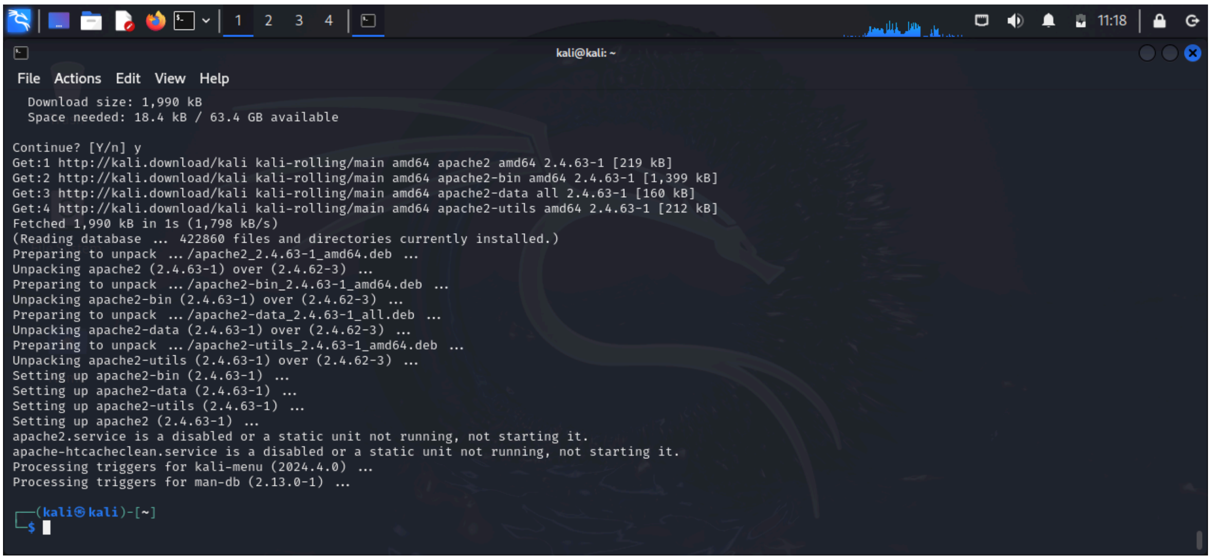
PoC Task 3: Firewall & Network Security

1) Setup

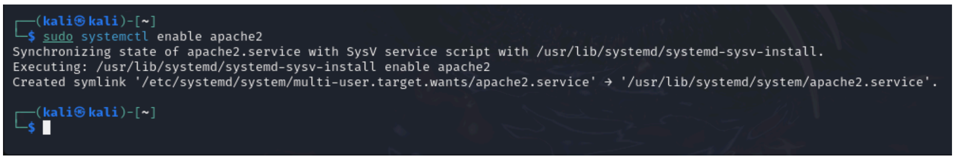
1.1) Install a web server:

sudo apt install apache2



```
  Download size: 1,990 kB
  Space needed: 18.4 kB / 63.4 GB available

Continue? [Y/n] y
Get:1 http://kali.download/kali kali-rolling/main amd64 apache2 amd64 2.4.63-1 [219 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 2.4.63-1 [212 kB]
Fetched 1,990 kB in 1s (1,798 kB/s)
(Reading database ... 422860 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) ...
Preparing to unpack .../apache2-data_2.4.63-1_all.deb ...
Unpacking apache2-data (2.4.63-1) over (2.4.62-3) ...
Preparing to unpack .../apache2-utils_2.4.63-1_amd64.deb ...
Unpacking apache2-utils (2.4.63-1) over (2.4.62-3) ...
Setting up apache2-bin (2.4.63-1) ...
Setting up apache2-data (2.4.63-1) ...
Setting up apache2-utils (2.4.63-1) ...
Setting up apache2 (2.4.63-1) ...
apache2.service is a disabled or a static unit not running, not starting it.
apache-htcacheclean.service is a disabled or a static unit not running, not starting it.
Processing triggers for kali-menu (2024.4.0) ...
Processing triggers for man-db (2.13.0-1) ...

┌──(kali㉿kali)-[~]
└─$ 
```

