CYSE 301: Cybersecurity Technique and Operations

Assignment 3: Sword vs. Shield

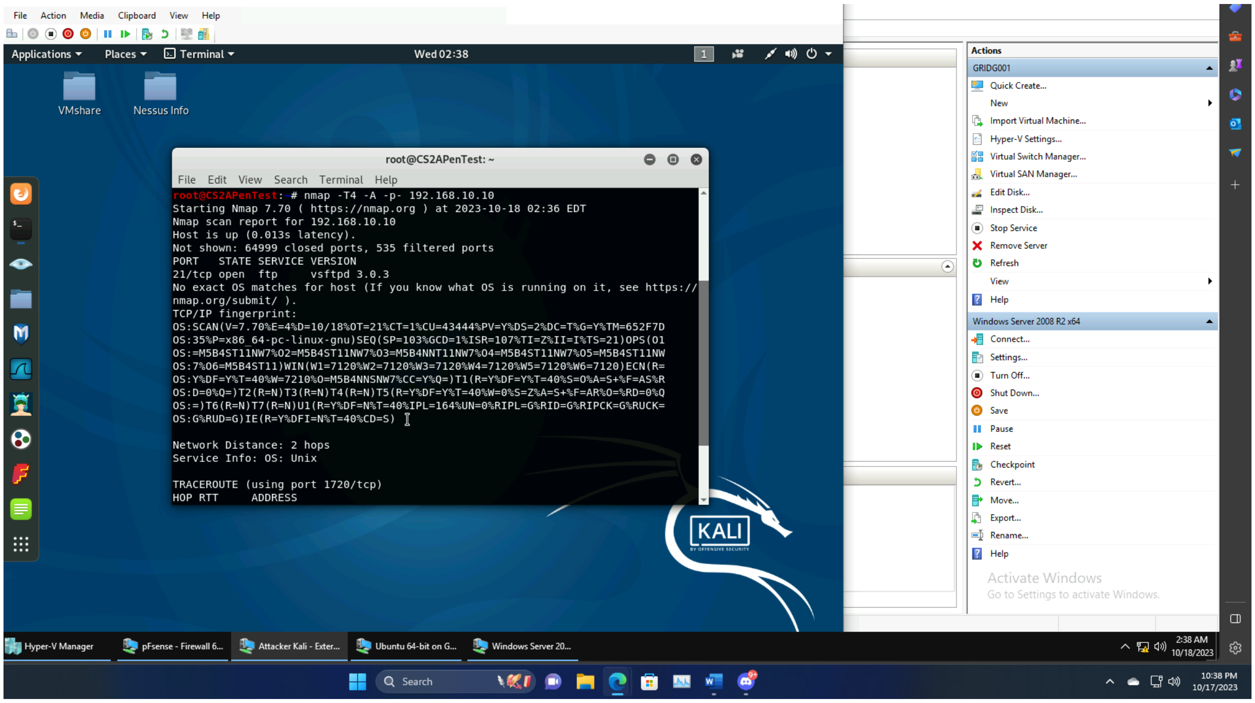
In this assignment, you will act as an attacker to identify the vulnerabilities in the LAN network and a defender to apply proper countermeasures. You need to provide a screenshot for each task below.

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 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.



```
root@CS2APenTest:~# nmap -T4 -A -p- 192.168.10.10
Starting Nmap 7.70 ( https://nmap.org ) at 2023-10-18 02:36 EDT
Nmap scan report for 192.168.10.10
Host is up (0.013s latency).
Not shown: 64999 closed ports, 535 filtered ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
No exact OS matches for host (If you know what OS is running on it, see https://
nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.70%E=4%D=10/18%OT=21%CT=1%CU=43444%PV=Y%DS=2%DC=T%G=Y%TM=652F7D
OS:35%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=107%TI=Z%II=I%TS=21)OPS(O1
OS:=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=M5B4ST11NW
OS:7%O6=M5B4ST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN(R=
OS:Y%DF=Y%T=40%W=7210%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%R
OS:D=0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q
OS:=)T6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=
OS:G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Unix

TRACEROUTE (using port 1720/tcp)
HOP RTT     ADDRESS
```

