

CYSE 301: Cybersecurity Technique and Operations

Assignment 3: Sword vs. Shield

Owin Ifill

01230552

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.

```
Attacker Kali - External Workstation on CY301-OIFIL001 - Virtual Machine Connection
File Action Media View Help
root@kali: ~
File Actions Edit View Help
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-10-02 11:44 EDT
Nmap scan report for 192.168.10.18
Host is up (0.013s 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)
Device type: general purpose|storage-misc|firewall
Running (JUST GUESSING): Linux 2.6.X|4.X|3.X|5.X (92%), Synology DiskStation Manager 5.X (86%), WatchGuard Firewall 11.X (85%)
OS CPE: cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:4.4 cpe:/o:linux:linux_kernel:3.10 cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:5.1 cpe:/o:watchguard:fireware:11.8
Aggressive OS guesses: Linux 2.6.32 (92%), Linux 4.4 (92%), Linux 2.6.32 or 3.10 (91%), Linux 2.6.32 - 2.6.35 (90%), Linux 2.6.32 - 2.6.39 (90%), Linux 4.0 (89%), Linux 5.0 - 5.4 (88%), Linux 3.11 - 4.1 (88%), Linux 3.2 - 3.8 (88%), Linux 2.6.18 (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.07 seconds
(root@kali)-[~]
#
```

```
Attracker Kali - External Workstation on CV301-OIFIL001 (genmon)
root@kali ~
File Actions Edit View Help
2.0)
Device type: general purpose|storage-misc|firewall
Running (JUST GUESSING): Linux 2.6.X|4.X|3.X|5.X (92%), Synology DiskStation
Manager 5.X (86%), WatchGuard Firewall 11.X (85%)
OS CPE: cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:4.4 cpe:/o
:linux:linux_kernel:3.10 cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kerne
l cpe:/a:synology:diskstation_manager:5.1 cpe:/o:watchguard:fireware:11.8
Aggressive OS guesses: Linux 2.6.32 (92%), Linux 4.4 (92%), Linux 2.6.32 or 3
.10 (91%), Linux 2.6.32 - 2.6.35 (90%), Linux 2.6.32 - 2.6.39 (90%), Linux 4.
0 (89%), Linux 5.0 - 5.4 (88%), Linux 3.11 - 4.1 (88%), Linux 3.2 - 3.8 (88%)
, Linux 2.6.18 (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.07 seconds

root@kali ~# nmap -sS -sV -O 192.168.10.19
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-10-02 11:46 EDT
Nmap scan report for 192.168.10.19
Host is up (0.014s 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?
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2022|11|2016 (97%)
OS CPE: cpe:/o:microsoft:windows_server_2016
Aggressive OS guesses: Microsoft Windows Server 2022 (97%), Microsoft Windows 11 21H2 (91%), Microsoft Windows Server 2016 (91%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

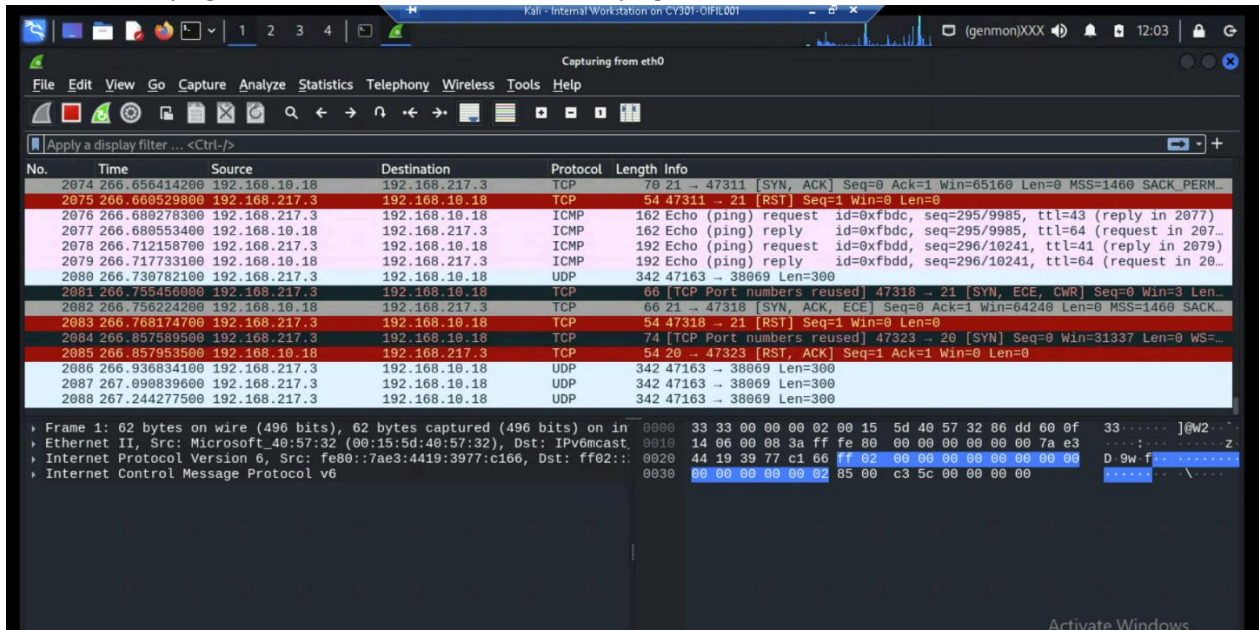
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.31 seconds

root@kali ~#
```

2. 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.**

When I scanned the network from the External Kali machine, I used Wireshark on the Internal Kali machine to watch the traffic. What I saw was a lot of small packets going to many different devices and ports very quickly. Most of these were TCP SYN packets, which are like the first “hello” a computer sends when trying to start a connection. The scanner sent these to many ports to check which ones would answer. I also noticed ICMP packets, which are used for things like “ping” to see if a device is online. When Nmap was checking for service versions, I saw packets with more data, like requests to web servers or SSH services. This is how Nmap learns what software and versions are running. The traffic looked different from normal network use because it was fast, repetitive, and touched many different devices and ports. This is a big clue that a scan is happening. As a defender, watching for this type of traffic can help you spot attackers early. If you see a pattern like this on your network, it likely means

someone is trying to discover weaknesses before trying to break in.

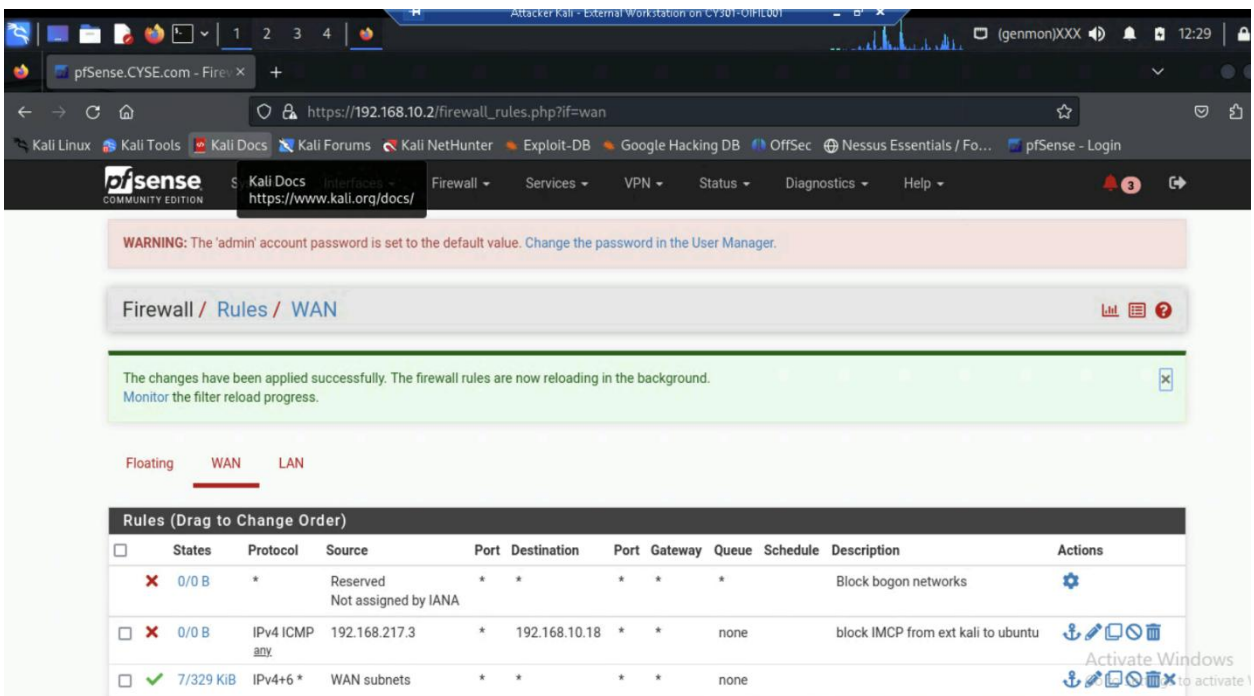


Task B: Shield – Protect your network with a firewall (10 + 10+ 20 + 20 = 60 points)

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.

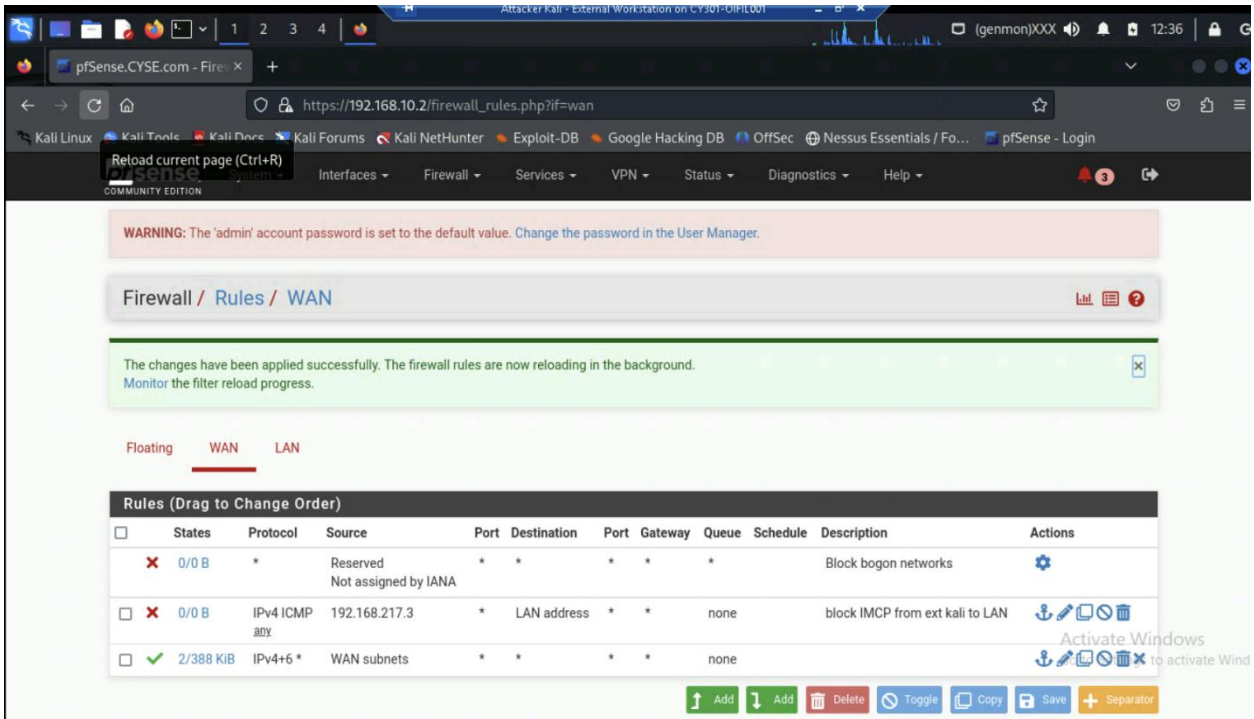
1. Configure the pfSense firewall rule to block the ICMP traffic from External Kali to Ubuntu VM.

