

**International Cybersecurity and Digital Forensic  
Academy**

**PROGRAMME: CYBERSECURITY AND ETHICAL  
HACKING INTERNSHIP**

**ASSIGNMENT**

**PRESENTED BY**

**AYILARA BUSARI DARE**

**IDEAS/24/28133**

**COURSE CODE: INT301**

**COURSE TITLE: Operating Systems Fundamentals**

## **INT301: Operating Systems Fundamentals – Week 1 Labs: Investigate Kali Linux**

**An operating system (OS)** is the fundamental software that manages a computer's hardware and software resources, providing a user interface and enabling communication between hardware and software.

### **Key Concepts:**

- **Kernel:** The core of the OS that manages hardware and software resources at a low level.
- **Shell:** The user interface that allows users to interact with the OS.
- **Process Management:** The OS manages the execution of programs (processes) and allocates resources to them.
- **Memory Management:** The OS allocates and manages memory space for running programs.
- **File System:** The OS organizes and manages files and directories on storage devices

**Linux** is an open-source operating system known for its speed, reliability, and efficiency. It can run on minimal hardware resources and is highly customizable. Unlike proprietary systems like Windows and Mac OS X, Linux is maintained by a community of developers, making it adaptable for various applications, from embedded devices to supercomputers.

Kali Linux is a specialized distribution designed for security auditing and penetration testing. It includes numerous tools for these tasks, but it is not intended for everyday use like gaming or general development. As a cybersecurity professional, it's crucial to be adept at navigating both the graphical user interface (GUI) and the command line in Kali Linux.

### **Step 1: Command Documentation**

1. **Learn About the Man Page:**

```
File Actions Edit View Help
MAN(1) Manual pager utils MAN(1)
NAME
man - an interface to the system reference manuals
SYNOPSIS
man [man options] [[section] page ...] ...
man -k [apropos options] regexp ...
man -K [man options] [section] term ...
man -f [whatis options] page ...
man -l [man options] file ...
man -w|-W [man options] page ...
DESCRIPTION
man is the system's manual pager. Each page argument given to man is normally the name of a program, utility or function. The manual page associated with each of these arguments is then found and displayed. A section, if provided, will direct man to look only in that section of the manual. The default action is to search in all of the available sections following a pre-defined order (see DEFAULTS), and to show only the first page found, even if page exists in several sections.
The table below shows the section numbers of the manual followed by the types of pages they contain.
Manual page man(1) line 1 (press h for help or q to quit)
```

Command	Description
mv	Moves or renames files and directories.
chmod	Modifies file permissions.
chown	Changes the ownership of a file.
dd	Copies data from an input to an output.
pwd	Displays the name of the current directory.
ps	Lists the processes currently running in the system.
su	Simulates a login as another user or to become a superuser.
sudo	Runs a command as a superuser or another named user.
grep	Searches for specific strings of characters within a file.
ifconfig	Displays or configures network card information (deprecated; use ip address).
apt-get	Installs, configures, and removes packages on Debian-based systems.
iwconfig	Displays or configures wireless network card information.

<b>shutdown</b>	Shuts down the computer or performs related tasks.
<b>passwd</b>	Changes the password for the current user.
<b>cat</b>	Lists the contents of a file.

## Step 2: Create and Change Directories

In this step, you will use the cd, mkdir, and ls commands.

### 1. Print the Current Working Directory: pwd

```
File Actions Edit View Help
(kali@kali)-[~]
$ pwd
/home/kali
```

### 2. Navigate to the /home/kali Directory: cd /home/kali

```
(kali@kali)-[~]
$ cd /home/kali

(kali@kali)-[~]
$
```

### 3. List Files in the Current Directory: ls -l

```
(kali@kali)-[~]
$ ls -l
total 68
drwxr-xr-x 5 kali      kali      4096 Jan 31 02:54 BurpSuitePro
drwxr-xr-x 2 kali      kali      4096 Jan 31 03:02 Desktop
drwxr-xr-x 2 kali      kali      4096 Dec 23 09:38 Documents
drwxr-xr-x 3 kali      kali      4096 Jan 30 03:43 Downloads
-rw-rw-r-- 1 kali      kali         0 Dec 29 13:11 file1.txt
-rw-rw-r-- 1 kali      kali      147 Dec 28 02:34 ismal2.txt
-rw-rw-r-- 1 kali      kali      253 Dec 28 02:34 ismal2.txt.nc
-rw-rw-r-- 1 kali      kali      240 Dec 28 02:22 ismal.txt
-rwxr-xr-x 1 kali      kali      147 Dec 28 02:13 manage.txt
drwxr-xr-x 2 kali      kali      4096 Dec 23 09:38 Music
drwxrwxr-x 2 kali      kali      4096 Dec 23 16:14 myfolder
drwxr-xr-x 2 kali      kali      4096 Jan 31 01:57 Pictures
drwxr-xr-x 2 student1 students 4096 Dec 23 16:16 project
drwxrwx--- 3 root      developers 4096 Dec 29 10:40 projects
drwxr-xr-x 2 kali      kali      4096 Dec 23 09:38 Public
drwxr-xr-x 2 kali      kali      4096 Dec 23 09:38 Templates
drwxr-xr-x 2 kali      kali      4096 Dec 23 09:38 Videos
-rw-r--r-- 1 kali      kali         28 Dec 30 13:44 welcome.txt
```

**Create a New Directory:** mkdir Test and **Verify the Directory Creation:** ls

```
File Actions Edit View Help
(kali㉿kali)-[~]
$ mkdir Test

(kali㉿kali)-[~]
$ ls
BurpSuitePro  file1.txt      manage.txt  project  Test
Desktop       ismal2.txt    Music      projects Videos
Documents     ismal2.txt.nc myfolder   Public   welcome.txt
Downloads     ismal.txt     Pictures   Templates
```

**Remove the Directory:** rmdir Test and **Verify the Directory Removal:** ls

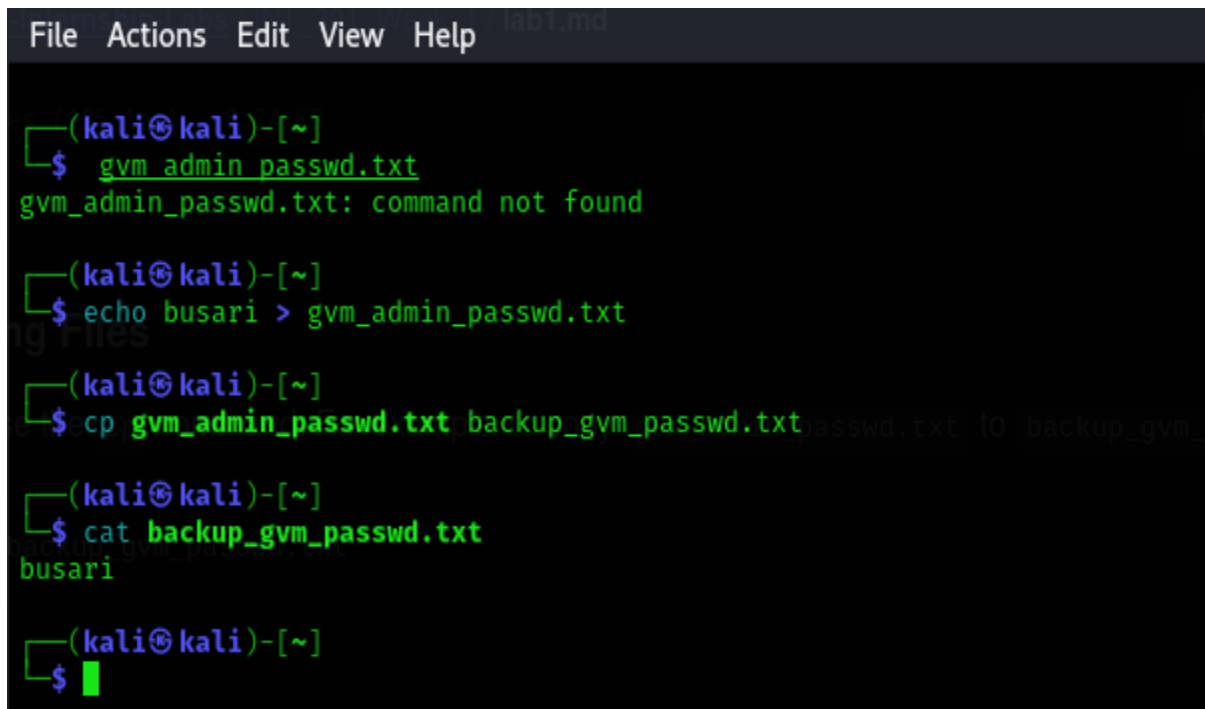
```
(kali㉿kali)-[~]
$ rmdir Test

(kali㉿kali)-[~]
$ ls
BurpSuitePro  Downloads  ismal2.txt.nc  Music  project  Templates
Desktop       file1.txt  ismal.txt     myfolder  projects  Videos
Documents     ismal2.txt manage.txt    Pictures  Public    welcome.txt
```