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.**

When running Wireshark on an Ubuntu VM while an external Kali machine scans the network, the captured traffic pattern would reveal several critical observations. ARP (Address Resolution Protocol) plays a fundamental role in this scenario. ARP is responsible for mapping IP addresses to MAC addresses within a local network, and it's evident from the traffic that the Kali machine is actively employing ARP to discover the active hosts in the network. These ARP requests aim to ascertain the MAC addresses associated with each IP address within the subnet, facilitating the identification of live hosts.

In addition to the ARP traffic, Wireshark would capture a substantial number of TCP queries initiated by the Kali machine. These queries are part of a port scanning operation, with the Kali machine attempting to identify available services running on the target hosts. Each TCP packet represents an attempt to establish a connection with a specific port on the target. Suspicion arises from the detection of empty TCP packets, which can be indicative of reconnaissance or scanning activities.

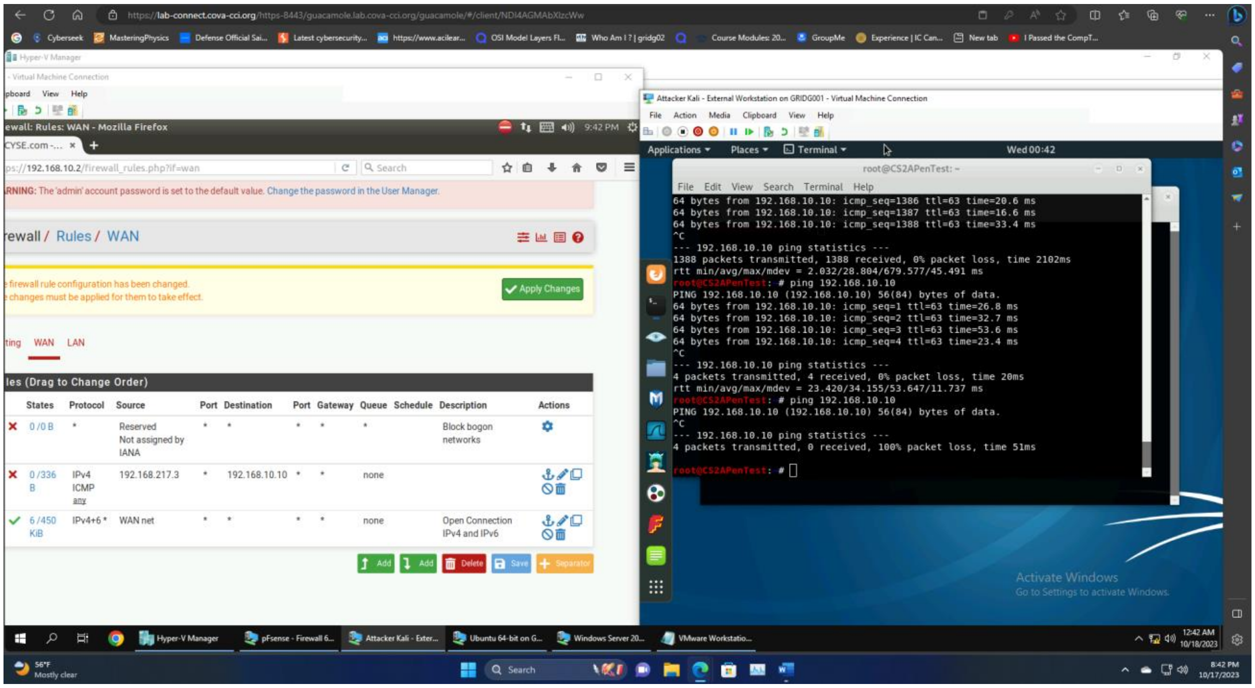
Furthermore, the analysis of the packet hierarchy reveals that a total of 3413 packets were collected. Notably, the 'win' (window size) and 'len' (length) values for the TCP packets were consistently set to zero. This could indicate that the Kali machine was either attempting to minimize its footprint or experiencing issues during the scanning operation.

In summary, the observed traffic pattern is characterized by ARP requests seeking to map IP addresses to MAC addresses, TCP queries for service identification, and peculiar empty TCP packets. The collection of a significant number of packets suggests an extensive scanning operation, while the use of zero 'win' and 'len' values in TCP packets raises questions about the scanning methodology employed. This network traffic pattern could be indicative of a security audit or, potentially, unauthorized probing, underscoring the importance of vigilant network monitoring and security measures.

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.



ewall: Rules: WAN - Mozilla Firefox
ps://192.168.10.2/firewall_rules.php?if=wan
Attacker Kali - External Workstation on GRIDG001 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal
Wed 00:42
root@CS2APenTest: ~
File Edit View Search Terminal Help
Apply Changes
Add
Add
Delete
Save
Separator
Activate Windows
Go to Settings to activate Windows.
Hyper-V Manager
pFsense - Firewall 6...
Attacker Kali - Exter...
Ubuntu 64-bit on G...
Windows Server 20...
VMware Workstatio...

RNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

rewall / Rules / WAN

e firewall rule configuration has been changed.
e changes must be applied for them to take effect.

ting WAN LAN

les (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 /336 B	IPv4 ICMP any	192.168.217.3	*	192.168.10.10	*	*	none			
✓	6 /450 KiB	IPv4+6 *	WAN net	*	*	*	*	none		Open Connection IPv4 and IPv6	

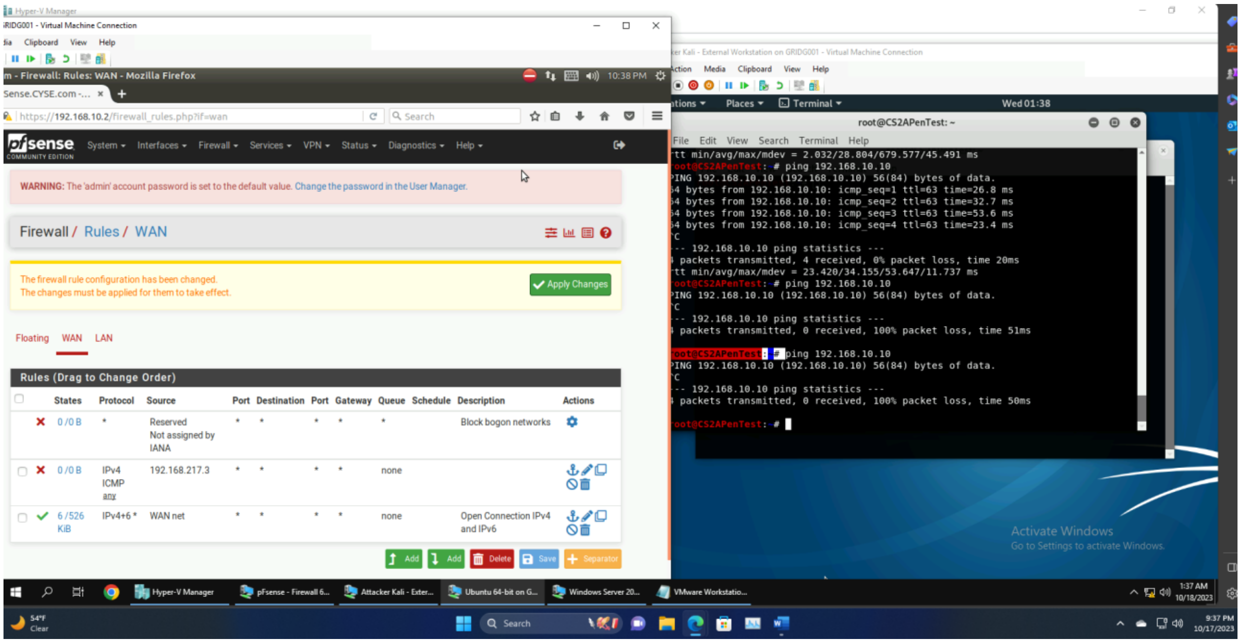
```
64 bytes from 192.168.10.10: icmp_seq=1386 ttl=63 time=20.6 ms
64 bytes from 192.168.10.10: icmp_seq=1387 ttl=63 time=16.6 ms
64 bytes from 192.168.10.10: icmp_seq=1388 ttl=63 time=33.4 ms
^C
--- 192.168.10.10 ping statistics ---
1388 packets transmitted, 1388 received, 0% packet loss, time 2102ms
rtt min/avg/max/mdev = 2.032/28.804/679.577/45.491 ms
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=26.8 ms
64 bytes from 192.168.10.10: icmp_seq=2 ttl=63 time=32.7 ms
64 bytes from 192.168.10.10: icmp_seq=3 ttl=63 time=53.6 ms
64 bytes from 192.168.10.10: icmp_seq=4 ttl=63 time=23.4 ms
^C
--- 192.168.10.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 20ms
rtt min/avg/max/mdev = 23.420/34.155/53.647/11.737 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 ---
4 packets transmitted, 0 received, 100% packet loss, time 51ms

root@CS2APenTest:~# 
```

Verification:-Ping Ubuntu (No)-Ping WS Server (Yes)-FTP Ubuntu (Yes)

Rule #	Interface	Action	Source IP	Destination IP	Protocol

					(port # if appliable)
1	WAN	Block	192.168.217.3	192.168.10.10	N/A

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



WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Firewall / Rules / WAN

The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

Rules (Drag to Change Order)

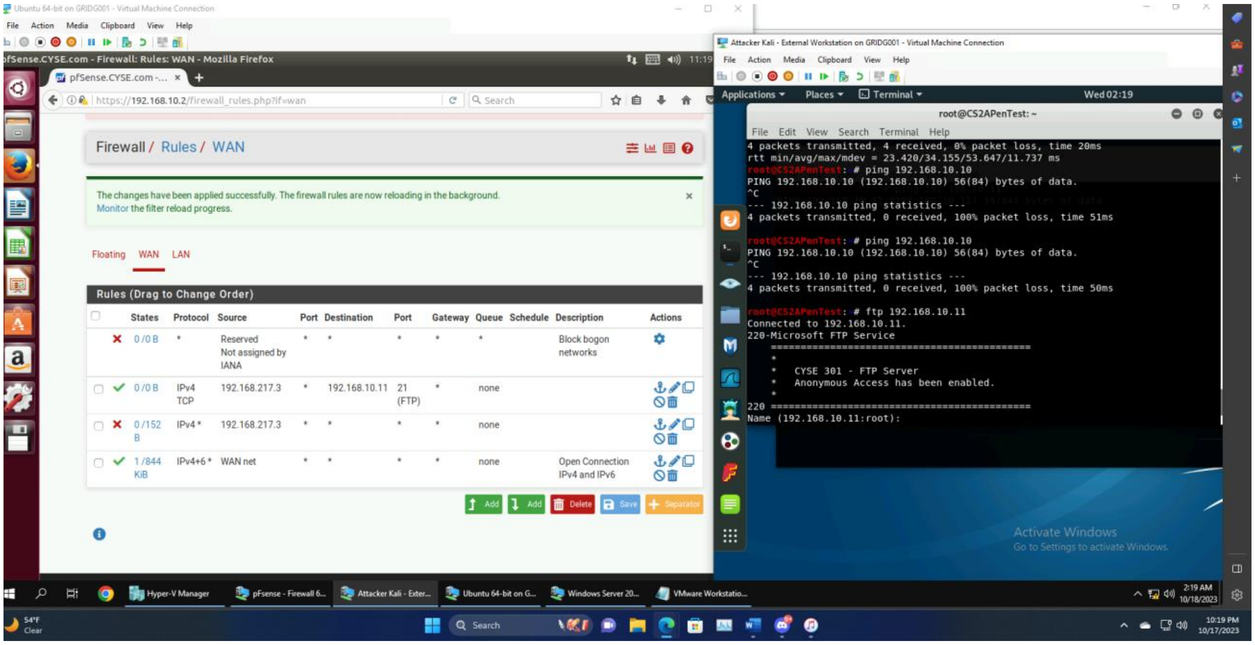
		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
	✗	0 /0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks
□	✗	0 /0 B	IPv4 ICMP any	192.168.217.3	*	*	*	*	none		
□	✓	6 /526 KiB	IPv4+6 *	WAN net	*	*	*	*	none		Open Connection IPv4 and IPv6

```
rtt min/avg/max/mdev = 2.032/28.804/679.577/45.491 ms
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=26.8 ms
64 bytes from 192.168.10.10: icmp_seq=2 ttl=63 time=32.7 ms
64 bytes from 192.168.10.10: icmp_seq=3 ttl=63 time=53.6 ms
64 bytes from 192.168.10.10: icmp_seq=4 ttl=63 time=23.4 ms
^C
--- 192.168.10.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 20ms
rtt min/avg/max/mdev = 23.420/34.155/53.647/11.737 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 ---
4 packets transmitted, 0 received, 100% packet loss, time 51ms

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 50ms

root@CS2APenTest:~# 
```

Verification:-Ping Ubuntu (No)-Ping WS Server (No)-FTP Ubuntu (Yes)

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
1	Wan	Block	192.168.217.3	All	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 2008.



Ubuntu 64-bit on GRIDG001 - Virtual Machine Connection
File Action Media Clipboard View Help
pfSense.CYSE.com - Firewall: Rules: WAN - Mozilla Firefox
11:19
pfSense.CYSE.com -...
https://192.168.10.2/firewall_rules.php?if=wan
Search
Attacker Kali - External Workstation on GRIDG001 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal
Wed 02:19
root@CS2APenTest: ~
File Edit View Search Terminal Help
Activate Windows
Go to Settings to activate Windows.
Hyper-V Manager
pFsense - Firewall 6...
Attacker Kali - Exter...
Ubuntu 64-bit on G...
Windows Server 20...
VMware Workstatio...
2:19 AM
10/18/2023
54°F
Clear
Search
10:19 PM
10/17/2023

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			
□	✗	0 /152 B	IPv4 *	192.168.217.3	*	*	*	*	none			
□	✓	1 /844 KiB	IPv4+6 *	WAN net	*	*	*	*	none		Open Connection IPv4 and IPv6	

Add Add Delete Save Separator

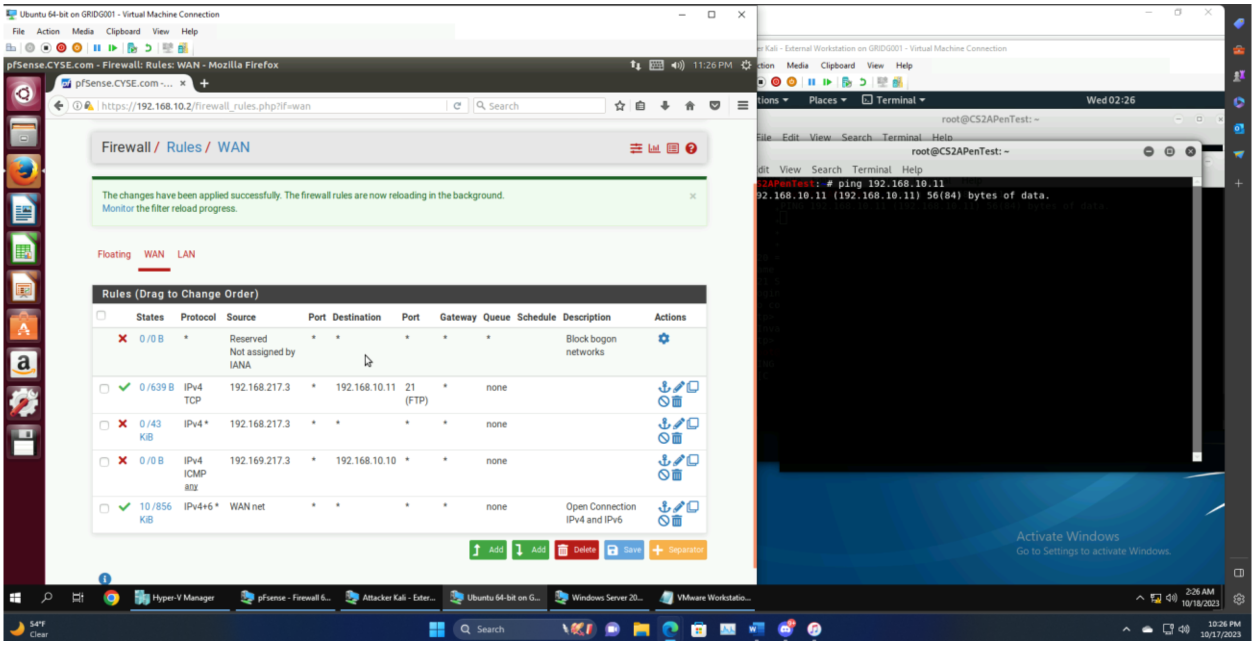
```
4 packets transmitted, 4 received, 0% packet loss, time 20ms
rtt min/avg/max/mdev = 23.420/34.155/53.647/11.737 ms
root@CS2APenTest:~# ping 192.168.10.10
PING 192.168.10.10 (192.168.10.10) 56(84) bytes of data.
^C
--- 192.168.10.10 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 51ms

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 50ms

root@CS2APenTest:~# ftp 192.168.10.11
Connected to 192.168.10.11.
220-Microsoft FTP Service
    ============================================
    *
    *   CYSE 301 - FTP Server
    *   Anonymous Access has been enabled.
    *
220 ============================================
Name (192.168.10.11:root):
```

Verification:-Ping Ubuntu (No)-Ping WS Server (No)-FTP Ubuntu (No)-FTP. WS2008 (Yes)

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
1	wan	pass	192.168.217.3	192.168.10.11	FTP
2	wan	block	192.168.217.3	All	ALL

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

It now says that the pings are possibly being blocked.


Ubuntu 64-bit on GRIDG001 - Virtual Machine Connection
File Action Media Clipboard View Help
pfSense.CYSE.com - Firewall: Rules: WAN - Mozilla Firefox
11:26 PM
pfSense.CYSE.com -...
https://192.168.10.2/firewall_rules.php?if=wan
Search
Floating
WAN
LAN
Add
Add
Delete
Save
Separator
Kali - External Workstation on GRIDG001 - Virtual Machine Connection
Places
Terminal
Wed 02:26
root@CS2APenTest: ~
File Edit View Search Terminal Help
Activate Windows
Go to Settings to activate Windows.
Hyper-V Manager
pFsense - Firewall 6...
Attacker Kali - Exter...
Ubuntu 64-bit on G...
Windows Server 20...
VMware Workstatio...
2:26 AM
10/18/2023
54°F
Clear
Search
10:26 PM
10/17/2023

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	Actions
	✗	0 /0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
□	✓	0 /639 B	IPv4 TCP	192.168.217.3	*	192.168.10.11	21 (FTP)	*	none			
□	✗	0 /43 KiB	IPv4 *	192.168.217.3	*	*	*	*	none			
□	✗	0 /0 B	IPv4 ICMP any	192.169.217.3	*	192.168.10.10	*	*	none			
□	✓	10 /856 KiB	IPv4+6 *	WAN net	*	*	*	*	none		Open Connection IPv4 and IPv6	

```
S2APenTest:~# ping 192.168.10.11
92.168.10.11 (192.168.10.11) 56(84) bytes of data.
```

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