OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

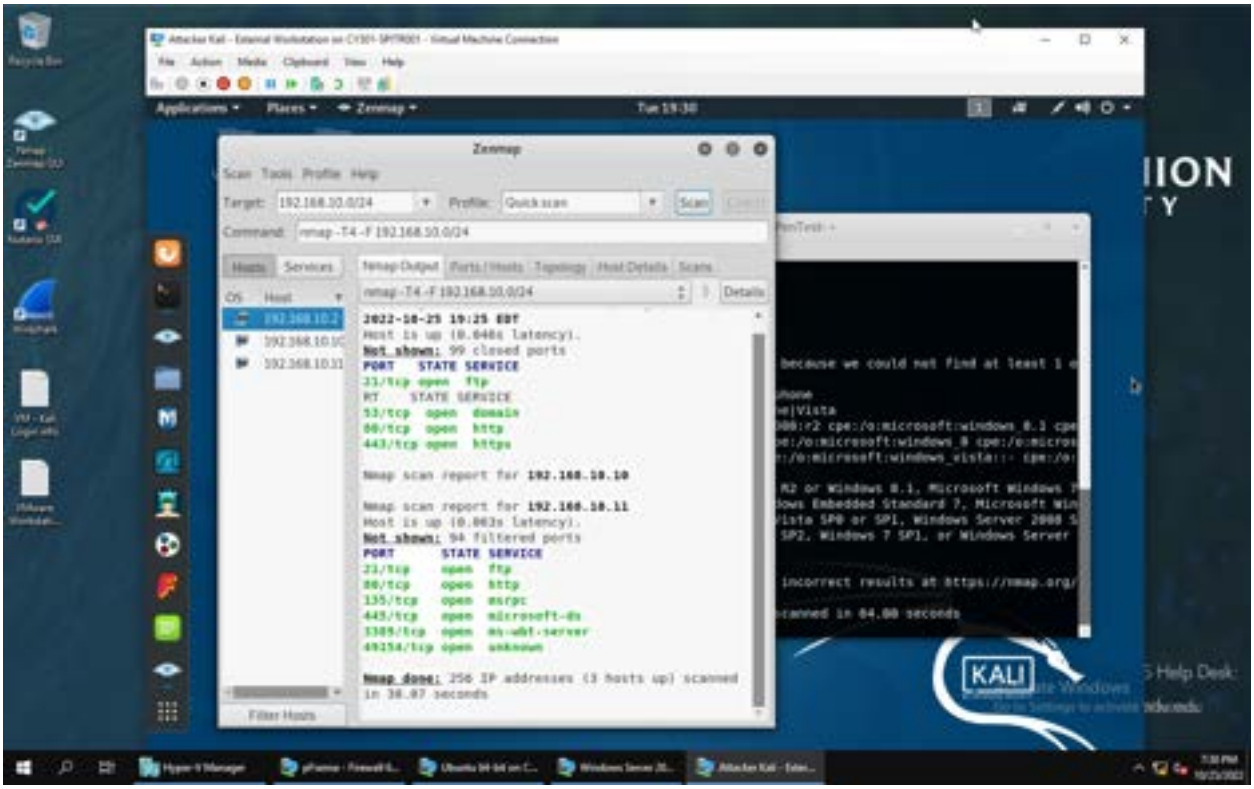
Assignment #3 Sword v Shield

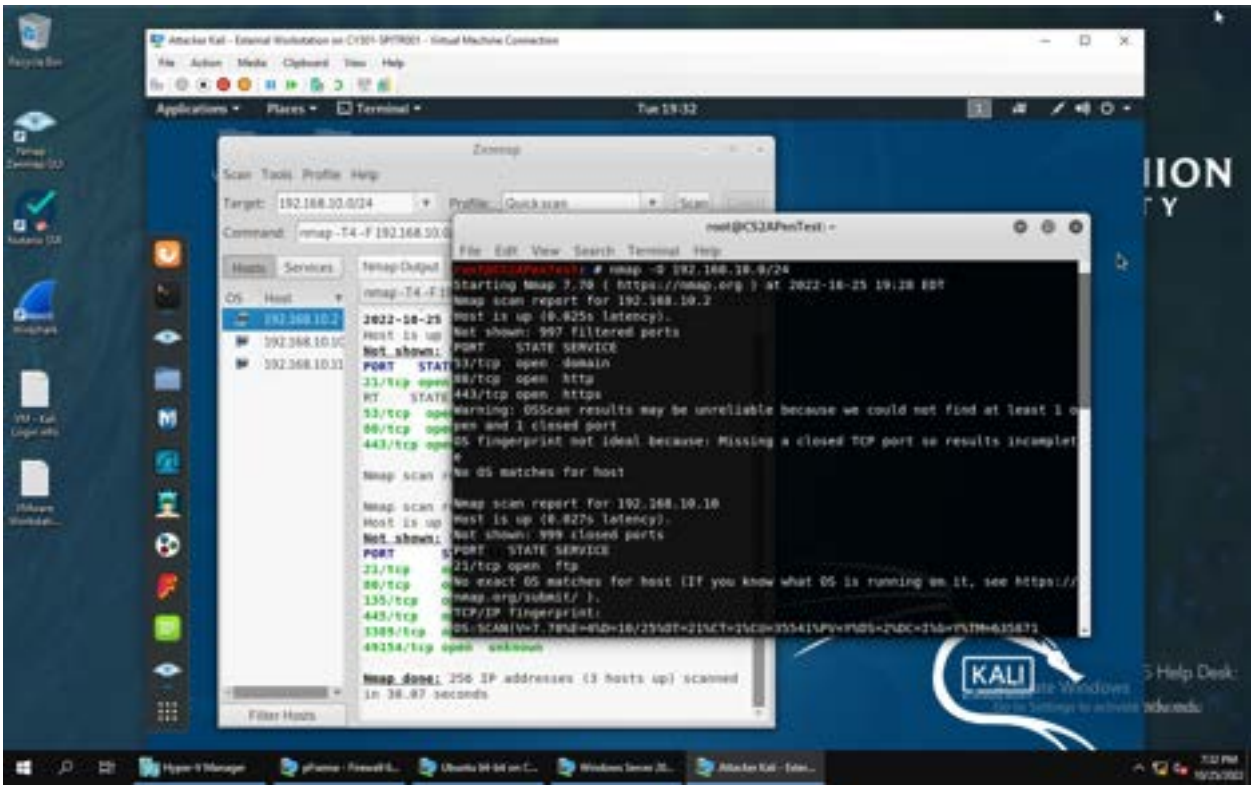
Shacara Pitre

01204408

TASK A

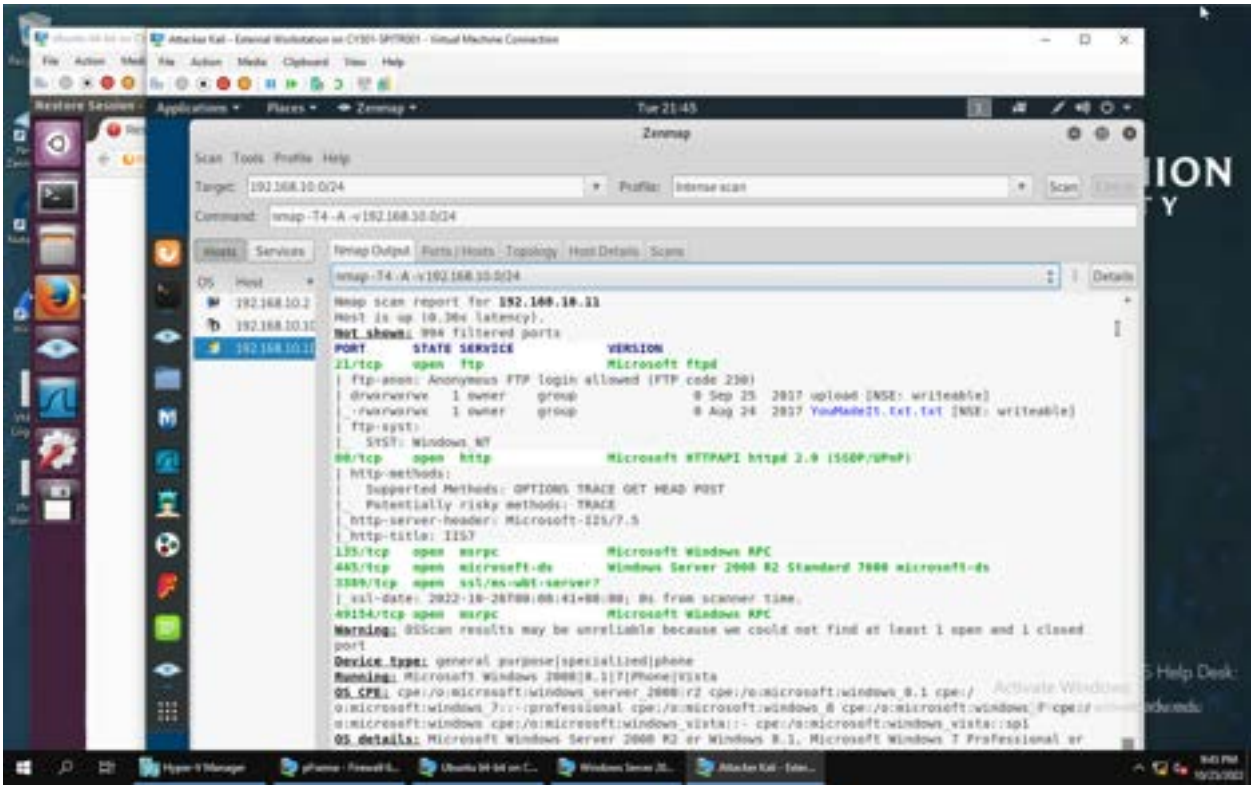
1.