### Part 3: Copying and Moving Files

**Copy a File:** To copy a file, use the cp command. For example, to copy gvm\_admin\_passwd.txt to backup\_gvm\_passwd.txt: cp gvm\_admin\_passwd.txt

backup\_gvm\_passwd.txt

A terminal window with a dark background and light green text. The window has a menu bar at the top with 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal shows a series of commands and their outputs. The first command is 'gvm admin passwd.txt', which results in an error 'gvm\_admin\_passwd.txt: command not found'. The second command is 'echo busari > gvm\_admin\_passwd.txt', which successfully creates the file. The third command is 'cp gvm\_admin\_passwd.txt backup\_gvm\_passwd.txt', which successfully copies the file. The fourth command is 'cat backup\_gvm\_passwd.txt', which displays the output 'busari'. The prompt is '(kali@kali)-[~]' and the cursor is at the end of the last command line.

```
(kali@kali)-[~]
$ gvm admin passwd.txt
gvm_admin_passwd.txt: command not found

(kali@kali)-[~]
$ echo busari > gvm_admin_passwd.txt

(kali@kali)-[~]
$ cp gvm_admin_passwd.txt backup_gvm_passwd.txt

(kali@kali)-[~]
$ cat backup_gvm_passwd.txt
busari

(kali@kali)-[~]
$
```

#### Part 4: Deleting Files

**Delete a File:** To delete backup\_gvm\_passwd.txt: rm backup\_gvm\_passwd.txt

#### Part 5: Viewing File Content

**View File Contents:** To view the contents of a file: cat gvm\_admin\_passwd.txt

**Paginated Viewing:** If the file is long, use less for paginated viewing: less gvm\_admin\_passwd.txt

```
File Actions Edit View Help lab1.md
(kali㉿kali)-[~]
$ gvm_admin_passwd.txt
gvm_admin_passwd.txt: command not found

(kali㉿kali)-[~]
$ echo busari > gvm_admin_passwd.txt

(kali㉿kali)-[~]
$ cp gvm_admin_passwd.txt backup_gvm_passwd.txt

(kali㉿kali)-[~]
$ cat backup_gvm_passwd.txt
busari

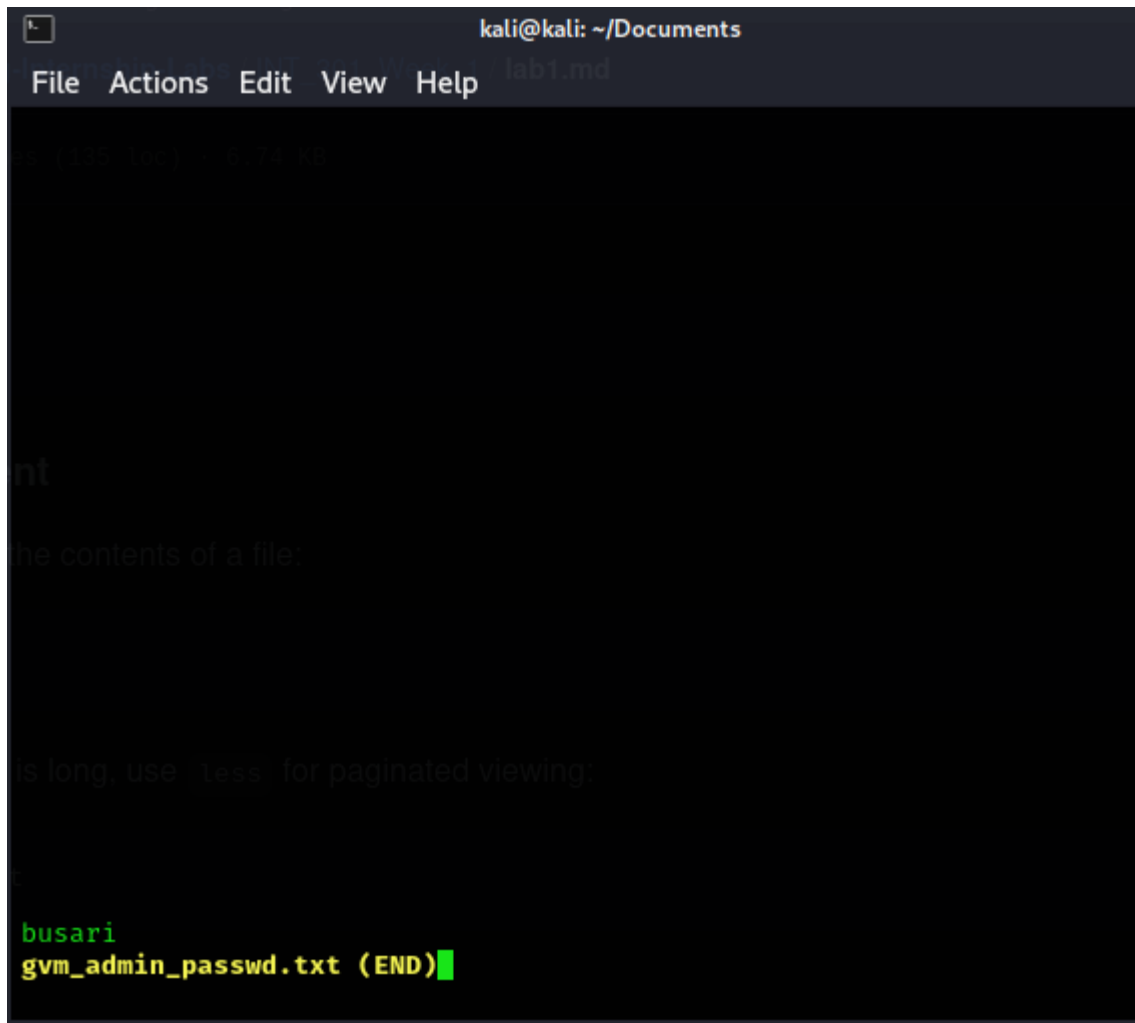
(kali㉿kali)-[~]
$ ls
backup_gvm_passwd.txt  file1.txt  manage.txt  projects
BurpSuitePro          gvm_admin_passwd.txt  Music       Public
Desktop               ismal2.txt  myfolder   Templates
Documents              ismal2.txt.nc  Pictures   Videos
Downloads              ismal.txt     project    welcome.txt

(kali㉿kali)-[~]
$
```

```
File Actions Edit View Help lab1.md
(kali㉿kali)-[~]
$ mv gvm_admin_passwd.txt Documents/

(kali㉿kali)-[~]
$ ls Documents
gvm_admin_passwd.txt

(kali㉿kali)-[~]
$
```



The screenshot shows a terminal window with the title bar 'kali@kali: ~/Documents'. The menu bar includes 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal content shows a command being executed: `cat /dev/urandom | tr -dc 'a-z0-9' | fold -w 64 | xargs -n1 sh`. The output of the command is `busari gvm_admin_passwd.txt (END)`.

