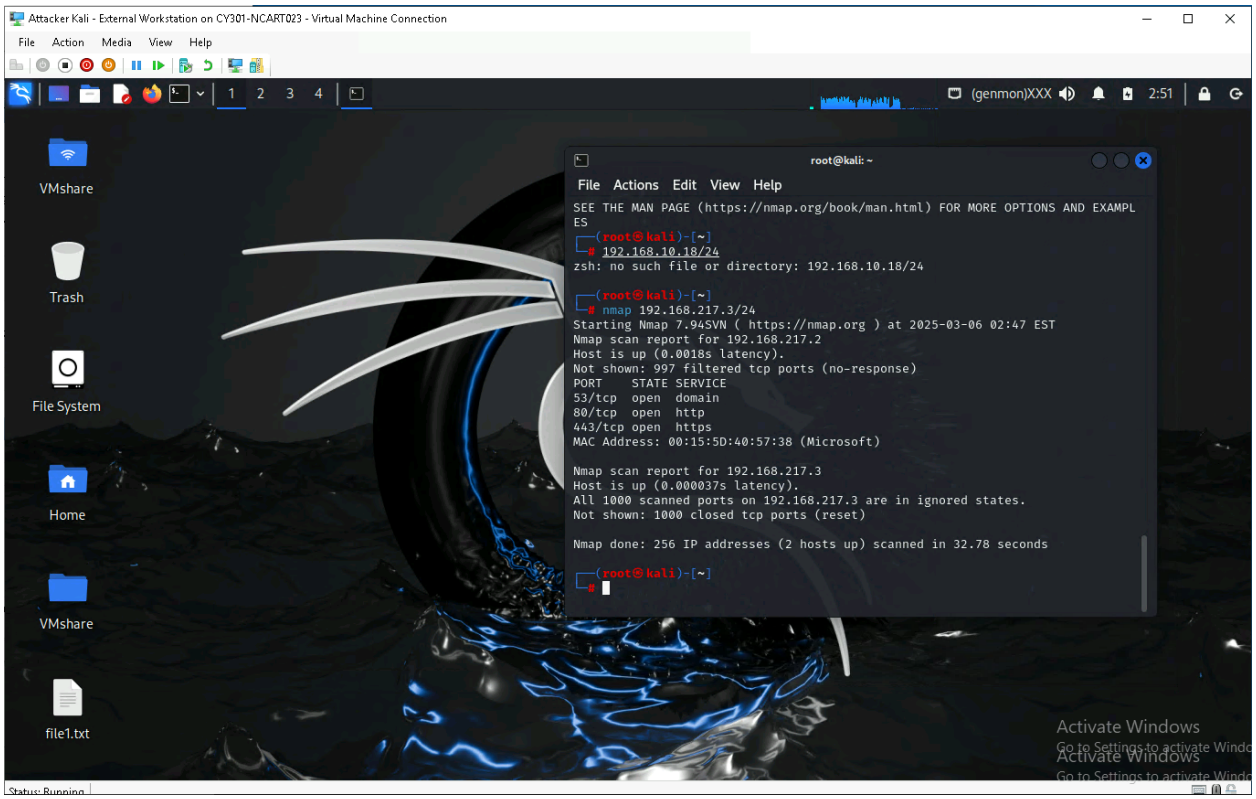
Power on the listed VMs and complete the following steps from the **External Kali** (you can use either nmap or zenmap to complete the assignment)

