

# Lab 1: Investigate Kali Linux

## Objectives

In this lab, you will complete the following objectives:

- Familiarize yourself with the Kali Linux GUI.
- Familiarize yourself with the Kali Linux shell.
- Understand basic file and directory operations.
- Learn about file permissions and how to manipulate them.

## Background / Scenario

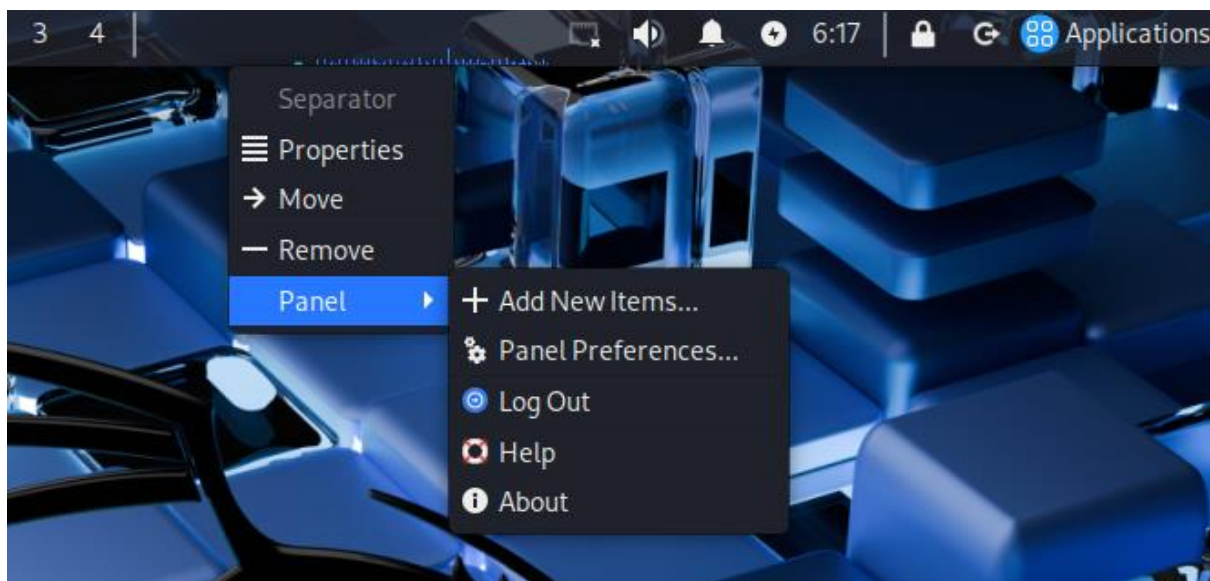
Linux is an open-source operating system known for its speed, reliability, and efficiency. It can run on minimal hardware resources and is highly customizable. Unlike proprietary systems like Windows and Mac OS X, Linux is maintained by a community of developers, making it adaptable for various applications,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

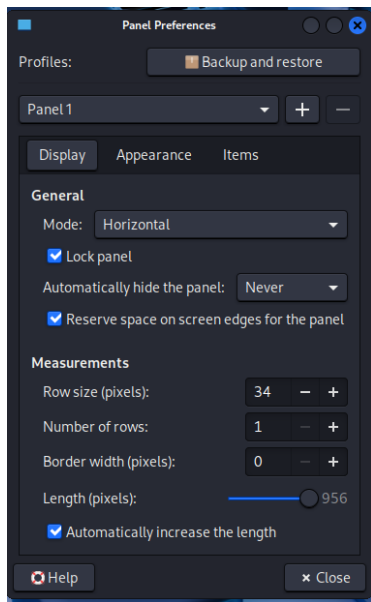
## Required Resources

- Kali Linux virtual machine (VM) customized for Internship Training course.
- Internet access.

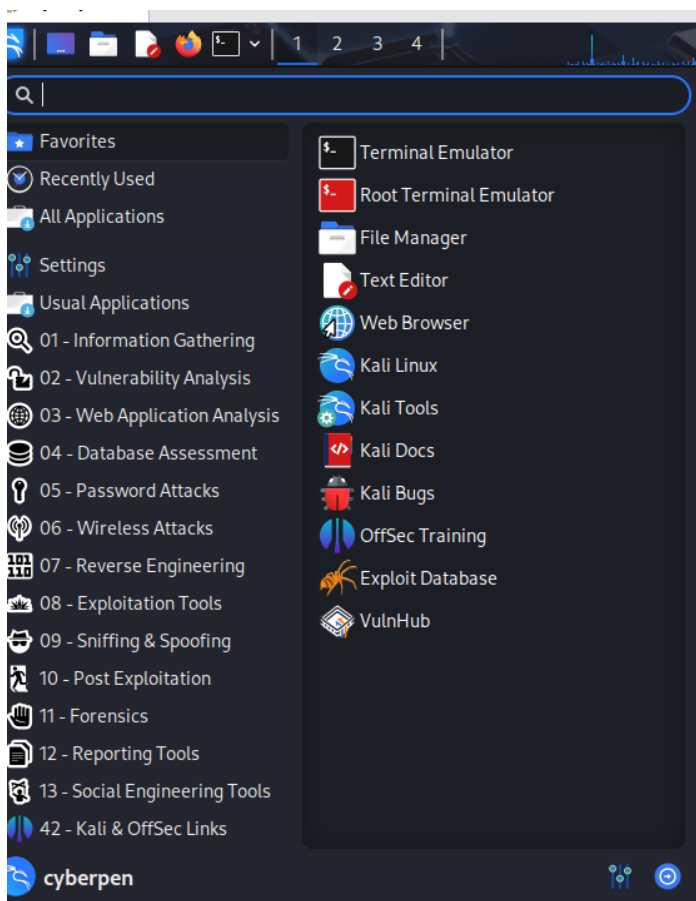
## Part 1: Familiarize Yourself with the Kali Linux GUI



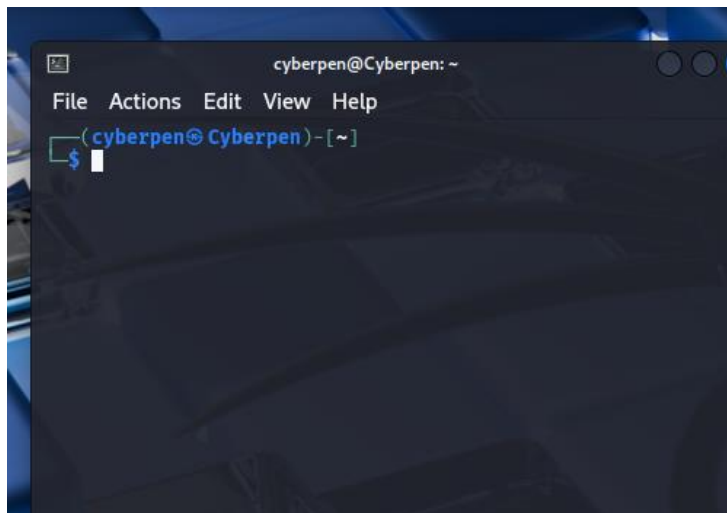
*Outlook Of The panel*



## Panel Preference



## Application Menu



A Terminal

## Part 2: Familiarize Yourself with the Kali Linux Shell

### Step 1: Command Documentation

#### 1. Learning About the man page

```
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 p
  ro-
  vided, 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.

  1 Executable programs or shell commands
  2 System calls (functions provided by the kernel)
  3 Library calls (functions within program libraries)
  4 Special files (usually found in /dev)
  5 File formats and conventions, e.g. /etc/passwd
  6 Games
  7 Miscellaneous (including macro packages and conventions), e.g. man(7), groff(7), man-pages(7)
  8 System administration commands (usually only for root)
  9 Kernel routines [Non standard]

  A manual page consists of several sections.

  Conventional section names include NAME, SYNOPSIS, CONFIGURATION, DESCRIPTION, OPTIONS, EXIT STATUS, RETURN V
  ALUE, ERRORS, ENVIRONMENT, FILES, VERSIONS, STANDARDS, NOTES, BUGS, EXAMPLE, AUTHORS, and SEE ALSO.

  The following conventions apply to the SYNOPSIS section and can be used as a guide in other sections.

  bold text      type exactly as shown.
  italic text    replace with appropriate argument.
  [-abc]         any or all arguments within [ ] are optional.
  -a|-b          options delimited by | cannot be used together.

Manual page man(1) line 1 (press h for help or q to quit)
```

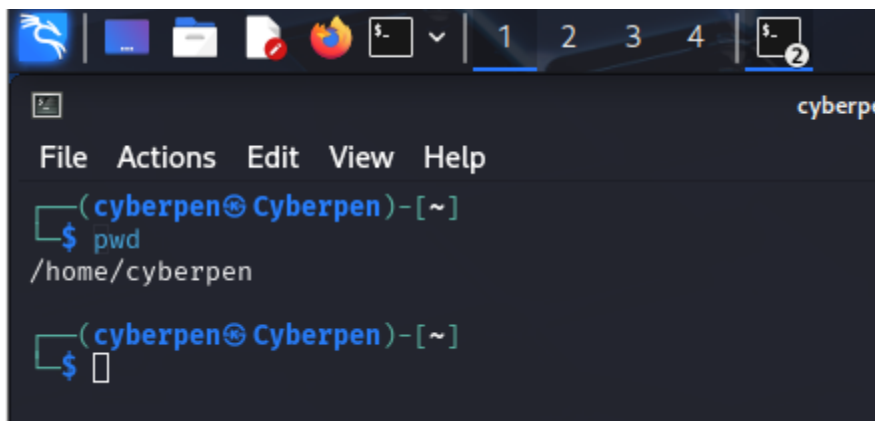
Displaying the man page using the man man command

Some sections in the man page are:

- Synopsis
- Description
- Examples
- Overview
- Default
- Option
- Getting Help
- Exit Status
- Environment

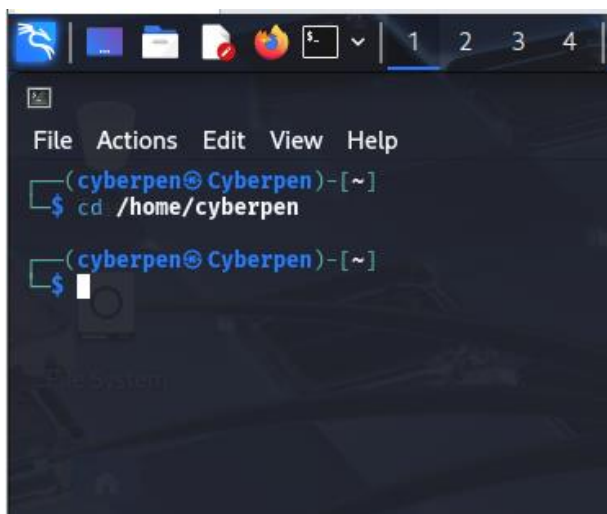
## Step 2: Create and Change Directory

1. The current working directory is “/home/cyberpen



A terminal window with a dark background and a menu bar (File, Actions, Edit, View, Help). The prompt is `(cyberpen@Cyberpen)-[~]`. The user enters `$ pwd` and the output is `/home/cyberpen`. The prompt then returns to `(cyberpen@Cyberpen)-[~]` with a cursor.

