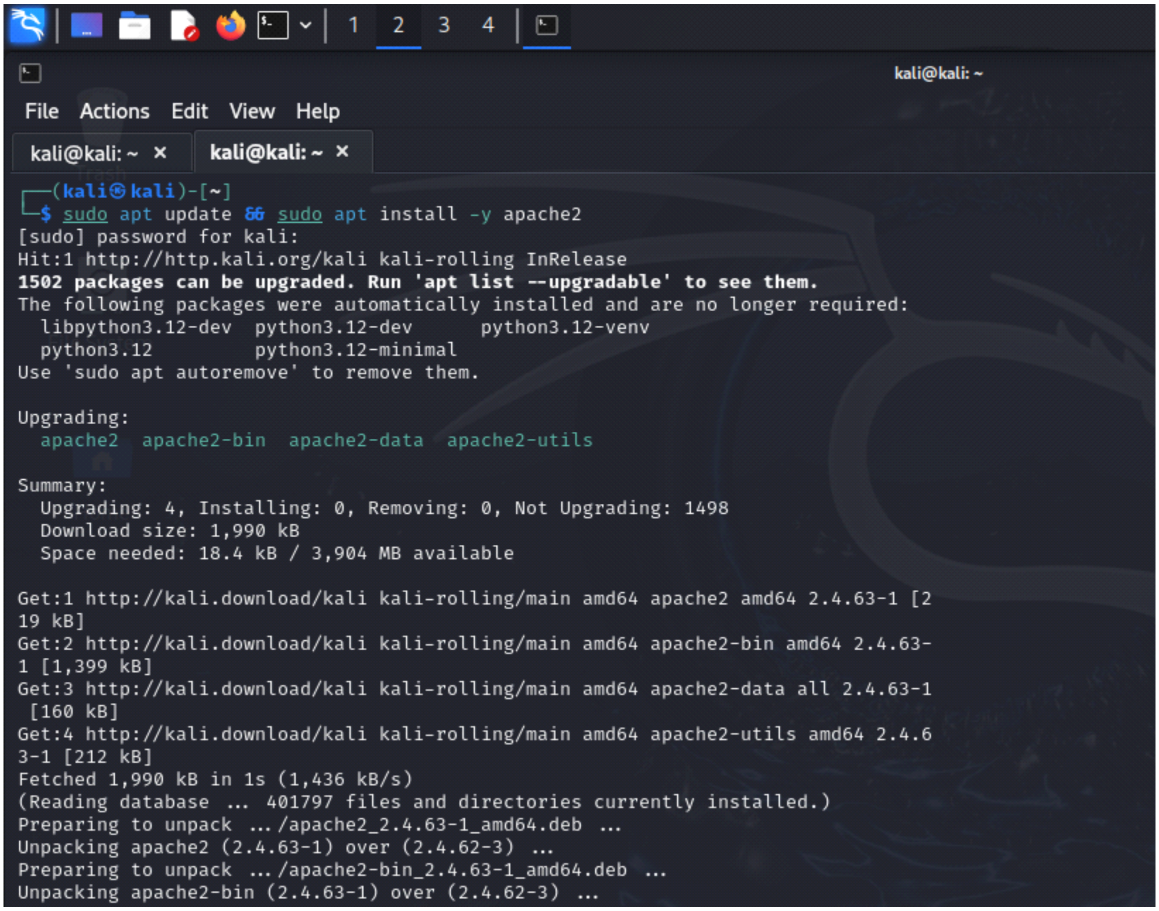
POC Task - 3

◆ Task 3: Firewall & Network Security

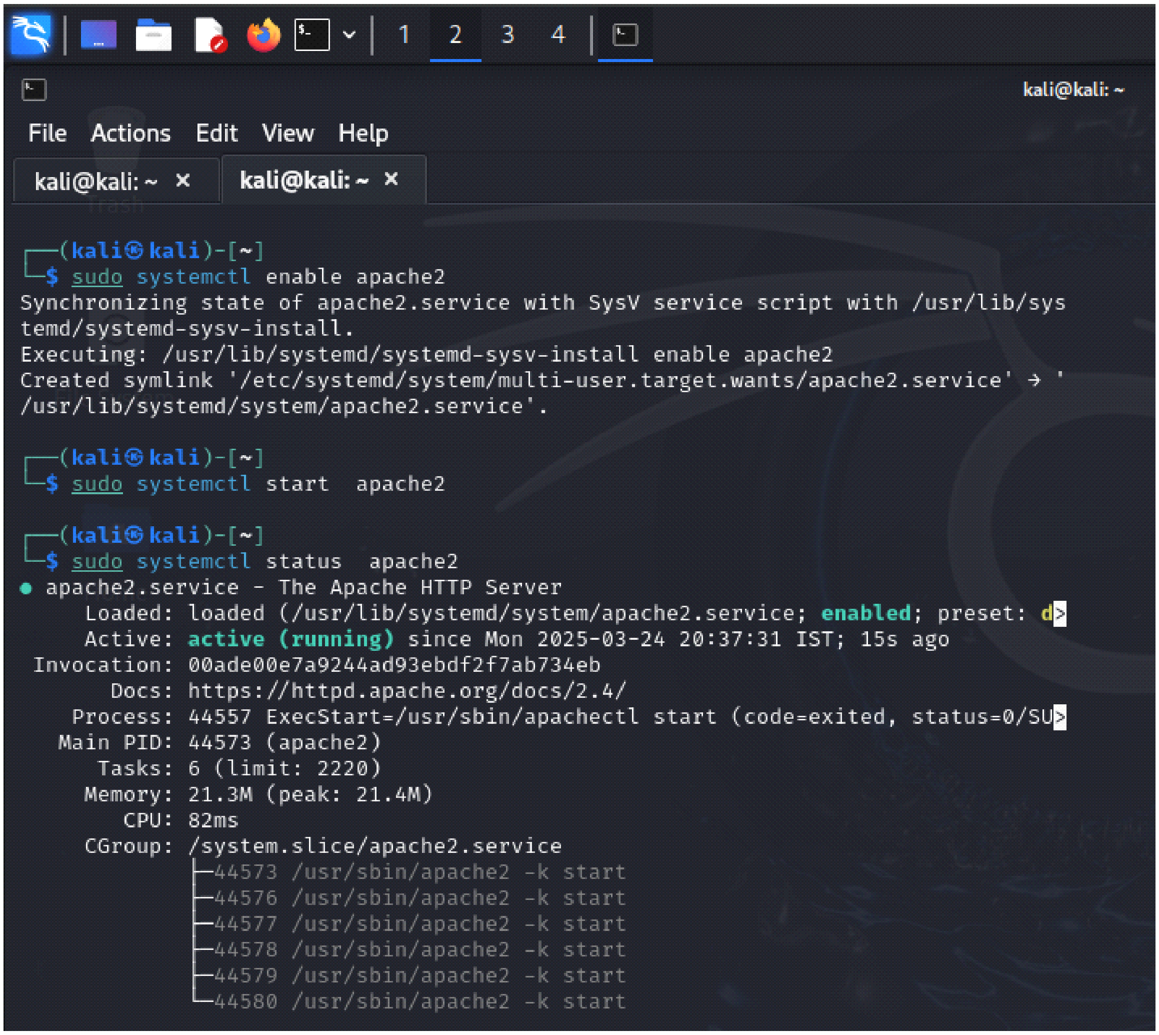
1. Setup: Install & Configure a Basic Web Server

1.1 Install Apache Web Server



```
┌──(kali㉿kali)-[~]
└─$ sudo apt update && sudo apt install -y apache2
[sudo] password for kali:
Hit:1 http://http.kali.org/kali kali-rolling InRelease
1502 packages can be upgraded. Run 'apt list --upgradable' to see them.
The following packages were automatically installed and are no longer required:
  libpython3.12-dev  python3.12-dev      python3.12-venv
  python3.12         python3.12-minimal
Use 'sudo apt autoremove' to remove them.

Upgrading:
  apache2  apache2-bin  apache2-data  apache2-utils

Summary:
  Upgrading: 4, Installing: 0, Removing: 0, Not Upgrading: 1498
  Download size: 1,990 kB
  Space needed: 18.4 kB / 3,904 MB available

Get:1 http://kali.download/kali kali-rolling/main amd64 apache2 amd64 2.4.63-1 [2
19 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 apache2-bin amd64 2.4.63-
1 [1,399 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 apache2-data all 2.4.63-1
 [160 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 apache2-utils amd64 2.4.6
3-1 [212 kB]
Fetched 1,990 kB in 1s (1,436 kB/s)
(Reading database ... 401797 files and directories currently installed.)
Preparing to unpack .../apache2_2.4.63-1_amd64.deb ...
Unpacking apache2 (2.4.63-1) over (2.4.62-3) ...
Preparing to unpack .../apache2-bin_2.4.63-1_amd64.deb ...
Unpacking apache2-bin (2.4.63-1) over (2.4.62-3) ...
```

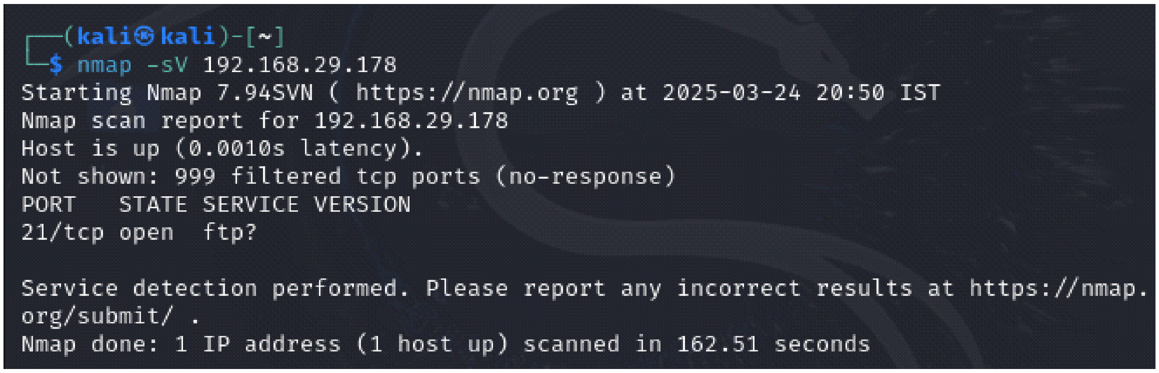
Start and enable the service:



```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /usr/lib/sys
temd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable apache2
Created symlink '/etc/systemd/system/multi-user.target.wants/apache2.service' → '
/usr/lib/systemd/system/apache2.service'.

┌──(kali㉿kali)-[~]
└─$ sudo systemctl start  apache2

┌──(kali㉿kali)-[~]
└─$ sudo systemctl status  apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: d>
     Active: active (running) since Mon 2025-03-24 20:37:31 IST; 15s ago
 Invocation: 00ade00e7a9244ad93ebdf2f7ab734eb
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 44557 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SU>
   Main PID: 44573 (apache2)
      Tasks: 6 (limit: 2220)
     Memory: 21.3M (peak: 21.4M)
        CPU: 82ms
     CGroup: /system.slice/apache2.service
             ├─44573 /usr/sbin/apache2 -k start
             ├─44576 /usr/sbin/apache2 -k start
             ├─44577 /usr/sbin/apache2 -k start
             ├─44578 /usr/sbin/apache2 -k start
             ├─44579 /usr/sbin/apache2 -k start
             └─44580 /usr/sbin/apache2 -k start
```

3)Disable firewall

Sudo ufw disable

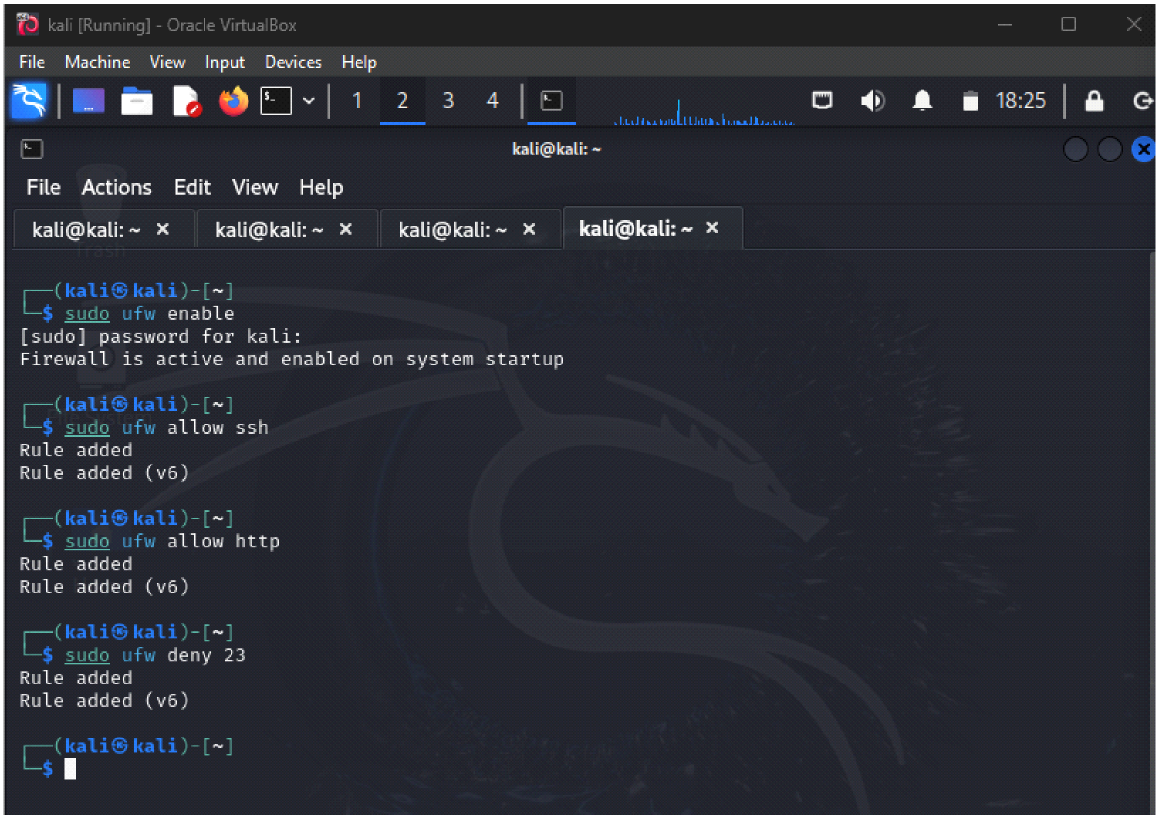


```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.29.178
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-24 20:50 IST
Nmap scan report for 192.168.29.178
Host is up (0.0010s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
21/tcp open  ftp?

Service detection performed. Please report any incorrect results at https://nmap.
org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 162.51 seconds
```

3) Mitigation

3.1) Enable firewall and restrict access:

sudo ufw enable
sudo ufw allow ssh
sudo ufw allow http
sudo ufw deny 23

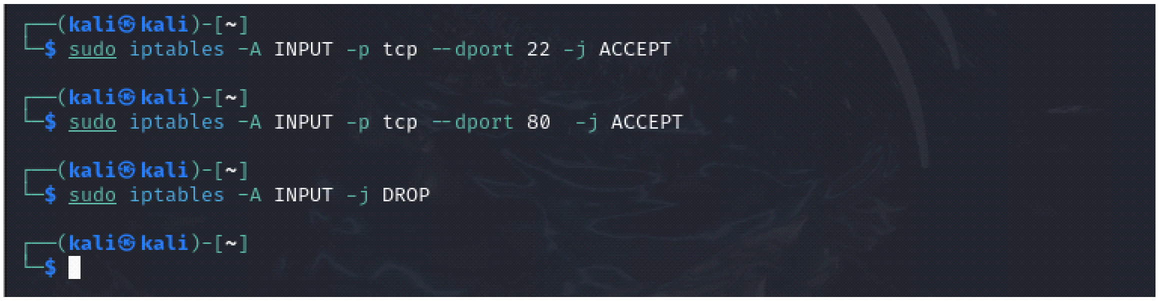

kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
18:25
kali@kali: ~
File Actions Edit View Help
kali@kali: ~ ✕
kali@kali: ~ ✕
kali@kali: ~ ✕
kali@kali: ~ ✕

```
┌──(kali㉿kali)-[~]
└─$ sudo ufw enable
[sudo] password for kali:
Firewall is active and enabled on system startup

┌──(kali㉿kali)-[~]
└─$ sudo ufw allow ssh
Rule added
Rule added (v6)

┌──(kali㉿kali)-[~]
└─$ sudo ufw allow http
Rule added
Rule added (v6)

┌──(kali㉿kali)-[~]
└─$ sudo ufw deny 23
Rule added
Rule added (v6)

┌──(kali㉿kali)-[~]
└─$ 
```

Implement iptables Rules to Block Unnecessary Traffic

To drop all incoming traffic except SSH (22) and HTTP (80):

```
  sudo iptables -P INPUT DROP
sudo iptables -P FORWARD DROP
sudo iptables -P OUTPUT ACCEPT
sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
sudo iptables -A INPUT -j DROP
```



```
┌──(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 -j DROP

┌──(kali㉿kali)-[~]
└─$ 
```