

CYSE 301: Cybersecurity Technique and Operations

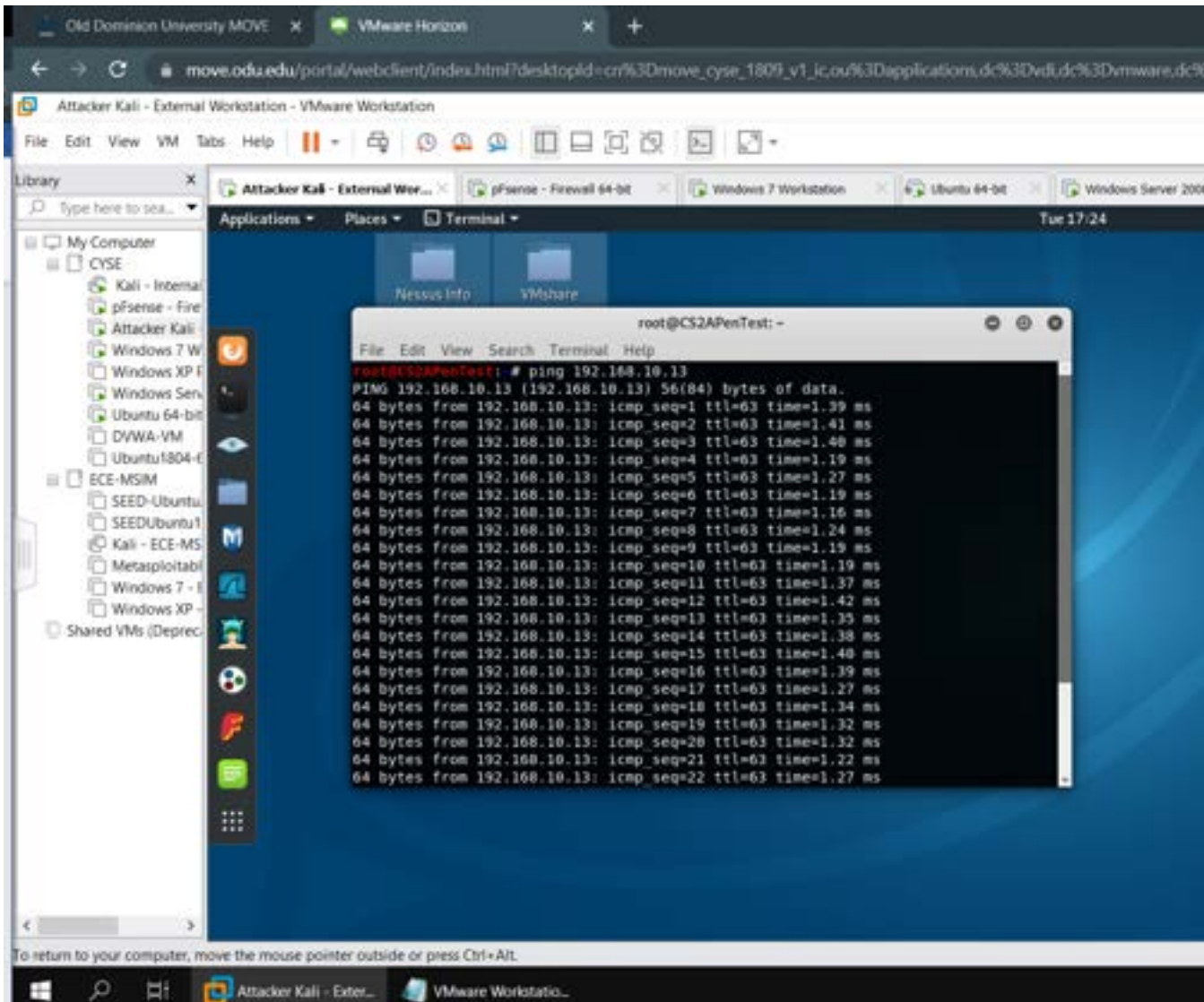
Assignment M2.1: pfSense Practice

Chris Evans

01206431

Task A

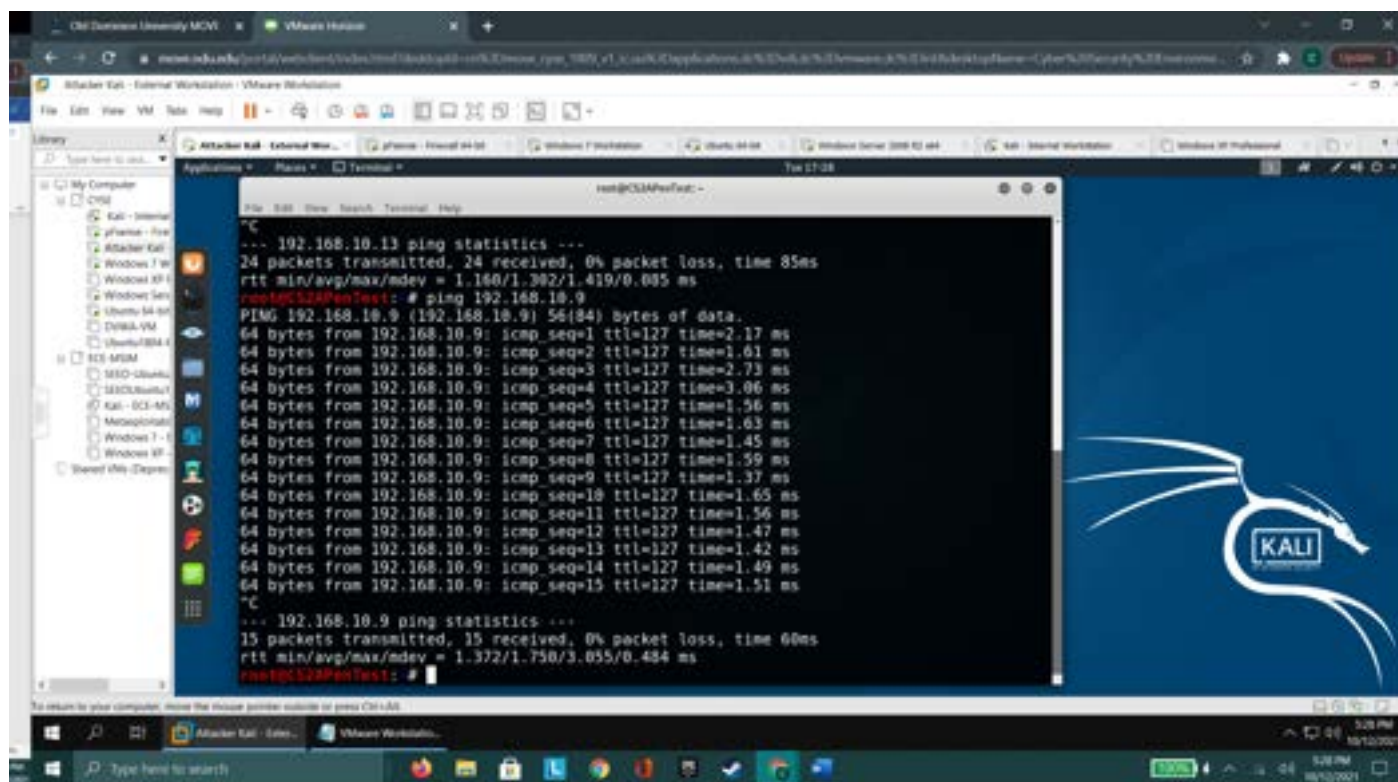
I used the command “ping 192.168.10.13” as that IP address is the address of internal Kali. I also used CTRL+C to stop the pings.



The screenshot shows a VMware Horizon interface with a browser window at the top displaying a URL from move.edu.edu. Below the browser is a VMware Workstation window titled "Attacker Kali - External Workstation - VMware Workstation". Inside this window, a terminal window is open with the title "root@CS2APenTest: ~". The terminal shows the command "ping 192.168.10.13" being executed, resulting in 22 successful ping responses. Each response line includes the source IP (192.168.10.13), the sequence number (icmp_seq), the TTL (63), and the time taken (ranging from 1.19 ms to 1.42 ms). The terminal window also shows standard menu options: File, Edit, View, Search, Terminal, Help.

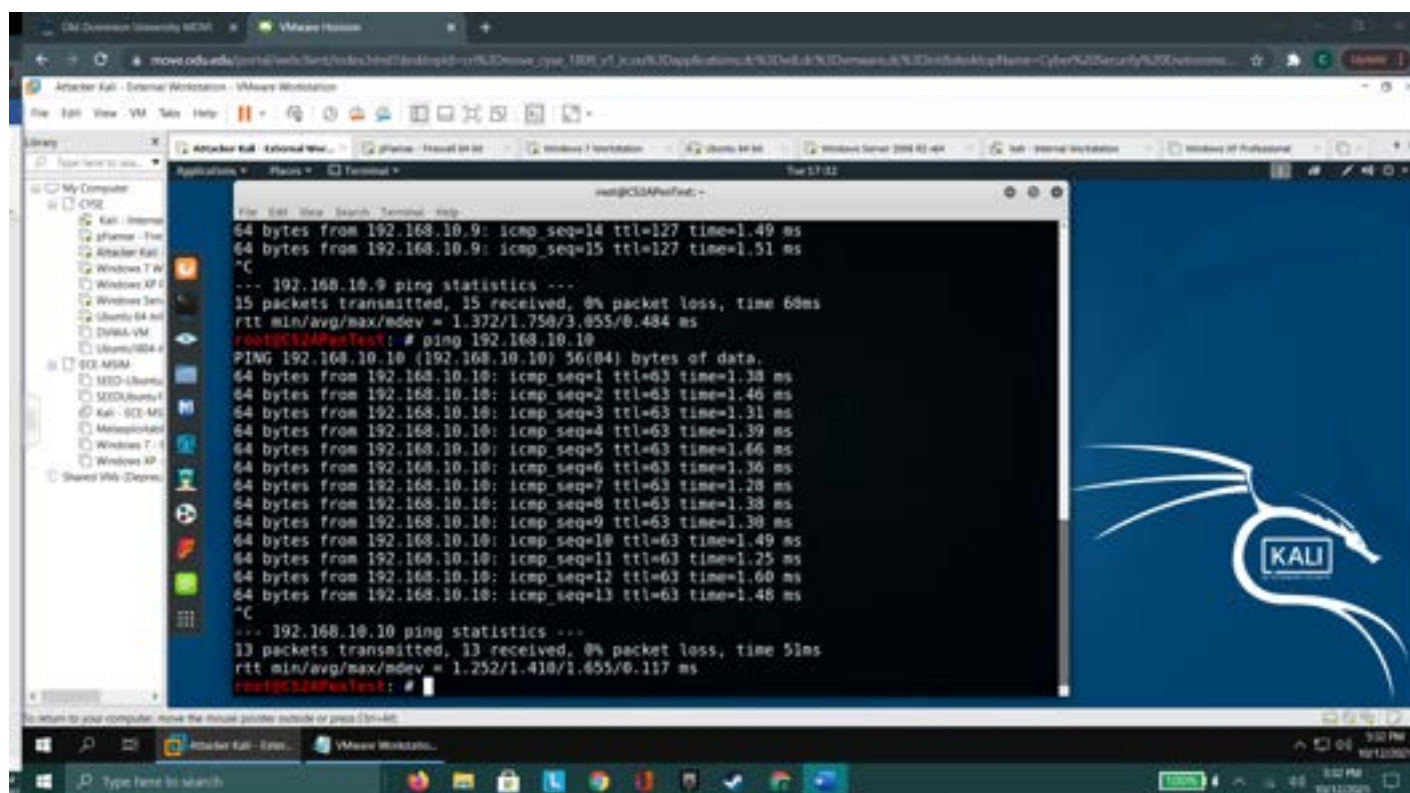
```
root@CS2APenTest: ~  
File Edit View Search Terminal Help  
root@CS2APenTest: # ping 192.168.10.13  
PING 192.168.10.13 (192.168.10.13) 56(84) bytes of data:  
64 bytes from 192.168.10.13: icmp_seq=1 ttl=63 time=1.39 ms  
64 bytes from 192.168.10.13: icmp_seq=2 ttl=63 time=1.41 ms  
64 bytes from 192.168.10.13: icmp_seq=3 ttl=63 time=1.40 ms  
64 bytes from 192.168.10.13: icmp_seq=4 ttl=63 time=1.19 ms  
64 bytes from 192.168.10.13: icmp_seq=5 ttl=63 time=1.27 ms  
64 bytes from 192.168.10.13: icmp_seq=6 ttl=63 time=1.19 ms  
64 bytes from 192.168.10.13: icmp_seq=7 ttl=63 time=1.16 ms  
64 bytes from 192.168.10.13: icmp_seq=8 ttl=63 time=1.24 ms  
64 bytes from 192.168.10.13: icmp_seq=9 ttl=63 time=1.19 ms  
64 bytes from 192.168.10.13: icmp_seq=10 ttl=63 time=1.19 ms  
64 bytes from 192.168.10.13: icmp_seq=11 ttl=63 time=1.37 ms  
64 bytes from 192.168.10.13: icmp_seq=12 ttl=63 time=1.42 ms  
64 bytes from 192.168.10.13: icmp_seq=13 ttl=63 time=1.35 ms  
64 bytes from 192.168.10.13: icmp_seq=14 ttl=63 time=1.38 ms  
64 bytes from 192.168.10.13: icmp_seq=15 ttl=63 time=1.40 ms  
64 bytes from 192.168.10.13: icmp_seq=16 ttl=63 time=1.39 ms  
64 bytes from 192.168.10.13: icmp_seq=17 ttl=63 time=1.27 ms  
64 bytes from 192.168.10.13: icmp_seq=18 ttl=63 time=1.34 ms  
64 bytes from 192.168.10.13: icmp_seq=19 ttl=63 time=1.32 ms  
64 bytes from 192.168.10.13: icmp_seq=20 ttl=63 time=1.32 ms  
64 bytes from 192.168.10.13: icmp_seq=21 ttl=63 time=1.22 ms  
64 bytes from 192.168.10.13: icmp_seq=22 ttl=63 time=1.27 ms
```

Below I pinged Windows 7 workstation from External Kali using the commands, “ ping 192.168.10.9 “ As that is the IP address of the Win7 workstation.

A screenshot of a Kali Linux terminal window. The terminal shows the output of a ping command to 192.168.10.9. The output includes ping statistics and 15 individual ping results. The background of the terminal window features the Kali Linux logo.

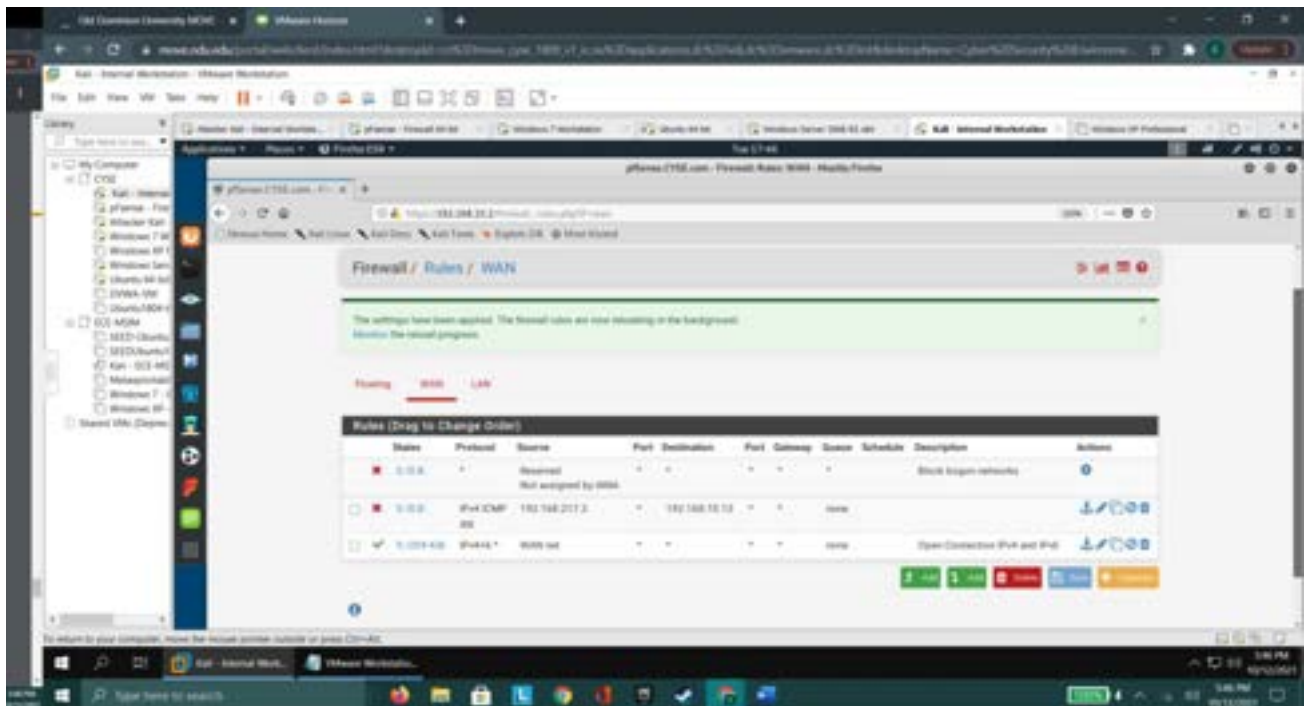
```
root@kali:~# ping 192.168.10.9
PING 192.168.10.9 (192.168.10.9) 56(84) bytes of data:
64 bytes from 192.168.10.9: icmp_seq=1 ttl=127 time=2.17 ms
64 bytes from 192.168.10.9: icmp_seq=2 ttl=127 time=1.61 ms
64 bytes from 192.168.10.9: icmp_seq=3 ttl=127 time=2.73 ms
64 bytes from 192.168.10.9: icmp_seq=4 ttl=127 time=3.06 ms
64 bytes from 192.168.10.9: icmp_seq=5 ttl=127 time=1.56 ms
64 bytes from 192.168.10.9: icmp_seq=6 ttl=127 time=1.63 ms
64 bytes from 192.168.10.9: icmp_seq=7 ttl=127 time=1.45 ms
64 bytes from 192.168.10.9: icmp_seq=8 ttl=127 time=1.59 ms
64 bytes from 192.168.10.9: icmp_seq=9 ttl=127 time=1.37 ms
64 bytes from 192.168.10.9: icmp_seq=10 ttl=127 time=1.65 ms
64 bytes from 192.168.10.9: icmp_seq=11 ttl=127 time=1.56 ms
64 bytes from 192.168.10.9: icmp_seq=12 ttl=127 time=1.47 ms
64 bytes from 192.168.10.9: icmp_seq=13 ttl=127 time=1.42 ms
64 bytes from 192.168.10.9: icmp_seq=14 ttl=127 time=1.49 ms
64 bytes from 192.168.10.9: icmp_seq=15 ttl=127 time=1.51 ms
--- 192.168.10.9 ping statistics ---
15 packets transmitted, 15 received, 0% packet loss, time 60ms
rtt min/avg/max/mdev = 1.372/1.750/3.055/0.484 ms
root@kali:~#
```

Below I pinged the Ubuntu machine from External Kali using commands, “ ping 192.168.10.10. “ That IP address is for the Ubuntu machine.

A screenshot of a Kali Linux terminal window. The terminal shows the output of a ping command to 192.168.10.10. The output includes ping statistics and 13 individual ping results. The background of the terminal window features the Kali Linux logo.

```
root@kali:~# ping 192.168.10.10
PING 192.168.10.10 (192.168.10.10) 56(84) bytes of data:
64 bytes from 192.168.10.10: icmp_seq=1 ttl=63 time=1.38 ms
64 bytes from 192.168.10.10: icmp_seq=2 ttl=63 time=1.46 ms
64 bytes from 192.168.10.10: icmp_seq=3 ttl=63 time=1.31 ms
64 bytes from 192.168.10.10: icmp_seq=4 ttl=63 time=1.39 ms
64 bytes from 192.168.10.10: icmp_seq=5 ttl=63 time=1.66 ms
64 bytes from 192.168.10.10: icmp_seq=6 ttl=63 time=1.36 ms
64 bytes from 192.168.10.10: icmp_seq=7 ttl=63 time=1.28 ms
64 bytes from 192.168.10.10: icmp_seq=8 ttl=63 time=1.38 ms
64 bytes from 192.168.10.10: icmp_seq=9 ttl=63 time=1.30 ms
64 bytes from 192.168.10.10: icmp_seq=10 ttl=63 time=1.49 ms
64 bytes from 192.168.10.10: icmp_seq=11 ttl=63 time=1.25 ms
64 bytes from 192.168.10.10: icmp_seq=12 ttl=63 time=1.60 ms
64 bytes from 192.168.10.10: icmp_seq=13 ttl=63 time=1.48 ms
--- 192.168.10.10 ping statistics ---
13 packets transmitted, 13 received, 0% packet loss, time 51ms
rtt min/avg/max/mdev = 1.252/1.410/1.655/0.117 ms
root@kali:~#
```

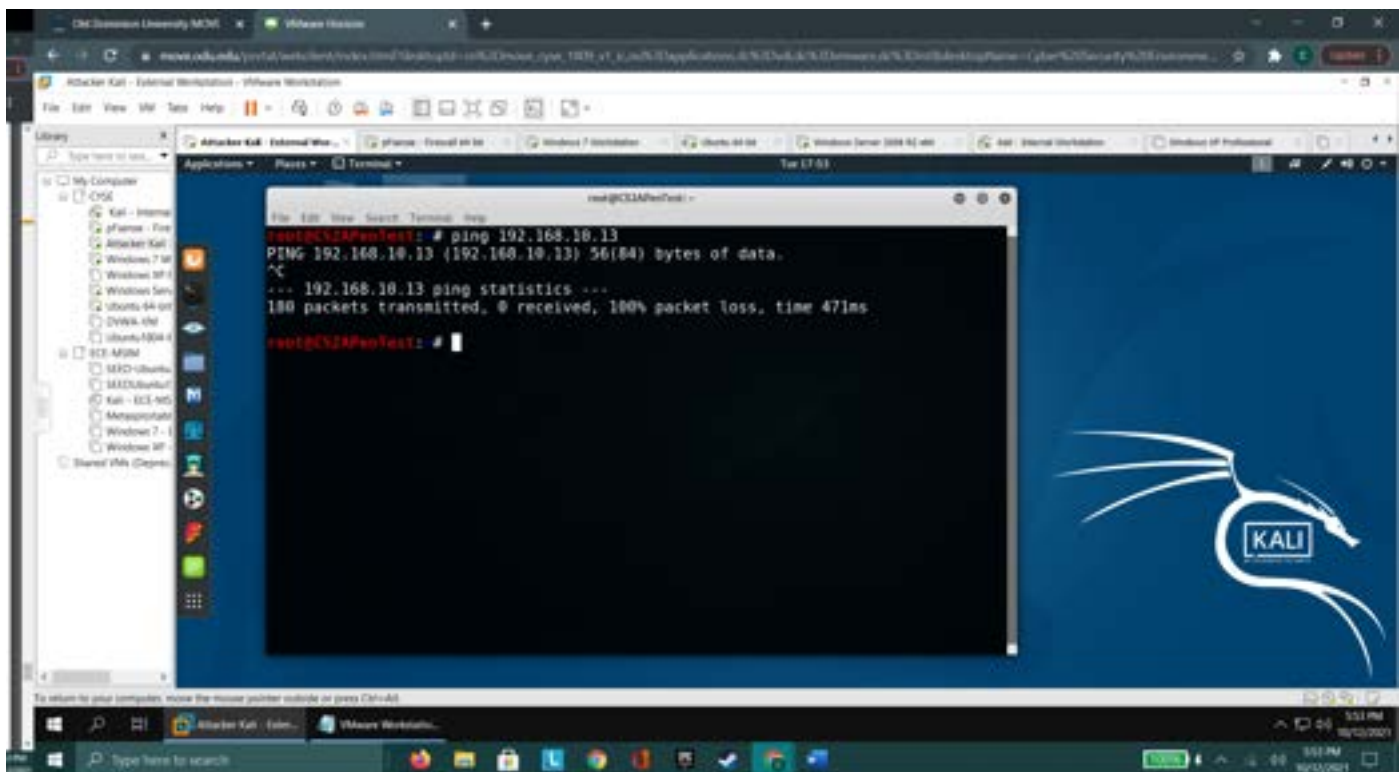
1. Configure the pfSense firewall rule to block the ICMP traffic from External Kali to Internal Kali.



Above I used the pfSense firewall to add a rule to block (drop) ICMP traffic coming from the WAN (or internet) into the LAN. I blocked traffic from the source IP address of the External Kali attack machine, and to the destination internal Kali Machine.

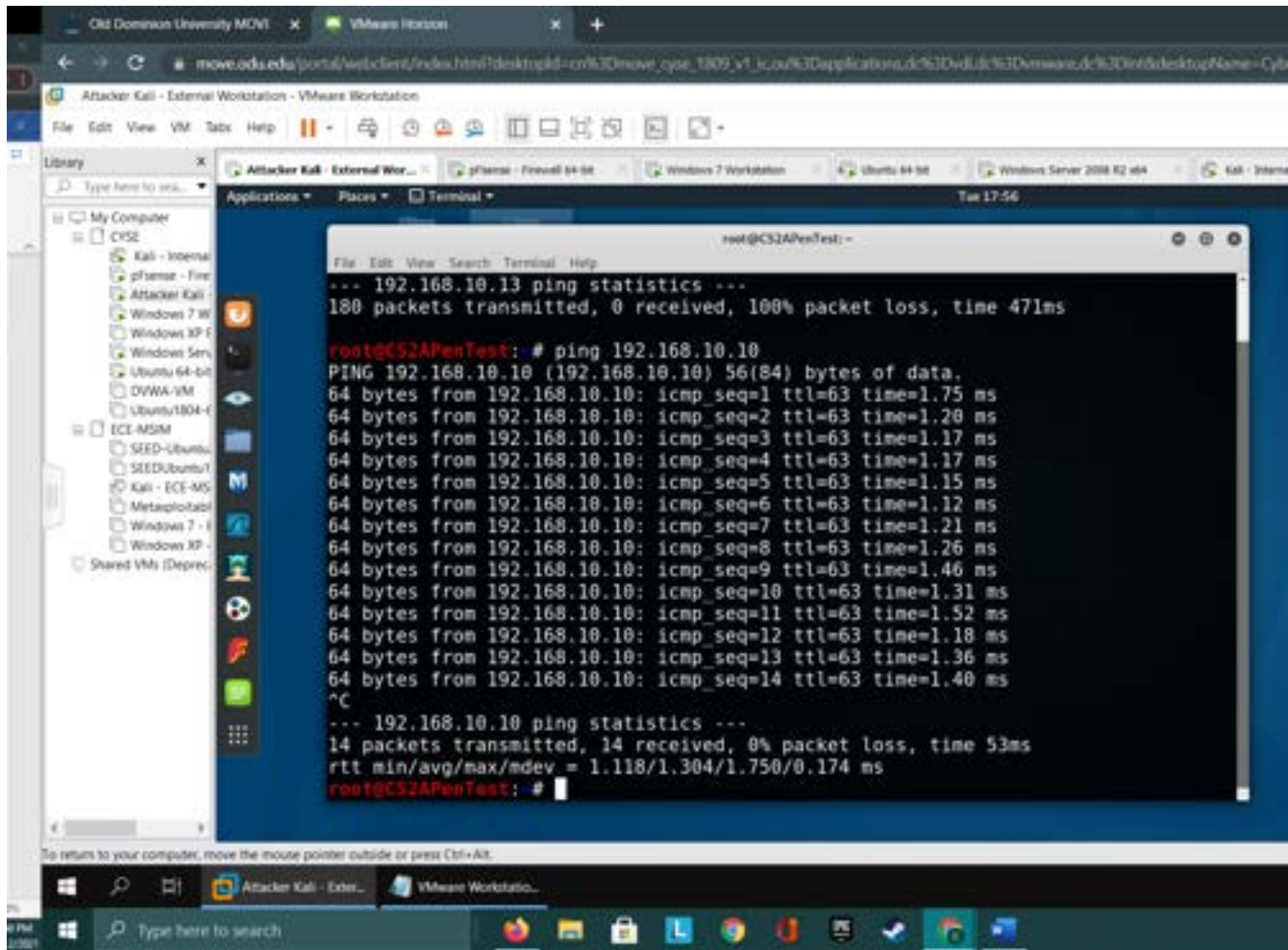
- a. Can you ping Internal Kali from External Kali?

No you can't. Below you can see the firewall blocking external traffic to ping the internal Kali machine.



b. Can you ping Ubuntu from External Kali?

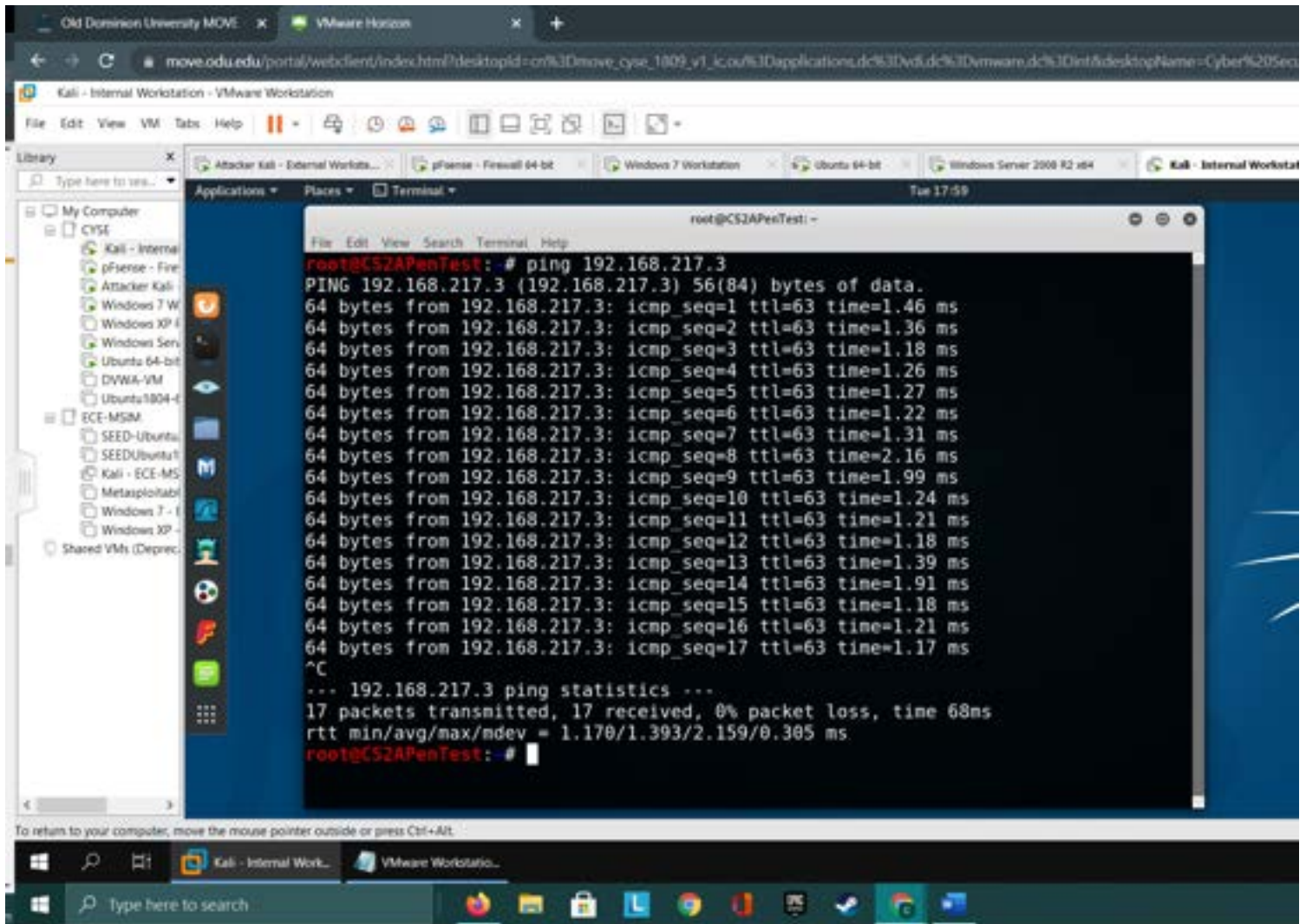
Yes you still can ping Ubuntu from external Kali, because the rule was simply to block one computer, External Kali, from sending one type of packet, ICMP to one internal computer, Internal Kali. To block ping's to Ubuntu you would have wanted to change the rule in pfSense to simply block all ICMP traffic from External Kali.



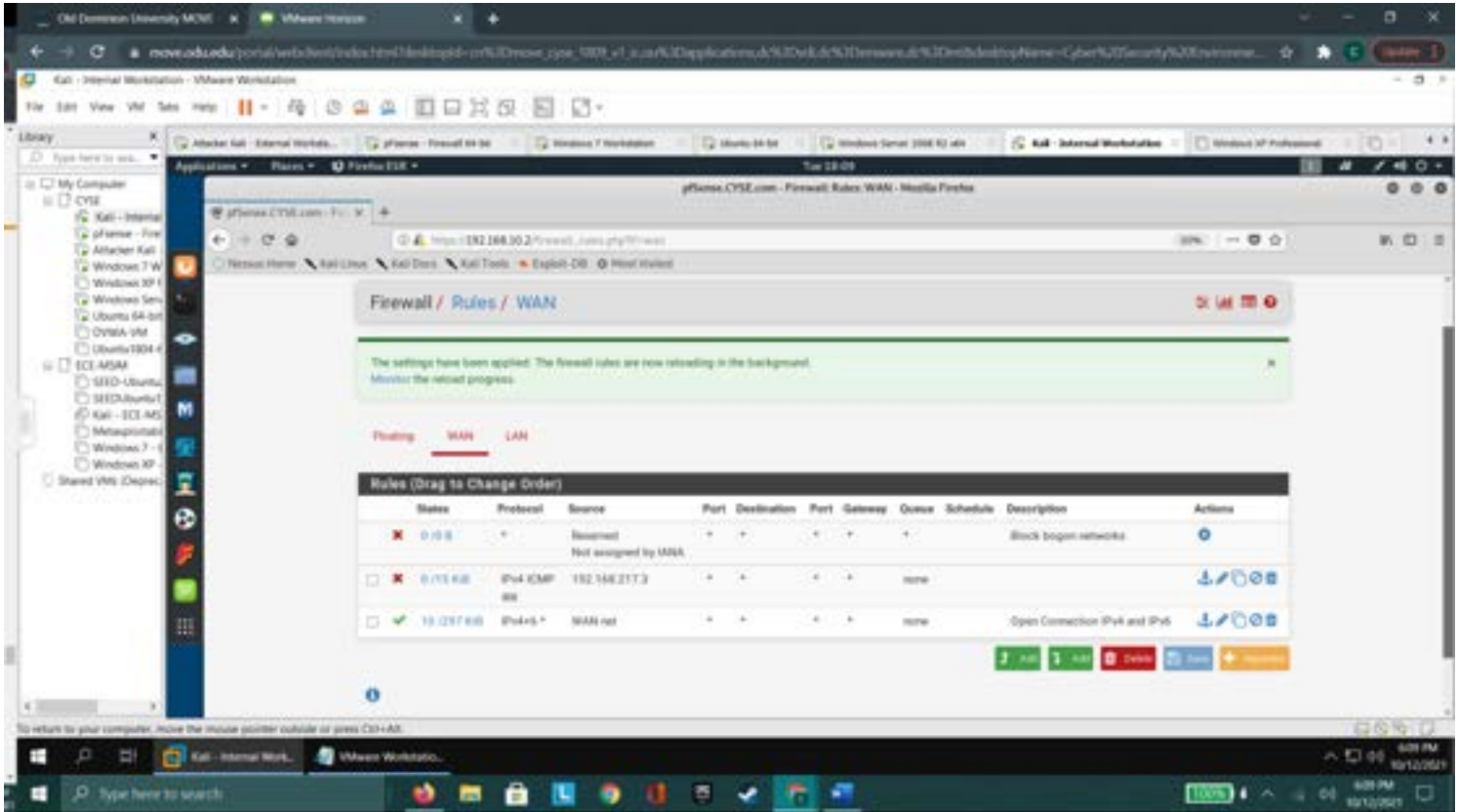
```
root@CS2APenTest: ~  
File Edit View Search Terminal Help  
--- 192.168.10.13 ping statistics ---  
180 packets transmitted, 0 received, 100% packet loss, time 471ms  
  
root@CS2APenTest: # ping 192.168.10.10  
PING 192.168.10.10 (192.168.10.10) 56(84) bytes of data:  
64 bytes from 192.168.10.10: icmp_seq=1 ttl=63 time=1.75 ms  
64 bytes from 192.168.10.10: icmp_seq=2 ttl=63 time=1.28 ms  
64 bytes from 192.168.10.10: icmp_seq=3 ttl=63 time=1.17 ms  
64 bytes from 192.168.10.10: icmp_seq=4 ttl=63 time=1.17 ms  
64 bytes from 192.168.10.10: icmp_seq=5 ttl=63 time=1.15 ms  
64 bytes from 192.168.10.10: icmp_seq=6 ttl=63 time=1.12 ms  
64 bytes from 192.168.10.10: icmp_seq=7 ttl=63 time=1.21 ms  
64 bytes from 192.168.10.10: icmp_seq=8 ttl=63 time=1.26 ms  
64 bytes from 192.168.10.10: icmp_seq=9 ttl=63 time=1.46 ms  
64 bytes from 192.168.10.10: icmp_seq=10 ttl=63 time=1.31 ms  
64 bytes from 192.168.10.10: icmp_seq=11 ttl=63 time=1.52 ms  
64 bytes from 192.168.10.10: icmp_seq=12 ttl=63 time=1.18 ms  
64 bytes from 192.168.10.10: icmp_seq=13 ttl=63 time=1.36 ms  
64 bytes from 192.168.10.10: icmp_seq=14 ttl=63 time=1.40 ms  
^C  
--- 192.168.10.10 ping statistics ---  
14 packets transmitted, 14 received, 0% packet loss, time 53ms  
rtt min/avg/max/mdev = 1.118/1.304/1.750/0.174 ms  
root@CS2APenTest: #
```

c. Can you ping External Kali from Internal Kali?

Yes you can ping External Kali from Internal Kali still. Again the rule added to the pfSense router is very specific and does not stop ICMP traffic coming from the LAN going to the WAN (internet). If you had wanted to stop internal Kali from being able to ping External Kali, you would have had to use a rule to block or reject internal ICMP traffic heading to the WAN and external Kali machine.



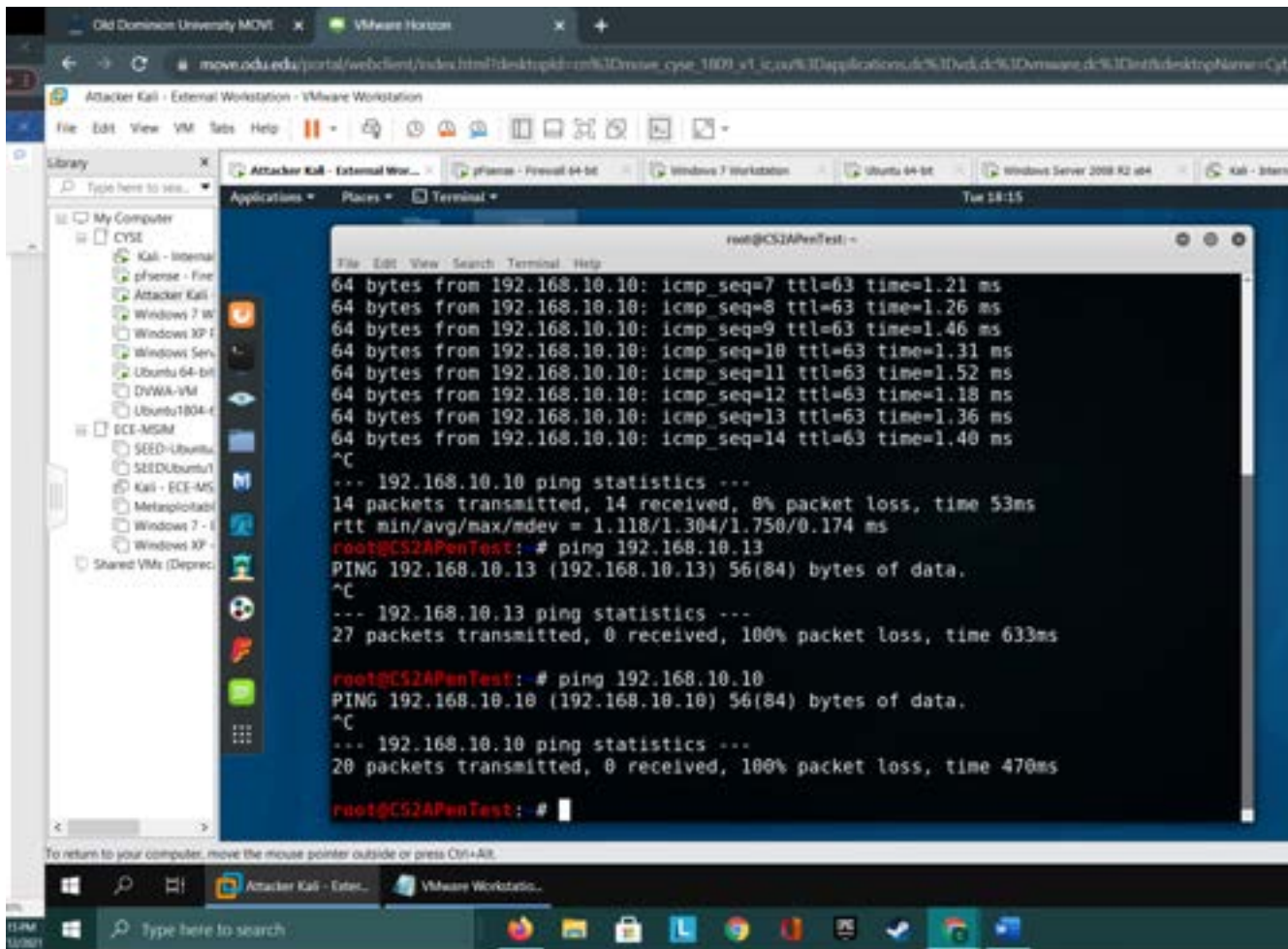
2. Now, configure the pfSense to block all ICMP traffic from External Kali to LAN side. After you applied the rule, answer the following questions: (30 points)



I updated the rule in pfSense to block ICMP packets coming into any place on the LAN from the external Kali machine with IP 192.168.217.3

a. *Can you ping Internal Kali from External Kali?*

No. Below you can see I tried to ping internal Kali (IP 192.168.10.13) from external Kali and had 633ms with no response. The firewall is using the rule we gave it to block the ICMP packets.

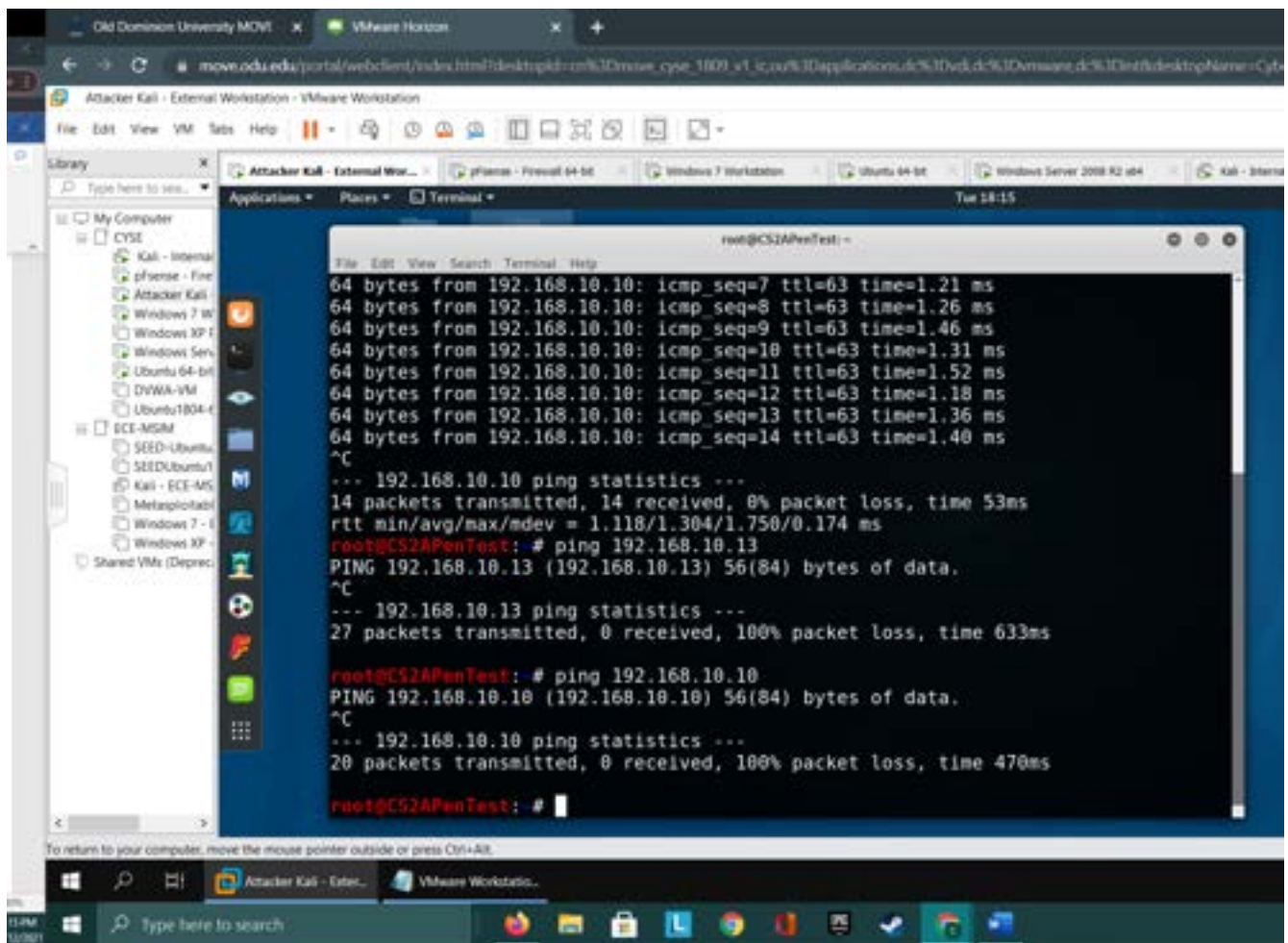


The screenshot shows a VMware Workstation interface with a terminal window open. The terminal output shows the following:

```
root@CS2APenTest: ~  
File Edit View Search Terminal Help  
64 bytes from 192.168.10.10: icmp_seq=7 ttl=63 time=1.21 ms  
64 bytes from 192.168.10.10: icmp_seq=8 ttl=63 time=1.26 ms  
64 bytes from 192.168.10.10: icmp_seq=9 ttl=63 time=1.46 ms  
64 bytes from 192.168.10.10: icmp_seq=10 ttl=63 time=1.31 ms  
64 bytes from 192.168.10.10: icmp_seq=11 ttl=63 time=1.52 ms  
64 bytes from 192.168.10.10: icmp_seq=12 ttl=63 time=1.18 ms  
64 bytes from 192.168.10.10: icmp_seq=13 ttl=63 time=1.36 ms  
64 bytes from 192.168.10.10: icmp_seq=14 ttl=63 time=1.40 ms  
^C  
--- 192.168.10.10 ping statistics ---  
14 packets transmitted, 14 received, 0% packet loss, time 53ms  
rtt min/avg/max/mdev = 1.118/1.304/1.750/0.174 ms  
root@CS2APenTest: # ping 192.168.10.13  
PING 192.168.10.13 (192.168.10.13) 56(84) bytes of data.  
^C  
--- 192.168.10.13 ping statistics ---  
27 packets transmitted, 0 received, 100% packet loss, time 633ms  
root@CS2APenTest: # ping 192.168.10.10  
PING 192.168.10.10 (192.168.10.10) 56(84) bytes of data.  
^C  
--- 192.168.10.10 ping statistics ---  
20 packets transmitted, 0 received, 100% packet loss, time 470ms  
root@CS2APenTest: #
```

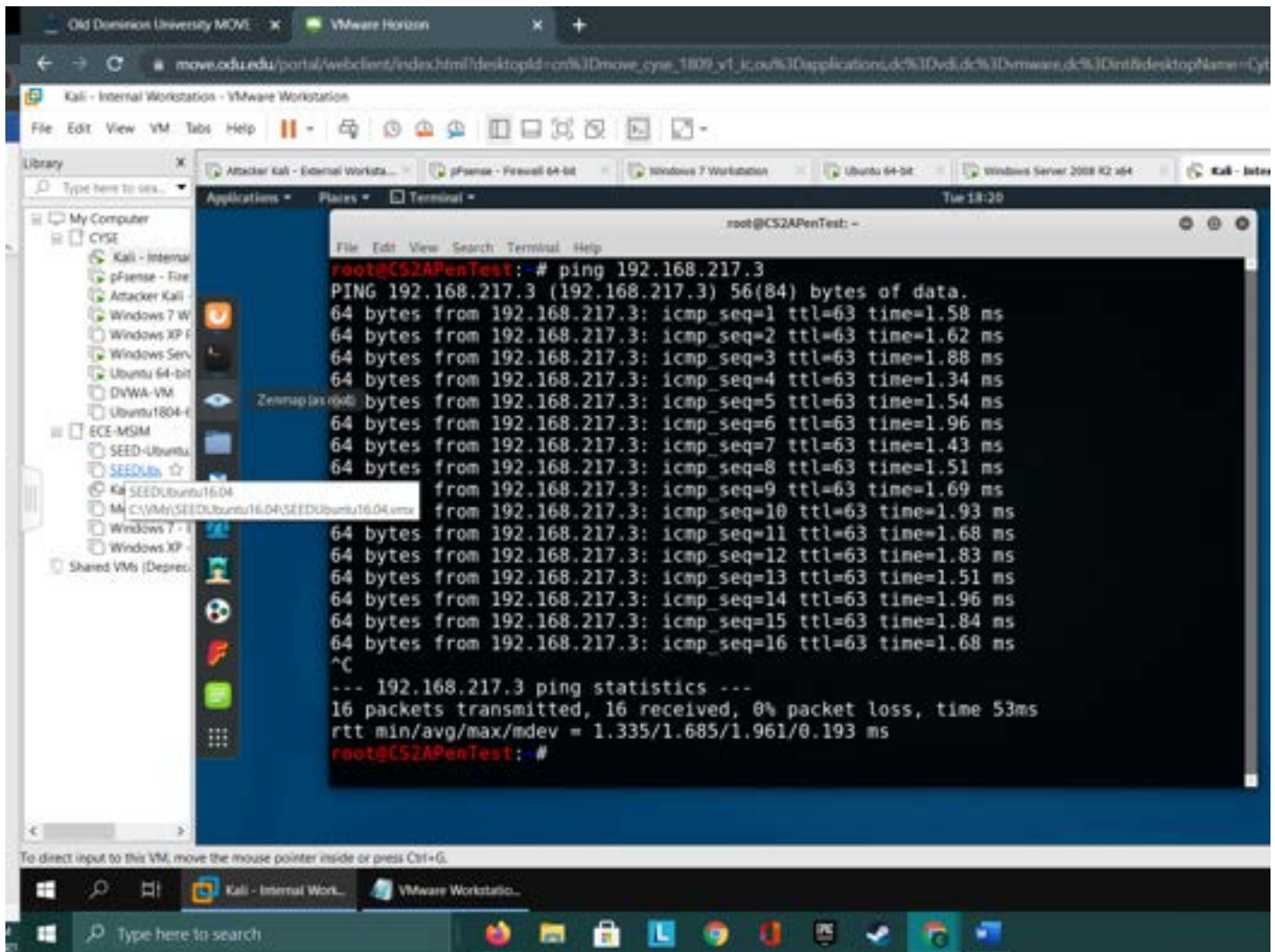
b. *Can you ping Ubuntu from External Kali?*

No. You can see below I pinged Ubuntu (IP 192.168.10.10) from external Kali and after 470ms no ICMP packets went through. The Firewall is using the rule we gave it.



c. Can you ping External Kali from Internal Kali?

Yes. The rule we gave pfSense was to block all incoming to the LAN ICMP traffic from the external machine. We never told the firewall to block ICMP traffic leaving the LAN.

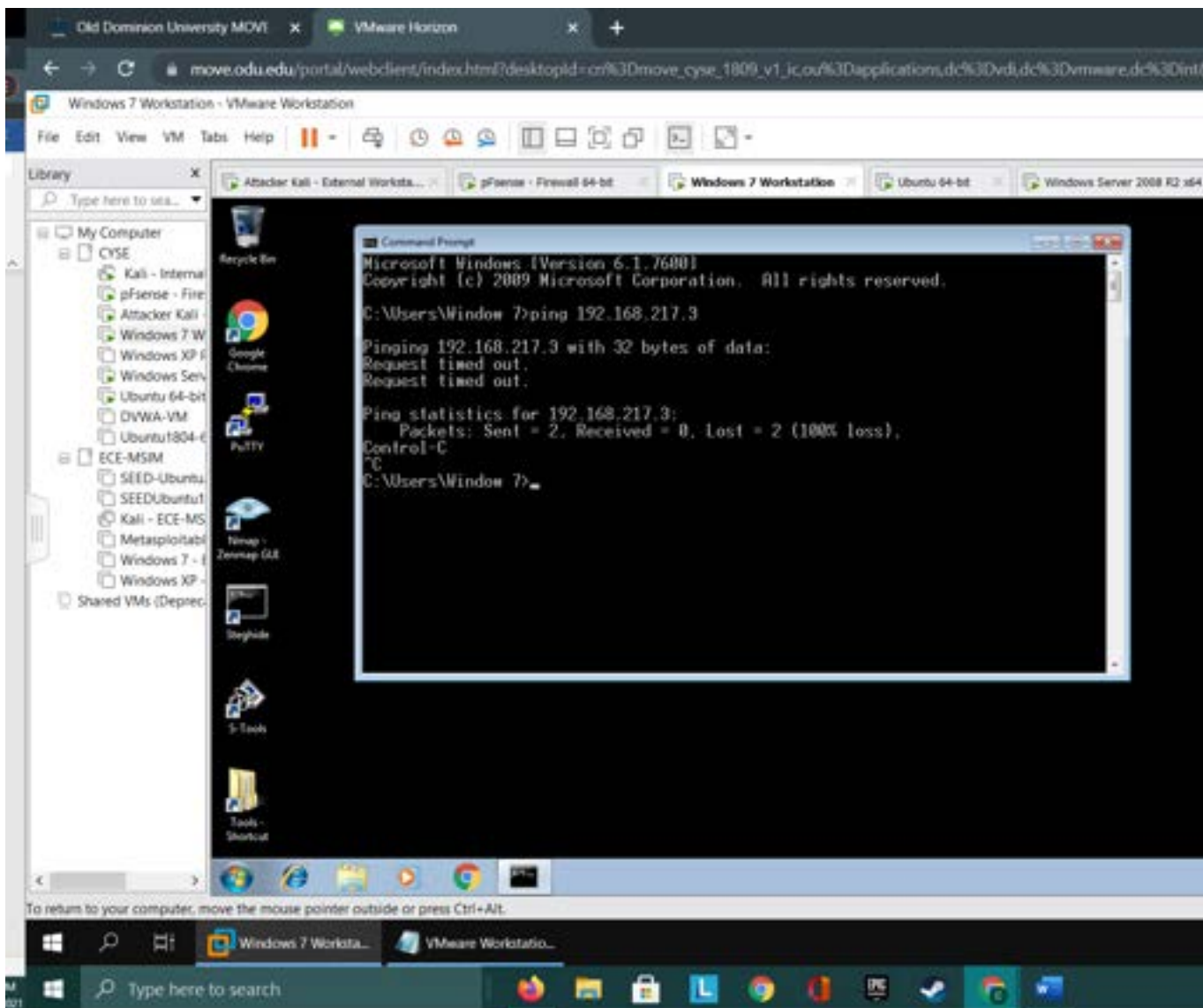


```
root@CS2APenTest: # ping 192.168.217.3
PING 192.168.217.3 (192.168.217.3) 56(84) bytes of data:
64 bytes from 192.168.217.3: icmp_seq=1 ttl=63 time=1.58 ms
64 bytes from 192.168.217.3: icmp_seq=2 ttl=63 time=1.62 ms
64 bytes from 192.168.217.3: icmp_seq=3 ttl=63 time=1.88 ms
64 bytes from 192.168.217.3: icmp_seq=4 ttl=63 time=1.34 ms
64 bytes from 192.168.217.3: icmp_seq=5 ttl=63 time=1.54 ms
64 bytes from 192.168.217.3: icmp_seq=6 ttl=63 time=1.96 ms
64 bytes from 192.168.217.3: icmp_seq=7 ttl=63 time=1.43 ms
64 bytes from 192.168.217.3: icmp_seq=8 ttl=63 time=1.51 ms
64 bytes from 192.168.217.3: icmp_seq=9 ttl=63 time=1.69 ms
64 bytes from 192.168.217.3: icmp_seq=10 ttl=63 time=1.93 ms
64 bytes from 192.168.217.3: icmp_seq=11 ttl=63 time=1.68 ms
64 bytes from 192.168.217.3: icmp_seq=12 ttl=63 time=1.83 ms
64 bytes from 192.168.217.3: icmp_seq=13 ttl=63 time=1.51 ms
64 bytes from 192.168.217.3: icmp_seq=14 ttl=63 time=1.96 ms
64 bytes from 192.168.217.3: icmp_seq=15 ttl=63 time=1.84 ms
64 bytes from 192.168.217.3: icmp_seq=16 ttl=63 time=1.68 ms
^C
--- 192.168.217.3 ping statistics ---
16 packets transmitted, 16 received, 0% packet loss, time 53ms
rtt min/avg/max/mdev = 1.335/1.685/1.961/0.193 ms
root@CS2APenTest: #
```

I updated the pfSense rule to block all ICMP traffic from Windows 7 (192.168.10.9) to External Kali (192.168.217.3). And updated the rule to apply to the devices on the LAN.

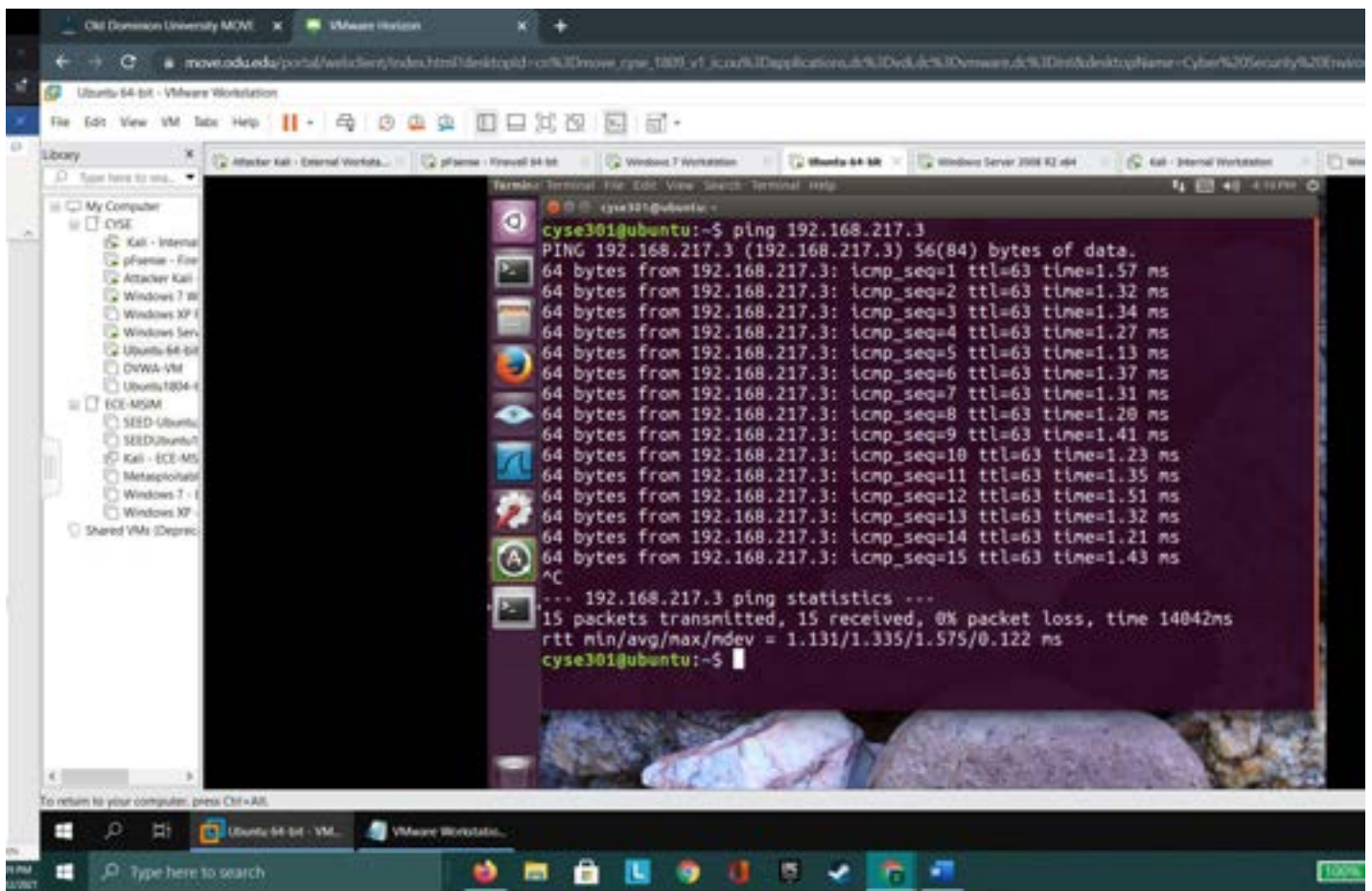
a. Can you ping External Kali from Windows 7?

No you cannot ping external Kali (192.168.217.3) from windows 7 (192.168.10.9) because we expressly made the rule to block ICMP packets in pfSense.



b. Can you ping External Kali from Ubuntu VM?

Yes you can ping External Kali from Ubuntu VM because the rules in the pfSense did not stop a Ubuntu from sending pings, only Windows 7 machine.



The screenshot shows a VMware Workstation interface with several virtual machines. The active VM is 'Ubuntu 64-bit'. Inside the VM, a terminal window is open, showing the following output:

```
cyse301@ubuntu:~$ ping 192.168.217.3
PING 192.168.217.3 (192.168.217.3) 56(84) bytes of data:
64 bytes from 192.168.217.3: icmp_seq=1 ttl=63 time=1.57 ms
64 bytes from 192.168.217.3: icmp_seq=2 ttl=63 time=1.32 ms
64 bytes from 192.168.217.3: icmp_seq=3 ttl=63 time=1.34 ms
64 bytes from 192.168.217.3: icmp_seq=4 ttl=63 time=1.27 ms
64 bytes from 192.168.217.3: icmp_seq=5 ttl=63 time=1.13 ms
64 bytes from 192.168.217.3: icmp_seq=6 ttl=63 time=1.37 ms
64 bytes from 192.168.217.3: icmp_seq=7 ttl=63 time=1.31 ms
64 bytes from 192.168.217.3: icmp_seq=8 ttl=63 time=1.20 ms
64 bytes from 192.168.217.3: icmp_seq=9 ttl=63 time=1.41 ms
64 bytes from 192.168.217.3: icmp_seq=10 ttl=63 time=1.23 ms
64 bytes from 192.168.217.3: icmp_seq=11 ttl=63 time=1.35 ms
64 bytes from 192.168.217.3: icmp_seq=12 ttl=63 time=1.51 ms
64 bytes from 192.168.217.3: icmp_seq=13 ttl=63 time=1.32 ms
64 bytes from 192.168.217.3: icmp_seq=14 ttl=63 time=1.21 ms
64 bytes from 192.168.217.3: icmp_seq=15 ttl=63 time=1.43 ms
^C
--- 192.168.217.3 ping statistics ---
15 packets transmitted, 15 received, 0% packet loss, time 14042ms
rtt min/avg/max/mdev = 1.131/1.335/1.575/0.122 ms
cyse301@ubuntu:~$
```

c. Can you ping Windows 7 from External Kali?

Yes you can because again the rule we put into pfSense was to block outgoing ICMP requests from Windows 7 in the LAN to External Kali machine on the WAN (internet).