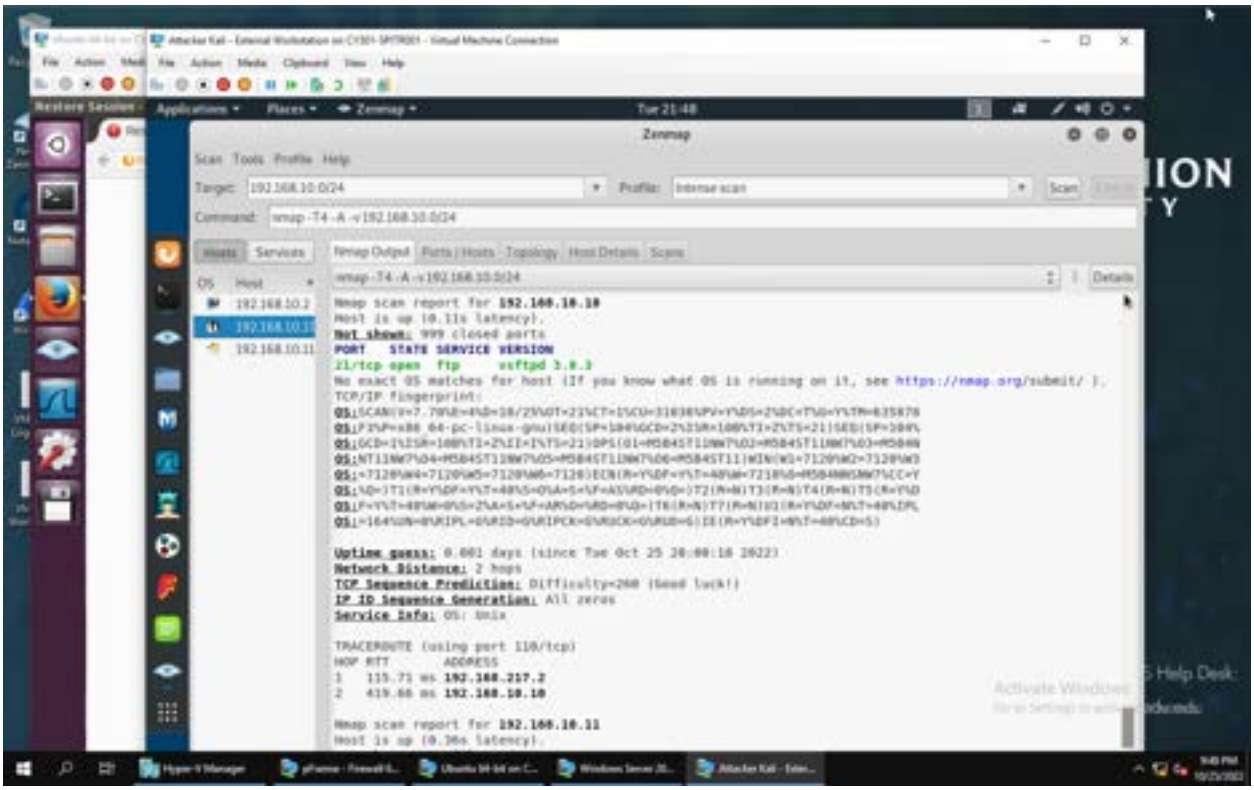

Zenmap
Scan Tools Profile Help
Target: 192.168.10.0/24
Profile: Quick scan
Scan
Command: nmap -T4 -F 192.168.10.0/24
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -T4 -F 192.168.10.0/24
Details
OS Host
192.168.10.2
192.168.10.10
192.168.10.11
2022-10-25 19:25 EDT
Host is up (0.048s latency).
Not shown: 99 closed ports
PORT STATE SERVICE
21/tcp open ftp
PORT STATE SERVICE
53/tcp open domain
80/tcp open http
443/tcp open https
Nmap scan report for 192.168.10.10
Nmap scan report for 192.168.10.11
Host is up (0.003s latency).
Not shown: 94 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
49154/tcp open unknown
Nmap done: 256 IP addresses (3 hosts up) scanned in 38.07 seconds
Filter Hosts
because we could not find at least 1
incorrect results at https://nmap.org/
KALI



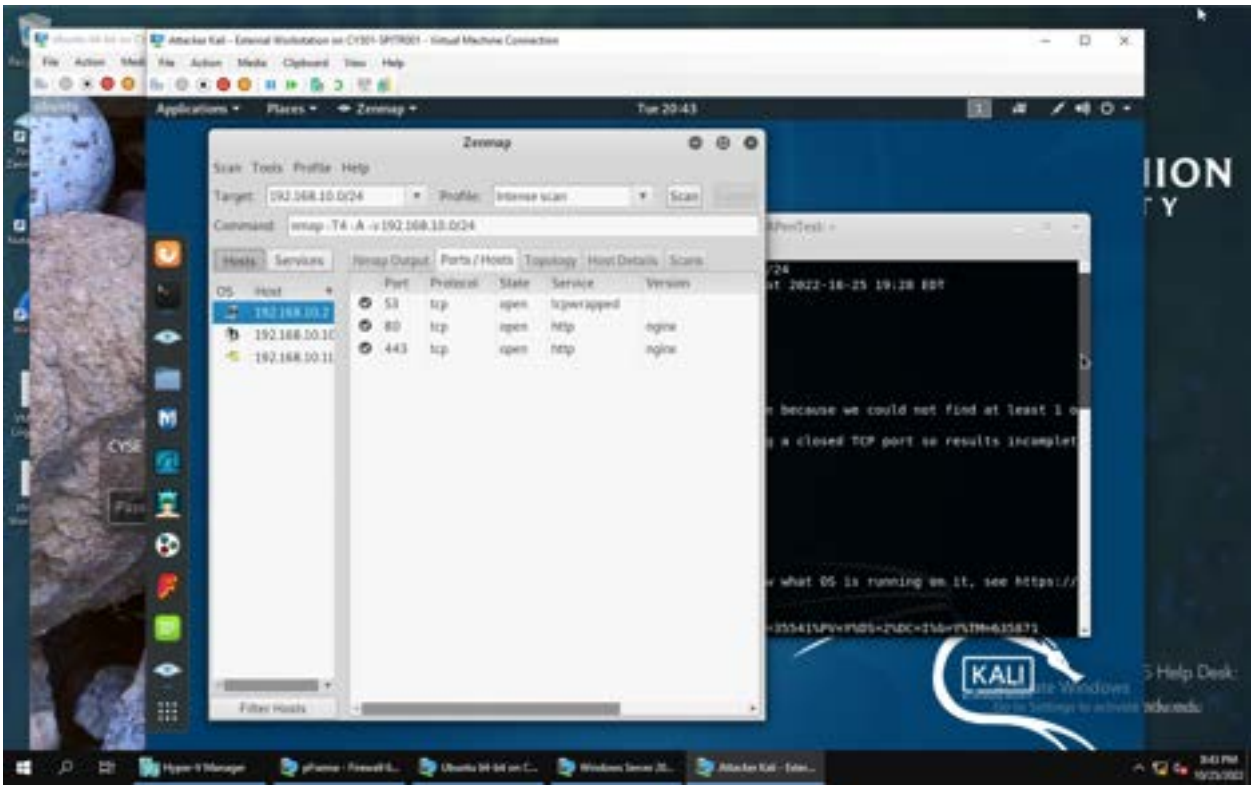
In both screenshots, you can see the tcp ports whether on nmap or zenmap which are 53, 80, and 443 while running a simple (quick) scan. However, there is no operating system.

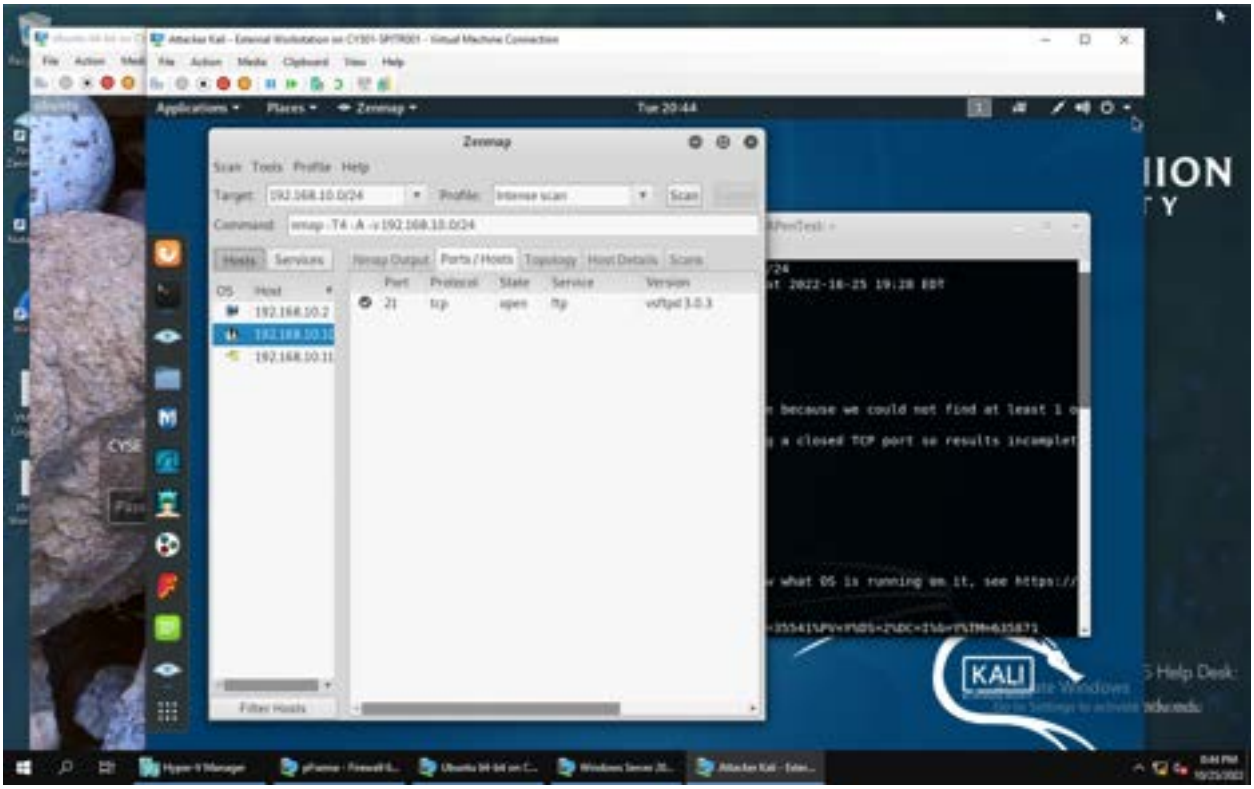
2.

