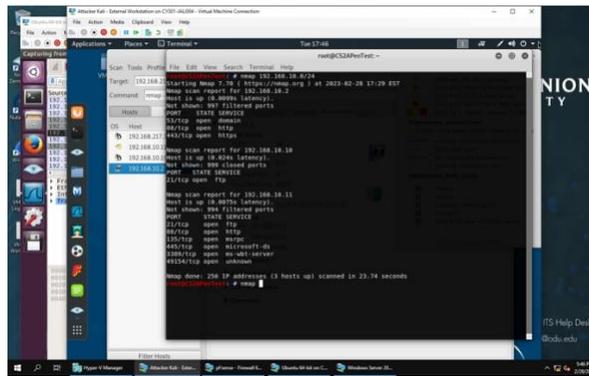
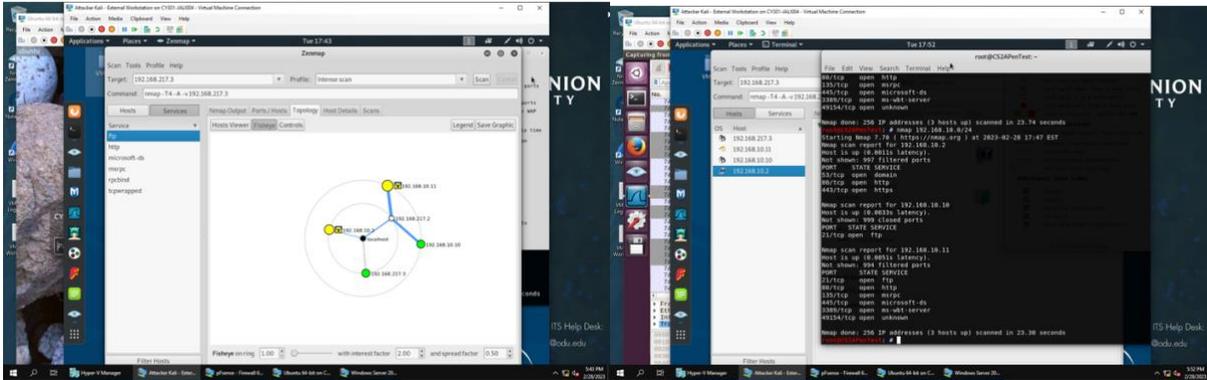


Task A: Sword-Network Scanning



192.168.10.2

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

Hosts	Services	Nmap Output	Ports / Hosts	Topology	Host Details		
OS	Host		Port	Protocol	State	Service	Version
	192.168.10.2		53	tcp	open	tcpwrapped	
	192.168.10.10		80	tcp	open	http	nginx
	192.168.10.11		443	tcp	open	http	nginx

Hosts	Services	Nmap Output	Ports / Hosts	Topology	Host Details	Scans
OS	Host					
	192.168.10.11					
	192.168.10.10					
	192.168.10.2	<pre> nmap -T4 -A -v 192.168.10.0/24 Nmap scan report for 192.168.10.2 Host is up (0.0041s latency). Not shown: 997 filtered ports PORT STATE SERVICE VERSION 53/tcp open tcpwrapped 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://192 443/tcp open ssl/http nginx _ http-favicon: Unknown favicon MD5: 5567E9CE23E5549 _ http-methods: _ Supported Methods: GET HEAD POST _ http-server-header: nginx _ http-title: pfSense - Login _ ssl-cert: Subject: commonName=pfSense-61c4e5e912521 webConfigurator Self-Signed Certificate Subject Alternative Name: DNS:pfSense-61c4e5e912521 </pre>				