2. `cd /home/cyberpen`



A terminal window with a dark background and a menu bar (File, Actions, Edit, View, Help). The prompt is `(cyberpen@Cyberpen)-[~]`. The user enters `$ cd /home/cyberpen`. The prompt then returns to `(cyberpen@Cyberpen)-[~]` with a cursor.

3. List the files in the Current Directory using the command: `ls -l`

```
(cyberpen@ Cyberpen)-[~]
$ ls -l
total 265696
drwxrwxr-x 4 cyberpen cyberpen 4096 Mar 31 04:45 2025-03-31-ZAP-Report-
-rw-rw-r-- 1 cyberpen cyberpen 159998 Mar 31 06:44 2025-03-31-ZAP-Report-.html
drwxrwxr-x 4 cyberpen cyberpen 4096 Mar 31 04:45 2025-03-31-ZAP-Report-2
drwxrwxr-x 4 cyberpen cyberpen 4096 Mar 31 04:45 2025-03-31-ZAP-Report-3
drwxrwxr-x 4 cyberpen cyberpen 4096 Mar 31 04:45 2025-03-31-ZAP-Report-4
drwxrwxr-x 4 cyberpen cyberpen 4096 Mar 31 04:45 2025-03-31-ZAP-Report-5
drwxrwxr-x 4 cyberpen cyberpen 4096 Mar 31 04:45 2025-03-31-ZAP-Report-6
drwxr-xr-x 2 cyberpen cyberpen 4096 Dec 27 07:54 Desktop
drwxr-xr-x 2 cyberpen cyberpen 4096 Dec 27 07:54 Documents
drwxr-xr-x 2 cyberpen cyberpen 4096 Mar 31 06:39 Downloads
drwxr-xr-x 2 cyberpen cyberpen 4096 Dec 27 07:54 Music
drwxr-xr-x 2 cyberpen cyberpen 4096 Dec 27 07:54 Pictures
drwxr-xr-x 2 cyberpen cyberpen 4096 Dec 27 07:54 Public
drwxr-xr-x 2 cyberpen cyberpen 4096 Dec 27 07:54 Templates
drwxr-xr-x 2 cyberpen cyberpen 4096 Dec 27 07:54 Videos
-rwxrwxr-x 1 cyberpen cyberpen 237450190 Mar 25 18:47 ZAP_2_16_1_unix.sh
-rw-rw-r-- 1 cyberpen cyberpen 180194 Mar 31 04:25 latest
-rw-rw-r-- 1 cyberpen cyberpen 184 Mar 31 05:47 testphp.session
-rw-rw-r-- 1 cyberpen cyberpen 50331648 Mar 31 06:45 testphp.session.data
-rw-rw-r-- 1 cyberpen cyberpen 104 Mar 31 06:45 testphp.session.properties
-rw-rw-r-- 1 cyberpen cyberpen 12233 Mar 31 06:45 testphp.session.script
(cyberpen@ Cyberpen)-[~]
$
```

4. Create a New Directory using the command: `mkdir Test`

```
(cyberpen@ Cyberpen)-[~]
$ mkdir Test

(cyberpen@ Cyberpen)-[~]
$
```

5. Verify the Directory Creation using the command: `ls`

```
(cyberpen@ Cyberpen)-[~]
$ ls
2025-03-31-ZAP-Report-  2025-03-31-ZAP-Report-5  Music  Videos  testphp.session.properties
2025-03-31-ZAP-Report-.html  2025-03-31-ZAP-Report-6  Pictures  ZAP_2_16_1_unix.sh  testphp.session.script
2025-03-31-ZAP-Report-2  Desktop  Public  latest
2025-03-31-ZAP-Report-3  Documents  Templates  testphp.session
2025-03-31-ZAP-Report-4  Downloads  Test  testphp.session.data
(cyberpen@ Cyberpen)-[~]
$
```

6. Remove the Directory using the command: `rmdir Test`

```
(cyberpen@ Cyberpen)-[~]
$ rmdir Test

(cyberpen@ Cyberpen)-[~]
$
```

7. Verify the Directory Removal using the command: ls

```
(cyberpen@Cyberpen)-[~]
$ ls
2025-03-31-ZAP-Report-      2025-03-31-ZAP-Report-6  Public      testphp.session.data
2025-03-31-ZAP-Report-.html Desktop      Templates   testphp.session.properties
2025-03-31-ZAP-Report-2    Documents     Videos     testphp.session.script
2025-03-31-ZAP-Report-3    Downloads    ZAP_2_16_1_unix.sh
2025-03-31-ZAP-Report-4    Music        latest
2025-03-31-ZAP-Report-5    Pictures     testphp.session
```

## Part 3: Copying and Moving Files

1. copy a File using the command: cp

```
(cyberpen@Cyberpen)-[~]
$ touch gvm_admin_passwd.txt

(cyberpen@Cyberpen)-[~]
$ ls
2025-03-31-ZAP-Report-      2025-03-31-ZAP-Report-5  Music        ZAP_2_16_1_unix.sh  testphp.session.properties
2025-03-31-ZAP-Report-.html 2025-03-31-ZAP-Report-6  Pictures     gvm_admin_passwd.txt testphp.session.script
2025-03-31-ZAP-Report-2    Desktop                  Public       latest
2025-03-31-ZAP-Report-3    Documents                Templates   testphp.session
2025-03-31-ZAP-Report-4    Downloads                Videos     testphp.session.data

(cyberpen@Cyberpen)-[~]
$ cp gvm_admin_passwd.txt backup_gvm_passwd.txt
```

2. Verify the Copy using the command: ls

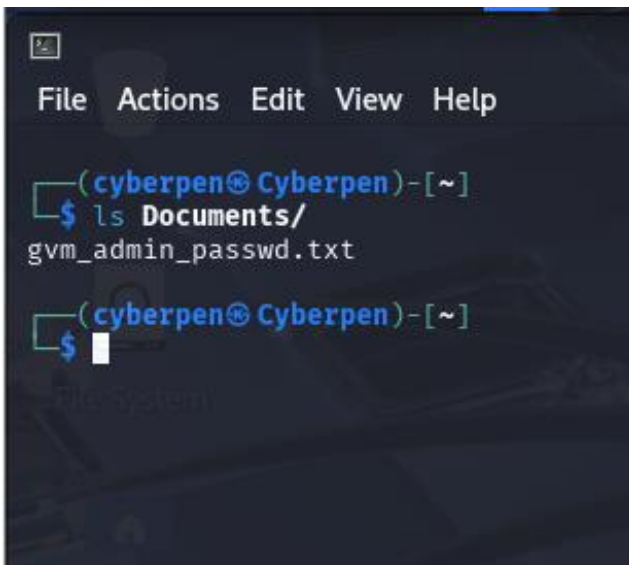
```
cyberpen@Cyberpen: ~
File Actions Edit View Help
(cyberpen@Cyberpen)-[~]
$ ls
2025-03-31-ZAP-Report-      2025-03-31-ZAP-Report-5  Music        ZAP_2_16_1_unix.sh  testphp.session.data
2025-03-31-ZAP-Report-.html 2025-03-31-ZAP-Report-6  Pictures     backup_gvm_passwd.txt testphp.session.properties
2025-03-31-ZAP-Report-2    Desktop                  Public       gvm_admin_passwd.txt testphp.session.script
2025-03-31-ZAP-Report-3    Documents                Templates   latest
2025-03-31-ZAP-Report-4    Downloads                Videos     testphp.session
```

3. Move a File using the command: mv

A terminal window with a dark background. The prompt is (cyberpen@Cyberpen)-[~]. The command mv gvm\_admin\_passwd.txt Documents/ is entered and executed. The prompt returns to (cyberpen@Cyberpen)-[~].

```
(cyberpen@Cyberpen)-[~]  
$ mv gvm_admin_passwd.txt Documents/  
  
(cyberpen@Cyberpen)-[~]  
$
```

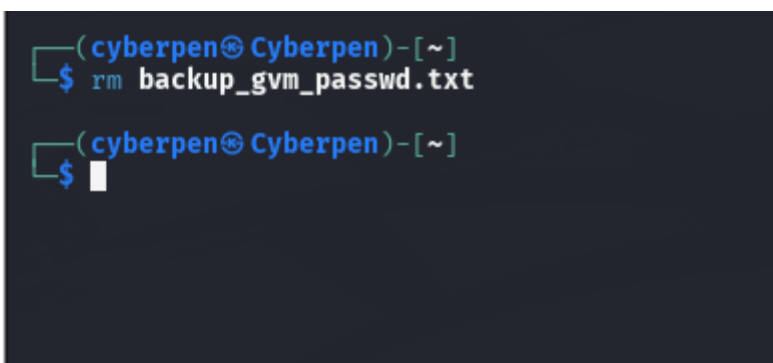
4. Verify the move using the command: ls Documents/

A terminal window with a dark background. The prompt is (cyberpen@Cyberpen)-[~]. The command ls Documents/ is entered and executed, showing gvm\_admin\_passwd.txt. The prompt returns to (cyberpen@Cyberpen)-[~].

```
(cyberpen@Cyberpen)-[~]  
$ ls Documents/  
gvm_admin_passwd.txt  
  
(cyberpen@Cyberpen)-[~]  
$
```

## Part 4: Deleting Files

1. Delete a File using the command: rm backup\_gvm\_passwd.txt

A terminal window with a dark background. The prompt is (cyberpen@Cyberpen)-[~]. The command rm backup\_gvm\_passwd.txt is entered and executed. The prompt returns to (cyberpen@Cyberpen)-[~].

```
(cyberpen@Cyberpen)-[~]  
$ rm backup_gvm_passwd.txt  
  
(cyberpen@Cyberpen)-[~]  
$
```

