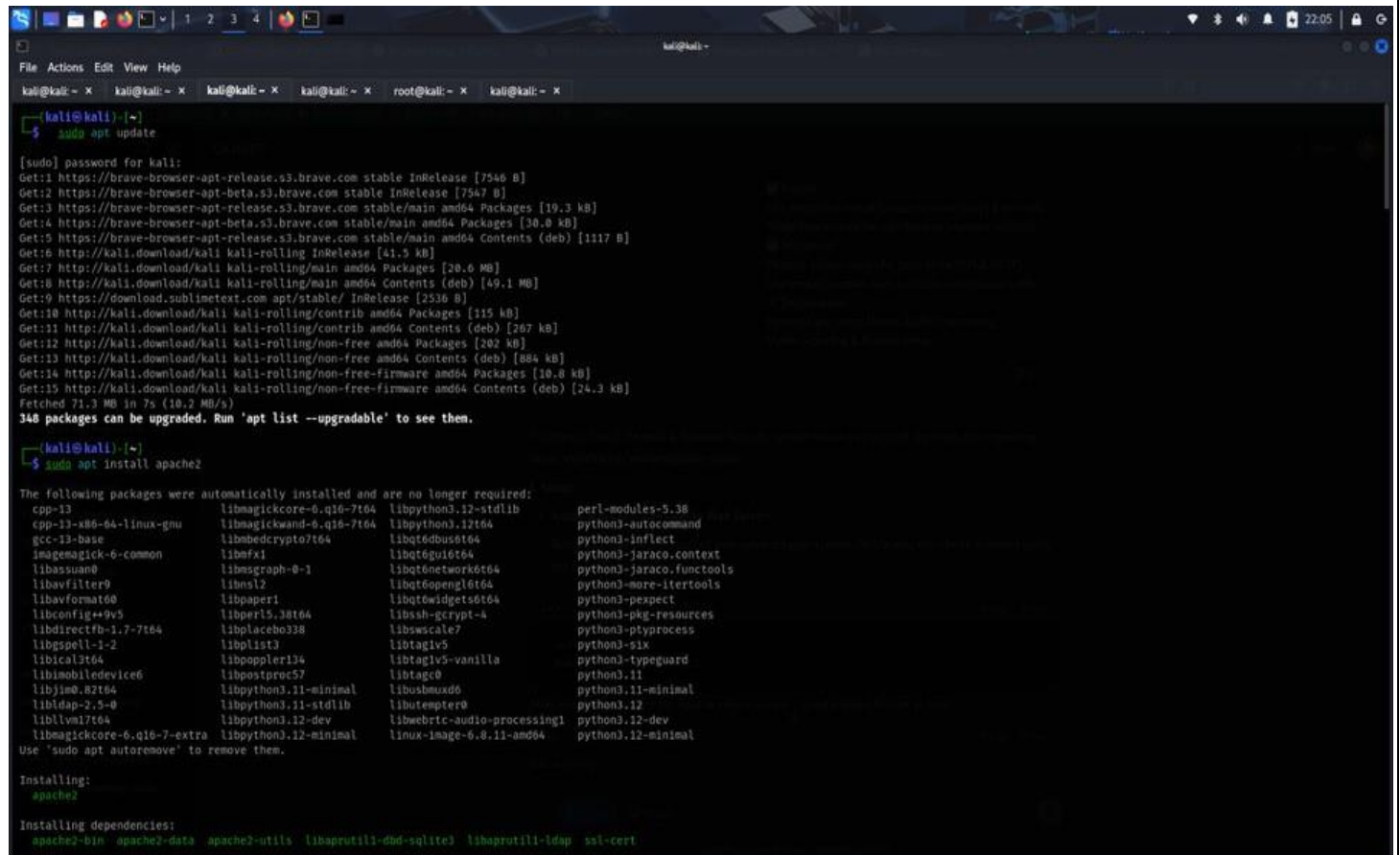


POC TASK 3

1. Setup:

- **Install and Configure Apache Web Server:**



```
(kali@kali) ~$ sudo apt update
[sudo] password for kali:
Get:1 https://brave-browser-apt-release.s3.brave.com stable InRelease [7546 B]
Get:2 https://brave-browser-apt-beta.s3.brave.com stable InRelease [7547 B]
Get:3 https://brave-browser-apt-release.s3.brave.com stable/main amd64 Packages [19.3 kB]
Get:4 https://brave-browser-apt-beta.s3.brave.com stable/main amd64 Packages [30.0 kB]
Get:5 https://brave-browser-apt-release.s3.brave.com stable/main amd64 Contents (deb) [1117 B]
Get:6 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:7 http://kali.download/kali kali-rolling/main amd64 Packages [20.6 MB]
Get:8 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [49.1 MB]
Get:9 https://download.sublimetext.com apt/stable/ InRelease [2536 B]
Get:10 http://kali.download/kali kali-rolling/contrib amd64 Packages [115 kB]
Get:11 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [767 kB]
Get:12 http://kali.download/kali kali-rolling/non-free amd64 Packages [202 kB]
Get:13 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [884 kB]
Get:14 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [10.8 kB]
Get:15 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [24.3 kB]
Fetched 71.3 MB in 7s (10.2 MB/s)
348 packages can be upgraded. Run 'apt list --upgradable' to see them.

(kali@kali) ~$ sudo apt install apache2

The following packages were automatically installed and are no longer required:
  cpp-13 libmagickcore-6.q16-7t64 libpython3.12-stdlib perl-modules-5.38
  cpp-13-x86-64-linux-gnu libmagickwand-6.q16-7t64 libpython3.12t64 python3-autocommand
  gcc-13-base libnbdcrypto7t64 libqt6dbus6t64 python3-infect
  imagemagick-6-common libbfx1 libqt6gui6t64 python3-jaraco.context
  libassuan0 libbng0 libqt6network6t64 python3-jaraco.functions
  libavfilter9 libbns12 libqt6opengl6t64 python3-more-itertools
  libavformat60 libbzip2 libqt6widgets6t64 python3-pexpect
  libconfig++9v5 libperl5.38t64 libssh-gcrypt-4 python3-pkg-resources
  libdirectfb-1.7-7t64 libplacebo338 libswscale7 python3-ptyprocess
  libgspell-1-2 libplist3 libtag1v5 python3-six
  libical3t64 libpoppler134 libtag1v5-vanilla python3-typeguard
  libmobiledevice6 libpostproc57 libtag0 python3.11
  libjme82t64 libpython3.11-minimal libusbmuxd0 python3.11-minimal
  libldap-2.5-0 libpython3.11-stdlib libutempter0 python3.12
  liblvm1t64 libpython3.12-dev libwebp1t64 python3.12-dev
  libmagickcore-6.q16-7-extra libpython3.12-minimal linux-image-6.8.11-amd64 python3.12-minimal

Use 'sudo apt autoremove' to remove them.