192.168.10.10

OS	Host	Port	Protocol	State	Service	Version
	192.168.10.2	21	tcp	open	ftp	vsftpd 3.0.3
	192.168.10.10					
	192.168.10.11					

```

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

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host nmap -T4 -A -v 192.168.10.0/24
192.168.10.11 Nmap scan report for 192.168.10.10
192.168.10.10 Host is up (0.011s latency).
192.168.10.2 Not shown: 999 closed ports
PORT STATE SERVICE
21/tcp open ftp vsftpd 3.0.3
No exact OS matches for host (if you know what OS is runn
https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.78AE=4D=2/2810T=21VCT=1%CU=43584PV=Y0S=23D
OS:14P=X86_64-pc-linux-gnu)SEQ(SP=185)NGCD=IIS=16AVTI=2%
OS:10B4ST11W703=MSB4ST11W703=MSB4ST11W703=MSB4ST11
OS:1006=MSB4ST11)WIN(W=7120)W2=7120W3=7120W4=7120W5=71
OS:10P=V1T=40U=V21810=MSB4NSM7LCC=Y0=V11)R=V0DF=YVLT=4
OS:1=MS02121(R=N)T3(R=N)T4(R=N)T5(R=V)DF=V1T=40U=MS-C
OS:1T6(R=N)T7(R=N)U1(R=V)DF=MS-T=40L1PL=164UUN=0UR1PL=0UR1
OS:1URUD=0)IE(R=V)DF=HNT=49PCD=5)

Uptime guess: 0.901 days (since Tue Feb 28 17:23:49 2023)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=260 (Good Luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: UNIX

TRACEROUTE (using port 587/tcp)
HOP RTT ADDRESS
1 3.65 ms 192.168.217.2
2 11.56 ms 192.168.10.10
  
```

192.168.10.11

OS	Host	Port	Protocol	State	Service	Version
	192.168.10.2	21	tcp	open	ftp	Microsoft ftpd
	192.168.10.10	80	tcp	open	http	Microsoft IIS httpd 7.5
	192.168.10.11	135	tcp	open	msrpc	Microsoft Windows RPC
		445	tcp	open	microsoft-ds	Windows Server 2008 R2 Standard 7600 microsoft-ds
		3389	tcp	open	tcpwrapped	
		49154	tcp	open	msrpc	Microsoft Windows RPC

```

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host nmap -T4 -A -v 192.168.10.0/24
192.168.10.11 Nmap scan report for 192.168.10.11
192.168.10.10 Host is up (0.0002s latency).
192.168.10.2 Not shown: 994 filtered ports
PORT STATE SERVICE VERSION
21/tcp open ftp Microsoft ftpd
| ftp-mgmt: Anonymous FTP login allowed (FTP code 230)
| drwxrwxrwx 1 owner group 0 Sep 25 2017 upload [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 IIS httpd 7.5
| 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
| ssl-date: 2023-02-28T22:24:16+00:00; 0s from scanner time.
49154/tcp open msrpc Microsoft Windows RPC
  
