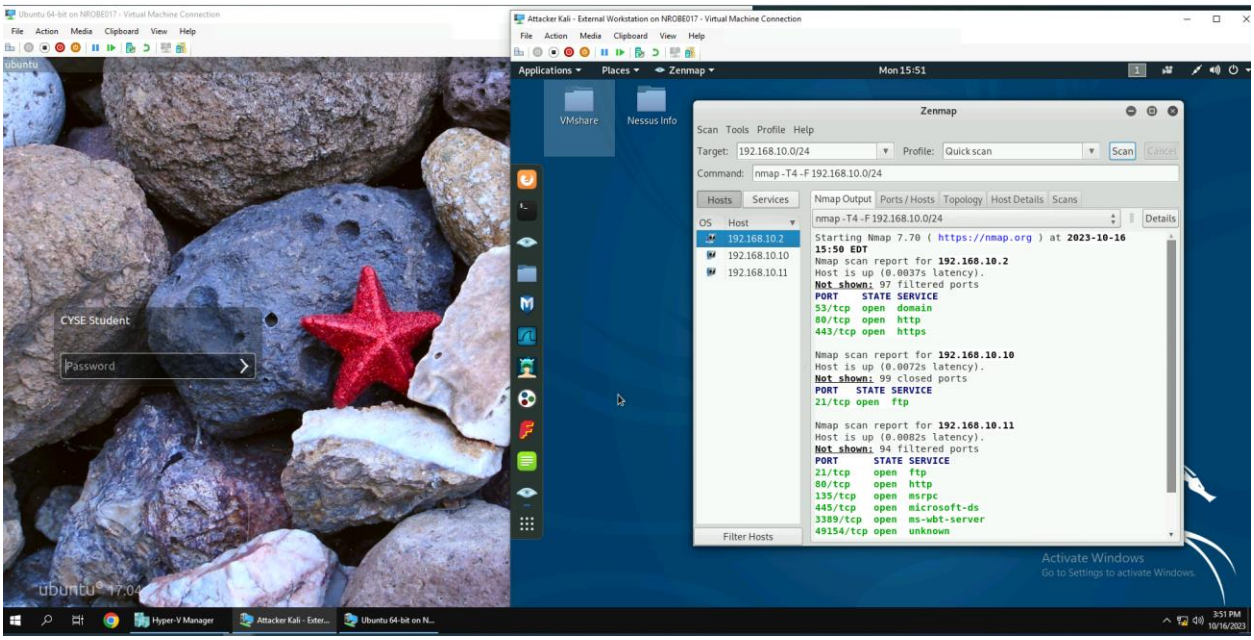
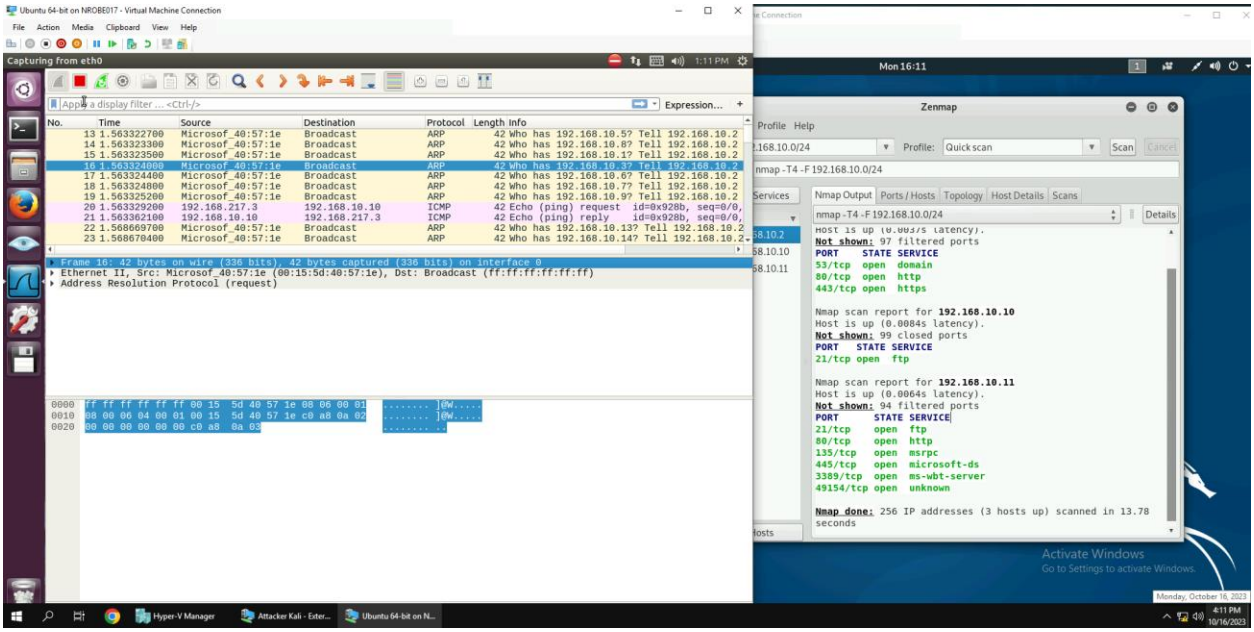
Nicholas Robertson

Assignment 3 Sword and Shield

Task A

1. 

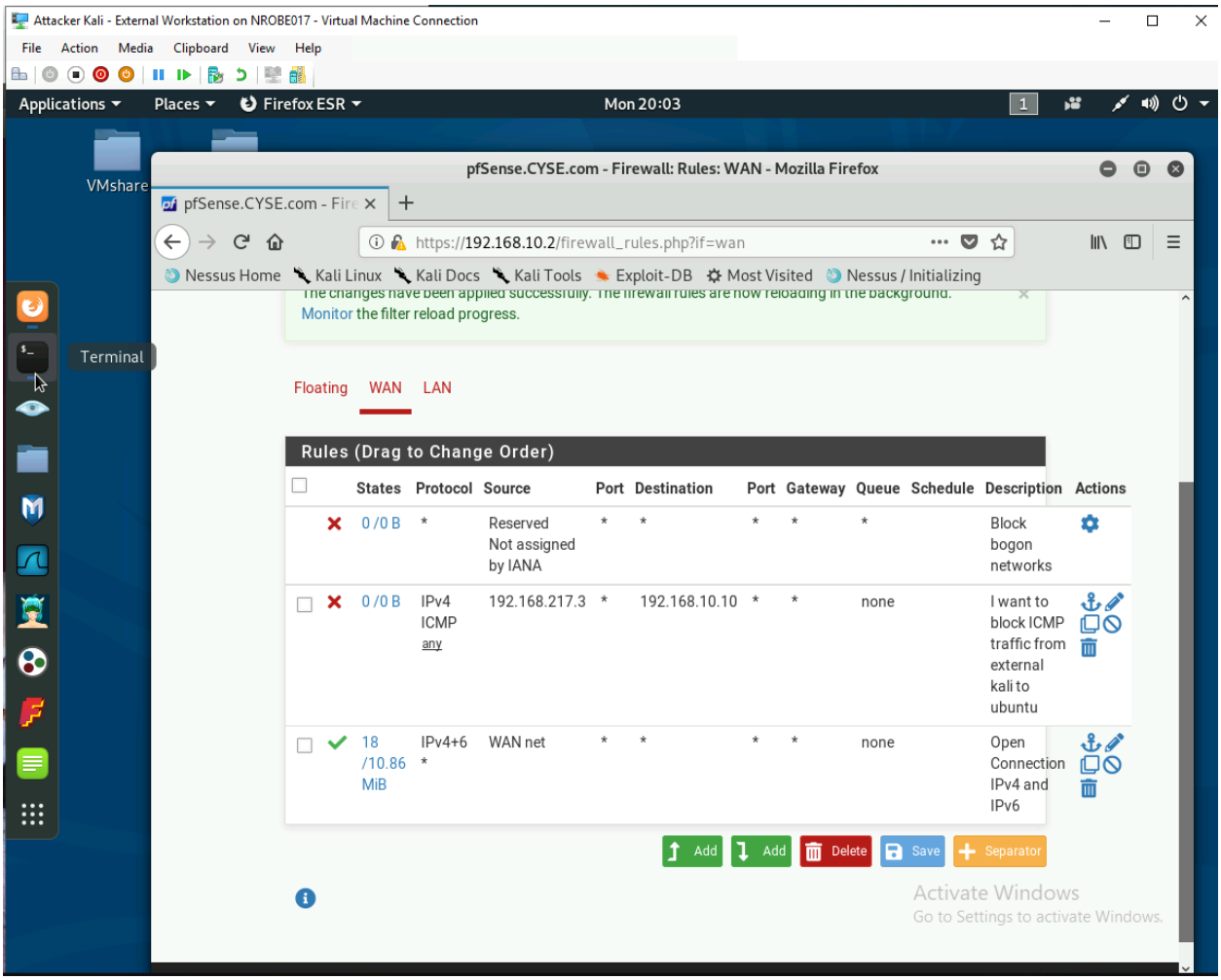
2. 

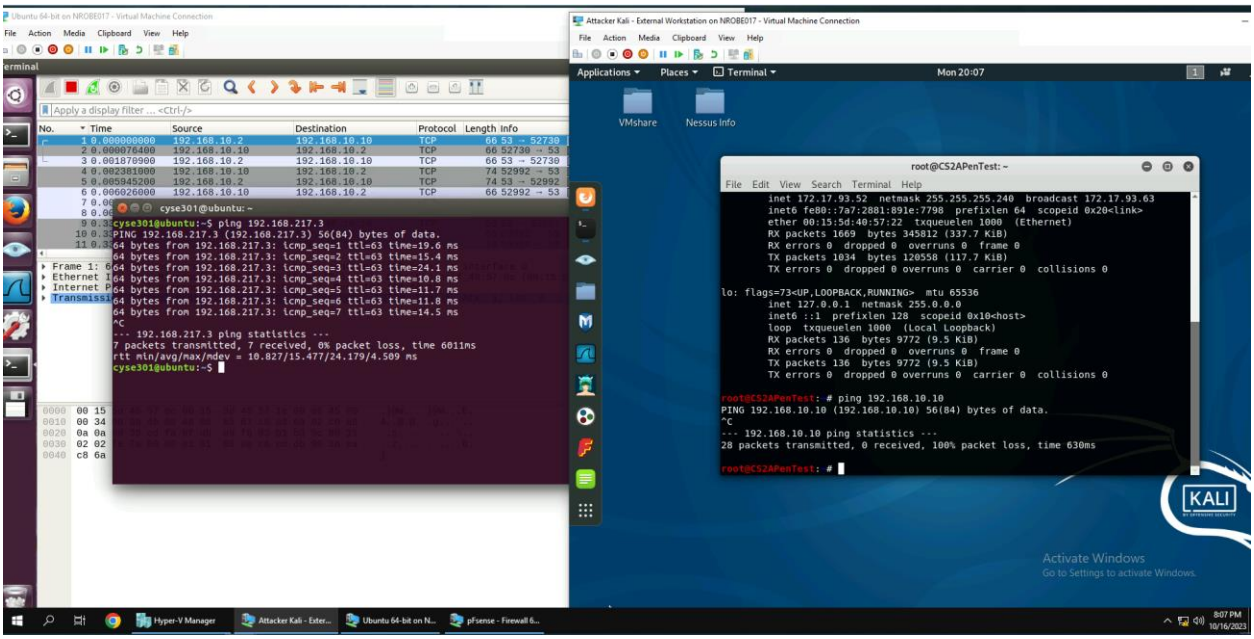
I Allowed for the external kali to quick scan the target 192.168.10.0/24 while Ubuntu was running Wireshark in the background, which took it about 13 seconds to complete. After it was done and zenmap was able to display the open ports and the services, I looked over the wire shark to see what it had captured. What Wireshark had displayed was a ton of source packets listing the different IP address of the machines that ware running in the background, like 192.168.217.3, 192.168.10.10 and for the windows 2008 machine it was displaying in the source column Microsof_40:57:1e. On the destination column, it ranges from the different IP addresses bouncing off each other (so, 192.168.217.3 in the source and 192.168.10.10 in the destination), but in the destination column for the corresponding Mircrosof_40:57:1e it says Broadcast, which means that the any packets from the Microsoft 2008 machine, the destination for all stations on the network segment is considered broadcast traffic. These broadcasts usually transmit the packets of ARP or DHCP, in this case for the Microsoft 2008 machine were transporting ARP packets, while the other machines (192.168.217.3 and 192.168.10.10) were giving off the ICMP packets. Finally, information section of 192.168.217.3 and 192.168.10.10 has the standard Echo (ping) request/reply action, but the Microsoft 2008 machine info message was, “Who has 192.168.10.44? Tell 192.168.10.2” and “Who has 192.168.10.220? Tell 192.168.10.2”.

Task B

B1

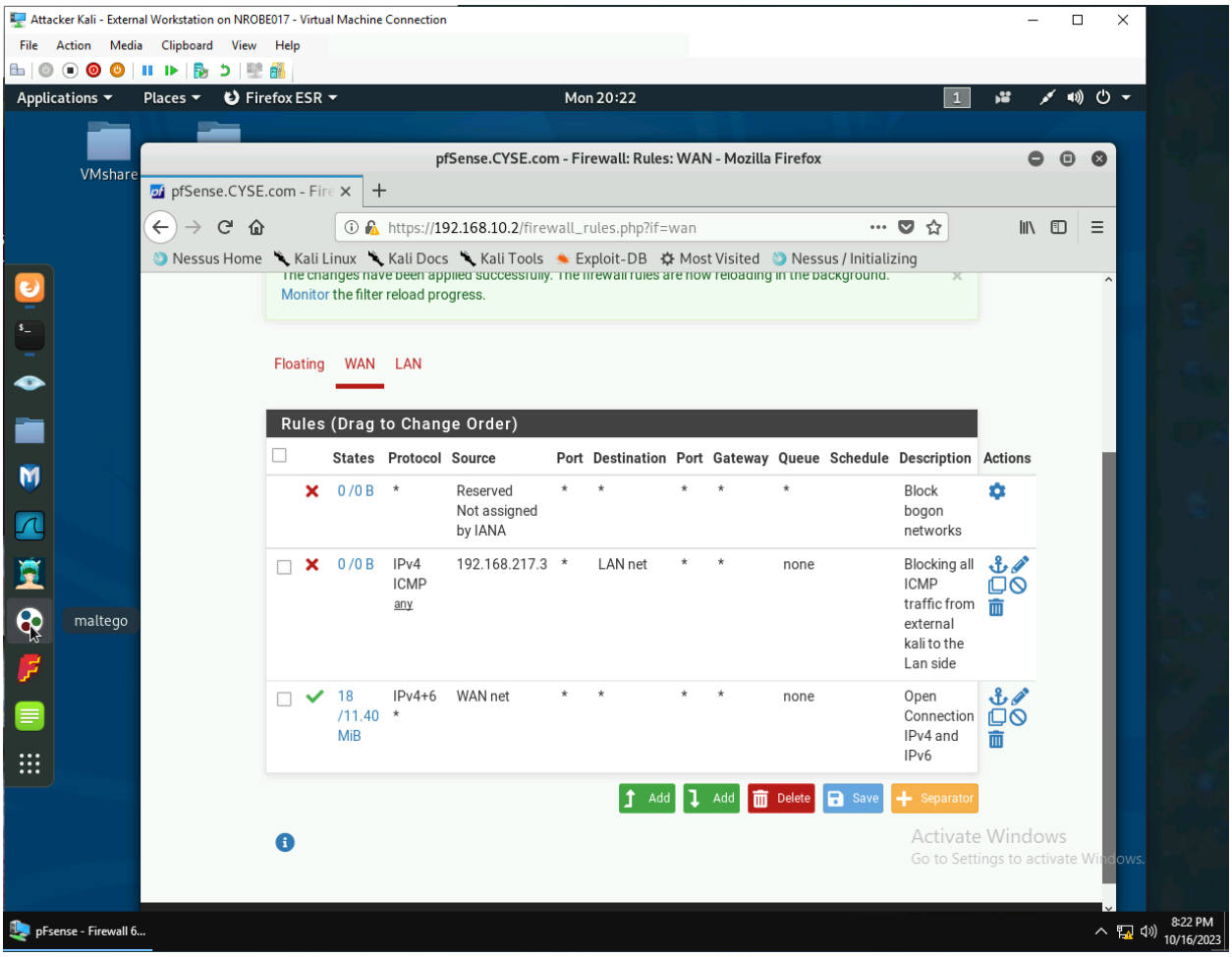
Rule #	Interface	Action	Source IP	Destination IP	Protocol (Port # if appliable)
1	WAN	Block	192.168.217.3	192.168.10.10	ICMP

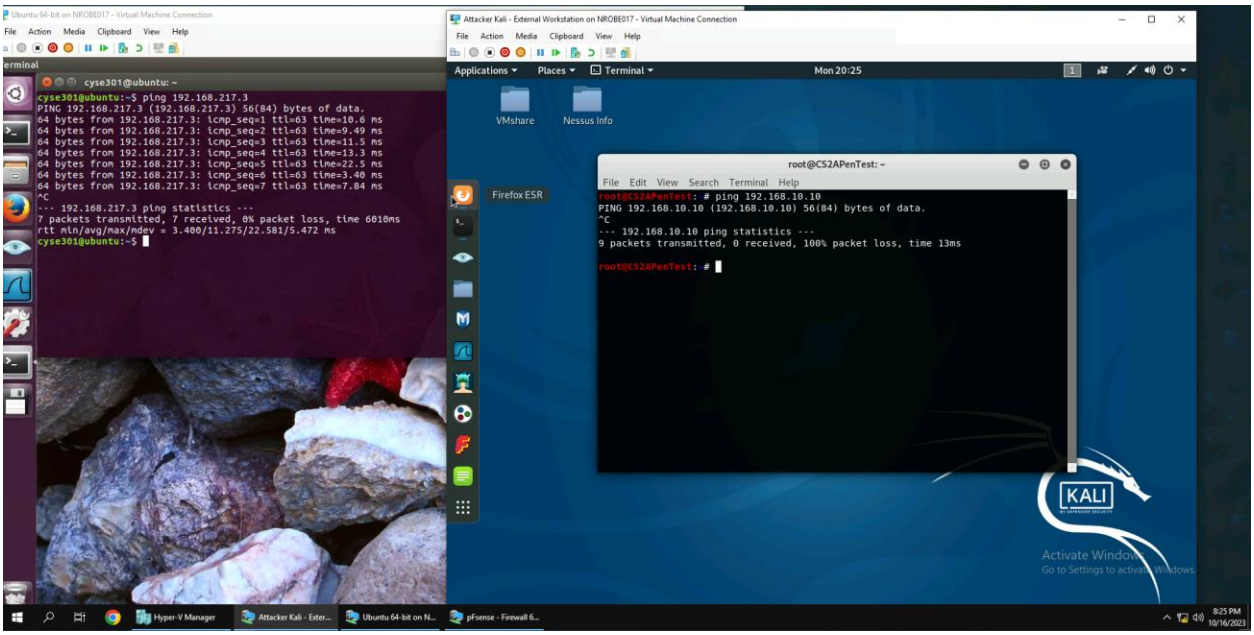

Attacker Kali - External Workstation on NROBE017 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Firefox ESR Mon 20:03
VMshare
pfSense.CYSE.com - Firewall: Rules: WAN - Mozilla Firefox
pfSense.CYSE.com - Fire
https://192.168.10.2/firewall_rules.php?if=wan
Nessus Home Kali Linux Kali Docs Kali Tools Exploit-DB Most Visited Nessus / Initializing
Terminal
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 * 192.168.10.10 * * none I want to block ICMP traffic from external kali to ubuntu
18 /10.86 MiB IPv4+6 * WAN net * * * * none Open Connection IPv4 and IPv6
Add Add Delete Save Separator
Activate Windows
Go to Settings to activate Windows.

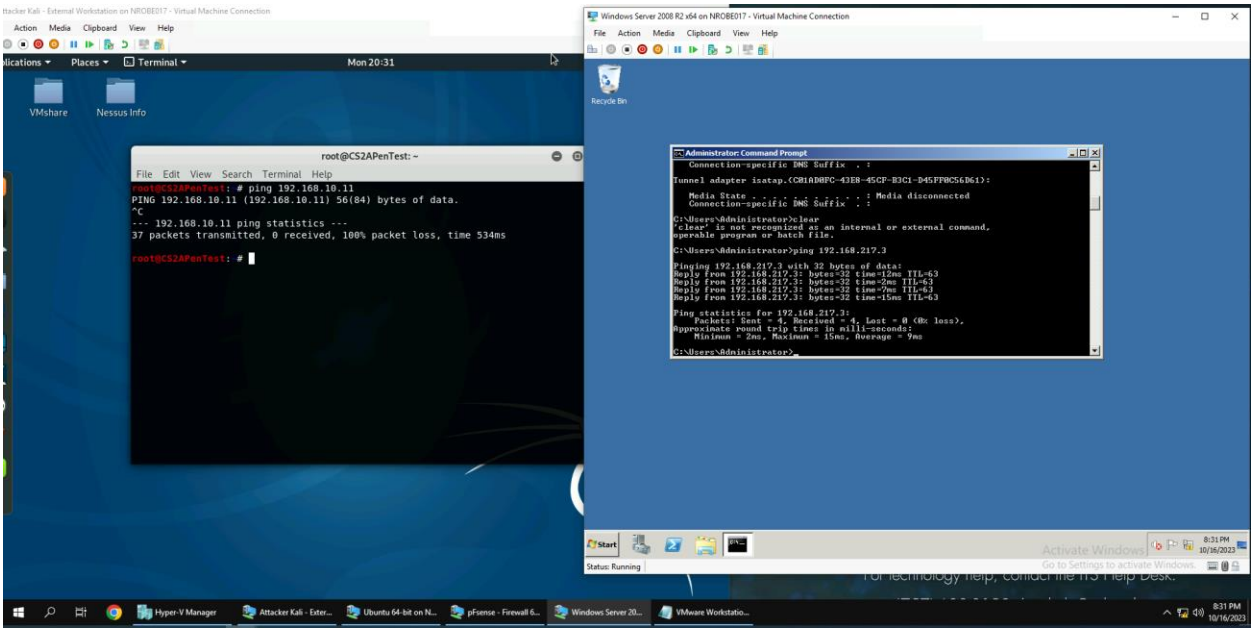

Attacker Kali - External Workstation on NROBE017 - Virtual Machine Connection
Applications Places Terminal Mon 20:07
VMshare
Nessus Info
root@CS2APenTest: ~
File Edit View Search Terminal Help
inet 172.17.93.52 netmask 255.255.255.240 broadcast 172.17.93.63
inet6 fe80::7a7:2881:891e:7798 prefixlen 64 scopeid 0x20<link>
ether 00:15:5d:40:57:22 txqueuelen 1000 (Ethernet)
RX packets 1669 bytes 345812 (337.7 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 1034 bytes 120558 (117.7 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 136 bytes 9772 (9.5 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 136 bytes 9772 (9.5 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
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 ---
28 packets transmitted, 0 received, 100% packet loss, time 630ms
root@CS2APenTest: #
KALI
Activate Windows
Go to Settings to activate Windows.

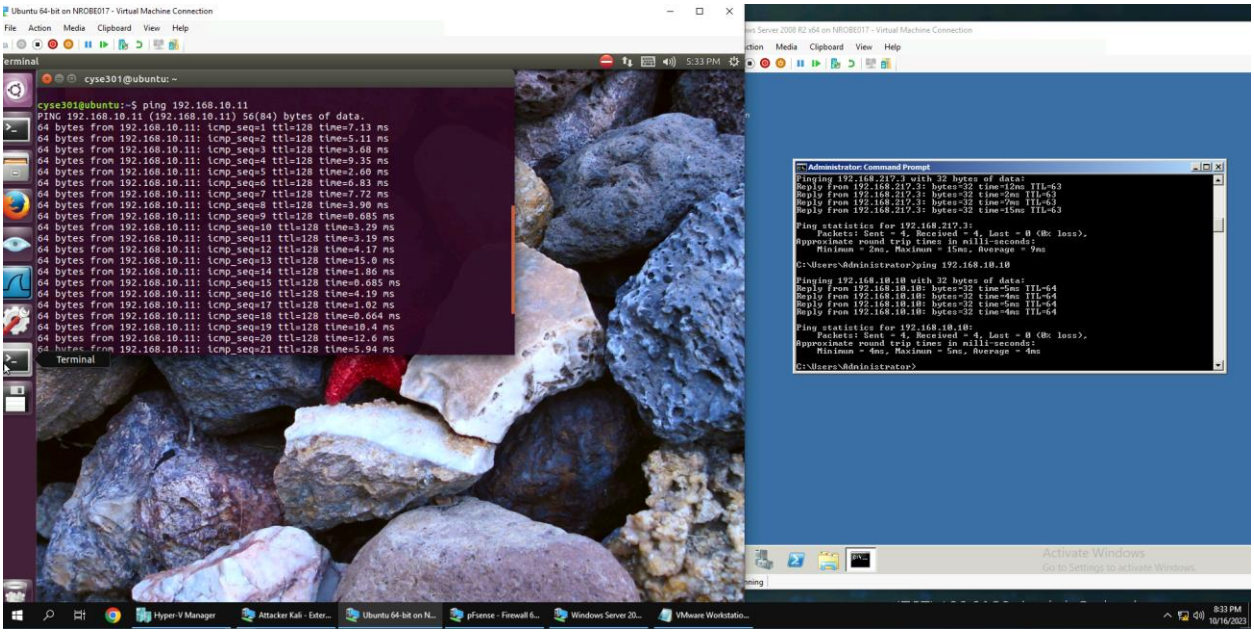
B2

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable
1	WAN	Block	192.168.217.3	LAN net	ICMP




Ubuntu 64-bit on NROBE017 - Virtual Machine Connection
File Action Media Clipboard View Help
cyse301@ubuntu: ~
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=10.6 ms
64 bytes from 192.168.217.3: icmp_seq=2 ttl=63 time=9.49 ms
64 bytes from 192.168.217.3: icmp_seq=3 ttl=63 time=11.5 ms
64 bytes from 192.168.217.3: icmp_seq=4 ttl=63 time=13.3 ms
64 bytes from 192.168.217.3: icmp_seq=5 ttl=63 time=22.5 ms
64 bytes from 192.168.217.3: icmp_seq=6 ttl=63 time=3.40 ms
64 bytes from 192.168.217.3: icmp_seq=7 ttl=63 time=7.84 ms
^C
--- 192.168.217.3 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6010ms
rtt min/avg/max/mdev = 3.400/11.275/22.581/5.472 ms
cyse301@ubuntu:~$
Attacker Kali - External Workstation on NROBE017 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Mon 20:25
VMshare
Nessus Info
Firefox ESR
root@CS2APenTest: ~
File Edit View Search Terminal Help
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 ---
9 packets transmitted, 0 received, 100% packet loss, time 13ms
root@CS2APenTest: #
KALI
Activate Windows
Go to Settings to activate Windows.
Hyper-V Manager
Attacker Kali - Exter...
Ubuntu 64-bit on N...
pFsense - Firewall 6...
8:25 PM
10/16/2023

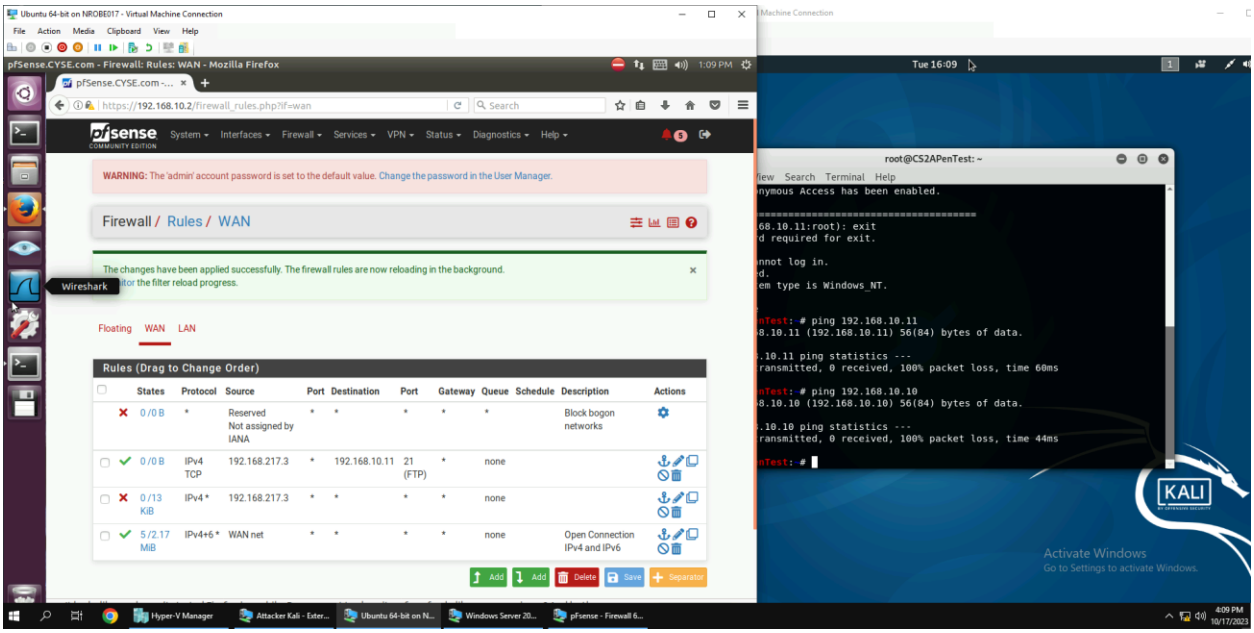

Action Media Clipboard View Help
Places Terminal Mon 20:31
VMshare
Nessus Info
root@CS2APenTest: ~
File Edit View Search Terminal Help
root@CS2APenTest: # ping 192.168.10.11
PING 192.168.10.11 (192.168.10.11) 56(84) bytes of data.
^C
--- 192.168.10.11 ping statistics ---
37 packets transmitted, 0 received, 100% packet loss, time 534ms
root@CS2APenTest: #
Windows Server 2008 R2 x64 on NROBE017 - Virtual Machine Connection
File Action Media Clipboard View Help
Recycle Bin
Administrator: Command Prompt
Connection-specific DNS Suffix . :
Tunnel adapter isatap.CCB1ADBFC-43E8-45CF-B3C1-D45FF0C56D61):
Media State . . . . . Media disconnected
Connection-specific DNS Suffix . :
C:\Users\Administrator>clear
'clear' is not recognized as an internal or external command,
operable program or batch file.
C:\Users\Administrator>ping 192.168.217.3
Pinging 192.168.217.3 with 32 bytes of data:
Reply from 192.168.217.3: bytes=32 time=12ms TTL=63
Reply from 192.168.217.3: bytes=32 time=2ms TTL=63
Reply from 192.168.217.3: bytes=32 time=7ms TTL=63
Reply from 192.168.217.3: bytes=32 time=15ms TTL=63
Ping statistics for 192.168.217.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 15ms, Average = 9ms
C:\Users\Administrator>
Start
Status: Running
Activate Windows
Go to Settings to activate Windows.
8:31 PM
10/16/2023
Hyper-V Manager
Attacker Kali - Exter...
Ubuntu 64-bit on N...
pFsense - Firewall 6...
Windows Server 20...
VMware Workstatio...

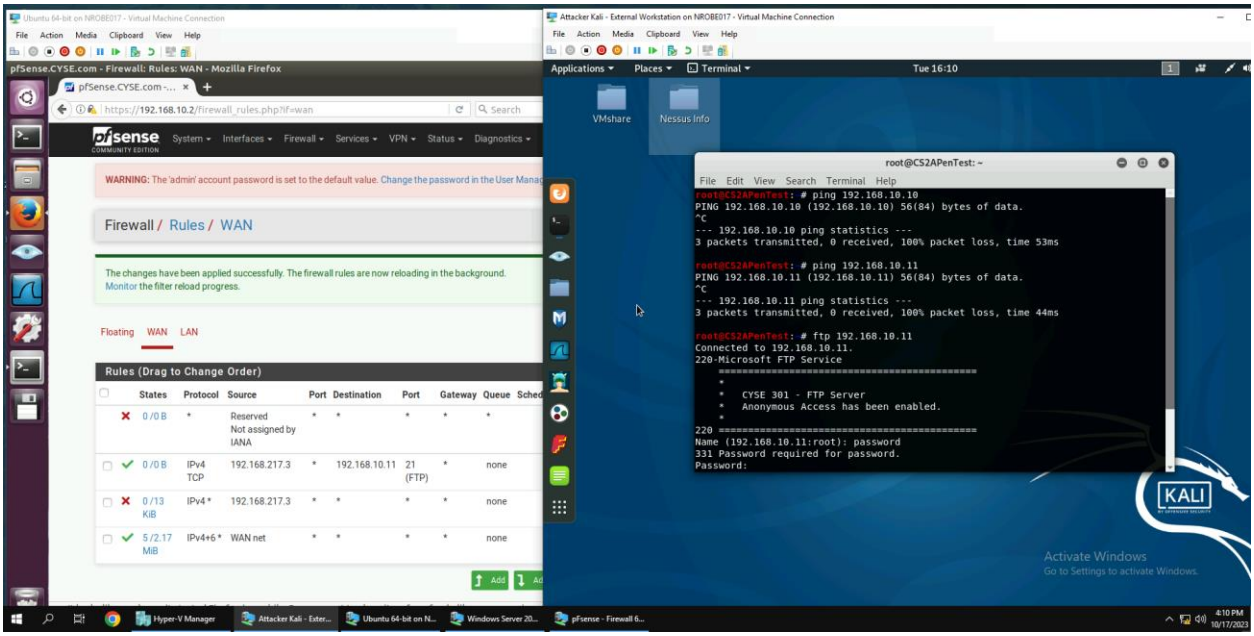


Applying this rule made it where the attacker kali could not communicate to any of the devices that were on the LAN side, but the devices within the LAN could communicate with the attacker and to each other. So, for instance ubuntu and Microsoft 2008 could communicate with each other and to attacker.

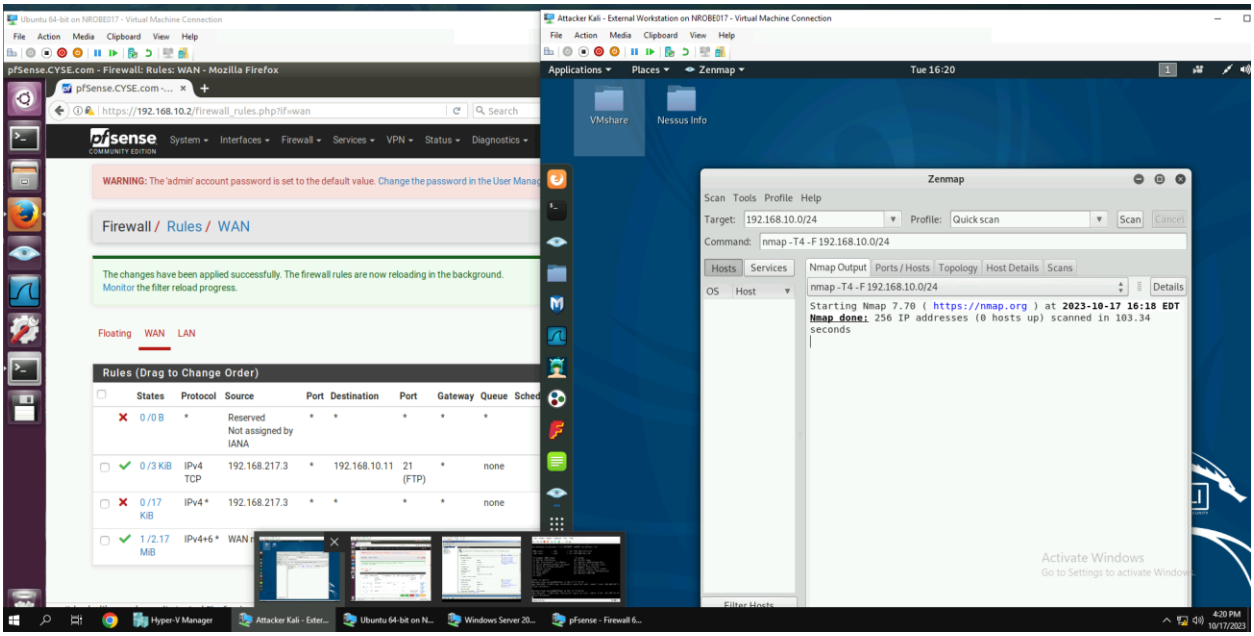
B3

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
1	WAN	Pass	192.168.217.3	192.168.10.11	TCP
2	WAN	Block	192.168.217.3	Any	Any
3	WAN	Pass	WAN net	Any	Any


Ubuntu 64-bit on NROBE017 - Virtual Machine Connection
pfSense.CYSE.com - Firewall: Rules: WAN - Mozilla Firefox
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Firewall / Rules / WAN
The changes have been applied successfully. The firewall rules are now reloading in the background.
Floating WAN LAN
Rules (Drag to Change Order)
Wireshark
root@CS2APenTest: ~
KALI
Activate Windows


pfSense.CYSE.com - Firewall: Rules: WAN - Mozilla Firefox
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manag
Firewall / Rules / WAN
The changes have been applied successfully. The firewall rules are now reloading in the background.
Floating WAN LAN
Rules (Drag to Change Order)
Attacker Kali - External Workstation on NROBE017 - Virtual Machine Connection
VMshare
Nessus Info
root@CS2APenTest: ~
KALI
Activate Windows

B4



After keeping the pfsense there is no subnet topology, no service, no backend software information and no port openings. There is no information showing on the zenmap/nmap at all after a quick scan. This is most likely due to everything being blocked to the attacker kali machine.