- External Kali
- pfSense
- Ubuntu
- Windows Server 2022

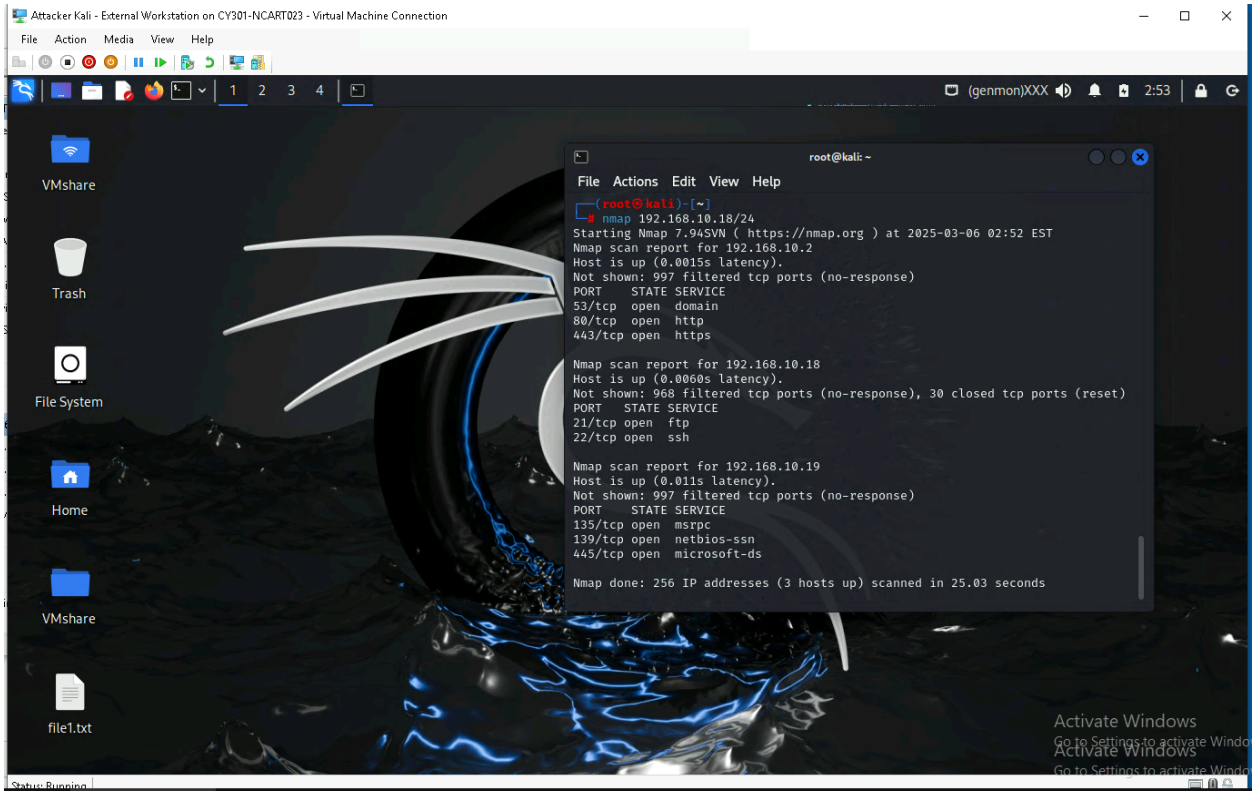
Make sure you didn't add/delete any firewall policy before continuing.

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.

