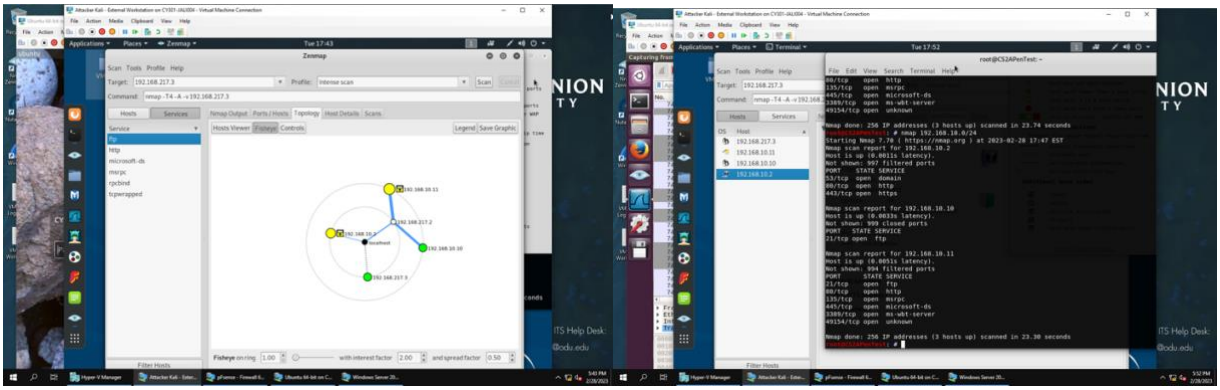
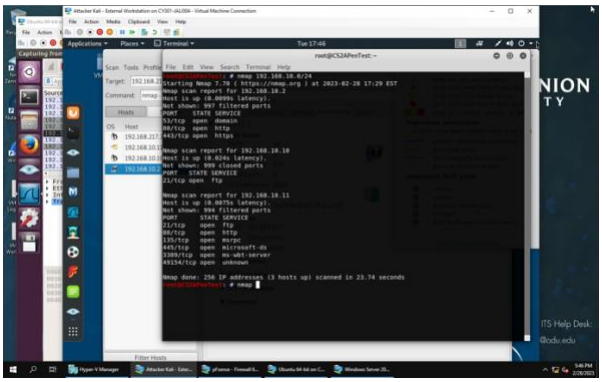
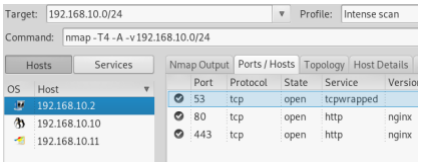
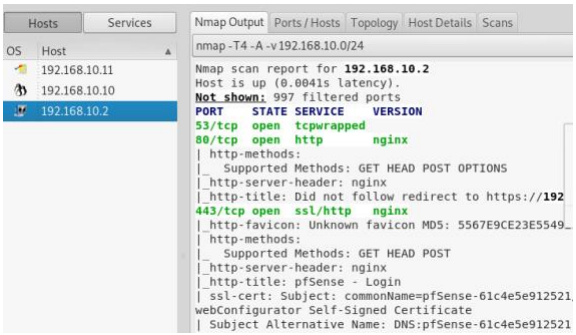
Task A: Sword-Network Scanning



