Network Security Project

Prepared by:
Khulod Jaber

PROJECT DOCUMENTATION

DATE: 01/11/2023

Introduction

This project focuses on:

Vulnerability Scanning and Detection:

- Conducting thorough scans, including Wireshark analysis, to identify potential weaknesses within the network.

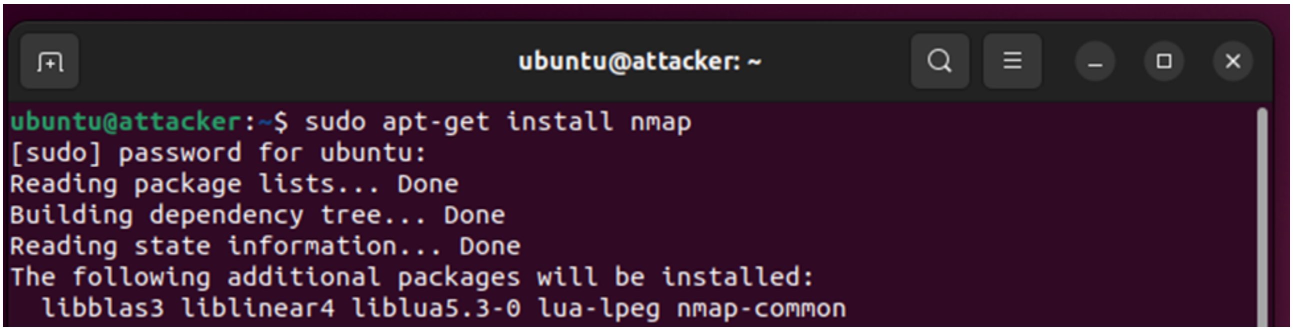
Proactive Defense Measures:

- Employing firewall rules as a preemptive step to fortify the network's defense mechanisms.

Security Monitoring through Logging:

- Implementing logging systems, including Wireshark for packet analysis, to monitor and prevent unauthorized activities, contributing to an overall robust security posture.

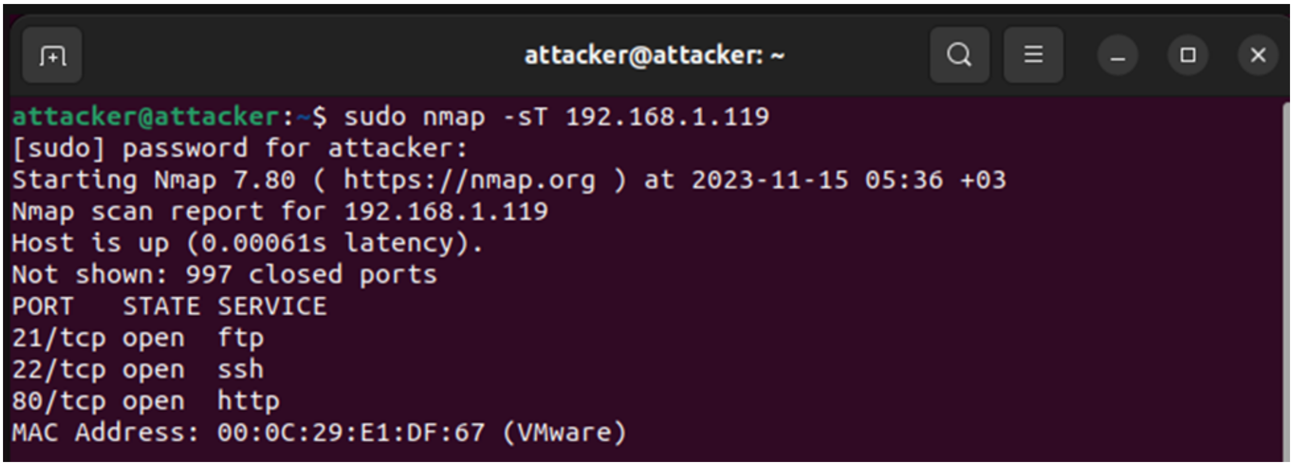
Vulnerability Scanning



```
ubuntu@attacker:~$ sudo apt-get install nmap
[sudo] password for ubuntu:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libblas3 liblinear4 liblua5.3-0 lua-lpeg nmap-common
```

Installed and verified the version of Nmap on the system.

Nmap is a network scanning tool used to discover hosts and services on a computer network, creating a map of the network's structure.

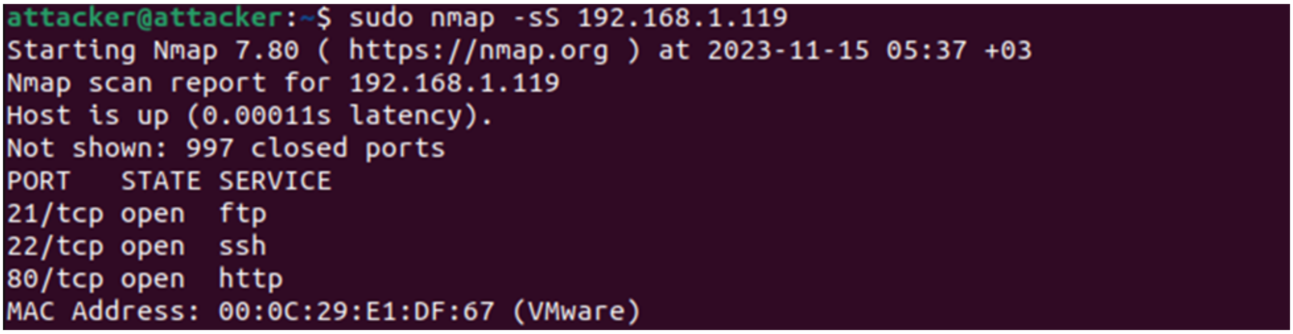


```
attacker@attacker:~$ sudo nmap -sT 192.168.1.119
[sudo] password for attacker:
Starting Nmap 7.80 ( https://nmap.org ) at 2023-11-15 05:36 +03
Nmap scan report for 192.168.1.119
Host is up (0.00061s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:0C:29:E1:DF:67 (VMware)
```

Executed an Nmap stealth TCP scan (-sT) from the attacker machine to the server.

Stealth Scan:

A stealth scan in Nmap is designed to evade detection by minimizing the footprint of the scanning activity. It is conducted with the intention of being less intrusive and avoiding triggering alerts on the target system. The primary goal of a stealth scan is to gather information about open ports and services on the target without alarming the intrusion detection systems or firewall.

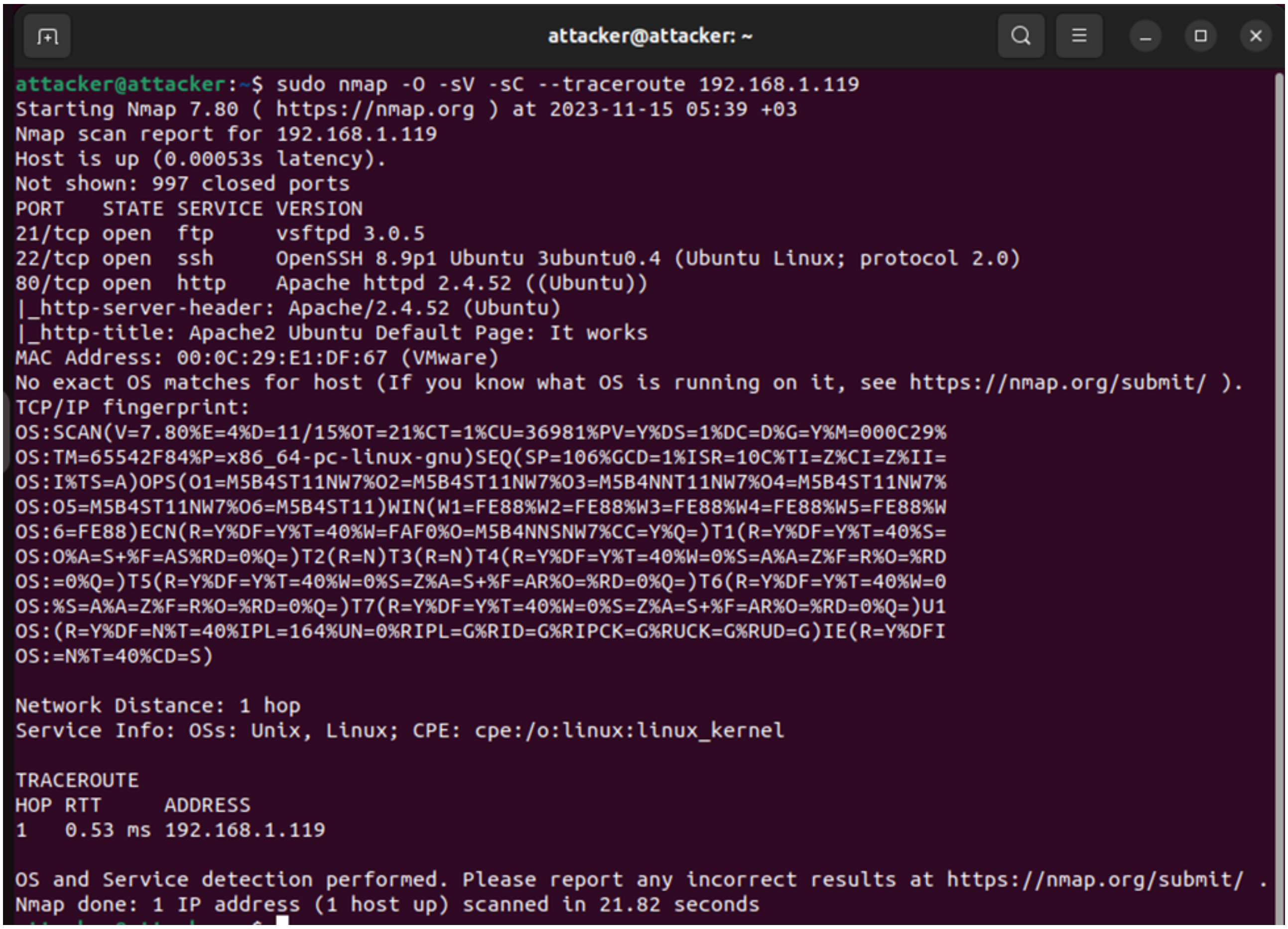


```
attacker@attacker:~$ sudo nmap -sS 192.168.1.119
Starting Nmap 7.80 ( https://nmap.org ) at 2023-11-15 05:37 +03
Nmap scan report for 192.168.1.119
Host is up (0.00011s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:0C:29:E1:DF:67 (VMware)
```

Conducted an Nmap SYN scan (-sS) from the attacker machine to the server.

Nmap SYN Scan:

A SYN scan (or half-open scan) is a type of port scanning method in Nmap that takes advantage of the TCP three-way handshake process. Instead of completing the entire handshake, where the client sends a SYN, the server responds with a SYN-ACK, and the client acknowledges with an ACK, the SYN scan stops after receiving the SYN-ACK. By not completing the handshake, the scanner avoids establishing a full connection, making it faster and less detectable.



```
attacker@attacker:~$ sudo nmap -O -sV -sC --traceroute 192.168.1.119
Starting Nmap 7.80 ( https://nmap.org ) at 2023-11-15 05:39 +03
Nmap scan report for 192.168.1.119
Host is up (0.00053s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.5
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 00:0C:29:E1:DF:67 (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=11/15%OT=21%CT=1%CU=36981%PV=Y%DS=1%DC=D%G=Y%M=000C29%
OS:TM=65542F84%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=10C%TI=Z%CI=Z%II=
OS:I%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%
OS:O5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W
OS:6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=
OS:O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD
OS:=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0
OS:%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1
OS:(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI
OS:=N%T=40%CD=S)

Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.53 ms 192.168.1.119

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 21.82 seconds
```

Executed a comprehensive Nmap scan (sudo nmap -O -sV -sC --traceroute 192.168.1.119) on the server, incorporating OS detection, version detection, script scanning, and traceroute functionality.

The findings from the scanning process are:

-ST Scan:

- Identified open ports 21 (ftp), 22 (ssh), 80 (http).

-sS Scan:

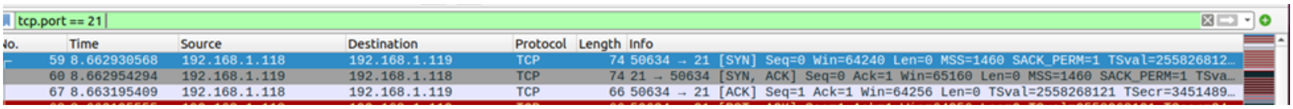
- Confirmed open ports and services on 21 (ftp), 22 (ssh), 80 (http).

-O -SV -SC --traceroute Scan:

- Detailed information on open ports, services, and OS.
- Detected vsftpd 3.0.5, OpenSSH 8.9p1, Apache httpd 2.4.52.
- Executed a traceroute and found Unix/Linux OS.

Analyzing Packets Using Wireshark

FTP Connection Establishment



tcp.port == 21

No.	Time	Source	Destination	Protocol	Length	Info
59	8.662930568	192.168.1.118	192.168.1.119	TCP	74	50634 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=255826812…
60	8.662954294	192.168.1.119	192.168.1.118	TCP	74	21 → 50634 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSva…
67	8.663195409	192.168.1.118	192.168.1.119	TCP	66	50634 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2558268121 TSecr=3451489…

Initiation (Packet 1):

- Attacker (192.168.1.118) initiates a TCP SYN connection to Victim (192.168.1.119) on port 21 (FTP).

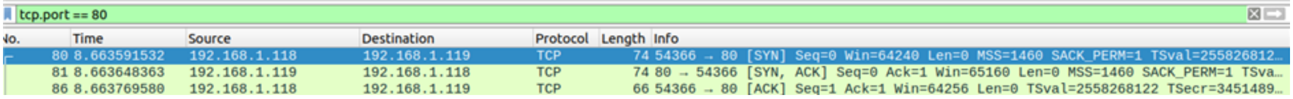
Response (Packet 2):

- Victim (192.168.1.119) responds with a SYN-ACK packet, indicating readiness.

Acknowledgment (Packet 3):

- Attacker (192.168.1.118) acknowledges the response, confirming the connection.

Connection Attempt to Port 80 (HTTP)



tcp.port == 80

No.	Time	Source	Destination	Protocol	Length	Info
80	8.663591532	192.168.1.118	192.168.1.119	TCP	74	54366 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=255826812…
81	8.663648363	192.168.1.119	192.168.1.118	TCP	74	80 → 54366 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSva…
86	8.663769580	192.168.1.118	192.168.1.119	TCP	66	54366 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2558268122 TSecr=3451489…

Initiation (Packet 1):

- Attacker (192.168.1.118) initiates a connection to the victim (192.168.1.119) on port 80 (HTTP) using a TCP SYN packet.

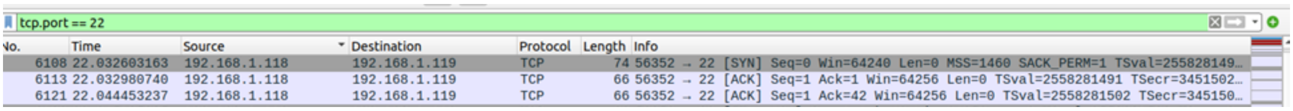
Response (Packet 2):

- Victim responds with a SYN-ACK packet, indicating readiness to establish a connection.

Acknowledgment (Packet 3):

- Attacker acknowledges the response, confirming the successful connection establishment.

SSH Connection Establishment



tcp.port == 22

No.	Time	Source	Destination	Protocol	Length	Info
6108	22.032603163	192.168.1.118	192.168.1.119	TCP	74	56352 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=255828149…
6113	22.032980740	192.168.1.118	192.168.1.119	TCP	66	56352 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2558281491 TSecr=3451502…
6121	22.044453237	192.168.1.118	192.168.1.119	TCP	66	56352 → 22 [ACK] Seq=1 Ack=42 Win=64256 Len=0 TSval=2558281502 TSecr=345150…

Initiation (SYN Packet - Packet 1):

- Attacker initiates a TCP connection to Victim on port 22 (SSH) with a SYN flag, signaling an attempt to establish a connection.

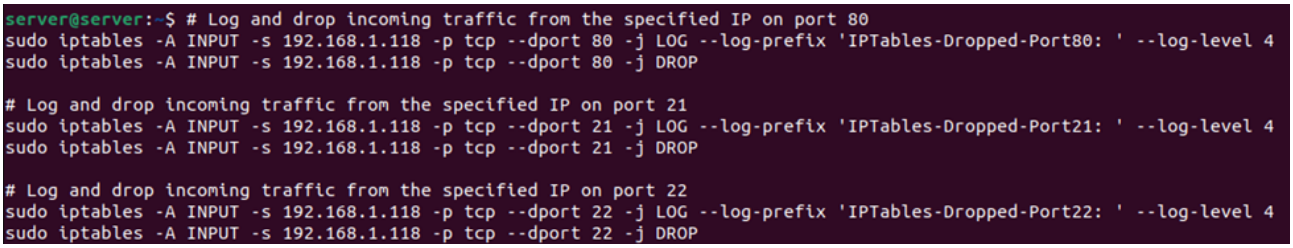
Response (ACK Packet - Packet 2):

- Victim responds with an acknowledgment (ACK), confirming receipt of the SYN packet.
- The TCP connection is in the process of being established.

Confirmation (SYN-ACK Packet - Packet 3):

- Attacker acknowledges the response with a SYN-ACK packet, finalizing the connection establishment.

Firewall Configurations and Logging

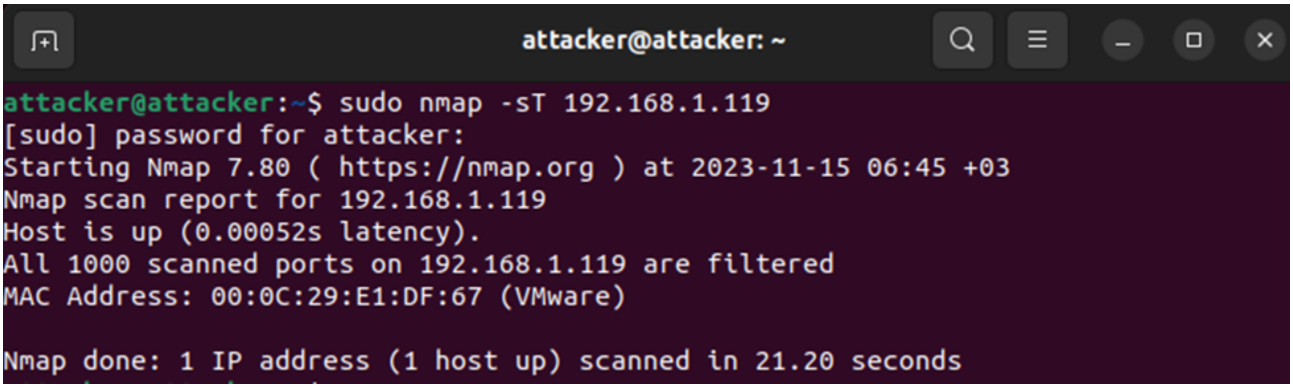


```
server@server:~$ # Log and drop incoming traffic from the specified IP on port 80
sudo iptables -A INPUT -s 192.168.1.118 -p tcp --dport 80 -j LOG --log-prefix 'IPTables-Dropped-Port80: ' --log-level 4
sudo iptables -A INPUT -s 192.168.1.118 -p tcp --dport 80 -j DROP

# Log and drop incoming traffic from the specified IP on port 21
sudo iptables -A INPUT -s 192.168.1.118 -p tcp --dport 21 -j LOG --log-prefix 'IPTables-Dropped-Port21: ' --log-level 4
sudo iptables -A INPUT -s 192.168.1.118 -p tcp --dport 21 -j DROP

# Log and drop incoming traffic from the specified IP on port 22
sudo iptables -A INPUT -s 192.168.1.118 -p tcp --dport 22 -j LOG --log-prefix 'IPTables-Dropped-Port22: ' --log-level 4
sudo iptables -A INPUT -s 192.168.1.118 -p tcp --dport 22 -j DROP
```

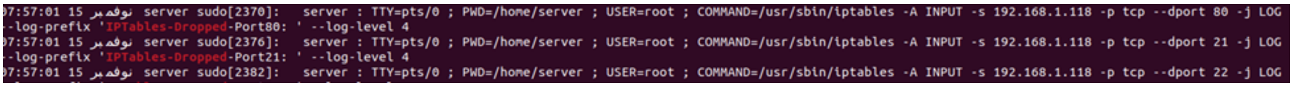
adding firewall rules and logging any attempt from the attacker machine to access port 80, 21, and 22



```
attacker@attacker:~$ sudo nmap -sT 192.168.1.119
[sudo] password for attacker:
Starting Nmap 7.80 ( https://nmap.org ) at 2023-11-15 06:45 +03
Nmap scan report for 192.168.1.119
Host is up (0.00052s latency).
All 1000 scanned ports on 192.168.1.119 are filtered
MAC Address: 00:0C:29:E1:DF:67 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.20 seconds
```

performed another scan to test the firewall and it works because the ports are now closed



```
07:57:01 15 نوفمبر server sudo[2370]:   server : TTY=pts/0 ; PWD=/home/server ; USER=root ; COMMAND=/usr/sbin/iptables -A INPUT -s 192.168.1.118 -p tcp --dport 80 -j LOG
--log-prefix 'IPTables-Dropped-Port80: ' --log-level 4
07:57:01 15 نوفمبر server sudo[2376]:   server : TTY=pts/0 ; PWD=/home/server ; USER=root ; COMMAND=/usr/sbin/iptables -A INPUT -s 192.168.1.118 -p tcp --dport 21 -j LOG
--log-prefix 'IPTables-Dropped-Port21: ' --log-level 4
07:57:01 15 نوفمبر server sudo[2382]:   server : TTY=pts/0 ; PWD=/home/server ; USER=root ; COMMAND=/usr/sbin/iptables -A INPUT -s 192.168.1.118 -p tcp --dport 22 -j LOG
```

the logs of the scan attempt

Conclusion

In summary, I was able to assess network vulnerabilities, and stegnthen defenses with firewalls, and delved into packet data using Nmap and Wireshark. Exploring the TCP three-way handshake shed light on port states. The project focused on enhancing network security through hands-on scanning and analysis.