Old Dominion University

CYSE 301 Cybersecurity Techniques and Operations

Assignment #3 Shield vs Sword

Bradley Hamilton

01240068

TASK A

1. Using Nmap to profile basic information about the subnet topology:

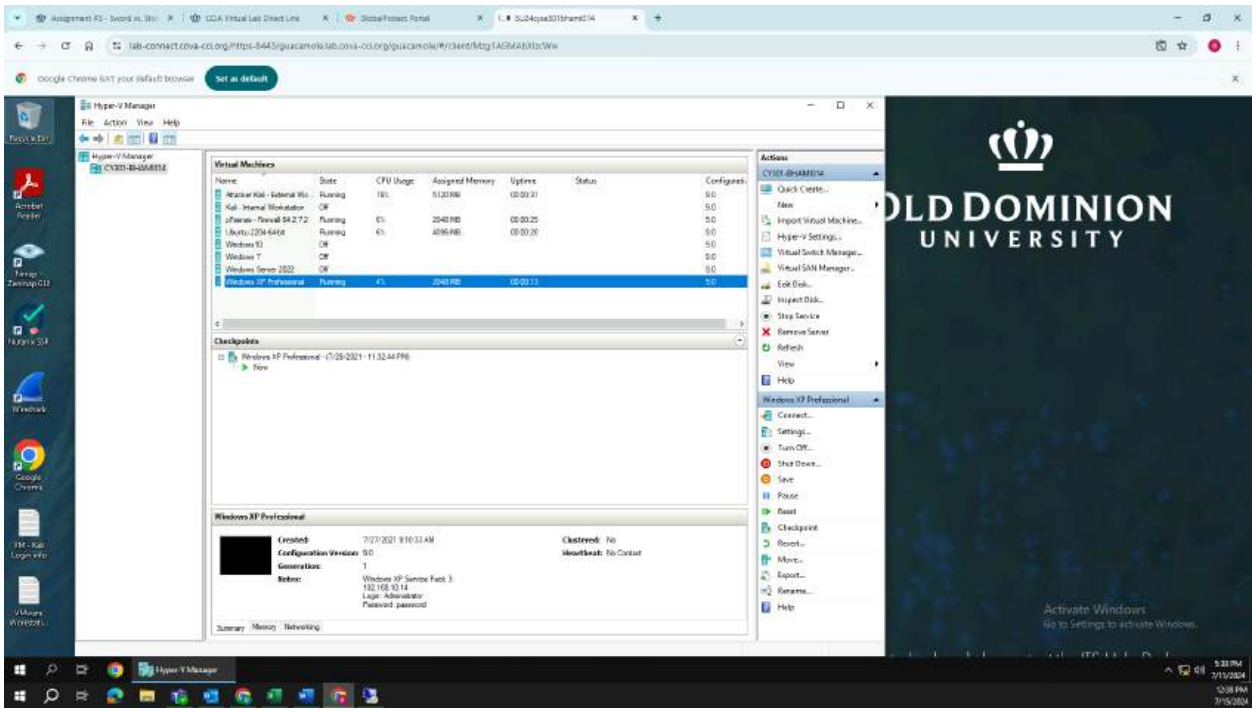


Figure 1 Screenshot of powered on VMs.

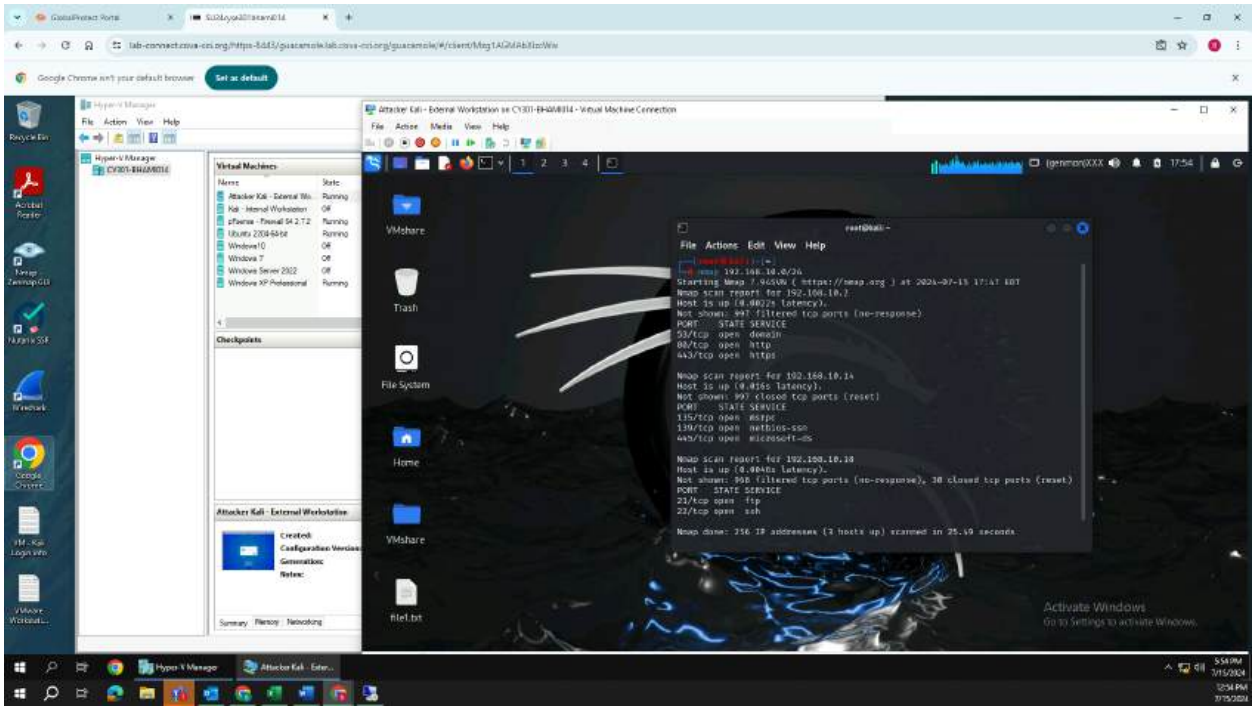


Figure 2 Screenshot of Nmap topology for IP addresses.

Figure 2 displays the Nmap topology for the IP addresses connected to the network. each one has specific ports attached to them and what software and service is associated with each one.

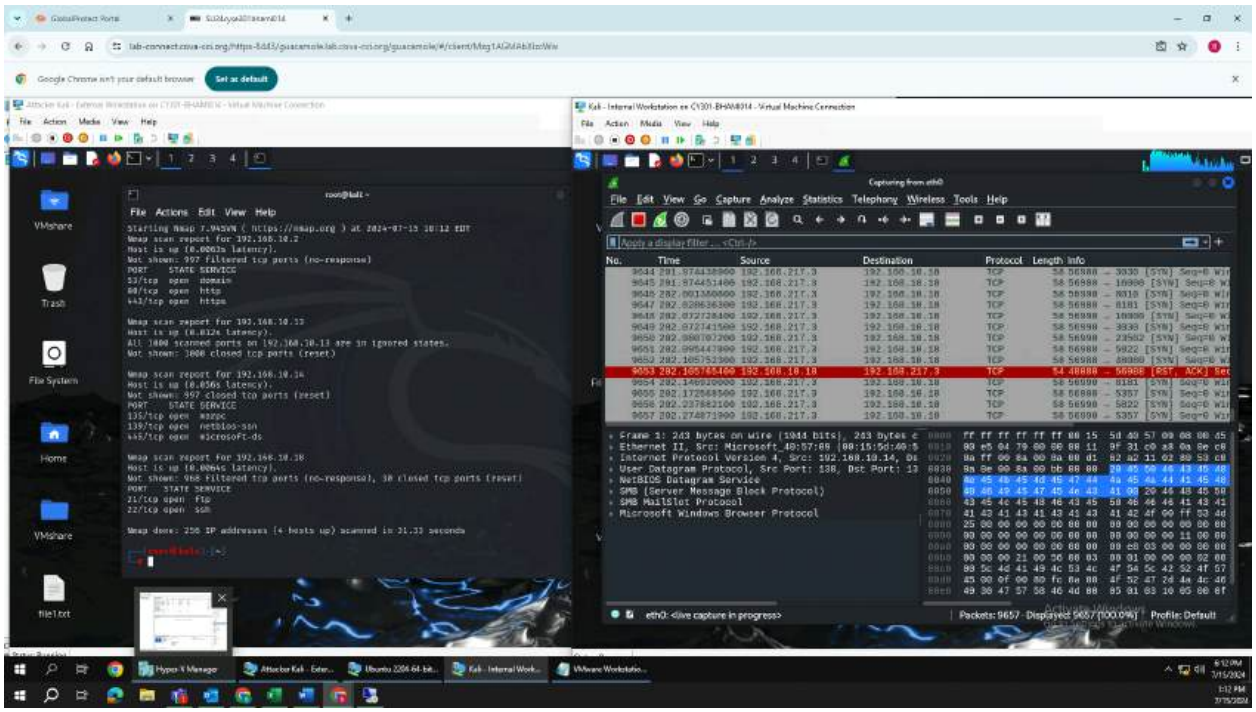


Figure 3 Screenshot of Wireshark while scanning network.

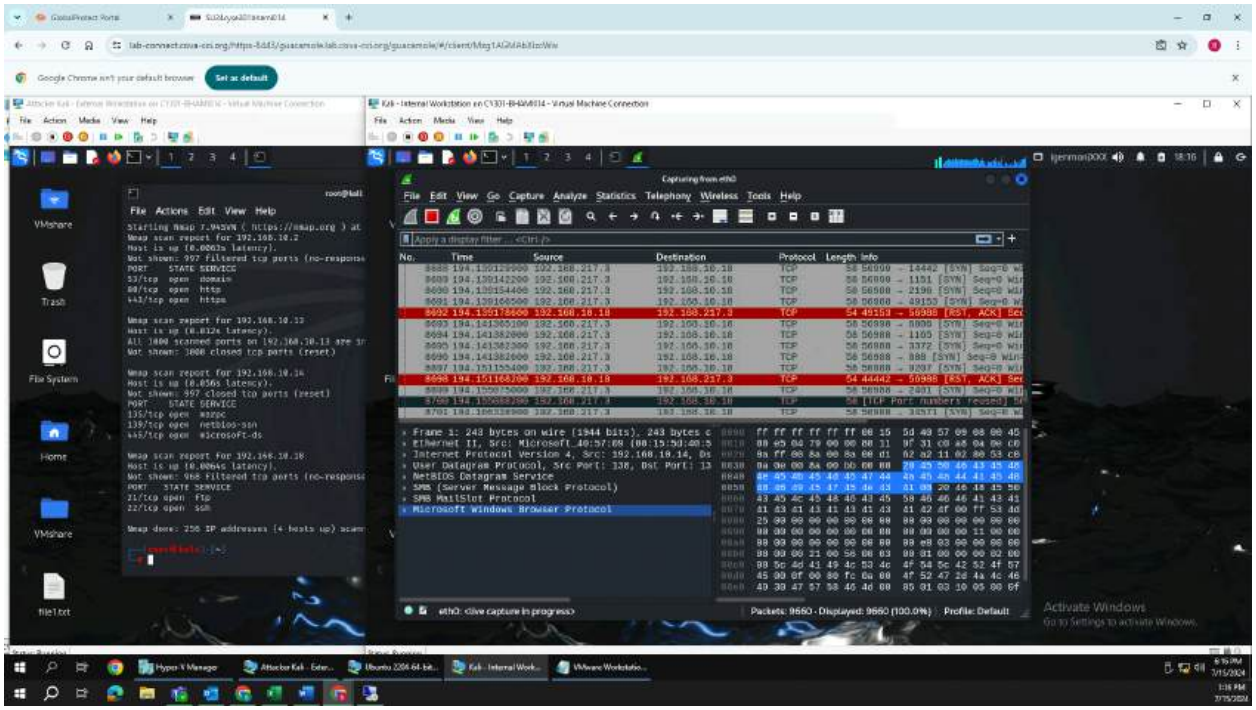


Figure 4 Screenshot of Wireshark while scanning network.

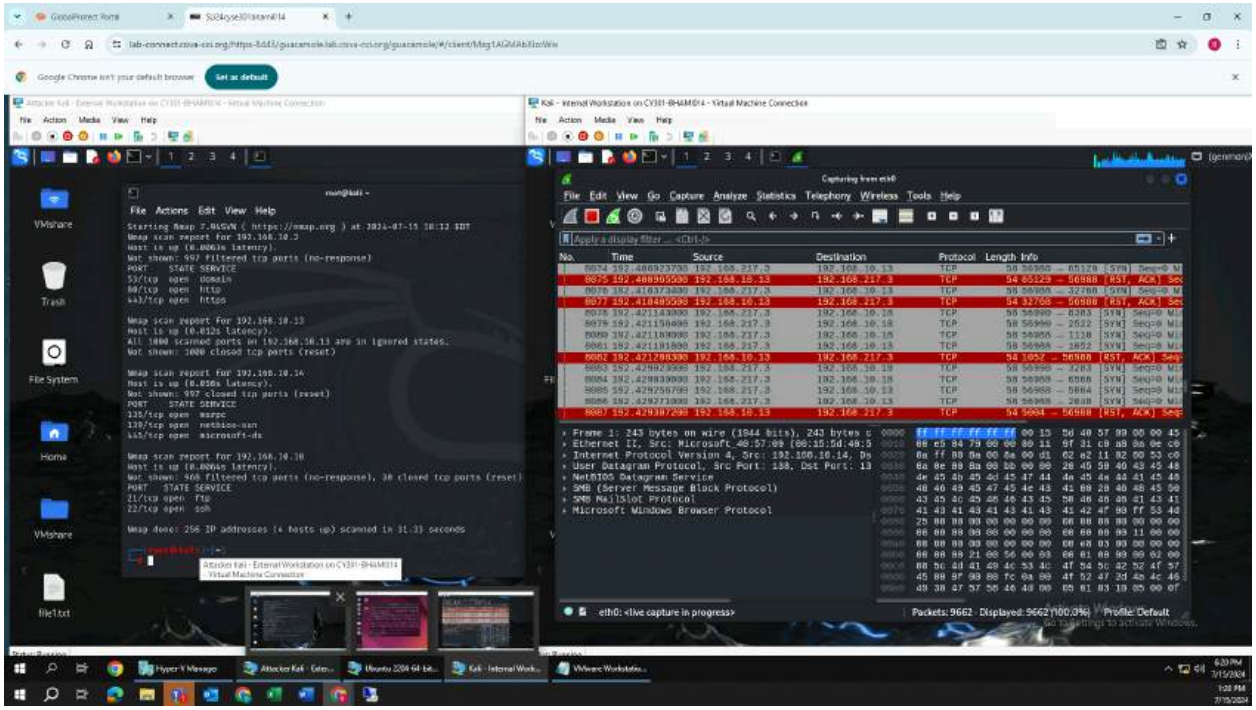


Figure 5 Screenshot of Wireshark while scanning network.

Figures 3 thru 5 all provide screenshots depicting the Wireshark program running and collecting data for the traffic patterns on the network. The Internal Kali was used in place of the Ubuntu VM due to issues arising, but the network was still able to be scanned with this method.

When observing the Wireshark program, one is able to see what kind of protocols are being sent and it details what the source and destination of each packet is. Much can be seen as to whether or not the packets are accepted or rejected and the highlights help to emphasize unusual traffic from the normal.

As far as sources go, it was seen that the majority of the packets that were transmitted had the source of the attacking (External Kali) VM. The ability to be able to see these intrusions or attacks would help defenses to be made and stop attacks that are occurring or could potentially occur because one would be able to detect any discrepancies or anomalies within the network. Being able to monitor a network would prove to be beneficial as any vulnerabilities can be seen when performing white-hat testing, allowing for security to strengthen any safeguards that are available in order to mitigate risks and vulnerabilities within the system.

TASK B

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)
1	WAN	BLOCK	192.168.217.3	192.168.10.18	ICMP
2	WAN	BLOCK	192.168.10.18	192.168.217.3	ICMP

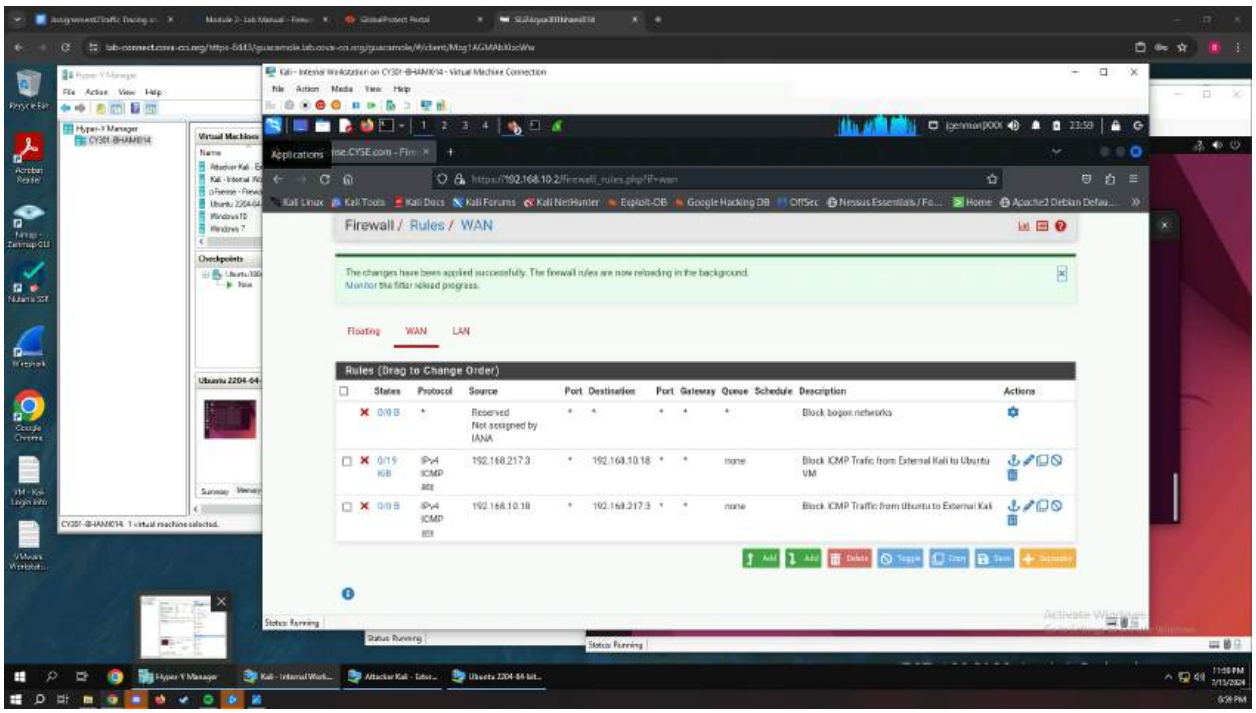


Figure 5 Screenshot of Firewall rules for ICMP Traffic block from External Kali to Ubuntu VM

Figure 5 shows the firewall rule configuration in order to block traffic from the Attack External Kali system to the Ubuntu VM. A second rule was put in place which blocks the inverse of packet transfer from the two systems, but this was put in place due to LAN rules that were still in place. Those rules were removed and the one rule (Attacker to Ubuntu VM) worked by itself.

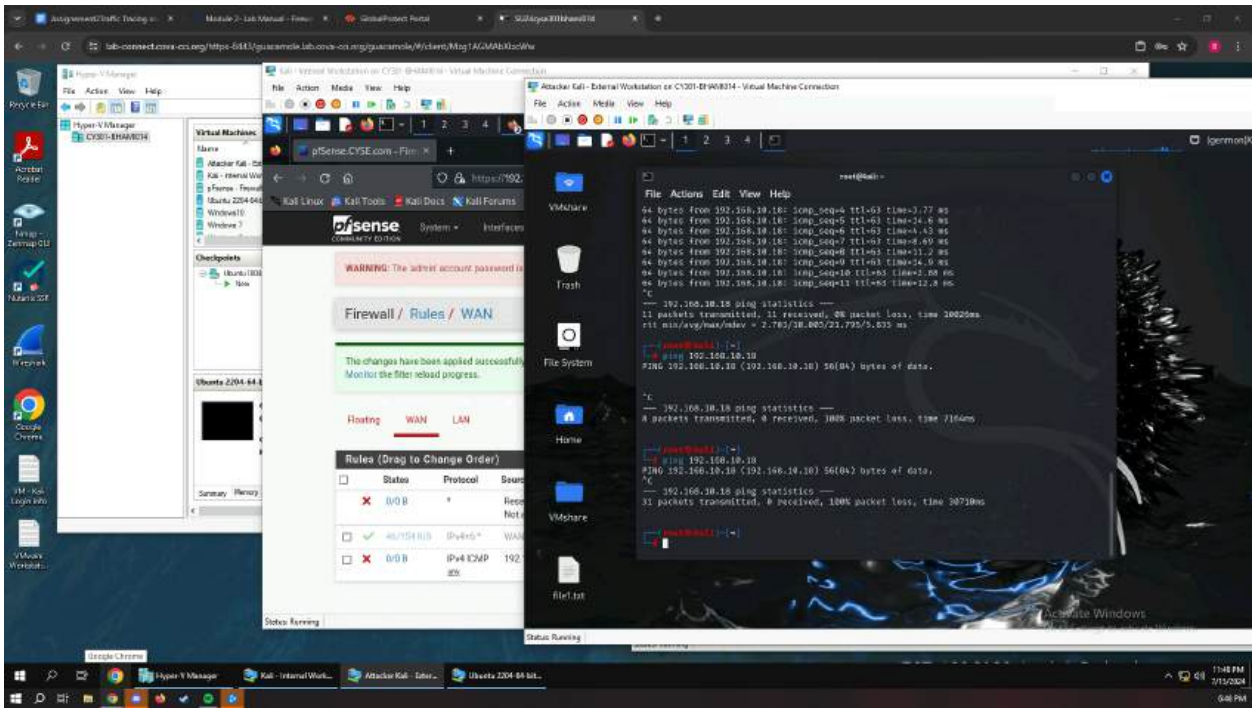
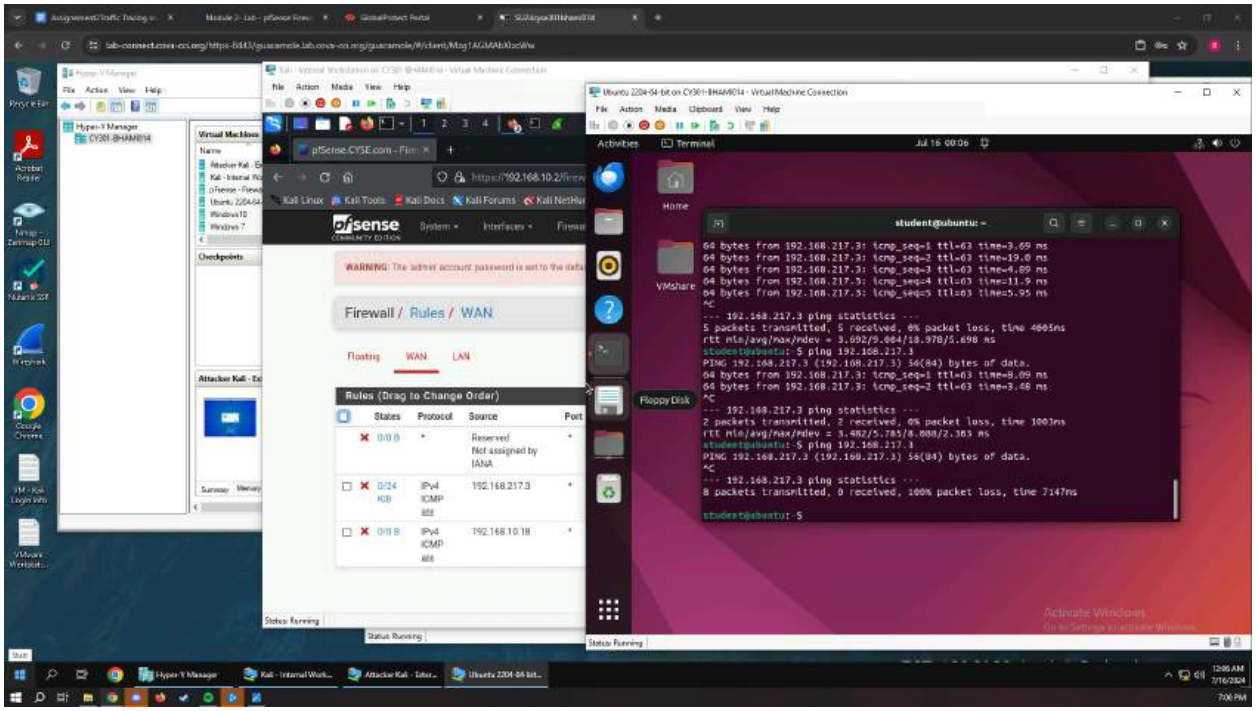


Figure 6 and 7 Screenshot of ping from External Kali to Ubuntu VM and vice versa



2. Clear 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)
1	LAN	BLOCK	192.168.217.3	ANY	ICMP

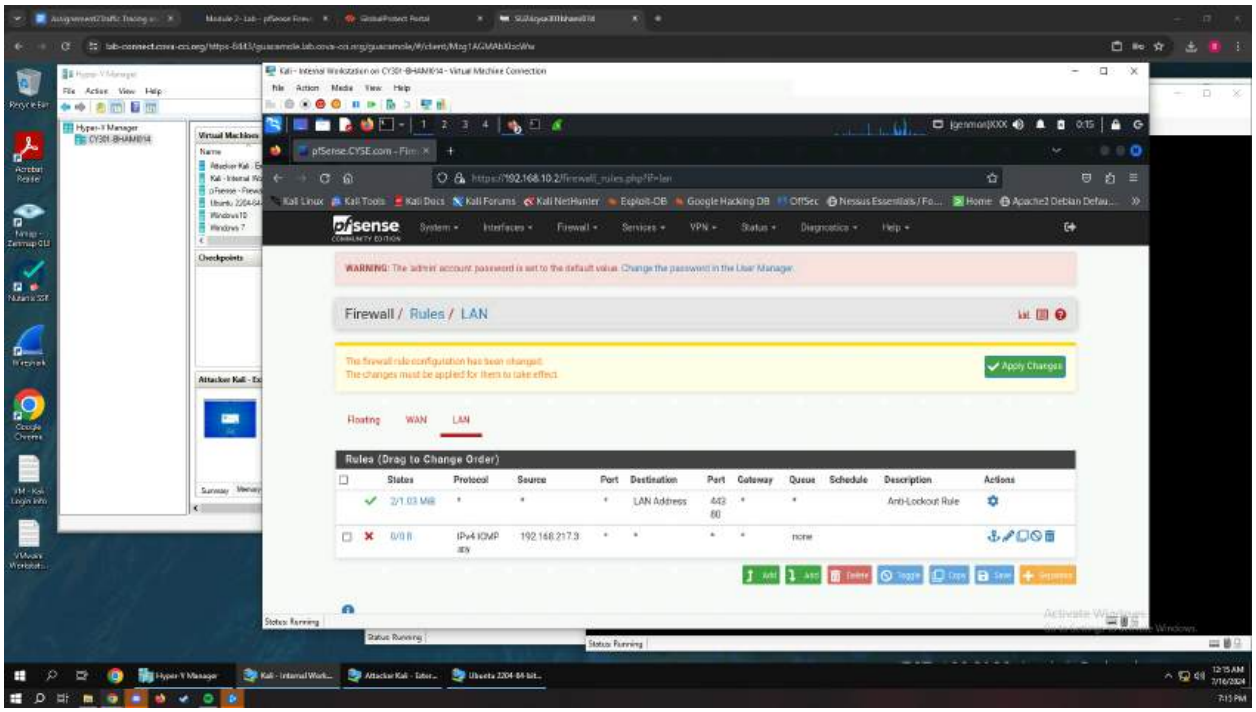


Figure 8 Screenshot of External Kali LAN block

Figure 9 shows the pings of each IP for the LAN VMs and that they are no longer able to transmit packets to the Attacker External Kali.

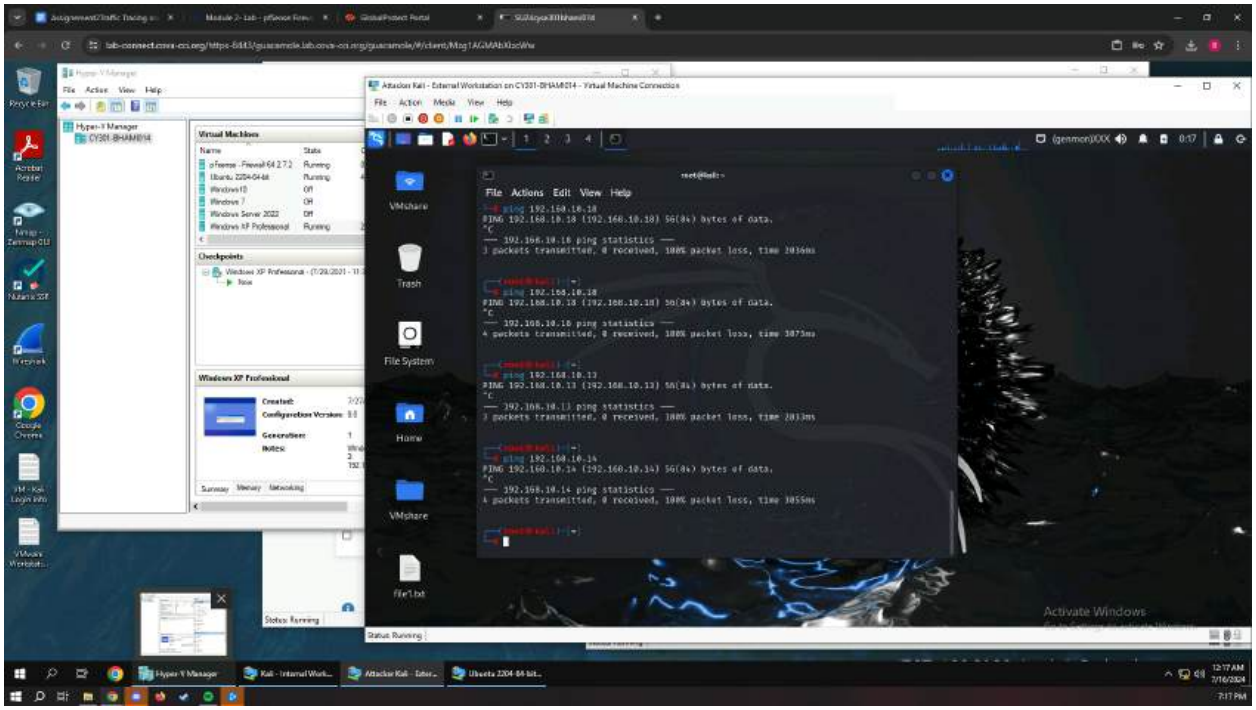


Figure 9 Screenshot of LAN block IP pings

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 SSH protocol towards Ubuntu:

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
1	LAN	BLOCK	192.168.217.3	ANY	ANY
2	LAN	PASS	192.168.217.3	192.168.10.18	PORT 22

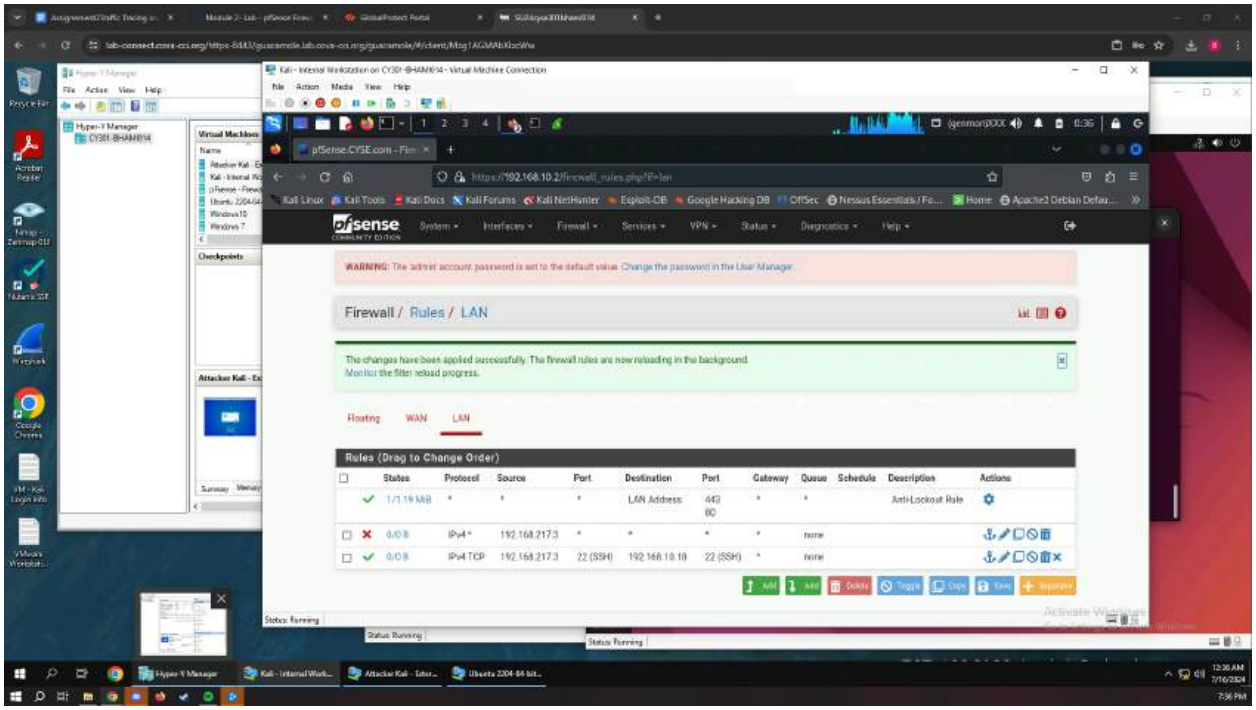


Figure 10 Screenshot of rules for Task B.3

Figure 10 and the table above show the rules used for Task B.3. With these rules packets were able to pass through to the Ubuntu VM, but not back to the source which causes the echoes because a reply is not sent back to the attacking External Kali.

Because of this, the traffic is different from the first Wireshark scan as all of the VMs in the network were able to communicate with each other and transmit packets without issue. However, with the rules in place, certain packets may be able to be sent across the network, but not replied to and ultimately many packets can be blocked from being received at all.

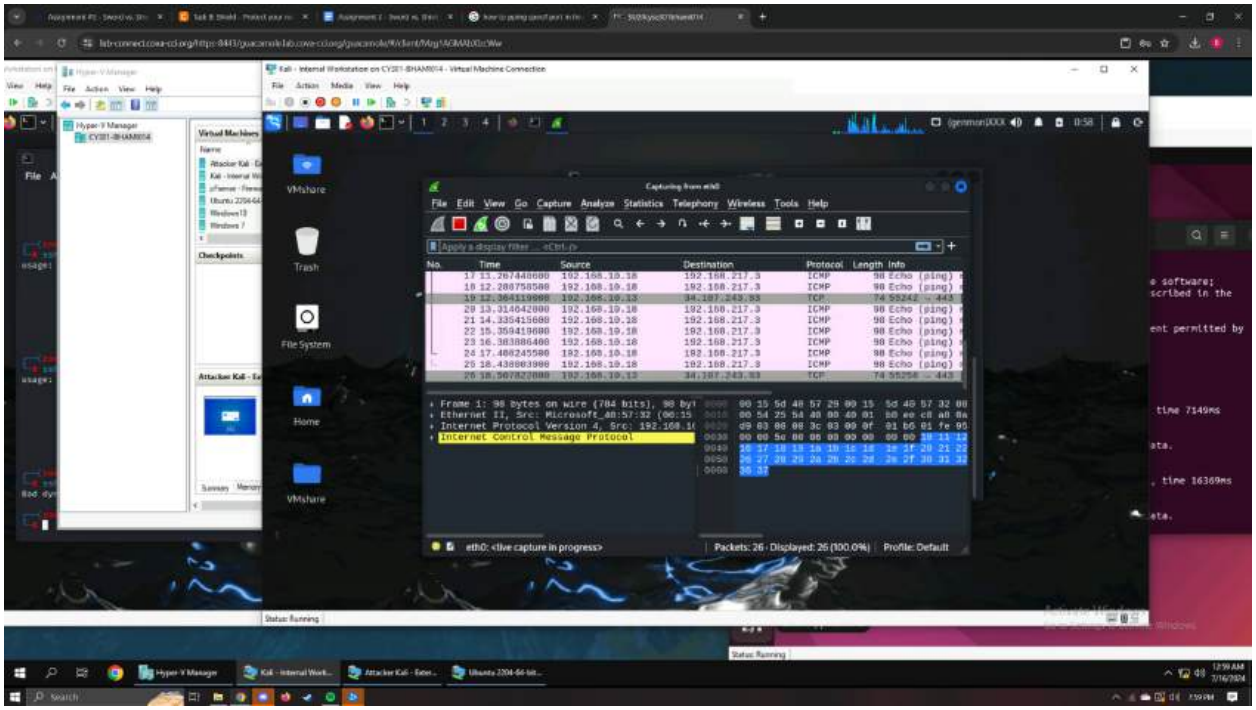


Figure 11 Screenshot of Wireshark after Task B.3 rules in place

In conclusion, the entire lab was very helpful in learning about the communications between networks and how rules can allow for the blocking, rejection, or passing of packets. There were some issues on the technical side of things, but that comes with technology at some points, but there was a work around in order to obtain similar results to what is to be achieved during the lab.