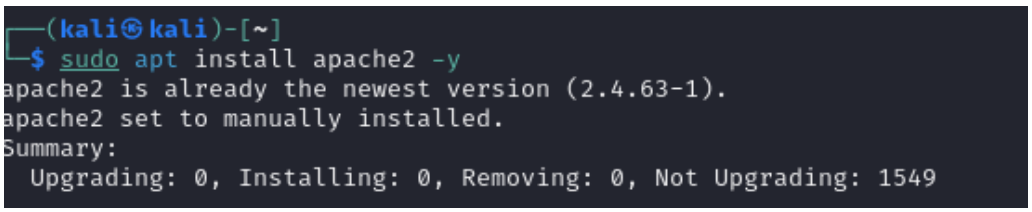
TASK 3

TASK 3:

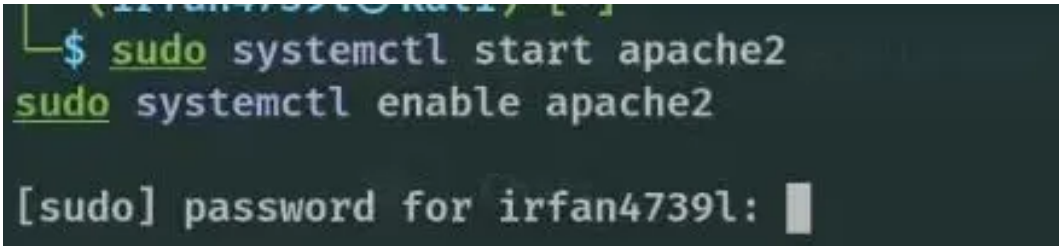
Firewall & Network Security

Setup: Install & configureapache2:

1 .First, I ensure my system is up-to-date by running sudo apt update && sudo apt upgrade -y Then, I install the **Apache2** web server using:



2. Next, I initiate the Apache service and configure it to start automatically on boot, ensuring uninterrupted web server functionality.



3. To check the status of Apache using the command **sudo systemctl status apache2**

```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: disabled)
     Active: active (running) since Sat 2025-03-22 23:28:58 EDT; 34min ago
 Invocation: d24056e3050f4fbda529ca80e722c6be
       Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 731 (apache2)
      Tasks: 6 (limit: 3425)
     Memory: 21.4M (peak: 21.8M)
        CPU: 204ms
     CGroup: /system.slice/apache2.service
             ├─731 /usr/sbin/apache2 -k start
             ├─745 /usr/sbin/apache2 -k start
             ├─746 /usr/sbin/apache2 -k start
             ├─747 /usr/sbin/apache2 -k start
             ├─748 /usr/sbin/apache2 -k start
             └─749 /usr/sbin/apache2 -k start
```

TASK 3 .1

Disabling UFW to Allow All Traffic:

1.To allow all traffic, we want to disable the ufw by using the command: **sudo ufw disable**

Exploitation: Use Nmap and Netcat to Scan for Open Ports &

Services:

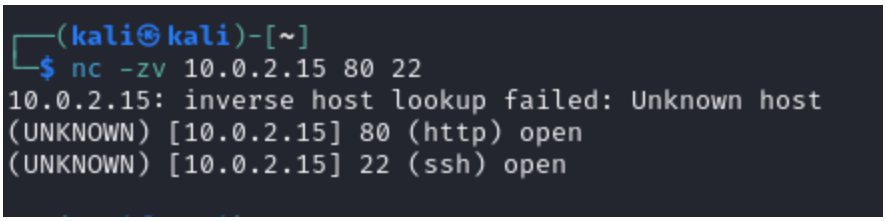
1.With the server running and traffic open, we use **Nmap** and **Netcat** to scan for exposed services and open ports attackers might target.

Before Hardening:

```
┌──(kali㉿kali)-[~]
└─$ nmap 10.0.2.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-23 00:07 EDT
Nmap scan report for 10.0.2.15
Host is up (0.0000010s latency).
Not shown: 998 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 0.28 seconds
```

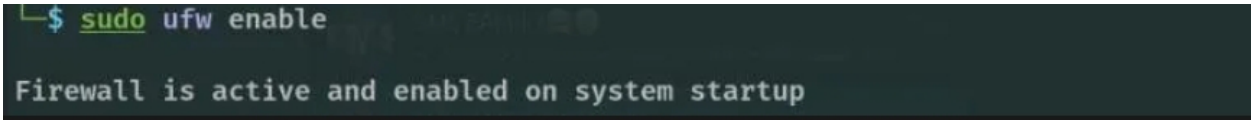
TASK 3 .2



Mitigation:

Restrict access using ufw (only allow SSH & HTTP):

1.Allow only SSH and HTTP traffic using the **sudo ufw allow 22 $ sudo ufw allow 80 and enable ufw**



Implement iptables Rules to Block Unnecessary Traffic:

1.To enhance security, we configure firewall rules to permit only **SSH (port 22)** and **HTTP (port 80)** traffic while blocking all other incoming connections. This ensures that only essential services remain accessible. After defining these rules, we save the firewall configuration to persist across system reboots, maintaining a secure network environment.

```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT

┌──(kali㉿kali)-[~]
└─$ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT

┌──(kali㉿kali)-[~]
└─$ sudo iptables -A INPUT i -j DROP
Bad argument `i'
Try `iptables -h' or 'iptables --help' for more information.

┌──(kali㉿kali)-[~]
└─$ sudo iptables -A INPUT -j DROP
```

After Hardening:

```
┌──(kali㉿kali)-[~]
└─$ nmap 10.0.2.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-23 00:07 EDT
Nmap scan report for 10.0.2.15
Host is up (0.0000010s latency).
Not shown: 998 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 0.28 seconds
```