Installing:
  apache2

Installing dependencies:
  apache2-bin apache2-data apache2-utils libaprutil1-dbd-sqlite3 libaprutil1-ldap ssl-cert
```

Begin by installing the Apache2 web server on your system. On Ubuntu, this can be achieved using the following commands:

To update the package lists for available software and install Apache2, use the following commands:

Sudo apt update

The above command is essential as it refreshes the package index and ensures we fetch the latest version of Apache2:

sudo apt install apache2

- **After installation, ensure the Apache service is running and enabled to start at boot**

```
File Actions Edit View Help
kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x root@kali: ~ x kali@kali: ~ x

Enabling conf localized-error-pages.
Enabling conf other-vhosts-access-log.
Enabling conf security.
Enabling conf serve-cgi-bin.
Enabling site 000-default.
update-rc.d: As per Kali policy, apache2 init script is left disabled.
update-rc.d: We have no instructions for the apache-htcacheclean init script.
update-rc.d: It looks like a non-network service, we enable it.
apache2.service is a disabled or a static unit, not starting it.
apache-htcacheclean.service is a disabled or a static unit, not starting it.
Processing triggers for kali-menu (2025.1.1) ...
Processing triggers for man-db (2.13.0-1) ...

(kali@kali)~$ sudo systemctl start 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.serv
ice'.

(kali@kali)~$ sudo ufw disable
sudo: ufw: command not found

(kali@kali)~$ sudo apt update
(kali@kali)~$ sudo apt install ufw

Hit:1 https://brave-browser-apt-beta.s3.brave.com stable InRelease
Hit:2 https://brave-browser-apt-release.s3.brave.com stable InRelease
Hit:3 http://http.kali.org/kali kali-rolling InRelease
Hit:4 https://download.sublimetext.com apt/stable/ InRelease
348 packages can be upgraded. Run 'apt list --upgradable' to see them.
The following packages were automatically installed and are no longer required:
  cpp-13 libmagickcore-6.q16-7t64 libpython3.12-stdlib
  cpp-13-x86-64-linux-gnu libmagickwand-6.q16-7t64 libpython3.12t64
  gcc-13-base libb6d-crypto7t64 libt6dbs6t64
  imagemagick-6-common libwebp1 libt6dgui6t64
  libassuan0 libassuan0 libt6dnetwork6t64
  libavfilter9 libb6d libt6dopencl6t64
  libavformat60 libb6d libt6dwidg6t64
  libconfig++9v5 libperl5.38t64 libt6d-gcrypt-4
  libdirectfb-1.7-7t64 libplacebo338 libswscale7
  perl-modules-5.38 python3-autocommand
  python3-infiect python3-jaraco.context
  python3-jaraco.funcitools
  python3-more-iteritools
  python3-pexpect python3-pkg-resources
  python3-ptyprocess
```

After the installation is complete, the next crucial step is to ensure that the Apache service is up and running. Additionally, it should be enabled to start automatically whenever the system reboots. To achieve this, use the following commands:

sudo systemctl start apache2

sudo systemctl enable apache2

- **Disable UFW to Allow All Traffic:**

To disable the Uncomplicated Firewall (UFW) and allow all incoming and outgoing traffic, I used this command

sudo ufw disable

- **Exploit:**

Scan for Open Ports and Services Using Nmap and Netcat:

With the firewall disabled, an attacker can utilize tools like Nmap and Netcat to identify open ports and running services:

- **Nmap Scan:**

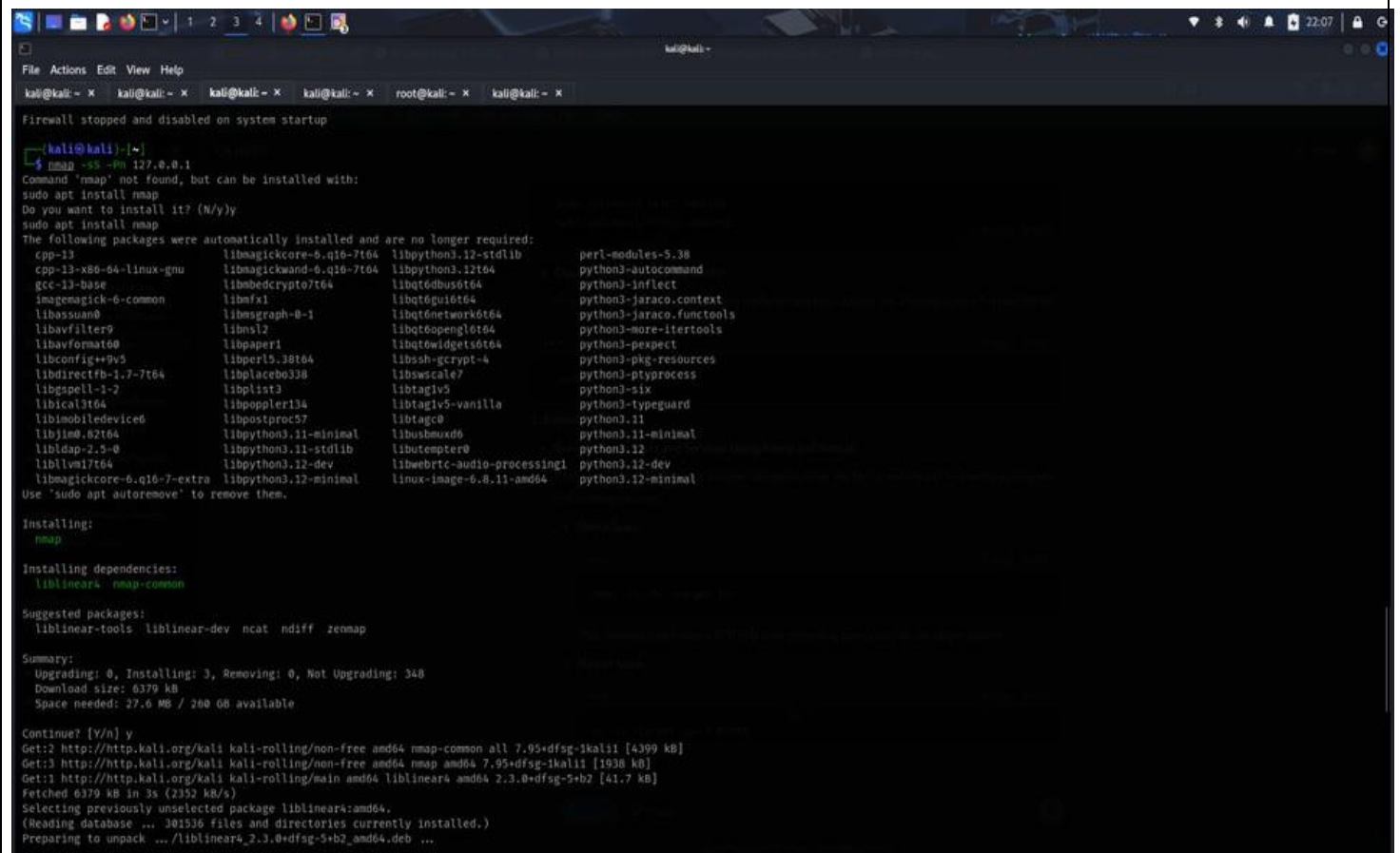
`nmap -sS -Pn <target_ip>`

This command performs a TCP SYN scan, detecting open ports on the target system.

- **Netcat Scan:**

To check open ports with Netcat, I used this command:

`nc -zv <target_ip> 1-65535`



```
kali@kali: ~  
File Actions Edit View Help  
kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x root@kali: ~ x kali@kali: ~ x  
Firewall stopped and disabled on system startup  
kali@kali: ~  
$ nmap -sS -Pn 127.0.0.1  
Command 'nmap' not found, but can be installed with:  
sudo apt install nmap  
Do you want to install it? (N/y)y  
sudo apt install nmap  
The following packages were automatically installed and are no longer required:  
  cpp-13 libmagiccore-6.q16-7t64 libpython3.12-stdlib perl-modules-5.38  
  gcc-13-base libmagicwand-6.q16-7t64 libpython3.12t64 python3-autocommand  
  imagemagick-6-common libmfx1 libqt6dbus6t64 python3-infect  
  libassuan0 libmsgpack-0-1 libqt6gui6t64 python3-jaraco.context  
  libavfilter9 libns12 libqt6network6t64 python3-jaraco.funtools  
  libavformat6 libpaper1 libqt6opengl6t64 python3-more-iterools  
  libconfig++9v5 libperl5.38t64 libssh-gcrypt-4 python3-pepext  
  libdirectfb-1.7-7t64 libplacebo338 libswscale7 python3-pkg-resources  
  libgspell-1-2 libplist3 libtag1v5 python3-ptypprocess  
  libical3t64 libpoppler134 libtag1v5-vanilla python3-six  
  libmobiledevice6 libpostproc57 libtagc0 python3-typeguard  
  libjme0.62t64 libpython3.11-minimal libusbmuxd6 python3.11-minimal  
  libldap-2.5-0 libpython3.11-stdlib libutempter0 python3.12  
  liblvm1t64 libpython3.12-dev libwebRTC-audio-processing1 python3.12-dev  
  libmagiccore-6.q16-7-extra libpython3.12-minimal linux-image-6.8.11-amd64 python3.12-minimal  
Use 'sudo apt autoremove' to remove them.  
  
Installing:  
  nmap  
  
Installing dependencies:  
  liblinear4 nmap-common  
  
Suggested packages:  
  liblinear-tools liblinear-dev ncat ndiff zenmap  
  
Summary:  
  Upgrading: 0, Installing: 3, Removing: 0, Not Upgrading: 348  
  Download size: 6379 kB  
  Space needed: 27.6 MB / 268 GB available  
  
Continue? [Y/n] y  
Get:2 http://http.kali.org/kali kali-rolling/non-free amd64 nmap-common all 7.95+dfsg-1kali1 [4399 kB]  
Get:3 http://http.kali.org/kali kali-rolling/non-free amd64 nmap amd64 7.95+dfsg-1kali1 [1938 kB]  
Get:1 http://http.kali.org/kali kali-rolling/main amd64 liblinear4 amd64 2.3.0+dfsg-5+b2 [41.7 kB]  
Fetched 6379 kB in 3s (2352 kB/s)  
Selecting previously unselected package liblinear4:amd64.  
(Reading database ... 301536 files and directories currently installed.)  
Preparing to unpack .../liblinear4_2.3.0+dfsg-5+b2_amd64.deb ...
```

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x root@kali: ~ x kali@kali: ~ x  
Get:2 http://http.kali.org/kali kali-rolling/non-free amd64 nmap-common all 7.95+dfsg-1kali1 [4399 kB]  
Get:3 http://http.kali.org/kali kali-rolling/non-free amd64 nmap amd64 7.95+dfsg-1kali1 [1938 kB]  
Get:1 http://http.kali.org/kali kali-rolling/main amd64 liblinear4 amd64 2.3.0+dfsg-5+b2 [41.7 kB]  
Fetched 6379 kB in 3s (2352 kB/s)  
Selecting previously unselected package liblinear4:amd64.  
(Reading database ... 301536 files and directories currently installed.)  
Preparing to unpack .../liblinear4_2.3.0+dfsg-5+b2_amd64.deb ...  
Unpacking liblinear4:amd64 (2.3.0+dfsg-5+b2) ...  
Selecting previously unselected package nmap-common.  
Preparing to unpack .../nmap-common_7.95+dfsg-1kali1_all.deb ...  
Unpacking nmap-common (7.95+dfsg-1kali1) ...  
Selecting previously unselected package nmap.  
Preparing to unpack .../nmap_7.95+dfsg-1kali1_amd64.deb ...  
Unpacking nmap (7.95+dfsg-1kali1) ...  
Setting up liblinear4:amd64 (2.3.0+dfsg-5+b2) ...  
Setting up nmap-common (7.95+dfsg-1kali1) ...  
Setting up nmap (7.95+dfsg-1kali1) ...  
Setcap worked! Adding configuration to environment  
Processing triggers for kali-menu (2025.1.1) ...  
Processing triggers for libc-bin (2.40-3) ...  
Processing triggers for man-db (2.13.0-1) ...  
Processing triggers for wordlists (2023.2.0) ...  
  
(kali@kali)~$ nmap -sS -pN 127.0.0.1  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-11 20:59 IST  
Nmap scan report for localhost (127.0.0.1)  
Host is up (0.0000030s 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 0.11 seconds  
  
(kali@kali)~$ nc -zv 127.0.0.1 1-65535  
localhost [127.0.0.1] 56870 (?) open  
localhost [127.0.0.1] 80 (http) open  
localhost [127.0.0.1] 22 (ssh) open
```

This command checks for open TCP ports in the specified range on the target.

These scans can reveal exposed services, providing potential entry points for attackers.

2. Mitigation:

• Restrict Access Using UFW:

Re-enable UFW and configure it to allow only essential services, such as SSH (port 22) and HTTP (port 80):

`sudo ufw enable`

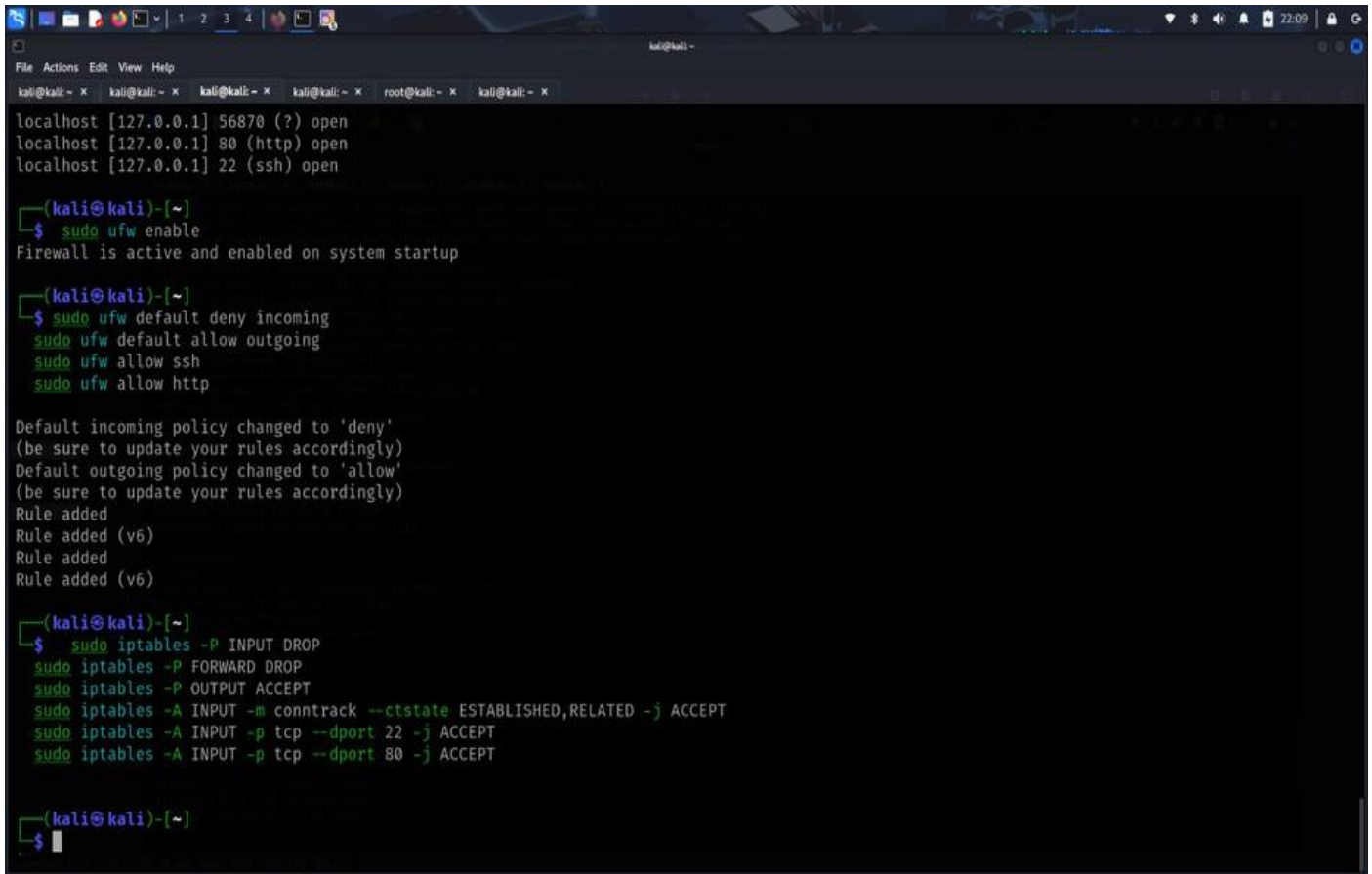
`sudo ufw default deny incoming`

`sudo ufw default allow outgoing`

`sudo ufw allow ssh`

`sudo ufw allow http`

This configuration denies all incoming traffic except for SSH and HTTP, enhancing security.



```
kali@kali: ~  
File Actions Edit View Help  
kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x root@kali: ~ x kali@kali: ~ x  
localhost [127.0.0.1] 56870 (?) open  
localhost [127.0.0.1] 80 (http) open  
localhost [127.0.0.1] 22 (ssh) open  
  
(kali@kali)-[~]  
$ sudo ufw enable  
Firewall is active and enabled on system startup  
  
(kali@kali)-[~]  
$ sudo ufw default deny incoming  
$ sudo ufw default allow outgoing  
$ sudo ufw allow ssh  
$ sudo ufw allow http  
  
Default incoming policy changed to 'deny'  
(be sure to update your rules accordingly)  
Default outgoing policy changed to 'allow'  
(be sure to update your rules accordingly)  
Rule added  
Rule added (v6)  
Rule added  
Rule added (v6)  
  
(kali@kali)-[~]  
$ sudo iptables -P INPUT DROP  
$ sudo iptables -P FORWARD DROP  
$ sudo iptables -P OUTPUT ACCEPT  
$ sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT  
$ sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT  
$ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT  
  
(kali@kali)-[~]  
$
```

- **Implement iptables Rules to Block Unnecessary Traffic:**

For more granular control, iptables can be used to define specific rules:

```
sudo iptables -P INPUT DROP  
sudo iptables -P FORWARD DROP  
sudo iptables -P OUTPUT ACCEPT  
sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT  
sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT  
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

These commands set default policies to drop incoming and forwarding traffic, accept outgoing traffic, and allow established connections along with SSH and HTTP traffic.