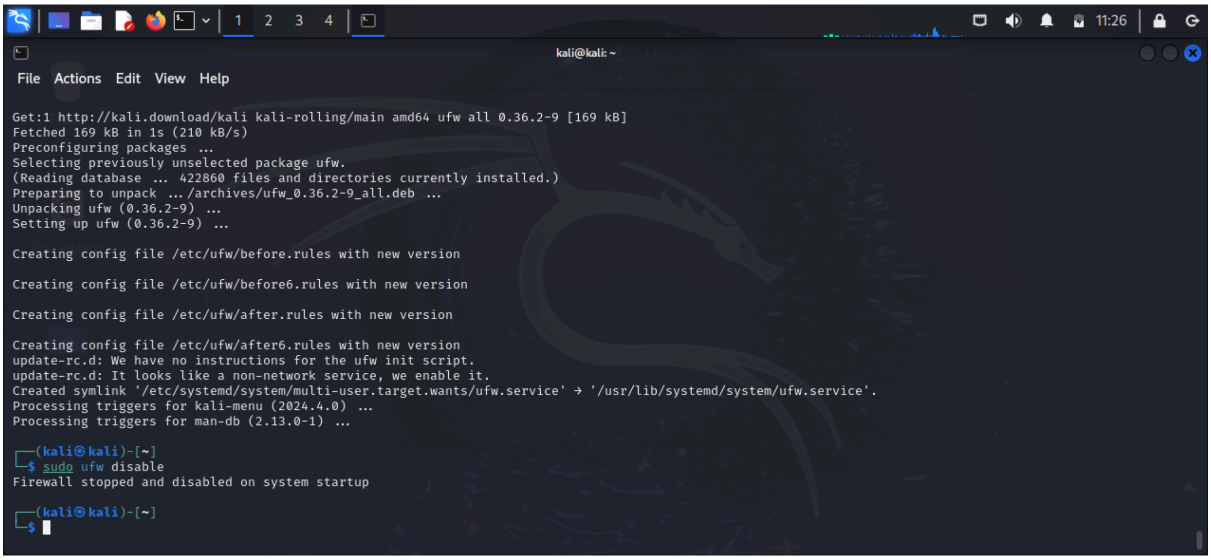
1.2) sudo systemctl enable apache2



```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /usr/lib/systemd/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)-[~]
└─$ 
```

1.3) Disable firewall:

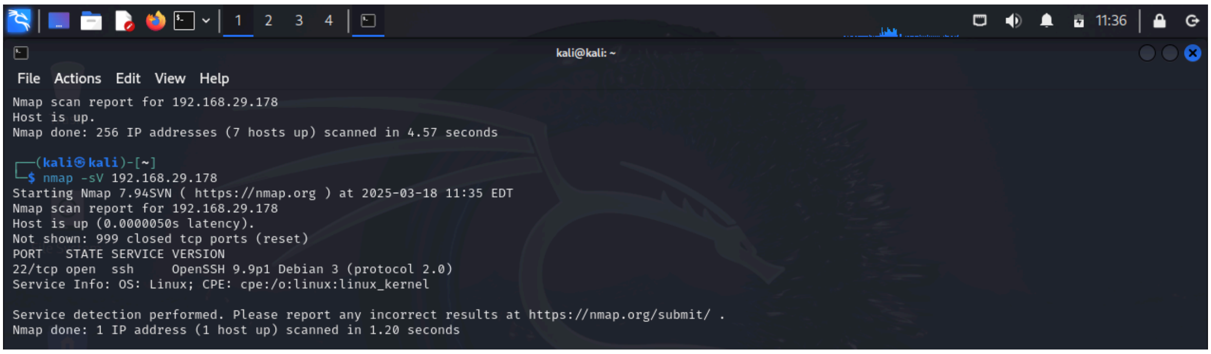
sudo ufw disable



```
Get:1 http://kali.download/kali kali-rolling/main amd64 ufw all 0.36.2-9 [169 kB]
Fetched 169 kB in 1s (210 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ufw.
(Reading database ... 422860 files and directories currently installed.)
Preparing to unpack .../archives/ufw_0.36.2-9_all.deb ...
Unpacking ufw (0.36.2-9) ...
Setting up ufw (0.36.2-9) ...

Creating config file /etc/ufw/before.rules with new version

Creating config file /etc/ufw/before6.rules with new version

Creating config file /etc/ufw/after.rules with new version

Creating config file /etc/ufw/after6.rules with new version
update-rc.d: We have no instructions for the ufw init script.
update-rc.d: It looks like a non-network service, we enable it.
Created symlink '/etc/systemd/system/multi-user.target.wants/ufw.service' → '/usr/lib/systemd/system/ufw.service'.
Processing triggers for kali-menu (2024.4.0) ...
Processing triggers for man-db (2.13.0-1) ...

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

┌──(kali㉿kali)-[~]
└─$ 
```

2) Exploit

2.1) Scan open ports:



```
Nmap scan report for 192.168.29.178
Host is up.
Nmap done: 256 IP addresses (7 hosts up) scanned in 4.57 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.29.178
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-18 11:35 EDT
Nmap scan report for 192.168.29.178
Host is up (0.0000050s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.9p1 Debian 3 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.20 seconds
```

3) Mitigation

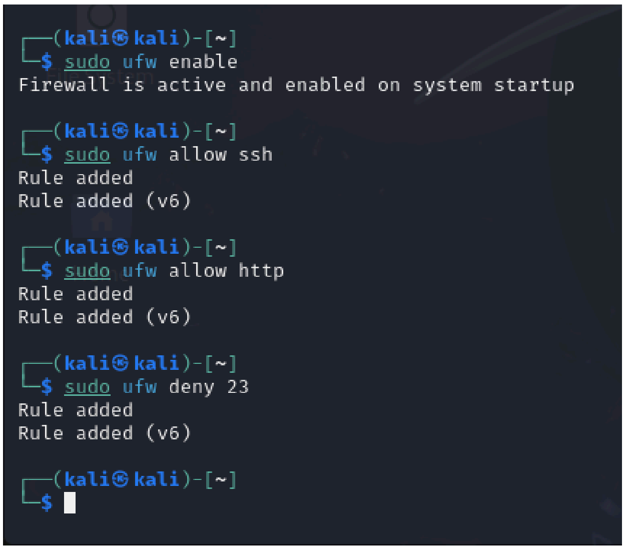
3.1) Enable firewall and restrict access:

sudo ufw enable

sudo ufw allow ssh

sudo ufw allow http

sudo ufw deny 23



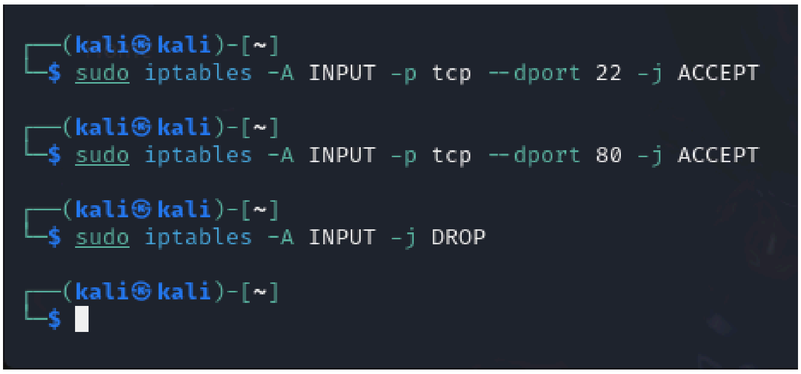
```
┌──(kali㉿kali)-[~]
└─$ sudo ufw enable
Firewall is active and enabled on system startup

┌──(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)-[~]
└─$ 
```

3.2) Implement iptables rules:

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)-[~]
└─$ 
```