CYSE 301: Cybersecurity Technique and Operations

Assignment 3: Sword vs. Shield

Rahil Patel

01208235

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.

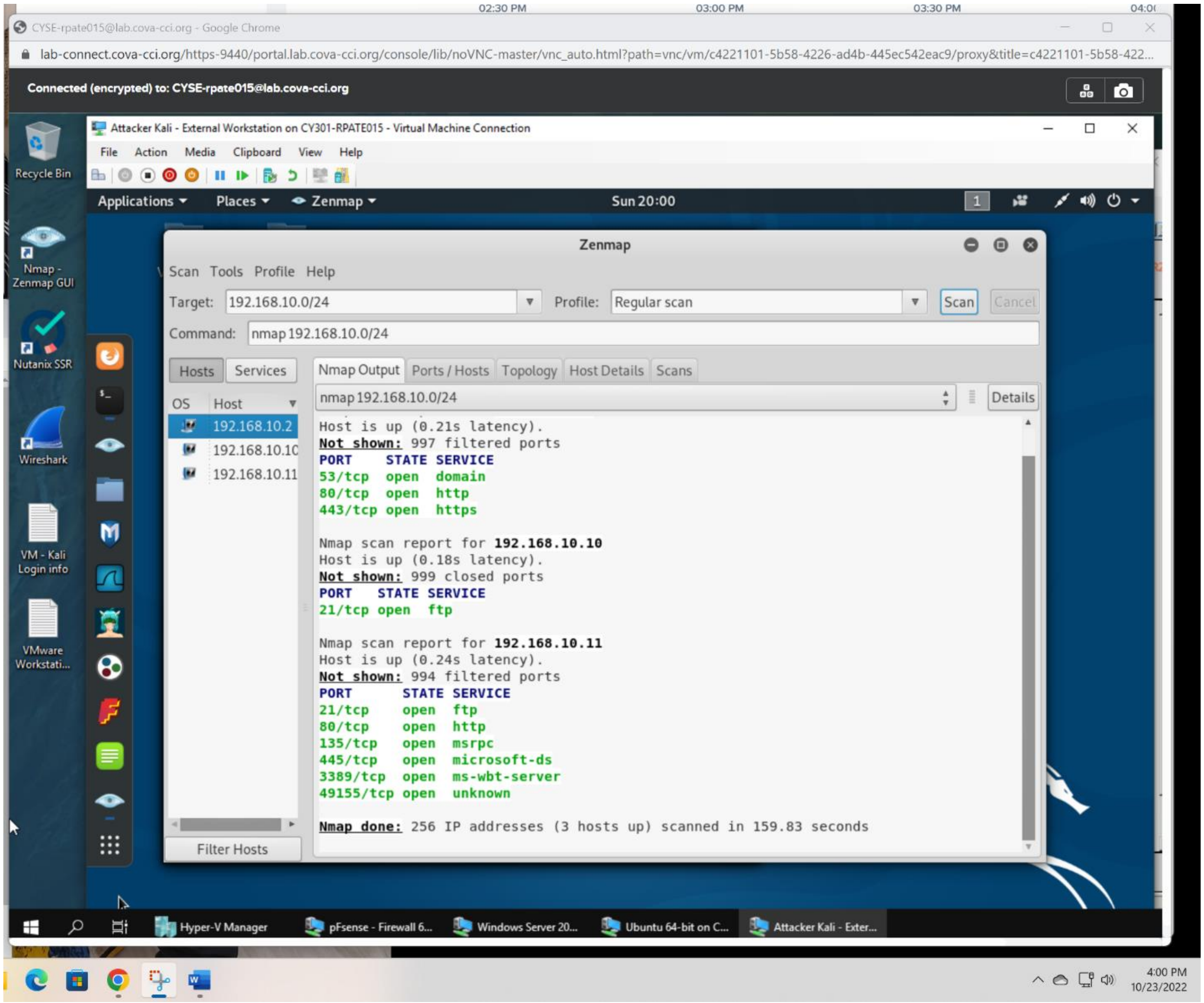
Task A: Sword - Network Scanning (10 + 10 + 20 = 40 points)

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. Run a simple scan to obtain the basic information about the **subnet** topology (including open ports information, operation systems, etc.)



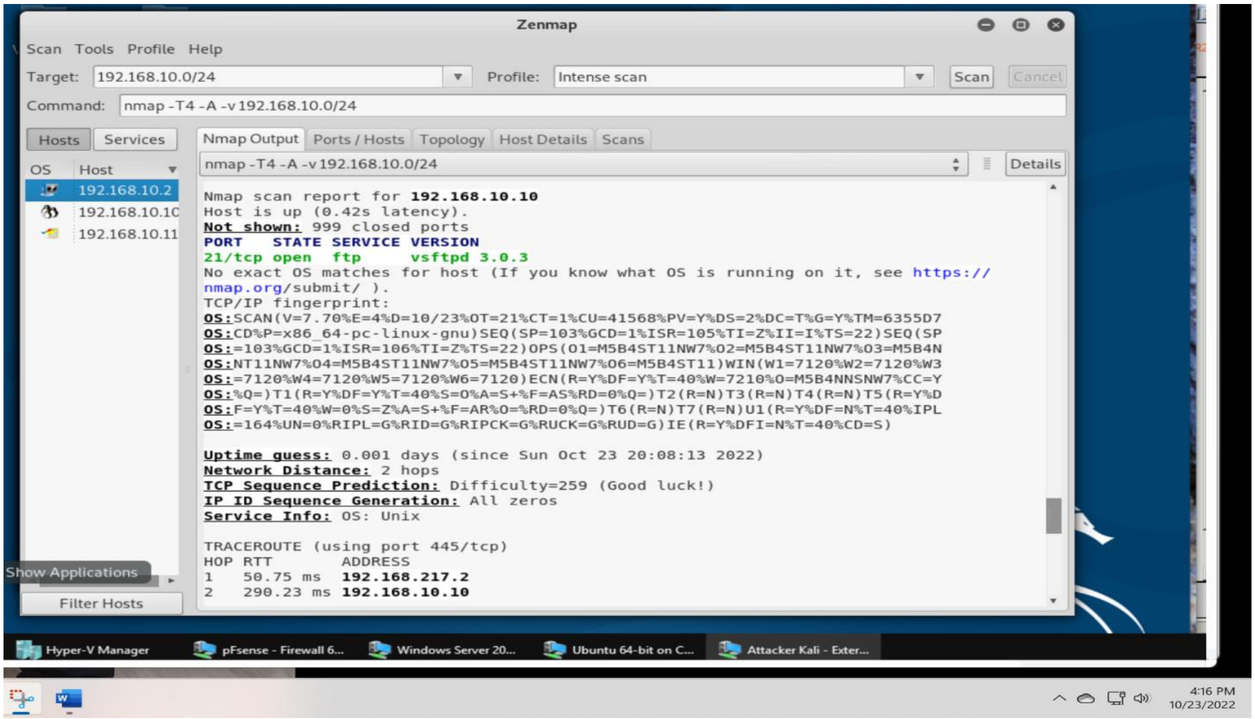
Target: 192.168.10.0/24 Profile: Regular scan

Command: nmap 192.168.10.0/24

Hosts: 192.168.10.2, 192.168.10.10, 192.168.10.11

```
nmap 192.168.10.0/24
Host is up (0.21s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https

Nmap scan report for 192.168.10.10
Host is up (0.18s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
21/tcp open  ftp

Nmap scan report for 192.168.10.11
Host is up (0.24s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
49155/tcp open  unknown

Nmap done: 256 IP addresses (3 hosts up) scanned in 159.83 seconds
```

