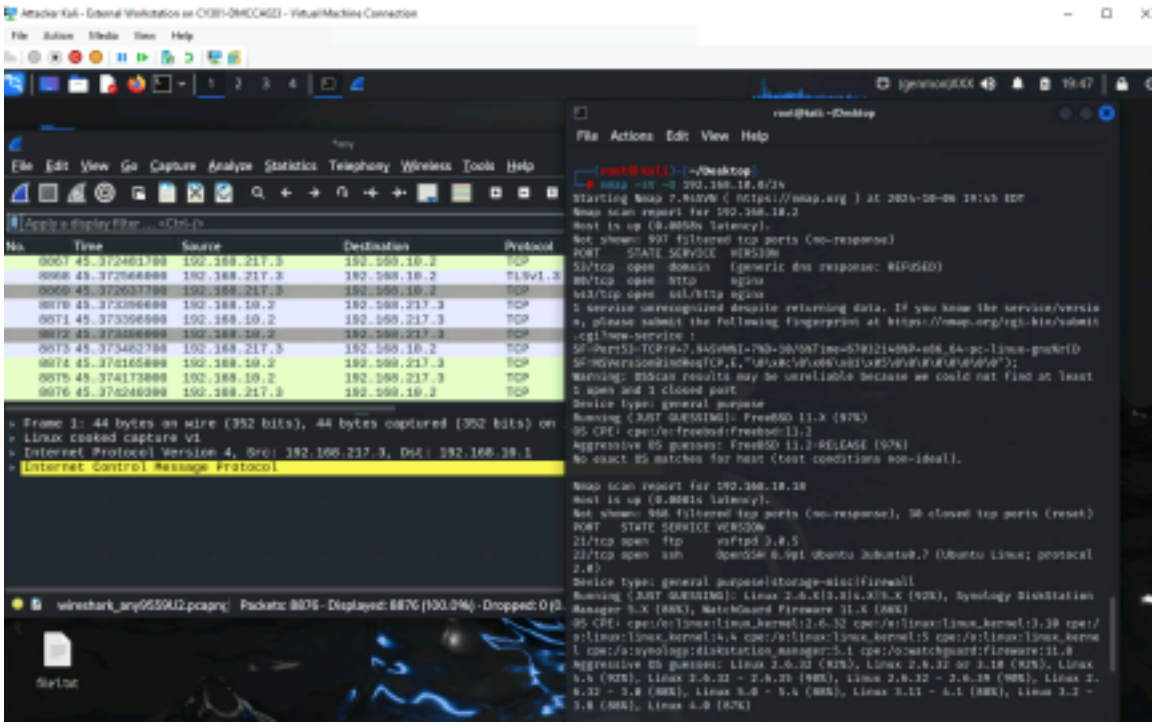
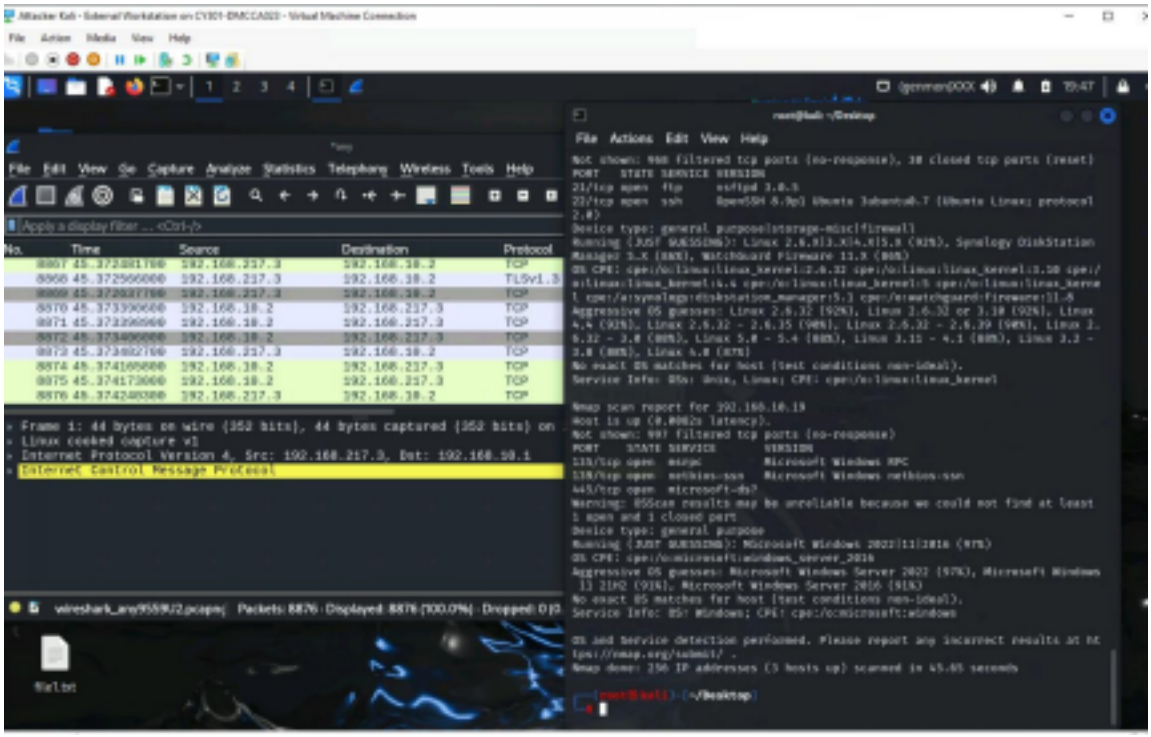
Dylan McCann	CYSE 301	Sword vs. Shield