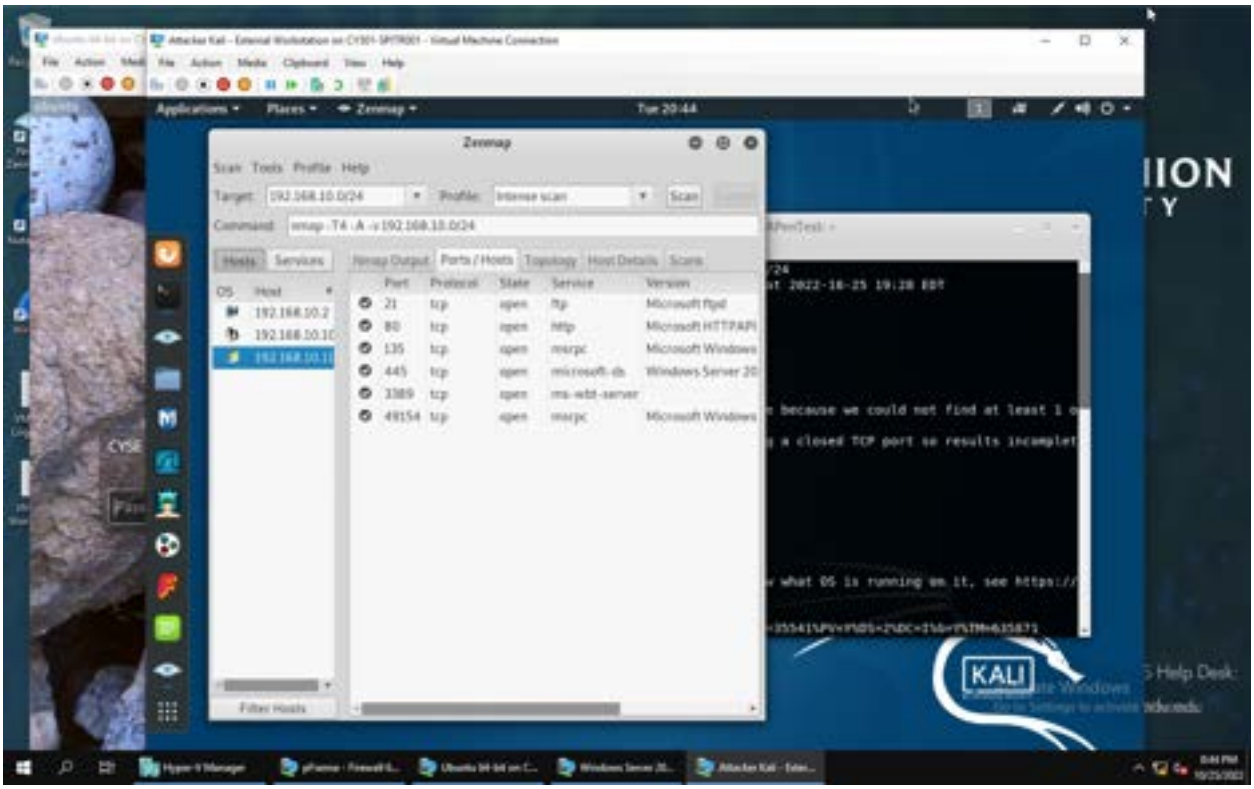




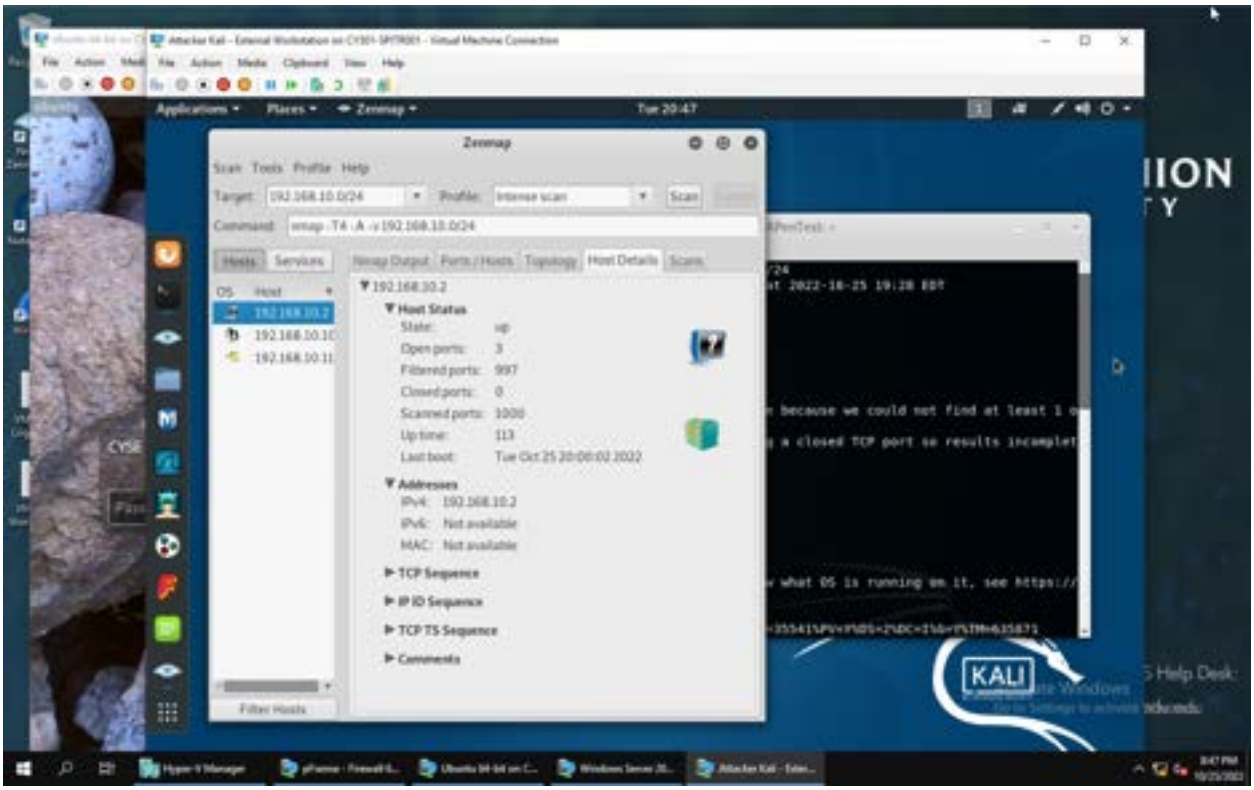
These screenshots show intense scan on each VM.

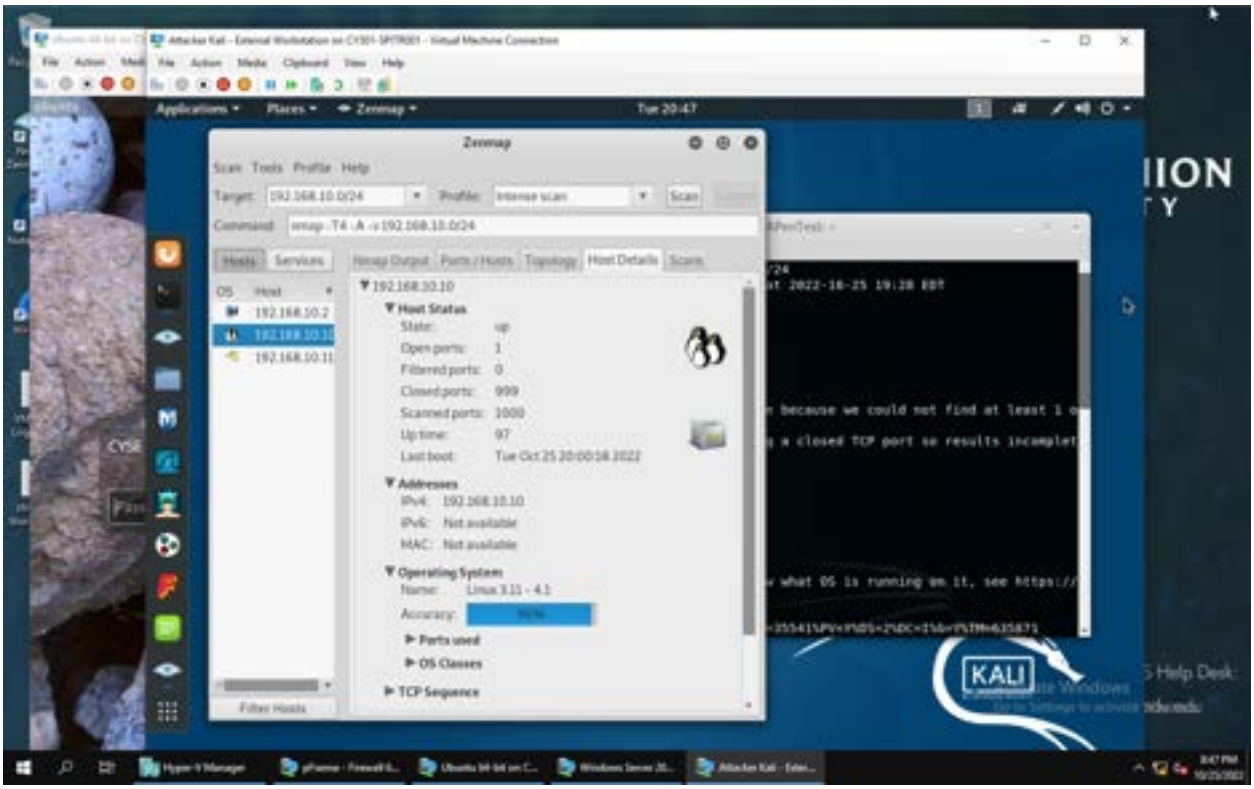

Zenmap
Scan Tools Profile Help
Target: 192.168.10.0/24
Profile: Intense scan
Scan
Command: nmap -T4 -A -v 192.168.10.0/24
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
Port Protocol State Service Version
53 tcp open tcpwrapped
80 tcp open http nginx
443 tcp open http nginx
Filter Hosts
KALI

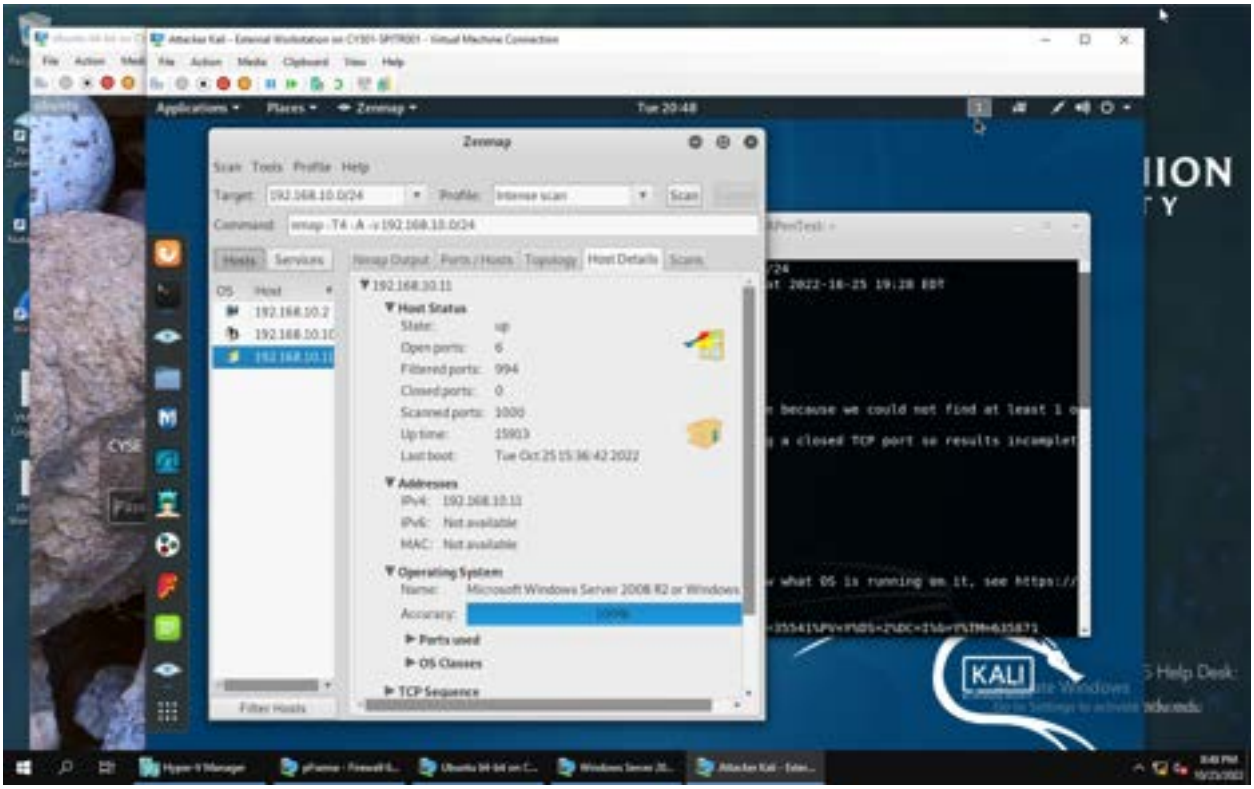

Zenmap
Scan Tools Profile Help
Target: 192.168.10.0/24
Profile: Intense scan
Scan
Command: nmap -T4 -A -v 192.168.10.0/24
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
Port Protocol State Service Version
21 tcp open ftp vsftpd 3.0.3
Filter Hosts
KALI



In these screenshots above you can see the service associated with each port in each VM (pfsense, ubuntu, and windows server).