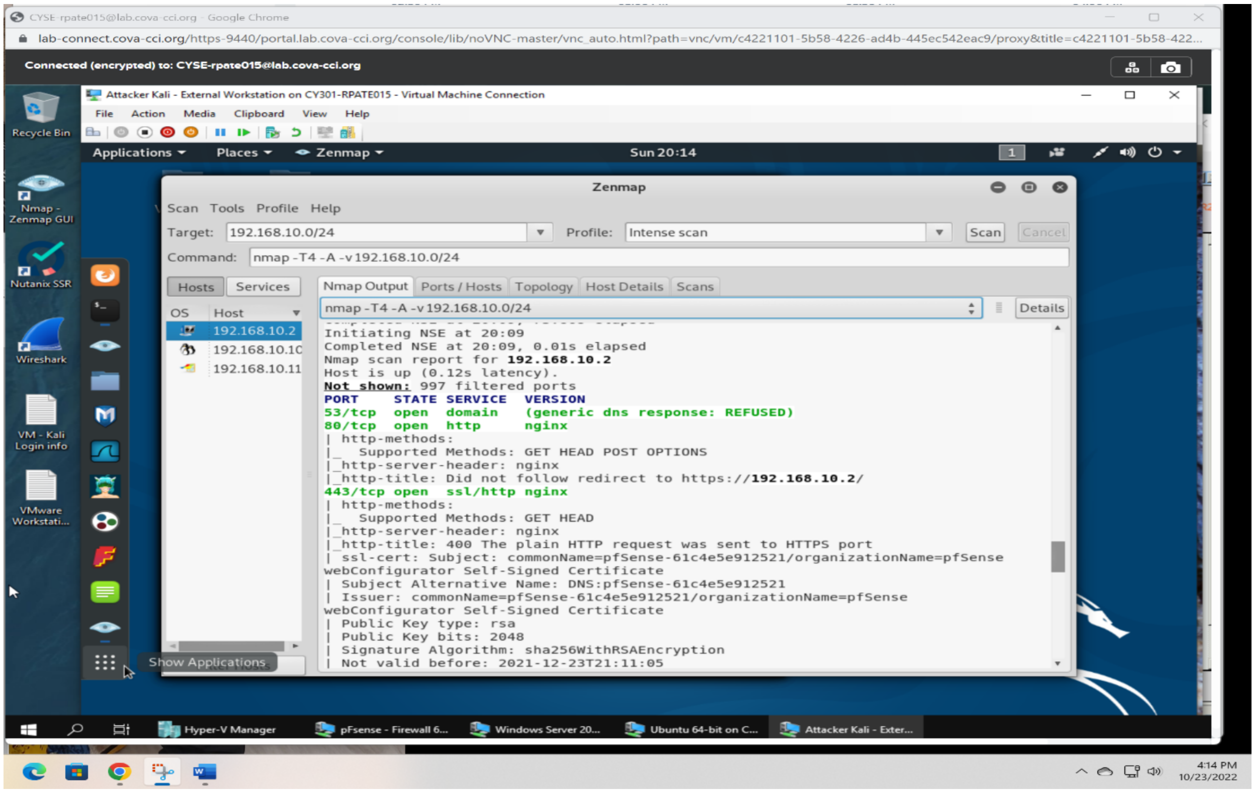
2. Run an intensive scan to obtain detailed information about the **subnet** topology. Get the **service** and **backend software** information associated with each opening port in each VM.



Target: 192.168.10.0/24 Profile: Intense scan

Command: nmap -T4 -A -v 192.168.10.0/24

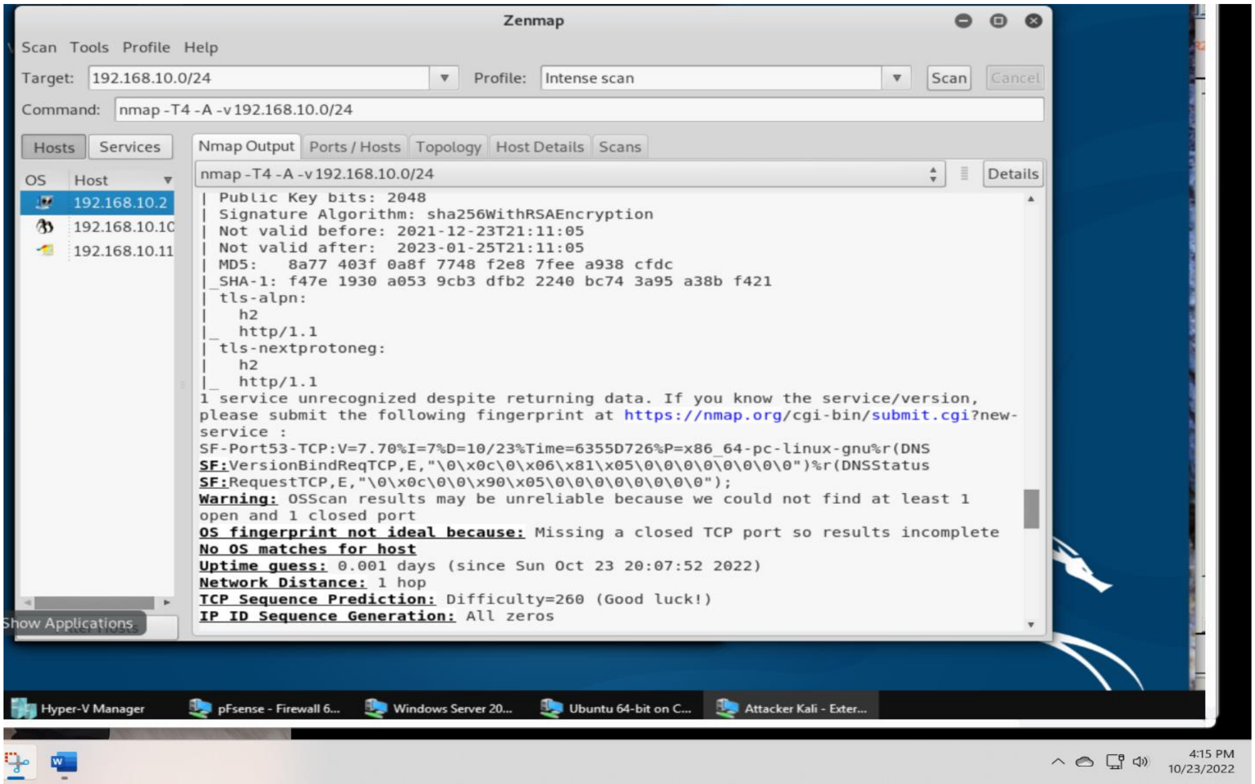
```
Nmap scan report for 192.168.10.10
Host is up (0.42s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
No exact OS matches for host (If you know what OS is running on it, see https://
nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.70%E=4%D=10/23%OT=21%CT=1%CU=41568%PV=Y%DS=2%DC=T%G=Y%TM=6355D7
OS:CD%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=105%TI=Z%II=I%TS=22)SEQ(SP
OS:=103%GCD=1%ISR=106%TI=Z%TS=22)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4N
OS:NT11NW7%O4=M5B4ST11NW7%O5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=7120%W2=7120%W3
OS:=7120%W4=7120%W5=7120%W6=7120)ECN(R=Y%DF=Y%T=40%W=7210%O=M5B4NNSNW7%CC=Y
OS:%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%D
OS:F=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL
OS:=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Uptime guess: 0.001 days (since Sun Oct 23 20:08:13 2022)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Unix

TRACEROUTE (using port 445/tcp)
HOP RTT       ADDRESS
1   50.75 ms  192.168.217.2
2   290.23 ms 192.168.10.10
```



Target: 192.168.10.0/24 Profile: Intense scan

Command: nmap -T4 -A -v 192.168.10.0/24

```
Initiating NSE at 20:09
Completed NSE at 20:09, 0.01s elapsed
Nmap scan report for 192.168.10.2
Host is up (0.12s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE  VERSION
53/tcp   open  domain   (generic dns response: REFUSED)
80/tcp   open  http     nginx
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: nginx
|_http-title: Did not follow redirect to https://192.168.10.2/
443/tcp open  ssl/http nginx
| http-methods:
|_  Supported Methods: GET HEAD
|_http-server-header: nginx
|_http-title: 400 The plain HTTP request was sent to HTTPS port
| ssl-cert: Subject: commonName=pfSense-61c4e5e912521/organizationName=pfSense
webConfigurator Self-Signed Certificate
| Subject Alternative Name: DNS:pfSense-61c4e5e912521
| Issuer: commonName=pfSense-61c4e5e912521/organizationName=pfSense
webConfigurator Self-Signed Certificate
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-12-23T21:11:05
```

