CYSE 301: Cybersecurity Technique and Operations

Assignment 3: Sword vs. Shield

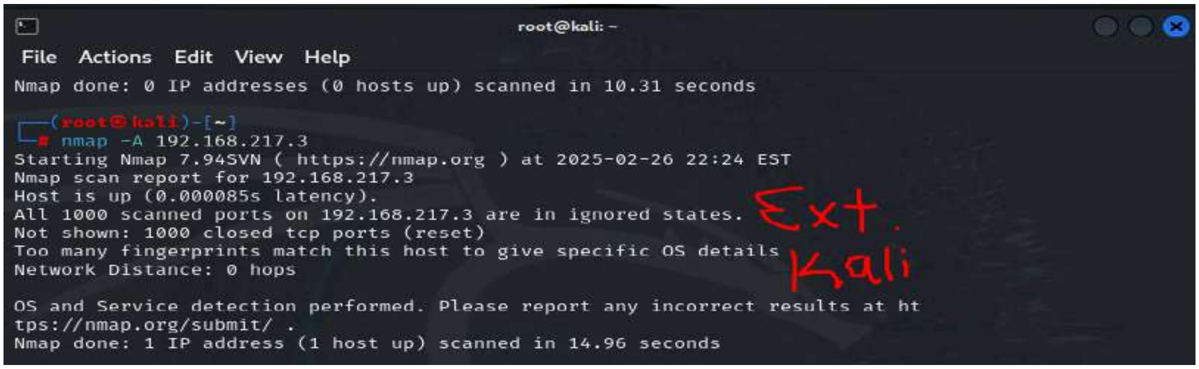
In this assignment, you will act as an attacker to identify the vulnerabilities in the LAN network and a defender to apply proper countermeasures. You need to provide a screenshot for each task below.

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)

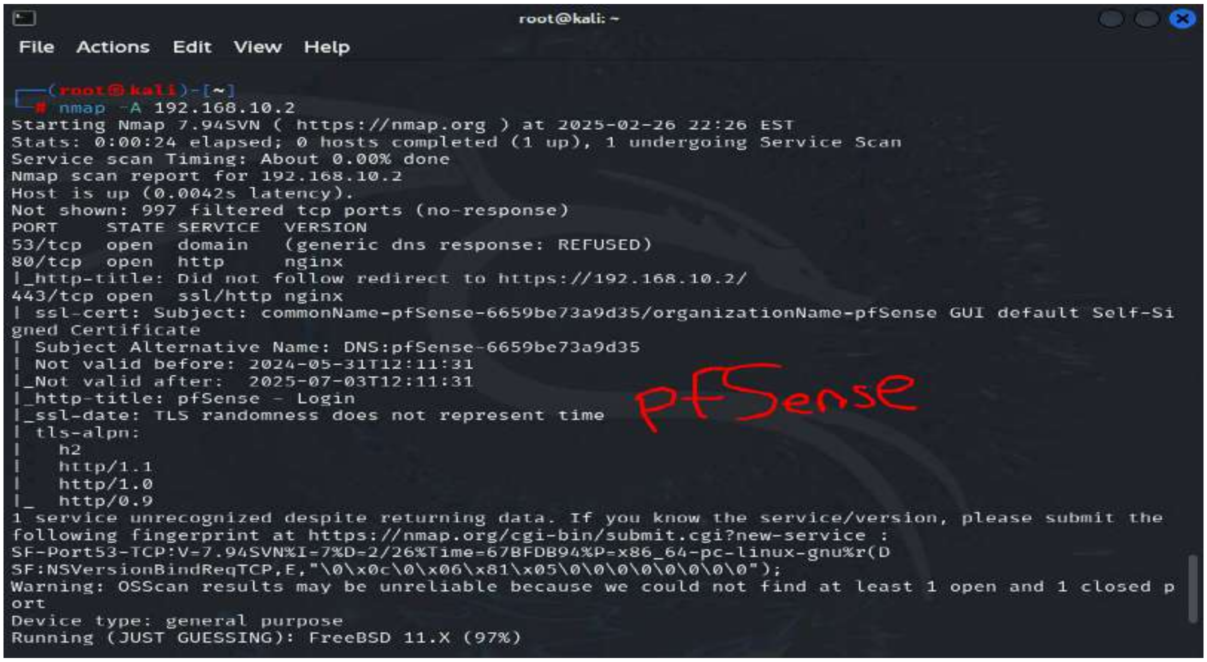
- External Kali
- pfSense
- Ubuntu
- Windows Server 2022

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

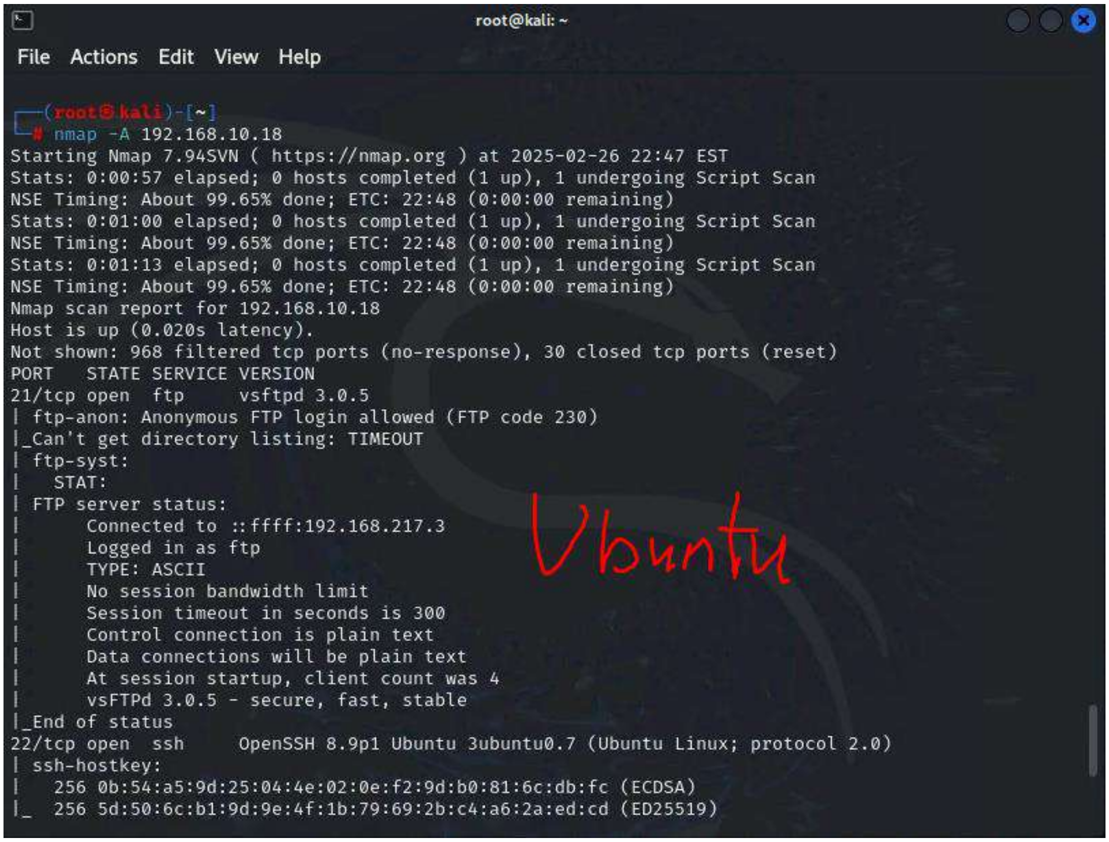
1. Use Nmap to profile the basic information about the **subnet** topology (including open ports information, operation systems, etc.) You need to get the **service** and **backend software** information associated with each opening port in each VM.



```
Nmap done: 0 IP addresses (0 hosts up) scanned in 10.31 seconds

┌──(root㉿kali)-[~]
└─# nmap -A 192.168.217.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-26 22:24 EST
Nmap scan report for 192.168.217.3
Host is up (0.000085s latency).
All 1000 scanned ports on 192.168.217.3 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.96 seconds
```

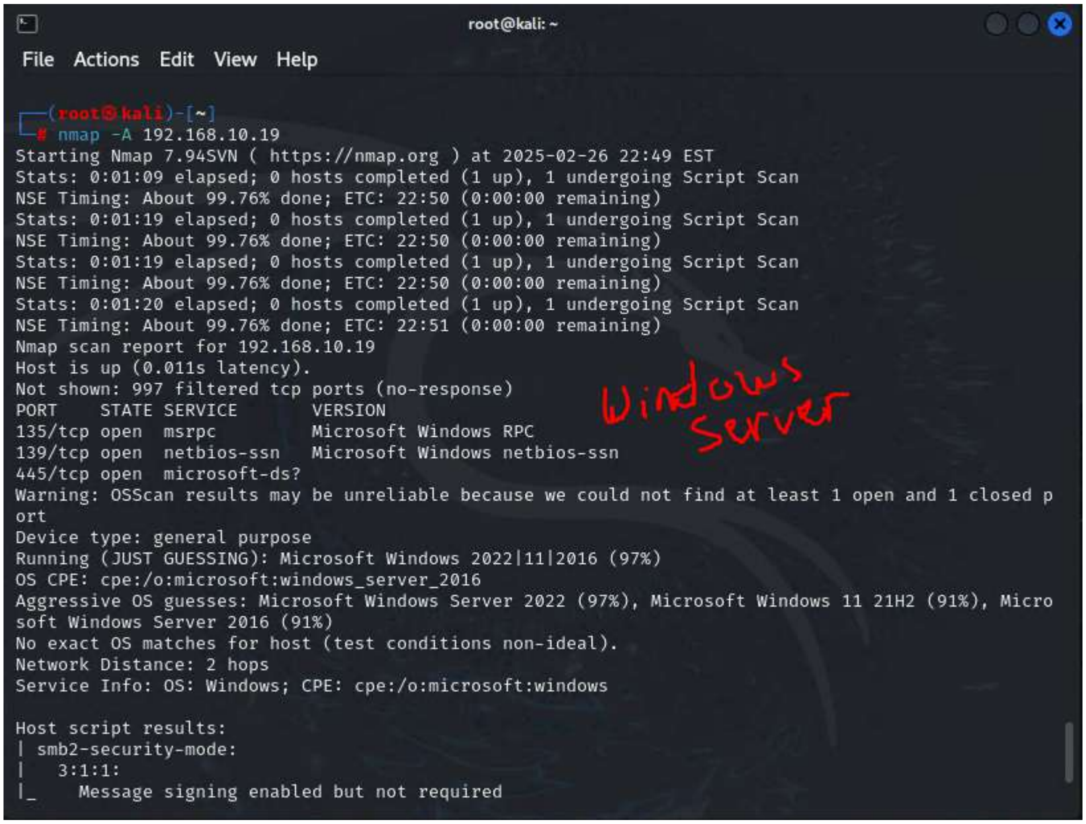


```
┌──(root㉿kali)-[~]
└─# nmap -A 192.168.10.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-26 22:26 EST
Stats: 0:00:24 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Nmap scan report for 192.168.10.2
Host is up (0.0042s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
53/tcp  open  domain   (generic dns response: REFUSED)
80/tcp  open  http     nginx
|_http-title: Did not follow redirect to https://192.168.10.2/
443/tcp open  ssl/http nginx
| ssl-cert: Subject: commonName=pfSense-6659be73a9d35/organizationName=pfSense GUI default Self-Si
gned Certificate
| Subject Alternative Name: DNS:pfSense-6659be73a9d35
| Not valid before: 2024-05-31T12:11:31
|_Not valid after:  2025-07-03T12:11:31
|_http-title: pfSense - Login
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|   h2
|   http/1.1
|   http/1.0
|_  http/0.9
1 service unrecognized despite returning data. If you know the service/version, please submit the
following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.94SVN%I=7%D=2/26%Time=67BFDB94%P=x86_64-pc-linux-gnu%r(D
SF:NSVersionBindReqTCP,E,"\0\x0c\0\x06\x81\x05\0\0\0\0\0\0\0\0");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed p
ort
Device type: general purpose
Running (JUST GUESSING): FreeBSD 11.X (97%)
```



```
┌──(root㉿kali)-[~]
└─# nmap -A 192.168.10.18
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-26 22:47 EST
Stats: 0:00:57 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.65% done; ETC: 22:48 (0:00:00 remaining)
Stats: 0:01:00 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.65% done; ETC: 22:48 (0:00:00 remaining)
Stats: 0:01:13 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.65% done; ETC: 22:48 (0:00:00 remaining)
Nmap scan report for 192.168.10.18
Host is up (0.020s 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
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.217.3
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.5 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 0b:54:a5:9d:25:04:4e:02:0e:f2:9d:b0:81:6c:db:fc (ECDSA)
|_  256 5d:50:6c:b1:9d:9e:4f:1b:79:69:2b:c4:a6:2a:ed:cd (ED25519)
```

Ubuntu



```
┌──(root㉿kali)-[~]
└─# nmap -A 192.168.10.19
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-26 22:49 EST
Stats: 0:01:09 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.76% done; ETC: 22:50 (0:00:00 remaining)
Stats: 0:01:19 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.76% done; ETC: 22:50 (0:00:00 remaining)
Stats: 0:01:19 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.76% done; ETC: 22:50 (0:00:00 remaining)
Stats: 0:01:20 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.76% done; ETC: 22:51 (0:00:00 remaining)
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       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 p
ort
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2022|11|2016 (97%)
OS CPE: cpe:/o:microsoft:windows_server_2016
Aggressive OS guesses: Microsoft Windows Server 2022 (97%), Microsoft Windows 11 21H2 (91%), Micro
soft Windows Server 2016 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
```

Windows Server

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.**

After running Wireshark in Internal Kali VM while External Kali was scanning the network, several findings can be observed in the traffic pattern. The scanning started with a few ARP packets where the External Kali VM queried the subnet for live hosts. Afterwards an ICMP packet was produced. It can be assumed that this was during the Nmap scanning of active virtual machines and that it was working to detect what active devices were in the network. There were a high number of DNS packets that appeared as standard queries during the Nmap's scanning of services. The ARP packets that were reported tells that 192.168.10.2 is at 00:15:5d:40:57:29. There was a high number of TCP SYN packets sent to different ports via various IPS, which can be traced back to a SYN scan. Based on these findings, the behavior of these traffic patterns on Wireshark is the typical behavior of network discovery and activities related to investigations. The main takeaway is that this sort of behavior has the aim to discover in the network what the live hosts are, what open ports exist, and the current services. All of this together can be used in providing security in the network.

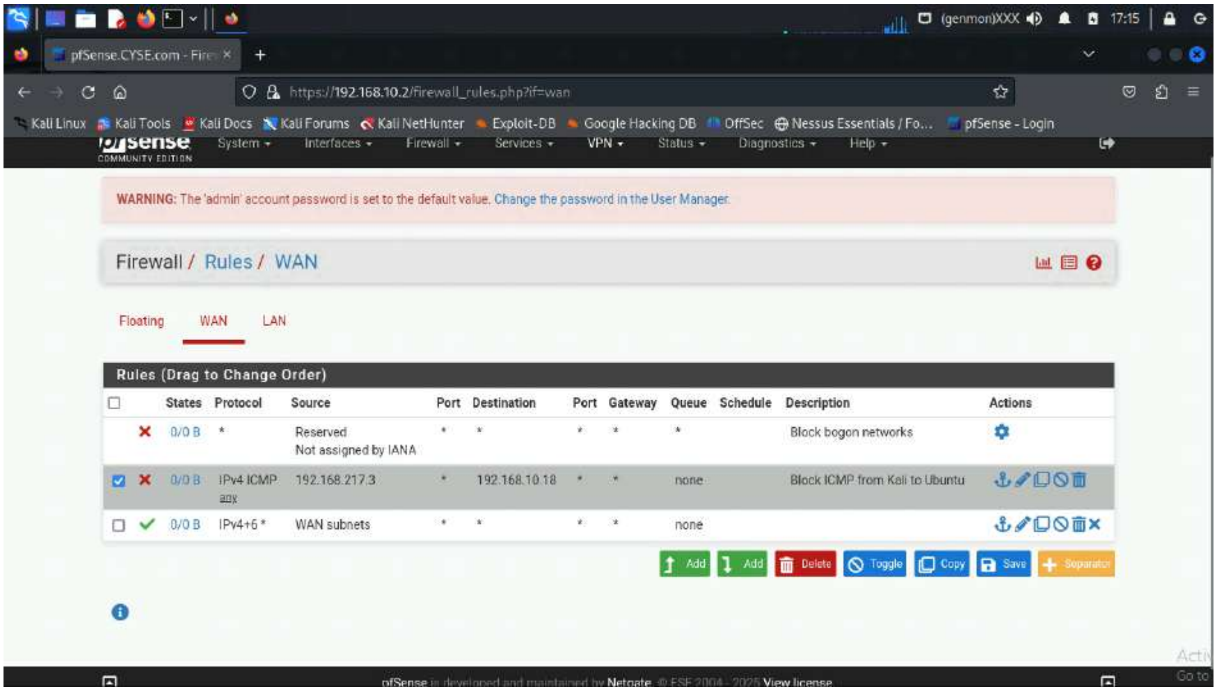
Task B: Shield – Protect your network with a firewall (10 + 10+ 20 + 20 = 60 points)

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	IPv4 ICMP

[Add the screenshot here]

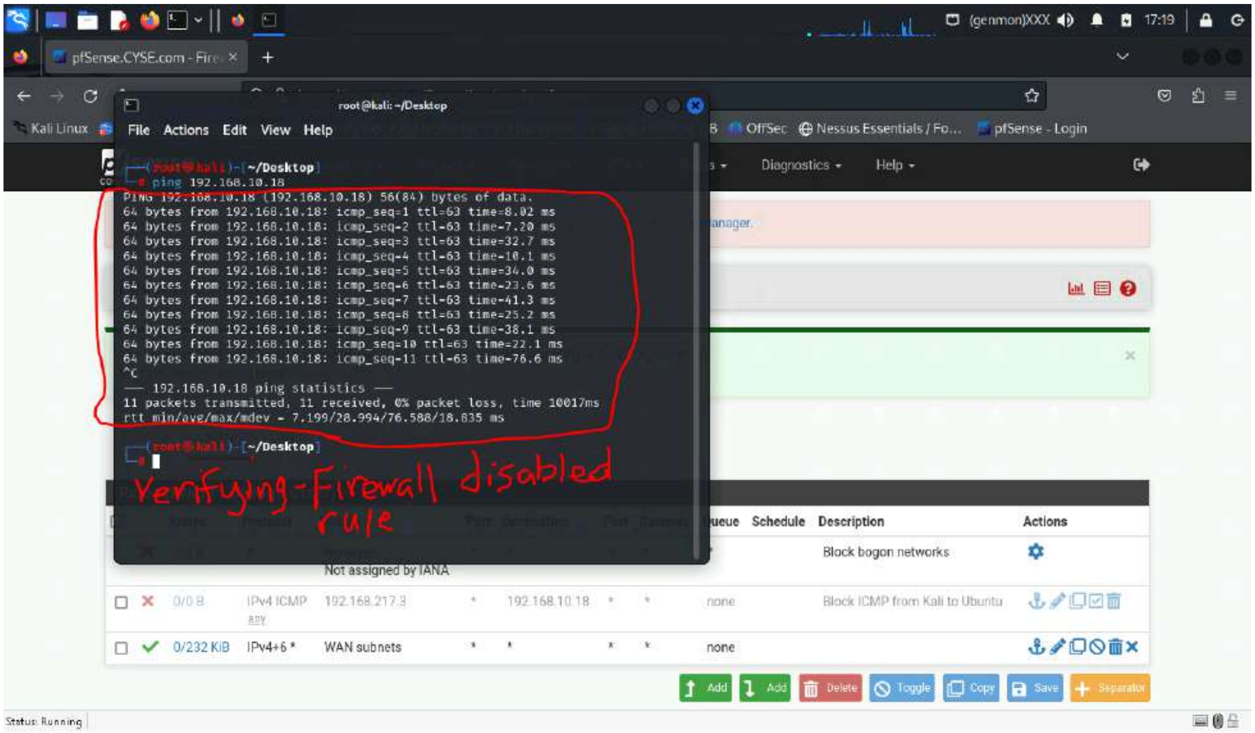


WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Firewall / Rules / WAN

Rules (Drag to Change Order)

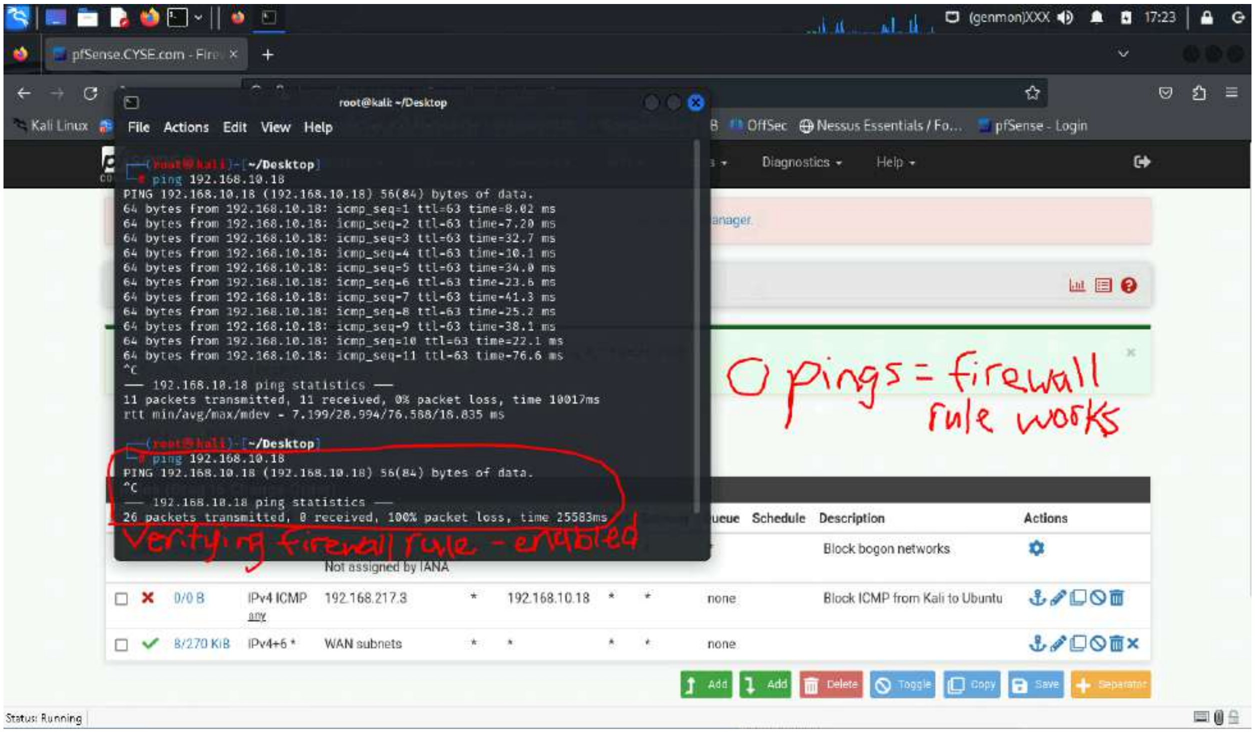
□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✗	0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
☑	✗	0/0 B	IPv4 ICMP any	192.168.217.3	*	192.168.10.18	*	*	none		Block ICMP from Kali to Ubuntu	
□	✓	0/0 B	IPv4+6 *	WAN subnets	*	*	*	*	none			



```
┌──(root㉿kali)-[~/Desktop]
└─# ping 192.168.10.18
PING 192.168.10.18 (192.168.10.18) 56(84) bytes of data.
64 bytes from 192.168.10.18: icmp_seq=1 ttl=63 time=8.02 ms
64 bytes from 192.168.10.18: icmp_seq=2 ttl=63 time=7.20 ms
64 bytes from 192.168.10.18: icmp_seq=3 ttl=63 time=32.7 ms
64 bytes from 192.168.10.18: icmp_seq=4 ttl=63 time=10.1 ms
64 bytes from 192.168.10.18: icmp_seq=5 ttl=63 time=34.0 ms
64 bytes from 192.168.10.18: icmp_seq=6 ttl=63 time=23.6 ms
64 bytes from 192.168.10.18: icmp_seq=7 ttl=63 time=41.3 ms
64 bytes from 192.168.10.18: icmp_seq=8 ttl=63 time=25.2 ms
64 bytes from 192.168.10.18: icmp_seq=9 ttl=63 time=38.1 ms
64 bytes from 192.168.10.18: icmp_seq=10 ttl=63 time=22.1 ms
64 bytes from 192.168.10.18: icmp_seq=11 ttl=63 time=76.6 ms
^C
--- 192.168.10.18 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10017ms
rtt min/avg/max/mdev = 7.199/28.994/76.588/18.835 ms

┌──(root㉿kali)-[~/Desktop]
└─# █
```

Verifying - Firewall disabled rule

										Queue	Schedule	Description	Actions
												Block bogon networks	
			Not assigned by IANA										
☐	✗	0/0 B	IPv4 ICMP any	192.168.217.3	*	192.168.10.18	*	*	none			Block ICMP from Kali to Ubuntu	
☐	✓	0/232 KiB	IPv4+6 *	WAN subnets	*	*	*	*	none				

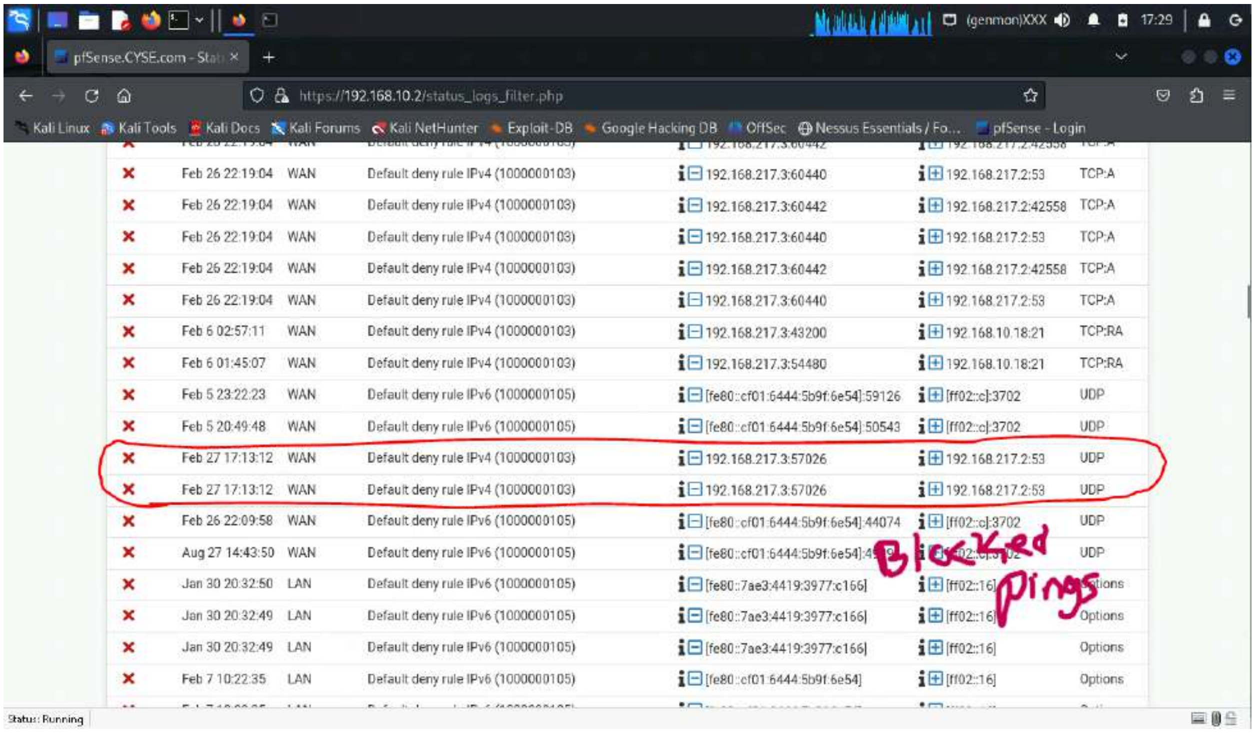


```
┌──(root㉿kali)-[~/Desktop]
└─# ping 192.168.10.18
PING 192.168.10.18 (192.168.10.18) 56(84) bytes of data.
64 bytes from 192.168.10.18: icmp_seq=1 ttl=63 time=8.02 ms
64 bytes from 192.168.10.18: icmp_seq=2 ttl=63 time=7.20 ms
64 bytes from 192.168.10.18: icmp_seq=3 ttl=63 time=32.7 ms
64 bytes from 192.168.10.18: icmp_seq=4 ttl=63 time=10.1 ms
64 bytes from 192.168.10.18: icmp_seq=5 ttl=63 time=34.0 ms
64 bytes from 192.168.10.18: icmp_seq=6 ttl=63 time=23.6 ms
64 bytes from 192.168.10.18: icmp_seq=7 ttl=63 time=41.3 ms
64 bytes from 192.168.10.18: icmp_seq=8 ttl=63 time=25.2 ms
64 bytes from 192.168.10.18: icmp_seq=9 ttl=63 time=38.1 ms
64 bytes from 192.168.10.18: icmp_seq=10 ttl=63 time=22.1 ms
64 bytes from 192.168.10.18: icmp_seq=11 ttl=63 time=76.6 ms
^C
--- 192.168.10.18 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10017ms
rtt min/avg/max/mdev = 7.199/28.994/76.588/18.835 ms

┌──(root㉿kali)-[~/Desktop]
└─# ping 192.168.10.18
PING 192.168.10.18 (192.168.10.18) 56(84) bytes of data.
^C
--- 192.168.10.18 ping statistics ---
26 packets transmitted, 0 received, 100% packet loss, time 25583ms
```

Verifying firewall rule - enabled

0 pings = firewall rule works

										Queue	Schedule	Description	Actions
												Block bogon networks	
			Not assigned by IANA										
☐	✗	0/0 B	IPv4 ICMP any	192.168.217.3	*	192.168.10.18	*	*	none			Block ICMP from Kali to Ubuntu	
☐	✓	8/270 KiB	IPv4+6 *	WAN subnets	*	*	*	*	none				



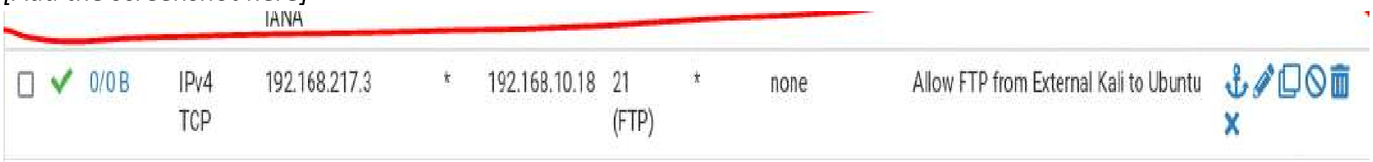
```
✗  Feb 26 22:19:04  WAN  Default deny rule IPv4 (1000000103)  192.168.217.3:60440                 192.168.217.2:53     TCP:A
✗  Feb 26 22:19:04  WAN  Default deny rule IPv4 (1000000103)  192.168.217.3:60442                 192.168.217.2:42558  TCP:A
✗  Feb 26 22:19:04  WAN  Default deny rule IPv4 (1000000103)  192.168.217.3:60440                 192.168.217.2:53     TCP:A
✗  Feb 26 22:19:04  WAN  Default deny rule IPv4 (1000000103)  192.168.217.3:60442                 192.168.217.2:42558  TCP:A
✗  Feb 26 22:19:04  WAN  Default deny rule IPv4 (1000000103)  192.168.217.3:60440                 192.168.217.2:53     TCP:A
✗  Feb 6 02:57:11   WAN  Default deny rule IPv4 (1000000103)  192.168.217.3:43200                 192.168.10.18:21     TCP:RA
✗  Feb 6 01:45:07   WAN  Default deny rule IPv4 (1000000103)  192.168.217.3:54480                 192.168.10.18:21     TCP:RA
✗  Feb 5 23:22:23   WAN  Default deny rule IPv6 (1000000105)  [fe80::cf01:6444:5b9f:6e54]:59126   [ff02::c]:3702       UDP
✗  Feb 5 20:49:48   WAN  Default deny rule IPv6 (1000000105)  [fe80::cf01:6444:5b9f:6e54]:50543   [ff02::c]:3702       UDP
✗  Feb 27 17:13:12  WAN  Default deny rule IPv4 (1000000103)  192.168.217.3:57026                 192.168.217.2:53     UDP
✗  Feb 27 17:13:12  WAN  Default deny rule IPv4 (1000000103)  192.168.217.3:57026                 192.168.217.2:53     UDP
✗  Feb 26 22:09:58  WAN  Default deny rule IPv6 (1000000105)  [fe80::cf01:6444:5b9f:6e54]:44074   [ff02::c]:3702       UDP
✗  Aug 27 14:43:50  WAN  Default deny rule IPv6 (1000000105)  [fe80::cf01:6444:5b9f:6e54]:4[illegible]  [ff02::c]:3702  UDP
✗  Jan 30 20:32:50  LAN  Default deny rule IPv6 (1000000105)  [fe80::7ae3:4419:3977:c166]          [ff02::16]           Options
✗  Jan 30 20:32:49  LAN  Default deny rule IPv6 (1000000105)  [fe80::7ae3:4419:3977:c166]          [ff02::16]           Options
✗  Jan 30 20:32:49  LAN  Default deny rule IPv6 (1000000105)  [fe80::7ae3:4419:3977:c166]          [ff02::16]           Options
✗  Feb 7 10:22:35   LAN  Default deny rule IPv6 (1000000105)  [fe80::cf01:6444:5b9f:6e54]          [ff02::16]           Options
```

Blocked Pings

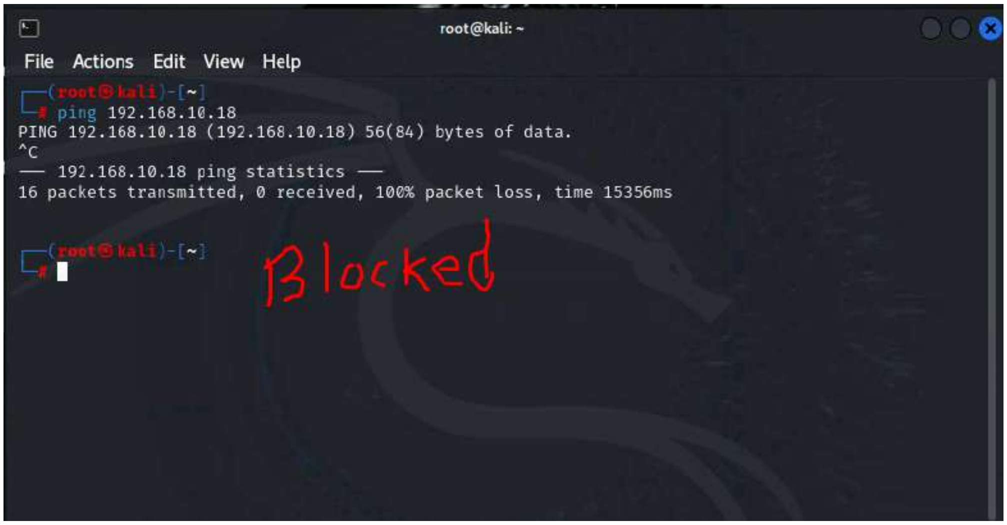
2. Clear the previous firewall policies and configure the pfSense firewall to block all ICMP traffic from External Kali to the LAN side.

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

[Add the screenshot here]



□ ✓	0/0 B	IPv4 TCP	192.168.217.3	*	192.168.10.18	21 (FTP)	*	none	Allow FTP from External Kali to Ubuntu



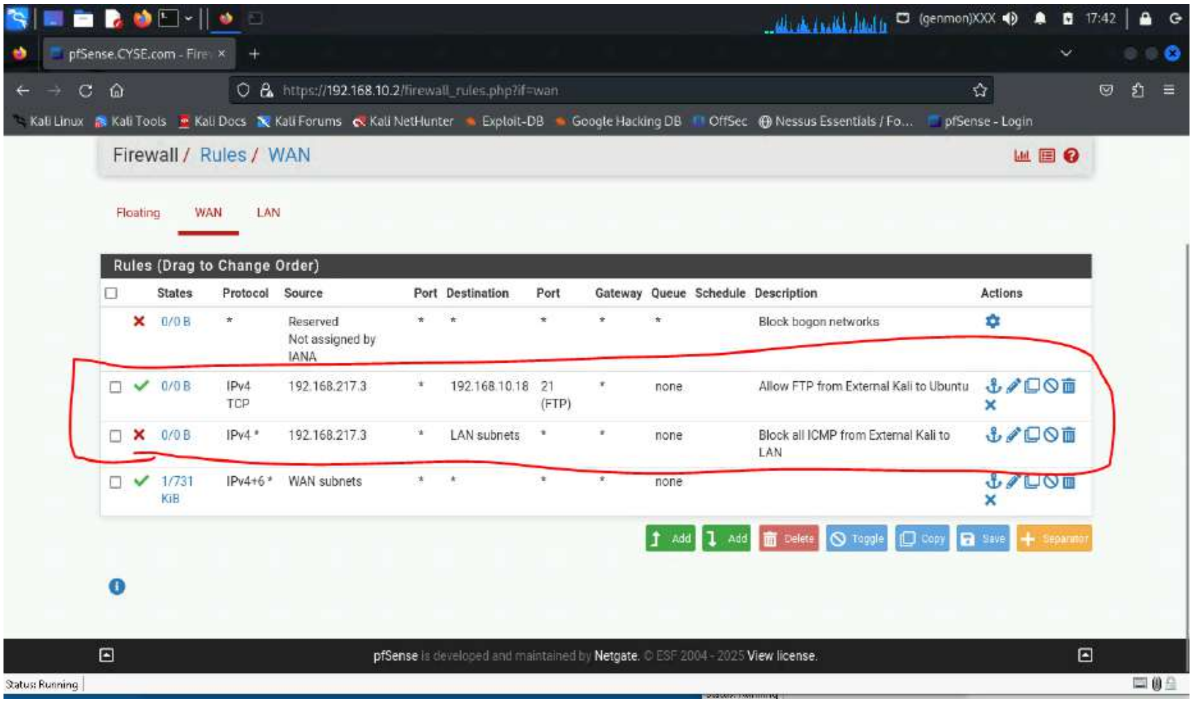
```
┌──(root㉿kali)-[~]
└─# ping 192.168.10.18
PING 192.168.10.18 (192.168.10.18) 56(84) bytes of data.
^C
── 192.168.10.18 ping statistics ──
16 packets transmitted, 0 received, 100% packet loss, time 15356ms

┌──(root㉿kali)-[~]
└─# 
```

Blocked

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	Block	192.168.217.3	LAN subnets	Any
3	WAN	Allow	192.168.217.3	192.168.10.18	FTP (21)

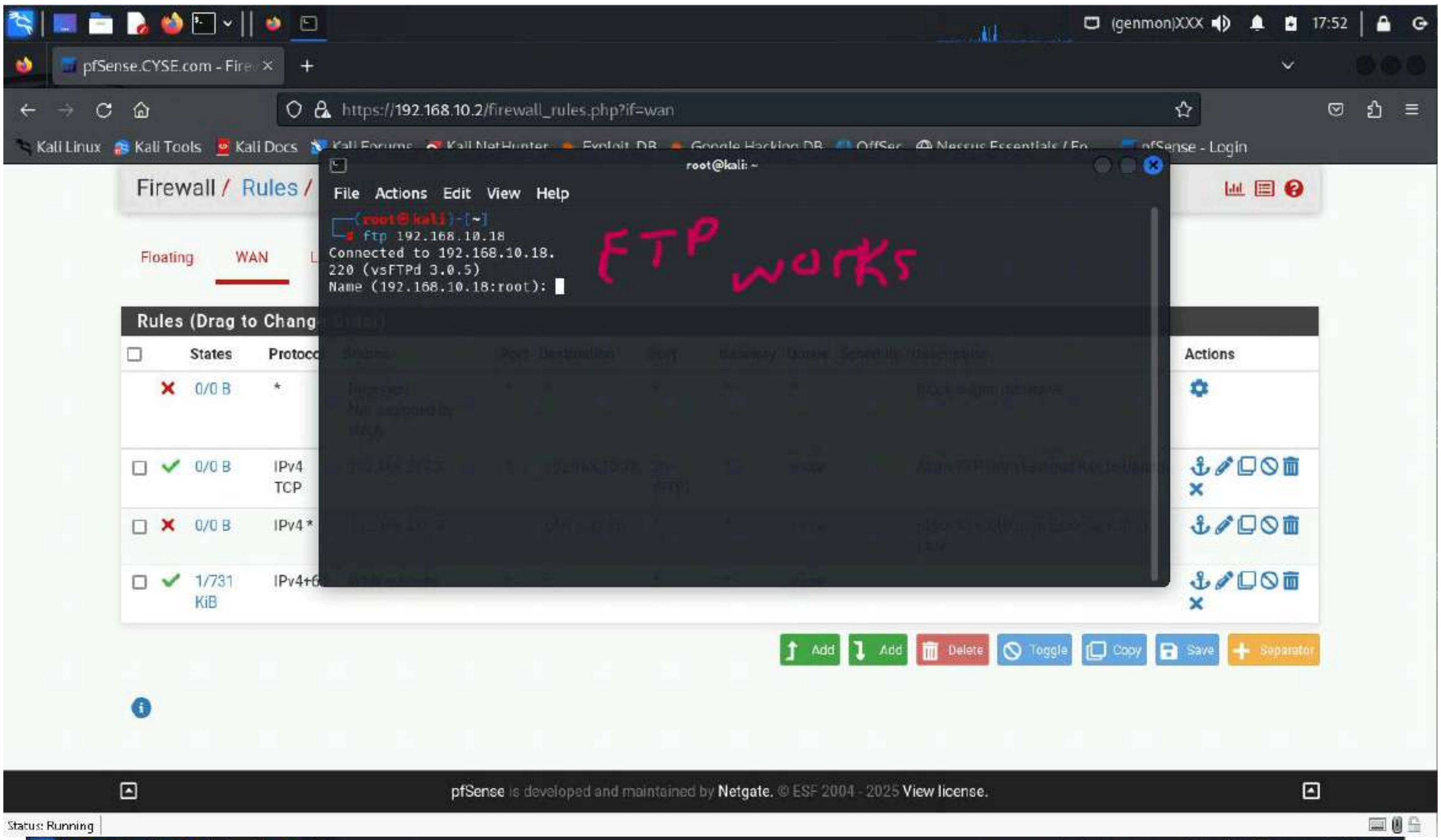
[Add the screenshot here]