2. Verify Deletion using the command: ls

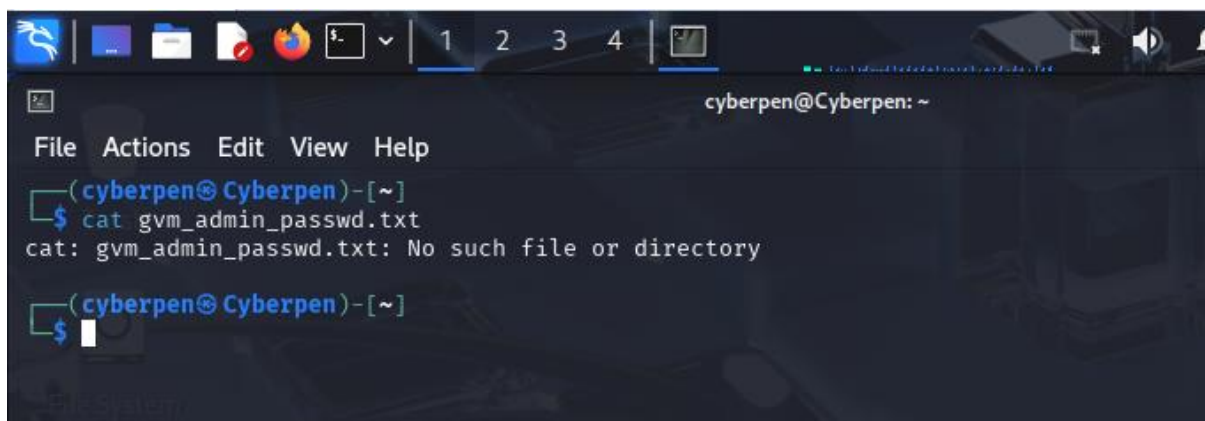
```
(cyberpen@Cyberpen)-[~]
$ rm backup_gvm_passwd.txt

(cyberpen@Cyberpen)-[~]
$ ls
2025-03-31-ZAP-Report-2025-03-31-ZAP-Report-6 Public testphp.session.data
2025-03-31-ZAP-Report-.html Desktop Templates testphp.session.properties
2025-03-31-ZAP-Report-2 Documents Downloads ZAP_2_16_1_unix.sh testphp.session.script
2025-03-31-ZAP-Report-3 Music Pictures latest
2025-03-31-ZAP-Report-4 testphp.session
2025-03-31-ZAP-Report-5

(cyberpen@Cyberpen)-[~]
$
```

## Part 5: Viewing File Content

1. View File Contents using the command: cat gvm\_admin\_passwd.txt  
Result says no such file because the file has already been removed



```
cyberpen@Cyberpen: ~
File Actions Edit View Help

(cyberpen@Cyberpen)-[~]
$ cat gvm_admin_passwd.txt
cat: gvm_admin_passwd.txt: No such file or directory

(cyberpen@Cyberpen)-[~]
$
```

Using the command “cat” to view the content of the file “testphp.session.data”

```
(cyberpen@Cyberpen)-[~]
$ cat testphp.session.data
@7[[]j♦♦Default Context♦♦true♦
Db♦
Db.CouchDB♦
Db.Firebird♦
Db.HypersonicSQL♦
Db.IBM DB2♦
Db.MariaDB♦
Db.Microsoft Access♦
Db.Microsoft SQL Server♦
b.MongoDB♦
b.MySQL♦
b.PostgreSQL♦/?/?/?
Db.SAP MaxDB♦### Db.SQLite♦!%'!%'!%' Db.Sybase♦##Language♦#/#/#/#/ Language.ASP♦+++
Language.Java♦'7'7'7[[]Language.Java.Spring♦333Language.JavaScript♦157157157[[] Language.PHP♦333language.Python♦3;/3;/3;/
Language.Ruby♦;;; Language.XML♦9=79=79=705♦;; OS.Linux♦000OS.MacOS♦CCC! WS.Apache♦KKK'WS.IIS♦G_?G_?Gc?( WS.
OS.Windows♦AEGAEGAEG"SCM♦CCC#SCM.Git♦CKOCKOCKO$SCM.SVN♦KKK%WS+IMGIMIMG6 Tomcat♦SSG)♦-org.zaproxy.zap.model.StandardParameterParser♦QUWQUWgUc♦*{"kvps":"6","kvs":"=","struct":[]}}♦SSWS♦-or
```

2. Paginated Viewing using the command: `less gvm_admin_passwd.txt`  
Result says no such file because the file has already been removed

```
(cyberpen@Cyberpen)-[~]
$ less gvm_admin_passwd.txt~
gvm_admin_passwd.txt~: No such file or directory

(cyberpen@Cyberpen)-[~]
$
```

Paginated Viewing of the “testphp.session.data”

```
testphp.session.data
B7'Za
Default Context
Db.CouchDB
Db.Firebird
Db.HypersonicSQL
Db.IBM DB2
Db.MariaDB
Db.Microsoft Access
Db.Microsoft SQL Server
Db.MongoDB
Db.MySQL
Db.Oracle
Db.PostgreSQL
Db.SAP MaxDB
Db.SQLite
Db.Sybase
HLanguage
LLanguage.ASP
```

## Conclusion

Navigating the Kali Linux file system is essential for effective system management. By mastering basic commands such as `cd`, `ls`, `mkdir`, `cp`, `mv`, `rm`, and `cat`, you can efficiently manage files and directories in your environment. Understanding the GUI and the shell will enhance your ability to perform tasks in Kali Linux.

# Lab 2: Installing Packages and Applications

## Objectives

In this lab, you will:

- Use the Advanced Package Tool (APT) to manage packages in Kali Linux.
- Install, upgrade, and remove applications using command-line tools.
- Search for packages and manage repositories.

## Background / Scenario

Kali Linux, built on Debian, utilizes the APT package management system, which simplifies the process of installing, upgrading, and managing software packages. Understanding how to use APT is essential for maintaining a functional and secure environment, particularly in cybersecurity roles.

## Required Resources

- Kali Linux virtual machine (VM).
- Internet access.

## Part 1: Updating Package Lists

```
File Actions Edit View Help
(cyberpen@Cyberpen)-[~]
$ sudo apt update
[sudo] password for cyberpen:
Ign:1 http://http.kali.org/kali kali-rolling InRelease
Ign:1 http://http.kali.org/kali kali-rolling InRelease
Ign:1 http://http.kali.org/kali kali-rolling InRelease
Err:1 http://http.kali.org/kali kali-rolling InRelease
      Temporary failure resolving 'http.kali.org'
57 packages can be upgraded. Run 'apt list --upgradable' to see them.
Warning: Failed to fetch http://http.kali.org/kali/dists/kali-rolling/InRelease Temporary failure resolving 'http.kali.org'
Warning: Some index files failed to download. They have been ignored, or old ones used instead.
```

## Part 2: Installing Packages

```
(cyberpen@Cyberpen)-[~]
$ sudo apt install curl
curl is already the newest version (8.13.0-rc2-2).
curl set to manually installed.
The following packages were automatically installed and are no longer required:
crackmapexec          libbfgsb0             libqt5multimediasstools5  openfortivpn
cython3               libblvm14             libqt5multimediawidgets5  openjdk-17-jre
firebird3.0-common   liblqr-1-0            libqt5sensors5            openjdk-17-jre-headless
firebird3.0-common-doc  liblua5.2-0          libqt5webkit5             perl-modules-5.36
fonts-liberation2     libmagickcore-6.q16-7  libqt5xmlextras5         python3-all-dev
libapt-pkg6.0t64      libmagickwand-6.q16-7  librpm9                  python3-beniget
libarmadillo12        libmbedcrypto7        librpmio9                 python3-gast
libassuan0            libmfx1               librpmjsm9               python3-gpg
libboost-dev          libndctl6             libsuperlu6              python3-jose
libcores2             libnetcdf19           libtag1v5                python3-lib2to3
libclang-cpp14        libnghttp3-3          libtag1v5-vanilla        python3-llvmlite
libconfig++9v5        libnsl-dev            libtagc0                 python3-pyrsistent
libconfig9           libopenblas-dev       libtirpc-dev             python3-pythran
libdaxctl1            libopenblas-pthread-dev  libuccl1                python3-requests-toolbelt
libdirectfb-1.7-7     libopenblas0          libusbmuxd6              python3-rsa
libebur128-1          libpaper1             libwebkit2gtk-4.0-37     python3.11
libflac12             libperl5.36           libwireless17            python3.11-dev
libgdal34             libplist3             libwiretap14            python3.11-minimal
libgeos3.12.1         libpmem1              libwpe-1.0-1            python3.12-dev
libglapi-mesa         libpoppler126         libwpebackend-fdo-1.0-1  ruby3.1
libgumbo2             libpthread-stubs0-dev  libwsutil15             ruby3.1-dev
libhdf5-103-1         libpython3-all-dev    libxsimd-dev            ruby3.1-doc
```

Verify The Installation using the command: curl --version

```
(cyberpen@Cyberpen)-[~]
$ curl --version
curl 8.13.0-rc2 (x86_64-pc-linux-gnu) libcurl/8.13.0-rc2 GnuTLS/3.8.9 zlib/1.3.1 brotli/1.1.0 zstd/1.5.6 libidn2/2.
3.8 libpsl/0.21.2 libssh2/1.11.1 nghttp2/1.64.0 ngtcp2/1.11.0 nghttp3/1.8.0 librtmp/2.3 OpenLDAP/2.6.9
Release-Date: 2025-03-17, security patched: 8.13.0-rc2-2
Protocols: dict file ftp ftps gopher gophers http https imap imaps ipfs ipns ldap ldaps mqtt pop3 pop3s rtsp rtp s
cp sftp smb smbs smtp smtps telnet tftp ws wss
Features: alt-svc AsynchDNS brotli GSS-API HSTS HTTP2 HTTP3 HTTPS-proxy IDN IPv6 Kerberos Largefile libz NTLM PSL S
PNEGO SSL threadsafe TLS-SRP UnixSockets zstd
```

## Part 3: Upgrading packages

1. Upgrade All Installed Packages using the command: sudo apt upgrade

```
(cyberpen@Cyberpen)-[~]
$ sudo apt upgrade
[sudo] password for cyberpen:
The following packages were automatically installed and are no longer required:
crackmapexec liblbfgsb0 libqt5multimedia5gsttools5 openfortivpn
cython3 libllvm14 libqt5multimediawidgets5 openjdk-17-jre
firebird3.0-common liblqr-1-0 libqt5sensors5 openjdk-17-jre-headl
firebird3.0-common-doc liblua5.2-0 libqt5webkit5 p7zip
fonts-liberation2 libmagickcore-6.q16-7 libqt5x11extras5 perl-modules-5.36
libapt-pkg6.0t64 libmagickcore-6.q16-7-extra librpm9 python3-all-dev
libarmadillo12 libmagickwand-6.q16-7 librpmbuild9 python3-beniget
libassuan0 libmbedcrypto7 librpmio9 python3-gast
libboost-dev libmfx1 librpmjs9 python3-gpg
libc-ares2 libndctl6 libsuperlu6 python3-jose
libcapstone4 libnetcdf19 libtag1v5 python3-lib2to3
libclang-cpp14 libnghttp3-3 libtag1v5-vanilla python3-llvmlite
libconfig++9v5 libnsd-dev libtagc0 python3-pyrsistent
libconfig9 libopenblas-dev libtirpc-dev python3-pythran
libdaxctl1 libopenblas-pthread-dev libuc1 python3-requests-too
libdirectfb-1.7-7 libopenblas0 libusbmuxd6 python3-rsa
libebur128-1 libpaper1 libwebkit2gtk-4.0-37 python3.11
libflac12 libperl5.36 libwireshark17 python3.11-dev
libgdal34 libplist3 libwireshark17 python3.11-minimal
libgeos3.12.1 libpmem1 libwpe-1.0-1 python3.12-dev
libglapi-mesa libpoppler126 libwpebackend-fdo-1.0-1 ruby3.1
libgumbo2 libpthread-stubs0-dev libwsutil15 ruby3.1-dev
libhdf5-103-1 libpython3-all-dev libxsimd-dev ruby3.1-doc
libhdf5-hl-100 libpython3.11 libzip4 samba-ad-provision
libhiredis0.14 libpython3.11-dev libzxing2 samba-dsdb-modules
libimobiledevice6 libpython3.11-minimal llvm-14 samba-vfs-modules
libiniparser1 libpython3.11-stdlib llvm-14-dev strongswan
libjavascriptcoregtk-4.0-18 libpython3.12-dev llvm-14-linker-tools xtl-dev
libjim0.82 libpython3.12t64 llvm-14-runtime
libjxr-tools libqt5multimedia5 llvm-14-tools
libkate1 libqt5multimedia5-plugins numba-doc
```