Task A: Q1: 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

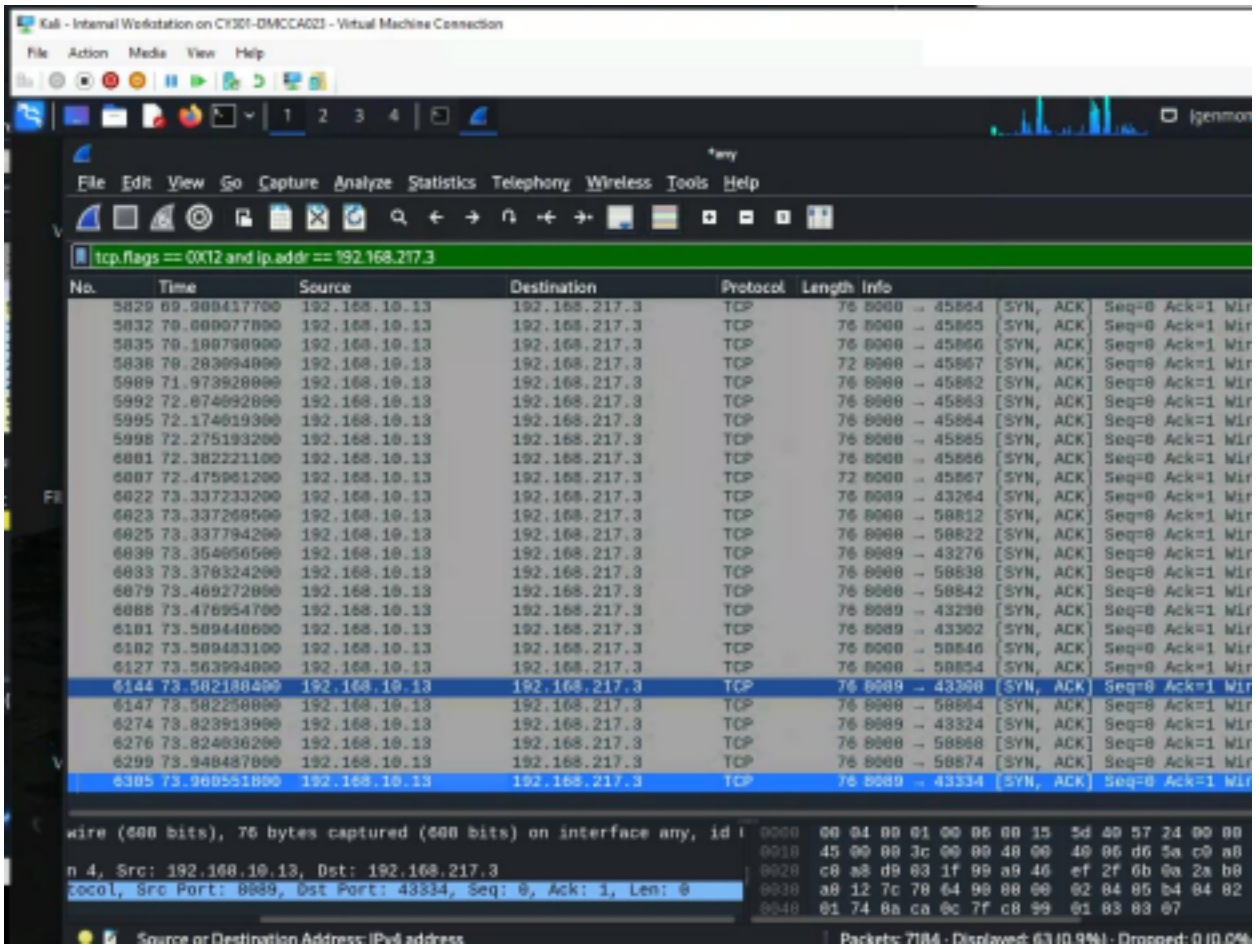




I used nmap –sV –O 192.168.10.0/24 to do a subnet scan for ports and OS detection