```

192.168.217.3

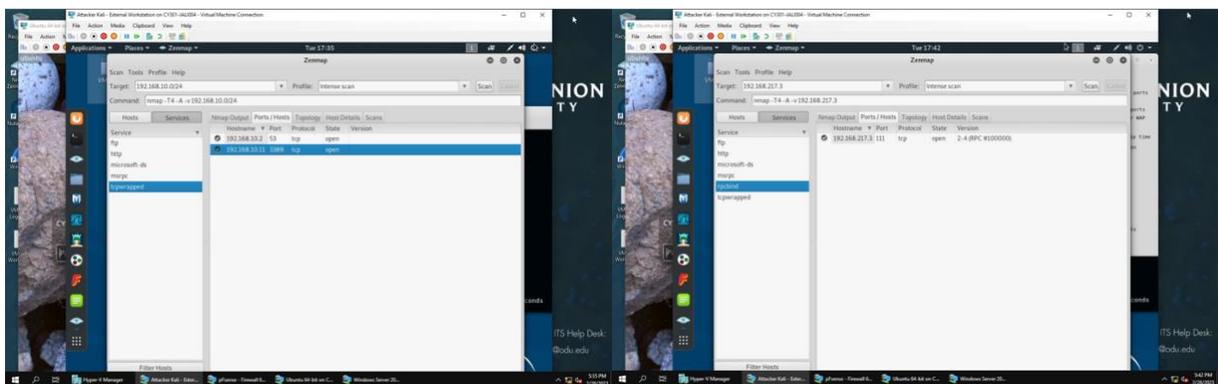
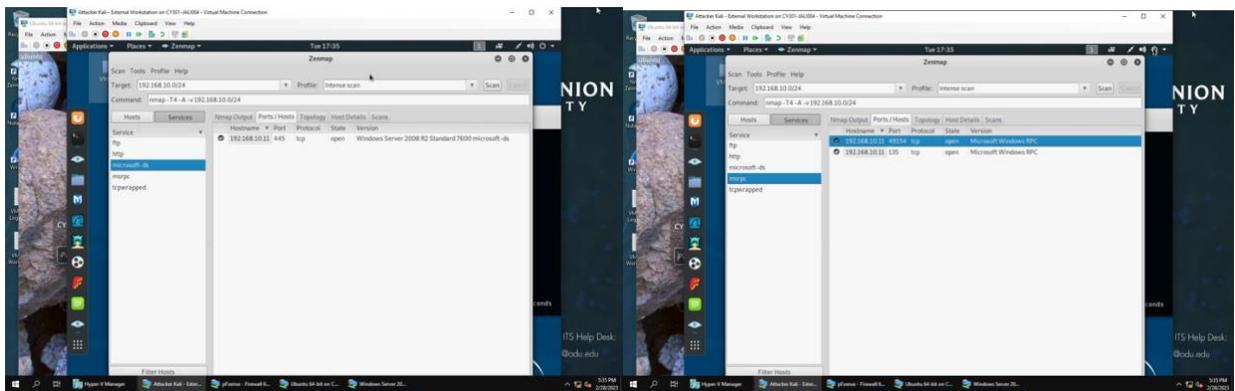
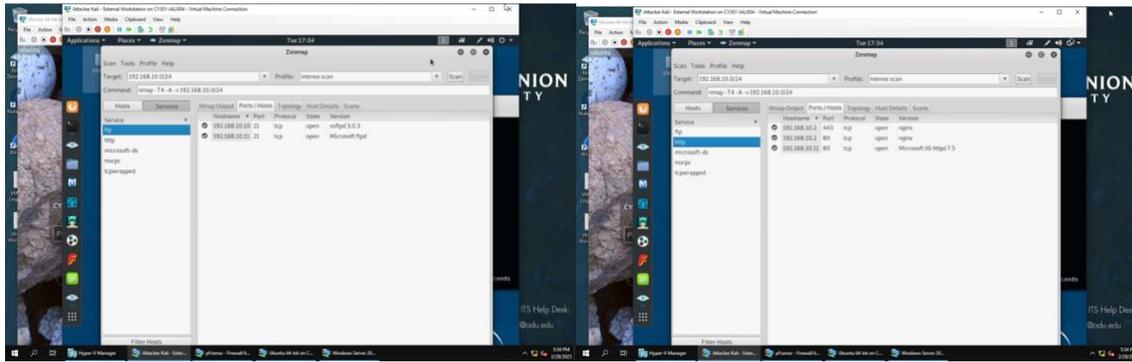
```

Target: 192.168.217.3 Profile: Intense scan
Command: nmap -T4 -A -v 192.168.217.3

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host nmap -T4 -A -v 192.168.217.3
192.168.217.3 Completed NSE at 17:41, 0.00s elapsed
192.168.10.11 Nmap scan report for 192.168.217.3
192.168.10.10 Host is up (0.000040s latency).
192.168.10.2 Not shown: 999 closed ports
PORT STATE SERVICE VERSION
111/tcp open rpcbind 2.4 (RPC #100000)
| rpcinfo:
| program version port/proto service
| 100000 2,3,4 111/tcp rpcbind
| 100000 2,3,4 111/udp rpcbind
Device type: general purpose
Running: Linux 3.X
OS_CPE: cpe:/o:linux:linux kernel:3
OS_details: Linux 3.7 - 3.10
Uptime guess: 7.629 days (since Tue Feb 21 02:35:06 2023)
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=258 (Good Luck!)
IP ID Sequence Generation: All zeros

NSE: Script Post-scanning.
Initiating NSE at 17:41
Completed NSE at 17:41, 0.00s elapsed
Initiating NSE at 17:41
Completed NSE at 17:41, 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: 1 IP address (1 host up) scanned in 20.93 seconds
Raw packets sent: 1022 (45.778KB) | Rcvd: 2043 (87.024KB)
  