## 2. Review Upgrade Messages:

```
Not upgrading:
cadaver          kali-desktop-xfce      libpocl2-common      pkexec
cherrytree       libblockdev-fs3        libpolkit-agent-1-0  pocl-opencl-icd
curlftpfs        libblockdev-nvme3      libpolkit-gobject-1-0 polkitd
e2fsprogs        libboost-dev           libspa-0.2-bluetooth python3-pypsrp
efibootmgr       libfluidsynth3         libspa-0.2-modules   python3-requests-ntlm
exiv2            libgail-common         libzmq5              strongswan
gparted          libgdata22             light-locker         testdisk
gparted-common  libgtk2.0-bin          ntfs-3g              theharvester
graphicsmagick   libgtk2.0-common       open-vm-tools        wireless-tools
grub-common      libgtksourceviewmm-3.0-0v5 open-vm-tools-desktop wireplumber
grub-efi-amd64   libjxr-tools           openvpn              xdg-desktop-portal
grub-efi-amd64-bin libmongocrypt0         parted              zerofree
grub2-common     libopenconnect5        pipewire
gstreamer1.0-libav libpipewire-0.3-modules pipewire-bin
hydra            libpocketsphinx3       pipewire-pulse
```

Summary:  
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 57

(cyberpen@Cyberpen)-[~]  
\$

## Part 4: Removing Packages

### 1. Remove curl using the command: sudo apt remove curl

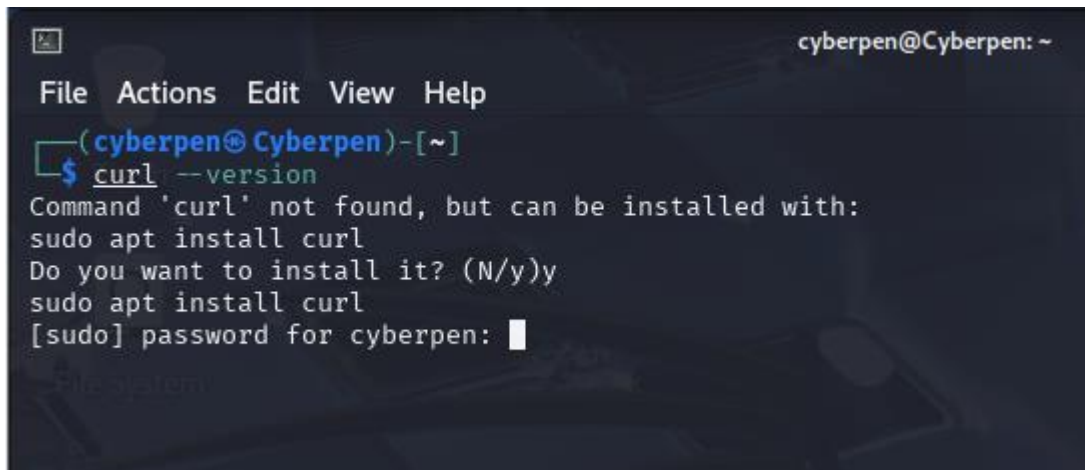
```
REMOVING:
commix  faraday-cli  kali-system-cli  legion  set
curl    kali-linux-default  kali-system-gui  metasploit-framework  unicorn-magic
faraday kali-linux-headless  kali-tools-top10  msfpc    wpscan
```

Summary:  
Upgrading: 0, Installing: 0, Removing: 15, Not Upgrading: 57  
Freed space: 597 MB

Continue? [Y/n] y  
(Reading database ... 464662 files and directories currently installed.)  
Removing kali-linux-default (2025.1.14) ...  
Removing kali-linux-headless (2025.1.14) ...  
Removing commix (4.0-0kali1) ...  
Removing legion (0.4.3-0kali7) ...  
Removing wpscan (3.8.28-0kali1) ...  
Removing unicorn-magic (3.12-0kali3) ...  
Removing faraday-cli (2.1.8-0kali1) ...  
Removing faraday (5.12.0-0kali1) ...  
Removing kali-system-gui (2025.1.14) ...  
Removing kali-system-cli (2025.1.14) ...  
Removing kali-tools-top10 (2025.1.14) ...  
Removing msfpc (1.4.5-0kali3) ...  
Removing set (8.0.3+git20241021-0kali1) ...  
Removing metasploit-framework (6.4.54-0kali1) ...  
Removing curl (8.13.0~rc2-2) ...  
Processing triggers for man-db (2.13.0-1) ...  
Processing triggers for wordlists (2023.2.0) ...  
Processing triggers for kali-menu (2025.1.1) ...

(cyberpen@Cyberpen)-[~]  
\$

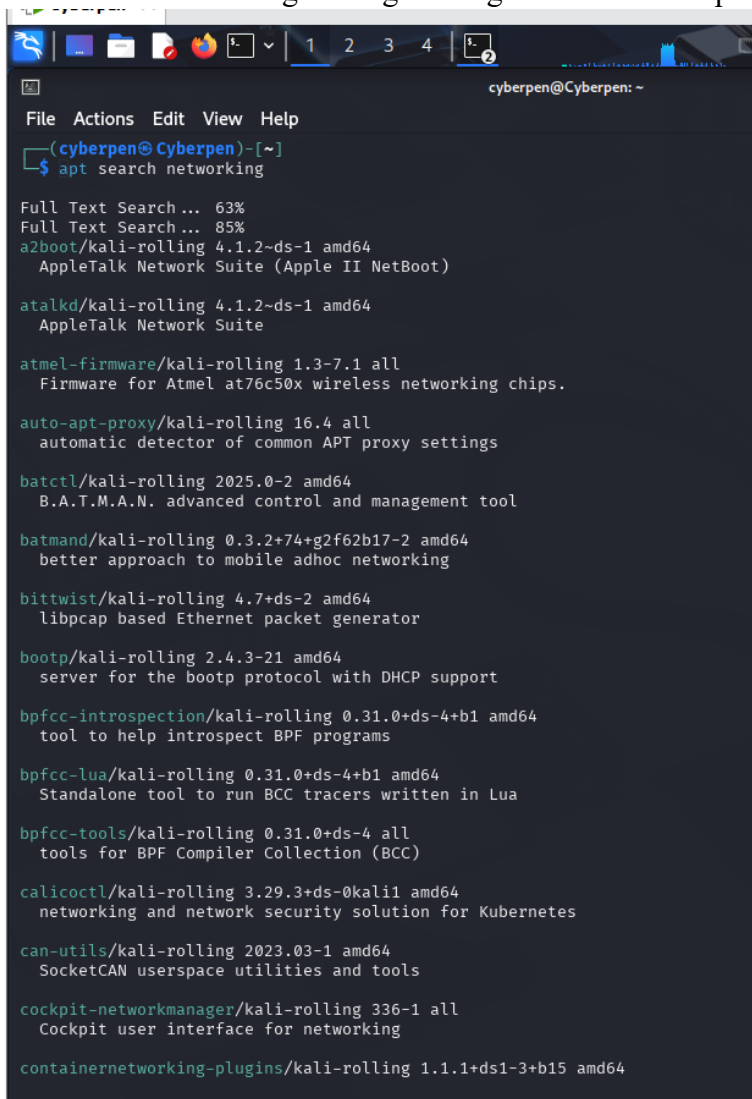
## 2. Confirm Removal:

A terminal window titled 'cyberpen@Cyberpen: ~' with a menu bar (File, Actions, Edit, View, Help). The prompt is '(cyberpen@Cyberpen)-[~]'. The user enters '\$ curl --version'. The terminal output says 'Command 'curl' not found, but can be installed with: sudo apt install curl'. The user enters 'y' to 'Do you want to install it? (N/y)'. The terminal then shows 'sudo apt install curl' and a password prompt '[sudo] password for cyberpen:'.

```
(cyberpen@Cyberpen)-[~]
$ curl --version
Command 'curl' not found, but can be installed with:
sudo apt install curl
Do you want to install it? (N/y)y
sudo apt install curl
[sudo] password for cyberpen: 
```

## Part 5: Searching for Packages

Search for Networking Packages using the command: apt search networking

A terminal window titled 'cyberpen@Cyberpen: ~' with a menu bar (File, Actions, Edit, View, Help). The prompt is '(cyberpen@Cyberpen)-[~]'. The user enters '\$ apt search networking'. The terminal output shows a list of networking-related packages and their descriptions.

```
(cyberpen@Cyberpen)-[~]
$ apt search networking

Full Text Search ... 63%
Full Text Search ... 85%
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 16.4 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

bpfcc-introspection/kali-rolling 0.31.0+ds-4+b1 amd64
  tool to help introspect BPF programs

bpfcc-lua/kali-rolling 0.31.0+ds-4+b1 amd64
  Standalone tool to run BCC tracers written in Lua

bpfcc-tools/kali-rolling 0.31.0+ds-4 all
  tools for BPF Compiler Collection (BCC)

calicoctl/kali-rolling 3.29.3+ds-0kali1 amd64
  networking and network security solution for Kubernetes

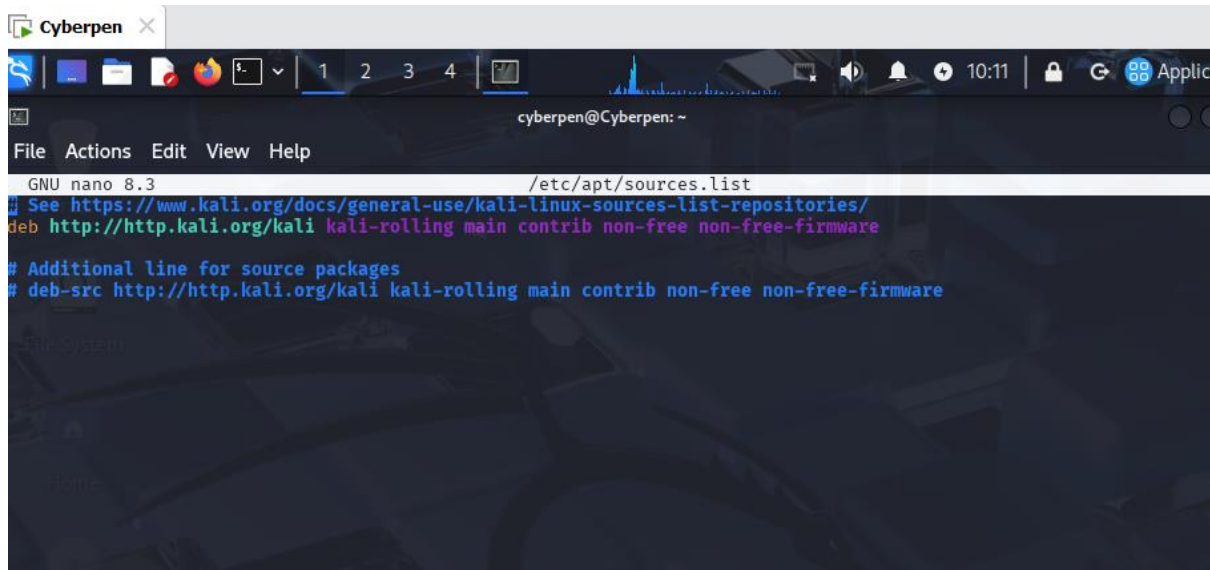
can-utils/kali-rolling 2023.03-1 amd64
  SocketCAN userspace utilities and tools

cockpit-networkmanager/kali-rolling 336-1 all
  Cockpit user interface for networking

containernetworking-plugins/kali-rolling 1.1.1+ds1-3+b15 amd64
```

