

Gerkeil Owens

**CYSE 301: Cybersecurity Technique and
Operations**

Assignment 3: Sword vs. Shield

In this assignment, you will act as an attacker to identify the vulnerabilities in the LAN network and a defender to apply proper countermeasures. You need to provide a screenshot for each task below.

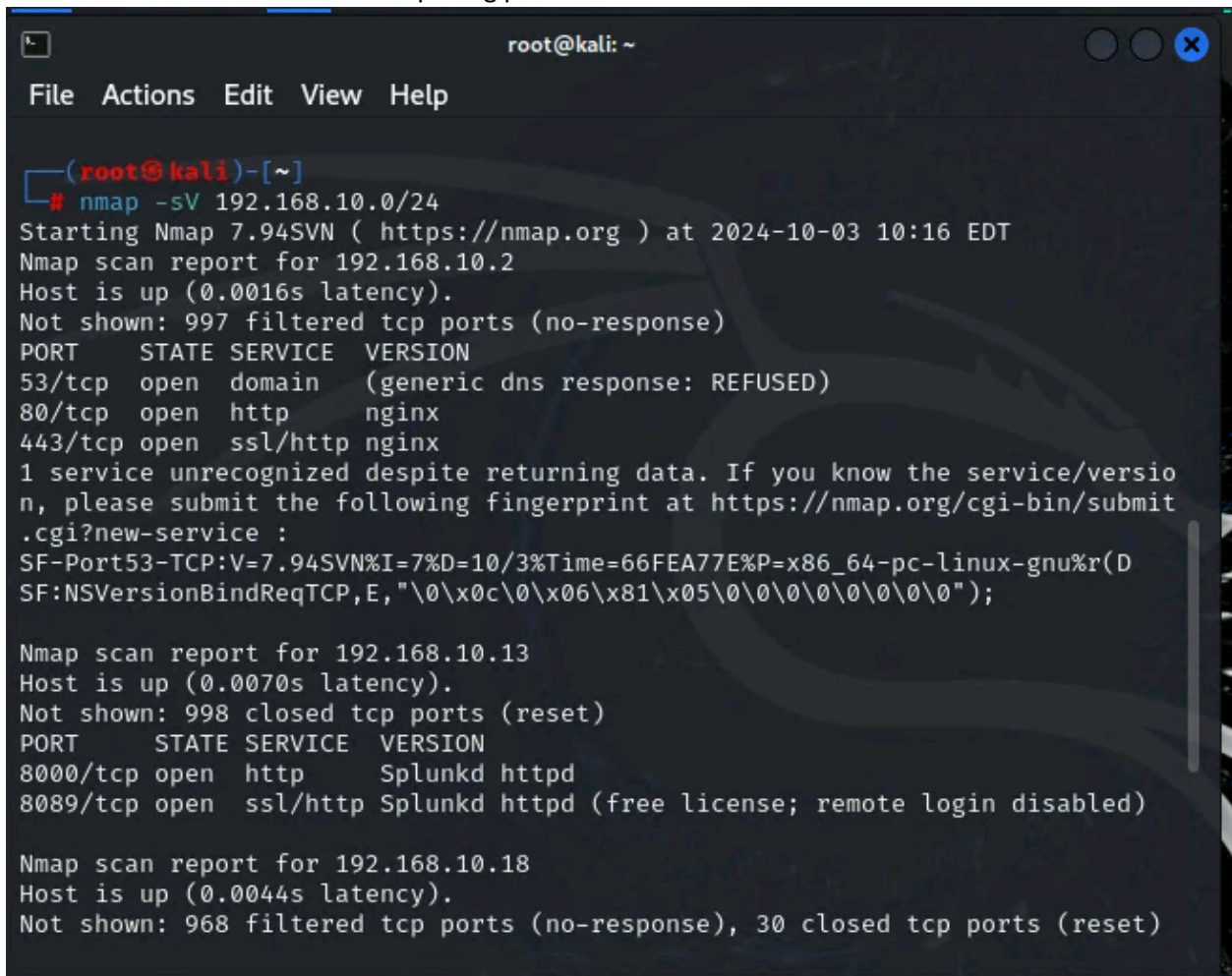
Task A: Sword - Network Scanning (20+ 20 = 40 points)