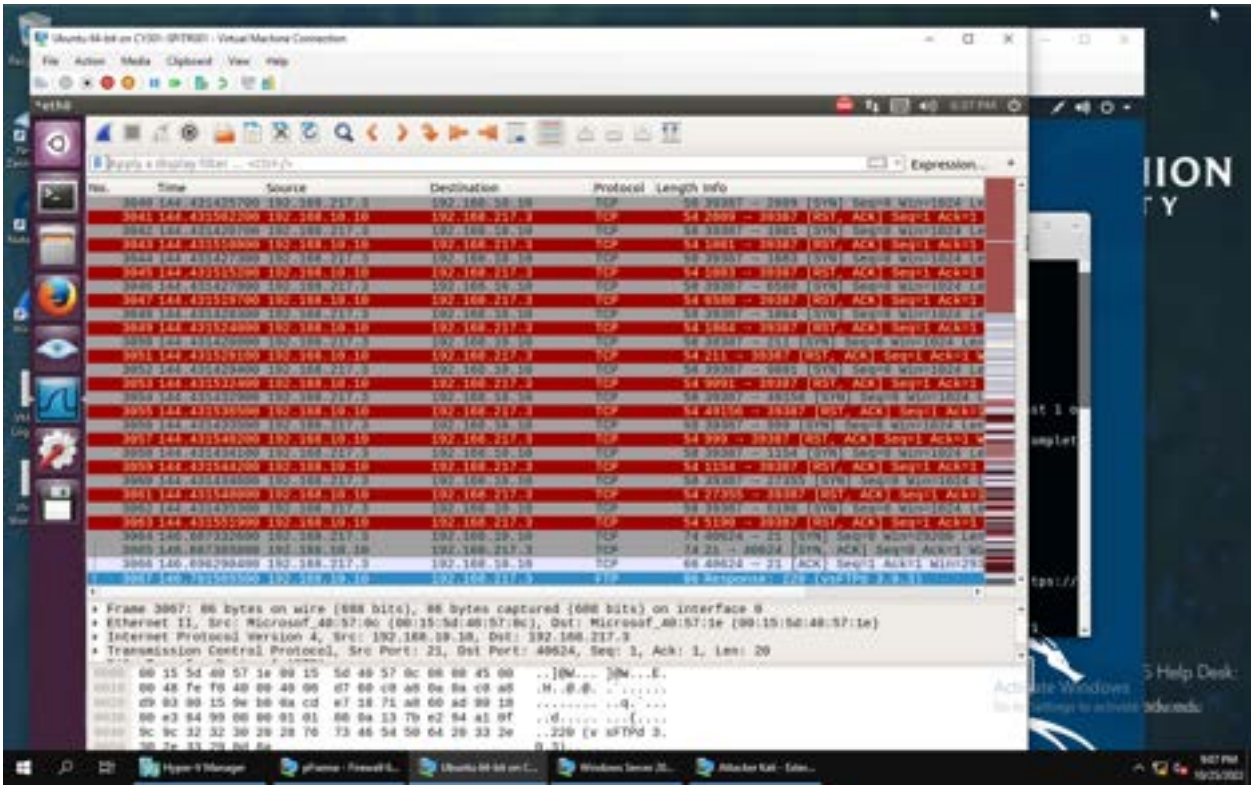


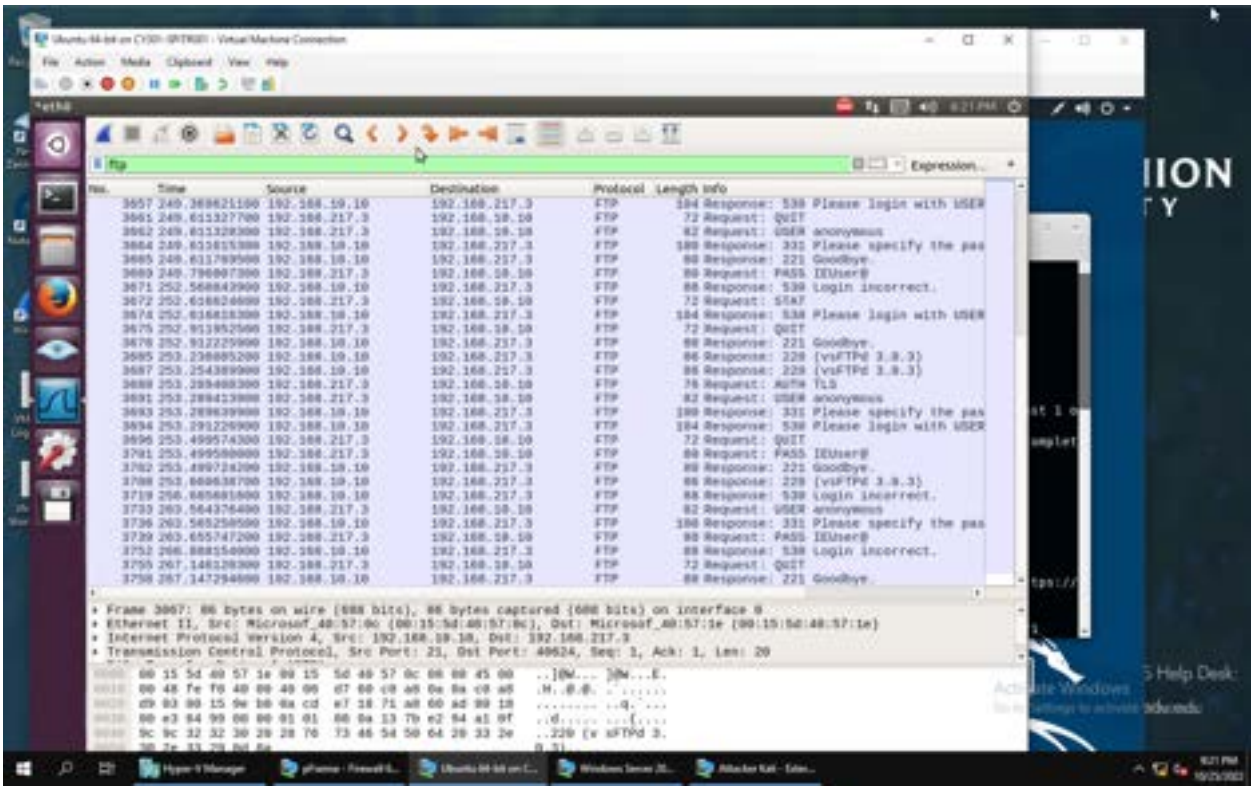


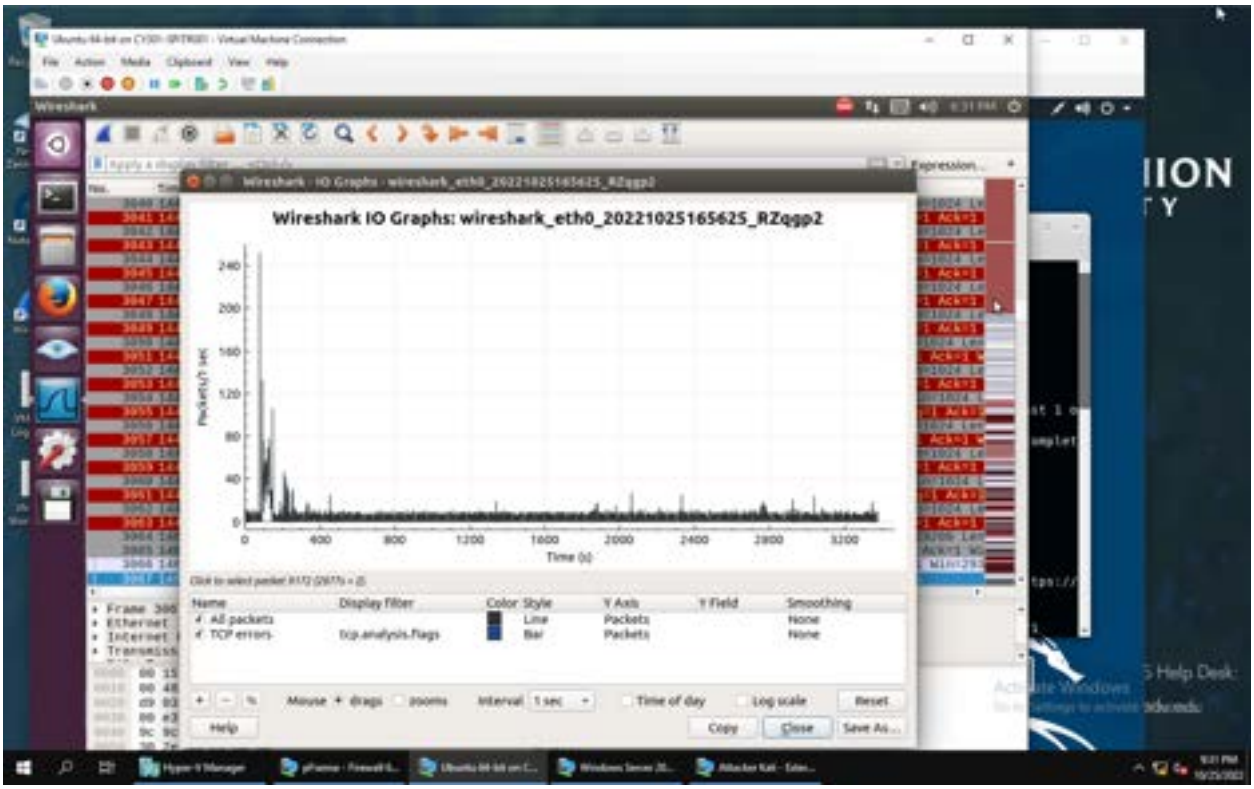


In the screenshots above, you can see the topology regarding the backend software for each VM.

3.





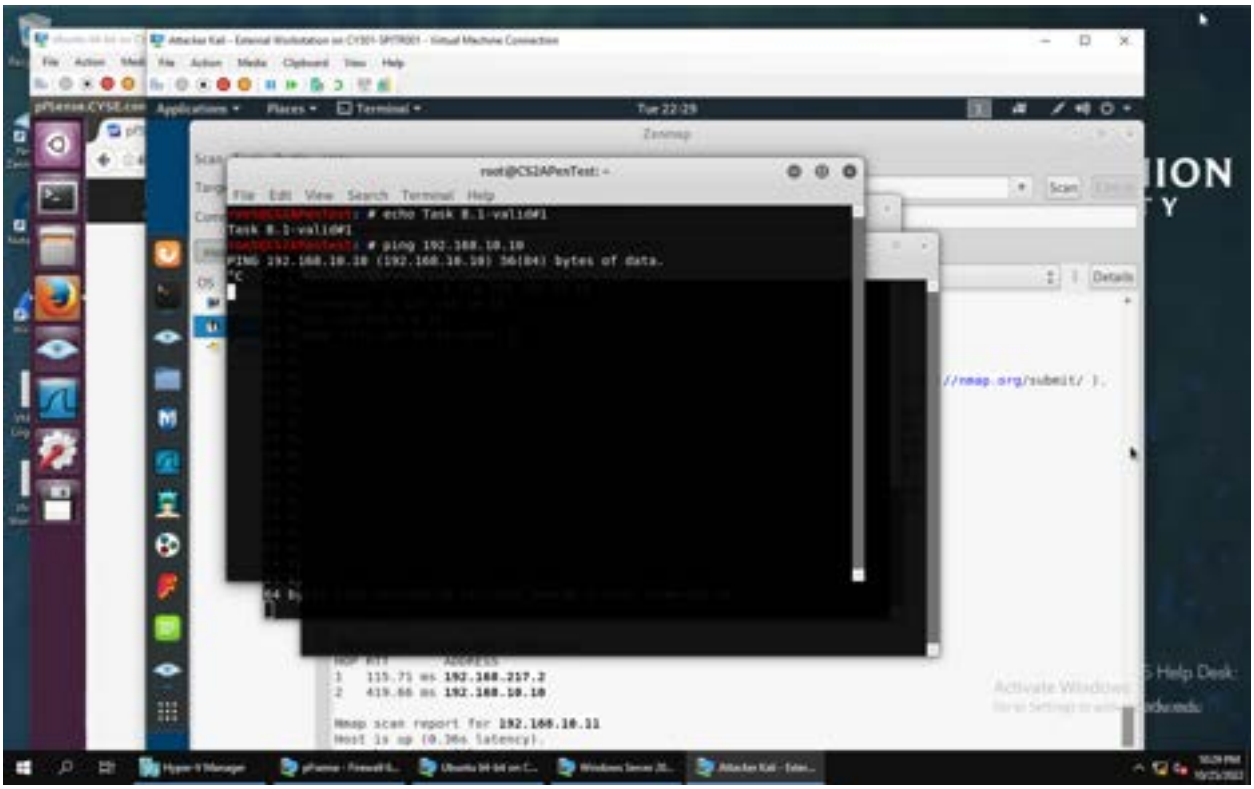


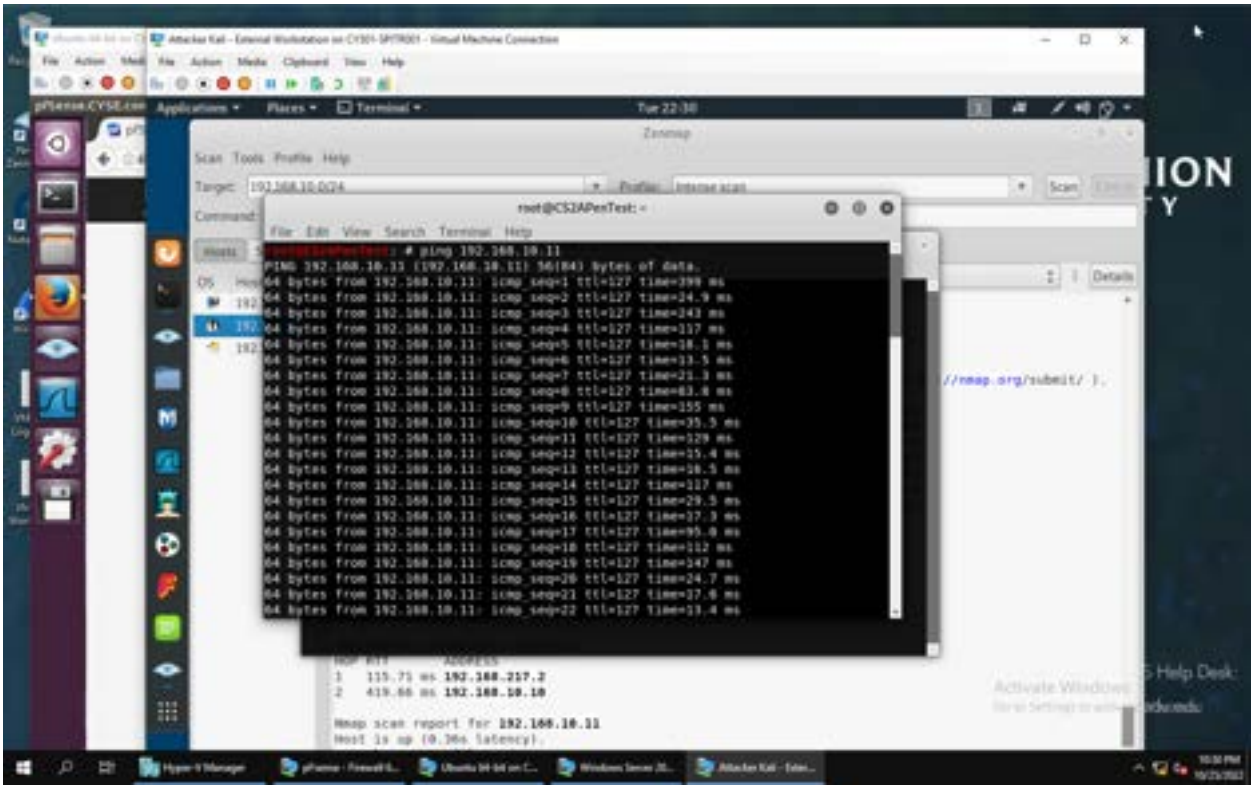
While running Wireshark on Ubuntu VM, I observed what was happening in the network. For instance, I went up to the statistics tab and clicked on protocol hierarchy and filtered out the Wireshark to FTP protocol. While in FTP, it looks like the user is logging in as anonymous and that they logged in incorrectly. They are trying to sneak their way in to get into FTP server. The user does not know the correct credential to log into FTP server even though they are trying different ways to communicate. Also, on the I/O graph, I noticed that there was a lot of information (peak) around 74s meaning that there could have been activities going on. After this time, you can see a normal traffic pattern. This makes me question whether there was an actual attack or if it could have been an error. Another thing to look at is the conversation to see who did the most communicating with me, which shows conversations from address a to address b and vice versa. Overall, the results from both screenshots show that the traffic pattern is questionable and that there was at least some kind of problem or issue going on.

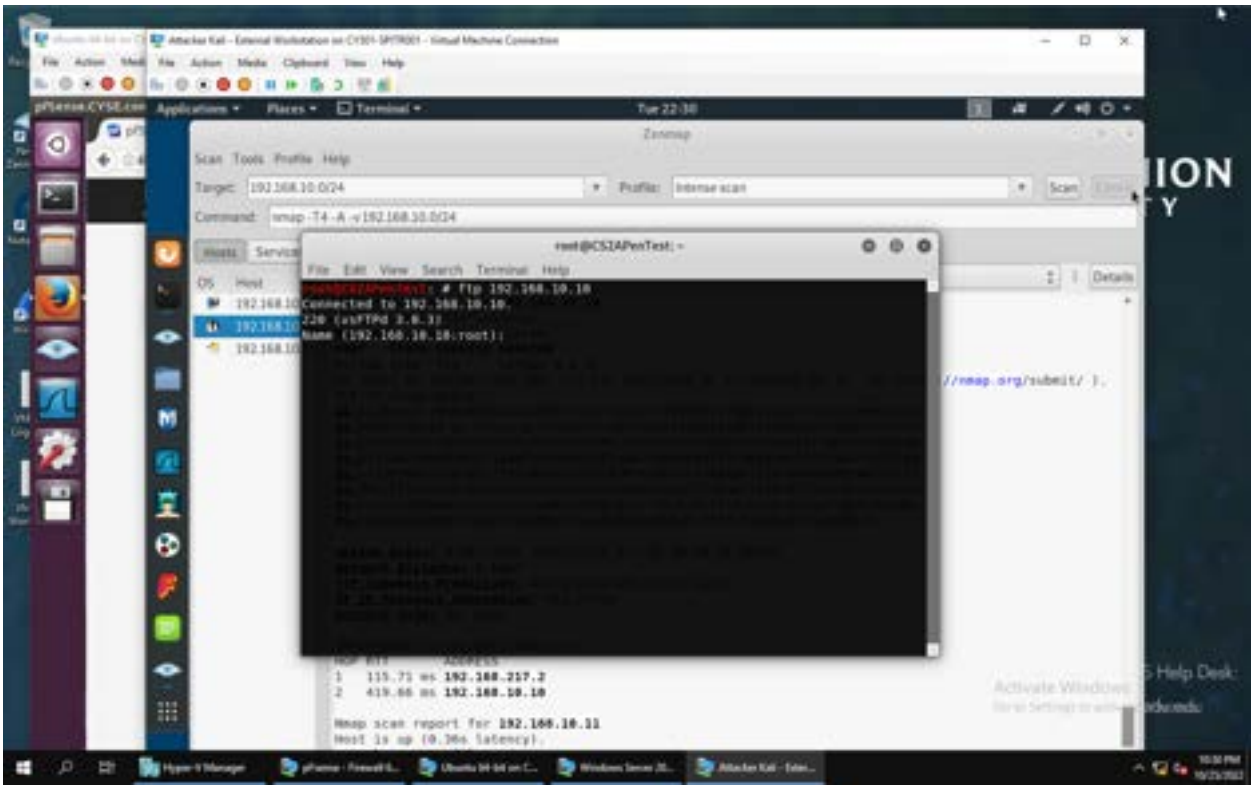
Task B

1. Inbound traffic

Rule #	Interface	Action	Source IP	Destination IP	Protocol
1	WAN	Block or reject	192.168.217.3	192.168.10.10	ICMP/no port #

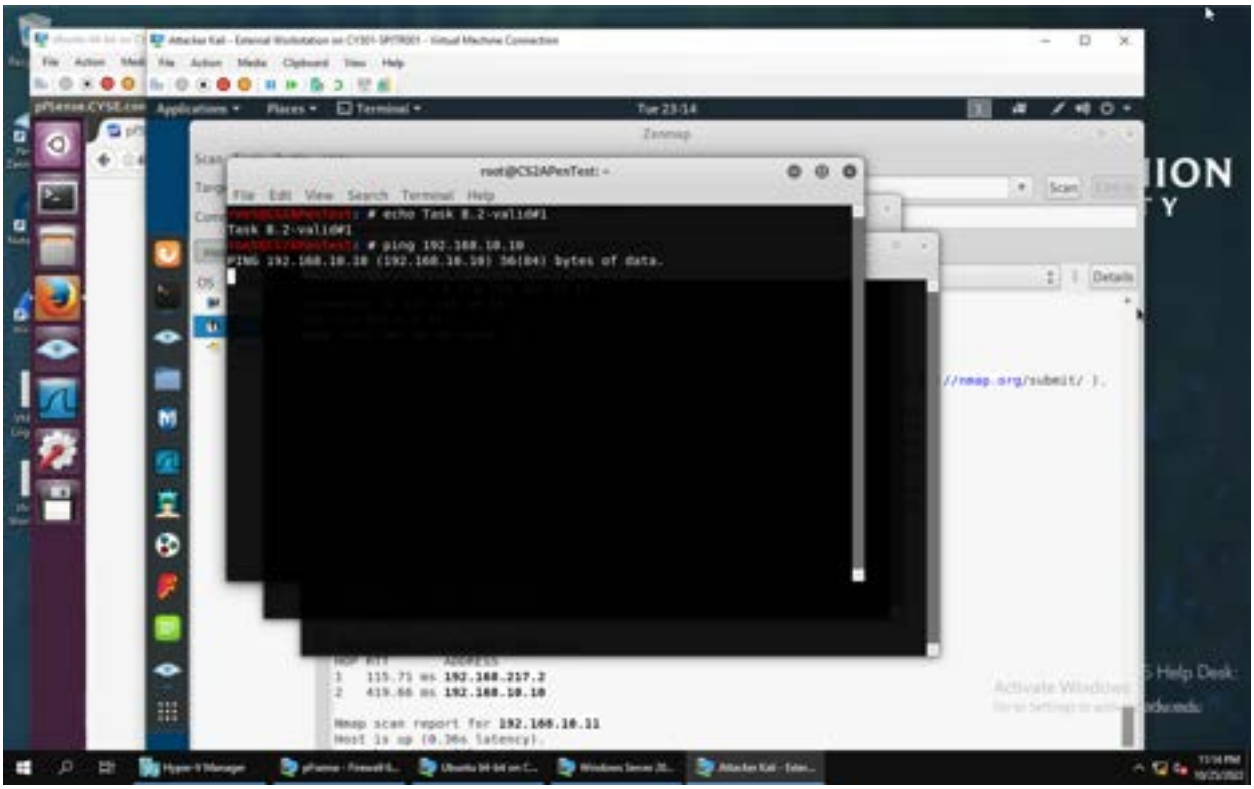

root@CSIAPenTest: ~
File Edit View Search Terminal Help
echo Task 8.1-validW1
Task 8.1-validW1
ping 192.168.10.10
PING 192.168.10.10 (192.168.10.10) 56(84) bytes of data.
^C
1 115.71 ms 192.168.217.2
2 419.66 ms 192.168.10.10
Nmap scan report for 192.168.10.11
Host is up (0.30s latency).

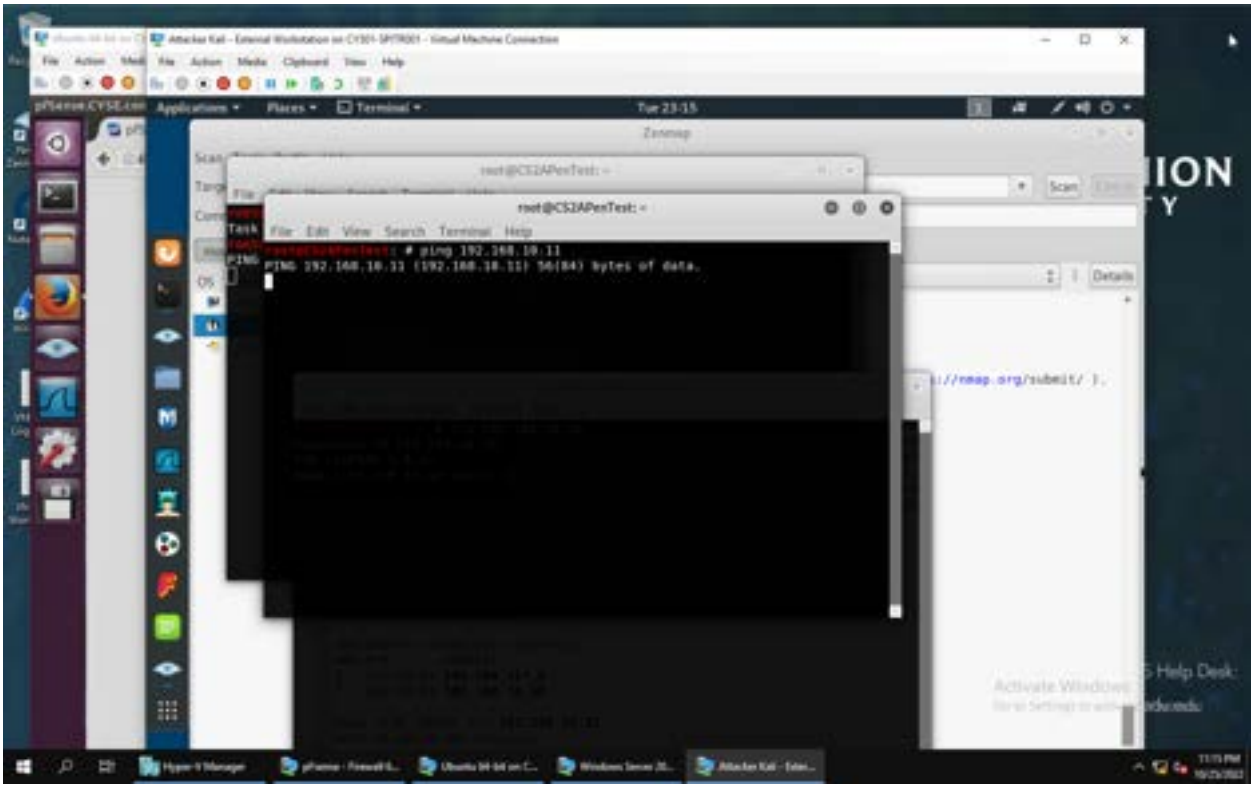

root@CSIAPenTest: ~
File Edit View Search Terminal Help
ping 192.168.10.11
PING 192.168.10.11 (192.168.10.11) 56(84) bytes of data.
64 bytes from 192.168.10.11: icmp_seq=1 ttl=127 time=399 ms
64 bytes from 192.168.10.11: icmp_seq=2 ttl=127 time=24.9 ms
64 bytes from 192.168.10.11: icmp_seq=3 ttl=127 time=243 ms
64 bytes from 192.168.10.11: icmp_seq=4 ttl=127 time=117 ms
64 bytes from 192.168.10.11: icmp_seq=5 ttl=127 time=18.1 ms
64 bytes from 192.168.10.11: icmp_seq=6 ttl=127 time=13.5 ms
64 bytes from 192.168.10.11: icmp_seq=7 ttl=127 time=21.3 ms
64 bytes from 192.168.10.11: icmp_seq=8 ttl=127 time=83.8 ms
64 bytes from 192.168.10.11: icmp_seq=9 ttl=127 time=155 ms
64 bytes from 192.168.10.11: icmp_seq=10 ttl=127 time=35.5 ms
64 bytes from 192.168.10.11: icmp_seq=11 ttl=127 time=129 ms
64 bytes from 192.168.10.11: icmp_seq=12 ttl=127 time=15.4 ms
64 bytes from 192.168.10.11: icmp_seq=13 ttl=127 time=16.5 ms
64 bytes from 192.168.10.11: icmp_seq=14 ttl=127 time=117 ms
64 bytes from 192.168.10.11: icmp_seq=15 ttl=127 time=29.5 ms
64 bytes from 192.168.10.11: icmp_seq=16 ttl=127 time=37.3 ms
64 bytes from 192.168.10.11: icmp_seq=17 ttl=127 time=95.0 ms
64 bytes from 192.168.10.11: icmp_seq=18 ttl=127 time=112 ms
64 bytes from 192.168.10.11: icmp_seq=19 ttl=127 time=147 ms
64 bytes from 192.168.10.11: icmp_seq=20 ttl=127 time=24.7 ms
64 bytes from 192.168.10.11: icmp_seq=21 ttl=127 time=37.6 ms
64 bytes from 192.168.10.11: icmp_seq=22 ttl=127 time=13.4 ms
1 115.71 ms 192.168.217.2
2 419.66 ms 192.168.10.10
Nmap scan report for 192.168.10.11
Host is up (0.30s latency).

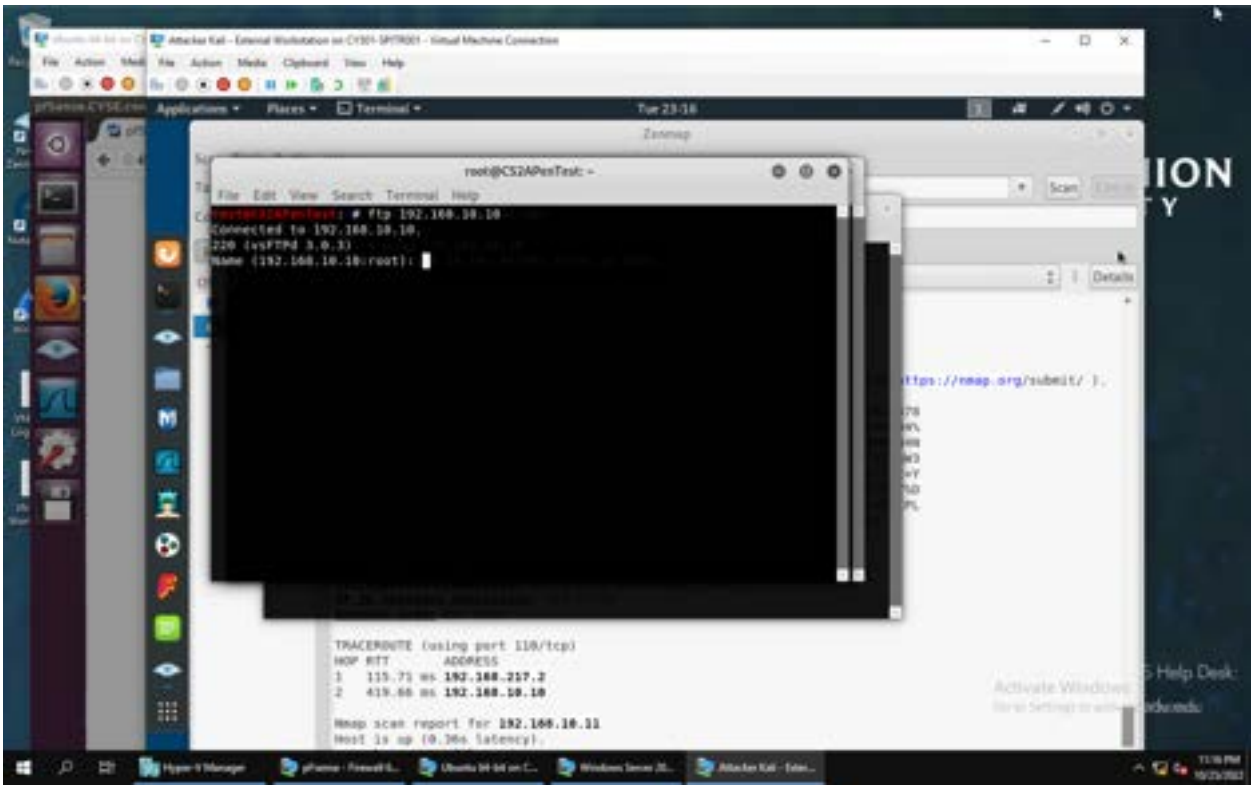


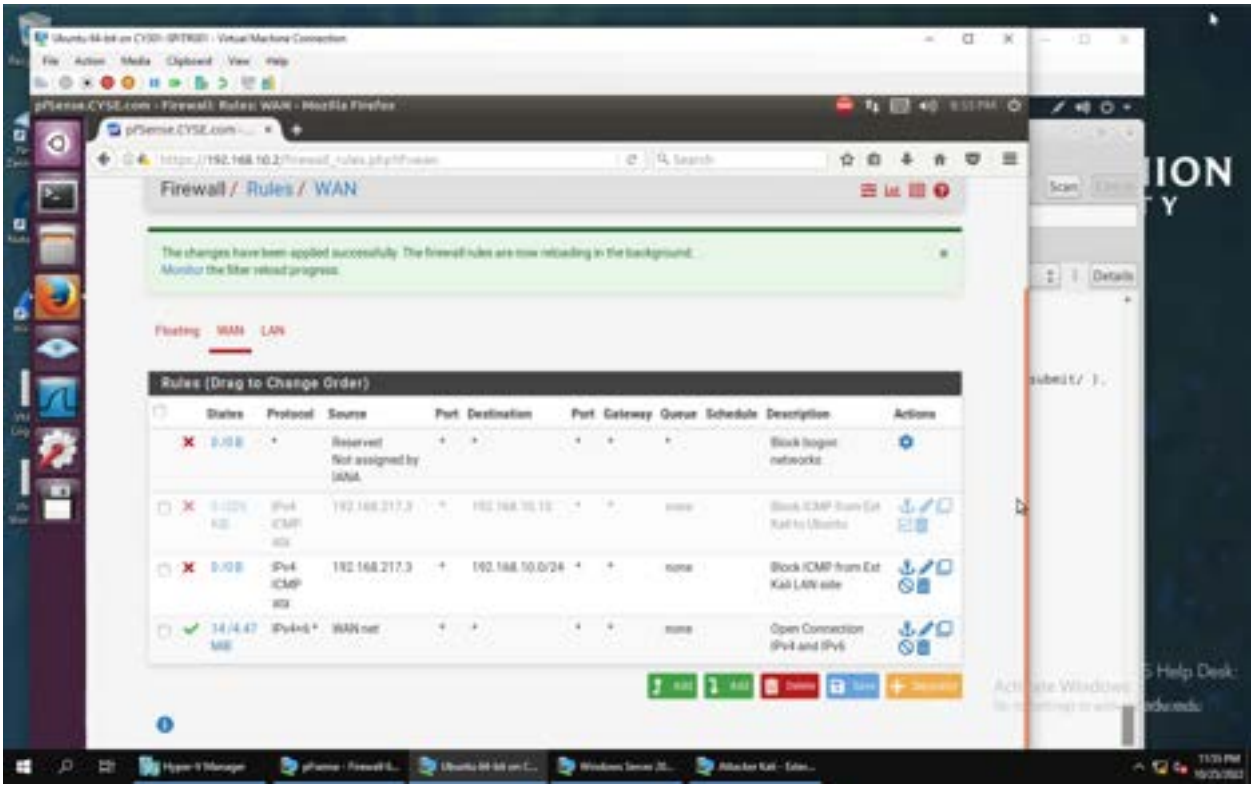
2. Inbound traffic

Rule #	Interface	Action	Source IP	Destination IP	Protocol
1	WAN	Block or reject	192.168.217.3	192.168.10.0/24	ICMP


root@CS2APenTest: ~
File Edit View Search Terminal Help
echo Task 8.2-valid#1
Task 8.2-valid#1
ping 192.168.10.10
PING 192.168.10.10 (192.168.10.10) 56(84) bytes of data.
1 115.71 ms 192.168.217.2
2 419.66 ms 192.168.10.10
Nmap scan report for 192.168.10.11
Host is up (0.30s latency).

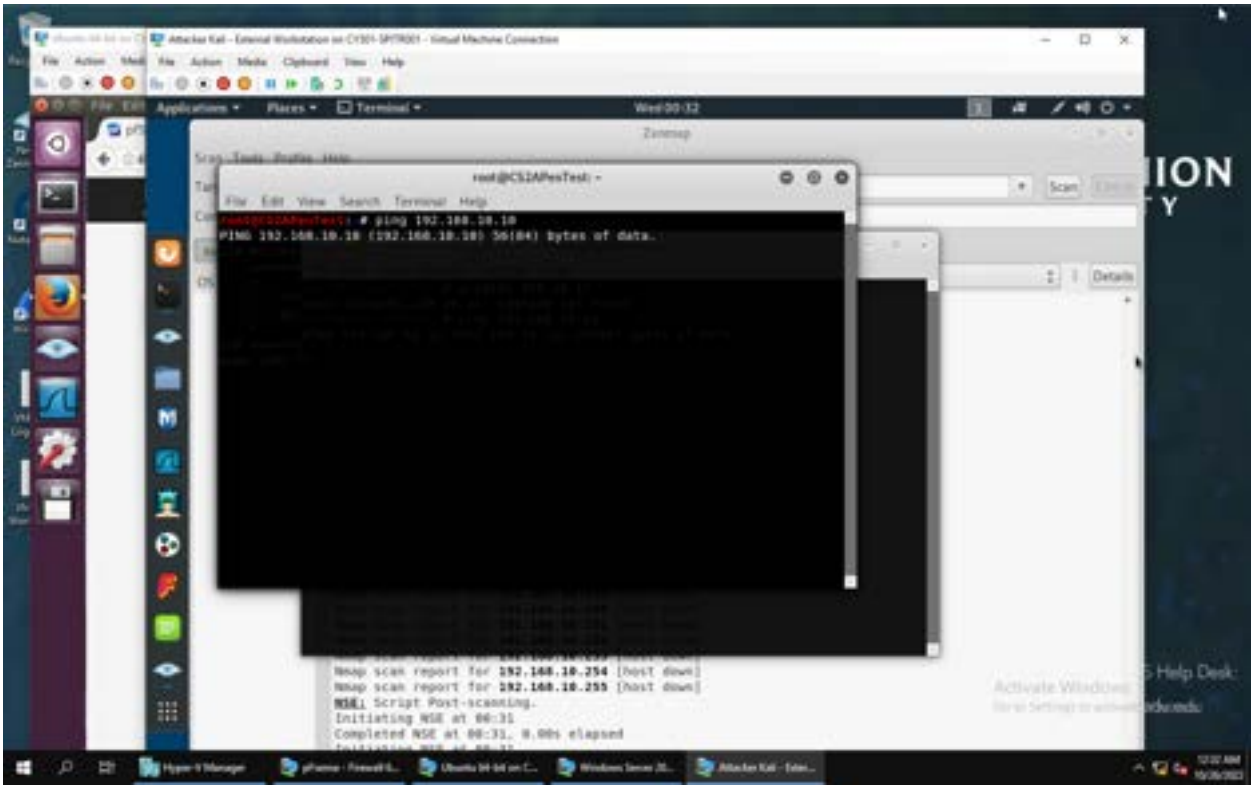

root@CS2APenTest: ~
File Edit View Search Terminal Help
ping 192.168.10.11
PING 192.168.10.11 (192.168.10.11) 56(84) bytes of data.

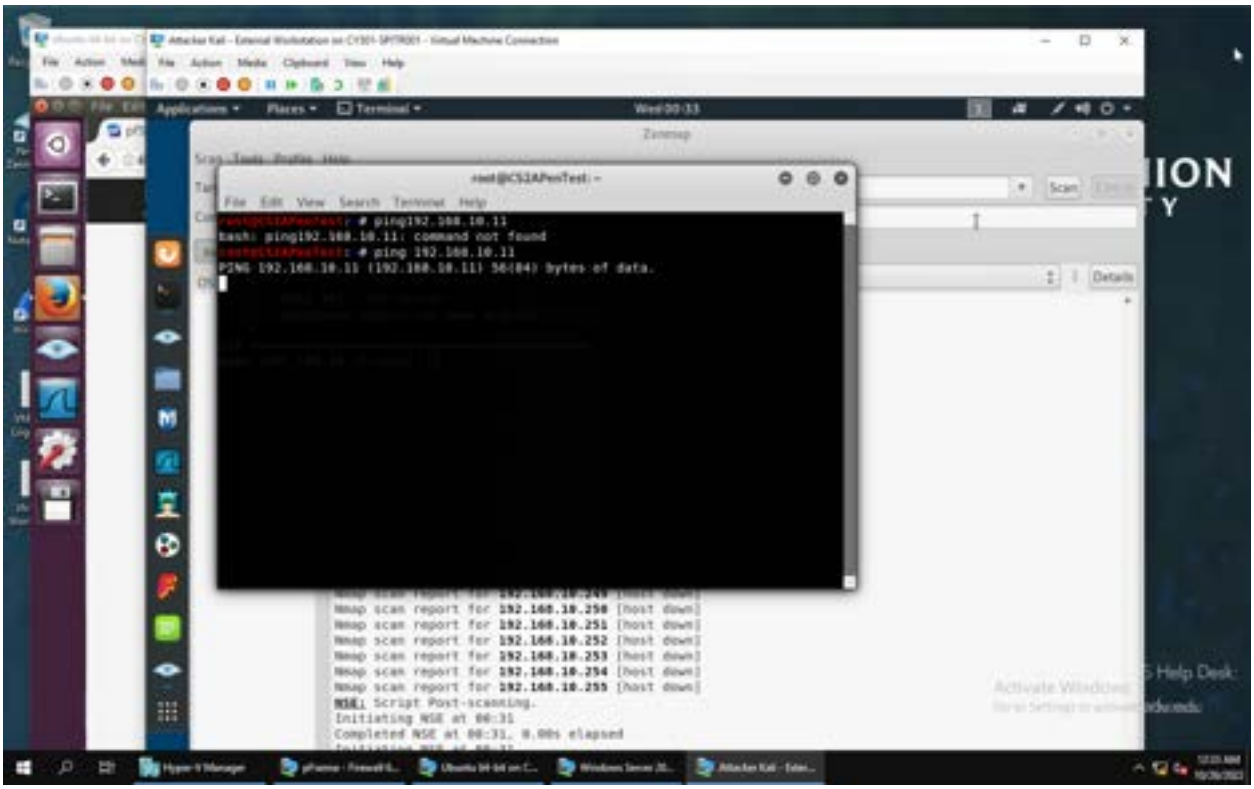

root@CS2APenTest: ~
File Edit View Search Terminal Help
ftp 192.168.10.10
Connected to 192.168.10.10.
220 (vsFTPd 3.0.3)
Name (192.168.10.10:root):
TRACEROUTE (using port 110/tcp)
HOP RTT ADDRESS
1 115.71 ms 192.168.217.2
2 419.66 ms 192.168.10.10
Nmap scan report for 192.168.10.11
Host is up (0.30s latency).