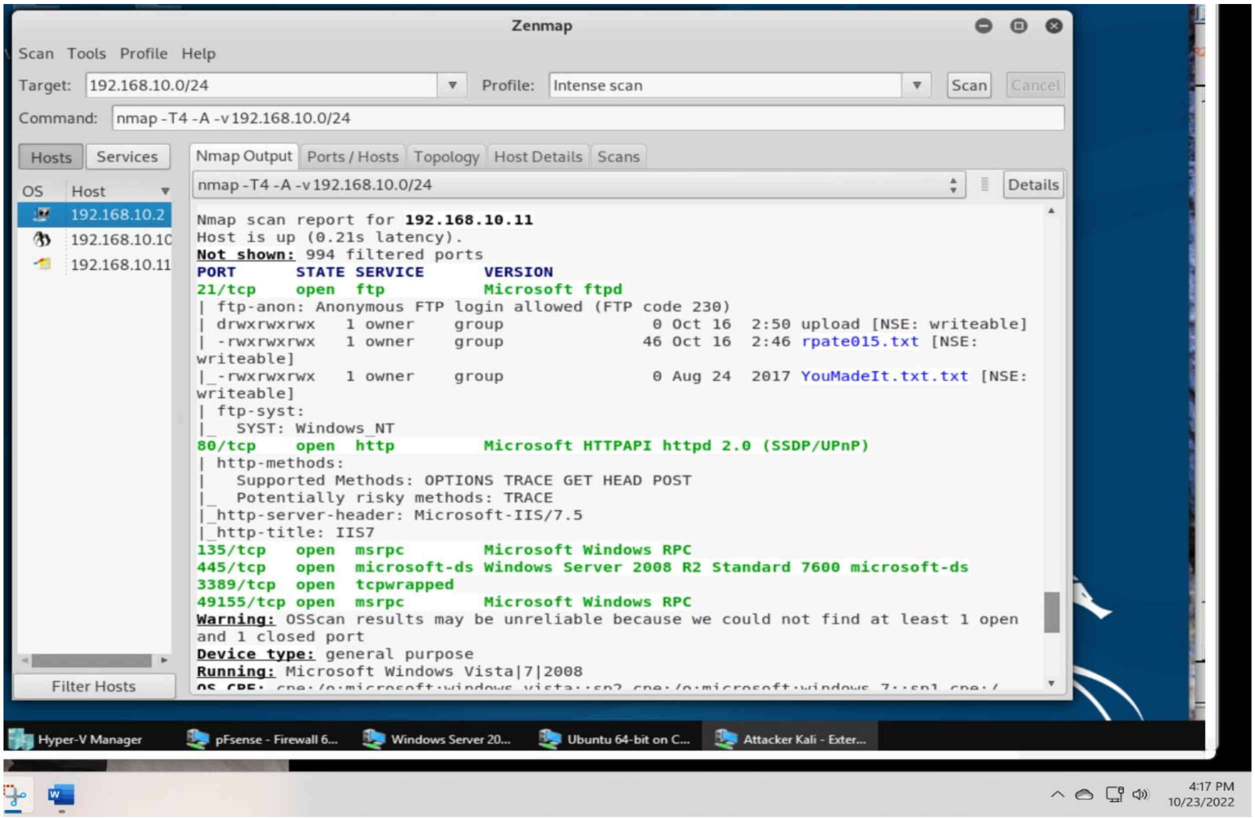


Target: 192.168.10.0/24

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.10.0/24

```
nmap -T4 -A -v 192.168.10.0/24
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-12-23T21:11:05
| Not valid after:  2023-01-25T21:11:05
| MD5:   8a77 403f 0a8f 7748 f2e8 7fee a938 cfdc
|_SHA-1: f47e 1930 a053 9cb3 dfb2 2240 bc74 3a95 a38b f421
| tls-alpn:
|   h2
|_  http/1.1
| tls-nextprotoneg:
|   h2
|_  http/1.1
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=7.70%I=7%D=10/23%Time=6355D726%P=x86_64-pc-linux-gnu%r(DNS
SF:VersionBindReqTCP,E,"\0\x0c\0\x06\x81\x05\0\0\0\0\0\0\0\0")%r(DNSStatus
SF:RequestTCP,E,"\0\x0c\0\0\x90\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 port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Uptime guess: 0.001 days (since Sun Oct 23 20:07:52 2022)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros
```

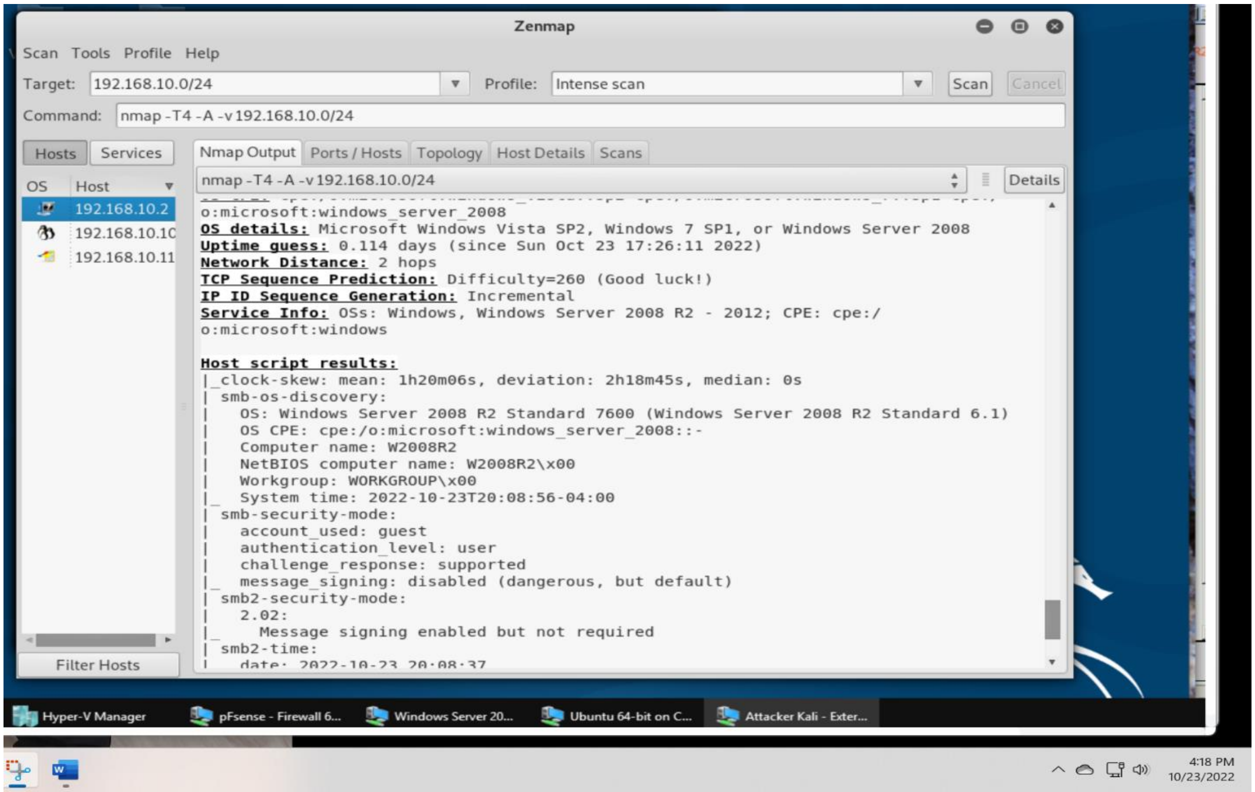


Target: 192.168.10.0/24

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.10.0/24

```
nmap -T4 -A -v 192.168.10.0/24
Nmap scan report for 192.168.10.11
Host is up (0.21s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drwxrwxrwx   1 owner    group              0 Oct 16  2:50 upload [NSE: writeable]
| -rwxrwxrwx   1 owner    group             46 Oct 16  2:46 rpate015.txt [NSE:
writeable]
|_-rwxrwxrwx   1 owner    group              0 Aug 24  2017 YouMadeIt.txt.txt [NSE:
writeable]
| ftp-syst:
|_  SYST: Windows_NT
80/tcp    open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
|_http-title: IIS7
135/tcp   open  msrpc        Microsoft Windows RPC
445/tcp   open  microsoft-ds Windows Server 2008 R2 Standard 7600 microsoft-ds
3389/tcp  open  tcpwrapped
49155/tcp open  msrpc        Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose
Running: Microsoft Windows Vista|7|2008
OS CPE: cpe:/o:microsoft:windows_vista::sp2 cpe:/o:microsoft:windows_7::sp1 cpe:/
```

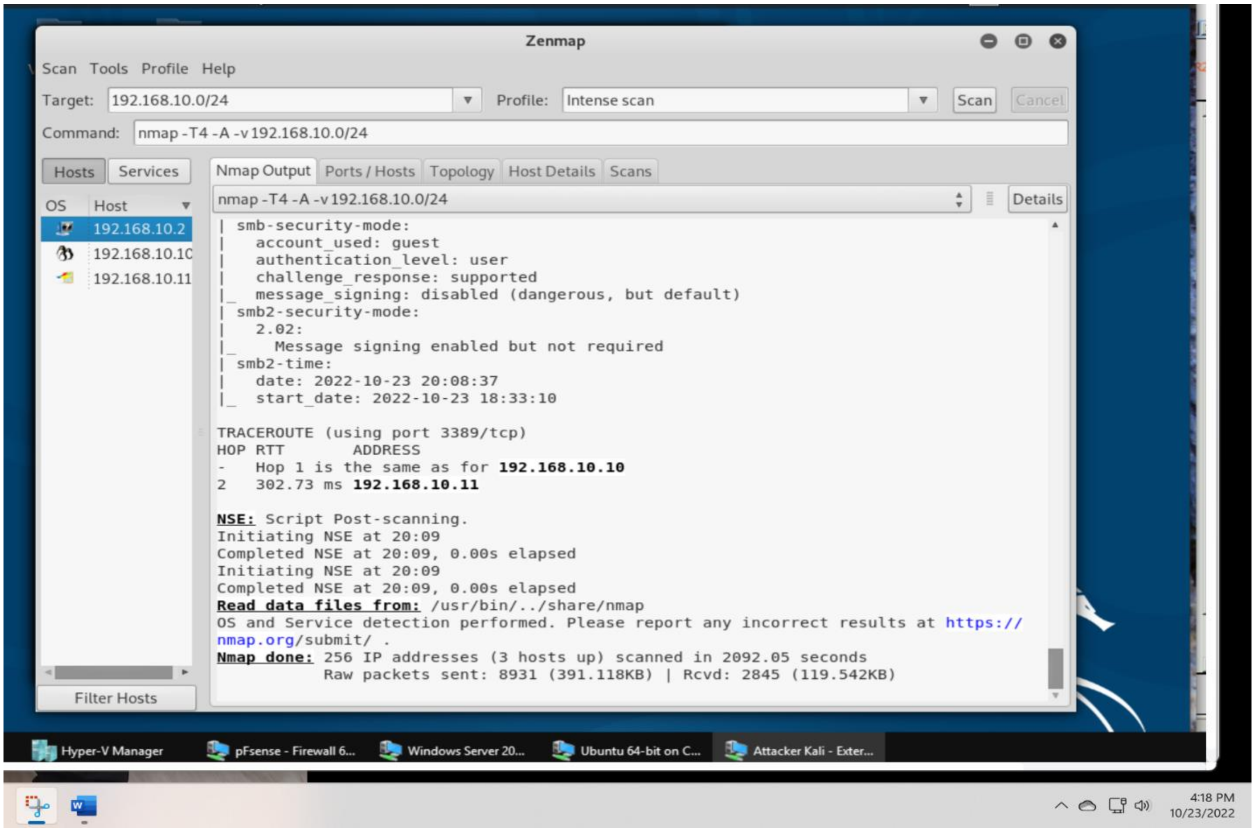


Target: 192.168.10.0/24

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.10.0/24

```
o:microsoft:windows_server_2008
OS details: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Uptime guess: 0.114 days (since Sun Oct 23 17:26:11 2022)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/
o:microsoft:windows

Host script results:
|_clock-skew: mean: 1h20m06s, deviation: 2h18m45s, median: 0s
| smb-os-discovery:
|   OS: Windows Server 2008 R2 Standard 7600 (Windows Server 2008 R2 Standard 6.1)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::-
|   Computer name: W2008R2
|   NetBIOS computer name: W2008R2\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2022-10-23T20:08:56-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2022-10-23 20:08:37
```