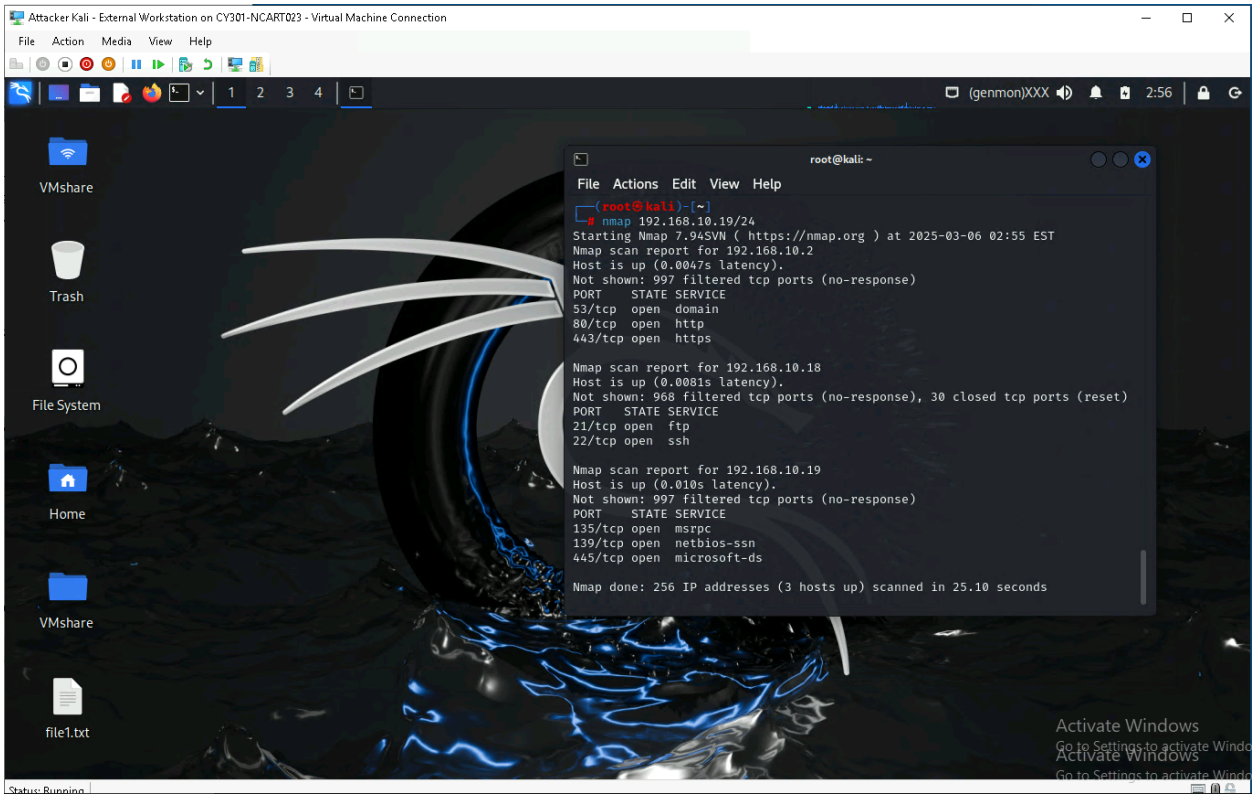
External Kali:



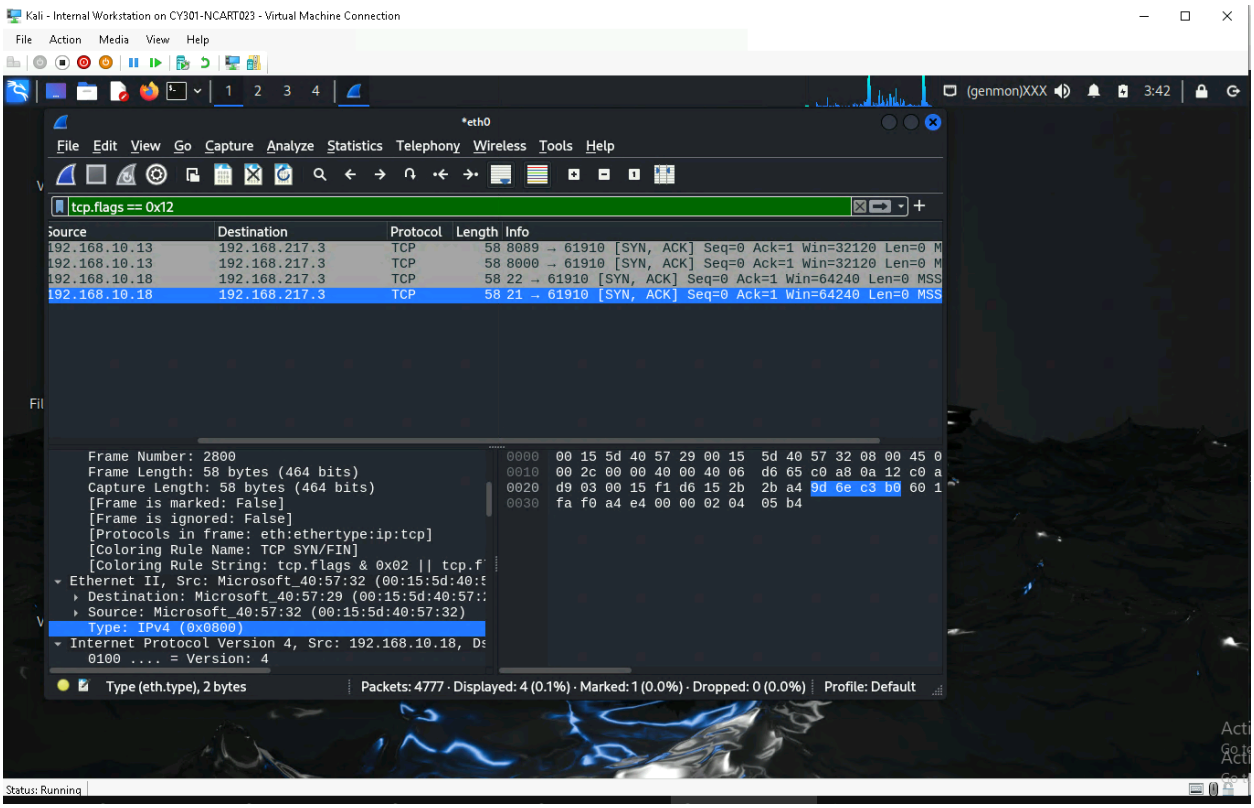
Ubuntu:


Attacker Kali - External Workstation on CY301-NCART023 - Virtual Machine Connection
File Action Media View Help
(genmon)XXX 2:53
VMshare
Trash
File System
Home
VMshare
file1.txt
root@kali: ~
File Actions Edit View Help
(root@kali)-[~]
nmap 192.168.10.18/24
Starting Nmap 7.94SVN (https://nmap.org) at 2025-03-06 02:52 EST
Nmap scan report for 192.168.10.2
Host is up (0.0015s 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 192.168.10.18
Host is up (0.0060s 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 (0.011s 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 (3 hosts up) scanned in 25.03 seconds
Activate Windows
Go to Settings to activate Windows.

Windows:


Attacker Kali - External Workstation on CY301-NCART023 - Virtual Machine Connection
File Action Media View Help
(genmon)XXX 2:56
VMshare
Trash
File System
Home
VMshare
file1.txt
root@kali: ~
File Actions Edit View Help
(root@kali)-[~]
nmap 192.168.10.19/24
Starting Nmap 7.94SVN (https://nmap.org) at 2025-03-06 02:55 EST
Nmap scan report for 192.168.10.2
Host is up (0.0047s 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 192.168.10.18
Host is up (0.0081s 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 (0.010s 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 (3 hosts up) scanned in 25.10 seconds
Activate Windows
Go to Settings to activate Windows.

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.**



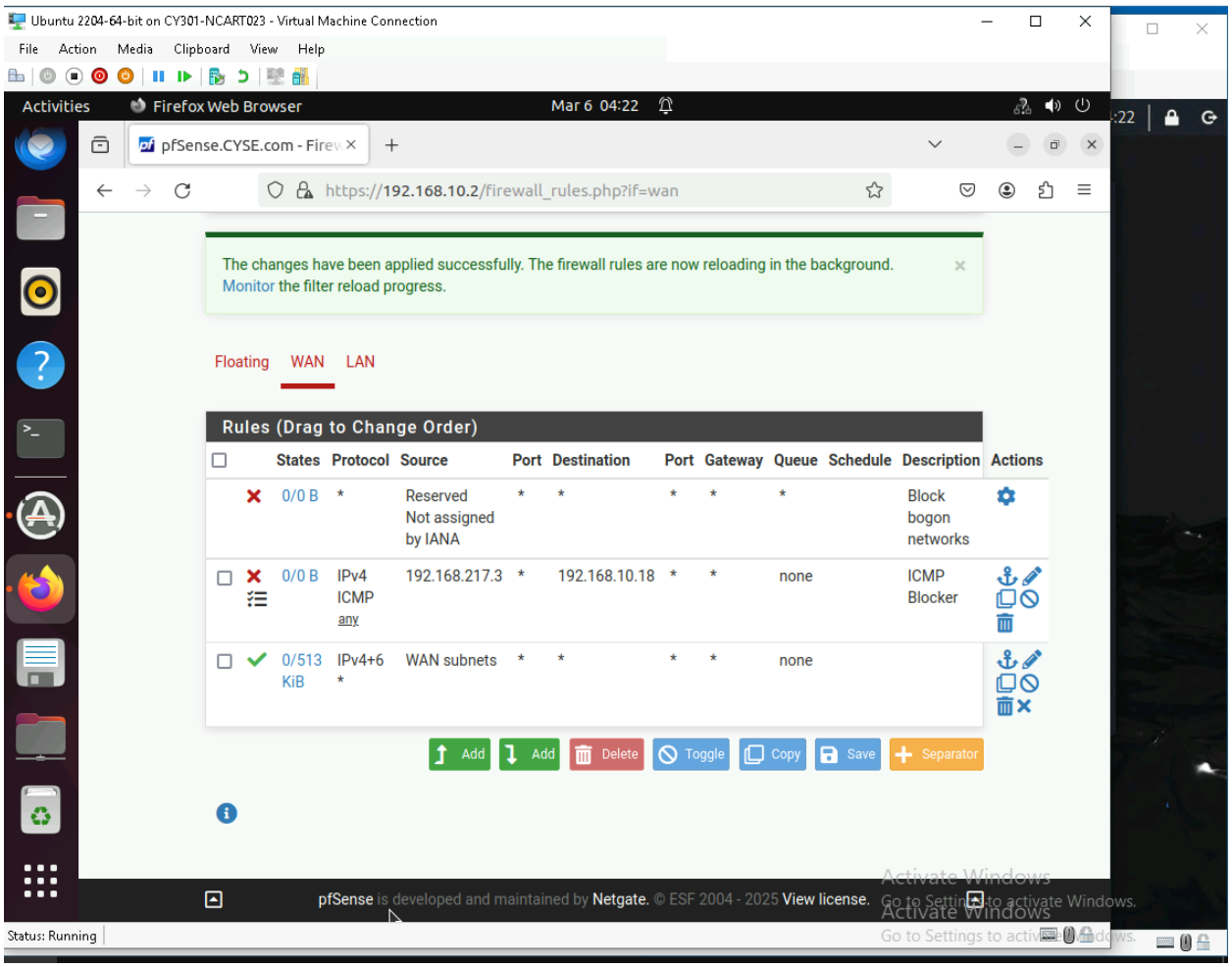
The pattern started out with a bunch of broadcast ARP requesting what different devices have the requested IP. Then a few ICMP echo request/reply packets are sent to measure the respone time from External Kali to subnetworks. Then you eventually see the TCP 3 way handshake start to develop. With the source port 61910 sending packets to a bunch of other ports at the SYN step to verify whether or not the ports are open. Then the ports start to send their response back with the majority sending [RST, ACK] which means the port is closed. With a few ports responding with [SYN,ACK] verifying that the port is open. Then when I go back and analyze the report I see the ones that responded with [SYN,ACK] are listed as open in the nmap report.

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.

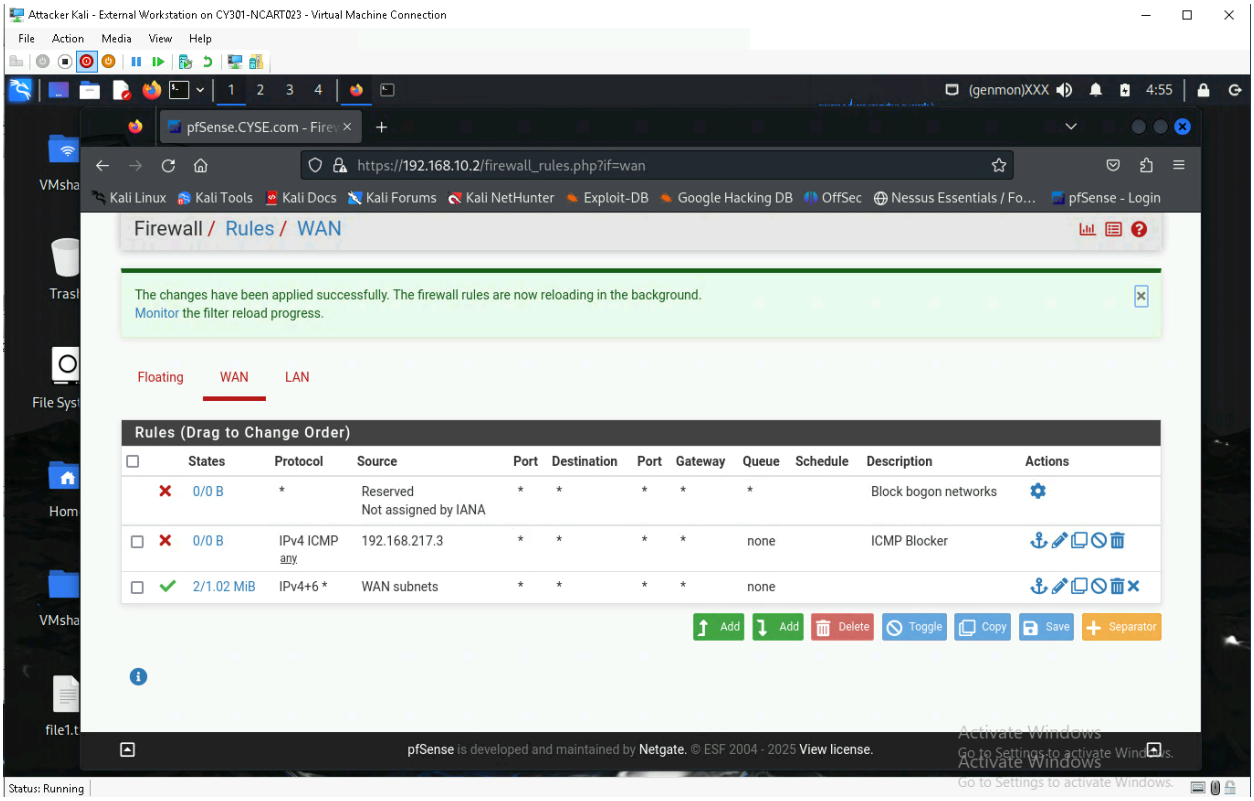
1. Configure the pfSense firewall rule to block the ICMP traffic from External Kali to Ubuntu VM.

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
2	WAN	Block	192.168.217.3	192.168.10.18	TCMP