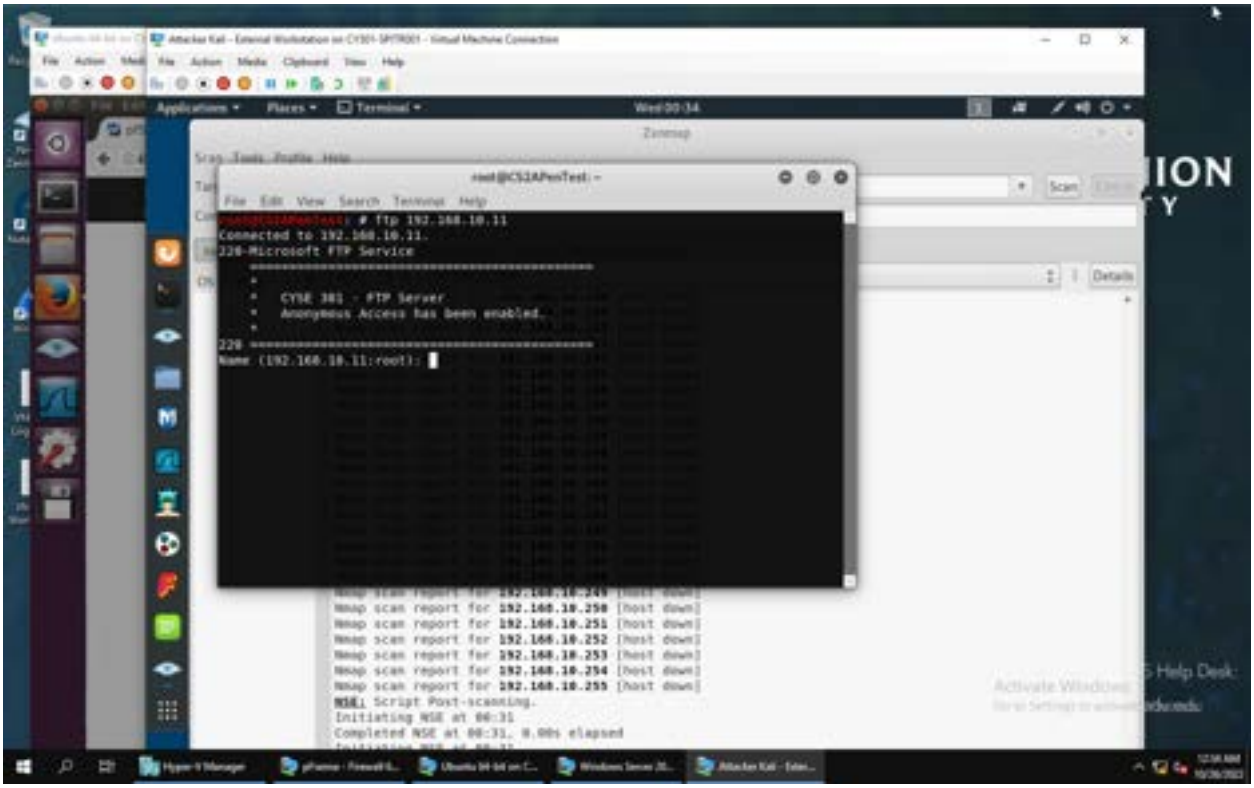

Firewall / Rules / WAN
The changes have been applied successfully. The firewall rules are now reloading in the background.
Floating WAN LAN
Rules (Drag to Change Order)
States Protocol Source Port Destination Port Gateway Queue Schedule Description Actions
Reserved Not assigned by IANA
Block bogon networks
IPv4 ICMP any
192.168.217.3
192.168.10.0/24
none
Block ICMP from Ext Kali LAN side
IPv4+6
WAN net
Open Connection IPv4 and IPv6

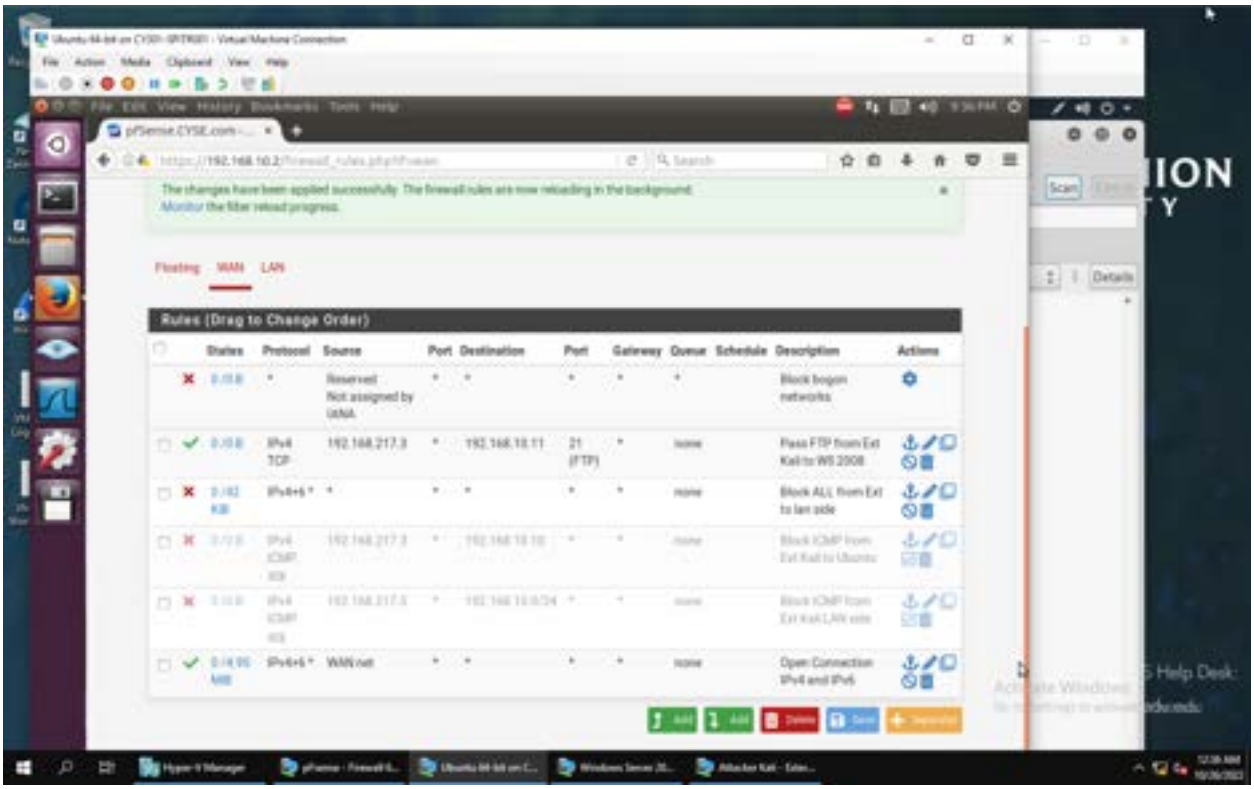
3.

Rule #	Interface	Action	Source IP	Destination IP	Protocol
1	WAN	Pass	192.168.217.3	192.168.10.11	FTP/Port 21
2	WAN	Block	192.168.217.3	192.168.10.0/24	All

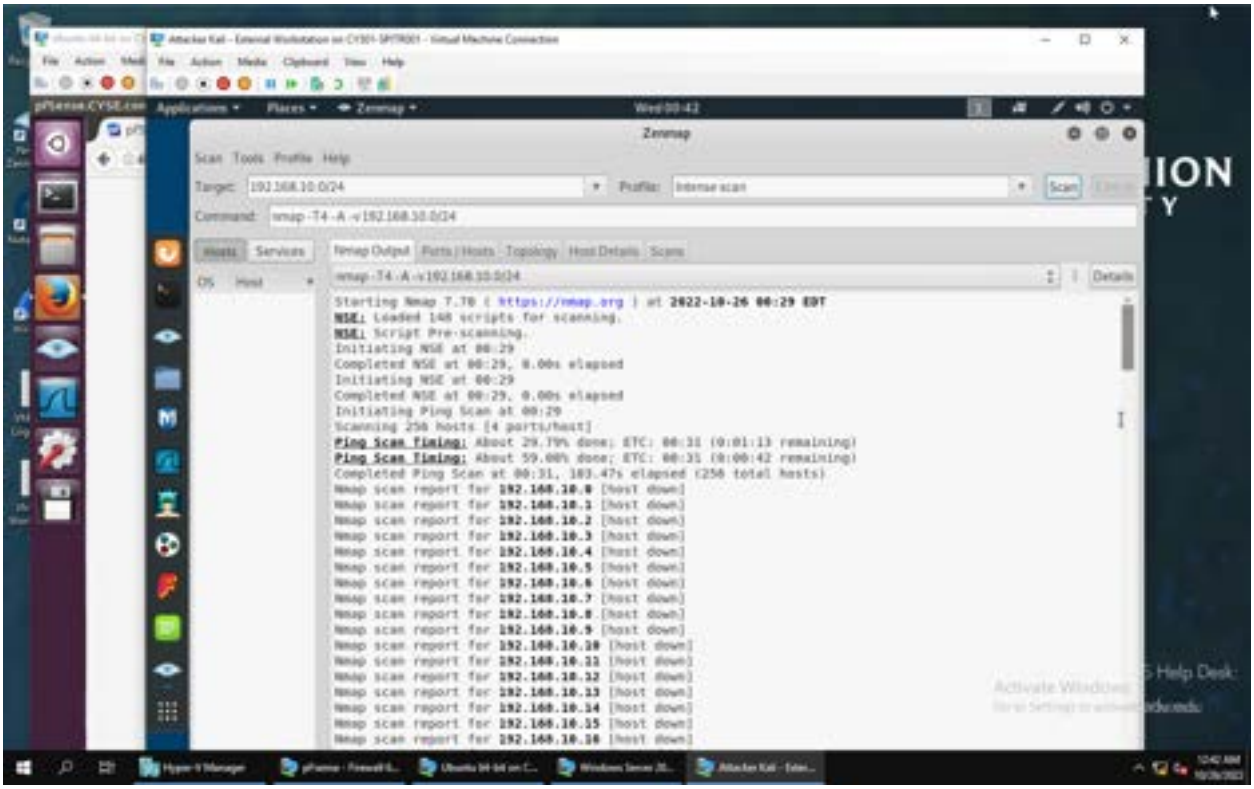



root@CSIAPenTest: ~
File Edit View Search Terminal Help
root@CSIAPenTest: # ping192.168.10.11
bash: ping192.168.10.11: command not found
root@CSIAPenTest: # ping 192.168.10.11
PING 192.168.10.11 (192.168.10.11) 56(84) bytes of data.
Nmap scan report for 192.168.10.250 [host down]
Nmap scan report for 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 00:31
Completed NSE at 00:31, 0.00s elapsed


root@CSIAPenTest: ~
File Edit View Search Terminal Help
root@CSIAPenTest: # ftp 192.168.10.11
Connected to 192.168.10.11.
220-Microsoft FTP Service
*
* CYSE 381 - FTP Server
* Anonymous Access has been enabled
*
220
Name (192.168.10.11:root):
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 00:31
Completed NSE at 00:31, 0.00s elapsed



4.



From the intense scan, you can see that all hosts are down.