```

OBSERVING FTP, HTTP, TCP PORTS



HOST DETAILS

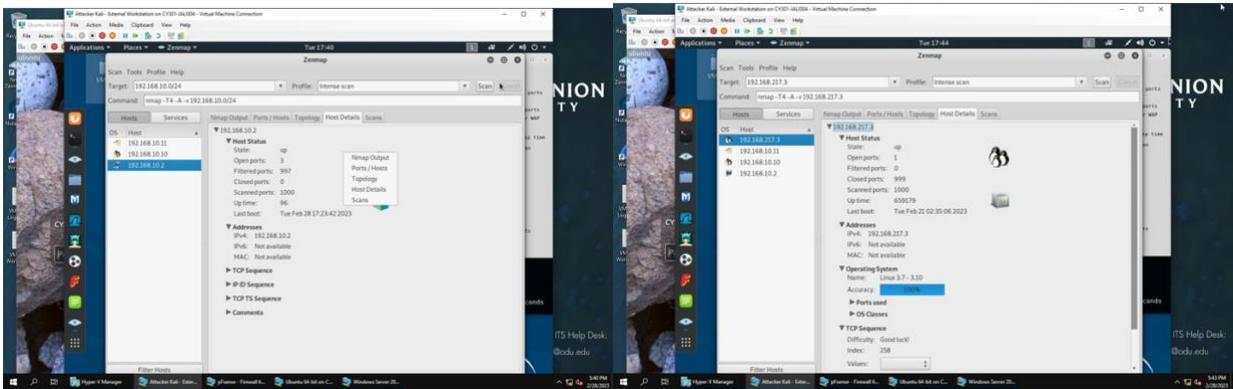
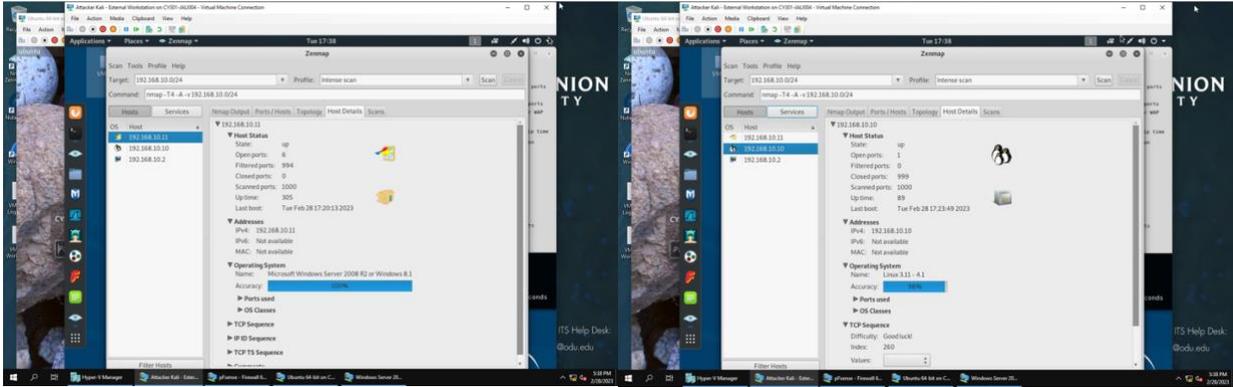
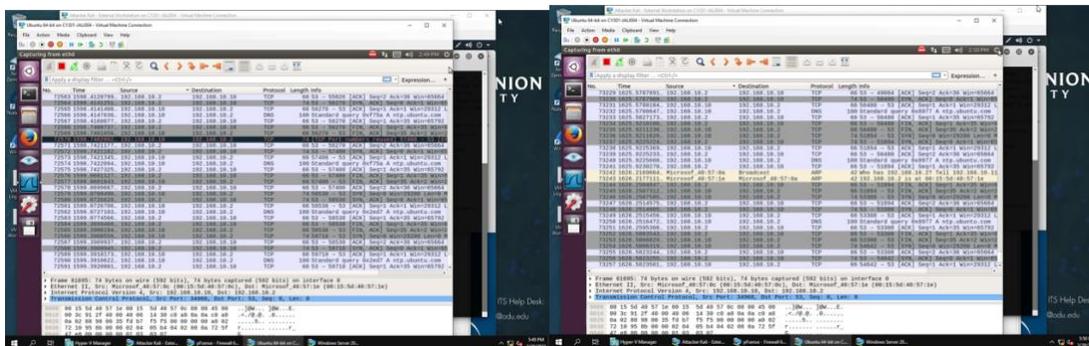