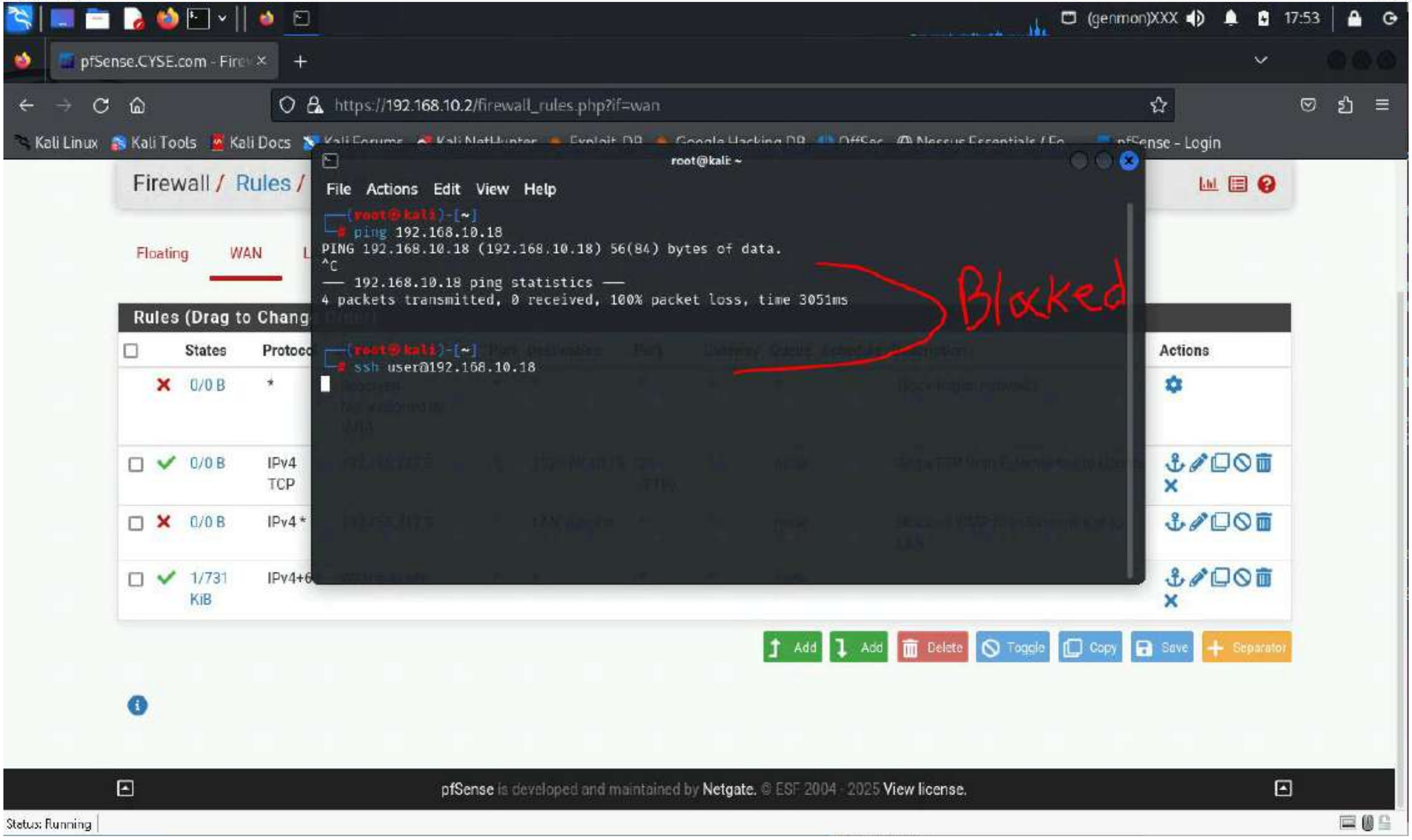
Firewall / Rules / WAN

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 TCP	192.168.217.3	*	192.168.10.18	21 (FTP)	*	none		Allow FTP from External Kali to Ubuntu
☐	✗	0/0 B	IPv4 *	192.168.217.3	*	LAN subnets	*	*	none		Block all ICMP from External Kali to LAN
☐	✓	1/731 KiB	IPv4+6 *	WAN subnets	*	*	*	*	none		


https://192.168.10.2/firewall_rules.php?if=wan
pfSense.CYSE.com - Fire
Firewall / Rules /
Floating
WAN
Rules (Drag to Change Order)
States
Protocol
Actions
root@kali: ~
File Actions Edit View Help
FTP works
Add
Add
Delete
Toggle
Copy
Save
Separator
pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.
Status: Running

```
┌──(root㉿kali)-[~]
└─# ftp 192.168.10.18
Connected to 192.168.10.18.
220 (vsFTPd 3.0.5)
Name (192.168.10.18:root):
```


https://192.168.10.2/firewall_rules.php?if=wan
pfSense.CYSE.com - Fire
Firewall / Rules /
Floating
WAN
Rules (Drag to Change Order)
States
Protocol
Actions
root@kali: ~
File Actions Edit View Help
Blocked
Add
Add
Delete
Toggle
Copy
Save
Separator
pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.
Status: Running

```
┌──(root㉿kali)-[~]
└─# ping 192.168.10.18
PING 192.168.10.18 (192.168.10.18) 56(84) bytes of data.
^C
--- 192.168.10.18 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3051ms

┌──(root㉿kali)-[~]
└─# ssh user@192.168.10.18
```

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

   Originally in Task A.1., there were no restrictions set in the firewall rules other than blocking ICMP traffic. The difference now is that ALL traffic is blocked except FTP from Kali to LAN. The only one that works now is FTP and if you test pings of SSH for example, it will be blocked and not work.

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