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 2022

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.



```
root@kali: ~
File Actions Edit View Help

(root@kali)-[~]
└─# nmap -sV 192.168.10.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-03 10:16 EDT
Nmap scan report for 192.168.10.2
Host is up (0.0016s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE  VERSION
53/tcp    open  domain  (generic dns response: REFUSED)
80/tcp    open  http     nginx
443/tcp   open  ssl/http nginx
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.94SVN%I=7%D=10/3%Time=66FEA77E%P=x86_64-pc-linux-gnu%r(D
SF:NSVersionBindReqTCP,E,"\0\0c\0\0\06\0x81\005\0\0\0\0\0\0\0");

Nmap scan report for 192.168.10.13
Host is up (0.0070s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE  VERSION
8000/tcp  open  http     Splunkd httpd
8089/tcp  open  ssl/http Splunkd httpd (free license; remote login disabled)

Nmap scan report for 192.168.10.18
Host is up (0.0044s latency).
Not shown: 968 filtered tcp ports (no-response), 30 closed tcp ports (reset)
```

- Entering the “nmap -Sv 192.168.10.0/24” command to profile the basic information about the subnet.

```
root@kali: ~
File Actions Edit View Help
8000/tcp open  http      Splunkd httpd
8089/tcp open  ssl/http Splunkd httpd (free license; remote login disabled)

Nmap scan report for 192.168.10.18
Host is up (0.0044s latency).
Not shown: 968 filtered tcp ports (no-response), 30 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.5
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.7 (Ubuntu Linux; protocol 2.0)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

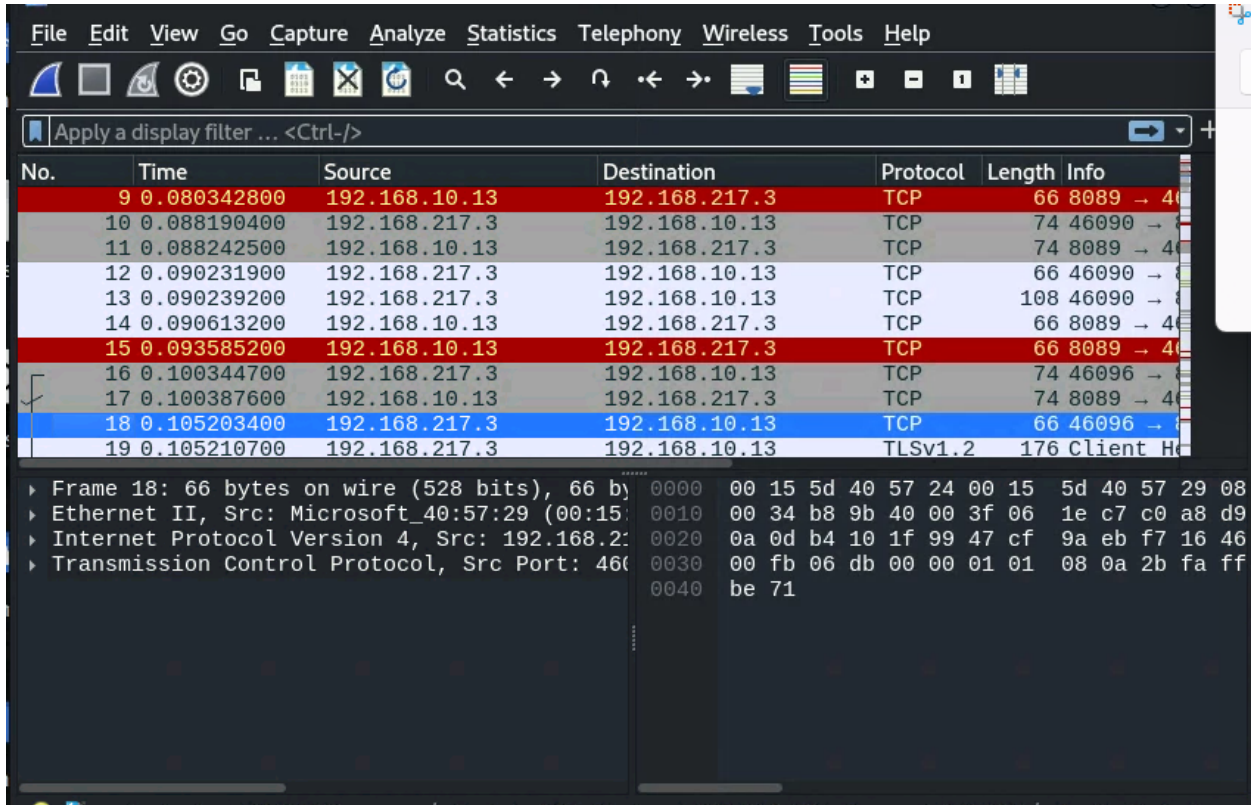
Nmap scan report for 192.168.10.19
Host is up (0.0089s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE          VERSION
135/tcp    open  msrpc           Microsoft Windows RPC
139/tcp    open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 56.56 seconds

(root@kali)-[~]
#
```