TABLE SUMMARY

Target 1 st Scan: 192.168.10.0/24 Target 2 nd Scan: 192.168.217.3		Ports	Port/State/Service/OS
External Kali	192.168.217.3	TCP port 111	TCP/UDP port 111 open Service is rpcbind Linux version is 3.7-3.10
pfSense	192.168.10.2	TCP port 53,80,443	TCP port 52 open Service is TCPwrapped TCP port 80 open Service is HTTP TCP port 443 open Service is ssl/HTTP Version is NGINX
Ubuntu	192.168.10.10	TCP port 21	TCP port 21 open Service is FTP OS is Unix
Windows 2008	192.168.10.11	TCP port 21,80,125,445,3389,49154	TCP port 21 open Service is FTP TCP port 80 open Service is HTTP TCP port 125 open Microsoft httpd 7.5 TCP port 445 open Windows Server TCP port 3389 open Tepwrapped TCP port 49154 open Windows Server OS is Windows 2008

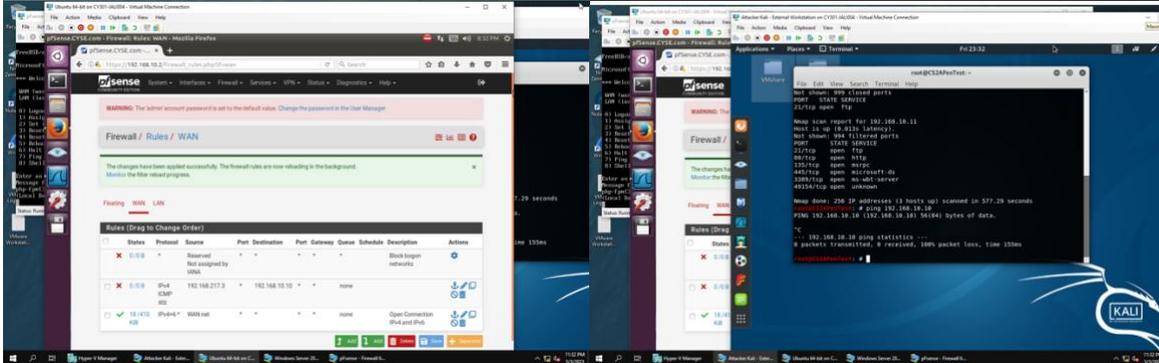
2. Ran Wireshark in Ubuntu VM while External Kali is scanning the network and discussion of traffic pattern observed below. An overall summary of the traffic patterns observed is that TCP, DNS, and ARP were flowing. There were no firewall rules, apart from the default, in place yet, so I could ping from external kali freely and create ftp traffic. This will change in B4, but to explain the screenshots below, one example is Ubuntu and pfSense communication back and forth. Notice the standard broadcast message highlighted in pastel yellow, ARP traffic. At this point, this is where I realized the zenmap I initiated from external kali was creating multiple traffic patterns. The scan is trying to reach everyone in the network I chose, which is what I see on Wireshark. Then the destinations are talking back and saying, "hey this is open, succesful!" It happened fast, but the ARP messages and TCP traffic filled my screen. Another traffic pattern to note, while not pictured, is below, but above instead via the zenmap intense scan is open ports and successful scans. Ultimately, ICMP traffic is happening with Ext Kali, Ubuntu, and Windows 2008. The last important traffic pattern, also not shown, is successful FTP traffic, which I created using External Kali to access Windows 2008 and Ubuntu's file transfers. In sum, I can access the VMs as a malicious attacker and packets moving back and forth. Another way to put it is Wireshark revealed while the scan was still running and, after completion, several open ports and packets of various protocols, letting me know which doors were open and what type of door they were. So I could figure out, hey, this destination is so and so on this platform using this type of software. All this information is in the packets on Wireshark, but zenmap puts it on a GUI so I can sift through the information faster and more efficiently.