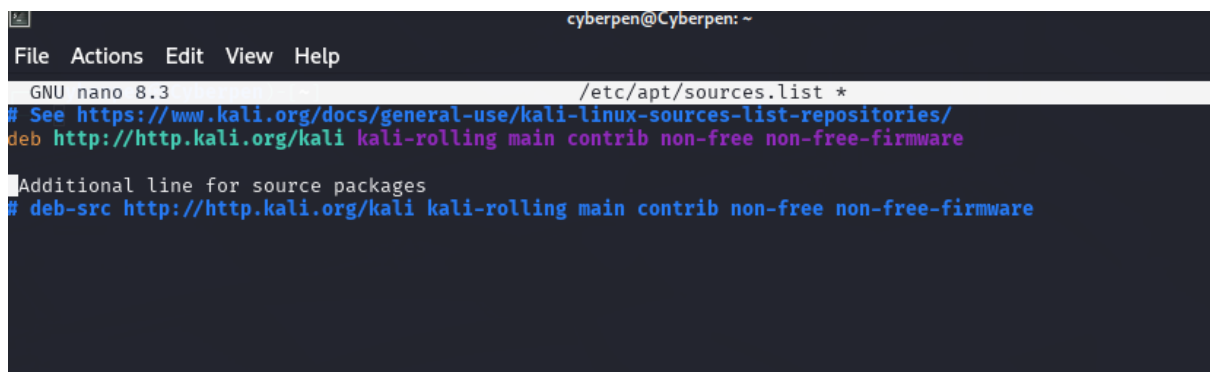
## Part 6: Managing Repositories

1. Edit Repositories using the command: `sudo nano /etc/apt/sources.list`



```
Cyberpen x
[Icons] 1 2 3 4
cyberpen@Cyberpen: ~
File Actions Edit View Help
GNU nano 8.3 /etc/apt/sources.list
# See https://www.kali.org/docs/general-use/kali-linux-sources-list-repositories/
deb http://http.kali.org/kali kali-rolling main contrib non-free non-free-firmware
# Additional line for source packages
# deb-src http://http.kali.org/kali kali-rolling main contrib non-free non-free-firmware
```

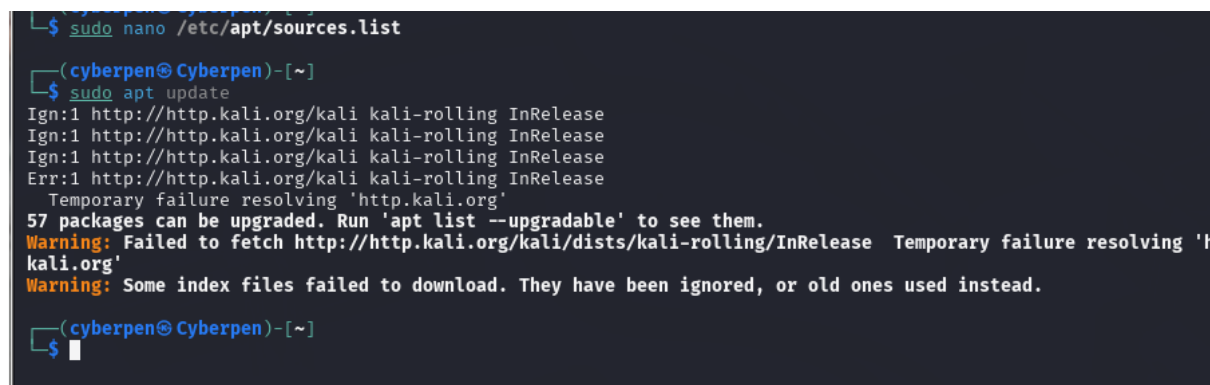
2. Modify Repository Entries: by Uncommenting (remove the #)



```
cyberpen@Cyberpen: ~
File Actions Edit View Help
GNU nano 8.3 /etc/apt/sources.list *
# See https://www.kali.org/docs/general-use/kali-linux-sources-list-repositories/
deb http://http.kali.org/kali kali-rolling main contrib non-free non-free-firmware
Additional line for source packages
# deb-src http://http.kali.org/kali kali-rolling main contrib non-free non-free-firmware
```

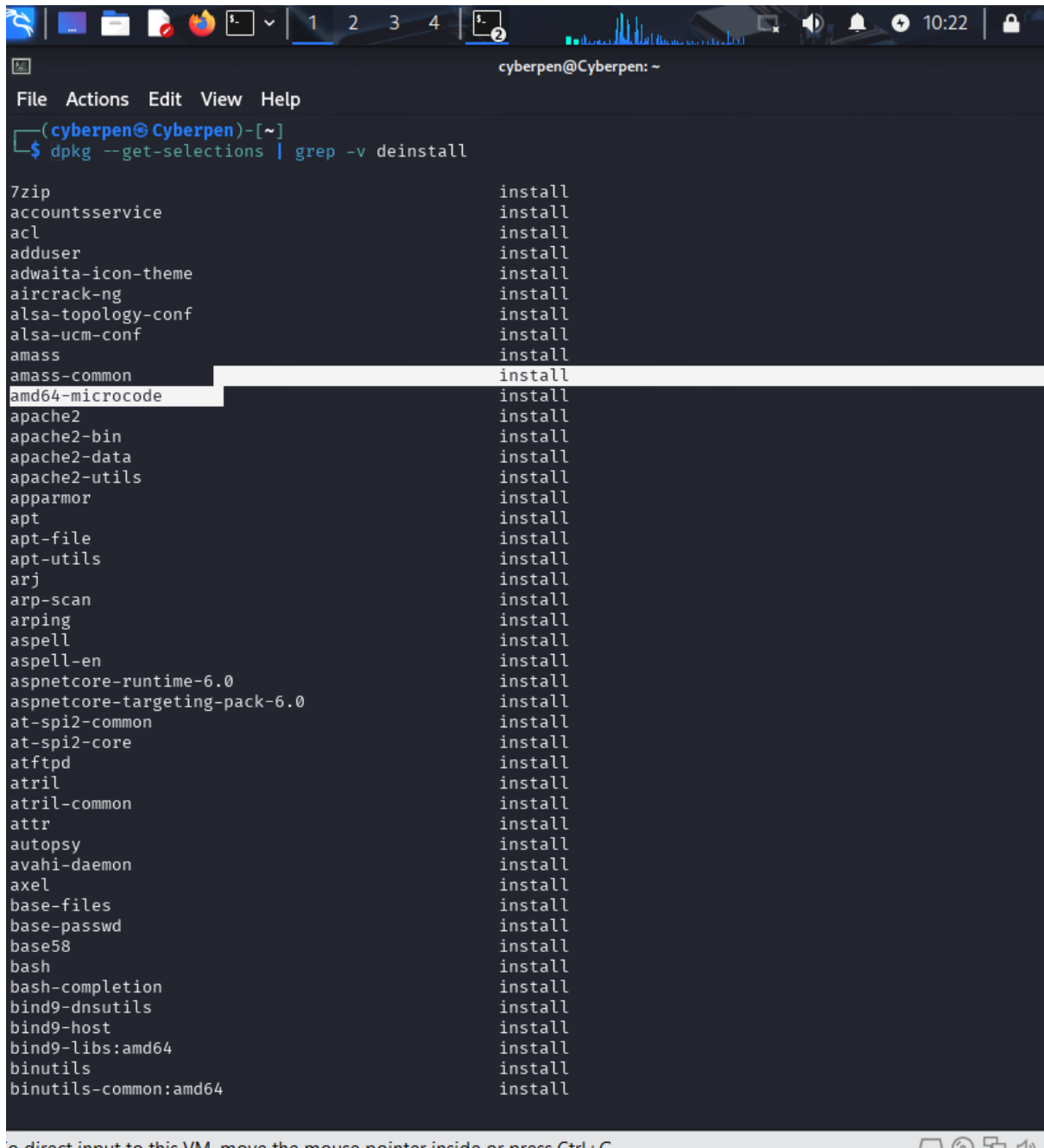
## Part 7: Final Review

1. Update Package List Again using the command: `sudo apt update`



```
cyberpen@Cyberpen: ~
$ sudo nano /etc/apt/sources.list
(cyberpen@Cyberpen)-[~]
$ sudo apt update
Ign:1 http://http.kali.org/kali kali-rolling InRelease
Ign:1 http://http.kali.org/kali kali-rolling InRelease
Ign:1 http://http.kali.org/kali kali-rolling InRelease
Err:1 http://http.kali.org/kali kali-rolling InRelease
Temporary failure resolving 'http.kali.org'
57 packages can be upgraded. Run 'apt list --upgradable' to see them.
Warning: Failed to fetch http://http.kali.org/kali/dists/kali-rolling/InRelease Temporary failure resolving 'h
kali.org'
Warning: Some index files failed to download. They have been ignored, or old ones used instead.
(cyberpen@Cyberpen)-[~]
$
```

2. Explore Installed Packages using the command: `dpkg --get-selections | grep -v deinstall`



```
cyberpen@Cyberpen: ~  
File Actions Edit View Help  
(cyberpen@Cyberpen)-[~]  
$ 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  
aspnetcore-runtime-6.0 install  
aspnetcore-targeting-pack-6.0 install  
at-spi2-common install  
at-spi2-core install  
atftpd install  
atril install  
atril-common install  
attr install  
autopsy install  
avahi-daemon install  
axel install  
base-files install  
base-passwd install  
base58 install  
bash install  
bash-completion install  
bind9-dnsutils install  
bind9-host install  
bind9-libs:amd64 install  
binutils install  
binutils-common:amd64 install
```

# Lab 3: Networking Commands

## Objectives

In this lab, you will:

- Learn how to use basic and advanced networking commands.
- Understand how to configure network interfaces and diagnose network issues.
- Use tools to monitor and analyse network traffic.