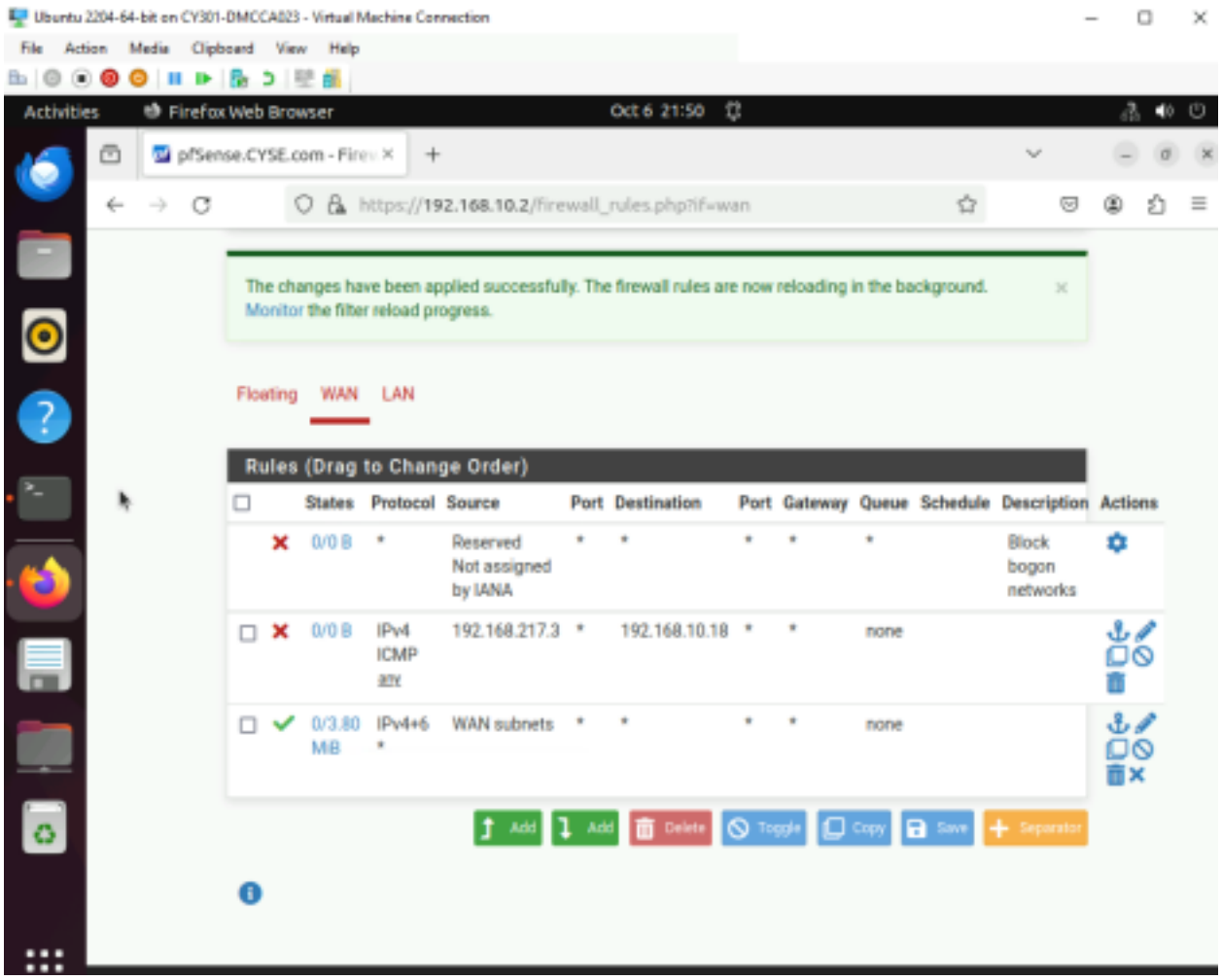
Task A Q2: Run Wireshark in Internal Kali VM while External Kali is scanning the network. Discuss the traffic pattern you observed. What do you find? Please write a 200-word essay to discuss your findings

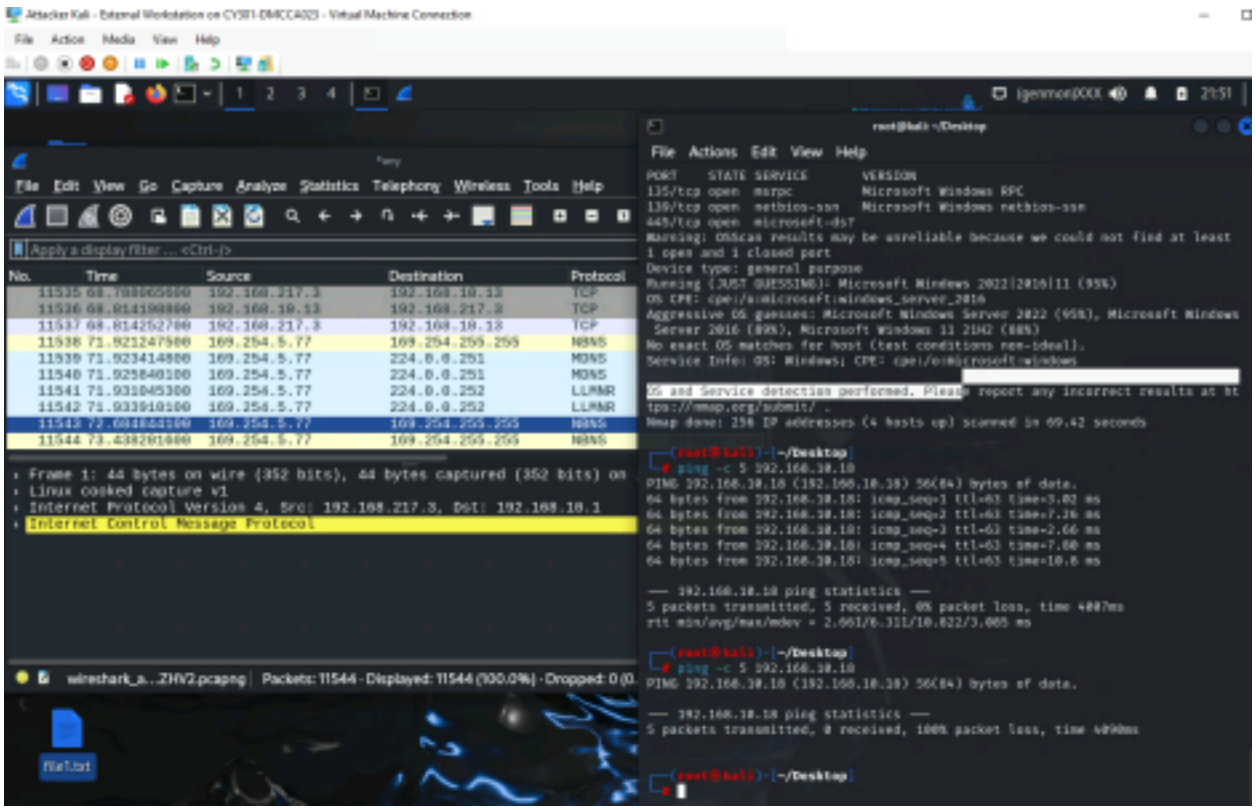
I filtered wireshark using ip.addr == 192.168.217.3 to only see communication that involved the external kali workstation. After browsing the log, I noticed that the external kali VM was sending SYN requests to scan for open ports on 192.168.10.13 IP. I believe it was trying to complete a three-way handshake to test which ports were open and which were blocked. After filtering wireshark using ip.addr == 192.168.217.3 and tcp.flags.syn == 1 and tcp.flags.ack == 1 I was able to see when the internal kali station was sending ack requests to the external kali to allow for a connection. Filtering using ip.addr == 192.168.217.3 && ip.addr == 192.168.10.13 and tcp.flags.syn == 1 and tcp.flags.ack == 1 I can see the direct communication between the internal and external kali through the accepted SYN and ACK packets. Filtering using tcp.flags == 0X12 and ip.addr == 192.168.217.3 I can see only when a SYN, ACK packet goes back to the external kali VM showing that the internal Kali VM is allowing connection to this port, open ports were found on 8089 and 8000



Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if applicable)

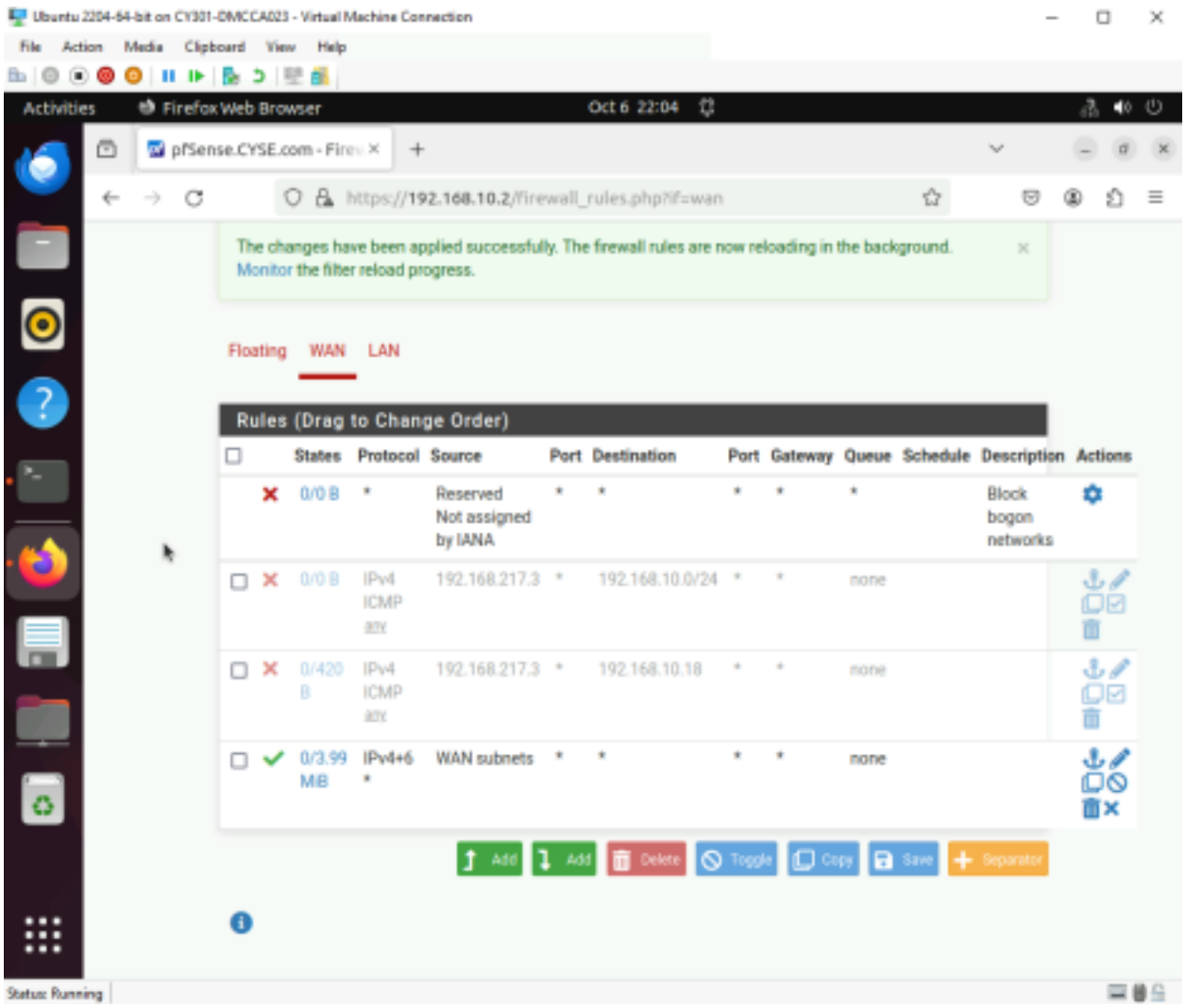
1	WAN	block	192.168.217.3	192.168.1 0.1 8	ICMP

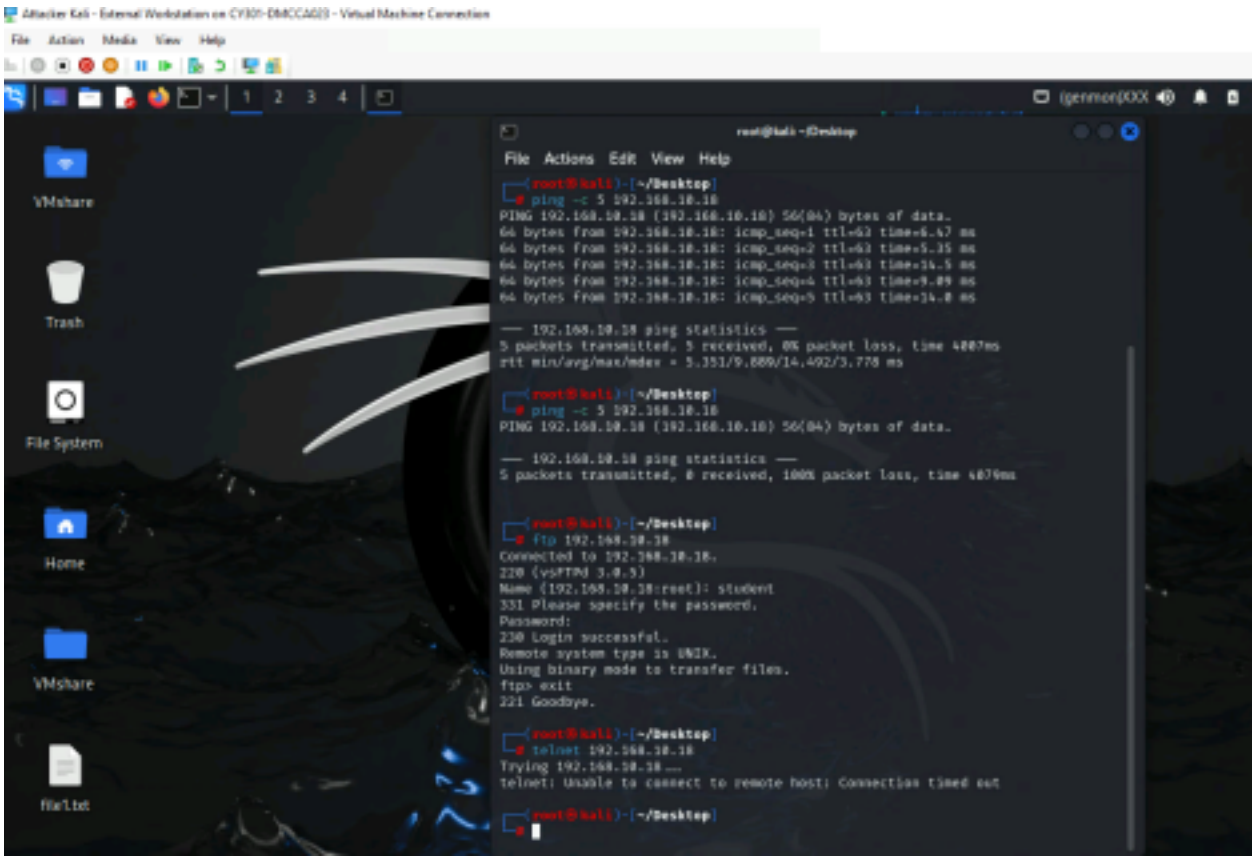




pinged the ubuntu server 5 times on 2 separate occasions using ping –c 192.168.10.18, once before applying changes to show connection to server and once after applying changes to see transmission being blocked

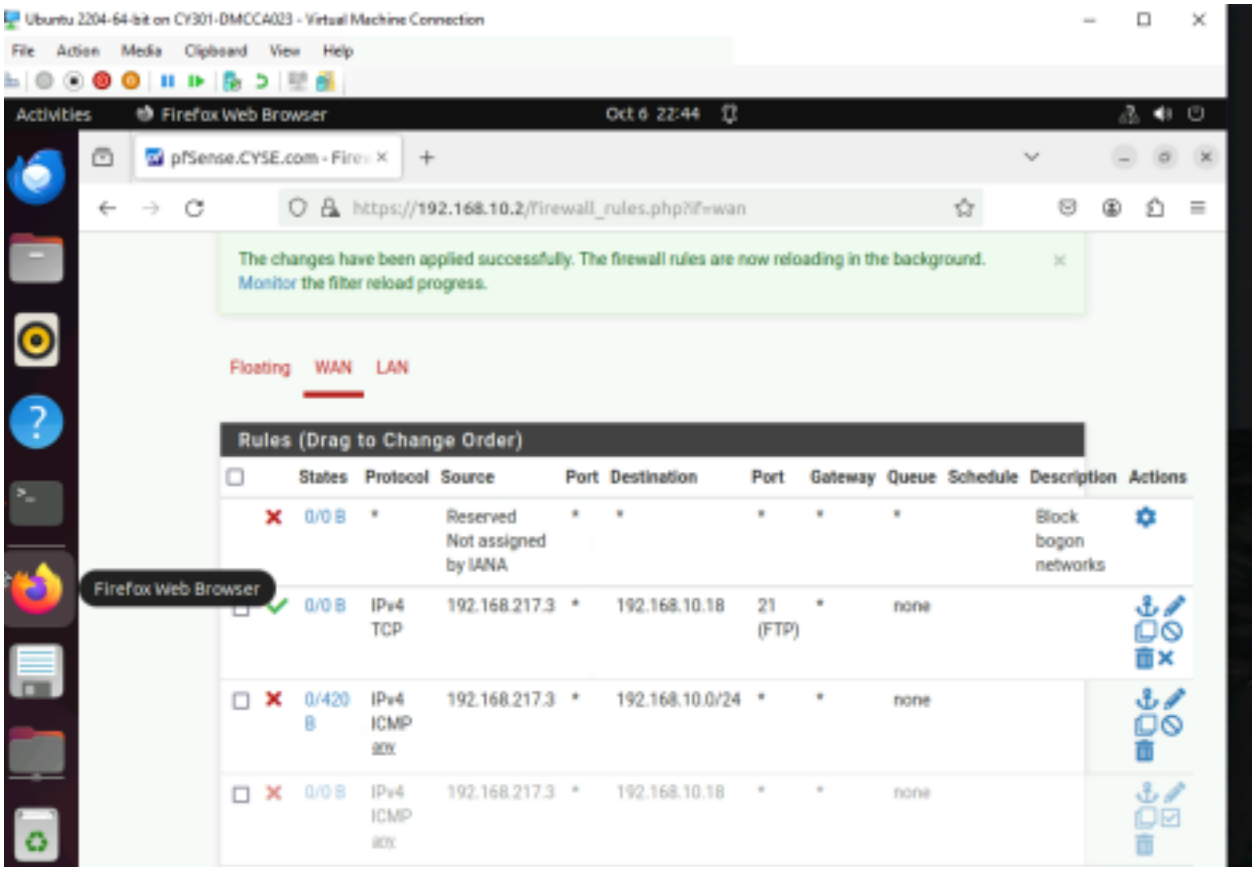
Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if applicable)
1	WAN	block	192.168.217.3	192.168.10 .0/ 24	ICMP

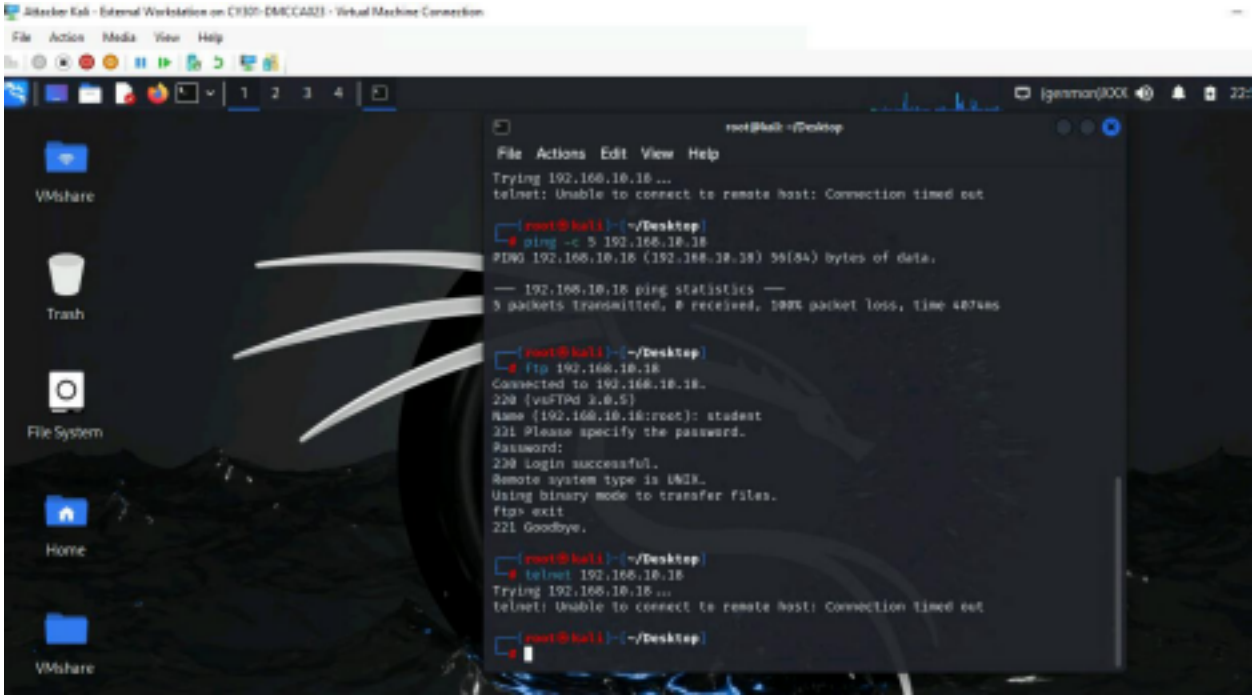

Ubuntu 2204-64-bit on CY301-DMCCA023 - Virtual Machine Connection
File Action Media Clipboard View Help
Activities
Firefox Web Browser
Oct 6 22:04
pfSense.CYSE.com - Firew
https://192.168.10.2/firewall_rules.php?if=wan
The changes have been applied successfully. The firewall rules are now reloading in 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
Actions
0/0 B
*
Reserved Not assigned by IANA
*
*
*
*
*
Block bogon networks
0/0 B
IPv4 ICMP any
192.168.217.3
*
192.168.10.0/24
*
*
none
0/420 B
IPv4 ICMP any
192.168.217.3
*
192.168.10.18
*
*
none
0/3.99 MiB
IPv4+6 *
WAN subnets
*
*
*
*
none
Add
Add
Delete
Toggle
Copy
Save
Separator
Status: Running

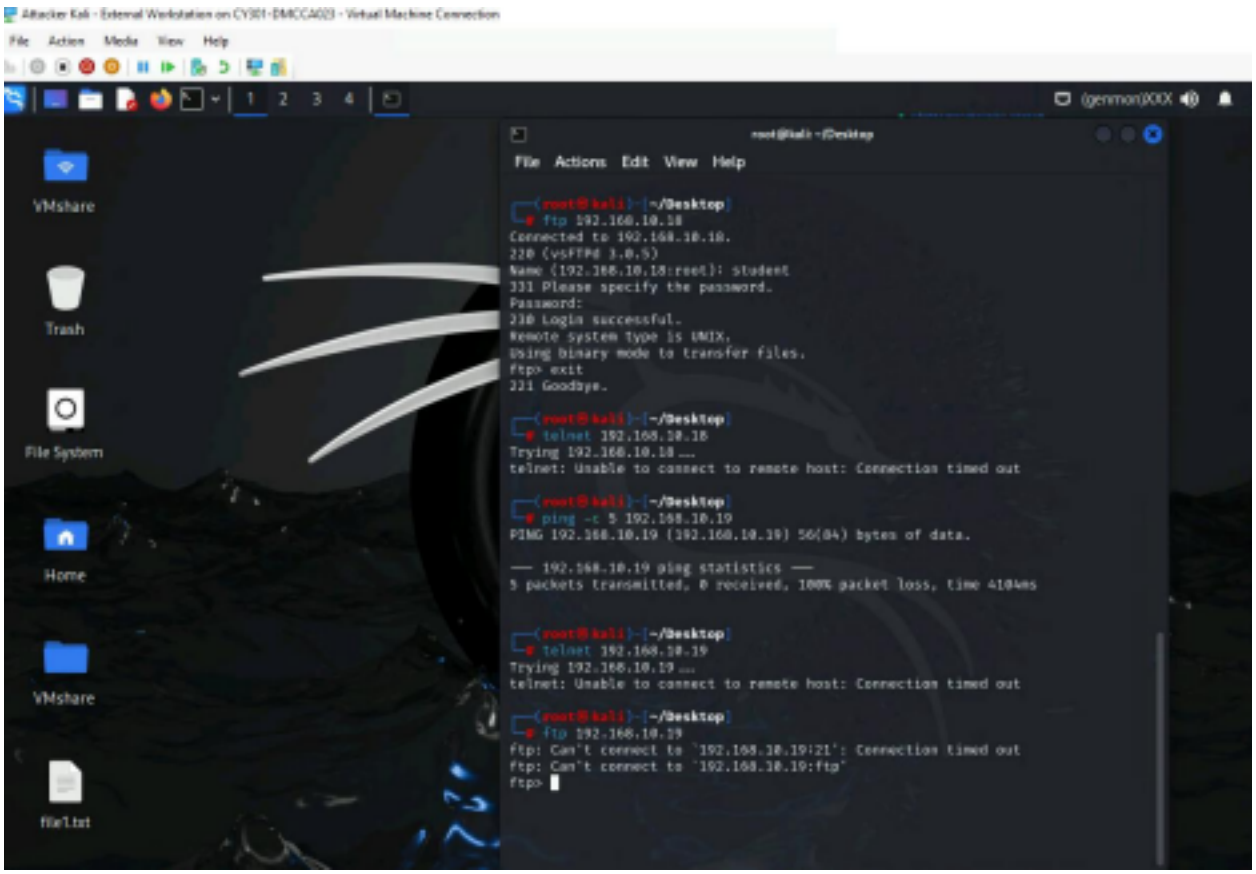


Toggled both blockers off to run a ping test to make sure attacker could still connect to ubuntu and then toggled new blocker back on before running ping, ftp, and telnet tests, the ping and telnet tests failed to connect to ubuntu but the ftp test was successful

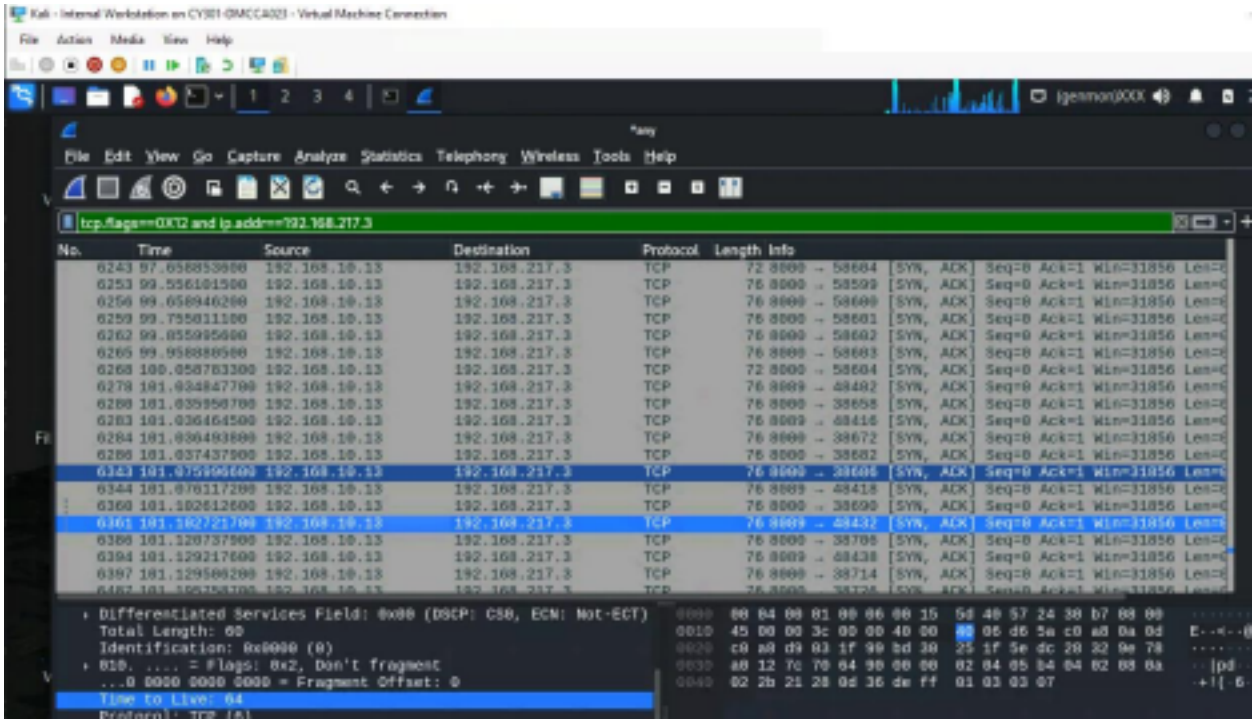
Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if applicable)
1	WAN	block	192.168.217.3	192.168.10.1 8	ICMP
2	WAN	Pass	192.168.217.3	192.168.10.1 8	FTP (21)


Ubuntu 2204-64-bit on CY301-DMCCA023 - Virtual Machine Connection
File Action Media Clipboard View Help
Activities
Firefox Web Browser
Oct 6 22:44
pfSense.CYSE.com - Firewall: Rules
https://192.168.10.2/firewall_rules.php?if=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
Actions
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
0/420 B
IPv4 ICMP any
192.168.217.3
192.168.10.0/24
none
0/0 B
IPv4 ICMP any
192.168.217.3
192.168.10.18
none
Firefox Web Browser


Attacker Kali - External Workstation on CY301-DMCCA023 - Virtual Machine Connection
File Action Media View Help
VMshare
Trash
File System
Home
VMshare
File Actions Edit View Help
Trying 192.168.10.18 ...
telnet: Unable to connect to remote host: Connection timed out
ping -c 5 192.168.10.18
PING 192.168.10.18 (192.168.10.18) 56(84) bytes of data.
--- 192.168.10.18 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4074ms
ftp 192.168.10.18
Connected to 192.168.10.18.
220 (vsFTPd 3.0.5)
Name (192.168.10.18:root): student
221 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> exit
221 Goodbye.
telnet 192.168.10.18
Trying 192.168.10.18 ...
telnet: Unable to connect to remote host: Connection timed out



After setting up the new firewalls, I ping and telnet connections to both windows and Ubuntu servers and failed to connect through ftp to the windows server but was able to connect to the ubuntu server



After running same commands and recording in kali internal, there does not seem to have been any difference in traffic, I'm not completely sure why or what is wrong.