Target: 192.168.10.0/24

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.10.0/24

```
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2022-10-23 20:08:37
|_  start_date: 2022-10-23 18:33:10

TRACEROUTE (using port 3389/tcp)
HOP RTT       ADDRESS
-   Hop 1 is the same as for 192.168.10.10
2   302.73 ms 192.168.10.11

NSE: Script Post-scanning.
Initiating NSE at 20:09
Completed NSE at 20:09, 0.00s elapsed
Initiating NSE at 20:09
Completed NSE at 20:09, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://
nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 2092.05 seconds
           Raw packets sent: 8931 (391.118KB) | Rcvd: 2845 (119.542KB)
```

3. 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. **

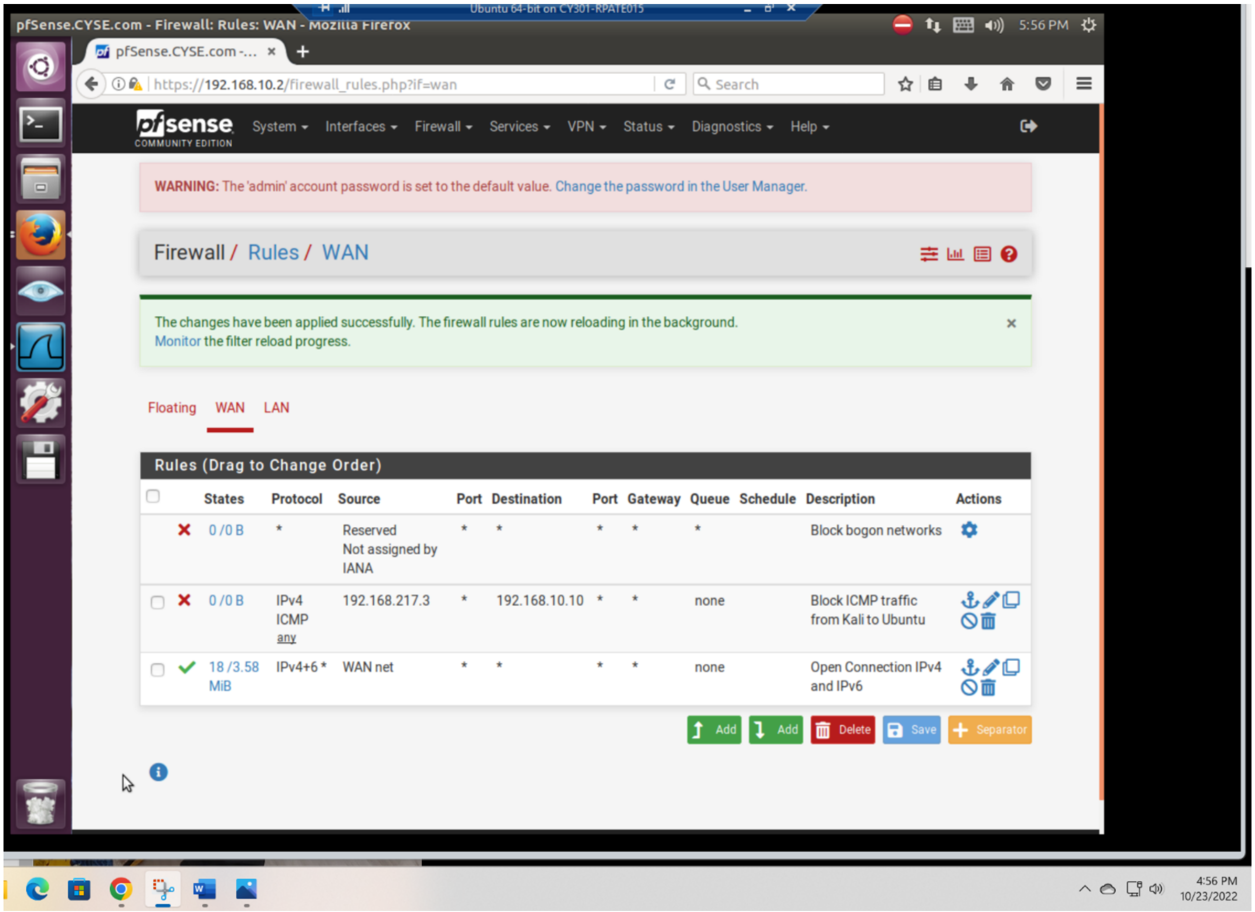
   I have used zenmap to perform both task. I have performed the regular scan on 192.168.10.0/24. It covers all the subnet that are on the network. There were 256 hosts were scanned during the regular scan. Only three hosts were up during the scanning progress. The up hosts are identified as the Ubuntu, Server 2008, and the pf sense. In the regular scan the detail are provided of the open TCP ports of the networks. The details are classified with the port number and the name if the services that are using the ports. On the windows server 2008, there is an unknown open port, and the port number is 49155. It is running on the TCP utilities. The function and services has not been identified, so the vulnerability is extreme on the network.
   The intense scan of the network shows all the details of the version, operating system, and the connection reports of the network. The fingerprint image can be identified of a system by using the intense scan. It is very powerful tool. It also list the files that are on the network. The traffic pattern is similar to the regular scan. It shows the report for the performed scans on the network with the inclusion of verification and acknowledgement. It does check the identity of the different networks.

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 policy, 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	BLOC K	192.168.217.3	192.168.10.10	ICMP



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

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

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

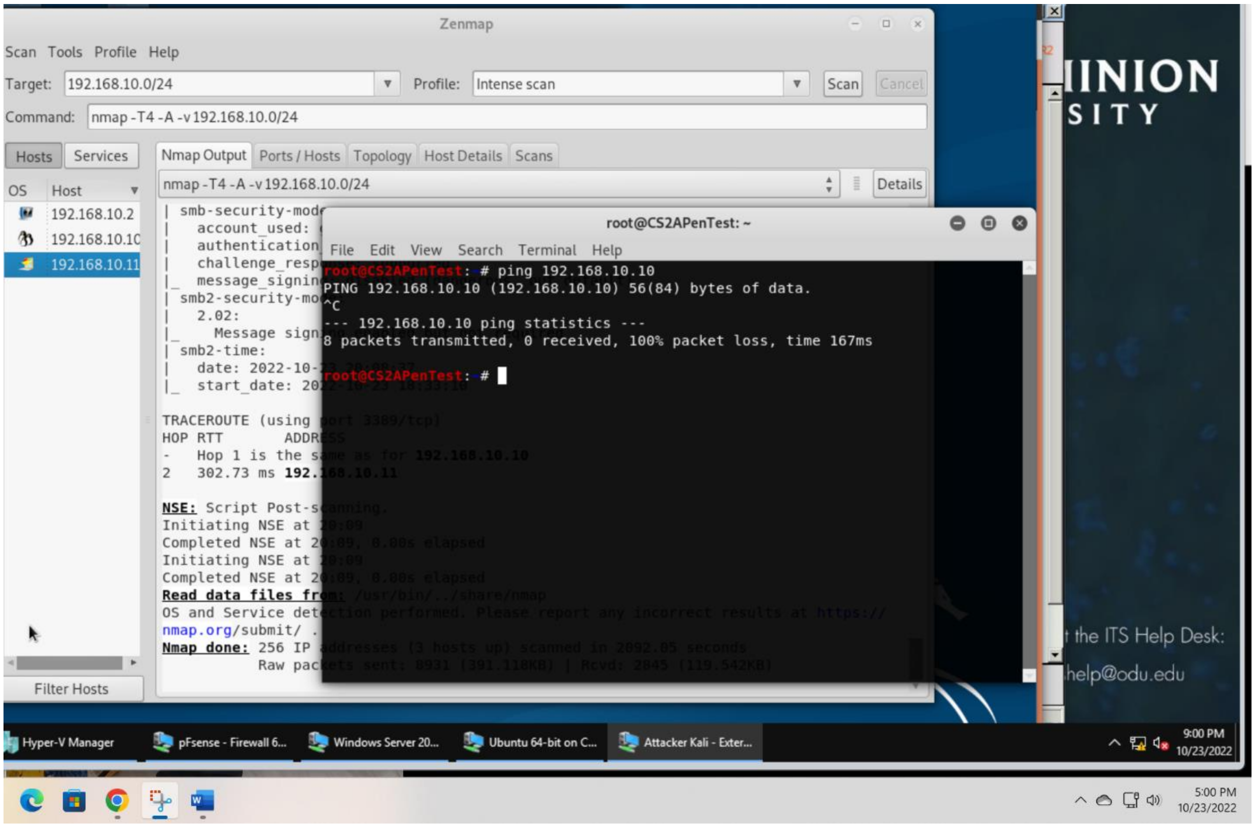
Firewall / Rules / WAN

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)

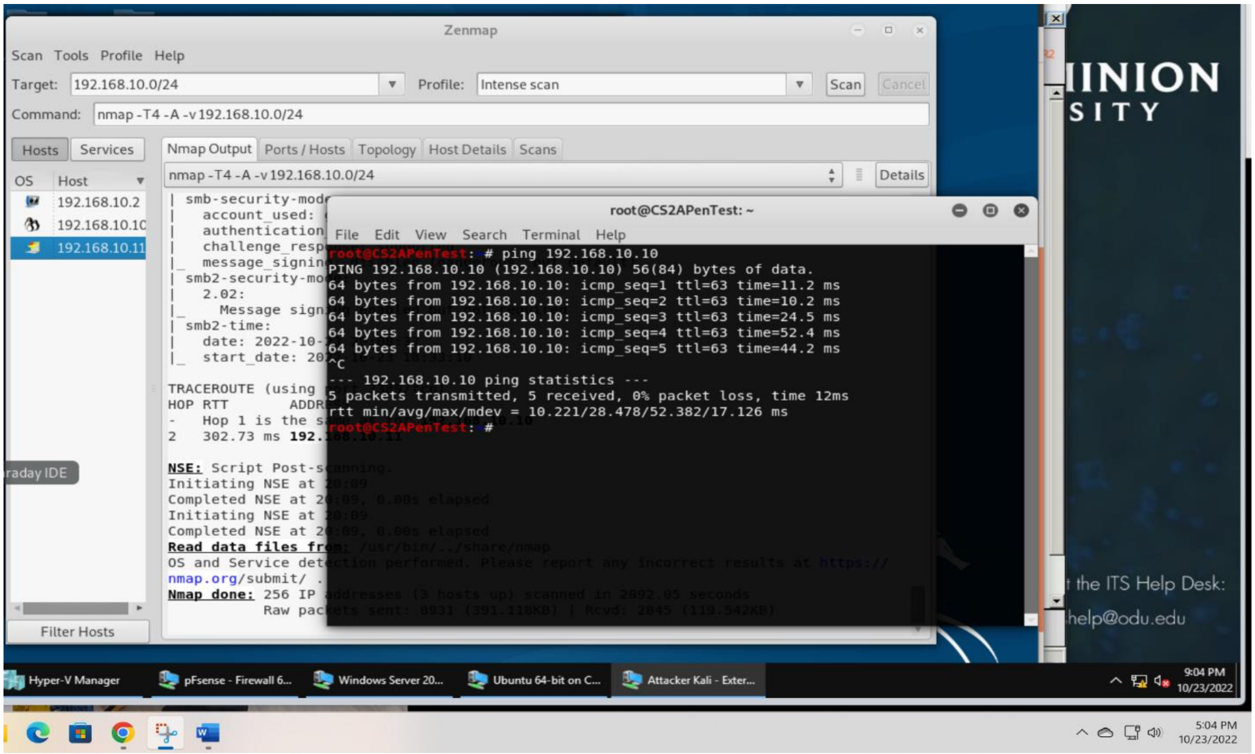
		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
	✗	0 / 0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks
□	✗	0 / 0 B	IPv4 ICMP any	192.168.217.3	*	192.168.10.10	*	*	none		Block ICMP traffic from Kali to Ubuntu
□	✓	18 / 3.58 MiB	IPv4+6 *	WAN net	*	*	*	*	none		Open Connection IPv4 and IPv6



```
| smb-security-mode
|   account_used:
|   authentication
|   challenge_resp
|_  message_signin
| smb2-security-mo
|   2.02:
|_    Message sign
| smb2-time:
|   date: 2022-10-
|_  start_date: 20

TRACEROUTE (using
HOP RTT      ADDR
-   Hop 1 is the s
2   302.73 ms 192.

NSE: Script Post-s
Initiating NSE at
Completed NSE at 2
Initiating NSE at
Completed NSE at 2
Read data files fr
OS and Service det
nmap.org/submit/ .
Nmap done: 256 IP
           Raw pac
```

root@CS2APenTest: ~

```
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 ---
8 packets transmitted, 0 received, 100% packet loss, time 167ms

root@CS2APenTest:~# 
```



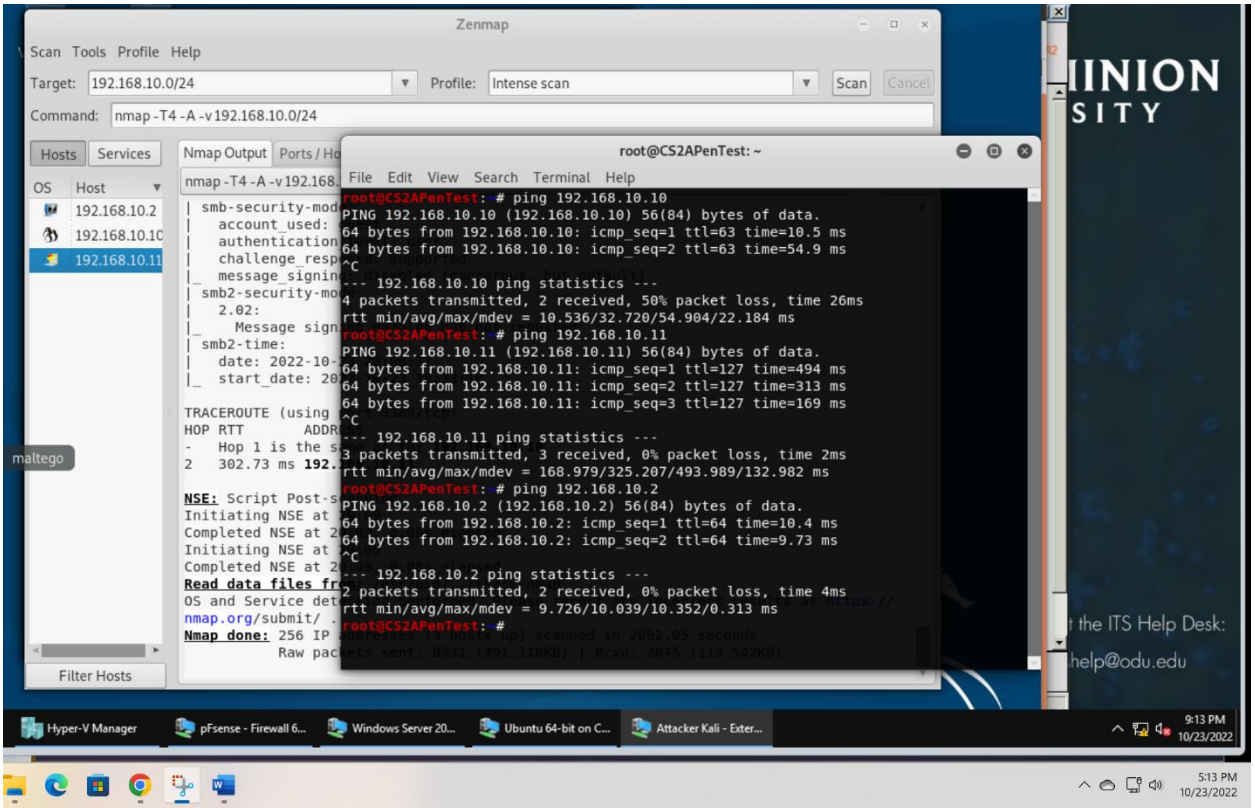
```
| smb-security-mode
|   account_used:
|   authentication
|   challenge_resp
|_  message_signin
| smb2-security-mo
|   2.02:
|_    Message sign
| smb2-time:
|   date: 2022-10-
|_  start_date: 20

TRACEROUTE (using
HOP RTT      ADDR
-   Hop 1 is the s
2   302.73 ms 192.

NSE: Script Post-s
Initiating NSE at
Completed NSE at 2
Initiating NSE at
Completed NSE at 2
Read data files fr
OS and Service det
nmap.org/submit/ .
Nmap done: 256 IP
           Raw pac
```

root@CS2APenTest: ~

```
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=11.2 ms
64 bytes from 192.168.10.10: icmp_seq=2 ttl=63 time=10.2 ms
64 bytes from 192.168.10.10: icmp_seq=3 ttl=63 time=24.5 ms
64 bytes from 192.168.10.10: icmp_seq=4 ttl=63 time=52.4 ms
64 bytes from 192.168.10.10: icmp_seq=5 ttl=63 time=44.2 ms
^C
--- 192.168.10.10 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 12ms
rtt min/avg/max/mdev = 10.221/28.478/52.382/17.126 ms
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.

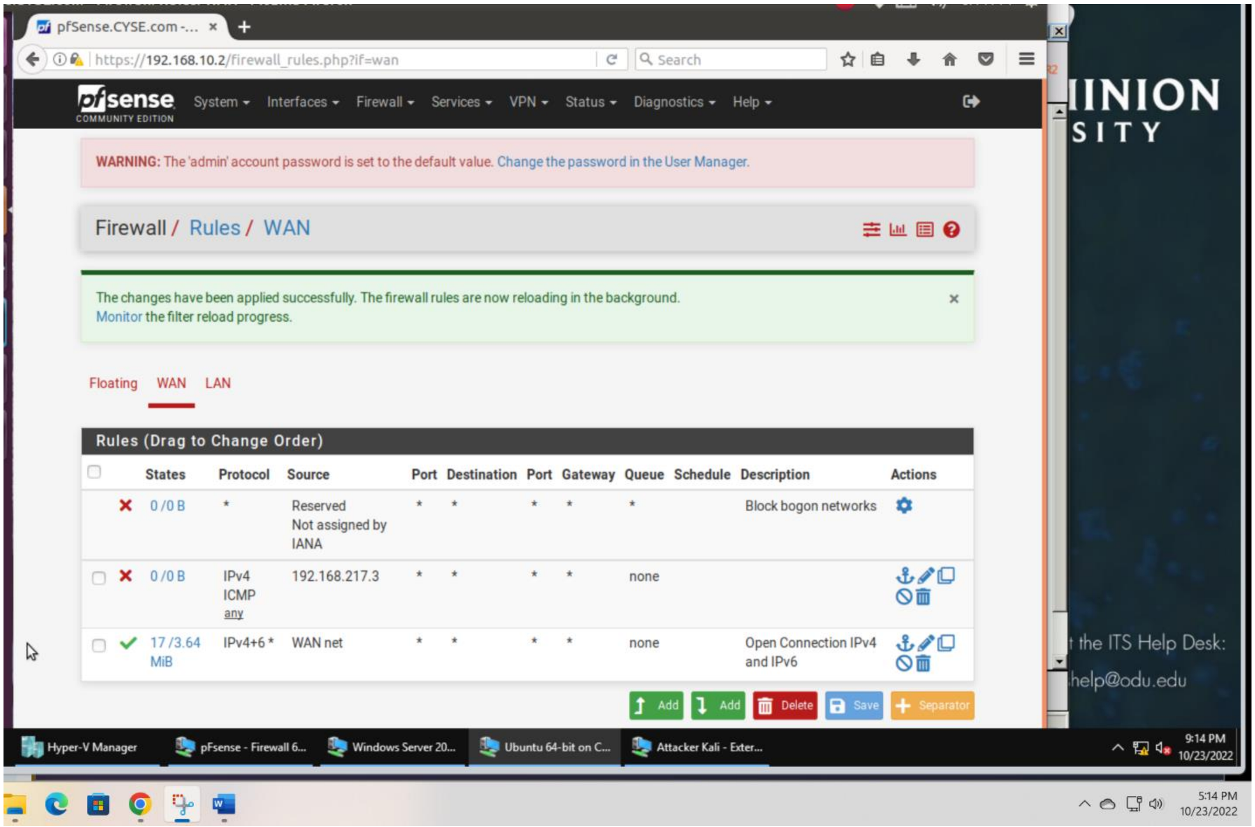
Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
2	WAN	BLOCK	192.168.217.3	ANY	ICMP



Target: 192.168.10.0/24
Profile: Intense scan
Command: nmap -T4 -A -v 192.168.10.0/24

root@CS2APenTest: ~

```
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=10.5 ms
64 bytes from 192.168.10.10: icmp_seq=2 ttl=63 time=54.9 ms
^C
--- 192.168.10.10 ping statistics ---
4 packets transmitted, 2 received, 50% packet loss, time 26ms
rtt min/avg/max/mdev = 10.536/32.720/54.904/22.184 ms
root@CS2APenTest:~# ping 192.168.10.11
PING 192.168.10.11 (192.168.10.11) 56(84) bytes of data.
64 bytes from 192.168.10.11: icmp_seq=1 ttl=127 time=494 ms
64 bytes from 192.168.10.11: icmp_seq=2 ttl=127 time=313 ms
64 bytes from 192.168.10.11: icmp_seq=3 ttl=127 time=169 ms
^C
--- 192.168.10.11 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2ms
rtt min/avg/max/mdev = 168.979/325.207/493.989/132.982 ms
root@CS2APenTest:~# ping 192.168.10.2
PING 192.168.10.2 (192.168.10.2) 56(84) bytes of data.
64 bytes from 192.168.10.2: icmp_seq=1 ttl=64 time=10.4 ms
64 bytes from 192.168.10.2: icmp_seq=2 ttl=64 time=9.73 ms
^C
--- 192.168.10.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 4ms
rtt min/avg/max/mdev = 9.726/10.039/10.352/0.313 ms
root@CS2APenTest:~#
```



pfSense.CYSE.com -...
https://192.168.10.2/firewall_rules.php?if=wan
System Interfaces Firewall Services VPN Status Diagnostics Help

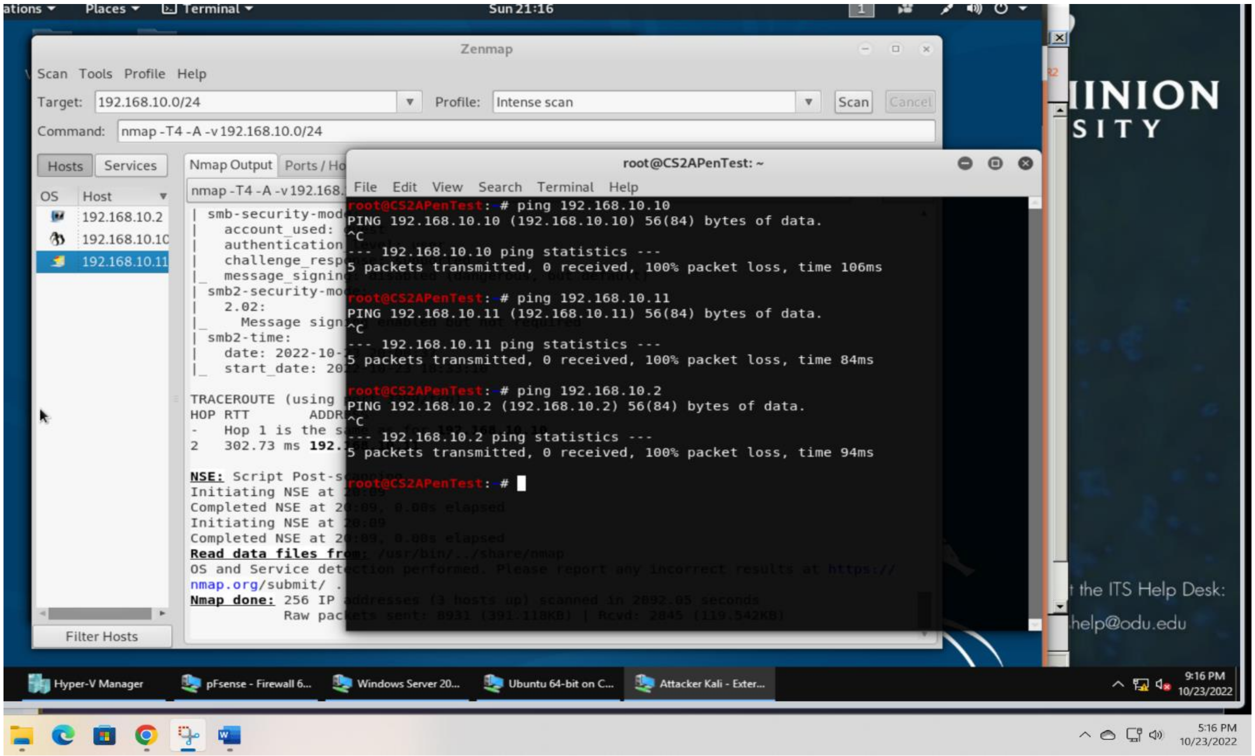
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

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 / 0 B	IPv4 ICMP any	192.168.217.3	*	*	*	*	none			
□ ✓	17 / 3.64 MiB	IPv4+6 *	WAN net	*	*	*	*	none		Open Connection IPv4 and IPv6	



Target: 192.168.10.0/24 Profile: Intense scan

Command: nmap -T4 -A -v 192.168.10.0/24

Hosts:
- 192.168.10.2
- 192.168.10.10
- 192.168.10.11

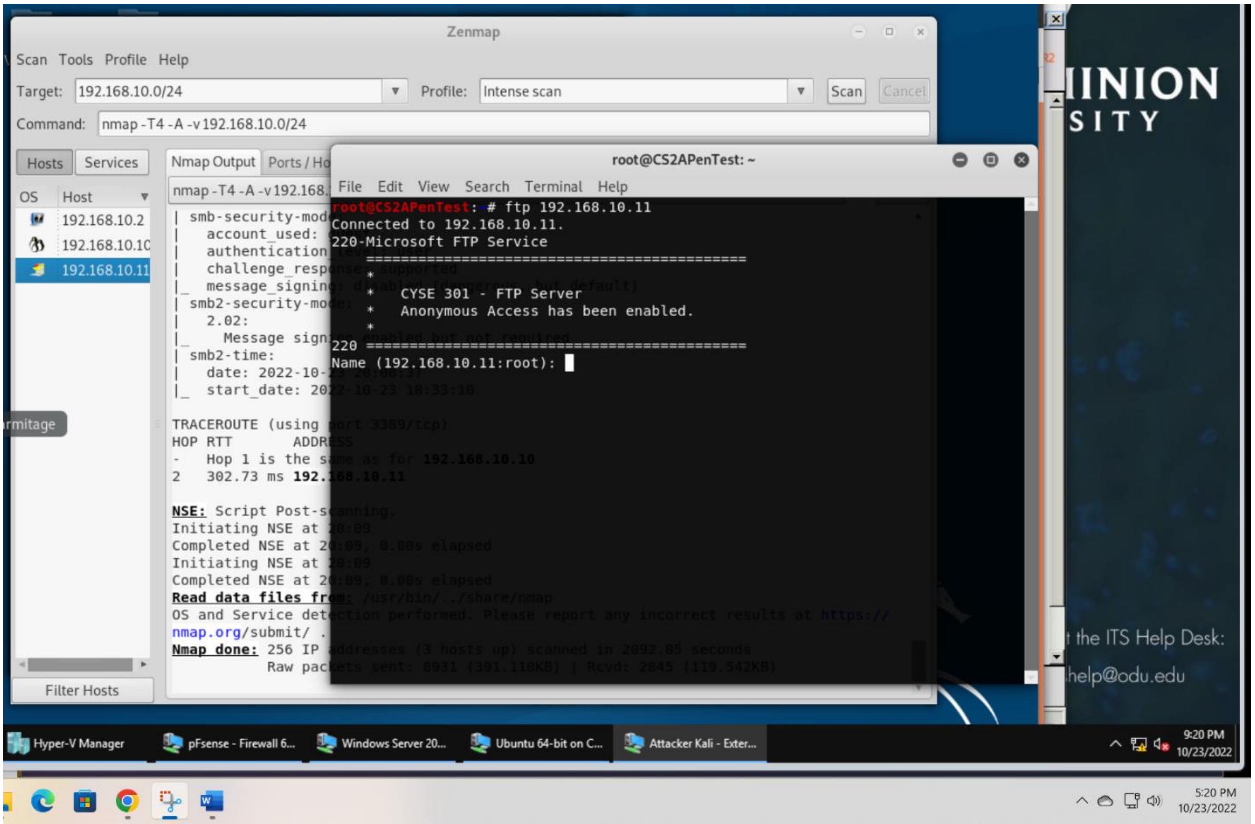
```
nmap -T4 -A -v 192.168.
| smb-security-mod
|   account_used:
|   authentication
|   challenge_resp
|_  message_signin
| smb2-security-mo
|   2.02:
|_    Message sign
| smb2-time:
|   date: 2022-10-
|_  start_date: 20