## Background / Scenario

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.

## Required Resources

- Kali Linux virtual machine (VM).
- Internet access

## Part 1: Displaying Network Configuration

Checking Network Interfaces using the command: `ip addr show`

```
(cyberpen@Cyberpen)-[~]
$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   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 group default qlen 1000
   link/ether 00:0c:29:85:8a:00 brd ff:ff:ff:ff:ff:ff
   inet 192.168.119.133/24 brd 192.168.119.255 scope global dynamic eth0
       valid_lft 1775sec preferred_lft 1775sec
   inet6 fe80::20c:29ff:fe85:8a00/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever

(cyberpen@Cyberpen)-[~]
$
```

List Routing Table using the command: `ip route show`

```
(cyberpen@Cyberpen)-[~]
$ ip route show
default via 192.168.119.2 dev eth0
192.168.119.0/24 dev eth0 proto kernel scope link src 192.168.119.133

(cyberpen@Cyberpen)-[~]
$
```

## Part 2: Testing Network Connectivity

1. Ping a Host using the command: `ping -c 4 google.com`

```
File Actions Edit View Help
(cyberpen@Cyberpen)-[~]
$ ping -c 4 google.com
PING google.com (142.250.200.110) 56(84) bytes of data.
64 bytes from mad41s13-in-f14.1e100.net (142.250.200.110): icmp_seq=1 ttl=128 time=163 ms
64 bytes from mad41s13-in-f14.1e100.net (142.250.200.110): icmp_seq=2 ttl=128 time=185 ms
64 bytes from mad41s13-in-f14.1e100.net (142.250.200.110): icmp_seq=3 ttl=128 time=207 ms
64 bytes from mad41s13-in-f14.1e100.net (142.250.200.110): icmp_seq=4 ttl=128 time=230 ms

— google.com ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 162.732/196.364/230.151/25.105 ms

(cyberpen@Cyberpen)-[~]
$
```

2. Trace Route to a Host using the command: `tracert google.com`

```
(cyberpen@Cyberpen)-[~]
$ tracert google.com
tracert to google.com (142.250.200.110), 30 hops max, 60 byte packets
 1  192.168.119.2 (192.168.119.2)  4.031 ms  3.900 ms  3.578 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

## Part 3: Configuring Network Interfaces

1. View Current Interface Configuration using the command: `ifconfig`

```
(cyberpen@Cyberpen)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.119.133 netmask 255.255.255.0 broadcast 192.168.119.255
    inet6 fe80::20c:29ff:fe85:8a00 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:85:8a:00 txqueuelen 1000 (Ethernet)
    RX packets 227 bytes 16658 (16.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 143 bytes 11278 (11.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 18 memory 0xfea20000-fea40000

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 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

2. Manually Configure an Interface using the command: `sudo ip addr add 192.168.1.20/24 dev eth0`

```
(cyberpen@Cyberpen)-[~]
$ sudo ip addr add 192.168.1.20/24 dev eth0
[sudo] password for cyberpen:
(cyberpen@Cyberpen)-[~]
$
```

3. Bring the Interface Up using the command: `sudo ip link set eth0 up`

```
(cyberpen@Cyberpen)-[~]
$ sudo ip link set eth0 up
(cyberpen@Cyberpen)-[~]
$
```

## Part 4: Monitoring Network Traffic

1. install tcpdump using the command: `sudo apt install tcpdump`

```
(cyberpen@Cyberpen)-[~]
$ sudo apt install tcpdump
[sudo] password for cyberpen:
tcpdump is already the newest version (4.99.5-2).
tcpdump set to manually installed.
The following packages were automatically installed and are no longer required:
base58 librpmbuild9 python3-lib2to3
binutils-mingw-w64-i686 librpmio9 python3-llvmlite
binutils-mingw-w64-x86-64 librpmsign10 python3-log-symbols
crackmapexec librpmsign9 python3-markdown
cython3 libsuperlu6 python3-marshmallow
debugedit libtag1v5 python3-marshmallow-sqlalchemy
dnsmap libtag1v5-vanilla python3-memcache
dsniff libtagc0 python3-mnemonic
ettercap-common libtirpc-dev python3-nplusone
ettercap-graphical libucl1 python3-numexpr
faraday-agent-dispatcher libusbmuxd6 python3-odf
figlet libwebkit2gtk-4.0-37 python3-ordered-set
finger libwireshark17 python3-paho-mqtt
firebird3.0-common libwiretap14 python3-pandas
firebird3.0-common-doc libwpe-1.0-1 python3-pandas-lib
fonts-liberation2 libwpebackend-fdo-1.0-1 python3-pefile
gcc-mingw-w64-base libwsutil15 python3-pgsql
gcc-mingw-w64-i686-win32 libxsimd-dev python3-plaster
gcc-mingw-w64-i686-win32-runtime libzip4 python3-plaster-pastedeploy
gcc-mingw-w64-x86-64-win32 libzxing2 python3-png
```

2. Capture Network Traffic using the command: `sudo tcpdump -i eth0 -c 10`

```
(cyberpen@Cyberpen)-[~]
$ 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
22:34:40.766682 IP 192.168.119.1.bootpc > 192.168.119.254.bootps: BOOTP/DHCP, Request from 00:50:56:c0:00:08 (oui U
nknown), length 316
22:34:40.766686 IP 192.168.119.254.bootps > 192.168.119.1.bootpc: BOOTP/DHCP, Reply, length 300
22:34:40.778794 IP6 fe80::7c65:5313:d7c0:9f7f > ff02::16: HBH ICMP6, multicast listener report v2, 1 group record(s
), length 28
22:34:40.778796 IP 192.168.119.1 > igmp.mcast.net: igmp v3 report, 1 group record(s)
22:34:40.819318 IP6 fe80::7c65:5313:d7c0:9f7f > ff02::16: HBH ICMP6, multicast listener report v2, 1 group record(s
), length 28
22:34:40.819547 IP 192.168.119.1 > igmp.mcast.net: igmp v3 report, 1 group record(s)
22:34:40.825782 IP6 fe80::7c65:5313:d7c0:9f7f > ff02::16: HBH ICMP6, multicast listener report v2, 1 group record(s
), length 28
22:34:40.825785 IP 192.168.119.1 > igmp.mcast.net: igmp v3 report, 1 group record(s)
22:34:40.829442 IP 192.168.119.133.50810 > 192.168.119.2.domain: 31033+ PTR? 254.119.168.192.in-addr.arpa. (46)
22:34:40.832277 IP6 fe80::7c65:5313:d7c0:9f7f > ff02::16: HBH ICMP6, multicast listener report v2, 1 group record(s
), length 28
10 packets captured
57 packets received by filter
21 packets dropped by kernel

(cyberpen@Cyberpen)-[~]
$
```

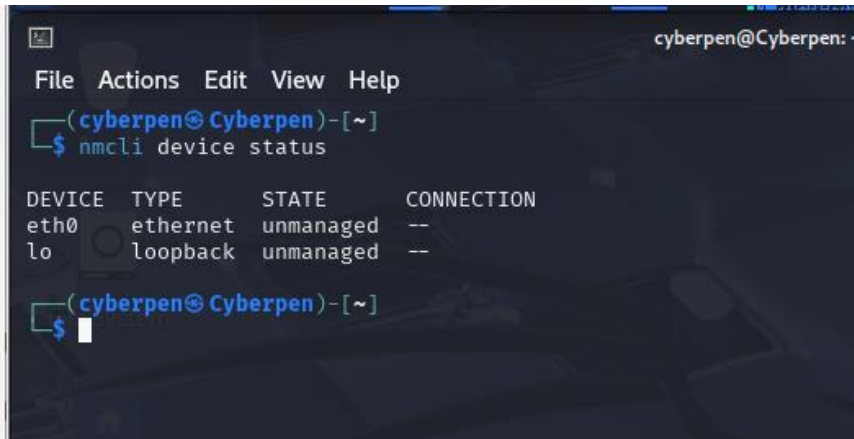
3. Analyze Network Traffic using the command: `sudo tcpdump -i eth0`

```
(cyberpen@Cyberpen)-[~]
$ sudo tcpdump -i eth0

tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
22:38:45.521458 ARP, Request who-has 192.168.119.2 tell 192.168.119.1, length 46
22:38:45.624286 IP 192.168.119.133.38575 > 192.168.119.2.domain: 32645+ PTR? 2.119.168.192.in-addr.arpa. (44)
22:38:45.631033 ARP, Request who-has 192.168.119.133 tell 192.168.119.2, length 46
22:38:45.631049 ARP, Reply 192.168.119.133 is-at 00:0c:29:85:8a:00 (oui Unknown), length 28
22:38:45.631223 IP 192.168.119.2.domain > 192.168.119.133.38575: 32645 NXDomain 0/0/0 (44)
22:38:45.631477 IP 192.168.119.133.38828 > 192.168.119.2.domain: 46381+ PTR? 1.119.168.192.in-addr.arpa. (44)
22:38:45.639480 IP 192.168.119.2.domain > 192.168.119.133.38828: 46381 NXDomain 0/0/0 (44)
22:38:45.727663 IP 192.168.119.133.54959 > 192.168.119.2.domain: 30097+ PTR? 133.119.168.192.in-addr.arpa. (46)
22:38:45.733937 IP 192.168.119.2.domain > 192.168.119.133.54959: 30097 NXDomain 0/0/0 (46)
22:38:46.829451 ARP, Request who-has 192.168.119.2 tell 192.168.119.1, length 46
22:38:47.520750 ARP, Request who-has 192.168.119.2 tell 192.168.119.1, length 46
22:38:48.520161 ARP, Request who-has 192.168.119.2 tell 192.168.119.1, length 46
22:38:50.683456 ARP, Request who-has 192.168.119.2 tell 192.168.119.133, length 28
22:38:50.683792 ARP, Reply 192.168.119.2 is-at 00:50:56:ec:cc:98 (oui Unknown), length 46
22:38:54.364875 ARP, Request who-has 192.168.119.2 tell 192.168.119.1, length 46
22:38:55.026162 ARP, Request who-has 192.168.119.2 tell 192.168.119.1, length 46
22:38:56.025712 ARP, Request who-has 192.168.119.2 tell 192.168.119.1, length 46
22:38:57.384468 ARP, Request who-has 192.168.119.2 tell 192.168.119.1, length 46
22:38:58.024930 ARP, Request who-has 192.168.119.2 tell 192.168.119.1, length 46
22:38:59.024776 ARP, Request who-has 192.168.119.2 tell 192.168.119.1, length 46
22:39:03.406977 ARP, Request who-has 192.168.119.2 tell 192.168.119.1, length 46
22:39:04.022648 ARP, Request who-has 192.168.119.2 tell 192.168.119.1, length 46
22:39:05.020801 ARP, Request who-has 192.168.119.2 tell 192.168.119.1, length 46
22:39:06.419272 ARP, Request who-has 192.168.119.2 tell 192.168.119.1, length 46
22:39:07.018828 ARP, Request who-has 192.168.119.2 tell 192.168.119.1, length 46
22:39:08.018250 ARP, Request who-has 192.168.119.2 tell 192.168.119.1, length 46
```

## Part 5: Final Review

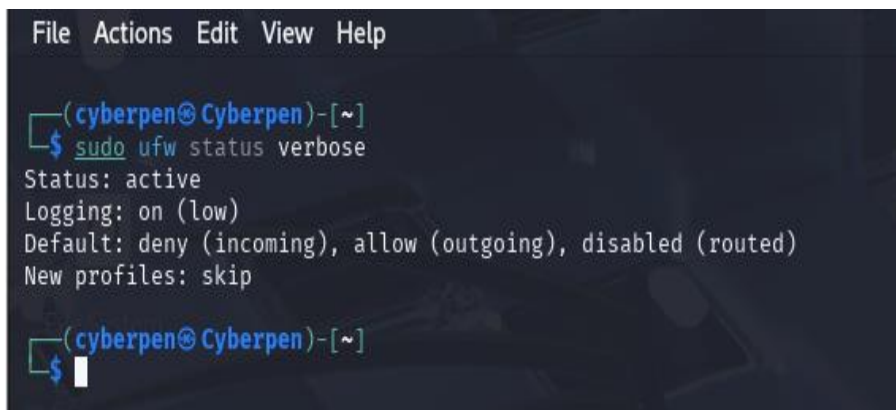
1. check Network Status on all interface using the command: nmcli device status



```
cyberpen@Cyberpen: ~  
File Actions Edit View Help  
(cyberpen@Cyberpen)-[~]  
$ nmcli device status  
  
DEVICE  TYPE      STATE      CONNECTION  
eth0    ethernet  unmanaged  --  
lo      loopback  unmanaged  --  
  
(cyberpen@Cyberpen)-[~]  
$
```

The screenshot shows a terminal window with a menu bar (File, Actions, Edit, View, Help) and a title bar (cyberpen@Cyberpen: ~). The user is in the home directory (~) and has executed the command `nmcli device status`. The output displays a table of network devices: `eth0` (ethernet, unmanaged, --) and `lo` (loopback, unmanaged, --). The prompt `(cyberpen@Cyberpen)-[~]` is shown before and after the command execution.

2. Check Firewall Status using the command: `sudo ufw status verbose`



```
File Actions Edit View Help  
(cyberpen@Cyberpen)-[~]  
$ sudo ufw status verbose  
Status: active  
Logging: on (low)  
Default: deny (incoming), allow (outgoing), disabled (routed)  
New profiles: skip  
  
(cyberpen@Cyberpen)-[~]  
$
```

The screenshot shows a terminal window with a menu bar (File, Actions, Edit, View, Help) and a title bar (cyberpen@Cyberpen: ~). The user is in the home directory (~) and has executed the command `sudo ufw status verbose`. The output displays the firewall status: `Status: active`, `Logging: on (low)`, `Default: deny (incoming), allow (outgoing), disabled (routed)`, and `New profiles: skip`. The prompt `(cyberpen@Cyberpen)-[~]` is shown before and after the command execution.

# Lab 4: Linux File Permissions and Ownership

## Objectives

In this lab, you will:

- Understand Linux file permissions and their implications.
- Learn to modify permissions and ownership of files and directories.
- Practice using permission-related commands with hands-on exercises.

## Background / Scenario

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.

## Required Resources

- Kali Linux VM
- Terminal access

## Concepts

### 1. File Permissions

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

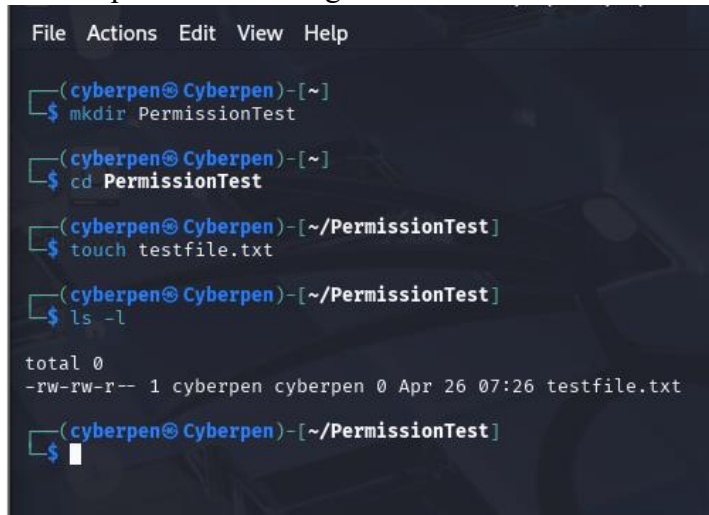
- Read (r): Permission to read the file.
- Write (w): Permission to modify or delete the file.
- Execute (x): Permission to run the file as a program.

## Part 1: Viewing File Permissions

### Step 1: Check Current Permissions

1. Open your terminal.
2. Create a new directory using the command: `mkdir PermissionTest`
3. Navigate into the directory using the command: `cd PermissionTest`
4. Create a new file using the command: `touch testfile.txt`

5. List the permissions using the command: `ls -l`



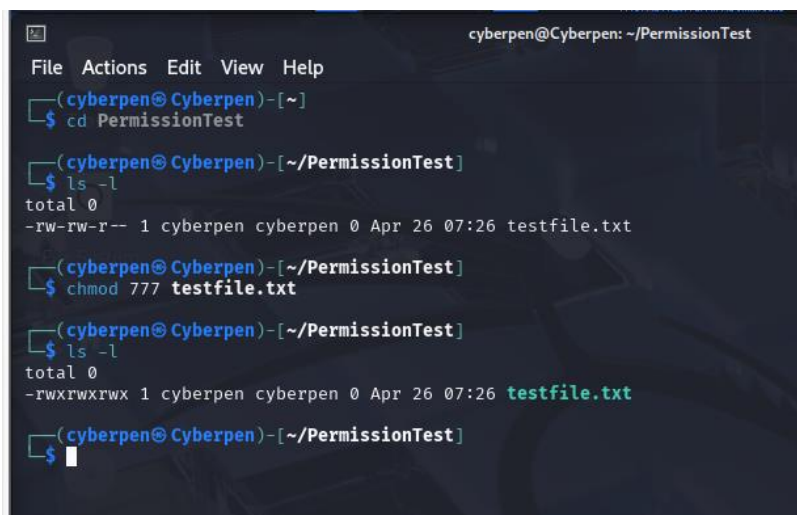
```
File Actions Edit View Help
(cyberpen@Cyberpen)-[~]
$ mkdir PermissionTest
(cyberpen@Cyberpen)-[~]
$ cd PermissionTest
(cyberpen@Cyberpen)-[~/PermissionTest]
$ touch testfile.txt
(cyberpen@Cyberpen)-[~/PermissionTest]
$ ls -l

total 0
-rw-rw-r-- 1 cyberpen cyberpen 0 Apr 26 07:26 testfile.txt
(cyberpen@Cyberpen)-[~/PermissionTest]
$
```

## Part 2: Modifying Permissions

### Step 2: Change File Permission

1. Change the permissions of testfile.txt to 777 (full permissions for everyone) using the command: `chmod 777 testfile.txt`
2. Verify the changes using the command: `ls -l`



```
cyberpen@Cyberpen: ~/PermissionTest
File Actions Edit View Help
(cyberpen@Cyberpen)-[~]
$ cd PermissionTest
(cyberpen@Cyberpen)-[~/PermissionTest]
$ ls -l
total 0
-rw-rw-r-- 1 cyberpen cyberpen 0 Apr 26 07:26 testfile.txt
(cyberpen@Cyberpen)-[~/PermissionTest]
$ chmod 777 testfile.txt
(cyberpen@Cyberpen)-[~/PermissionTest]
$ ls -l
total 0
-rwxrwxrwx 1 cyberpen cyberpen 0 Apr 26 07:26 testfile.txt
(cyberpen@Cyberpen)-[~/PermissionTest]
$
```

### Step 3: Revert Permissions

1. Revert the permissions to 644 (owner can read/write, group and others can read) using the command: `chmod 644 testfile.txt`
2. Check permissions again using the command: `ls -l`

```
(cyberpen@Cyberpen)-[~/PermissionTest]
$ ls -l
total 0
-rwxrwxrwx 1 cyberpen cyberpen 0 Apr 26 07:26 testfile.txt

(cyberpen@Cyberpen)-[~/PermissionTest]
$ chmod 644 testfile.txt

(cyberpen@Cyberpen)-[~/PermissionTest]
$ ls -l
total 0
-rw-r--r-- 1 cyberpen cyberpen 0 Apr 26 07:26 testfile.txt

(cyberpen@Cyberpen)-[~/PermissionTest]
$
```

## Exercise 1: Experiment with Permissions

1. Change the permissions of testfile.txt back to 777 using the command: `chmod 777 testfile.txt`
2. Verify the permissions again using the command: `ls -l`

```
(cyberpen@Cyberpen)-[~/PermissionTest]
$ ls -l
total 0
-rw-r--r-- 1 cyberpen cyberpen 0 Apr 26 07:26 testfile.txt

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

(cyberpen@Cyberpen)-[~/PermissionTest]
$ ls -l
total 0
-rwxrwxrwx 1 cyberpen cyberpen 0 Apr 26 07:26 testfile.txt

(cyberpen@Cyberpen)-[~/PermissionTest]
$
```

## Part 3: Changing Ownership

### Step 4: Change File Ownership

1. Create a new user for testing (this may require sudo privileges) using the command:  
`sudo adduser testuser`

2. Change the ownership of testfile.txt to testuser using the command: `sudo chown testuser:testuser testfile.txt`
3. Verify ownership using the command: `ls -l`

```
File Actions Edit View Help
(cyberpen@Cyberpen)-[~]
$ cd PermissionTest

(cyberpen@Cyberpen)-[~/PermissionTest]
$ sudo adduser testuser
[sudo] password for cyberpen:
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for testuser
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y

(cyberpen@Cyberpen)-[~/PermissionTest]
$ ls -l
total 0
-rwxrwxrwx 1 cyberpen cyberpen 0 Apr 26 07:26 testfile.txt

(cyberpen@Cyberpen)-[~/PermissionTest]
$
```

