CYSE 301: Cybersecurity Technique and Operations

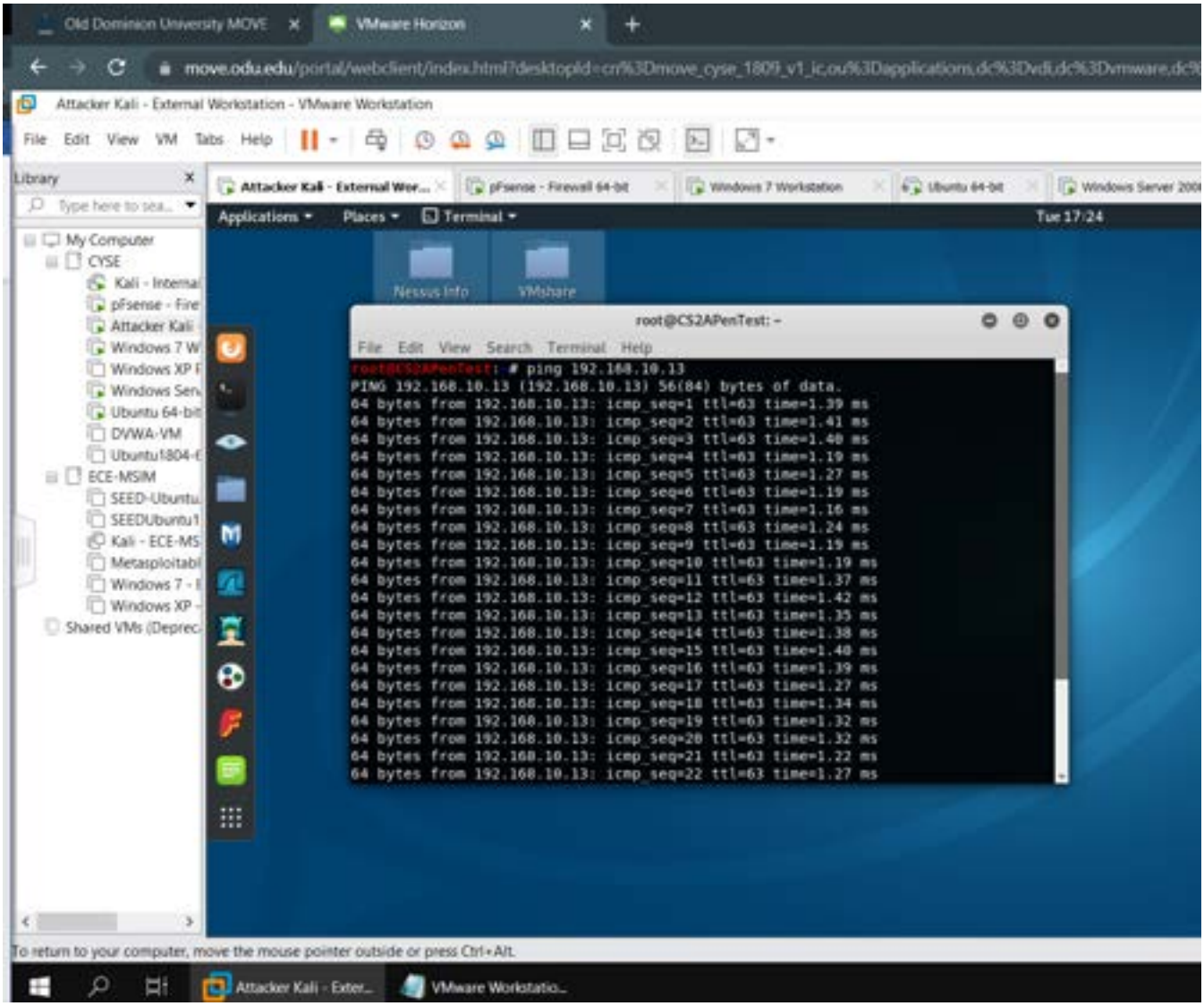
Assignment M2.1: pfSense Practice

Chris Evans

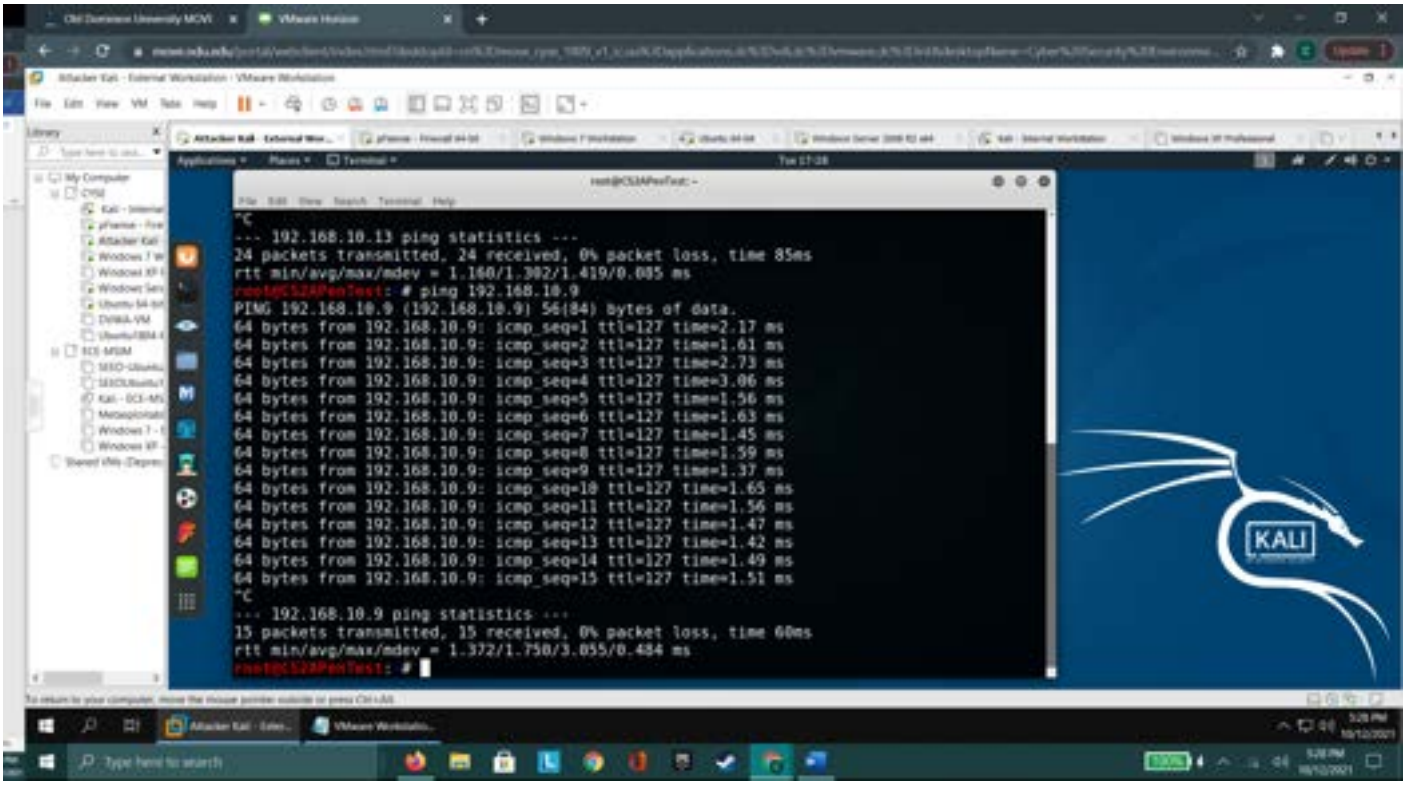
01206431

Task A

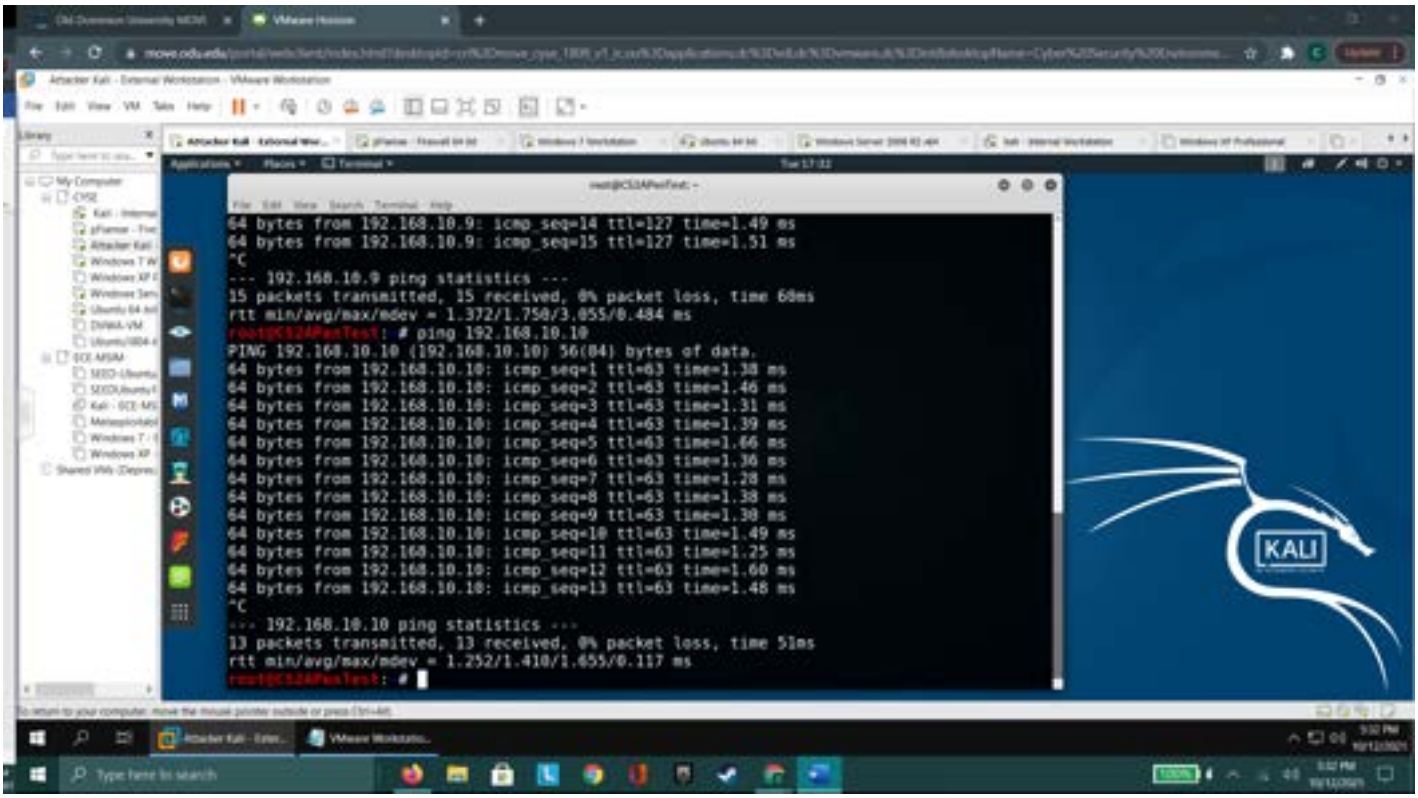
I used the command " ping 192.168.10.13 " as that IP address is the address of internal Kali. I also used CTRL+C to stop the pings.



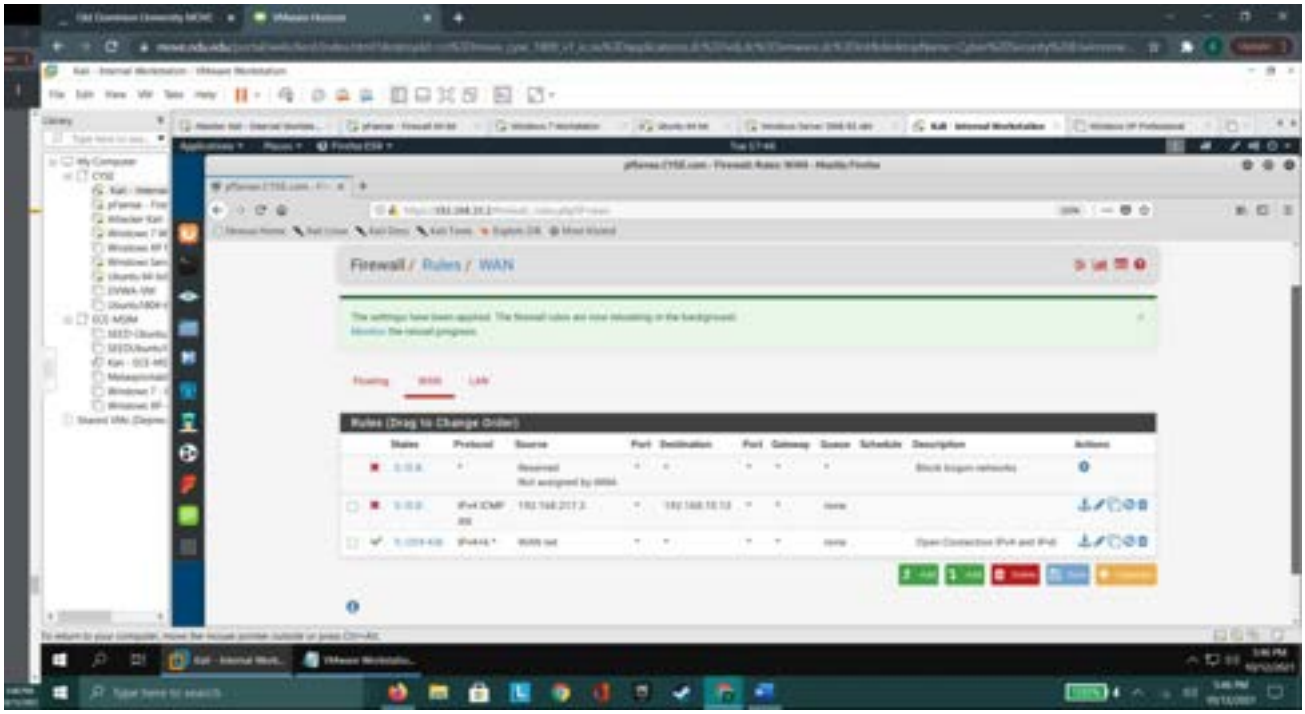
Below I pinged Windows 7 workstation from External Kali using the commands, “ ping 192.168.10.9 “ As that is the IP address of the Win7 workstation.



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



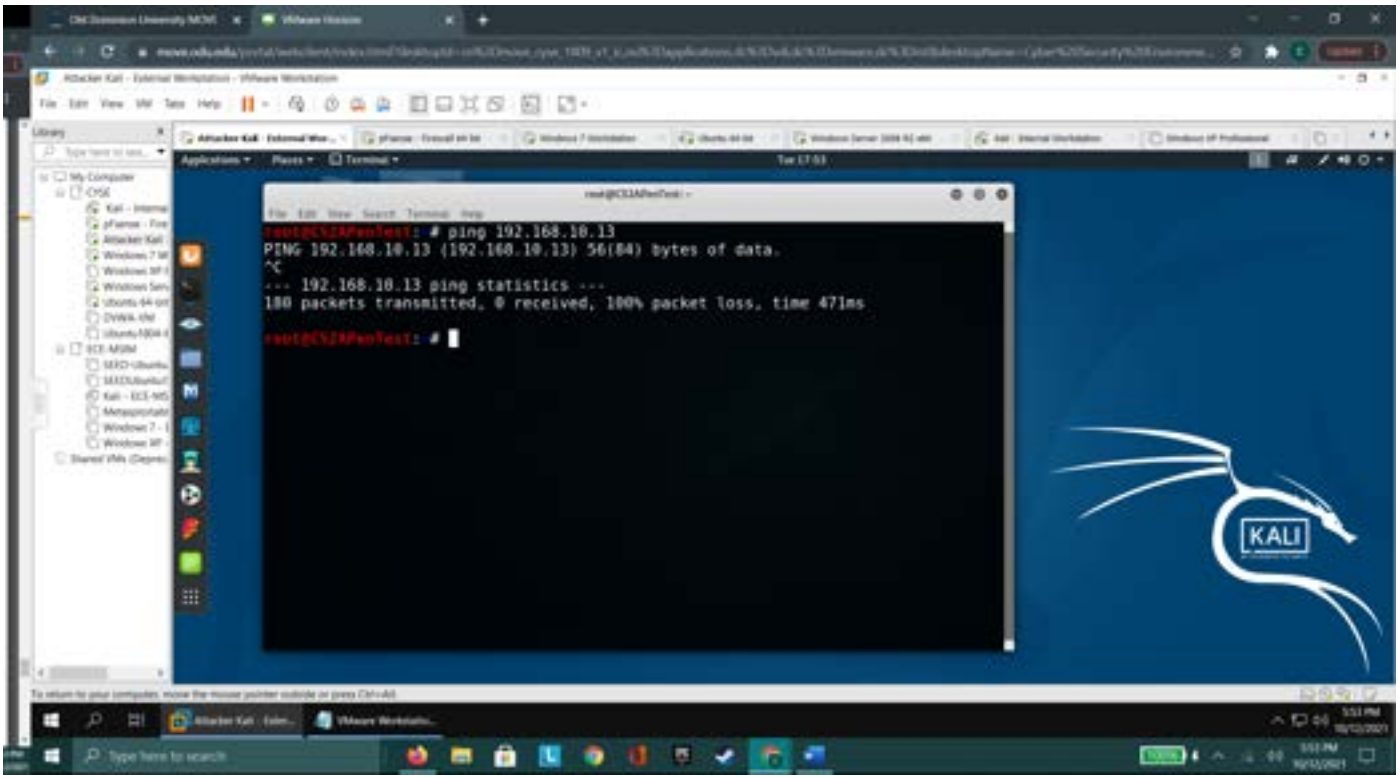
1. *Configure the pfSense firewall rule to block the ICMP traffic from External Kali to Internal Kali.*



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.

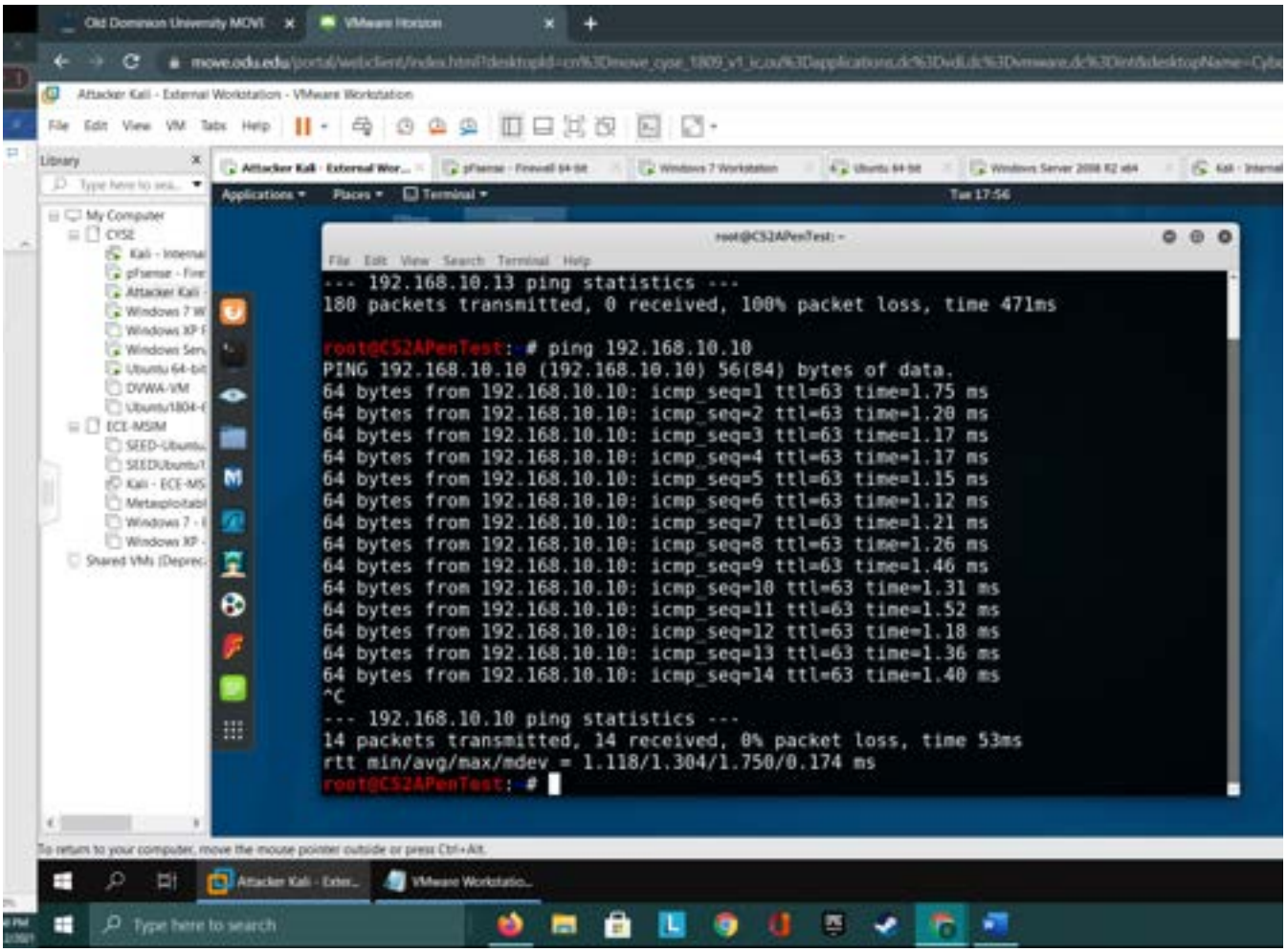
a. *Can you ping Internal Kali from External Kali?*

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



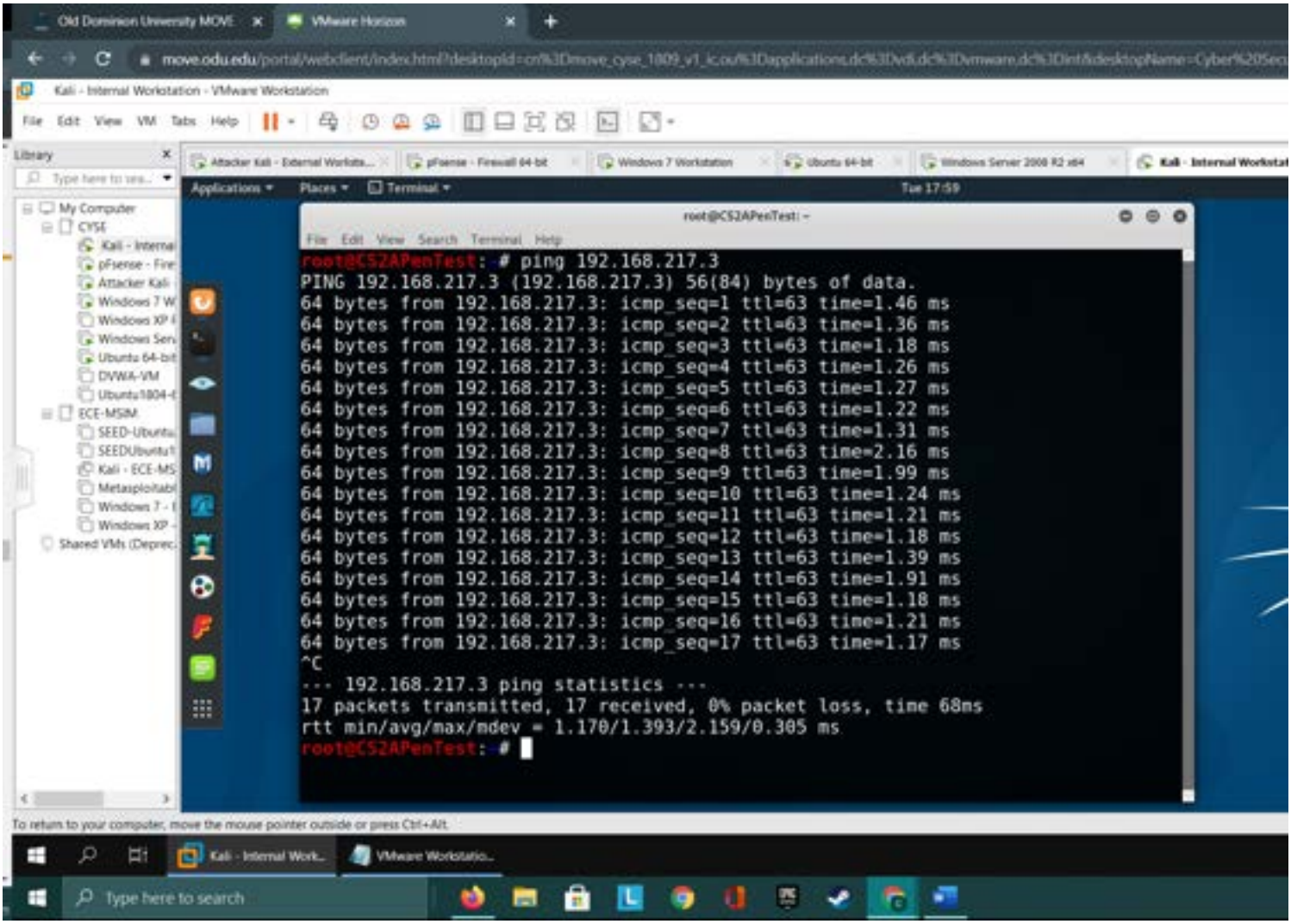
b. Can you ping Ubuntu from External Kali?

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.

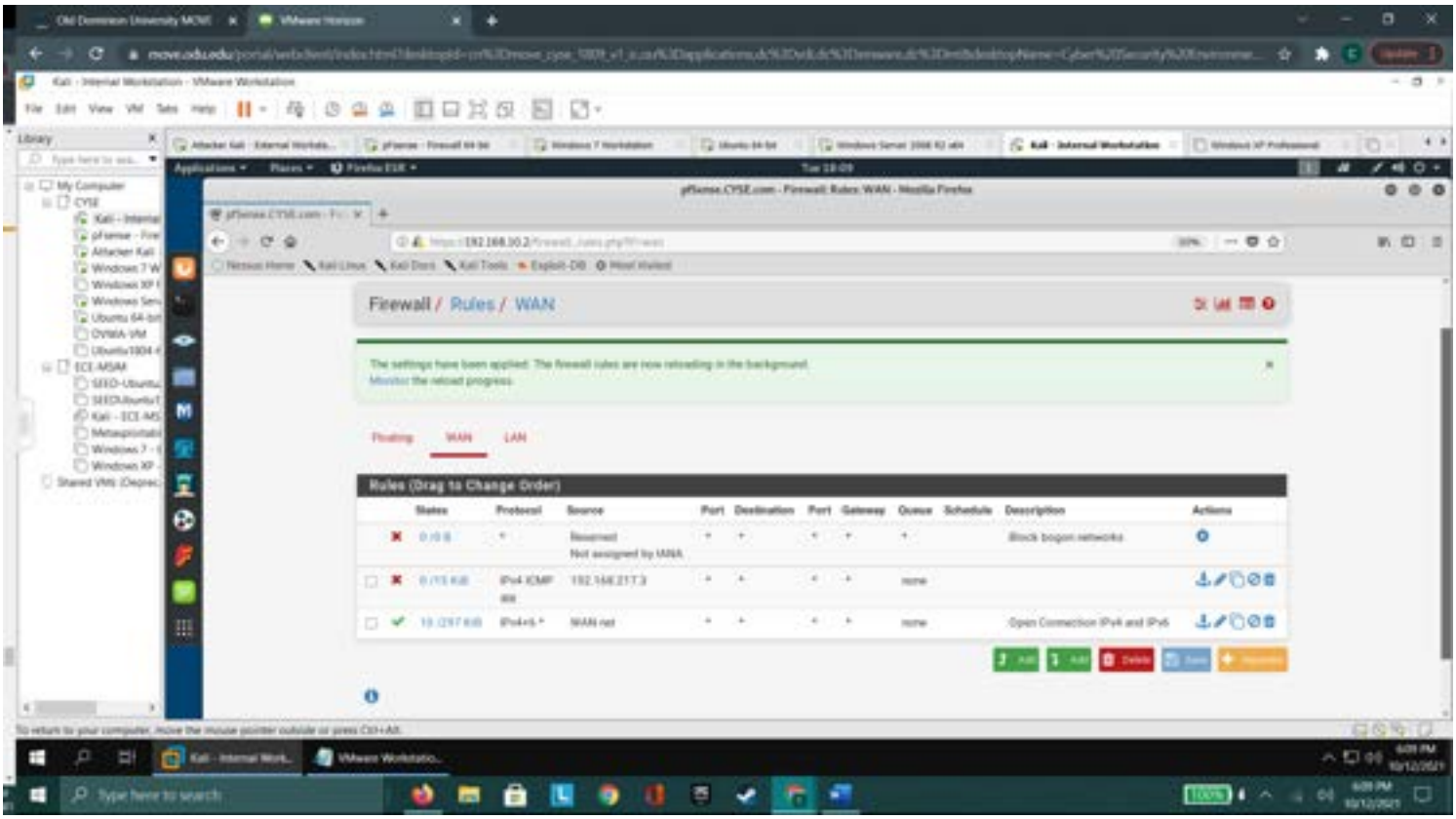


c. Can you ping External Kali from Internal Kali?

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.



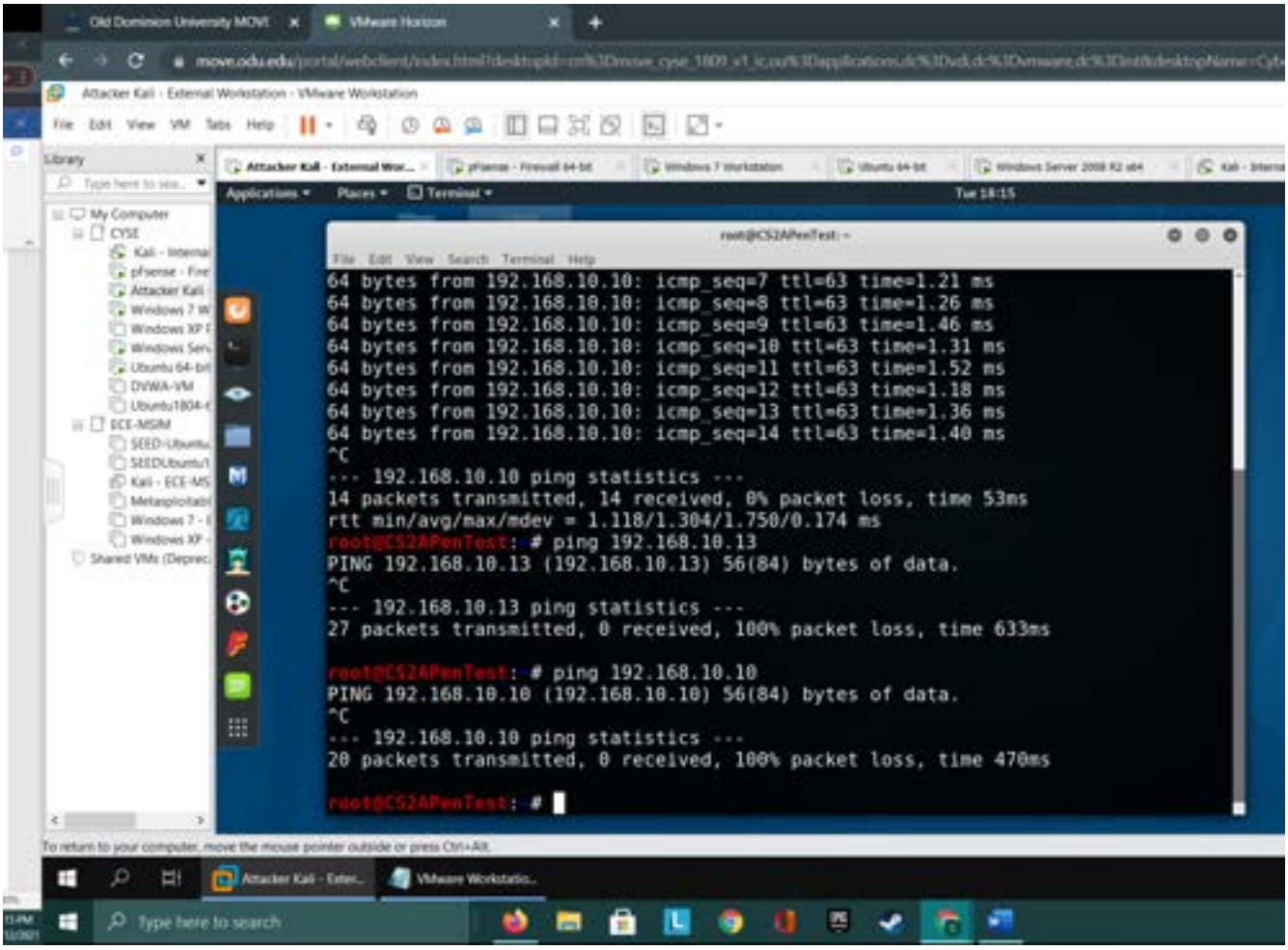
2. Now, configure the pfSense to block all ICMP traffic from External Kali to LAN side. After you applied the rule, answer the following questions: (30 points)



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

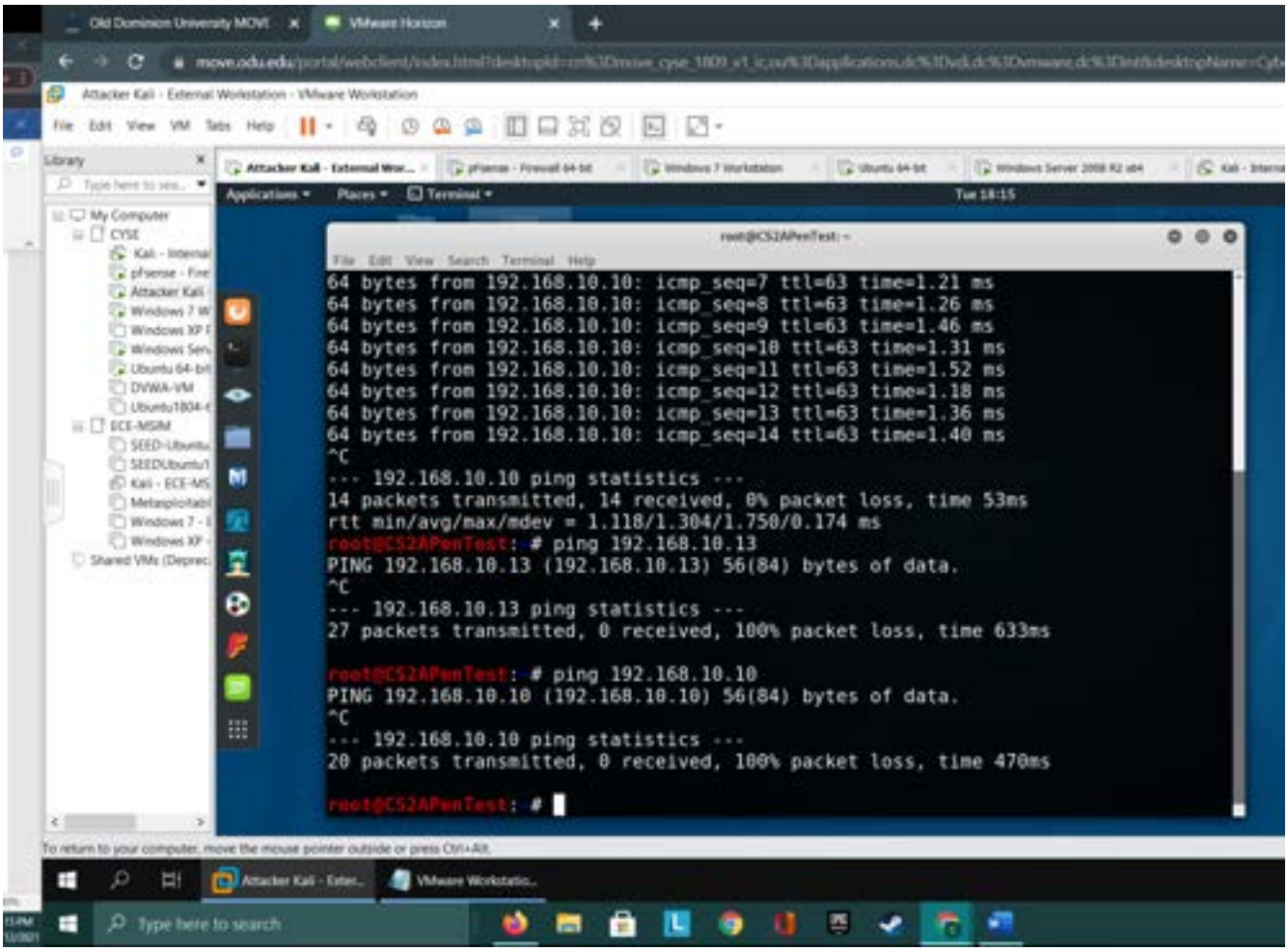
a. *Can you ping Internal Kali from External Kali?*

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.

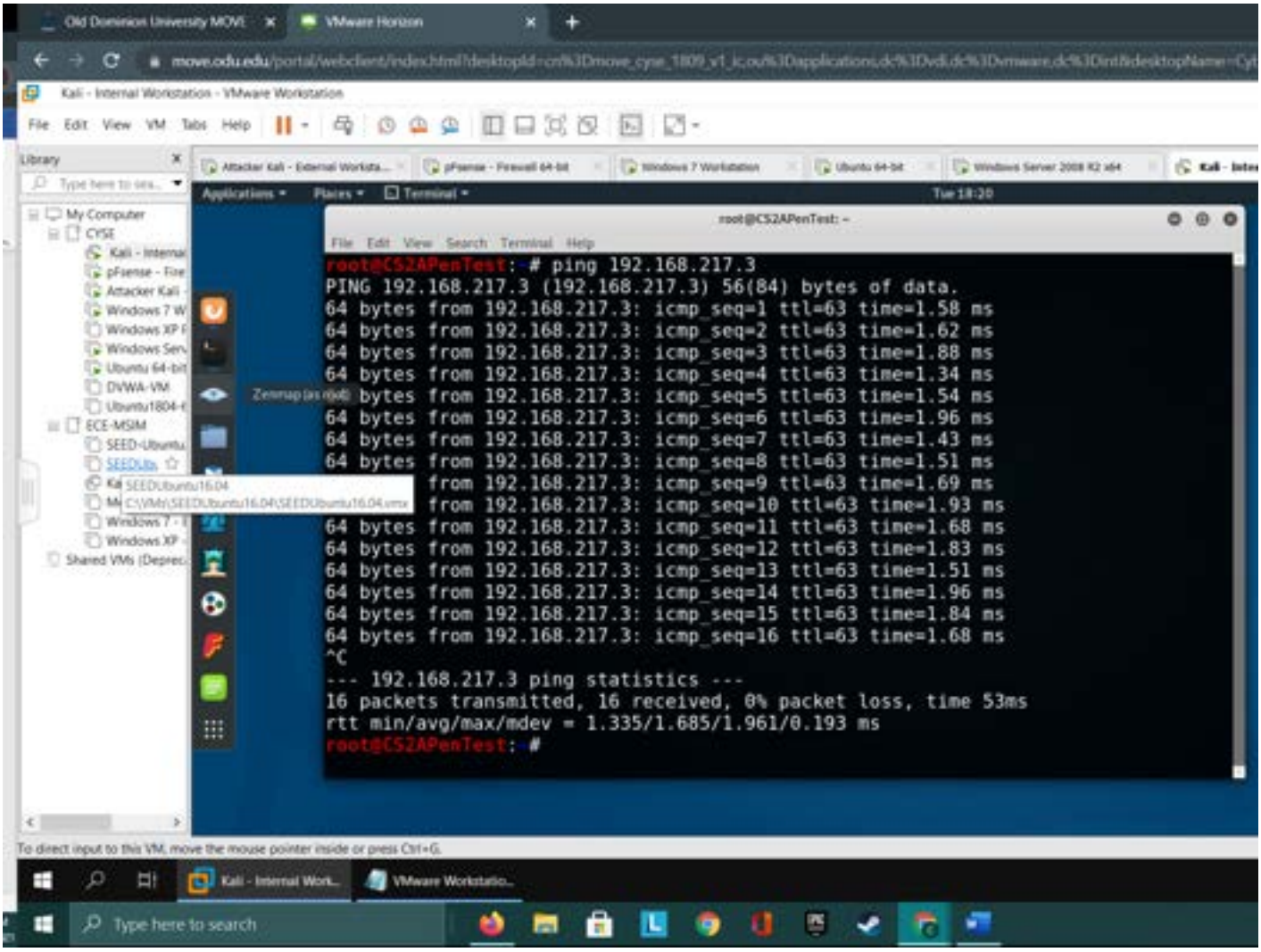


b. *Can you ping Ubuntu from External Kali?*

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.

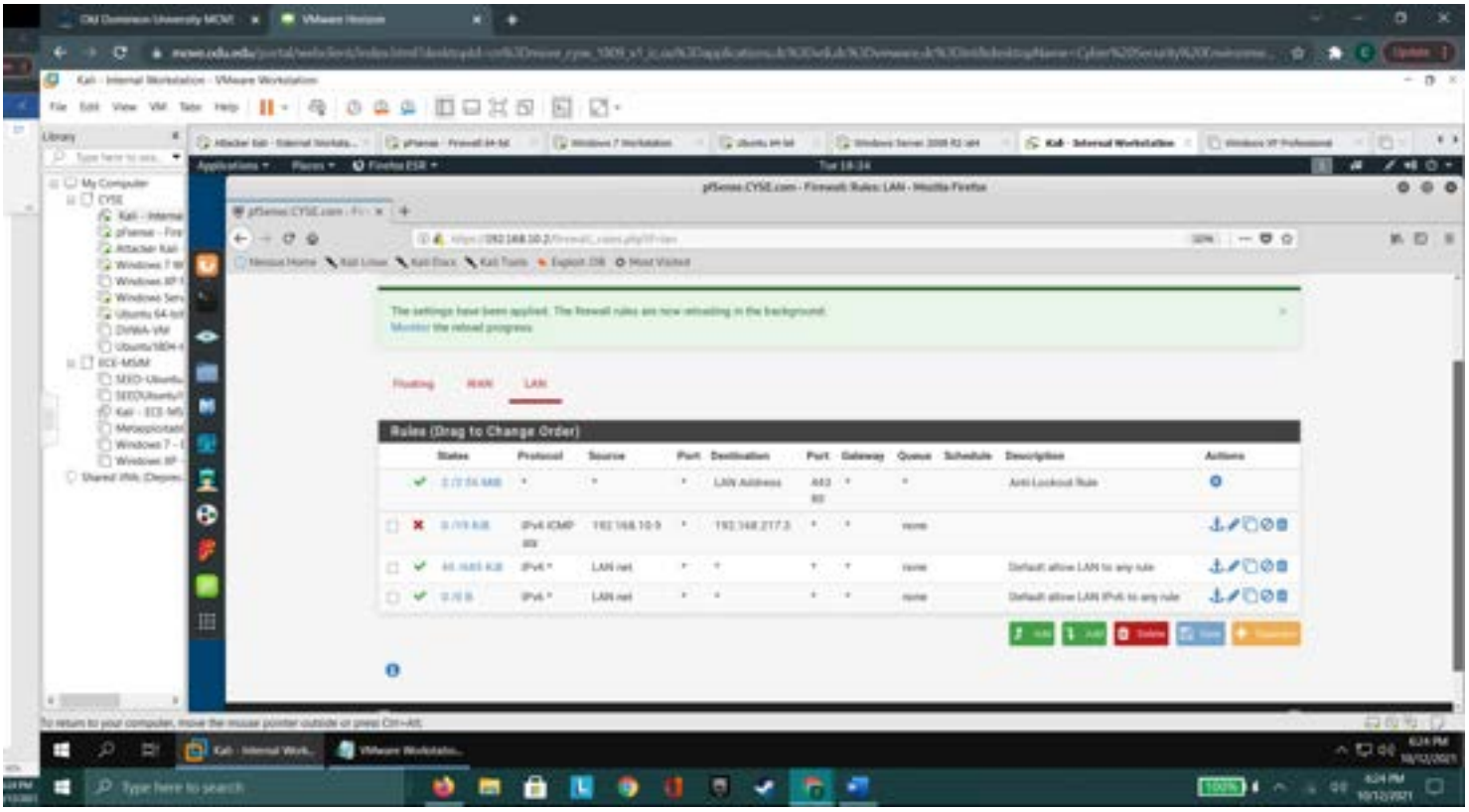

Attacker Kali - External Workstation - VMware Workstation
root@CS2APenTest: ~
64 bytes from 192.168.10.10: icmp_seq=7 ttl=63 time=1.21 ms
64 bytes from 192.168.10.10: icmp_seq=8 ttl=63 time=1.26 ms
64 bytes from 192.168.10.10: icmp_seq=9 ttl=63 time=1.46 ms
64 bytes from 192.168.10.10: icmp_seq=10 ttl=63 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:~#

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.



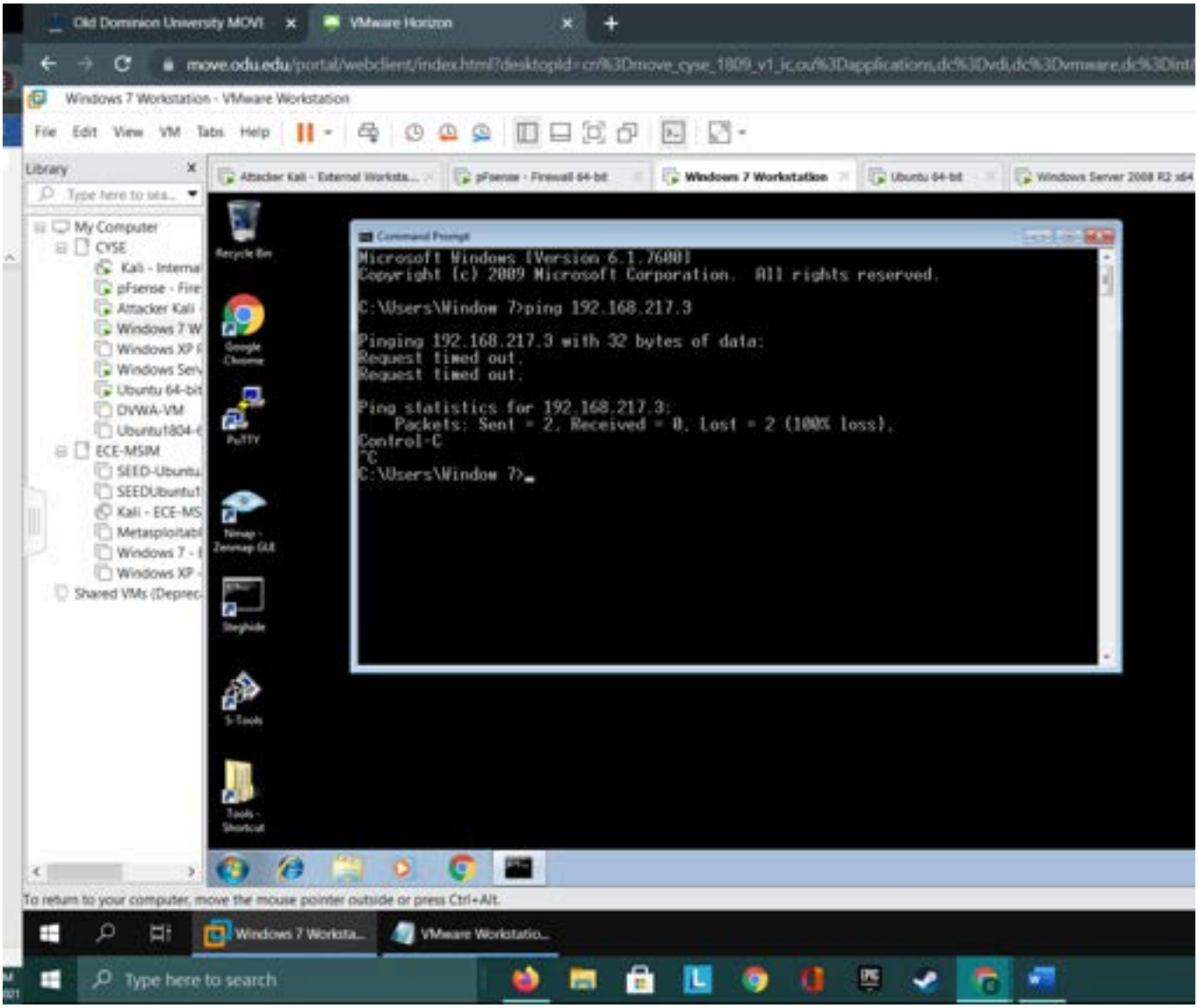
3. *Now, configure the pfSense to block all ICMP traffic from Windows 7 VM to External Kali. After you applied the rule, answer the following questions: (30 points)*

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.



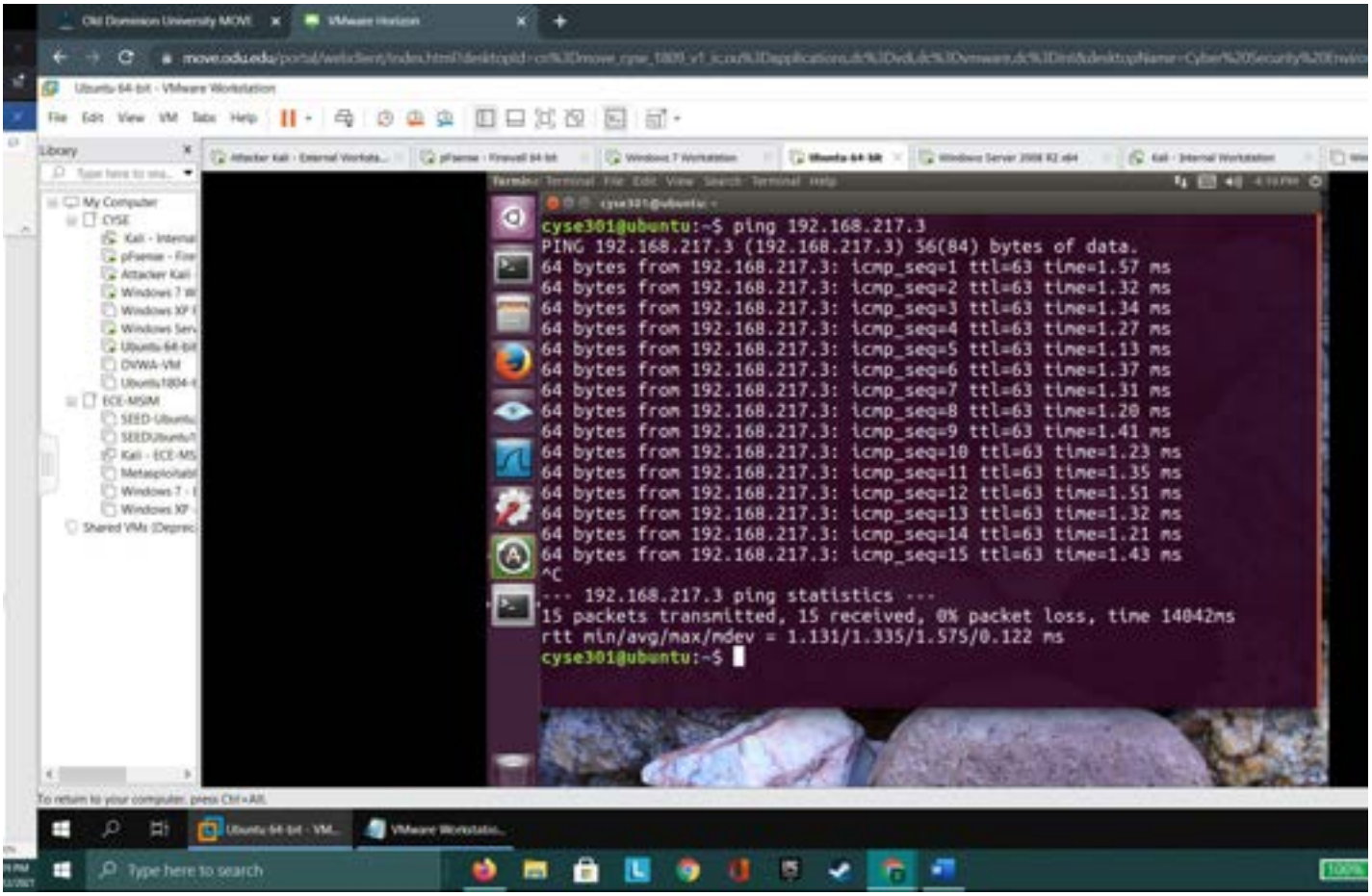
a. *Can you ping External Kali from Windows 7?*

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.



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).