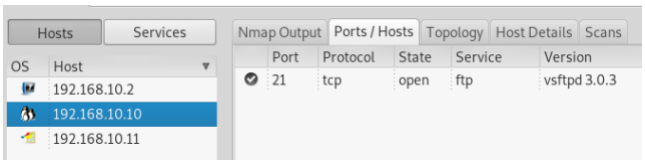


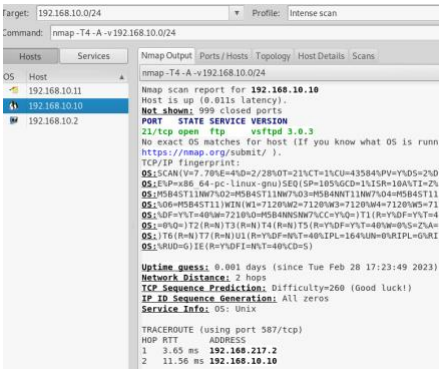
192.168.10.2



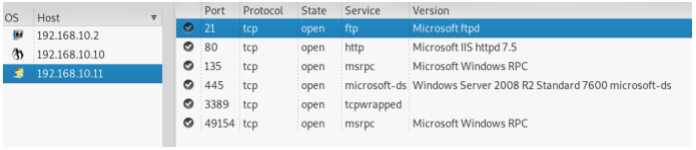



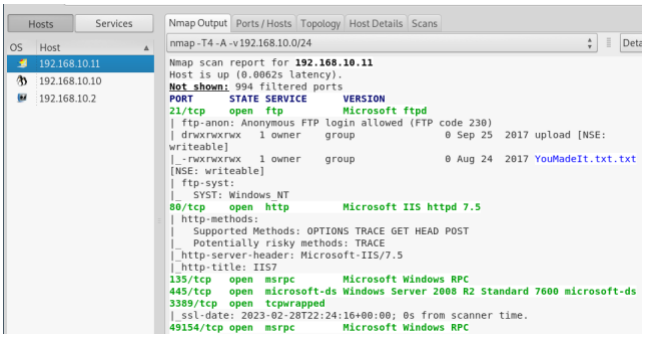

192.168.10.10



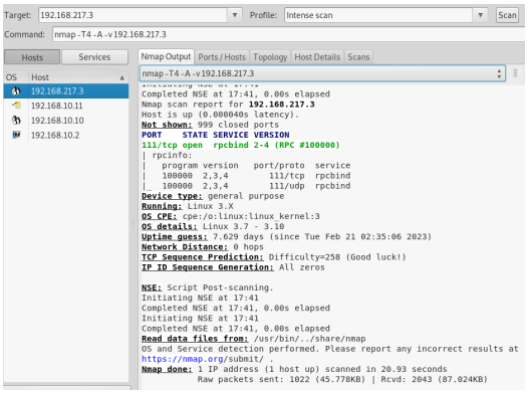




192.168.10.11

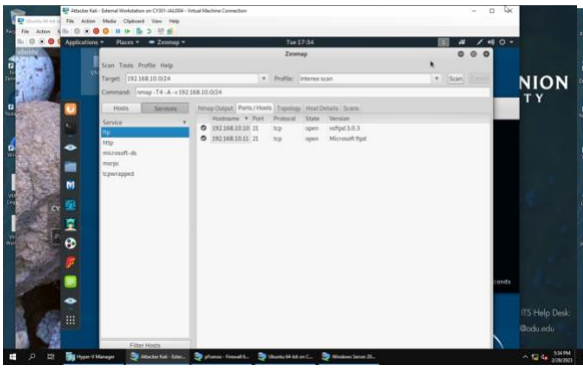


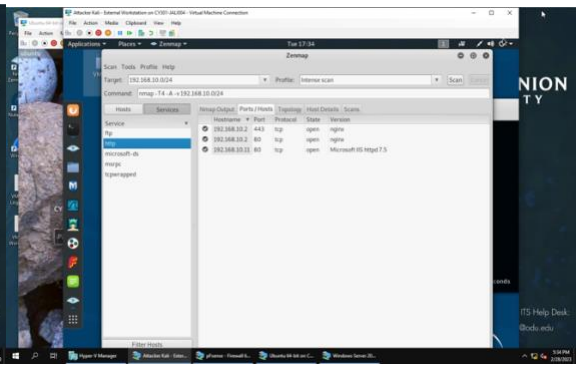



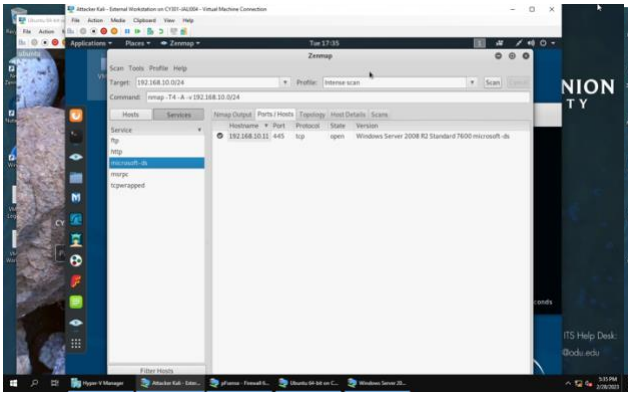

192.168.217.3