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if applicable)
2	WAN	Block	192.168.217.3	192.168.10.18	ICMP



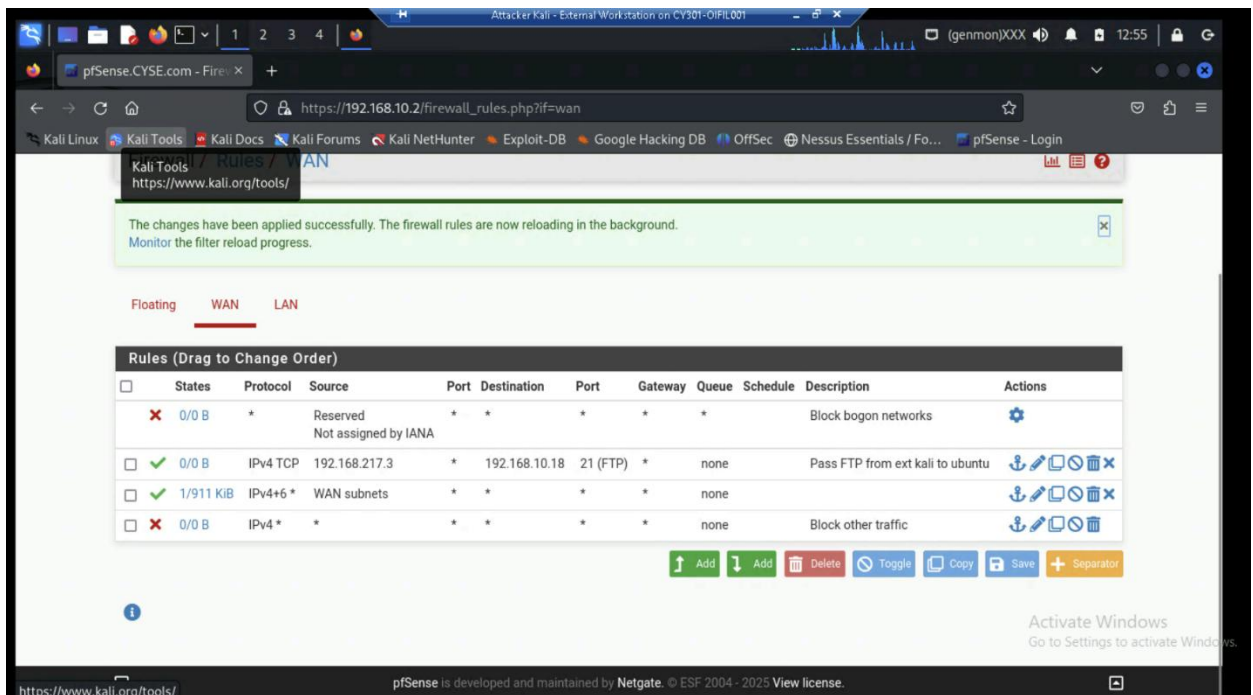
- Clear the previous firewall policies and configure the pfSense firewall to block all ICMP traffic from External Kali to the LAN side.

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



- 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 Ubuntu.

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if applicable)
2	WAN	Pass	192.168.217.3	192.168.10.18	21
Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if applicable)
4	WAN	Block	any	any	any



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

After making the firewall rules, the results of the Nmap scan changed a lot. Previously, multiple hosts and open ports were visible, and Nmap was able to retrieve detailed service and version information. Now, with the firewall in place, the scan results were mostly empty. Only the FTP service on the Ubuntu server responded, while all other traffic from the External Kali machine was blocked. ICMP echo requests no longer received replies, so Nmap was unable to map the subnet accurately.

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