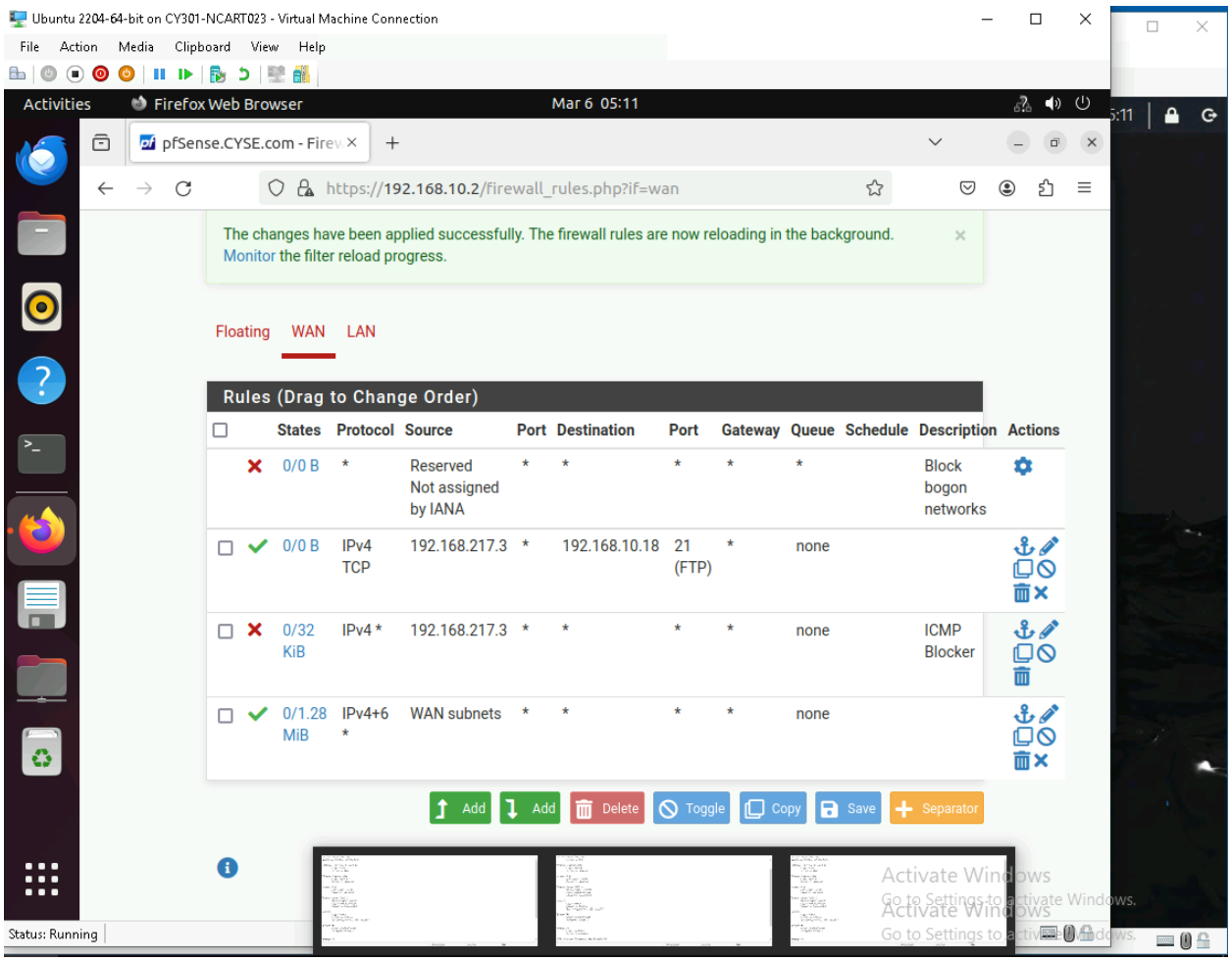
2. Clear the previous firewall policies and configure the pfSense firewall to block all ICMP traffic from External Kali to the LAN side.

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
2	WAN	Block	192.168.217.3	Any	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 Ubuntu.

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
2	WAN	Pass	192.168.10.18	192.168.10.18	TCP (21 FTP)
3	WAN	Block	192.168.10.18	Any	Any



4. Keep the firewall policies you created in Task B.3 and repeat Task A.1. What's the difference?

The only port that was shown as open was port 21, before the extra rules added to the firewall there were multiple other ports that were open.

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