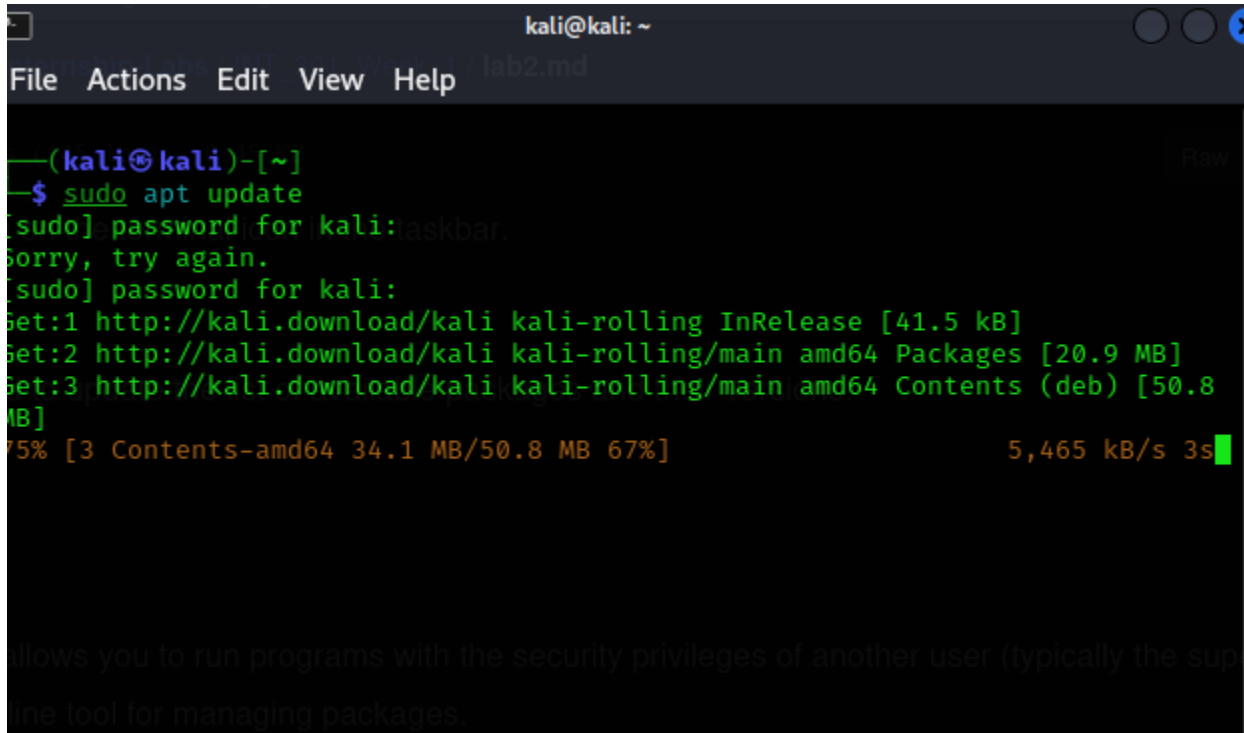
## Installing Packages and Applications - Lab 2: Installing Packages and Applications

### Update the Package List:

- Run the following command to update the list of available packages and their versions: **sudo apt update**
- **Explanation:**
  - The sudo command allows you to run programs with the security privileges of another user (typically the superuser).
  - apt is the command-line tool for managing packages.



- update fetches the latest package information from the repositories configured on your system. This ensures you have the most current information about the software available for installation.



```
(kali@kali)~$ sudo apt update
[sudo] password for kali:
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [20.9 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [50.8 MB]
75% [3 Contents-amd64 34.1 MB/50.8 MB 67%] 5,465 kB/s 3s
```

## Part 2: Installing Packages

### Install curl:

- Use APT to install curl, a command-line tool for transferring data with URLs:

`sudo apt install curl`

- **Explanation:**
  - install tells APT to fetch the specified package and any required dependencies from the repository and install them.
  - curl is a useful tool for testing endpoints and downloading files.

```
kali@kali: ~
lab2.md
File Actions Edit View Help

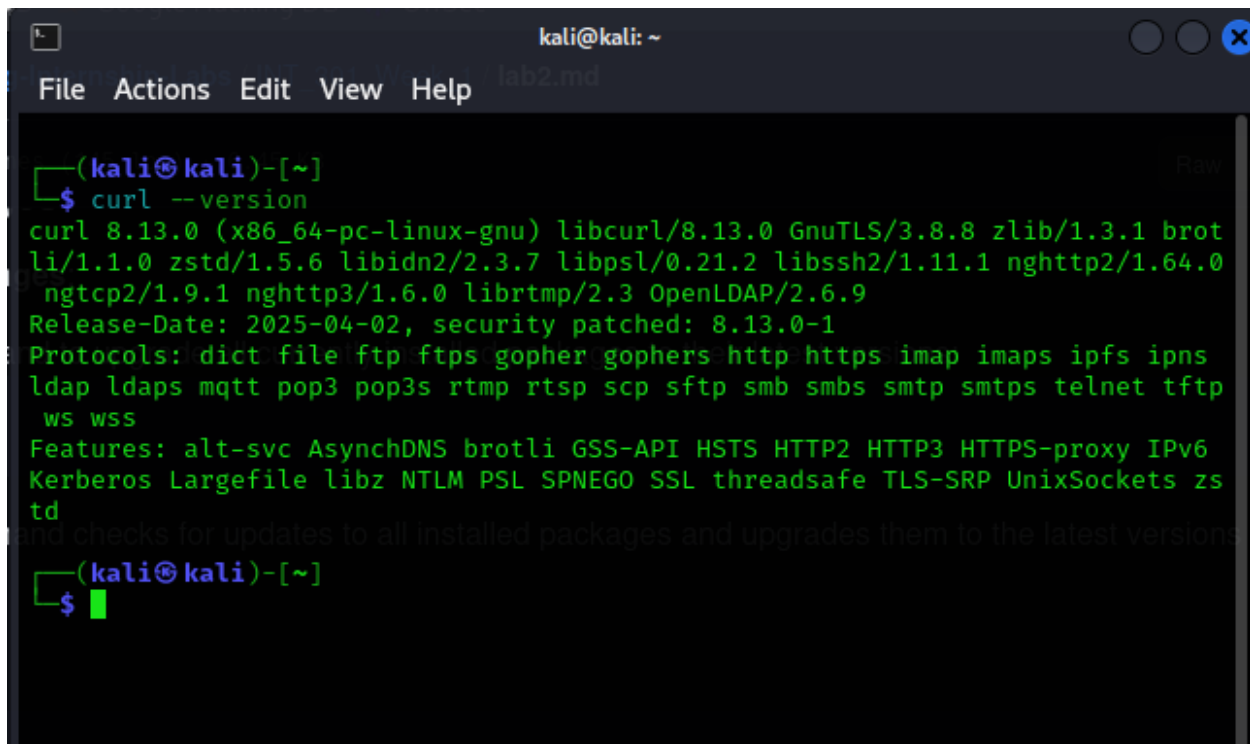
(kali@kali)-[~]
$ sudo apt install curl
The following packages were automatically installed and are no longer required:
  imagemagick-6-common libfmt9 libmagickcore-6.q16-7-extra
  imagemagick-6.q16 libgl1-mesa-dev libmagickcore-6.q16-7t64
  libbfgio1 libgles-dev libmagickwand-6.q16-7t64
  libc++1-19 libgles1 libmbedcrypto7t64
  libc++abi1-19 libglvnd-core-dev libsuperlu6
  libegl-dev libglvnd-dev libunwind-19
Use 'sudo apt autoremove' to remove them.
Upgrading:
  curl ldap-utils libcurl3t64-gnutls libcurl4t64 libldap-common
Installing dependencies:
  libldap2
Summary:
  Upgrading: 5, Installing: 1, Removing: 0, Not Upgrading: 1582
  Download size: 1,404 kB
  Space needed: 751 kB / 60.5 GB available
Continue? [Y/n] Y
```

## Verify the Installation:

- Check the version of curl to confirm the installation was successful:

curl --version

- **Explanation:** This command displays the installed version of curl. If installed correctly, it will show version information.

A terminal window titled 'kali@kali: ~' with a menu bar (File, Actions, Edit, View, Help) and a file named 'lab2.md'. The terminal shows the command 'curl --version' being executed, displaying detailed version information for curl 8.13.0, including supported protocols and features. The prompt returns to '(kali@kali)-[~]' after the command.

```
(kali@kali)-[~]
$ curl --version
curl 8.13.0 (x86_64-pc-linux-gnu) libcurl/8.13.0 GnuTLS/3.8.8 zlib/1.3.1 brot
li/1.1.0 zstd/1.5.6 libidn2/2.3.7 libpsl/0.21.2 libssh2/1.11.1 nghttp2/1.64.0
ngtcp2/1.9.1 nghttp3/1.6.0 librtmp/2.3 OpenLDAP/2.6.9
Release-Date: 2025-04-02, security patched: 8.13.0-1
Protocols: dict file ftp ftps gopher gophers http https imap imaps ipfs ipns
ldap ldaps mqtt pop3 pop3s rtmp rtsp scp sftp smb smbs smtp smtps telnet tftp
ws wss
Features: alt-svc AsynchDNS brotli GSS-API HSTS HTTP2 HTTP3 HTTPS-proxy IPv6
Kerberos Largefile libz NTLM PSL SPNEGO SSL threadsafe TLS-SRP UnixSockets zs
td
(kali@kali)-[~]
$
```

### Part 3: Upgrading Packages

#### Upgrade All Installed Packages:

- Run the following command to upgrade all currently installed packages to their latest versions:

#### **sudo apt upgrade**

- **Explanation:** This command checks for updates to all installed packages and upgrades them to the latest versions available in the repository.

```
kali@kali: ~  
File Actions Edit View Help lab2.md  
  
(kali@kali)-[~]  
$ sudo apt upgrade  
The following packages were automatically installed and are no longer required:  
firebird3.0-common libicu-dev  
firebird3.0-common-doc libmagickcore-6.q16-7-extra  
icu-devtools libmagickcore-6.q16-7t64  
imagemagick-6-common libmagickwand-6.q16-7t64  
imagemagick-6.q16 libmbedcrypto7t64  
libbfio1 libmsgpack-0-1  
libc++1-19 libpaper1  
libc++abi1-19 libqt5sensors5  
libcapstone4 libqt5webkit5  
libconfig++9v5 libsuperlu6  
libconfig9 libtag1v5  
libegl-dev libtag1v5-vanilla  
libflac12t64 libtagc0  
libfmt9 libunwind-19  
libgeos3.13.0 libwebRTC-audio-processing1  
libgl1-mesa-dev openjdk-23-jre  
libglapi-mesa openjdk-23-jre-headless  
libgles-dev python3-appdirs  
libgles1 python3-ntlm-auth  
libglvnd-core-dev python3-setproctitle  
libglvnd-dev ruby-zeitwerk  
libgtksourceview-3.0-1 ruby3.1
```

## Part 5: Searching for Packages

### Search for Networking Packages:

- Use the APT search functionality to find packages related to networking:

apt search networking

- **Explanation:** This command searches the package database for any packages that have "networking" in their name or description, displaying a list of matching packages.

```
kali@kali: ~  
File Actions Edit View Help lab2.md  
  
(kali@kali)-[~]  
$ apt search networking  
a2boot/kali-rolling 4.1.2~ds-1 amd64  
  AppleTalk Network Suite (Apple II NetBoot)  
  
atalkd/kali-rolling 4.1.2~ds-1 amd64  
  AppleTalk Network Suite  
  
atmel-firmware/kali-rolling 1.3-7.1 all  
  Firmware for Atmel at76c50x wireless networking chips.  
  
auto-apt-proxy/kali-rolling 16.5 all  
  automatic detector of common APT proxy settings  
  
batctl/kali-rolling 2025.0-2 amd64  
  B.A.T.M.A.N. advanced control and management tool  
  
batmand/kali-rolling 0.3.2+74+g2f62b17-2 amd64  
  better approach to mobile adhoc networking  
  
bittwist/kali-rolling 4.7+ds-2 amd64  
  libpcap based Ethernet packet generator  
  
bootp/kali-rolling 2.4.3-21 amd64  
  server for the bootp protocol with DHCP support
```

## Part 6: Managing Repositories

### Edit Repositories:

- Open the sources.list file to view and manage your APT repositories:

`sudo nano /etc/apt/sources.list`

- **Explanation:** This file contains a list of repositories that APT uses to fetch packages. Using nano opens the file in a text editor.

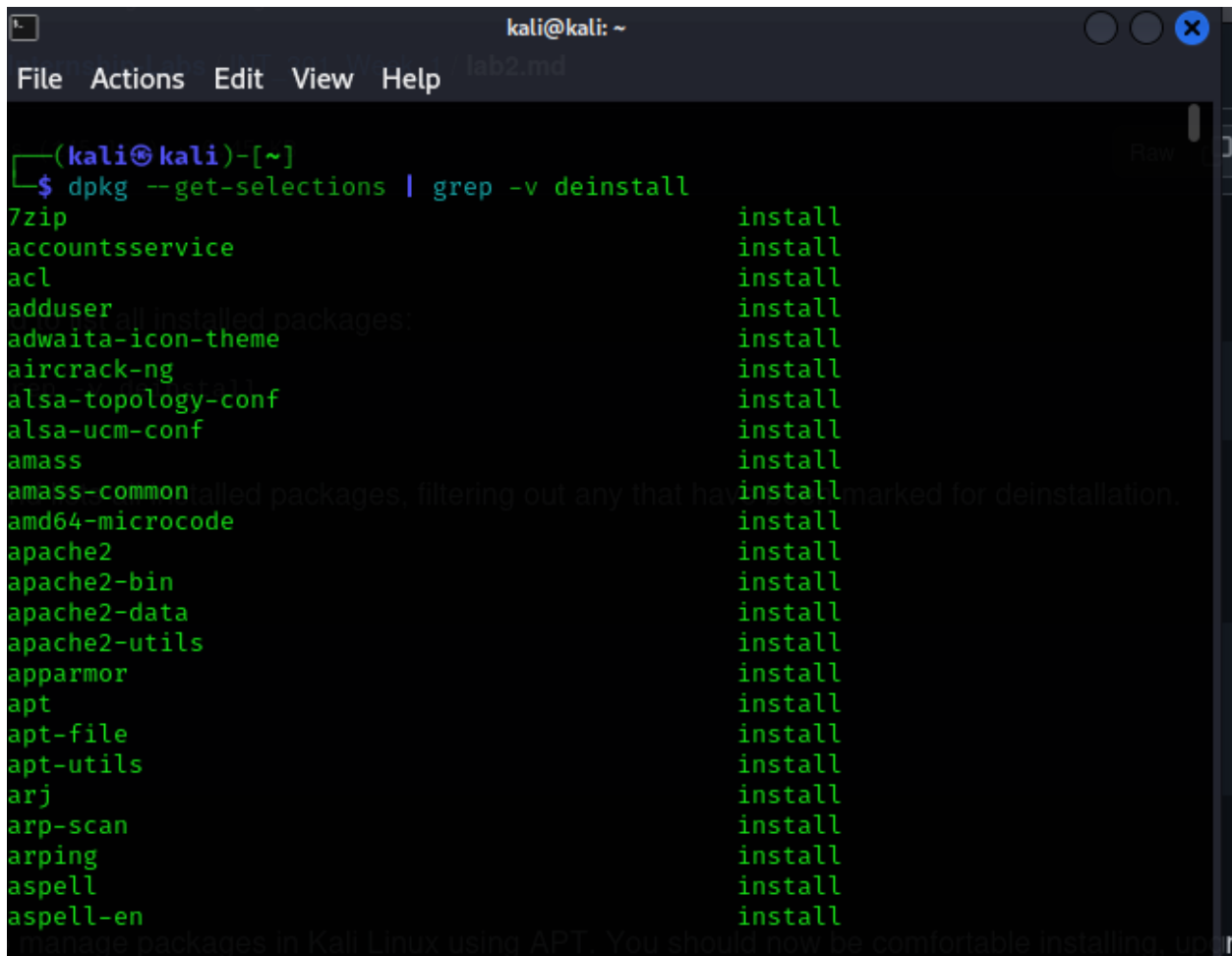
```
kali@kali: ~  
File Actions Edit View Help lab2.md  
GNU nano 8.2 /etc/apt/sources.list  
# See https://www.kali.org/docs/general-use/kali-linux-sources-list-reposito>  
deb http://http.kali.org/kali kali-rolling main contrib non-free non-free-fi>  
  
# Additional line for source packages  
# deb-src http://http.kali.org/kali kali-rolling main contrib non-free non-f>  
  
s, press ctrl + o to save and ctrl + x to exit the editor.  
  
es, run:  
  
and updates the package list again to include any new repositories you just enabled.  
  
^G Help      ^O Write Out  ^F Where Is  ^K Cut       ^T Execute  
^X Exit      ^R Read File  ^N Replace   ^U Paste     ^J Justify  
ad to list all installed packages:
```

### Explore Installed Packages:

- Use the following command to list all installed packages:

**dpkg --get-selections | grep -v deinstall**

- **Explanation:** This command lists all installed packages, filtering out any that have been marked for deinstallation.



```
kali@kali: ~  
File Actions Edit View Help lab2.md  
  
(kali@kali)-[~]  
$ dpkg --get-selections | grep -v deinstall  
7zip install  
accountsservice install  
acl install  
adduser install  
adwaita-icon-theme install  
aircrack-ng install  
alsa-topology-conf install  
alsa-ucm-conf install  
amass install  
amass-common install  
amd64-microcode install  
apache2 install  
apache2-bin install  
apache2-data install  
apache2-utils install  
apparmor install  
apt install  
apt-file install  
apt-utils install  
arj install  
arp-scan install  
arping install  
aspell install  
aspell-en install
```

### Lab 3: Networking Commands

Networking is a fundamental aspect of cybersecurity and system administration. Familiarity with networking commands allows you to configure, manage, and troubleshoot network connections effectively. Kali Linux includes a range of powerful tools for networking, making it an essential skill for ethical hackers and security professionals.

#### Part 1: Displaying Network Configuration

##### Open a Terminal:

- Start your Kali Linux VM.
- Open a terminal by clicking the terminal icon.

##### Check Network Interfaces:

- Use the following command to display the current network interfaces and their configuration: **ip addr show**

```

kali@kali: ~
File Actions Edit View Help lab3.md

(kali@kali)-[~]
$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
  link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
  inet 127.0.0.1/8 scope host lo
    valid_lft forever preferred_lft forever
  inet6 ::1/128 scope host noprefixroute
    valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
  link/ether 08:00:27:6e:13:6e brd ff:ff:ff:ff:ff:ff
  inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
    valid_lft 78875sec preferred_lft 78875sec
  inet6 fd00::e662:e8fe:f88c:f0ff/64 scope global dynamic noprefixroute
    valid_lft 86077sec preferred_lft 14077sec
  inet6 fe80::cf9c:8254:ec97:c32f/64 scope link noprefixroute
    valid_lft forever preferred_lft forever
(kali@kali)-[~]
$

```

### List Routing Table:

- To view the routing table, run: **ip route show**
- **Explanation:** This command displays the routing table, which contains information on how packets are routed through the network.

```

(kali@kali)-[~]
$ ip route show
default via 10.0.2.2 dev eth0 proto dhcp src 10.0.2.15 metric 100
10.0.2.0/24 dev eth0 proto kernel scope link src 10.0.2.15 metric 100
(kali@kali)-[~]
$

```

## Part 2: Testing Network Connectivity



## Ping a Host:

- Use the ping command to test connectivity to a remote host, such as Google: **ping -c 4 google.com**

**Explanation:** The -c 4 option sends 4 packets. The ping command checks if the host is reachable and measures the round-trip time for messages sent.

```
kali@kali: ~  
File Actions Edit View Help lab3.md  
  
(kali@kali)-[~]  
$ ping -c 4 google.com  
PING google.com (216.58.223.238) 56(84) bytes of data.  
64 bytes from 216.58.223.238: icmp_seq=1 ttl=255 time=963 ms  
64 bytes from 216.58.223.238: icmp_seq=2 ttl=255 time=1032 ms  
64 bytes from 216.58.223.238: icmp_seq=3 ttl=255 time=488 ms  
64 bytes from 216.58.223.238: icmp_seq=4 ttl=255 time=273 ms  
  
--- google.com ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 5169ms  
rtt min/avg/max/mdev = 272.541/688.783/1031.816/318.893 ms, pipe 2  
  
(kali@kali)-[~]  
$ █ connectivity to a remote host, such as Google.
```

## Trace Route to a Host:

- Use the traceroute command to see the path packets take to a destination:

traceroute google.com

- **Explanation:** traceroute shows the sequence of hops between your machine and the destination, helping diagnose where delays or failures occur.

```
(kali@kali)-[~]  
$ traceroute google.com  
traceroute to google.com (216.58.223.238), 30 hops max, 60 byte packets  
 1  10.0.2.2 (10.0.2.2)  44.774 ms  44.091 ms  43.356 ms  
 2  * * *  
 3  * * *  
 4  * * *  
 5  * * *  
 6  * * *  
 7  * * *  
 8  * * *  
 9  * * *  
10  * * *  
11  * * █
```

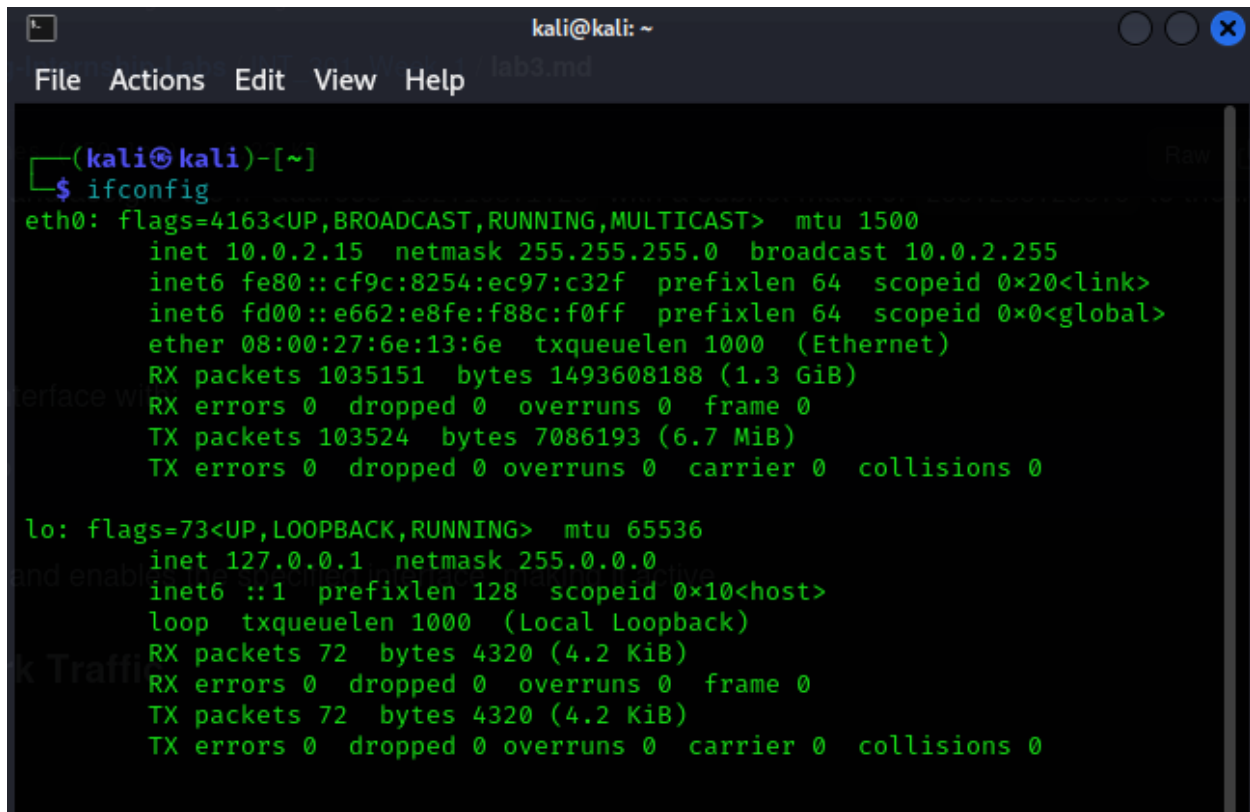
## Part 3: Configuring Network Interfaces

### View Current Interface Configuration:

- Use the following command to see the current settings for your network interfaces:

ifconfig

**Explanation:** The ifconfig command displays the configuration of all active network interfaces.

A screenshot of a Kali Linux terminal window. The window title is 'kali@kali: ~'. The menu bar shows 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal shows the command prompt '(kali@kali)-[~]' followed by '\$ ifconfig'. The output displays configuration for two interfaces: 'eth0' and 'lo'. 'eth0' is an Ethernet interface with flags 4163 (UP, BROADCAST, RUNNING, MULTICAST), MTU 1500, IP address 10.0.2.15, netmask 255.255.255.0, broadcast 10.0.2.255, and two IPv6 addresses. It shows statistics for RX and TX packets and bytes. 'lo' is a loopback interface with flags 73 (UP, LOOPBACK, RUNNING), MTU 65536, IP address 127.0.0.1, netmask 255.0.0.0, and one IPv6 address. It also shows RX and TX statistics.

```
(kali@kali)-[~]  
$ 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 fe80::cf9c:8254:ec97:c32f prefixlen 64 scopeid 0x20<link>  
    inet6 fd00::e662:e8fe:f88c:f0ff prefixlen 64 scopeid 0x0<global>  
    ether 08:00:27:6e:13:6e txqueuelen 1000 (Ethernet)  
    RX packets 1035151 bytes 1493608188 (1.3 GiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 103524 bytes 7086193 (6.7 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 72 bytes 4320 (4.2 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 72 bytes 4320 (4.2 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

### Manually Configure an Interface:

- To assign a static IP address to an interface (for example, eth0), use:

sudo ip addr add 192.168.1.20/24 dev eth0

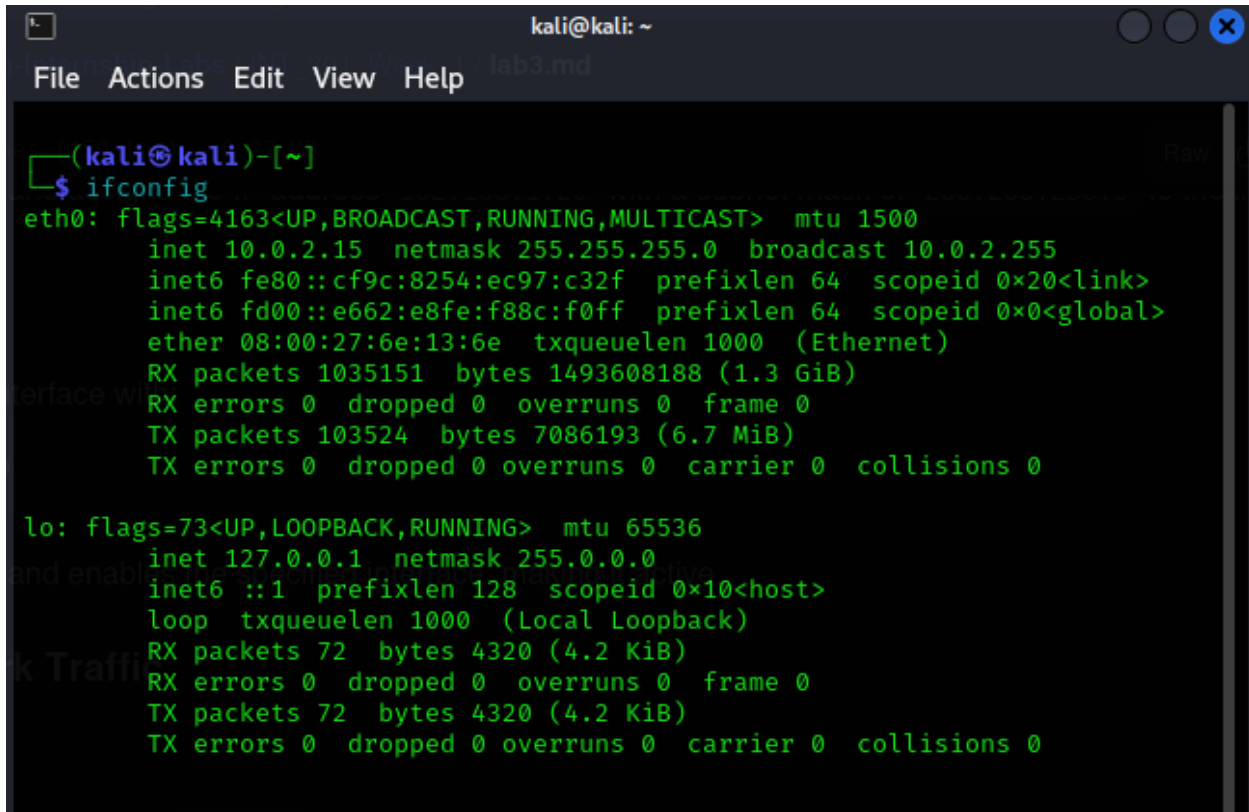
- **Explanation:** This command assigns the IP address 192.168.1.20 with a subnet mask of 255.255.255.0 to the interface eth0.

### Bring the Interface Up:

- Activate the configured interface with:

sudo ip link set eth0 up

- **Explanation:** This command enables the specified interface, making it active.



```
kali@kali: ~  
File Actions Edit View Help lab3.md  
  
(kali@kali)-[~]  
$ 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 fe80::cf9c:8254:ec97:c32f prefixlen 64 scopeid 0x20<link>  
    inet6 fd00::e662:e8fe:f88c:f0ff prefixlen 64 scopeid 0x0<global>  
    ether 08:00:27:6e:13:6e txqueuelen 1000 (Ethernet)  
    RX packets 1035151 bytes 1493608188 (1.3 GiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 103524 bytes 7086193 (6.7 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 72 bytes 4320 (4.2 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 72 bytes 4320 (4.2 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

## Part 4: Monitoring Network Traffic

### Install tcpdump:

- Use the following command to install tcpdump, a powerful packet analysis tool:  
**sudo apt install tcpdump**

**Explanation:** This command installs tcpdump, allowing you to capture and analyze network traffic.

```
kali@kali: ~
File Actions Edit View Help lab3.md

(kali@kali)-[~]
$ sudo apt install tcpdump
The following packages were automatically installed and are no longer required:
  imagemagick-6-common libfmt9 libmagickcore-6.q16-7-extra
  imagemagick-6.q16 libgl1-mesa-dev libmagickcore-6.q16-7t64
  libbfbio1 libgles-dev libmagickwand-6.q16-7t64
  libc++1-19 libgles1 libmbcrypto7t64
  libc++abi1-19 libglvnd-core-dev libssuperlu6
  libegl-dev libglvnd-dev libunwind-19
Use 'sudo apt autoremove' to remove them.

Upgrading:
  tcpdump

Summary:
  Upgrading: 1, Installing: 0, Removing: 0, Not Upgrading: 1581
  Download size: 471 kB
  Freed space: 4,096 B

0% [Connecting to http.kali.org]
```

### Capture Network Traffic:

- Use tcpdump to capture packets on eth0:

```
sudo tcpdump -i eth0 -c 10
```

**Explanation:** The -i option specifies the interface, and -c 10 limits the capture to 10 packets.

```
kali@kali: ~  
File Actions Edit View Help lab3.md  
Processing triggers for kali-menu (2024.4.0) ...  
Raw  
—(kali@kali)-[~]  
$ sudo tcpdump -i eth0 -c 10  
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode  
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes  
01:42:51.330067 IP 10.0.2.15.59320 > 93.243.107.34.bc.googleusercontent.com.h  
ttps: Flags [P.], seq 2394309471:2394309510, ack 1125696909, win 63333, lengt  
h 39  
01:42:51.335279 IP 10.0.2.15.59320 > 93.243.107.34.bc.googleusercontent.com.h  
ttps: Flags [P.], seq 39:63, ack 1, win 63333, length 24  
01:42:51.337170 IP 10.0.2.15.59320 > 93.243.107.34.bc.googleusercontent.com.h  
ttps: Flags [F.], seq 63, ack 1, win 63333, length 0  
01:42:51.362881 IP 93.243.107.34.bc.googleusercontent.com.https > 10.0.2.15.5  
9320: Flags [.], ack 39, win 65535, length 0  
01:42:51.362883 IP 93.243.107.34.bc.googleusercontent.com.https > 10.0.2.15.5  
9320: Flags [.], ack 63, win 65535, length 0  
01:42:51.362883 IP 93.243.107.34.bc.googleusercontent.com.https > 10.0.2.15.5  
9320: Flags [.], ack 64, win 65535, length 0  
01:42:51.421945 IP 10.0.2.15.52635 > 10.0.2.3.domain: 49848+ PTR? 93.243.107.  
34.in-addr.arpa. (44)  
01:42:51.461411 IP 93.243.107.34.bc.googleusercontent.com.https > 10.0.2.15.5  
9320: Flags [F.], seq 1, ack 64, win 65535, length 0  
01:42:51.461441 IP 10.0.2.15.59320 > 93.243.107.34.bc.googleusercontent.com.h  
ttps: Flags [.], ack 2, win 63333, length 0  
01:42:51.640429 IP6 fe80::2 > ip6-allnodes: ICMP6, router advertisement, leng  
th 56  
to see the status of all interfaces:
```

## Analyze Network Traffic:

- To see live traffic, run:

`sudo tcpdump -i eth0`

- **Explanation:** This command captures and displays all traffic on eth0 in real-time. Use Ctrl + C to stop the capture.

```
—(kali@kali)-[~]  
$ sudo tcpdump -i eth0 -c 10  
cpdump: verbose output suppressed, use -v[v]... for full protocol decode  
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes  
to see the status of all interfaces:
```

## Part 5: Final Review

### Check Network Status:

- Use the following command to see the status of all interfaces:

**nmcli device status**

**Explanation:** This command provides a summary of all network interfaces, showing their connection status.

```
(kali㉿kali)-[~]
$ nmcli device status
DEVICE    TYPE    CONNECTED STATE    CONNECTION
eth0      ethernet connected 1    Wired connection 1
lo        loopback  connected (externally)  lo
```

### Check Firewall Status:

- Check if the firewall is active and what rules are in place:

#### **sudo ufw status verbose**

- **Explanation:** This command shows the status of the Uncomplicated Firewall (UFW) and its rules.

```
(kali㉿kali)-[~]
$ sudo ufw status verbose
Status: inactive
```

## Lab 4: Linux File Permissions and Ownership

Linux employs a robust permission system that controls access to files and directories. Understanding and managing these permissions is crucial for system security. Each file and directory has an owner and a group associated with it, determining who can read, write, or execute the file.

### 1. File Permissions

Linux file permissions determine who can read, write, or execute files. Permissions are divided into three types:

- **Read (r):** Permission to read the file.
- **Write (w):** Permission to modify or delete the file.
- **Execute (x):** Permission to run the file as a program.

### 2. User Types

- **Owner:** The user who created the file.
- **Group:** Users who belong to the same group as the file's group.
- **Others:** All other users.

### 3. Permission Representation

Permissions are displayed as a string of ten characters:

- Example: -rwxr-xr--
  - The first character indicates the type (- for file, d for directory).
  - The next three characters are for the owner, the following three for the group, and the last three for others.

### 4. Permission Codes Table

Symbol	Meaning	Octal Value
r	Read permission	4
w	Write permission	2
x	Execute permission	1
-	No permission	0

### 5. Permissions Breakdown Table

Permissions String	Owner	Group	Others
rwxrwxrwx	rwx	rwx	rwx
Octal Equivalent	777		

### Commands to Learn

- ls -l: List files with permissions.
- chmod: Change file permissions.
- chown: Change file ownership.
- chgrp: Change group ownership.

## art 1: Viewing File Permissions

### Step 1: Check Current Permissions

1. Open your terminal.
2. Create a new directory: `mkdir PermissionTest`
3. Navigate into the directory: `cd PermissionTest`
4. Create a new file: `touch testfile.txt`
5. List the permissions: `ls -l`



```
kali@kali: ~/PermissionTest
File Actions Edit View Help lab4.md

(kali@kali)-[~]
$ mkdir PermissionTest

(kali@kali)-[~]
$ cd PermissionTest

(kali@kali)-[~/PermissionTest]
$ touch testfile.txt

(kali@kali)-[~/PermissionTest]
$ ls -l
total 0
-rw-rw-r-- 1 kali kali 0 Apr 11 01:56 testfile.txt

(kali@kali)-[~/PermissionTest]
$
```

### What to Observe:

- Notice the output showing permissions for testfile.txt

The file (testfile.txt) has permission of -rw-rw-r—for user, group and others.

## Part 2: Modifying Permissions

### Step 2: Change File Permissions

Change the permissions of testfile.txt to 777 (full permissions for everyone): **chmod 777 testfile.txt**

Verify the changes: **ls -l**

### Explanation:

- 777 means that the owner, group, and others all have read (r), write (w), and execute (x) permissions.



- This is useful for sharing files, but it poses security risks, as anyone can modify or delete the file.

```
kali@kali: ~/PermissionTest
File Actions Edit View Help lab4.md

(kali@kali)-[~/PermissionTest]
$ chmod 777 testfile.txt

(kali@kali)-[~/PermissionTest]
$ ls -l
total 0
-rwxrwxrwx 1 kali kali 0 Apr 11 01:56 testfile.txt

(kali@kali)-[~/PermissionTest]
$
```

### Step 3: Revert Permissions

Revert the permissions to 644 (owner can read/write, group and others can read): **chmod 644 testfile.txt**

Check permissions again: **ls -l**

```
(kali@kali)-[~/PermissionTest]
$ chmod 644 testfile.txt

(kali@kali)-[~/PermissionTest]
$ ls -l
total 0
-rw-r--r-- 1 kali kali 0 Apr 11 01:56 testfile.txt
```

## Exercise 1: Experiment with Permissions

### Part 3: Changing Ownership

#### Step 4: Change File Ownership

Create a new user for testing (this may require sudo privileges): **sudo adduser testuser**

Change the ownership of testfile.txt to testuser: **sudo chown testuser:testuser testfile.txt**

Verify ownership: **ls -l**

```
File Actions Edit View Help lab4.md

(kali㉿kali)-[~/PermissionTest]
$ sudo adduser testuser

[sudo] password for kali:
fatal: The user `testuser' already exists.

(kali㉿kali)-[~/PermissionTest]
$ sudo chown testuser:testuser testfile.txt

(kali㉿kali)-[~/PermissionTest]
$ ls -l
total 0
-rwxrwxrwx 1 testuser testuser 0 Apr 11 01:56 testfile.txt

(kali㉿kali)-[~/PermissionTest]
$ cat testfile.txt
```

## Exercise 2: Group Ownership

Change the group ownership of testfile.txt to another group (e.g., staff): **sudo chgrp staff testfile.txt**

```
kali@kali: ~/PermissionTest
File Actions Edit View Help lab4.md

(kali㉿kali)-[~/PermissionTest]
$ sudo chgrp staff testfile.txt

(kali㉿kali)-[~/PermissionTest]
$ ls -l
total 0
-rwxrwxrwx 1 testuser staff 0 Apr 11 01:56 testfile.txt

(kali㉿kali)-[~/PermissionTest]
$
```

## Part 4: Practical Exercises

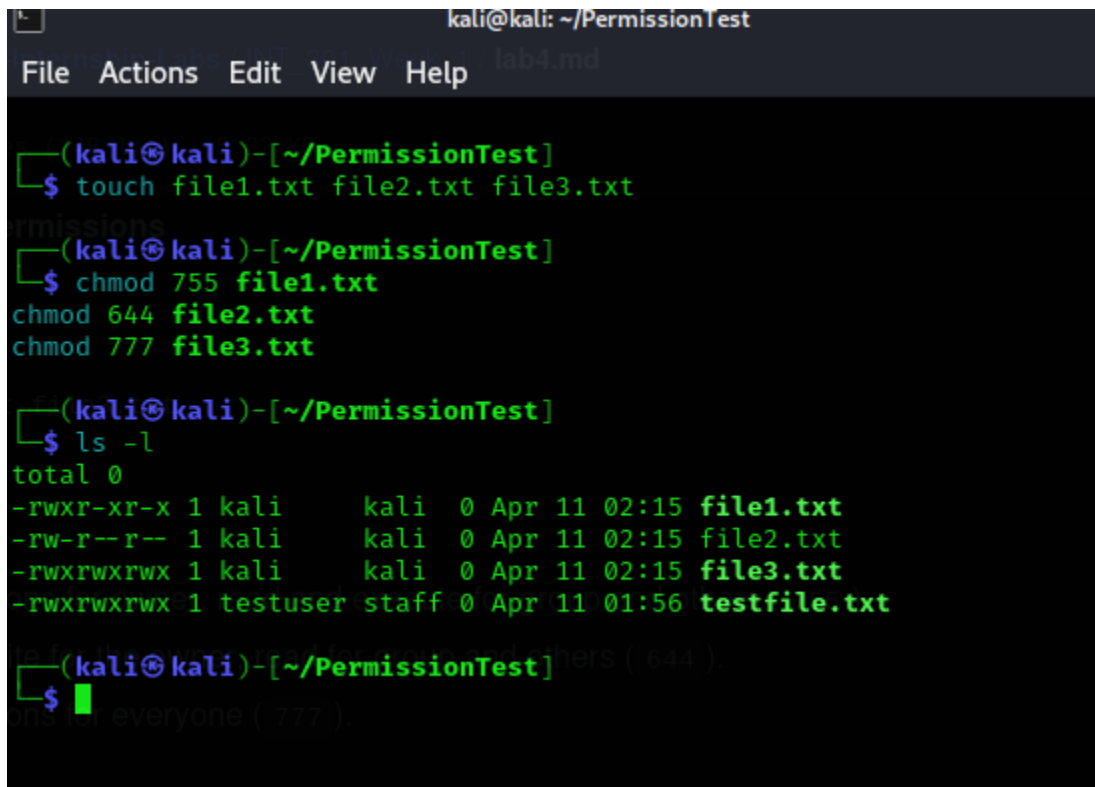
### Exercise 3: Create and Modify Permissions

- Create three new files:

```
touch file1.txt file2.txt file3.txt
```

Set permissions as follows:

- file1.txt: Full permissions for owner, read and execute for group and others (755).
- file2.txt: Read and write for the owner, read for group and others (644).
- file3.txt: Full permissions for everyone (777).



```
kali@kali: ~/PermissionTest
File Actions Edit View Help lab4.md

(kali@kali)-[~/PermissionTest]
$ touch file1.txt file2.txt file3.txt

(kali@kali)-[~/PermissionTest]
$ chmod 755 file1.txt
chmod 644 file2.txt
chmod 777 file3.txt

(kali@kali)-[~/PermissionTest]
$ ls -l
total 0
-rwxr-xr-x 1 kali      kali   0 Apr 11 02:15 file1.txt
-rw-r--r-- 1 kali      kali   0 Apr 11 02:15 file2.txt
-rwxrwxrwx 1 kali      kali   0 Apr 11 02:15 file3.txt
-rwxrwxrwx 1 testuser staff 0 Apr 11 01:56 testfile.txt

(kali@kali)-[~/PermissionTest]
$
```

### Lab 5: Individual Research on Linux

Linux distributions are operating systems built upon the Linux kernel and include various software packages, applications, and tools. They are developed by communities and businesses, and examples include Debian, Ubuntu, Fedora, and Red Hat Enterprise Linux. Linux distributions come in various flavors, including desktop distributions with GUI environments like GNOME or KDE Plasma, and server distributions with a command-line interface, [according to Zenarmor](#).

#### Popular Linux Distributions:



- 

### **Ubuntu:**

A popular desktop and server distribution known for its user-friendly interface and extensive community support.



- **debian**

### **Debian:**

A stable and widely used distribution known for its strict adherence to free software principles and extensive software repository.



- 

### **Fedora:**

A distribution sponsored by Red Hat, often used as a testing ground for new features in Red Hat Enterprise Linux.



- 

### **Linux Mint:**

A community-driven distribution based on Ubuntu, offering a user-friendly experience and excellent hardware support.



-

### **Red Hat Enterprise Linux:**

A commercial distribution known for its reliability and enterprise-grade features.



### **CentOS:**

A community-driven distribution based on Red Hat Enterprise Linux, offering a free alternative.



### **Manjaro:**

A distribution based on Arch Linux, known for its rolling release model and user-friendly installation process.

- **Arch Linux:**

A distribution designed for experienced Linux users, offering a high degree of customization but requiring more technical knowledge.



### **Kali Linux:**

A Linux distribution specialized for penetration testing and security auditing.



### **Elementary OS:**

A distribution based on Ubuntu, designed with usability and a minimalist look in mind.



### **Zorin OS:**

A distribution based on Ubuntu, offering a familiar Windows-like interface for new Linux users.



### **Slackware:**

One of the oldest and most traditional Linux distributions, known for its command-line focus.



### **MX Linux:**

A Debian-based distribution that balances performance and ease of use.



### **Linux Lite:**

A lightweight distribution based on Ubuntu LTS, designed for older hardware.



### **Lubuntu:**

A lightweight distribution based on Ubuntu and LXQT, offering a minimal resource footprint.

Key Features of Linux Distributions:

- **Customization:**

Many distributions offer a wide range of customization options, allowing users to tailor their operating system to their needs.

- **Community Support:**

Strong community support is a hallmark of many Linux distributions, providing users with resources and assistance.

- **Free and Open-Source Software:**

Linux distributions are typically based on free and open-source software, meaning they are freely distributable and can be modified by users.

- **Variety of Desktop Environments:**

Distributions often come with a variety of desktop environments, such as GNOME, KDE Plasma, XFCE, and others, offering different user interfaces.

- **Security and Privacy:**

Some distributions prioritize security and privacy, offering features like built-in drive encryption and robust authentication.

Choosing a Linux Distribution:

When selecting a Linux distribution, consider factors like:

- **Your technical expertise:**

Some distributions are easier to install and use than others, catering to beginners and experienced users alike.

- **Your hardware:**

Some distributions are designed for older hardware, while others are optimized for newer systems.

- **Your software needs:**

Determine which software you need to use and whether the distribution supports it.

- **Your preferences:**

Consider factors like desktop environment, customization options, and community support when choosing a distribution.

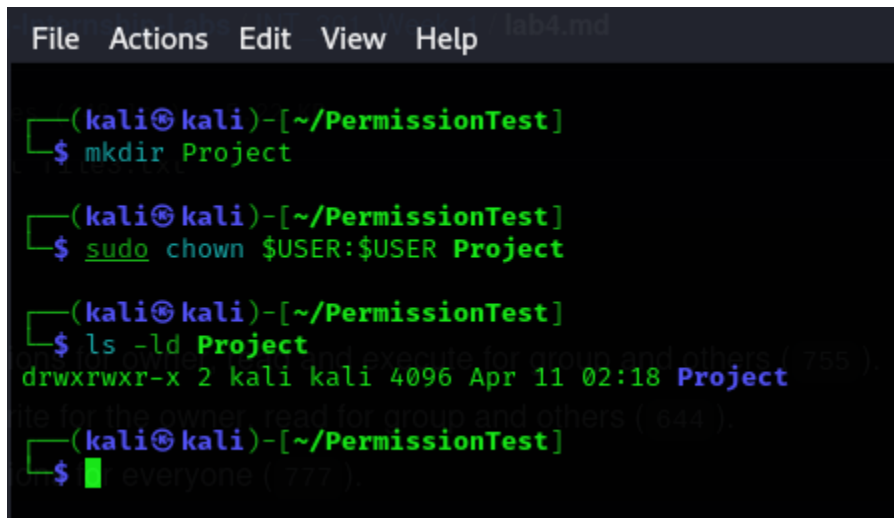
#### **Exercise 4: Ownership Challenge**

Create a directory named Project and set your current user as the owner:

**mkdir Project**

**sudo chown \$USER:\$USER Project**

Verify the ownership: **ls -ld Project**



```
File Actions Edit View Help lab4.md
(kali㉿kali)-[~/PermissionTest]
$ mkdir Project
(kali㉿kali)-[~/PermissionTest]
$ sudo chown $USER:$USER Project
(kali㉿kali)-[~/PermissionTest]
$ ls -ld Project
drwxrwxr-x 2 kali kali 4096 Apr 11 02:18 Project
(kali㉿kali)-[~/PermissionTest]
$
```