TASK B: SHIELD-PROTECT NETWORK

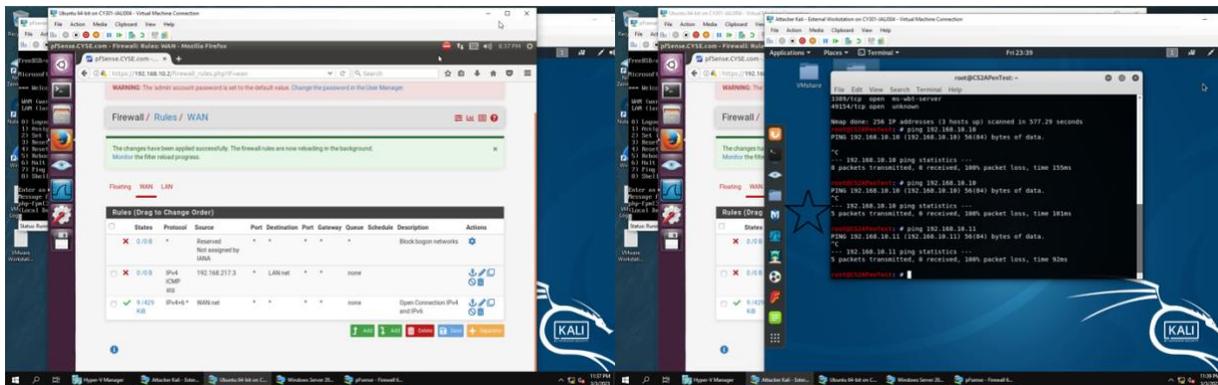
1. Configured the pfSense firewall rule to block the ICMP traffic from External Kali to Ubuntu VM and tested using ping command to communicate with Ubuntu because the ping command falls into the ICMP category. The ping was unsuccessful, therefore firewall rule is working. I also used the ping command to contact Windows 2008, which was successful because it is not a destination I excluded in my firewall rule.

Rule #	Interface	Action	Source IP	Destination IP	Protocol /Port #
2	WAN	BLOCK	192.168.217.3	192.168.10.10	ICMP/ N/A