TRACEROUTE (using
HOP RTT      ADDR
-   Hop 1 is the s
2   302.73 ms 192.

NSE: Script Post-s
Initiating NSE at
Completed NSE at 2
Initiating NSE at
Completed NSE at 2
Read data files fr
OS and Service det
nmap.org/submit/ .
Nmap done: 256 IP
           Raw pac
```

root@CS2APenTest: ~

```
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 ---
5 packets transmitted, 0 received, 100% packet loss, time 106ms

root@CS2APenTest:~# ping 192.168.10.11
PING 192.168.10.11 (192.168.10.11) 56(84) bytes of data.
^C
--- 192.168.10.11 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 84ms

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 ---
5 packets transmitted, 0 received, 100% packet loss, time 94ms

root@CS2APenTest:~# 
```

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	FTP
3	WAN	BLOCK	192.168.217.3	ANY	ANY

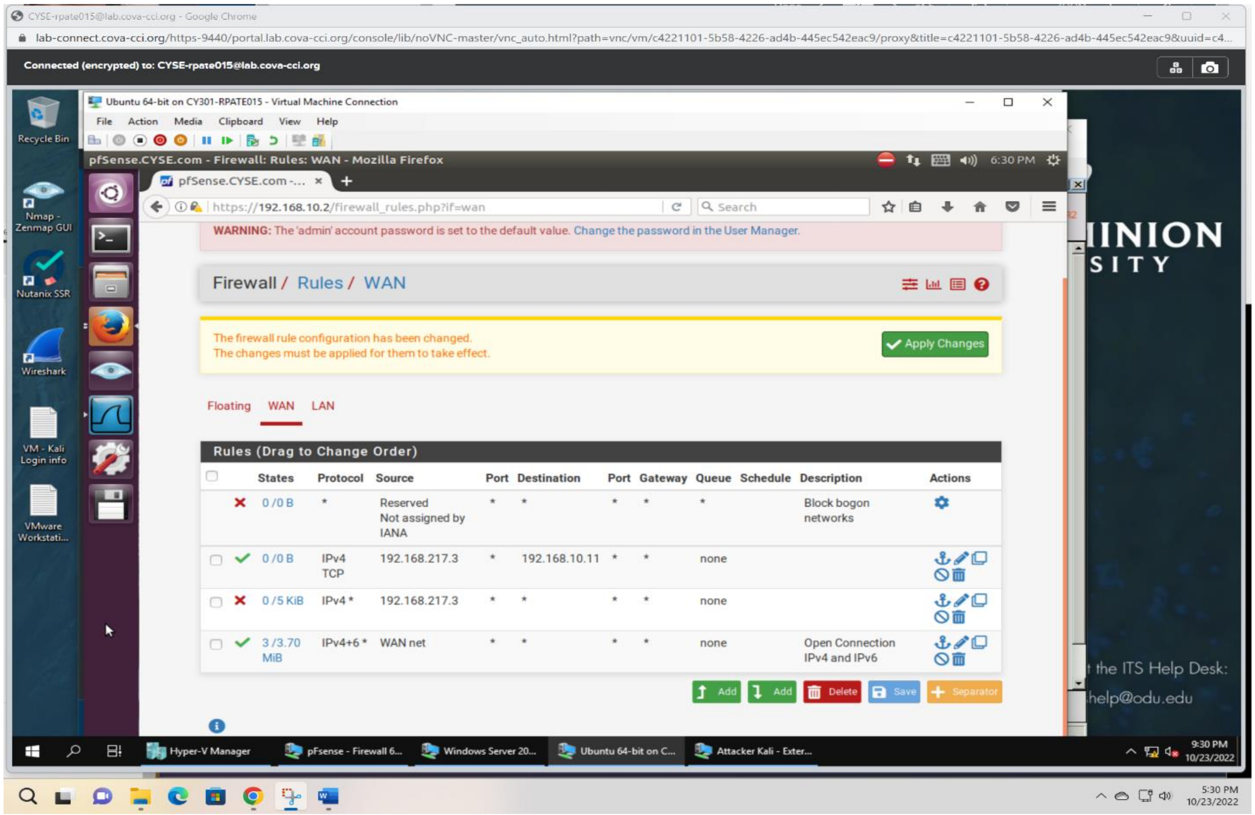


Target: 192.168.10.0/24
Profile: Intense scan
Command: nmap -T4 -A -v 192.168.10.0/24

```
nmap -T4 -A -v 192.168.
| smb-security-mod
|   account_used:
|   authentication
|   challenge_resp
|_  message_signin
| smb2-security-mo
|   2.02:
|_    Message sign
| smb2-time:
|   date: 2022-10-
|_  start_date: 20

TRACEROUTE (using
HOP RTT       ADDR
-   Hop 1 is the s
2   302.73 ms 192.

NSE: Script Post-s
Initiating NSE at
Completed NSE at 2
Initiating NSE at
Completed NSE at 2
Read data files fro
OS and Service det
nmap.org/submit/ .
Nmap done: 256 IP
           Raw pac
```

root@CS2APenTest: ~

```
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): 
```



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

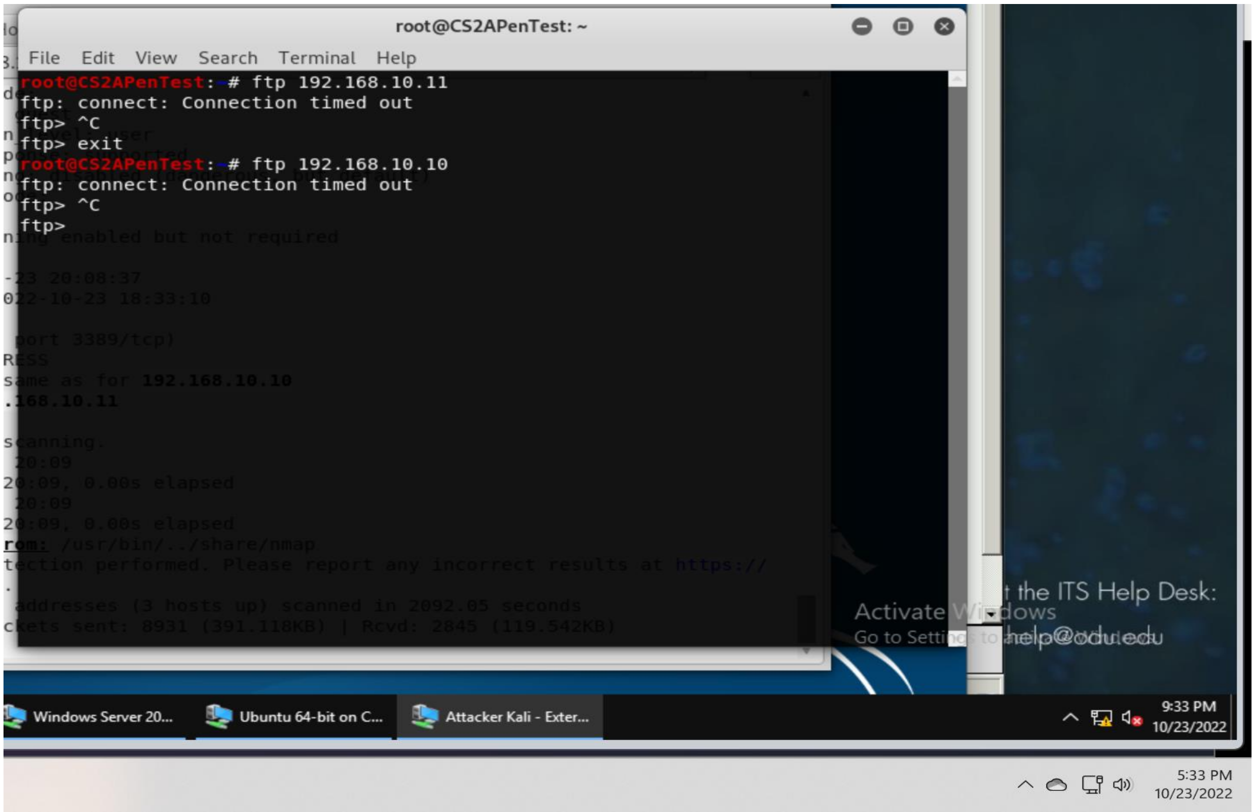
Firewall / Rules / WAN

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 TCP	192.168.217.3	*	192.168.10.11	*	*	none		
□	✗	0 /5 KiB	IPv4 *	192.168.217.3	*	*	*	*	none		
□	✓	3 /3.70 MiB	IPv4+6 *	WAN net	*	*	*	*	none		Open Connection IPv4 and IPv6

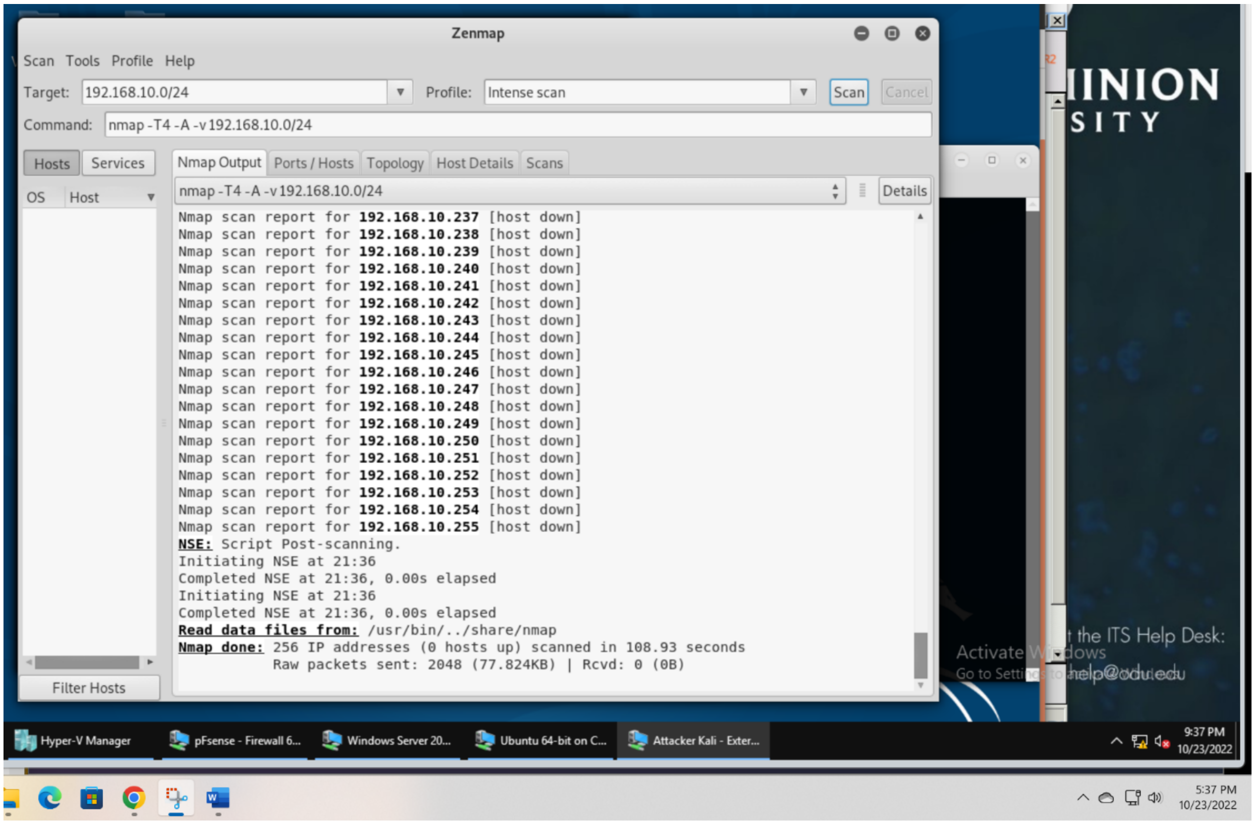
CYSE-rpate015@lab.cova-cci.org - Google Chrome
lab-connect.cova-cci.org/https-9440/portal.lab.cova-cci.org/console/lib/noVNC-master/vnc_auto.html?path=vnc/vm/c4221101-5b58-4226-ad4b-445ec542eac9/proxy&title=c4221101-5b58-4226-ad4b-445ec542eac9&uuid=c4...
Connected (encrypted) to: CYSE-rpate015@lab.cova-cci.org
Ubuntu 64-bit on CY301-RPATE015 - Virtual Machine Connection
File Action Media Clipboard View Help
pfSense.CYSE.com - Firewall: Rules: WAN - Mozilla Firefox
6:30 PM
pfSense.CYSE.com -...
https://192.168.10.2/firewall_rules.php?if=wan
Search
Apply Changes
Floating
WAN
LAN
Actions
Add
Add
Delete
Save
Separator
Recycle Bin
Nmap - Zenmap GUI
Nutanix SSR
Wireshark
VM - Kali Login info
VMware Workstati...
Hyper-V Manager
pFsense - Firewall 6...
Windows Server 20...
Ubuntu 64-bit on C...
Attacker Kali - Exter...
the ITS Help Desk:
help@odu.edu
9:30 PM
10/23/2022
5:30 PM
10/23/2022



```
root@CS2APenTest:~# ftp 192.168.10.11
ftp: connect: Connection timed out
ftp> ^C
ftp> exit
root@CS2APenTest:~# ftp 192.168.10.10
ftp: connect: Connection timed out
ftp> ^C
ftp>
```

root@CS2APenTest: ~
File Edit View Search Terminal Help
Activate Windows
Go to Settings to activate Windows.
the ITS Help Desk:
help@odu.edu
Windows Server 20...
Ubuntu 64-bit on C...
Attacker Kali - Exter...
9:33 PM
10/23/2022
5:33 PM
10/23/2022

4. Keep the firewall policies you created in Task B.3 and repeat Task A.2. What’s the difference?



Target: 192.168.10.0/24
Profile: Intense scan
Command: nmap -T4 -A -v 192.168.10.0/24

nmap -T4 -A -v 192.168.10.0/24

```
Nmap scan report for 192.168.10.237 [host down]
Nmap scan report for 192.168.10.238 [host down]
Nmap scan report for 192.168.10.239 [host down]
Nmap scan report for 192.168.10.240 [host down]
Nmap scan report for 192.168.10.241 [host down]
Nmap scan report for 192.168.10.242 [host down]
Nmap scan report for 192.168.10.243 [host down]
Nmap scan report for 192.168.10.244 [host down]
Nmap scan report for 192.168.10.245 [host down]
Nmap scan report for 192.168.10.246 [host down]
Nmap scan report for 192.168.10.247 [host down]
Nmap scan report for 192.168.10.248 [host down]
Nmap scan report for 192.168.10.249 [host down]
Nmap scan report for 192.168.10.250 [host down]
Nmap scan report for 192.168.10.251 [host down]
Nmap scan report for 192.168.10.252 [host down]
Nmap scan report for 192.168.10.253 [host down]
Nmap scan report for 192.168.10.254 [host down]
Nmap scan report for 192.168.10.255 [host down]
NSE: Script Post-scanning.
Initiating NSE at 21:36
Completed NSE at 21:36, 0.00s elapsed
Initiating NSE at 21:36
Completed NSE at 21:36, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 256 IP addresses (0 hosts up) scanned in 108.93 seconds
           Raw packets sent: 2048 (77.824KB) | Rcvd: 0 (0B)
```

All the traffic is blocked by the firewall policies on the network, so there is no discovery.