## Exercise 2: Group Ownership

1. Change the group ownership of testfile.txt to another group (e.g., staff) using the command: `sudo chgrp staff testfile.txt`
2. Check the ownership and permissions again

```
cyberpen@Cyberpen: ~/PermissionTest
File Actions Edit View Help
(cyberpen@Cyberpen)-[~]
$ cd PermissionTest

(cyberpen@Cyberpen)-[~/PermissionTest]
$ ls
testfile.txt

(cyberpen@Cyberpen)-[~/PermissionTest]
$ ls -l
total 0
-rwxrwxrwx 1 cyberpen cyberpen 0 Apr 26 07:26 testfile.txt

(cyberpen@Cyberpen)-[~/PermissionTest]
$ sudo chgrp staff testfile.txt
[sudo] password for cyberpen:

(cyberpen@Cyberpen)-[~/PermissionTest]
$ ls -l
total 0
-rwxrwxrwx 1 cyberpen staff 0 Apr 26 07:26 testfile.txt

(cyberpen@Cyberpen)-[~/PermissionTest]
$
```

## Part 4: Practical Exercises

### Exercise 3: Create and Modify Permissions

1. Create three new files using the command: `touch file1.txt file2.txt file3.txt`

```
File Actions Edit View Help

(cyberpen@Cyberpen) ~
$ touch file1.txt file2.txt file3.txt

(cyberpen@Cyberpen) ~
$ ls
file1.txt  file2.txt  file3.txt  testfile.txt

(cyberpen@Cyberpen) ~
$
```

2. Set permissions as follows:

- file1.txt: Full permissions for owner, read and execute for group and others (755) using the command: `chmod 755 file1.txt`

```
(cyberpen@Cyberpen) ~
$ ls -l
total 0
-rw-rw-r-- 1 cyberpen cyberpen 0 Apr 26 08:12 file1.txt
-rw-rw-r-- 1 cyberpen cyberpen 0 Apr 26 08:12 file2.txt
-rw-rw-r-- 1 cyberpen cyberpen 0 Apr 26 08:12 file3.txt
-rwxrwxrwx 1 cyberpen staff 0 Apr 26 07:26 testfile.txt

(cyberpen@Cyberpen) ~
$ chmod 755 file1.txt

(cyberpen@Cyberpen) ~
$ ls -l
total 0
-rwxr-xr-x 1 cyberpen cyberpen 0 Apr 26 08:12 file1.txt
-rw-rw-r-- 1 cyberpen cyberpen 0 Apr 26 08:12 file2.txt
-rw-rw-r-- 1 cyberpen cyberpen 0 Apr 26 08:12 file3.txt
-rwxrwxrwx 1 cyberpen staff 0 Apr 26 07:26 testfile.txt

(cyberpen@Cyberpen) ~
$
```

- file2.txt: Read and write for the owner, read for group and others (644) using the command: `chmod 644 file2.txt`

```
(cyberpen@Cyberpen)-[~/PermissionTest]
$ ls -l
total 0
-rwxr-xr-x 1 cyberpen cyberpen 0 Apr 26 08:12 file1.txt
-rw-rw-r-- 1 cyberpen cyberpen 0 Apr 26 08:12 file2.txt
-rw-rw-r-- 1 cyberpen cyberpen 0 Apr 26 08:12 file3.txt
-rwxrwxrwx 1 cyberpen staff 0 Apr 26 07:26 testfile.txt

(cyberpen@Cyberpen)-[~/PermissionTest]
$ chmod 644 file2.txt

(cyberpen@Cyberpen)-[~/PermissionTest]
$ ls -l
total 0
-rwxr-xr-x 1 cyberpen cyberpen 0 Apr 26 08:12 file1.txt
-rw-r--r-- 1 cyberpen cyberpen 0 Apr 26 08:12 file2.txt
-rw-rw-r-- 1 cyberpen cyberpen 0 Apr 26 08:12 file3.txt
-rwxrwxrwx 1 cyberpen staff 0 Apr 26 07:26 testfile.txt

(cyberpen@Cyberpen)-[~/PermissionTest]
$
```

- file3.txt: Full permissions for everyone (777) using the command: `chmod 777 file3.txt`

```
(cyberpen@Cyberpen)-[~/PermissionTest]
$ ls -l
total 0
-rwxr-xr-x 1 cyberpen cyberpen 0 Apr 26 08:12 file1.txt
-rw-r--r-- 1 cyberpen cyberpen 0 Apr 26 08:12 file2.txt
-rw-rw-r-- 1 cyberpen cyberpen 0 Apr 26 08:12 file3.txt
-rwxrwxrwx 1 cyberpen staff 0 Apr 26 07:26 testfile.txt

(cyberpen@Cyberpen)-[~/PermissionTest]
$ chmod 777 file3.txt

(cyberpen@Cyberpen)-[~/PermissionTest]
$ ls -l
total 0
-rwxr-xr-x 1 cyberpen cyberpen 0 Apr 26 08:12 file1.txt
-rw-r--r-- 1 cyberpen cyberpen 0 Apr 26 08:12 file2.txt
-rwxrwxrwx 1 cyberpen cyberpen 0 Apr 26 08:12 file3.txt
-rwxrwxrwx 1 cyberpen staff 0 Apr 26 07:26 testfile.txt

(cyberpen@Cyberpen)-[~/PermissionTest]
$
```

#### Exercise 4: Ownership Challenge

1. Create a directory named Project and set your current user as the owner using the command: `mkdir Project sudo chown $USER:$USER Project`
2. Verify the ownership using the command: `ls -ld Project`

```
(cyberpen@Cyberpen)-[~/PermissionTest]
$ cd

(cyberpen@Cyberpen)-[~]
$ mkdir Project

(cyberpen@Cyberpen)-[~]
$ sudo chown $USER:$USER Project
[sudo] password for cyberpen:

(cyberpen@Cyberpen)-[~]
$ ls -ld Project
drwxrwxr-x 2 cyberpen cyberpen 4096 Apr 26 08:29 Project

(cyberpen@Cyberpen)-[~]
$
```

Kali Linux

# Lab 5: Individual Research on Linux

## Objectives

In this lab, you will:

- Conduct individual research on various aspects of Linux.
- Analyze and present your findings in a structured format.
- Fill in a research table based on your findings.

## Required Resources

- Access to the internet for research.
- Document editor (e.g., Google Docs, Microsoft Word).

## Research Topic

Linux Distributions: Research different Linux distributions, their features, and typical use cases.

# Linux Distributions

## Introduction

A Linux distribution also known as distro is an installable operating system (OS) that's built from the Linux kernel and supports user programs, repositories, and libraries. Each vendor's or community's version of Linux is a distro.

Because Linux is open source and released under the GNU General Public License (GPL), anyone can run, study, modify, and redistribute the source code, or even sell copies of their modified code. This differs greatly from traditional operating systems like UNIX, Microsoft Windows, and macOS, which are proprietary and not modifiable.

## Key Features of Linux Distribution

All Linux distributions are built around the Linux kernel but differentiate themselves in several ways:

- **User Interface:** Some provide lightweight desktop environments for older hardware, while others offer polished, resource-intensive interfaces.
- **Package Management:** Different distributions use different tools to manage software (like APT for Ubuntu/Debian and DNF for Fedora/Red Hat).
- **Release Cycle:** Some are rolling releases (e.g., Arch Linux), providing cutting-edge updates, while others focus on long-term stability (e.g., Debian, Ubuntu LTS).

## Factors for Choosing a Distribution

When choosing the right distribution, several factors must be considered examples of which are

- **Purpose:** you need to consider the purpose you need the distribution for if its for cybersecurity, desktop, development or server
- **Hardware:** Lightweight distributions like MX Linux Ubuntu or Linux Mint are better for older hardware
- **Community Support:** Strong community forums and official documentation are crucial for troubleshooting and learning
- **Software Availability and Package Management:** Availability of necessary software through official repository

## Common Use Cases

- **Beginners and Desktop Users:** Ubuntu, Linux Mint, and Manjaro offer easy installation, a rich set of pre-installed applications, and an intuitive user interface
- **Advanced Users and Developers:** Arch Linux, Fedora, and EndeavourOS allow complete system customization and access to the latest software updates.
- **Server Environments:** Debian and CentOS are preferred for their reliability, stability, and extensive documentation.
- **Lightweight Systems:** MX Linux provides an excellent balance for older hardware or users seeking a lightweight and efficient system.
- **Rolling Release Enthusiasts:** Distributions like openSUSE Tumbleweed and Arch Linux provide continuous updates without the need for full upgrades.

## Overview of Some Popular Linux Distributions

Distributions	Key Features	Common Use Cases
<b>Ubuntu</b>	User-friendly interface, extensive community support, and regular Long-Term Support (LTS) releases	Ideal for beginners, general desk development environment
<b>Debian</b>	Known for its stability and extensive software repositories. Serves as the base for many other distributions.	Preferred for servers, advanced users, and as a foundation for other distros.
<b>Fedora</b>	Features the latest software and technologies, backed by Red Hat. Offers a balance between innovation and stability	suitable for developers and users seeking cutting-edge features.
<b>Arch Linux</b>	Minimalist and highly customizable, following a rolling release model.	Targeted at advanced users who desire complete control over their system.
<b>CentOS</b>	Derived from Red Hat Enterprise Linux (RHEL), focusing on stability and long-term support	Commonly used for servers and enterprise environments.
<b>Linux Mint</b>	Based on Ubuntu, offering a familiar interface and out-of-the-box multimedia support.	Great for users transitioning from Windows and those seeking a ready-to-use desktop experience.
<b>openSUSE</b>	Provides two main editions: Leap (stable) and Tumbleweed (rolling release). Features the YaST configuration tool.	Suitable for both desktop and server use, catering to a wide range of users.
<b>Manjaro</b>	Based on Arch Linux, but more user-friendly with a focus on accessibility and ease of use	Ideal for users who want the power of Arch with a more approachable setup.
<b>MX Linux</b>	Combines a lightweight design with a user-friendly interface, based on Debian.	Perfect for users with older hardware or those seeking a balance between performance and simplicity.
<b>EndeavourOS</b>	Provides a close-to-Arch experience with a focus on simplicity and community support.	Appeals to users who want to explore Arch Linux without the complexity of manual installation.

## Conclusion

Linux distributions offer a wide variety of options suited for different users, purposes, and technical requirements. Whether you're a beginner looking for simplicity or an expert seeking maximum customization, there is a Linux distribution tailored for you. Understanding the strengths and target audience of each distribution is essential for choosing the best one for your needs.

## References

1. GeeksforGeeks. (2023). What are Linux Distributions? Retrieved from: <https://www.geeksforgeeks.org/what-are-linux-distributions/>
2. eStart Hosting. (2023). Major Linux Distributions – A Comprehensive Overview. Retrieved from: <https://www.estart.co.za/major-linux-distributions-a-comprehensive-overview/>
3. Cloud News. (2024). The 10 Most Popular Linux Distributions of 2024. Retrieved from: <https://cloudnews.tech/the-10-most-popular-linux-distributions-of-2024/>

## Overall challenges and Solution

- Not typing in the correct command thus giving a wrong output or some of the command not running at all, the solution is to recheck, retype and confirm my commands
- Network malfunctioning, i solve this by getting an alternative sim to connect to the internet
- My Kali freezing at some point, i solve this by switching of my system