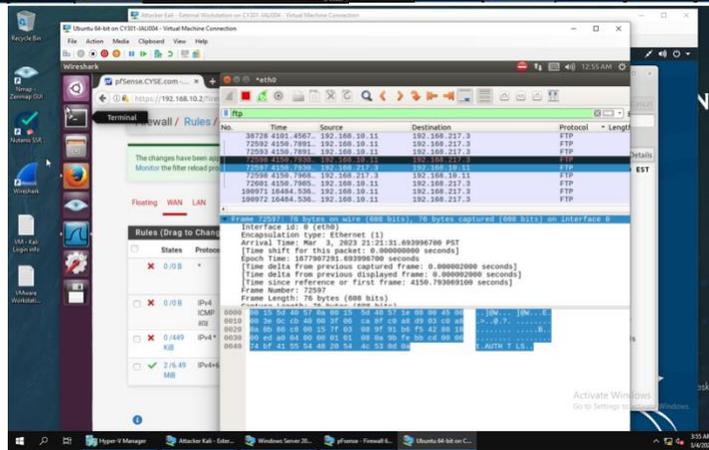
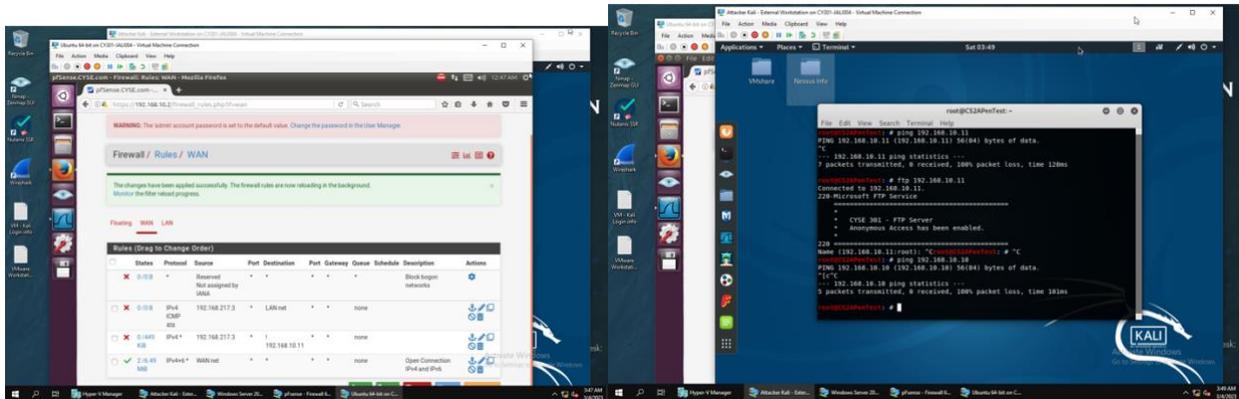
2. Cleared the previous firewall policies and configured the pfSense firewall to block all ICMP traffic from External Kali to the LAN side and tested using ping command for my LAN network (Ubuntu, Windows 2008). Successful ping, no packets transferred, successful firewall rule. Also tested by creating FTP traffic by trying to access from external Kali, this was successful because I did not create an additional rule to block this traffic.

Rule #	Interface	Action	Source IP	Destination IP	Protocol /Port #
2	WAN	BLOCK	192.168.217.3	ALL LAN	ICMP/ N/A



3. Cleared the previous firewall policies and configured the pfSense firewall to block ALL traffic from External Kali to the LAN side, except for the **FTP protocol** towards Windows Server 2008. This took me two rules to achieve, the first blocks ICMP traffic from Ext Kali to my Lan net and then the next rule blocks all the FTP traffic towards Windows from Ext Kali. I tested this by using the ping command and creating FTP traffic from Ext Kali. This time there weren't any successful pings and the only successful FTP connection was between Ext Kali and Windows 2008 as pictured below. I double checked this by looking at Wireshark from Ubuntu and adding the ftp display filter to see where my ftp traffic was coming and going, as in the destination and source IPs of Ext Kali and Windows 2008. I wanted to double check that this indeed was the only traffic FTP happening and it was.

Rule #	Interface	Action	Source IP	Destination IP	Protocol /Port #
2	WAN	BLOCK	192.168.217.3	LAN NET	ICMP/N/A
3	WAN	BLOCK EXCEPT !	192.168.217.3	LAN NET BUT !192.168.10.11	BLOCK FTP(TCP) 21



4. I kept the firewall policies I created in Task B.3 and repeated Task A.1. The difference is substantial because pfSense is still up, but Ubuntu and Windows 2008 are not. This is an important portion because I know they are running but the firewall rules I created are preventing the nmap scan to be completed because I blocked ICMP traffic. No pings mean no communication, and no communications means no data for zenmap to display for me on the GUI. I have included screenshots below for future reference:

