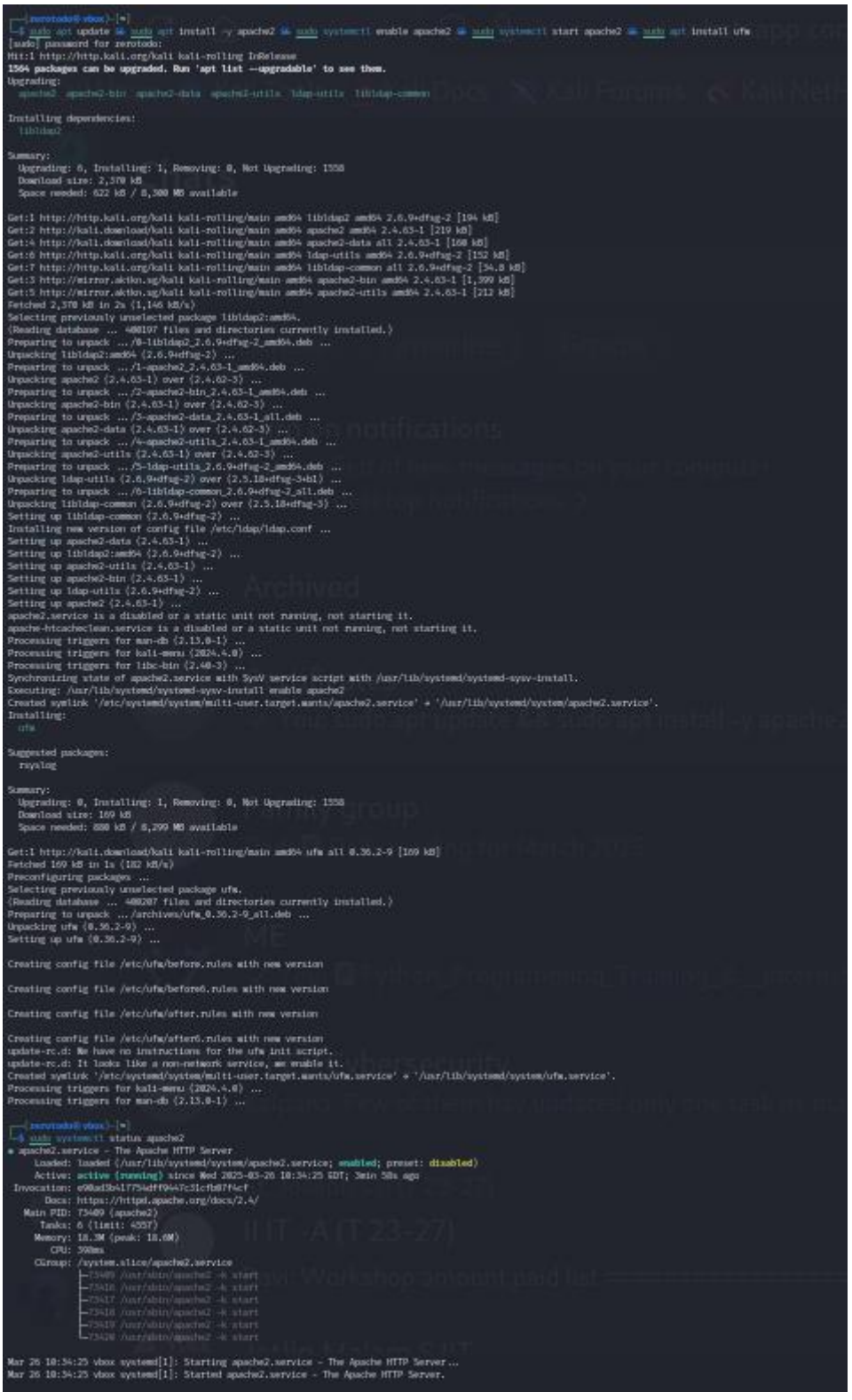
Task 3: Firewall & Network Security (PoC)

Setup: Install & Configure Web Server

Install Apache Web Server
sudo apt update && sudo apt install -y apache2
sudo systemctl enable apache2
sudo systemctl start apache2
sudo apt install ufw



Disable UFW (Uncomplicated Firewall)

sudo ufw disable

```
┌──(zerotodo㉿vbox)-[~]
└─$ sudo ufw disable
Firewall stopped and disabled on system startup
```

Verify Apache is Running

systemctl status apache2
Check Open Ports

sudo netstat -tulnp | grep LISTEN
Expected output:

```
┌──(zerotodo㉿vbox)-[~]
└─$ sudo netstat -tulnp | grep LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      40567/sshd: /usr/sb
tcp6       0      0 :::80                   :::*                    LISTEN      73409/apache2
tcp6       0      0 :::22                   :::*                    LISTEN      40567/sshd: /usr/sb
```

Exploit: Scanning for Open Ports & Services

1. Use Nmap to Find Open Ports
   nmap -sV -p- <Your-IP>

```
┌──(zerotodo㉿vbox)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fd00::c675:87e5:aac2:b315  prefixlen 64  scopeid 0x0<global>
        inet6 fd00::a00:27ff:fedd:f797  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::a00:27ff:fedd:f797  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:dd:f7:97  txqueuelen 1000  (Ethernet)
        RX packets 75144  bytes 98801948 (94.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 14564  bytes 2790230 (2.6 MiB)
        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 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(zerotodo㉿vbox)-[~]
└─$ nmap -p- 10.0.2.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-26 10:42 EDT
Nmap scan report for 10.0.2.15
Host is up (0.0000070s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 1.40 seconds
```

-sV: Service detection
-p-: Scan all 65,535 ports

2. Use Netcat to Interact with Open Ports
  nc -vz <YOUR-IP>

Expected output:
Connection to <YOUR_IP> 80 port [tcp/http] succeeded!

3. Impact Analysis

Without a firewall, attackers can discover all open services and attempt brute-force attacks or exploits.

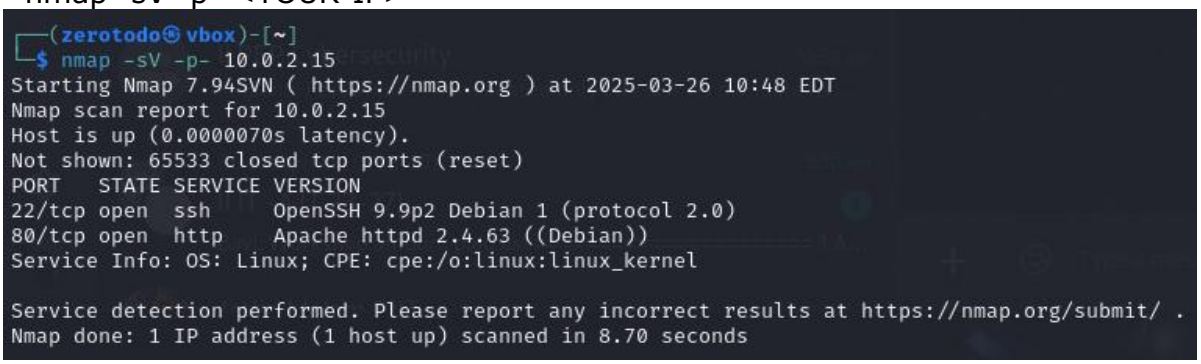
Mitigation: Firewall Hardening

Enable UFW & Allow Only Necessary Services
sudo ufw enable
sudo ufw allow 22/tcp
sudo ufw allow 80/tcp
sudo ufw deny 23/tcp # Block Telnet
sudo ufw deny 3306/tcp # Block MySQL

Verify UFW Rules
sudo ufw status verbose

Implement IPTables for Extra Protection
 sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
 sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
 sudo iptables -A INPUT -p tcp --dport 3306 -j DROP
 sudo iptables -A INPUT -p tcp --dport 23 -j DROP

Re-scan Using Nmap to Verify
nmap -sV -p- <YOUR-IP>



Conclusion

Before Hardening: Open services exposed to attacks.
After Hardening: Only SSH (22) & HTTP (80) remain accessible.
Firewall rules significantly reduce the attack surface.