CYSE 301: Cybersecurity Technique and Operations

Assignment 3: Sword vs. Shield

Jason Rivers

01236524

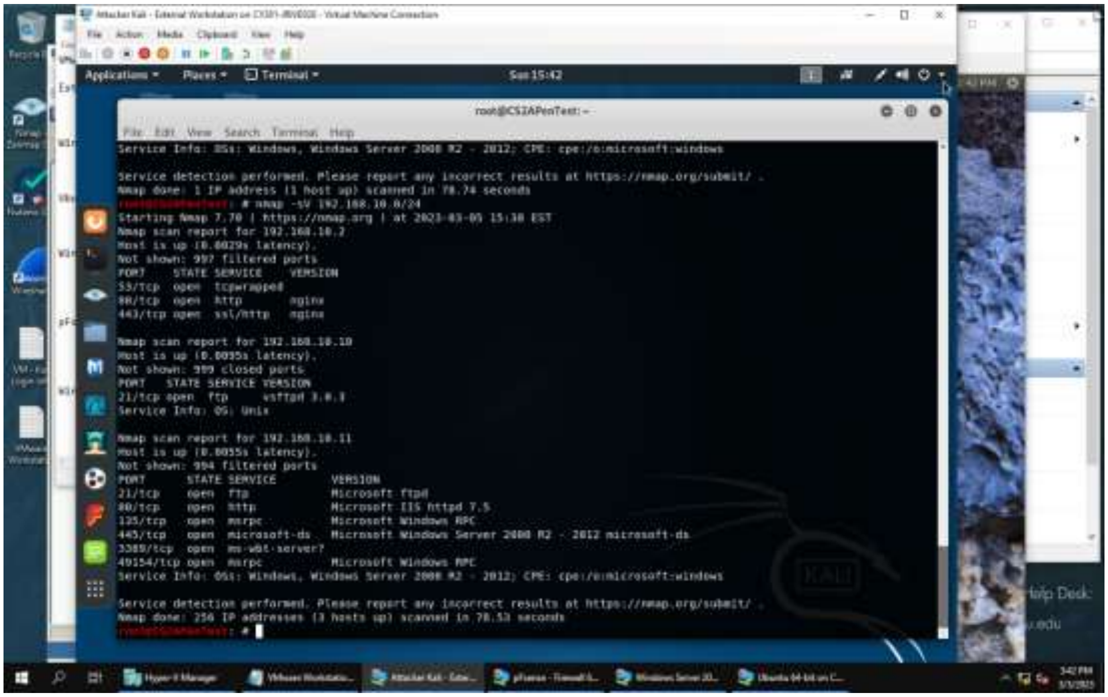
In this assignment, you will act as an attacker to identify the vulnerabilities in the LAN network and a defender to apply proper countermeasures. You need to provide a screenshot for each task below.

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 2008

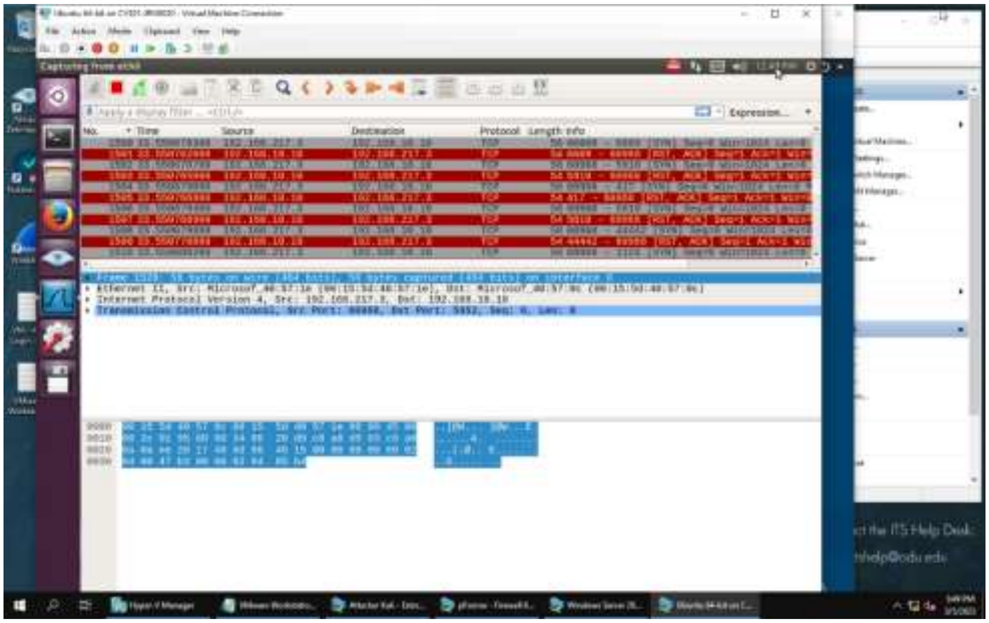
Make sure you didn't add/delete any firewall policy before continuing.