- Entering the “nmap -Sv 192.168.10.0/24” command to profile the basic information about the subnet continued.

- Run Wireshark in Internal Kali 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.**



- In analyzing the traffic captured during the Nmap scan using Wireshark, several patterns emerged that provided insight into the network's behavior. A significant number of requests were observed as the scanning tool attempted to identify active hosts within the subnet. This is normal behavior as requests are necessary for resolving IP addresses to MAC addresses. The majority of the traffic consisted of TCP scans, which aims to identify open ports without establishing a full TCP connection. This stealth approach minimizes detection, making it a preferred method. Also, there were a few ICMP echo requests and replies, suggesting that ping sweeps were occurring, though this depends on the specific Nmap options chosen.

Overall, the captured traffic illustrated typical patterns associated with network scanning, characterized by a high volume of TCP packets and requests. This data emphasizes the importance of monitoring network traffic to detect potential activities, which can serve as a precursor to more malicious actions. Also, I noticed the color pattern of red and grey. This might be a security feature to highlight suspicious activity in a network's traffic so cybersecurity engineers working within the network can filter through traffic more easily.

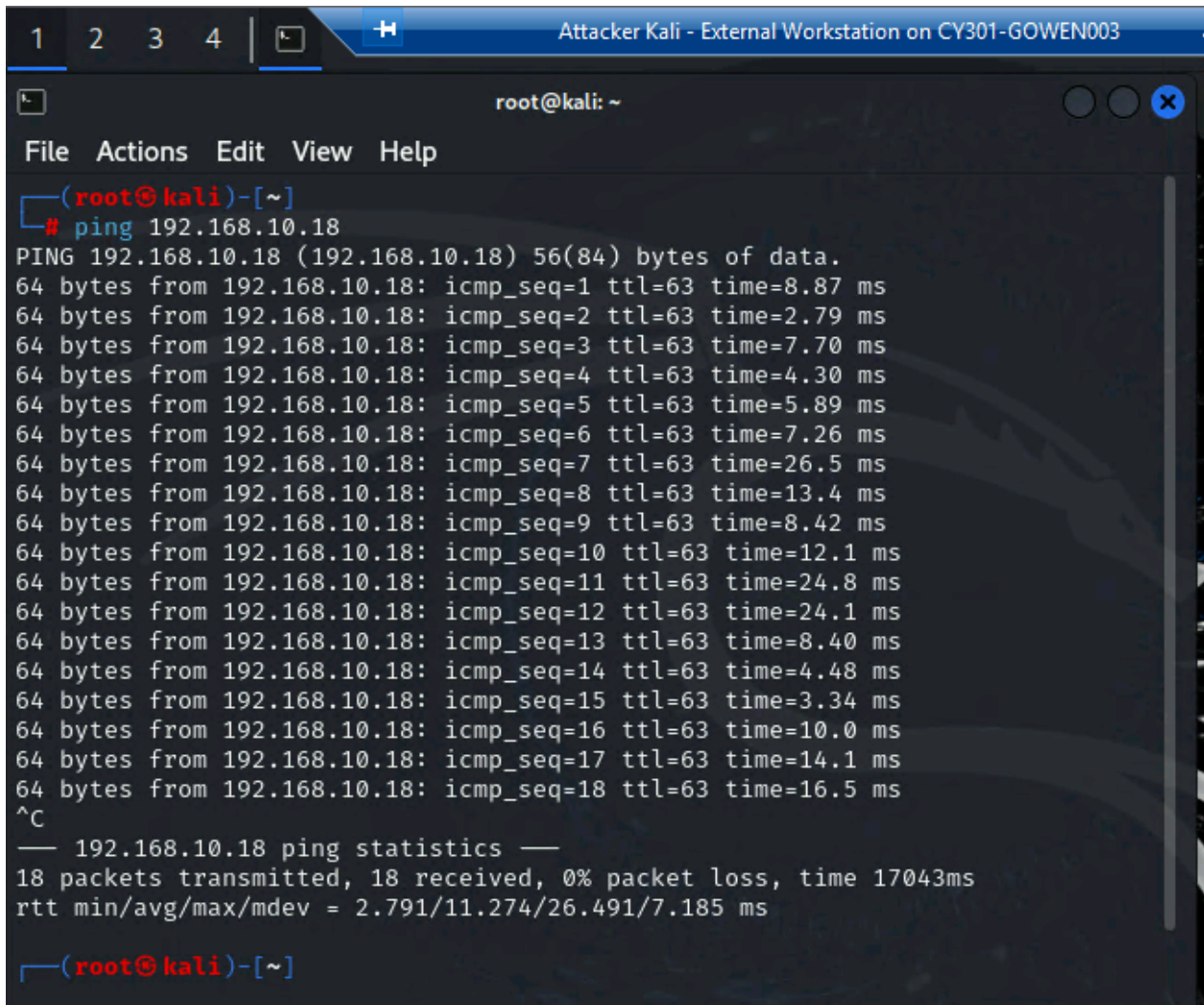
Task B: Shield – Protect your network with firewall (10 + 10+ 20 + 20 = 60 points)

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)
2	WAN	Block	192.168.217.3	192.168.10.18	ICMP

