OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #3 - Sword vs. Shield

Darren Pritchard

01241796

Task A: Sword - Network Scanning (20+ 20 = 40 points)

Power on the listed VMs and complete the following steps from the External Kali (you can use either

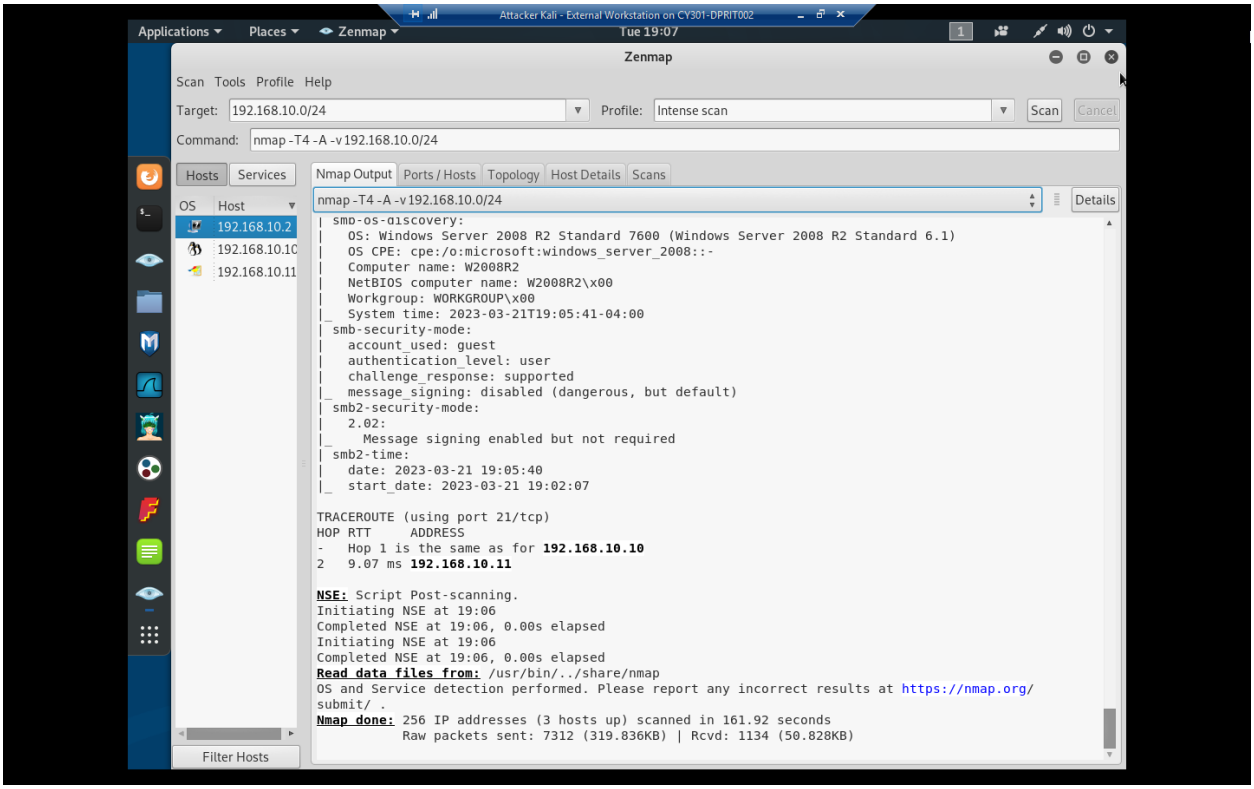
nmap or zenmap to complete the assignment)

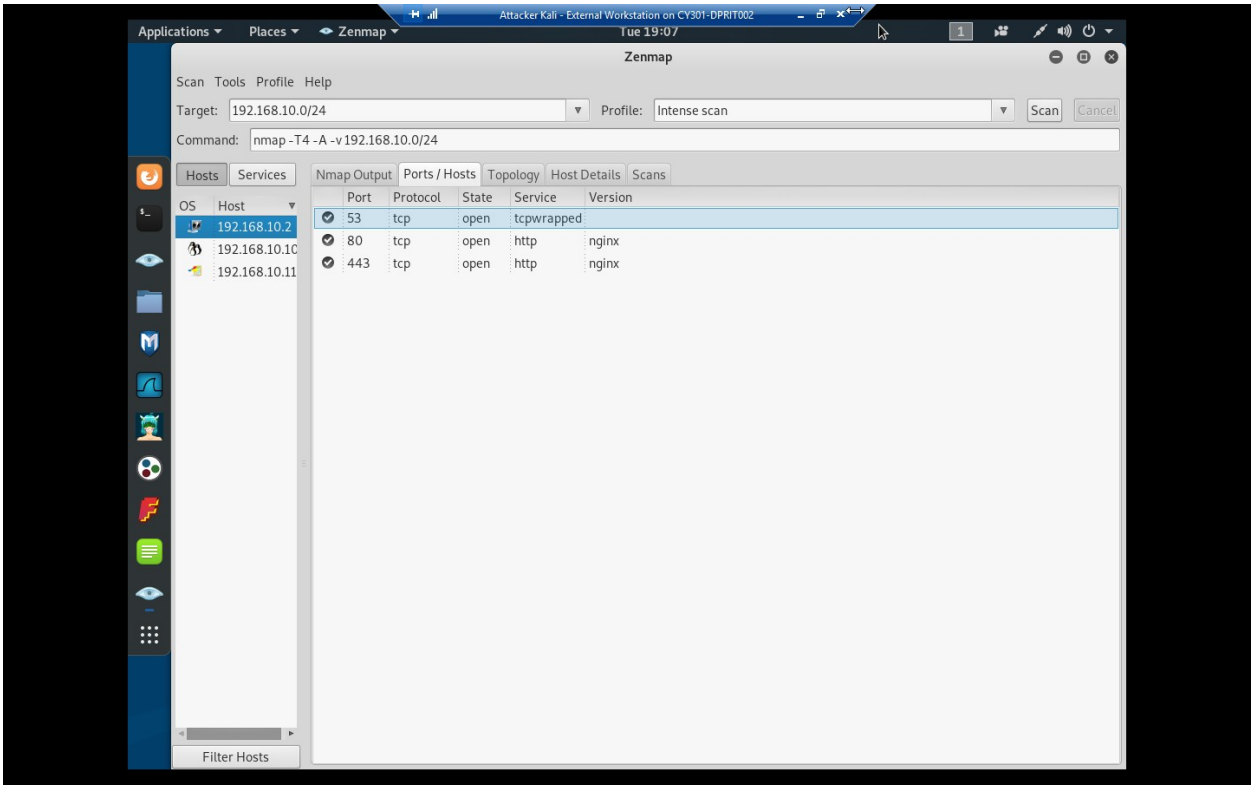
- **External Kali**
- **pfSense**
- **Ubuntu**
- **Windows Server 2008**

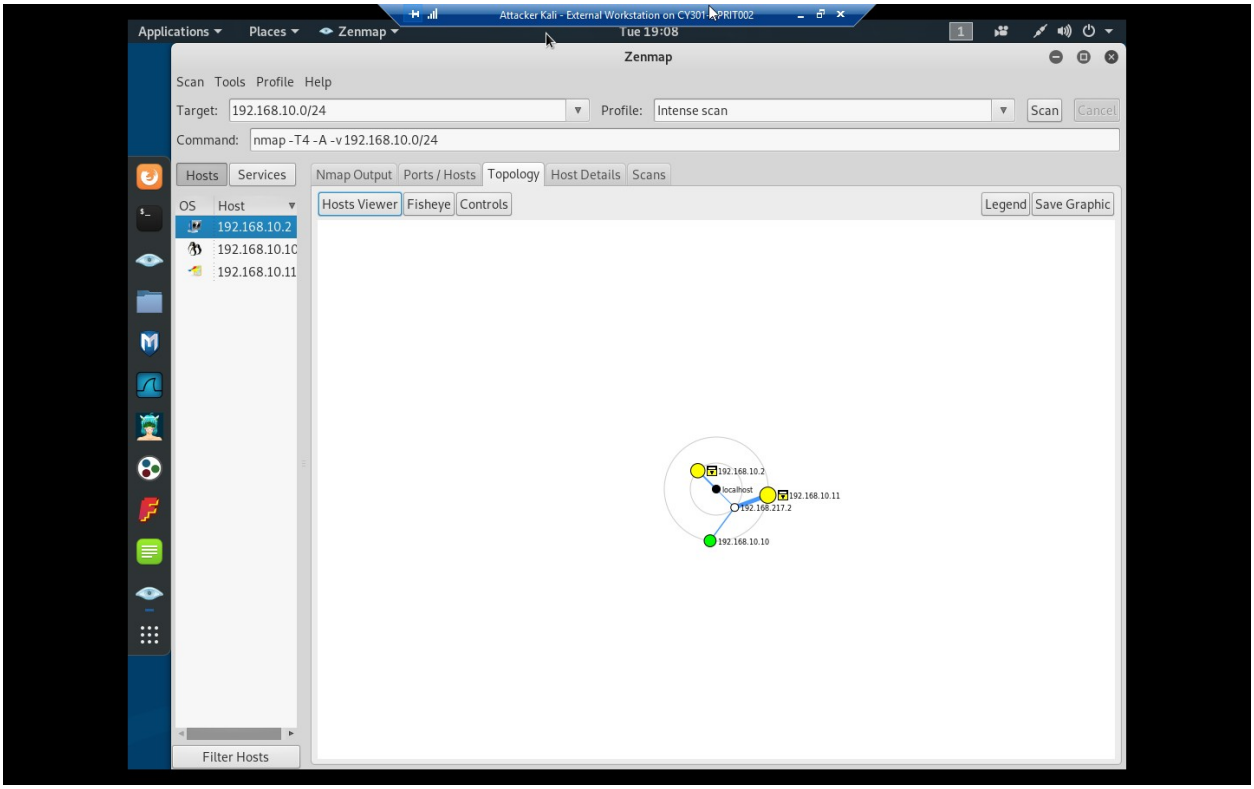
Make sure you didn't add/delete any firewall policy before continuing.

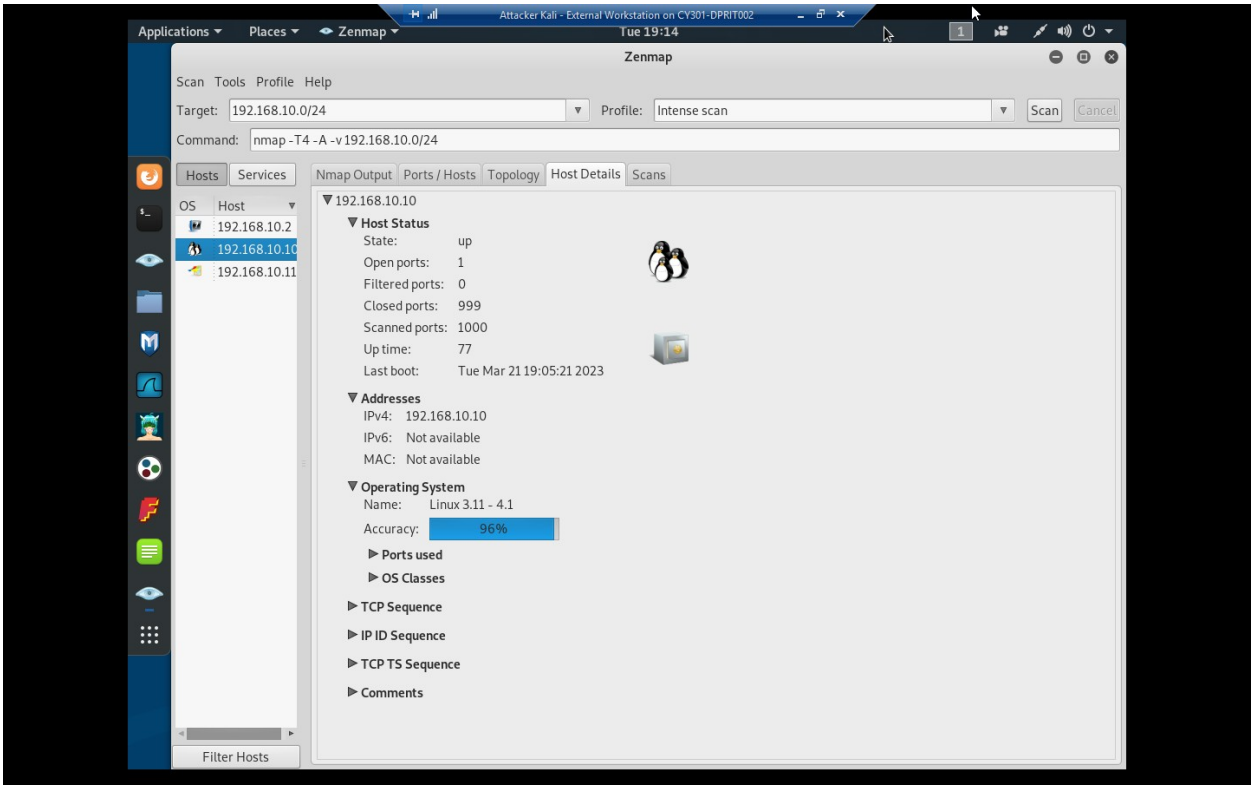
1. Use Nmap to profile the basic information about the subnet topology (including open ports information, operation systems, etc.) You need to get the service and backend software information associated with each opening port in each VM.

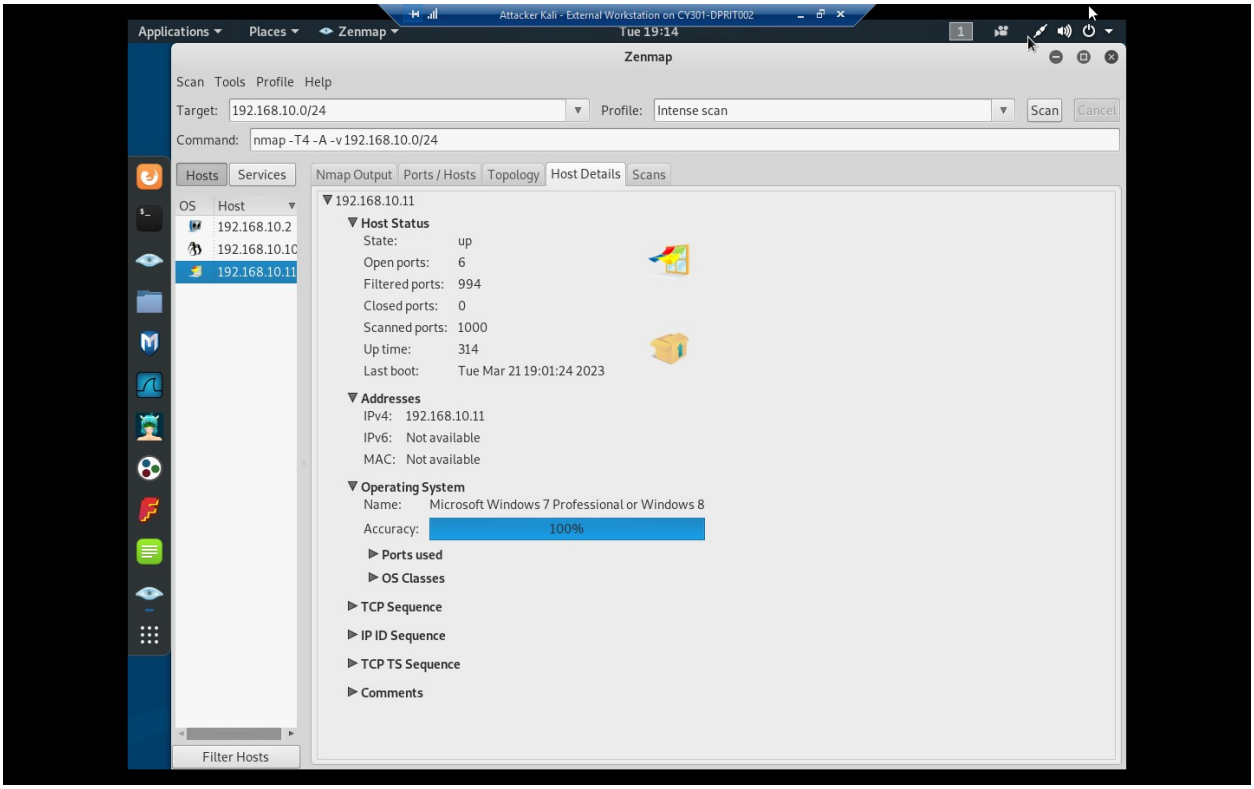
2. Run Wireshark in Ubuntu VM while External Kali is scanning the network. Discuss the traffic pattern you observed. What do you find? Please write a 200-word essay to discuss your findings.


Attacker Kali - External Workstation on CY301-DPRIT002
Applications
Places
Zenmap
Tue 19:07
Zenmap
Scan Tools Profile Help
Target: 192.168.10.0/24
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 192.168.10.0/24
Hosts
Services
OS
Host
192.168.10.2
192.168.10.10
192.168.10.11
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -A -v 192.168.10.0/24
Details
| smb-os-discovery:
| OS: Windows Server 2008 R2 Standard 7600 (Windows Server 2008 R2 Standard 6.1)
| OS CPE: cpe:/o:microsoft:windows_server_2008::-
| Computer name: W2008R2
| NetBIOS computer name: W2008R2\x00
| Workgroup: WORKGROUP\x00
|_ System time: 2023-03-21T19:05:41-04:00
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb2-security-mode:
| 2.02:
|_ Message signing enabled but not required
| smb2-time:
| date: 2023-03-21 19:05:40
|_ start_date: 2023-03-21 19:02:07
TRACEROUTE (using port 21/tcp)
HOP RTT ADDRESS
- Hop 1 is the same as for 192.168.10.10
2 9.07 ms 192.168.10.11
NSE: Script Post-scanning.
Initiating NSE at 19:06
Completed NSE at 19:06, 0.00s elapsed
Initiating NSE at 19:06
Completed NSE at 19:06, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 161.92 seconds
Raw packets sent: 7312 (319.836KB) | Rcvd: 1134 (50.828KB)
Filter Hosts

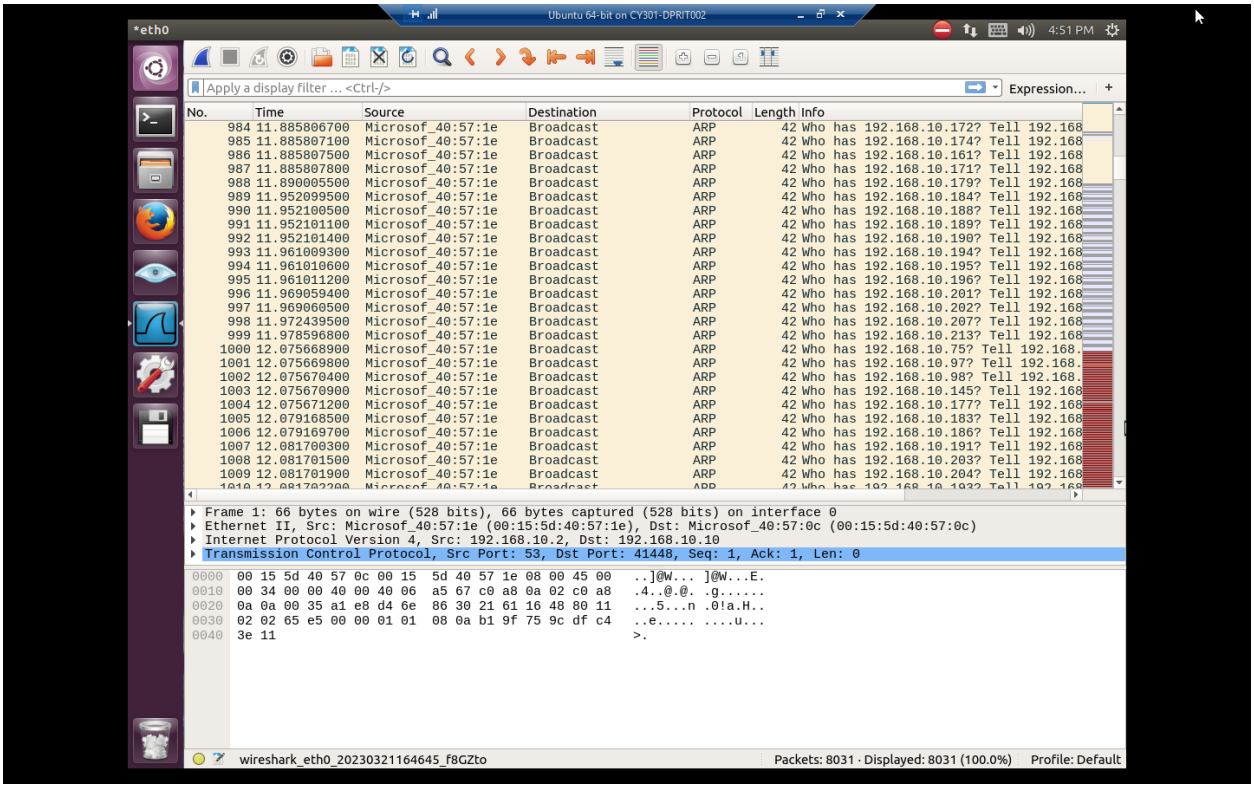

Attacker Kali - External Workstation on CY301-DPRIT002
Applications
Places
Zenmap
Tue 19:07
Zenmap
Scan Tools Profile Help
Target: 192.168.10.0/24
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 192.168.10.0/24
Hosts
Services
OS
Host
192.168.10.2
192.168.10.10
192.168.10.11
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Port
Protocol
State
Service
Version
53 tcp open tcpwrapped
80 tcp open http nginx
443 tcp open http nginx
Filter Hosts

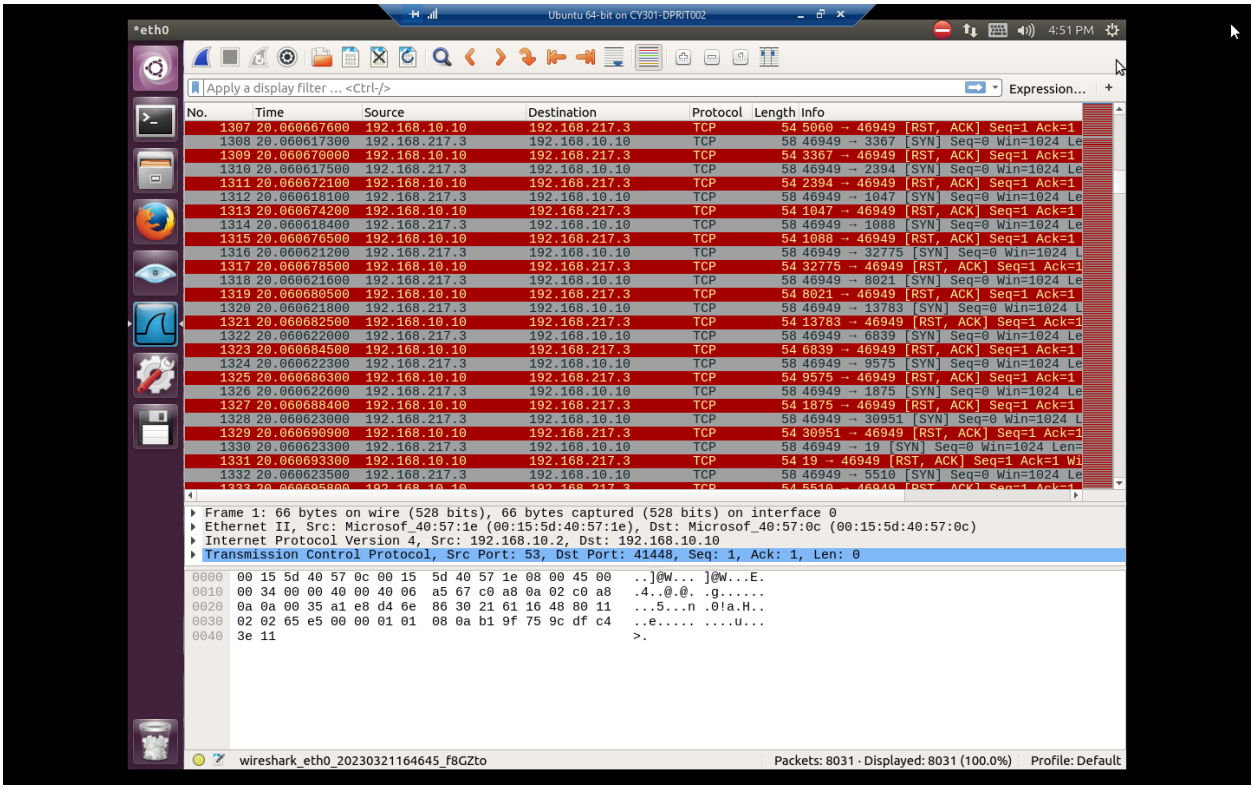

Attacker Kali - External Workstation on CY301-DPRIT002
Applications
Places
Zenmap
Tue 19:08
Zenmap
Scan Tools Profile Help
Target: 192.168.10.0/24
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 192.168.10.0/24
Hosts
Services
OS
Host
192.168.10.2
192.168.10.10
192.168.10.11
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Hosts Viewer
Fisheye
Controls
Legend
Save Graphic
192.168.10.2
localhost
192.168.10.11
192.168.217.2
192.168.10.10
Filter Hosts


Attacker Kali - External Workstation on CY301-DPRIT002
Applications
Places
Zenmap
Tue 19:14
Zenmap
Scan Tools Profile Help
Target: 192.168.10.0/24
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 192.168.10.0/24
Hosts
Services
OS
Host
192.168.10.2
192.168.10.10
192.168.10.11
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
192.168.10.10
Host Status
State: up
Open ports: 1
Filtered ports: 0
Closed ports: 999
Scanned ports: 1000
Up time: 77
Last boot: Tue Mar 21 19:05:21 2023
Addresses
IPv4: 192.168.10.10
IPv6: Not available
MAC: Not available
Operating System
Name: Linux 3.11 - 4.1
Accuracy: 96%
Ports used
OS Classes
TCP Sequence
IP ID Sequence
TCP TS Sequence
Comments
Filter Hosts



Explanation: *Nmap output along with the listed open ports, network topology, and host details after the initial scan in Zenmap.*





Explanation: *Screenshots of Wireshark in Ubuntu after the scan was complete showing some examples of the ARP and RST packets that were sent during the scan.*

Essay: As we run the network scan, we can see a lot of traffic on the network, with multiple packets being sent and received. We can see SYN, ACK, and RST packets being exchanged between External Kali and each VM. These packets are part of the three-way handshake process that establishes a TCP connection.

We can also see other types of packets, such as ICMP packets, which are used for diagnostic purposes, and ARP packets, which are used for mapping IP addresses to MAC addresses. ARP packets can be used to build a map of the network topology by discovering the IP addresses and MAC addresses of the devices on the network. This information can be used to identify the devices that are alive and active on the network and to determine the relationships between the devices. The ICMP packets, in this case, are being used to check for open ports on our systems.

We can observe that network scanning generates a significant amount of traffic on the network, which can be detected by network intrusion detection systems. If we wanted to avoid being detected while doing this, we could use techniques like rate limiting our port scanning frequency to better blend into the normal network traffic.

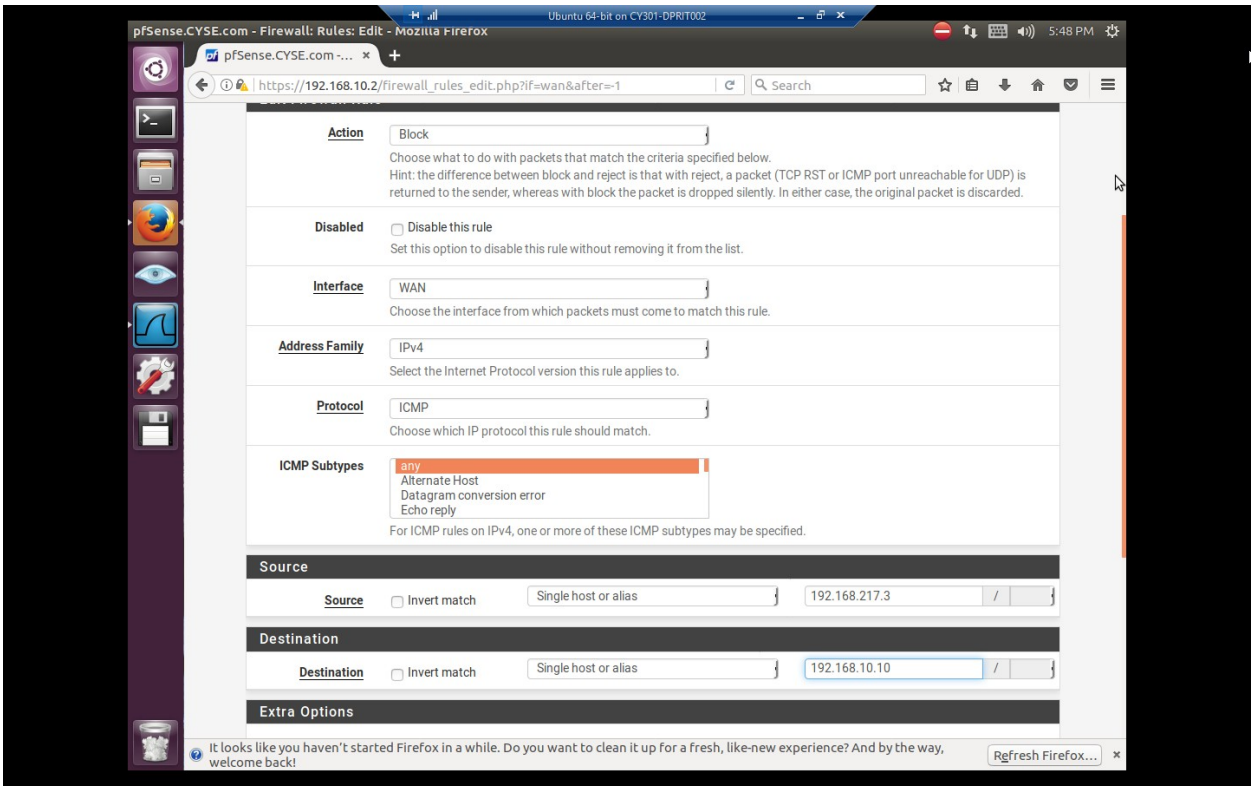
Task B: Shield – Protect your network with firewall (10 + 10+ 20 + 20 = 60 points)

In order to receive full credits, you need to fill the table (add more rows if needed), implement the

firewall rule(s), show me the screenshot of your firewall table, and verify the results.

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

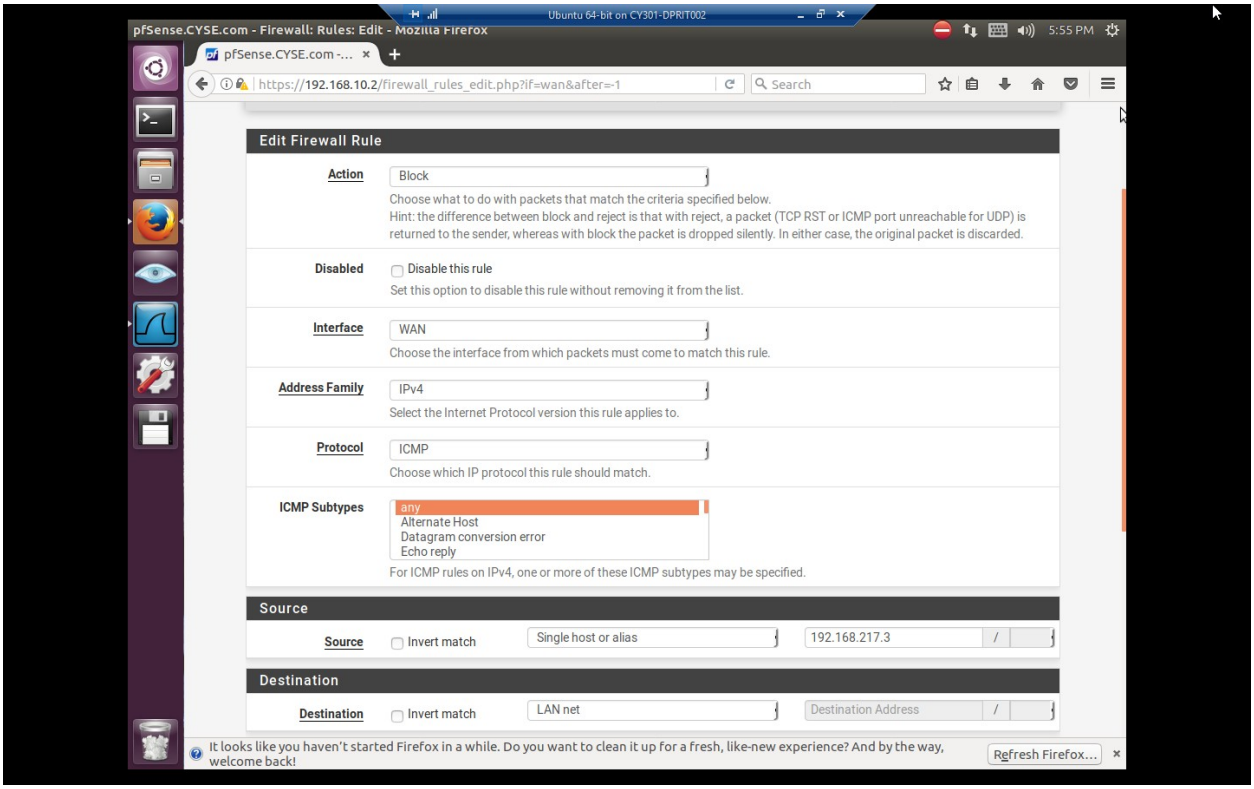
Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if applicable)
1	WAN	Block	192.168.217.3	192.168.10.10	ICMP



Explanation: *Settings on the pfsense web interface for this rule, showing that we are going to be blocking the ICMP traffic from 192.168.217.3 (External Kali)*

2. Clear the previous firewall policies and configure the pfSense firewall to block all ICMP traffic from External Kali to the LAN side.

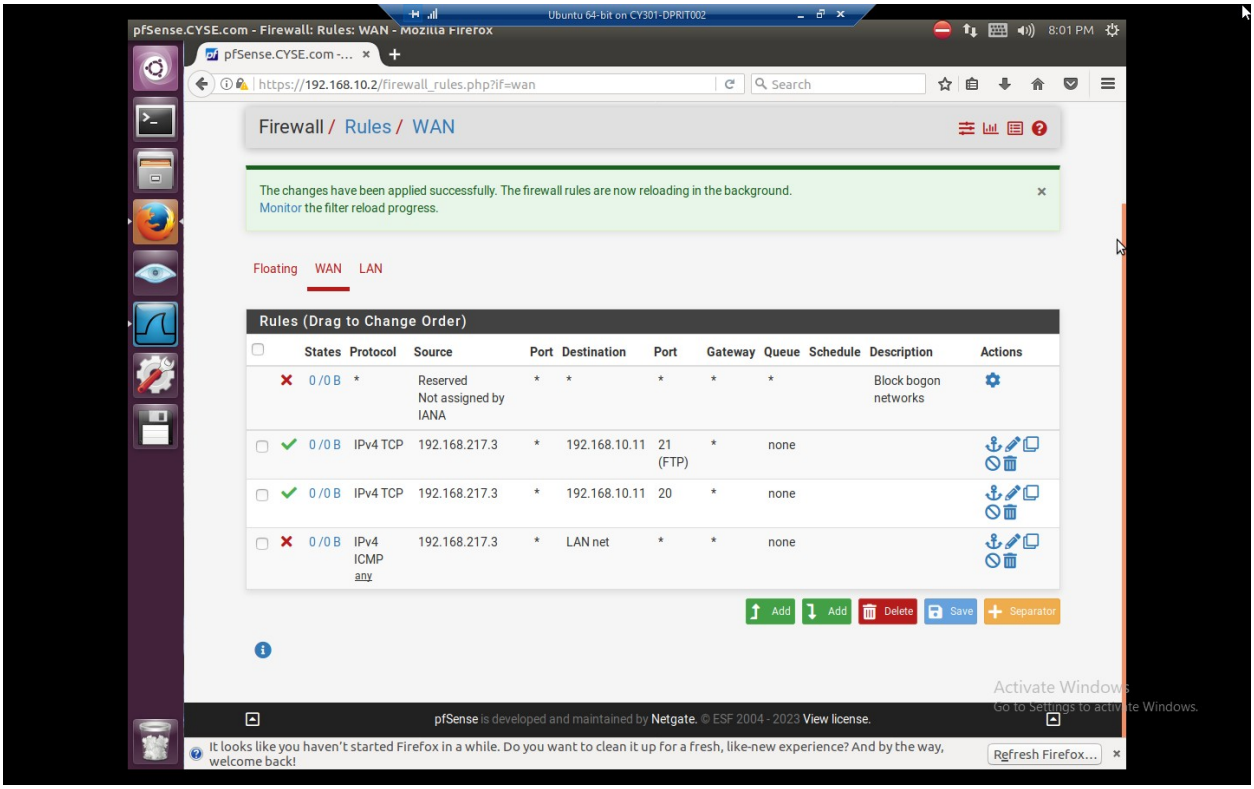
Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if applicable)
2	WAN	Block	192.168.217.3	LAN net	ICMP



Explanation: *Same as before, pfsense web interface showing that we are now just blocking all ICMP traffic to the LAN net entirely from 192.168.217.3.*

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 FTP protocol towards Windows Server 2008.

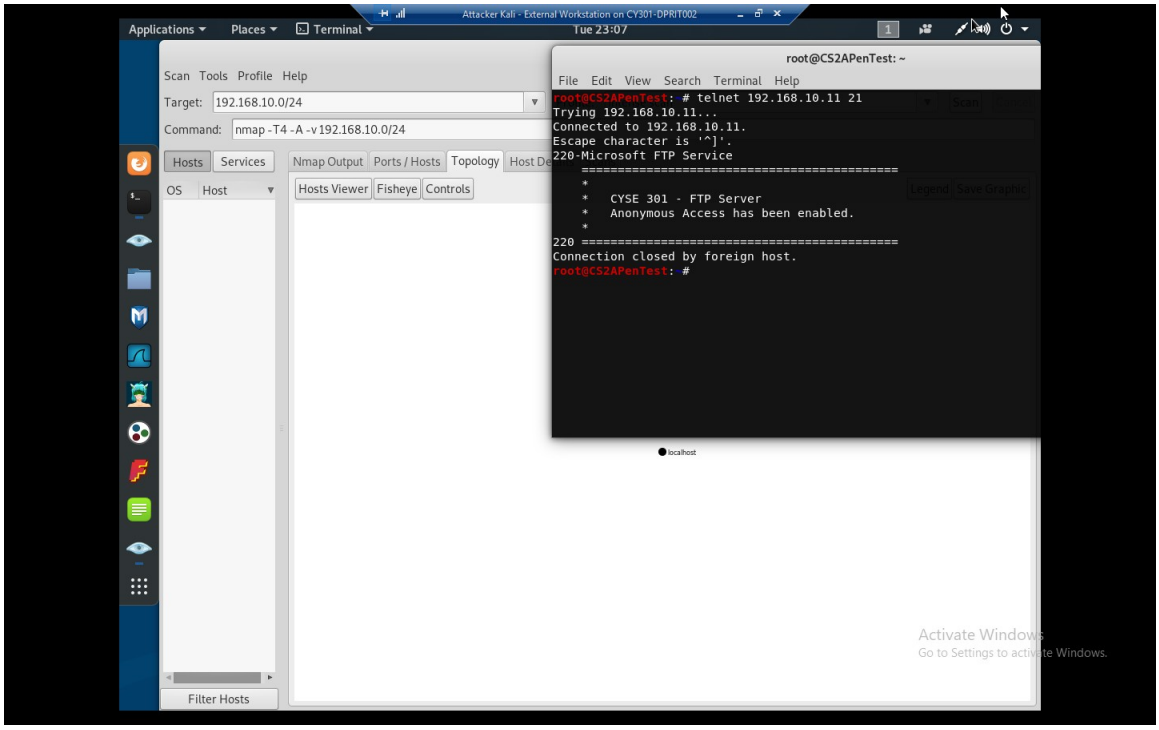
Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if applicable)
1	WAN	Pass	192.168.217.3	192.168.10.11	FTP (TCP /21)
2	WAN	Pass	192.168.217.3	192.168.10.11	TCP /20
3	WAN	Block	192.168.217.3	LAN net	ICMP



Explanation: *Shown is 3 WAN rules that pass traffic from 192.168.217.3 to 192.168.10.11 on ports 20 and 21, used for FTP, but block all ICMP traffic to the greater LAN net.*

4. Keep the firewall policies you created in Task B.3 and repeat Task A.1. What's the difference?

When a scan is attempted from External Kali, all traffic from External Kali to the LAN side, except for the FTP protocol towards Windows Server 2008, will be blocked. The scan will not be successful, as the firewall is now blocking all traffic except for FTP traffic to Windows Server 2008. This can help to protect the network and systems from potential attacks.



Explanation: *Attempting to use the telnet command to connect to port 21 on 192.168.10.11 with external kali succeeds, but the Nmap scan fails to discover anything.*