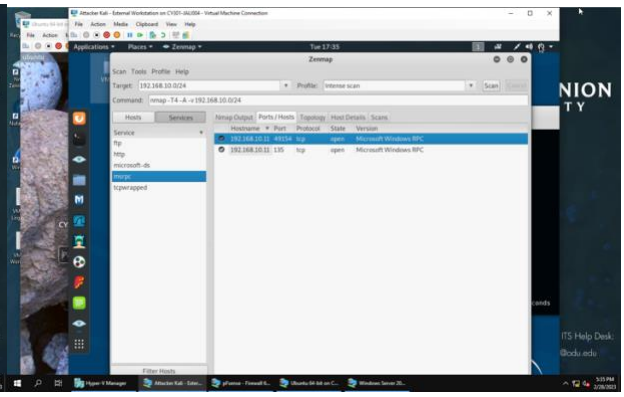


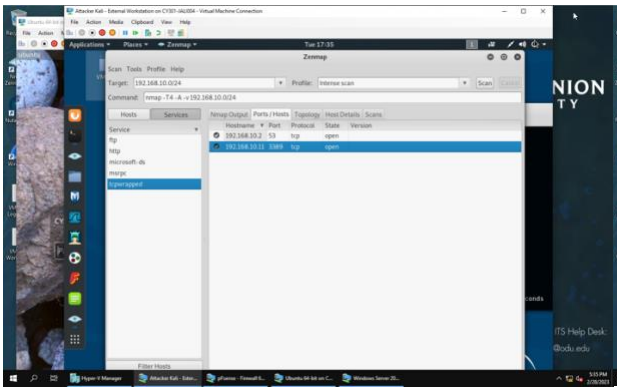
# OBSERVING FTP, HTTP, TCP PORTS

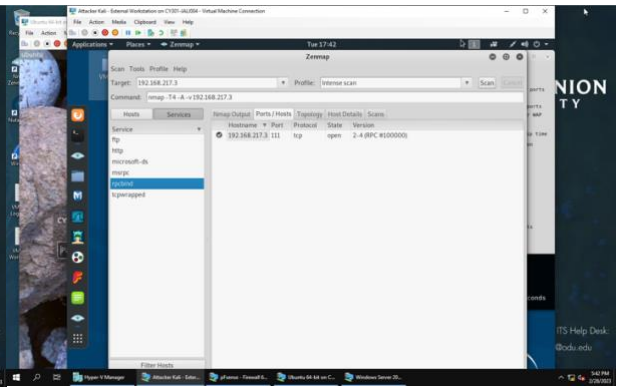




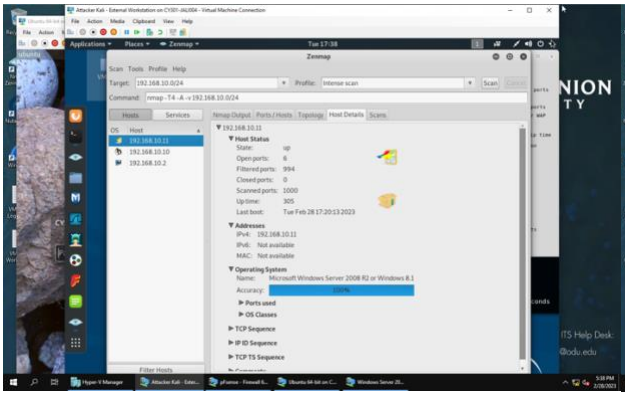


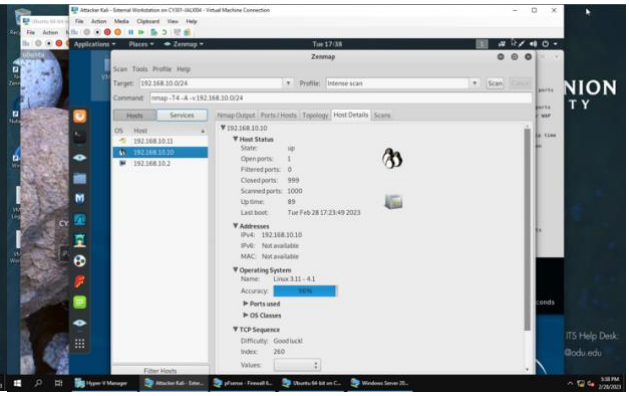


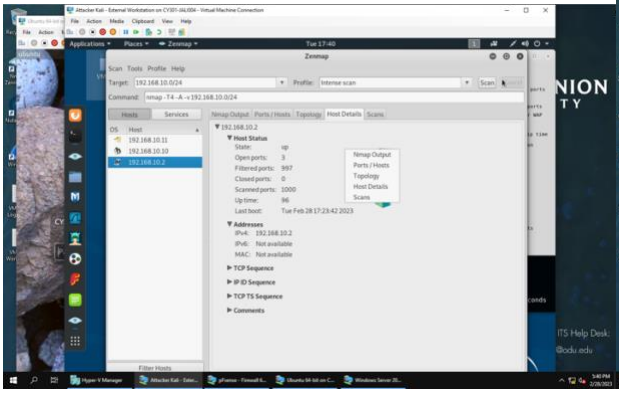


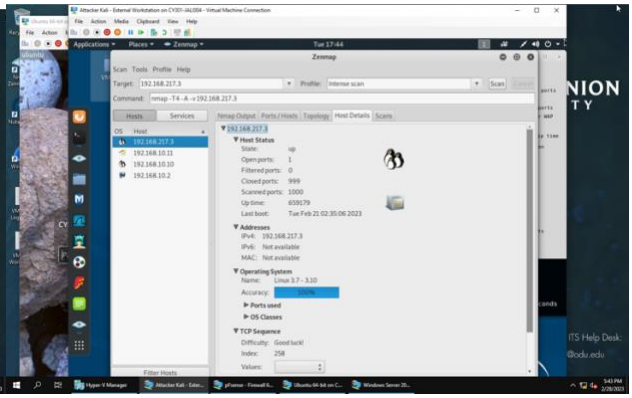


# Host Details





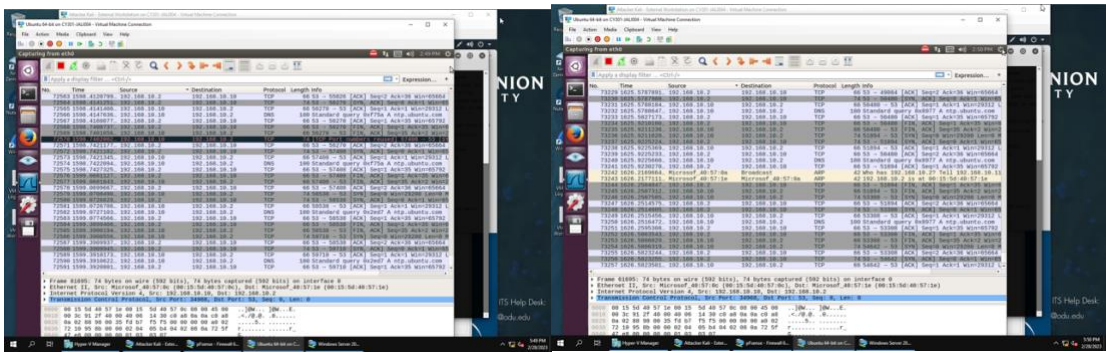