[Add the screenshot here]



```
Attacker Kali - External Workstation on CY301-GOWEN003
root@kali: ~
File Actions Edit View Help
(root@kali)-[~]
└─# ping 192.168.10.18
PING 192.168.10.18 (192.168.10.18) 56(84) bytes of data:
64 bytes from 192.168.10.18: icmp_seq=1 ttl=63 time=8.87 ms
64 bytes from 192.168.10.18: icmp_seq=2 ttl=63 time=2.79 ms
64 bytes from 192.168.10.18: icmp_seq=3 ttl=63 time=7.70 ms
64 bytes from 192.168.10.18: icmp_seq=4 ttl=63 time=4.30 ms
64 bytes from 192.168.10.18: icmp_seq=5 ttl=63 time=5.89 ms
64 bytes from 192.168.10.18: icmp_seq=6 ttl=63 time=7.26 ms
64 bytes from 192.168.10.18: icmp_seq=7 ttl=63 time=26.5 ms
64 bytes from 192.168.10.18: icmp_seq=8 ttl=63 time=13.4 ms
64 bytes from 192.168.10.18: icmp_seq=9 ttl=63 time=8.42 ms
64 bytes from 192.168.10.18: icmp_seq=10 ttl=63 time=12.1 ms
64 bytes from 192.168.10.18: icmp_seq=11 ttl=63 time=24.8 ms
64 bytes from 192.168.10.18: icmp_seq=12 ttl=63 time=24.1 ms
64 bytes from 192.168.10.18: icmp_seq=13 ttl=63 time=8.40 ms
64 bytes from 192.168.10.18: icmp_seq=14 ttl=63 time=4.48 ms
64 bytes from 192.168.10.18: icmp_seq=15 ttl=63 time=3.34 ms
64 bytes from 192.168.10.18: icmp_seq=16 ttl=63 time=10.0 ms
64 bytes from 192.168.10.18: icmp_seq=17 ttl=63 time=14.1 ms
64 bytes from 192.168.10.18: icmp_seq=18 ttl=63 time=16.5 ms
^C
— 192.168.10.18 ping statistics —
18 packets transmitted, 18 received, 0% packet loss, time 17043ms
rtt min/avg/max/mdev = 2.791/11.274/26.491/7.185 ms
(root@kali)-[~]
```

- Pinging Ubuntu before put the rules in place to block access

pfSense.CYSE.com - Firewall Rules / WAN

The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress.

Floating **WAN** LAN

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
<input type="checkbox"/>	0/0 B	IPv4 ICMP any	192.168.217.3	*	192.168.10.18	*	*	none		Block ICMP from Ext Kali to Ubuntu	
<input type="checkbox"/>	0/763 KiB	IPv4+6 *	WAN subnets	*	*	*	*	none			

Add Add Delete Toggle Copy Save Separator

- The rules changes being applied to block ICMP from external Kali to Ubuntu

```

Attacker Kali - External Workstation on CY301-GOWEN003
root@kali: ~
File Actions Edit View Help
64 bytes from 192.168.10.18: icmp_seq=2 ttl=63 time=2.79 ms
64 bytes from 192.168.10.18: icmp_seq=3 ttl=63 time=7.70 ms
64 bytes from 192.168.10.18: icmp_seq=4 ttl=63 time=4.30 ms
64 bytes from 192.168.10.18: icmp_seq=5 ttl=63 time=5.89 ms
64 bytes from 192.168.10.18: icmp_seq=6 ttl=63 time=7.26 ms
64 bytes from 192.168.10.18: icmp_seq=7 ttl=63 time=26.5 ms
64 bytes from 192.168.10.18: icmp_seq=8 ttl=63 time=13.4 ms
64 bytes from 192.168.10.18: icmp_seq=9 ttl=63 time=8.42 ms
64 bytes from 192.168.10.18: icmp_seq=10 ttl=63 time=12.1 ms
64 bytes from 192.168.10.18: icmp_seq=11 ttl=63 time=24.8 ms
64 bytes from 192.168.10.18: icmp_seq=12 ttl=63 time=24.1 ms
64 bytes from 192.168.10.18: icmp_seq=13 ttl=63 time=8.40 ms
64 bytes from 192.168.10.18: icmp_seq=14 ttl=63 time=4.48 ms
64 bytes from 192.168.10.18: icmp_seq=15 ttl=63 time=3.34 ms
64 bytes from 192.168.10.18: icmp_seq=16 ttl=63 time=10.0 ms
64 bytes from 192.168.10.18: icmp_seq=17 ttl=63 time=14.1 ms
64 bytes from 192.168.10.18: icmp_seq=18 ttl=63 time=16.5 ms
^C
— 192.168.10.18 ping statistics —
18 packets transmitted, 18 received, 0% packet loss, time 17043ms
rtt min/avg/max/mdev = 2.791/11.274/26.491/7.185 ms
(root@kali)-[~]
# ping 192.168.10.18
PING 192.168.10.18 (192.168.10.18) 56(84) bytes of data.

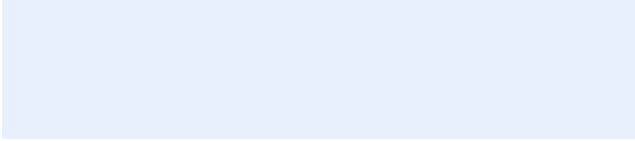
```

- Trying to ping Ubuntu after the rules changes were applied and after waiting a few minutes this is all that happened show not being able to access Ubuntu.

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)
	WAN	Block	192.168.217.3	192.168.10.0/24; all	

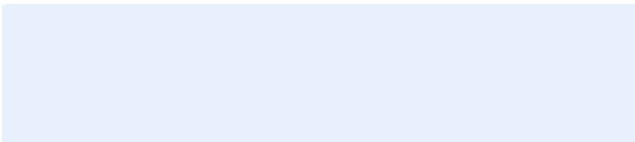
[Add the screenshot here]



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 2022.

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if applicable)

[Add the screenshot here]



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

Extra credit (15 points): Use NISSUS to enumerate the security vulnerabilities of Microsoft Windows Server 2022 VM in the CCIA network.