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.



```
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 78.74 seconds
root@CS2APenTest:~# nmap -sV 192.168.10.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2023-03-05 15:38 EST
Nmap scan report for 192.168.10.2
Host is up (0.0029s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE    VERSION
53/tcp  open  tcpwrapped
80/tcp  open  http       nginx
443/tcp open  ssl/http   nginx

Nmap scan report for 192.168.10.10
Host is up (0.0035s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
Service Info: OS: Unix

Nmap scan report for 192.168.10.11
Host is up (0.0055s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE       VERSION
21/tcp    open  ftp           Microsoft ftpd
80/tcp    open  http          Microsoft IIS httpd 7.5
135/tcp   open  msrpc         Microsoft Windows RPC
445/tcp   open  microsoft-ds  Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp  open  ms-wbt-server?
49154/tcp open  msrpc         Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; 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 78.53 seconds
root@CS2APenTest:~#
```

2. Run Wireshark in Ubuntu 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.**



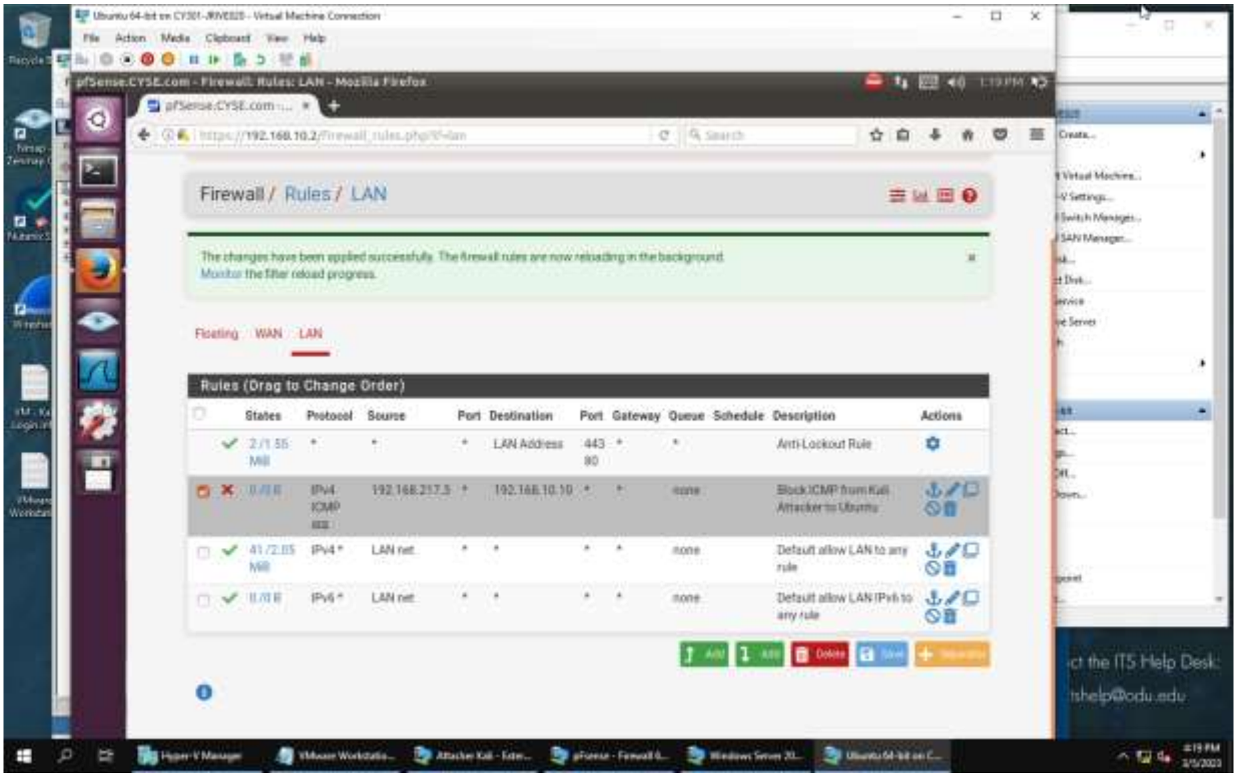
I attached a screenshot to help show what happened. When Nmap was commanded to scan the 192.168.10.0/24 subnet, it flooded the subnet with TCP traffic to see which ports would send an ACK response, and therefore show which were open and vulnerable. NMAP would send a TCP message to every port number it possibly could, and see if it got an ACK message back. If it didn't, it meant that either the port would not take the TCP message, or was secured against possible NMAP intrusion probing, or the firewall was stopping the traffic. If it did get an ACK message back, it meant that it could, in theory, be possible to access that port to gain access to a system, or a network if security measures weren't taken to prevent the open port's usage. From watching the traffic go by, it seems to work its way up from the smaller number ports to the larger number ports on a subnet's lift of devices. Another interesting thing I found was that the messages were color coded as well. I scanned twice, and the first time, red and grey seemed to be the most prominent number, but the second time I did, it was sort of lavender color. This might be a security feature to highlight possible suspicious activity in a network's traffic so cybersecurity engineers working within the network can filter through traffic more easily.

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 appliable)
2	**WAN**	**Block**	**192.168.217.3**	**192.168.10.10**	**IPv4 | ICMP:any**



pfSense.CYSE.com - Firewall: Rules: LAN - Mozilla Firefox

https://192.168.10.2/firewall_rules.php?if=lan

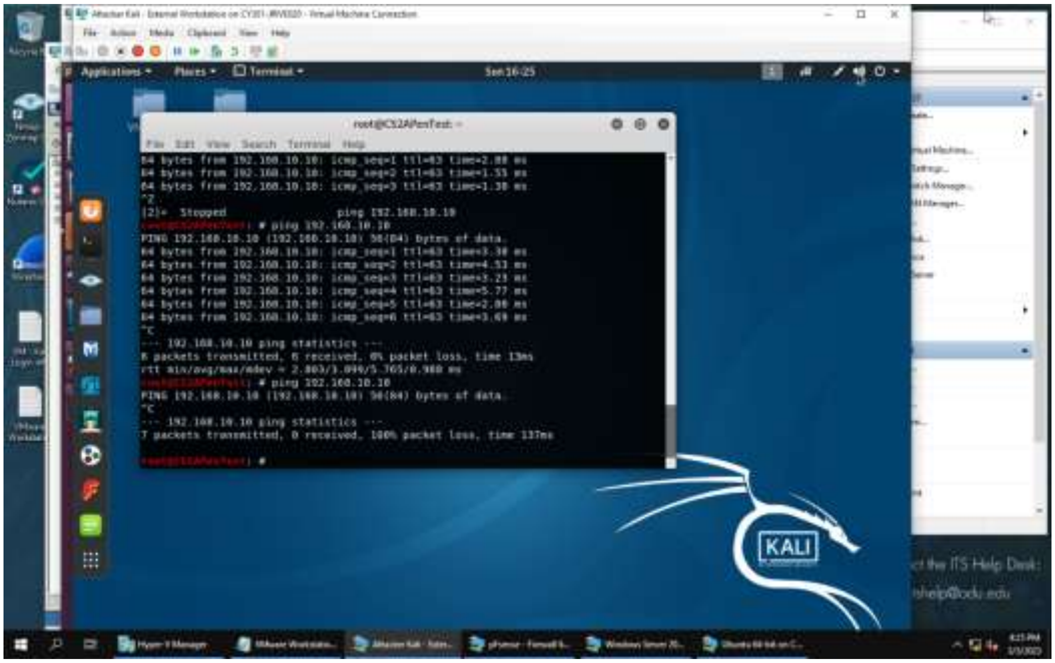
Firewall / Rules / LAN

The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
✓	2/1.55 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule
✗	0/0 B	IPv4 ICMP any	192.168.217.3	*	192.168.10.10	*	*	none		Block ICMP from Kali Attacker to Ubuntu
✓	41/2.05 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule
✓	0/0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule

Proof:

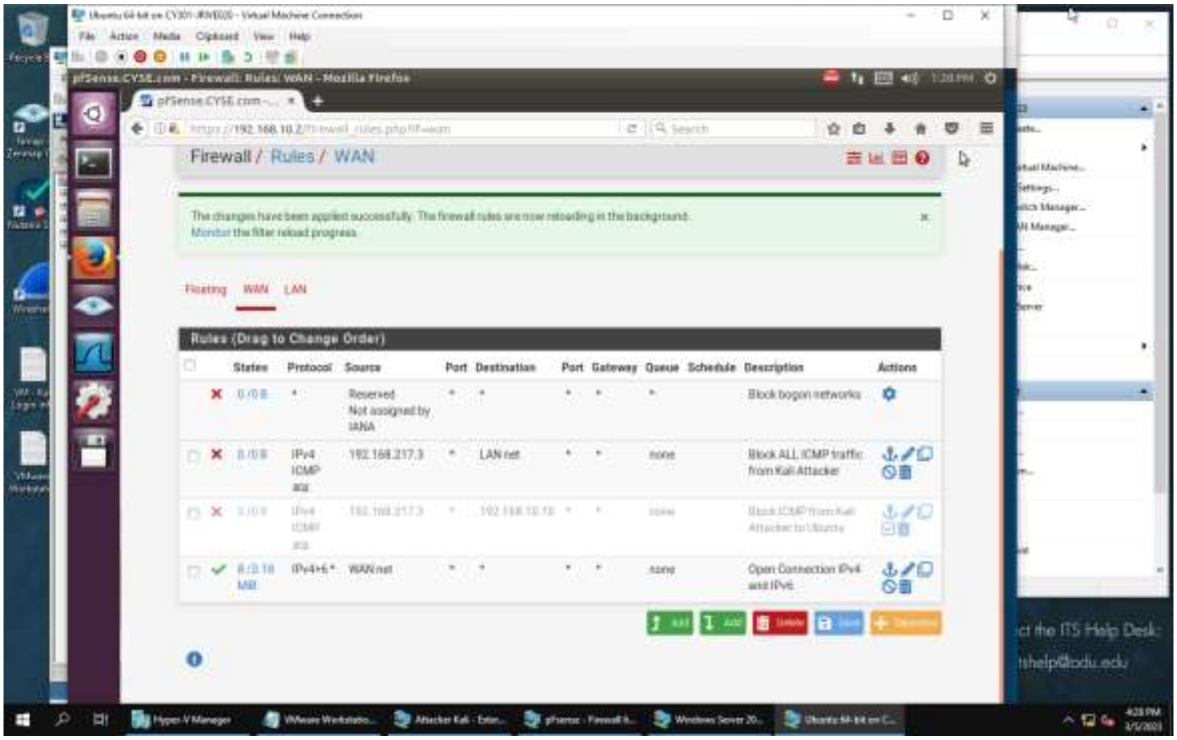


root@CS2APenTest: ~

```
64 bytes from 192.168.10.10: icmp_seq=1 ttl=63 time=2.88 ms
64 bytes from 192.168.10.10: icmp_seq=2 ttl=63 time=1.55 ms
64 bytes from 192.168.10.10: icmp_seq=3 ttl=63 time=1.38 ms
^Z
[2]+  Stopped                 ping 192.168.10.10
root@CS2APenTest:~# ping 192.168.10.10
PING 192.168.10.10 (192.168.10.10) 56(84) bytes of data.
64 bytes from 192.168.10.10: icmp_seq=1 ttl=63 time=3.38 ms
64 bytes from 192.168.10.10: icmp_seq=2 ttl=63 time=4.53 ms
64 bytes from 192.168.10.10: icmp_seq=3 ttl=63 time=3.23 ms
64 bytes from 192.168.10.10: icmp_seq=4 ttl=63 time=5.77 ms
64 bytes from 192.168.10.10: icmp_seq=5 ttl=63 time=2.80 ms
64 bytes from 192.168.10.10: icmp_seq=6 ttl=63 time=3.69 ms
^C
--- 192.168.10.10 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 13ms
rtt min/avg/max/mdev = 2.803/3.899/5.765/0.980 ms
root@CS2APenTest:~# ping 192.168.10.10
PING 192.168.10.10 (192.168.10.10) 56(84) bytes of data.
^C
--- 192.168.10.10 ping statistics ---
7 packets transmitted, 0 received, 100% packet loss, time 137ms

root@CS2APenTest:~#
```

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**	**LAN Network**	**IPv4 | ICMP:any**



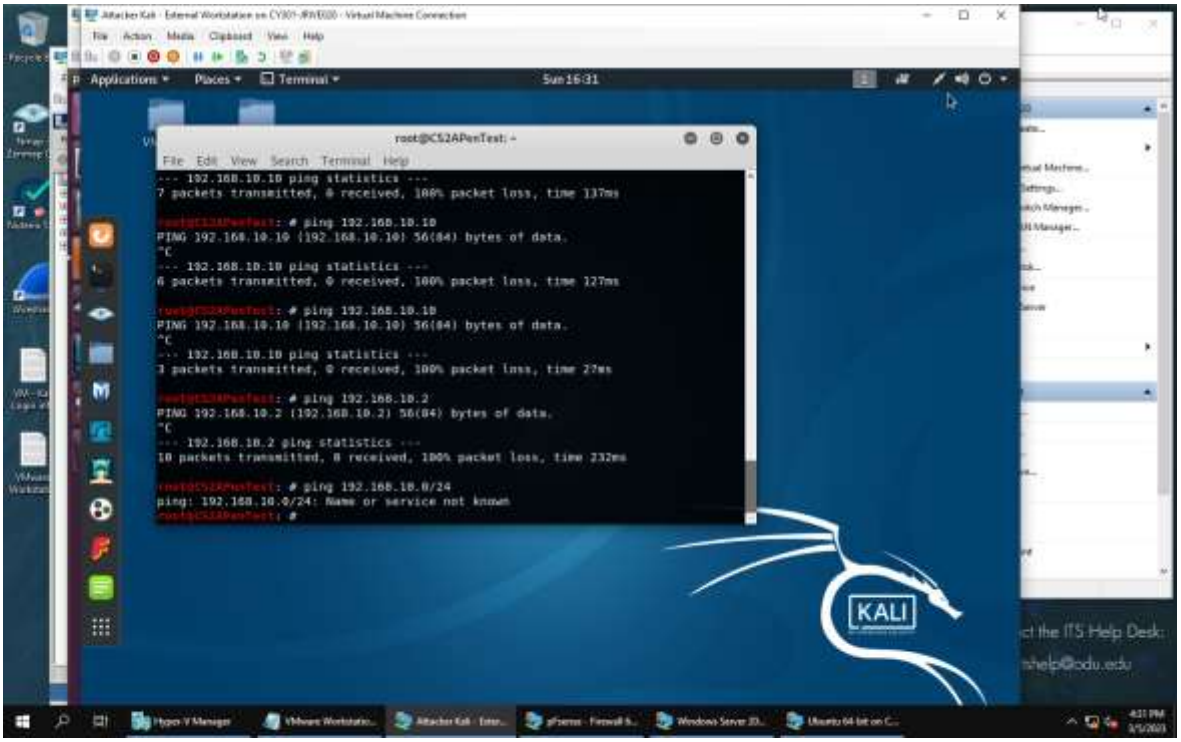
Firewall / Rules / WAN

The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
✗	0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks
✗	0/0 B	IPv4 ICMP any	192.168.217.3	*	LAN net	*	*	none		Block ALL ICMP traffic from Kali Attacker
✗	0/0 B	IPv4 ICMP any	192.168.217.3	*	192.168.10.10	*	*	none		Block ICMP from Kali Attacker to Ubuntu
✓	8/3.18 MiB	IPv4+6 *	WAN net	*	*	*	*	none		Open Connection IPv4 and IPv6

PROOF:

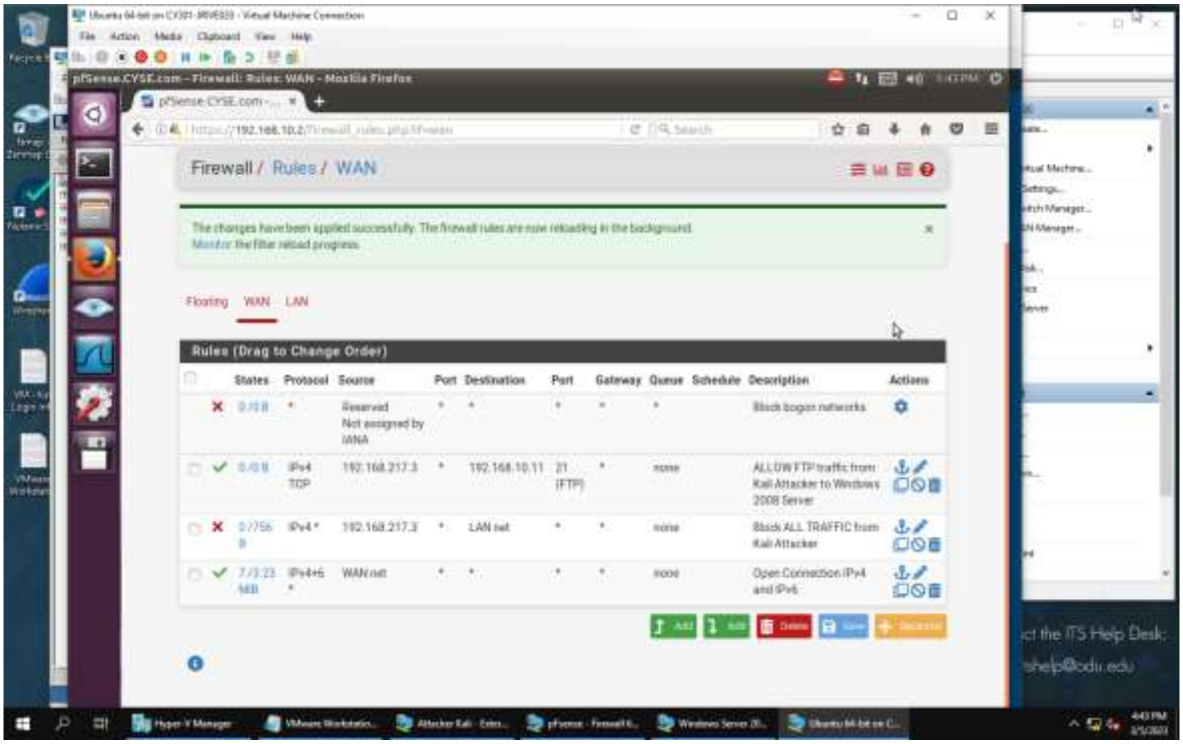


```
--- 192.168.10.10 ping statistics ---
7 packets transmitted, 0 received, 100% packet loss, time 137ms

root@CS2APenTest:~# ping 192.168.10.10
PING 192.168.10.10 (192.168.10.10) 56(84) bytes of data.
^C
--- 192.168.10.10 ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 127ms

root@CS2APenTest:~# ping 192.168.10.10
PING 192.168.10.10 (192.168.10.10) 56(84) bytes of data.
^C
--- 192.168.10.10 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 27ms

root@CS2APenTest:~# ping 192.168.10.2
PING 192.168.10.2 (192.168.10.2) 56(84) bytes of data.
^C
--- 192.168.10.2 ping statistics ---
10 packets transmitted, 0 received, 100% packet loss, time 232ms

root@CS2APenTest:~# ping 192.168.10.0/24
ping: 192.168.10.0/24: Name or service not known
root@CS2APenTest:~#
```

(Please ignore the last one, I was just testing something!)

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 2008.

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
2	**WAN**	**Pass**	**192.168.217.3**	**192.168.10.11**	**IPv4 | TCP:Port 21 (TFTP)**
3	**WAN**	**Block**	**192.168.217.3**	**LAN Network**	**IPv4 | ALL TRAFFIC**


pfSense.CYSE.com - Firewall: Rules: WAN - Mozilla Firefox

Firewall / Rules / WAN

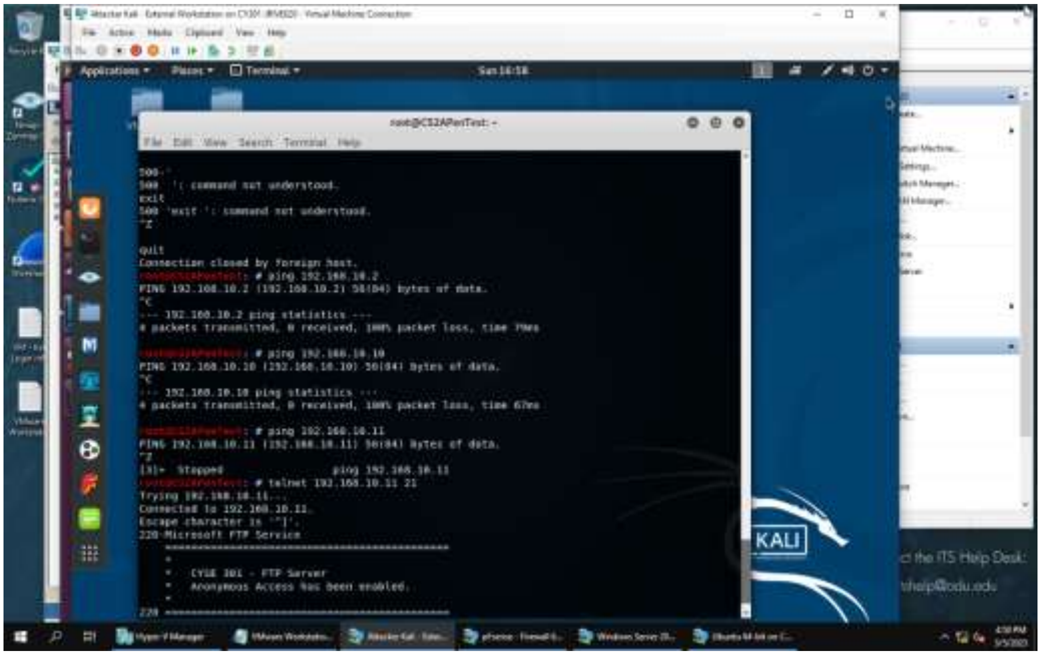
The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

Floating WAN LAN

Rules (Drag to Change Order)

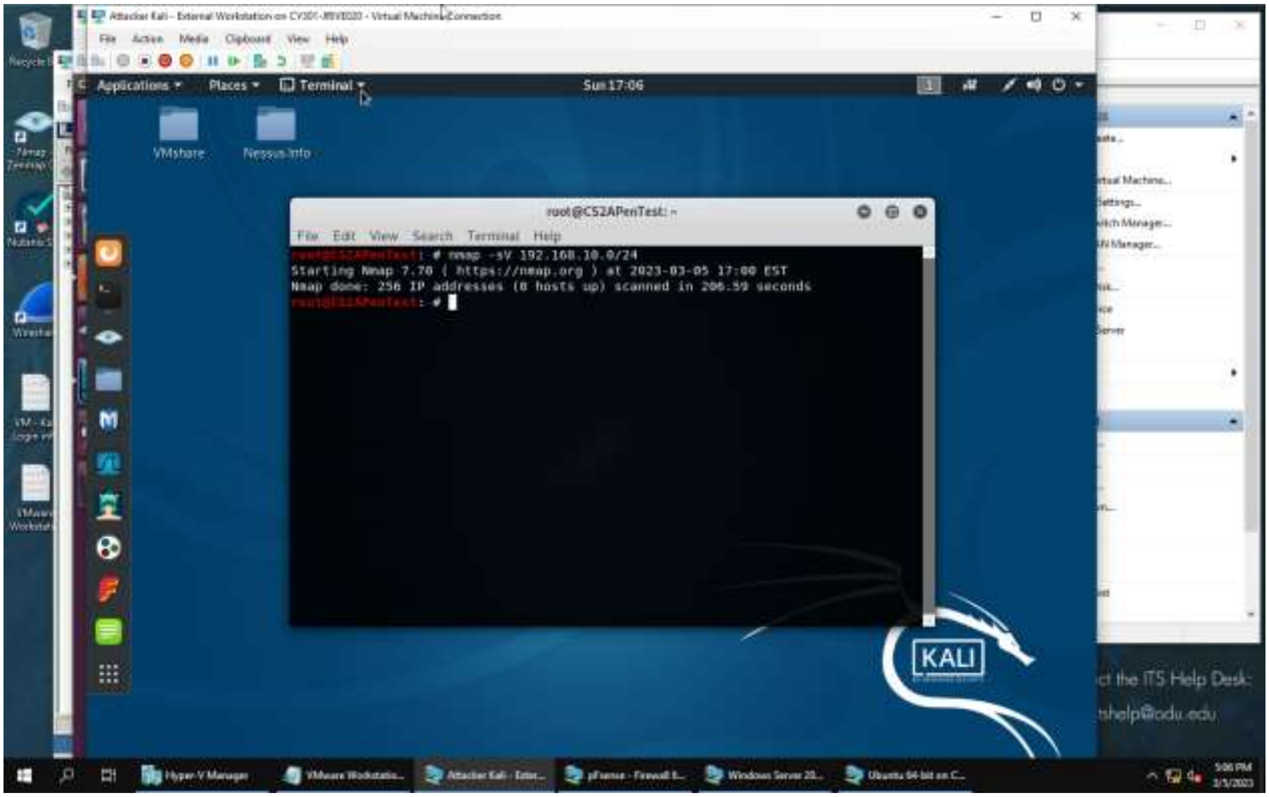
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✗	0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
✓	0/0 B	IPv4 TCP	192.168.217.3	*	192.168.10.11	21 (FTP)	*	none		ALLOW FTP traffic from Kali Attacker to Windows 2008 Server	
✗	0/756 B	IPv4 *	192.168.217.3	*	LAN net	*	*	none		Block ALL TRAFFIC from Kali Attacker	
✓	7/3.23 MiB	IPv4+6 *	WAN net	*	*	*	*	none		Open Connection IPv4 and IPv6	

Proof:


```
500-'
500 ' : command not understood.
exit
500 'exit ' : command not understood.
^Z

quit
Connection closed by foreign host.
root@CS2APenTest:~# ping 192.168.10.2
PING 192.168.10.2 (192.168.10.2) 56(84) bytes of data.
^C
--- 192.168.10.2 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 79ms

root@CS2APenTest:~# ping 192.168.10.10
PING 192.168.10.10 (192.168.10.10) 56(84) bytes of data.
^C
--- 192.168.10.10 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 67ms

root@CS2APenTest:~# ping 192.168.10.11
PING 192.168.10.11 (192.168.10.11) 56(84) bytes of data.
^Z
[1]+  Stopped                 ping 192.168.10.11
root@CS2APenTest:~# telnet 192.168.10.11 21
Trying 192.168.10.11...
Connected to 192.168.10.11.
Escape character is '^]'.
220-Microsoft FTP Service
    ****************************************
    *
    *   CYSE 301 - FTP Server
    *   Anonymous Access has been enabled.
    *
220 ****************************************
```

You can see that ICMP traffic is blocked overall, but we can use Telnet to see that port 21 is open for business!

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



```
root@CS2APenTest:~# nmap -sV 192.168.10.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2023-03-05 17:00 EST
Nmap done: 256 IP addresses (0 hosts up) scanned in 206.59 seconds
root@CS2APenTest:~# 
```

All traffic is blocked. I don’t think that NMAP scans port 21, but as you could see before, port 21 can be accessed.

Extra credit (15 points): Use NESSUS to enumerate the security vulnerabilities of Microsoft Windows Server 2008 VM in the CCIA network.