## TABLE SUMMARY

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

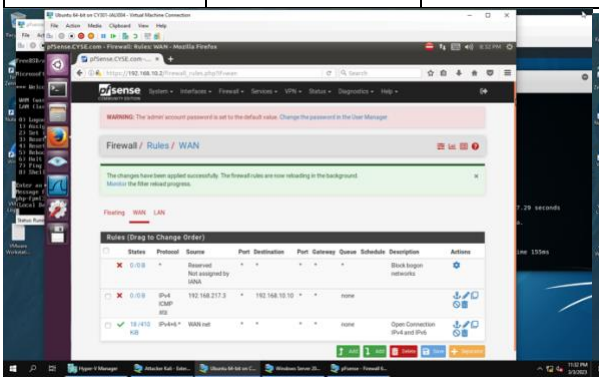
2. Ran Wireshark in Ubuntu VM while External Kali is scanning the network and discussion of traffic pattern observed below. An overall summary of the traffic patterns observed is that TCP, DNS, and ARP were flowing. There were no firewall rules, apart from the default, in place yet, so I could ping from 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.

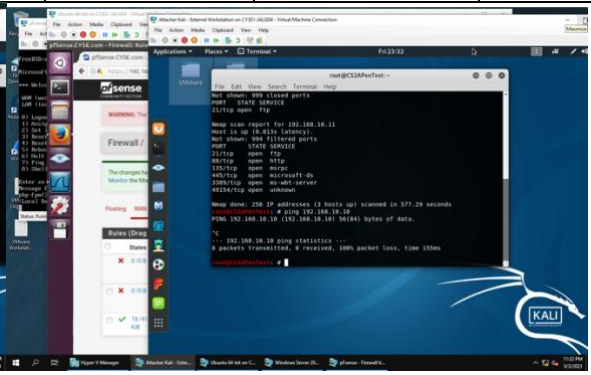


# TASK B: SHIELD-PROTECT NETWORK

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.

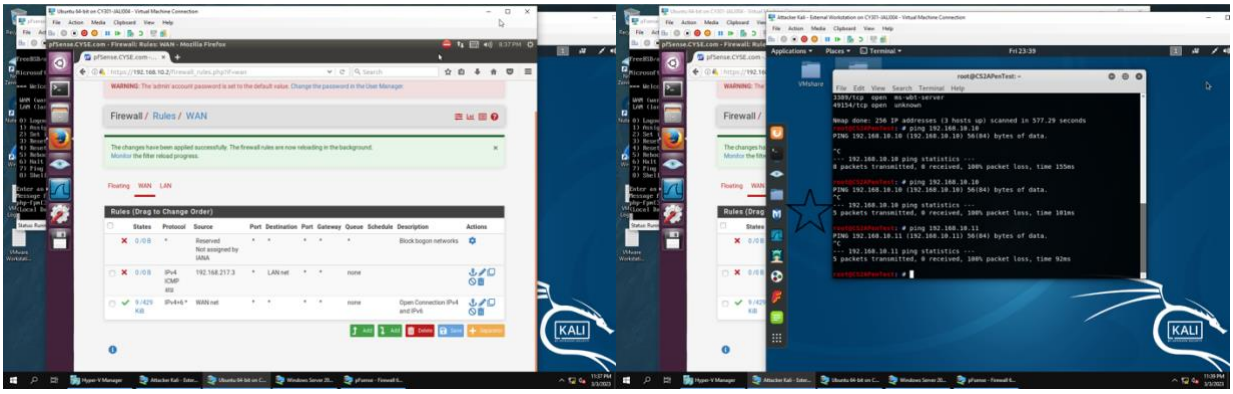
| Rule # | Interface | Action | Source IP | Destination IP | Protocol /Port # |
|---|---|---|---|---|---|
| 2 | WAN | BLOCK | 192.168.217.3 | 192.168.10.10 | ICMP/ N/A |





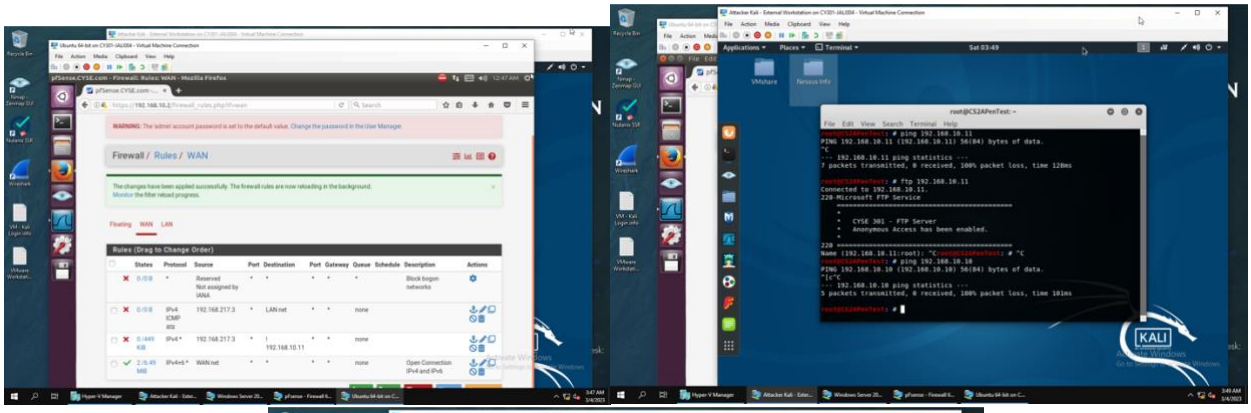
2. Cleared the previous firewall policies and configured the pfSense firewall to block all ICMP traffic from External Kali to the LAN side and tested using ping command for my LAN network (Ubuntu, Windows 2008). Saucerful ping, no packets transferred, successful firewall rule. Also tested by creating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

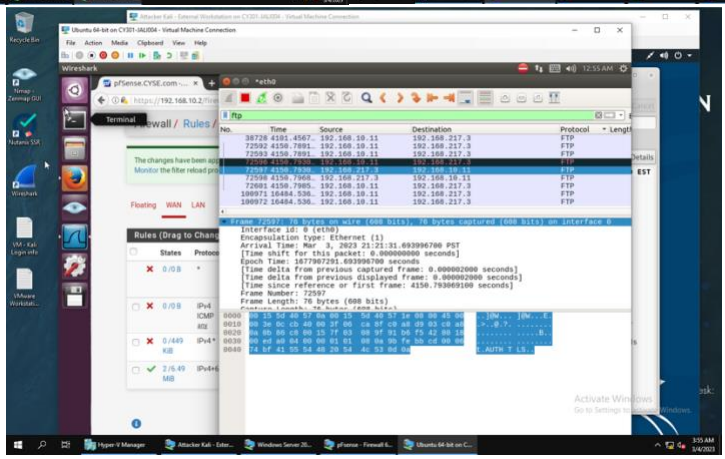
| Rule # | Interface | Action | Source IP | Destination IP | Protocol /Port # |
|---|---|---|---|---|---|
| 2 | WAN | BLOCK | 192.168.217.3 | ALL LAN | ICMP/ N/A |



3. Cleared the previous firewall polices 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 my 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 sources 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<br>EXCEPT ! | 192.168.217.3 | LAN NET BUT<br>!192.168.10.11 | BLOCK<br>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: