# Module 1: Linux Fundamentals

## Demo Document 1

edureka!

© Brain4ce Education Solutions Pvt. Ltd.

# File and Directory Commands

| Command | Description |
|---|---|
| ***pwd*** | The ***pwd***(present working directory) command is used to display the path of the directory that the terminal is currently active in. |

**Syntax**

```
pwd [options]
```

**Example**

Displays the present working directory.

**Command:** pwd

**Output:**

```
root@kali:~# pwd
/root
```

This means that the present working directory is **/root**

## File Types in Linux

| File Type | Representation |
|---|---|
| Regular file | - |
| Directory | d |
| Character device file | c |
| Block device file | b |
| Local socket file | s |
| Pipe | p |
| Symbolic Link | l |

| Command | Description |
|---|---|
| ***ls*** | The ***ls*** command is used to list the information about the files in a particular directory. |

**Syntax**

```
ls [options] <path of directory or file name>
```

**Example 1**

List all the files in the present directory.

**Command:** `ls`

**Output:**

```
root@kali:~# ls
Desktop    Downloads  Pictures  Templates  vmware_tools
Documents  Music      Public    Videos
```

List of the files present in the present working directory

**Example 2**

List all the files in the **/etc/apt** directory.

**Command:** `ls /etc/apt`

**Output:**

```
root@kali:~# ls /etc/apt/
apt.conf.d         preferences.d  sources.list~   trusted.gpg.d
listchanges.conf   sources.list   sources.list.d
```

**Example 3**

List all the files in the present working directory in long listing format.

**Command:** `ls -l`

**Output:**

```
root@kali:~# ls -l
total 36
drwxr-xr-x 2 root root 4096 Sep 19 05:47 Desktop
drwxr-xr-x 2 root root 4096 Feb 11  2019 Documents
drwxr-xr-x 5 root root 4096 Oct 25 03:22 Downloads
drwxr-xr-x 2 root root 4096 Feb 11  2019 Music
drwxr-xr-x 2 root root 4096 Aug 19 07:15 Pictures
drwxr-xr-x 2 root root 4096 Feb 11  2019 Public
drwxr-xr-x 2 root root 4096 Feb 11  2019 Templates
drwxr-xr-x 2 root root 4096 Feb 11  2019 Videos
drwxr-xr-x 3 root root 4096 May 28  2019 vmware_tools
```

The long listing format displays information as follows:

- File type and file permissions

  The first bit of the first section displays the file type followed by the permissions. In the above screenshot, the first bit '**d**' means that the file type is a directory.

  The next 3 bits displays the permissions of the user, followed by the next 3 bits displaying the permissions for the group, followed by the next 3 bits displaying the permissions for other users.

The character 'r' represents read permission, 'w' represents write permission and 'x' represents execute permission.

- The second section displays the number of hard links
- The third section displays the owner of the file
- The fourth section displays the group that the file belongs to
- The fifth section displays the size of the file in bytes
- The sixth section displays the last modification date of the file
- The last section displays the name of the file

You can find more options for ***ls*** command by running the command: `ls --help`

| Command | Description |
|---|---|
| ***sudo*** | The ***sudo*** command prefix is used to run a command with superuser privileges |

**Syntax**

```
sudo <command>
```

**Example**

Display the contents of the **/etc/sudoers/** file which requires superuser privileges using the **sudo** command

**Command:** `sudo cat /etc/sudoers`

**Output:**

edureka!

```
edureka@kali:~$ cat /etc/sudoers
cat: /etc/sudoers: Permission denied
edureka@kali:~$ sudo cat /etc/sudoers
[sudo] password for edureka:
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/
sbin:/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
```

## The **sudoers** file

The **sudoers** file is used to allocate system rights to the users. This file is used by the administrators to control user rights. When you use the **sudo** command, the system checks if the user's name using the **sudo** is mentioned in the **sudoers** file. The system allows the command execution with superuser privileges only if that user's name is mentioned in the **sudoers** file.

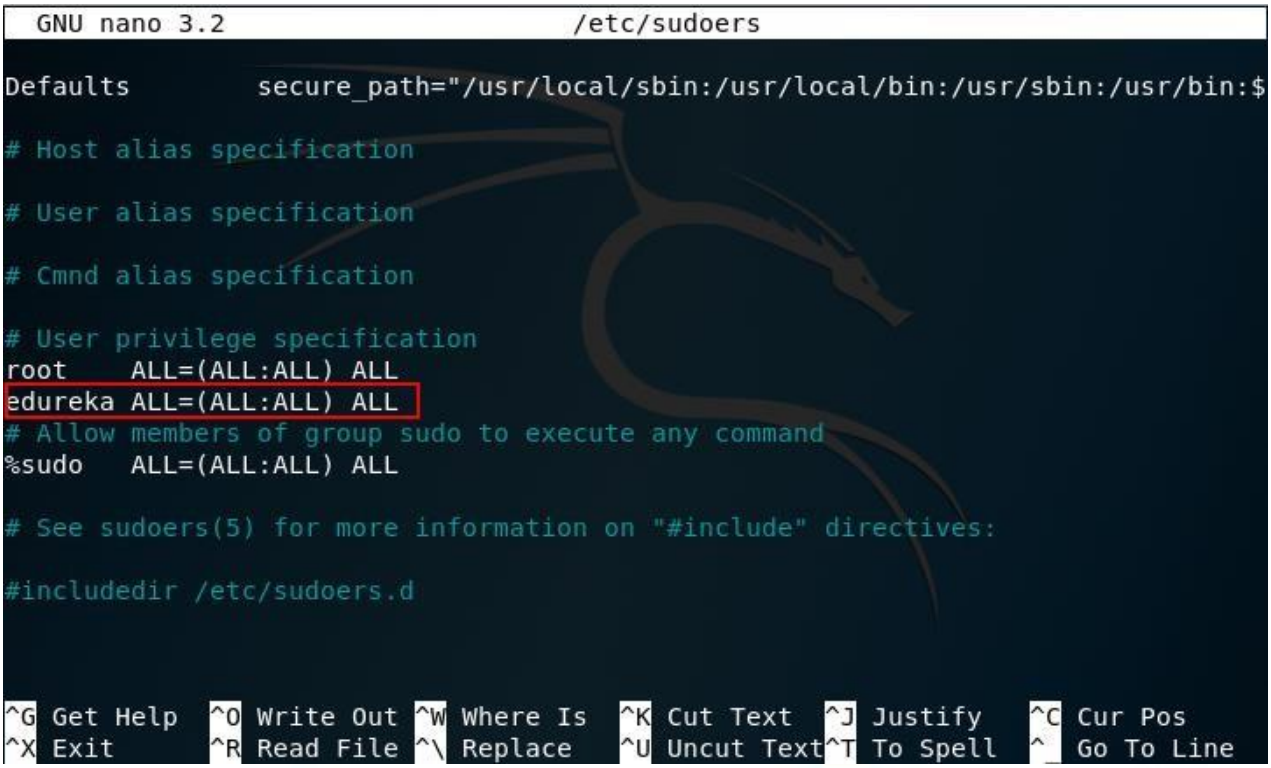
**Adding a user to the sudoers file:**

Only a root user can add users to the sudoers file.

To open the sudoers file, run the below command:

```
sudo nano /etc/sudoers
```

Then add the username as show in the screenshot below:




| Command | Description |
|---|---|
| ***mkdir*** | The ***mkdir*** command is used to create a new directory. |

**Syntax**

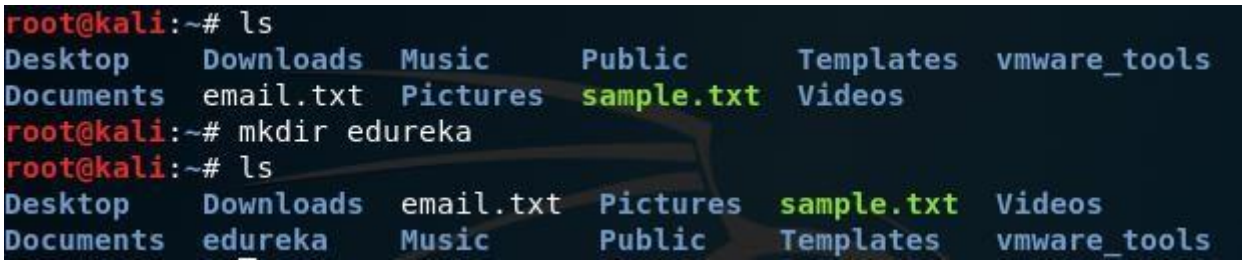
```
mkdir <directoryname>
```

**Example**

Create a directory named **edureka.**

**Command:** `mkdir edureka`

**Output:**



| Command | Description |
|---|---|
| *cd* | The ***cd*** command is used to change the present working directory. |

**Syntax**

```
cd [options] <path to directory>
```

**Example**

Change the present working directory to **/etc/apt**

**Command:** `cd /etc/apt`

**Output:**

```
root@kali:~# cd /etc/apt/
root@kali:/etc/apt#
```

| Command | Description |
|---|---|
| *cp* | The ***cp*** command is used to copy files and directories from one directory to another |

**Syntax**

```
cp <source filename> <destination path>
```

**Example**

Copy the **sources.list file** from **/etc/apt/** to the **/root** directory.

**Command:** `cd /etc/apt/sources.list /root`

**Output:**

```
root@kali:~# ls
Desktop    Downloads  Pictures  Templates  vmware_tools
Documents  Music      Public    Videos
root@kali:~# cp /etc/apt/sources.list /root/
root@kali:~# ls
Desktop    Downloads  Pictures  sources.list  Videos
Documents  Music      Public    Templates     vmware_tools
```

| Command | Description |
|---|---|
| *mv* | The ***mv*** command is used to move files and directories from one directory to another or to rename files |

**Syntax**

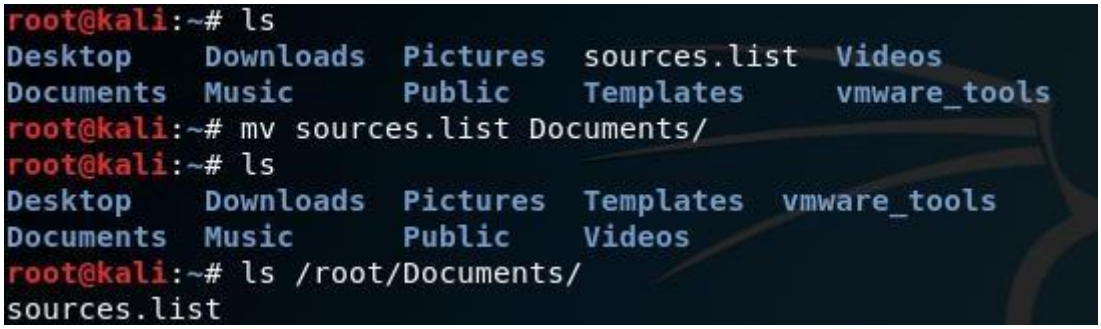
```
mv <source filename> <destination path>
```

**Example 1**

Move the **sources.list file** from **/root** to the **/root/Documents** directory.

**Command:** `mv sources.list /root/Documents`

**Output:**

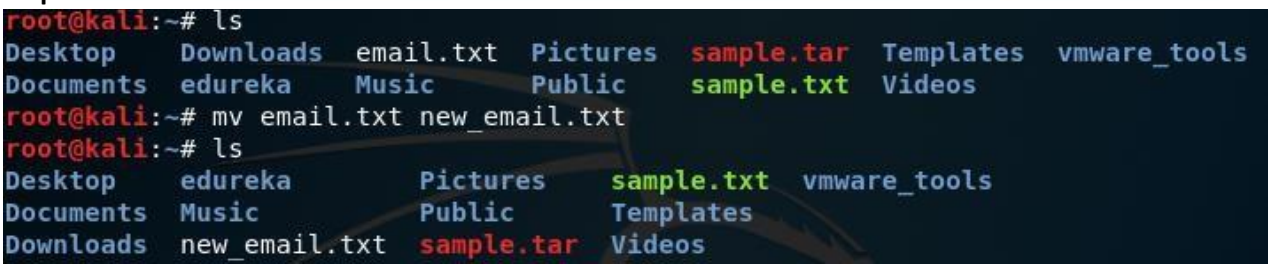



**Example 2**

Rename a file using the mv command

**Command:** `mv email.txt new_email.txt`

**Output:**




| Command | Description |
|---|---|
| ***cat*** | The ***cat*** command is used to create file(s), view the contents of the file, concatenate files and redirect output |

**Syntax**

```
cat <filename>
```

**Example 1**

Display the contents of the **/etc/hosts** file

**Command:** `cat /etc/hosts`

**Output:**

```
root@kali:~# cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
192.168.111.181 omkar.facebook.com

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

**Example 2**

Display the contents of the **/etc/hosts** and **/etc/apt/sources.list** file

**Command:** `cat /etc/hosts /etc/apt/sources.list`

**Output:**

```
root@kali:~# cat /etc/hosts /etc/apt/sources.list
127.0.0.1       localhost
127.0.1.1       kali
192.168.111.181 omkar.facebook.com

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
#

# deb cdrom:[Debian GNU/Linux 2019.1 _Kali-rolling_ - Official Snapshot amd64 LIVE/INSTALL Binary 20
190130-07:27]/ kali-last-snapshot contrib main non-free

#deb cdrom:[Debian GNU/Linux 2019.1 _Kali-rolling_ - Official Snapshot amd64 LIVE/INSTALL Binary 201
90130-07:27]/ kali-last-snapshot contrib main non-free

deb http://http.kali.org/kali kali-rolling main non-free contrib
deb-src http://http.kali.org/kali kali-rolling main non-free contrib

# This system was installed using small removable media
# (e.g. netinst, live or single CD). The matching "deb cdrom"
# entries were disabled at the end of the installation process.
# For information about how to configure apt package sources,
# see the sources.list(5) manual.
#deb http://http.kali.org/kali kali-rolling main contrib non-free
deb http://old.kali.org/kali sana main non-free contrib
```

You can find more options for ***cat*** command by running the command: `cat --help`

| Operator | Description |
|---|---|
| > | The **> (redirection)** operator is used to redirect the output of a command to a file |

**Syntax**

`<command 1> > <filename>`

**Example**

**Command:** `ls -l > a.txt`

**Output:**

```
root@kali:~# ls -l > a.txt
root@kali:~# cat a.txt
total 4060
-rw-r--r-- 1 root root       0 Jan 29 07:17 a.txt
drwxr-xr-x 2 root root    4096 Sep 19 05:47 Desktop
drwxr-xr-x 2 root root    4096 Jan 24 06:46 Documents
drwxr-xr-x 5 root root    4096 Jan 24 02:29 Downloads
drwxr-xr-x 2 root root    4096 Jan 27 23:45 edureka
drwxr-xr-x 2 root root    4096 Feb 11  2019 Music
-rw-r--r-- 1 root root    1980 Jan 24 07:11 new_email.txt
drwxr-xr-x 2 root root    4096 Jan 24 02:20 Pictures
drwxr-xr-x 2 root root    4096 Feb 11  2019 Public
-rw-r--r-- 1 root root 2058240 Jan 28 06:35 sample.tar
-rwxrwxrwt 1 root root 2052096 Jan 24 03:56 sample.txt
drwxr-xr-x 2 root root    4096 Feb 11  2019 Templates
drwxr-xr-x 2 root root    4096 Feb 11  2019 Videos
drwxr-xr-x 3 root root    4096 May 28  2019 vmware_tools
```

A single redirection operator writes into the file. If you want to append the file, you will have to use double redirection operator.

```
root@kali:~# echo Hello World > a.txt
root@kali:~# cat a.txt
Hello World
root@kali:~# echo Hi again > a.txt
root@kali:~# cat a.txt
Hi again
root@kali:~# echo This line was appended >> a.txt
root@kali:~# cat a.txt
Hi again
This line was appended
```

| Command | Description |
|---|---|
| *less* | The ***less*** command is used to read the contents of a file one page at a time |

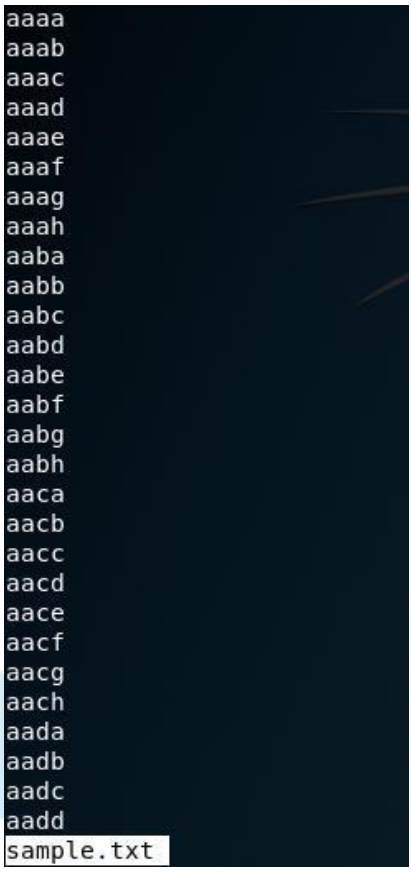
**Syntax**

```
less [options] <filename>
```

**Example 1**

**Command:** `less sample.txt`

**Output:**




You can find more options for ***less*** command by running the command: `less --help`

| Command | Description |
|---|---|
| *echo* | The ***echo*** command is used to display the string passed as an argument to the terminal |

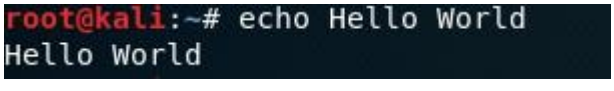
**Syntax**

```
echo [options] <string>
```

**Example 1**

**Command:** `echo Hello World`

**Output:**



You can find more options for ***echo*** command by running the command: `man echo`

| Command | Description |
|---|---|
| ***touch*** | The ***touch*** command is used to create a file or change the timestamp of the file |

**Syntax**

```
touch [options] <filename>
```

**Example 1**

**Command:** `touch sample.txt`

**Output:**

```
root@kali:~# ls -l sample.txt
-rw-r--r-- 1 root root 2052096 Jan 24 03:35 sample.txt
root@kali:~# touch sample.txt
root@kali:~# ls -l sample.txt
-rw-r--r-- 1 root root 2052096 Jan 24 03:56 sample.txt
```

You can find more options for ***touch*** command by running the command: `touch --help`

| Command | Description |
|---|---|
| ***chown*** | The ***chown*** command is used to change the owner and group of files |

**Syntax**

```
chown [options] <[Owner][:Group]> <filemename>
```

**Example 1**

Changing the owner of a file

**Command:** `chown edureka sample.txt`

**Output:**

```
root@kali:~# ls -l sample.txt
-rw-r--r-- 1 root root 2052096 Jan 24 03:56 sample.txt
root@kali:~# chown edureka sample.txt
root@kali:~# ls -l sample.txt
```

**Example 2**

Changing the group of a file

**Command:** `chown :edureka sample.txt`

**Output:**

```
root@kali:~# ls -l sample.txt
-rw-r--r-- 1 edureka root 2052096 Jan 24 03:56 sample.txt
root@kali:~# chown :edureka sample.txt
root@kali:~# ls -l sample.txt
-rw-r--r-- 1 edureka edureka 2052096 Jan 24 03:56 sample.txt
```

**Example 3**

Changing the owner and group of a file

**Command:** `chown root:root sample.txt`

**Output:**

```
root@kali:~# ls -l sample.txt
-rw-r--r-- 1 edureka edureka 2052096 Jan 24 03:56 sample.txt
root@kali:~# chown root:root sample.txt
root@kali:~# ls -l sample.txt
-rw-r--r-- 1 root root 2052096 Jan 24 03:56 sample.txt
```

You can find more options for ***chown*** command by running the command: `chown --help`

| Command | Description |
|---|---|
| ***chmod*** | The ***chmod*** command is used to change the permissions of a file |

**Syntax**

chmod [options] <new permissions> <filename>

The permissions can be set in two modes:

1. Octal Mode

   In octal mode the permissions are set using 3 bits for users('u'), group('g') and other('o') users respectively. Each bit is a binary to decimal conversion of permission

| read | write | execute | Decimal | Permission |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | No permissions |
| 0 | 0 | 1 | 1 | Only execute |
| 0 | 1 | 0 | 2 | Only write |
| 0 | 1 | 1 | 3 | Write and execute |
| 1 | 0 | 0 | 4 | Only read |
| 1 | 0 | 1 | 5 | Read and execute |
| 1 | 1 | 0 | 6 | Read and write |
| 1 | 1 | 1 | 7 | Read, write and execute |

**Example**

Changing the permissions of a file so that the user can read, write and execute, the group can read and execute and other users can only execute using octal mode.

**Command:** `chmod 751 sample.txt`

**Output:**

```
root@kali:~# ls -l sample.txt
-rw-r--r-- 1 root root 2052096 Jan 24 03:56 sample.txt
root@kali:~# chmod 751 sample.txt
root@kali:~# ls -l sample.txt
-rwxr-x--x 1 root root 2052096 Jan 24 03:56 sample.txt
```

2. Symbolic Mode

In symbolic mode the permissions are changed by using the character '+' to add, '-' to remove and '=' to set the permissions. The permissions are represented by 'r' for read, 'w' for write, 'x' for execute.

| Character | Represents |
|---|---|
| R | Read |
| w | Write |
| x | Execute |
| t | Sticky bit – used to restrict moving and deleting of a file to its owner |
| u+s | SUID – used to execute an executable file as the owner |
| g+s | SGID - used to execute an executable file with authority of the group |

**Example 1**

Changing the permissions of a file so that the user can read and execute, the group can only read, and other users can only read using symbolic mode.

**Command:** `chmod u=rx,g=r,o=r sample.txt` **Output:**

```
root@kali:~# ls -l sample.txt
-rwxr-x--x 1 root root 2052096 Jan 24 03:56 sample.txt
root@kali:~# chmod u=rx,g=r,o=r sample.txt
root@kali:~# ls -l sample.txt
-r-xr--r-- 1 root root 2052096 Jan 24 03:56 sample.txt
```

**Example 2**

Add execute permissions to a file using symbolic mode.

**Command:** `chmod +x sample.txt`

**Output:**

```
root@kali:~# ls -l sample.txt
-r-xr--r-- 1 root root 2052096 Jan 24 03:56 sample.txt
root@kali:~# chmod +x sample.txt
root@kali:~# ls -l sample.txt
-r-xr-xr-x 1 root root 2052096 Jan 24 03:56 sample.txt
```

**Example 3**

Remove write permissions of a file using symbolic mode.

**Command:** `chmod a-w sample.txt`

**Output:**

```
root@kali:~# ls -l sample.txt
-rwxrwxrwx 1 root root 2052096 Jan 24 03:56 sample.txt
root@kali:~# chmod a-w sample.txt
root@kali:~# ls -l sample.txt
-r-xr-xr-x 1 root root 2052096 Jan 24 03:56 sample.txt
```

You can find more options for ***chown*** command by running the command: `chown –help`

**Example 4**

Add sticky bit to a file using octal and symbolic mode.

**Command:** `chmod +t sample.txt`

**Output:**

```
root@kali:~# ls -l sample.txt
-r-xr-xr-x 1 root root 2052096 Jan 24 03:56 sample.txt
root@kali:~# chmod +t sample.txt
root@kali:~# ls -l sample.txt
-r-xr-xr-t 1 root root 2052096 Jan 24 03:56 sample.txt
```

**Command:** `chmod 1777 sample.txt`

**Output:**

```
root@kali:~# ls -l sample.txt
-rwxr-x--x 1 root root 2052096 Jan 24 03:56 sample.txt
root@kali:~# chmod 1777 sample.txt
root@kali:~# ls -l sample.txt
-rwxrwxrwt 1 root root 2052096 Jan 24 03:56 sample.txt
```

**Example 5**

Add SUID to a file using octal and symbolic mode.

**Command:** `chmod u+s a.txt` **Output:**

```
root@kali:~# chmod u+s a.txt
root@kali:~# ls -ld a.txt
-rwSr--r-- 1 root root 32 Feb  2 23:40 a.txt
```

**Command:** `chmod 4751 a.txt` **Output:**

```
root@kali:~# ls -ld a.txt
-rwsr-x--x 1 root root 32 Feb  2 23:40 a.txt
```

When the file has execute permission, the SUID bit is represented by a lower-case 's'. When the file does not has execute permission, the SUID bit is represented by a upper-case 'S'.

**Example 6**

Add SGID to a file using octal and symbolic mode.

**Command:** `chmod g+s a.txt` **Output:**

```
root@kali:~# ls -l sample.txt
-rwxr-x--x 1 root root 2052096 Jan 24 03:56 sample.txt
root@kali:~# chmod g+s sample.txt
root@kali:~# ls -l sample.txt
-rwxr-s--x 1 root root 2052096 Jan 24 03:56 sample.txt
```

**Command:** `chmod 2751 a.txt` **Output:**

```
root@kali:~# ls -l sample.txt
-rwxr-x--x 1 root root 2052096 Jan 24 03:56 sample.txt
root@kali:~# chmod 2751 sample.txt
root@kali:~# ls -l sample.txt
-rwxr-s--x 1 root root 2052096 Jan 24 03:56 sample.txt
```

When the file has execute permission, the SUID bit is represented by a lower-case 's'. When the file does not has execute permission, the SUID bit is represented by a upper-case 'S'.

You can find more options for ***chmod*** command by running the command: `chmod --help`

| Command | Description |
|---|---|
| ***rm*** | The ***rm*** command is used to remove file or directories |

**Syntax**

```
rm [options] <file or directory name>
```

**Example 1**

Remove the file **sources.list** from **/root/Documents** directory.

**Command:** `rm /root/Documents/sources.list`

**Output:**

```
root@kali:~# rm /root/Documents/sources.list
root@kali:~#
```

**Example 2**

Remove a directory named **test_directory** and all the contents in it.

**Command:** `rm -r test_directory`
**Output:**

```
root@kali:~# rm -r test_directory
```

The **-r** option is used to recursively remove all the contents of a directory

**Example 3**

Force remove a directory named **test_directory** and all the contents in it.

**Command:** `rm -rf test_directory`

**Output:**

```
root@kali:~# rm -rf test_directory
```

The **-f** option is used to force remove files or directories

You can find more options for ***rm*** command by running the command: `rm --help`

## Regular Expressions

| Command | Description |
|---|---|
| *grep* | The ***grep*** command is used to search for patterns in a file or a string |

**Syntax**

```
grep [options] <pattern> <filename>
```

```
cat <filename> | grep <pattern>
```

**Basic Regular Expressions**

| Symbol | Description |
|---|---|
| . | Match any character |
| ^ | Match the start of the string |
| $ | Match the end of the string |
| * | Match zero or more number of preceding characters |
| \ | Represent special character |
| () | Group regular expressions |
| ? | Match exactly one character |
| + | Match one or more number of preceding characters |

**Example 1**

List of the Hotmail email ids.

**Command:** `cat email.txt | grep $'hotmail.com'`

**Output:**

```
root@kali:~# cat email.txt | grep $'hotmail.com'
roy.morty@hotmail.com
ava1929@hotmail.com
1996mia@hotmail.com
kzelxw@hotmail.com
ajsparkchick@hotmail.com
ailuvzhoko4@hotmail.com
richardstalnaker@hotmail.com
kiss.kiss-07@hotmail.com
sup_drake@hotmail.com
hurapa@hotmail.com
paul_biezen@hotmail.com
woogy_83@hotmail.com
rieweria@hotmail.com
madak691@hotmail.com
duncanbladen@hotmail.com
goldbergxue@hotmail.com
semacanar@hotmail.com
carlosrobles777@hotmail.com
chrisman57@hotmail.com
chill_wind@hotmail.com
```

**Example 2**

List the email ids that start with a numeric character.

**Command:** `cat email.txt | grep '^[0-9]'`

**Output:**

```
root@kali:~# cat email.txt | grep '^[0-9]'
1996mia@hotmail.com
```

**Example 3**

List the email ids that has a numeric character in it.

**Command:** `cat email.txt | grep '[0-9]'`

**Output:**

```
root@kali:~# cat email.txt | grep '[0-9]'
olivia.jones1990@yahoo.in
ava1929@hotmail.com
1996mia@hotmail.com
ajhnstn87@gmail.com
ailuvzhoko4@hotmail.com
cottmchl9@gmail.com
s1ck@rediffmail.com
psy_cho182@yahoo.com
patrick96@rogers.com
nakunamen17@yahoo.com
seyenne89@yahoo.com
happydancer13@yahoo.com
valerianx1_032@yahoo.com
elma90016@gmail.com
baby_gurl123@windowslive.com
kiss.kiss-07@hotmail.com
jyaghy13@aol.com
thehelper06@yahoo.com
cmh2021@yahoo.com
ecampbell888@gmail.com
thehelper010@yahoo.com
bravehearted56@yahoo.com
```

**Example 4**

List the email ids whose usernames end with a number.

**Command:** `cat email.txt | grep -E '.+[0-9]+@.+'`

The above command is matched for the pattern where there are one or more number of any characters ('.+'') followed by one or more number of a numeric character ('[0-9]') followed by an **at** symbol ('@') followed by one or more number of any characters.

| | |
|---|---|
| Regex | **.+[0-9]+@.+** |
| Matches | [one or more characters][numberic characters]@[one or more characters] |

**Output:**

```
root@kali:~# cat email.txt | grep -E '.+[0-9]+@.+'
olivia.jones1990@yahoo.in
ava1929@hotmail.com
ajhnstn87@gmail.com
ailuvzhoko4@hotmail.com
cottmchl9@gmail.com
psy_cho182@yahoo.com
patrick96@rogers.com
nakunamen17@yahoo.com
seyenne89@yahoo.com
happydancer13@yahoo.com
valerianx1_032@yahoo.com
elma90016@gmail.com
baby_gurl123@windowslive.com
kiss.kiss-07@hotmail.com
jyaghy13@aol.com
thehelper06@yahoo.com
cmh2021@yahoo.com
ecampbell888@gmail.com
thehelper010@yahoo.com
bravehearted56@yahoo.com
woogy_83@hotmail.com
mastino0105@yahoo.com
```

**Example 5**

List the email ids having three consecutive vowels.

**Command:** `cat email.txt | grep -E '[aeiou]{3}]'`

**Output:**

```
root@kali:~# cat email.txt | grep -E '[aeiou]{3}'
ajmeia@yahoo.com
aituoipiedi78@gmail.com
```

You can find more options for ***grep*** command by running the command: `grep --help`

| Operator | Description |
|---|---|
| \| | The **\| (pipeline)** operator is used to redirect the output of one command as the input to another command |

**Syntax**

```
<command 1> | <command 2>
```

**Example**

**Command:** `cat /etc/hosts | grep root`

**Output:**

```
root@kali:~# cat /etc/passwd | grep root
root:x:0:0:root:/root:/bin/bash
```

## Searching Through File System

| Command | Description |
|---|---|
| *find* | The ***find*** command is used to search for a file or directory based on a pattern |

**Syntax**

```
find [options] [path] <pattern>
```

**Example 1**

Find the file named **resolv.conf**.

**Command:** `find . -name 'resolv.conf'` **Output:**

```
root@kali:/# find . -name 'resolv.conf'
./usr/share/metasploit-framework/vendor/bundle/ruby/2.5.0/gems/dnsruby-1.61.3/te
st/resolv.conf
./usr/lib/systemd/resolv.conf
./run/NetworkManager/resolv.conf
find: './run/user/1001/gvfs': Permission denied
find: './run/user/130/gvfs': Permission denied
./etc/resolv.conf
```

**Example 2**

Find all the files having **txt** extension.

**Command:** `find . -type f -name '*.txt'`

**Output:**

```
root@kali:~# find . -type f -name '*.txt'
./Downloads/BeeLogger/version.txt
./Downloads/BeeLogger/SERVERS-TEMPORARY-UNAVAILABLE-MODULE.txt
./Downloads/.extract/webapps/WebGoat/WEB-INF/lib/placeholder.txt
./Downloads/.extract/webapps/WebGoat/WEB-INF/classes/New Lesson Instructions.txt
./Downloads/.extract/webapps/WebGoat/users/ReadMe.txt
./Downloads/.extract/webapps/WebGoat/plugin_extracted/plugin/XXE/csv/flights.txt
./Downloads/.extract/webapps/WebGoat/plugin_lessons/ReadMe.txt
./Downloads/Zoom/requirements.txt
./.zenmap/recent_scans.txt
./.zenmap/target_list.txt
./sample.txt
./vmware_tools/manifest.txt
./vmware_tools/vmware-tools-distrib/doc/open_source_licenses.txt
./.cache/tracker/parser-version.txt
./.cache/tracker/db-version.txt
./.cache/tracker/locale-for-miner-apps.txt
./.cache/tracker/last-crawl.txt
./.cache/tracker/first-index.txt
./.cache/tracker/db-locale.txt
./.ZAP/licenses/fuzz/dk.brics.automaton-license.txt
./.ZAP/fuzzers/dirbuster/directory-list-1.0.txt
./.ZAP/jbrofuzz/log/28.10.2019-log.txt
./.ZAP/jbrofuzz/log/23.10.2019-log.txt
```

**Example 3**

Find all the files having read, write and execute permission.

**Command:** `find . -type f -perm 777 -print`

**Output:**

```
root@kali:~# find . -type f -perm 777 -print
./Downloads/xampp-linux-x64-7.3.5-1-installer.run
./Downloads/ZAP_2_8_0_unix.sh
root@kali:~# ls -l Downloads/
total 351020
drwxr-xr-x 8 root root      4096 Jul 30  2019 BeeLogger
-rw-r--r-- 1 root root       973 Sep 26 05:33 cacert.der
-rw-r--r-- 1 root root  71627034 Mar 29  2019 Nessus-8.3.0-ubuntu910_amd64.deb
-rw-r--r-- 1 root root       852 Jan 24 02:25 sources.list
-rwxrwxrwx 1 root root 146289715 May 28  2019 xampp-linux-x64-7.3.5-1-installer.run
-rwxrwxrwx 1 root root 141499868 Oct 23 06:45 ZAP_2_8_0_unix.sh
drwxr-xr-x 3 root root      4096 Oct 25 03:23 Zoom
```

**Example 4**

Find all the empty files.

**Command:** `find . -type f -empty`

**Output:**

```
root@kali:~# find . -type f -empty
./Downloads/.extract/logs/webgoat_perf.log
./Downloads/.extract/webapps/WebGoat/WEB-INF/lib/placeholder.txt
./.zenmap/recent_scans.txt
./vmware_tools/vmware-tools-distrib/etc/not_configured
./.ZAP/AcceptedLicense
./.config/chromium/First Run
./.config/chromium/Default/page_load_capping_opt_out.db-journal
./.config/chromium/Default/Web Data-journal
./.config/chromium/Default/Top Sites-journal
./.config/chromium/Default/Cookies-journal
./.config/chromium/Default/Local Storage/leveldb/LOCK
./.config/chromium/Default/Sync Data/LevelDB/LOCK
./.config/chromium/Default/Favicons-journal
./.config/chromium/Default/BudgetDatabase/LOCK
./.config/chromium/Default/BudgetDatabase/000003.log
./.config/chromium/Default/data_reduction_proxy_leveldb/LOCK
./.config/chromium/Default/data_reduction_proxy_leveldb/000003.log
./.config/chromium/Default/Network Action Predictor-journal
./.config/chromium/Default/Site Characteristics Database/LOCK
./.config/chromium/Default/History-journal
./.config/chromium/Default/Service Worker/Database/LOCK
```

You can find more options for ***find*** command by running the command: `find --help`

| Command | Description |
|---|---|
| ***locate*** | The ***locate*** command is used to search for a file by name. The locate command is fast because there is a background process that runs on your system that continuously finds new files and stores them in a database. |

**Syntax**

```
locate [options] <pattern>
```

**Example 1**

Find the file named **resolv.conf**.

**Command:** `locate resolv.conf`

**Output:**

```
root@kali:~# locate resolv.conf
/etc/resolv.conf
/usr/lib/systemd/resolv.conf
/usr/share/man/man5/resolv.conf.5.gz
/usr/share/metasploit-framework/vendor/bundle/ruby/2.5.0/gems/dnsruby-1.61.3/test/resolv.
conf
```

**Example 2**

Print the statistics of your database

**Command:** `locate -S`

**Output:**

```
root@kali:~# locate -S
Database /var/lib/mlocate/mlocate.db:
        34,932 directories
        521,130 files
        29,311,966 bytes in file names
        12,245,781 bytes used to store database
```

You can find more options for ***locate*** command by running the command: `locate --help`

## Operating System and Kernel Information

| Command | Description |
|---|---|
| ***lsb_release*** | The ***lsb_release*** command displays LSB (Linux Standard Base) information about your specific Linux distribution, including version number, release codename, and distributor ID. |

**Syntax**

```
lsb_release [options]
```

**Example 1**

Display the description of the distribution

**Command:** `lsb_release -d`

**Output:**

```
root@kali:/# lsb_release -d
Description:    Kali GNU/Linux Rolling
```

**Example 2**

Display all available information about the distribution

**Command:** `lsb_release -a`

**Output:**

```
root@kali:/# lsb_release -a
No LSB modules are available.
Distributor ID: Kali
Description:    Kali GNU/Linux Rolling
Release:        2019.1
Codename:       n/a
```

You can find more options for ***lsb_release*** command by running the command: `lsb_release --help`

| Command | Description |
|---|---|
| ***uname*** | The ***uname*** command is used to get basic information about the current system. |

**Syntax**

`uname [options]`

**Example 1**

Display the kernel name of the system

**Command:** `uname -s`

**Output:**

```
root@kali:/# uname -s
Linux
```

**Example 2**

Display all basic information about the current system

**Command:** `uname -a`

**Output:**

```
root@kali:/# uname -a
Linux kali 4.19.0-kali1-amd64 #1 SMP Debian 4.19.13-1kali1 (2019-01-03) x86_64 GNU/Linux
```

You can find more options for ***uname*** command by running the command: `uname --help`

## Archive Manager

| Command | Description |
|---|---|
| ***tar*** | The ***tar*** command is used to create archive and extract files from archive. |

**Syntax**

`tar [options] <filename>`

**Example 1**

Extract an archive

**Command:** `tar xvf sample.tar`

**Output:**


Option 'x' represents extract, 'v' represents verbose and 'f' represents file

**Example 2**

Create an archive of all the text files in the directory

**Command:** `tar cvf sample.tar *.txt`

**Output:**


Option 'c' represents create, 'v' represents verbose and 'f' represents file.

You can find more options for ***tar*** command by running the command: `tar –help`

## File Transfer Commands

| Command | Description |
|---|---|
| ***curl*** | The ***curl*** command is used to transfer data from or to a server. |

**Syntax**

```
curl [options] <url>
```

**Example 1**

Download a file from a server

**Command:** `curl -o curl.txt https://curl.haxx.se/`

**Output:**

```
root@kali:~# curl -o curl.txt https://curl.haxx.se/
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  8680  100  8680    0     0   6971      0  0:00:01  0:00:01 --:--:--  6971
```

**Example 2**

Resume a file download

**Command:** `curl -C - -O http://mirrors.estointernet.in/apache/zookeeper/zookeeper-3.4.14/zookeeper-3.4.14.tar.gz`

**Output:**

```
root@kali:~# curl -O http://mirrors.estointernet.in/apache/zookeeper/zookeeper-3.4.14/zoo
keeper-3.4.14.tar.gz
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0 35.9M    0  116k    0     0   212k      0  0:02:52 --:--:--  0:02:52  212k^C
root@kali:~# curl -C - -O http://mirrors.estointernet.in/apache/zookeeper/zookeeper-3.4.1
4/zookeeper-3.4.14.tar.gz
** Resuming transfer from byte position 1503232
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
 83 34.4M   83 28.9M    0     0  2869k      0  0:00:12  0:00:10  0:00:02 3319k^C
```

**Example 3**

Get the cookies from a website

**Command:** `curl --cookie-jar cookie.txt http://www.edureka.co/index.html -O`

**Output:**

```
root@kali:~# curl --cookie-jar cookie.txt http://www.edureka.co/index.html -O
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   321  100   321    0     0    407      0 --:--:-- --:--:-- --:--:--   407
root@kali:~# cat cookie.txt
# Netscape HTTP Cookie File
# https://curl.haxx.se/docs/http-cookies.html
# This file was generated by libcurl! Edit at your own risk.
```

You can find more options for ***curl*** command by running the command: `curl --help`

| Command | Description |
|---|---|
| ***wget*** | The ***wget*** command is used to retrieve files using the most widely used Internet protocols. |

**Syntax**

```
wget [options] <url>
```

**Example 1**

Download a file from a server

**Command:** `wget http://ftp.gnu.org/gnu/wget/wget-1.5.3.tar.gz`

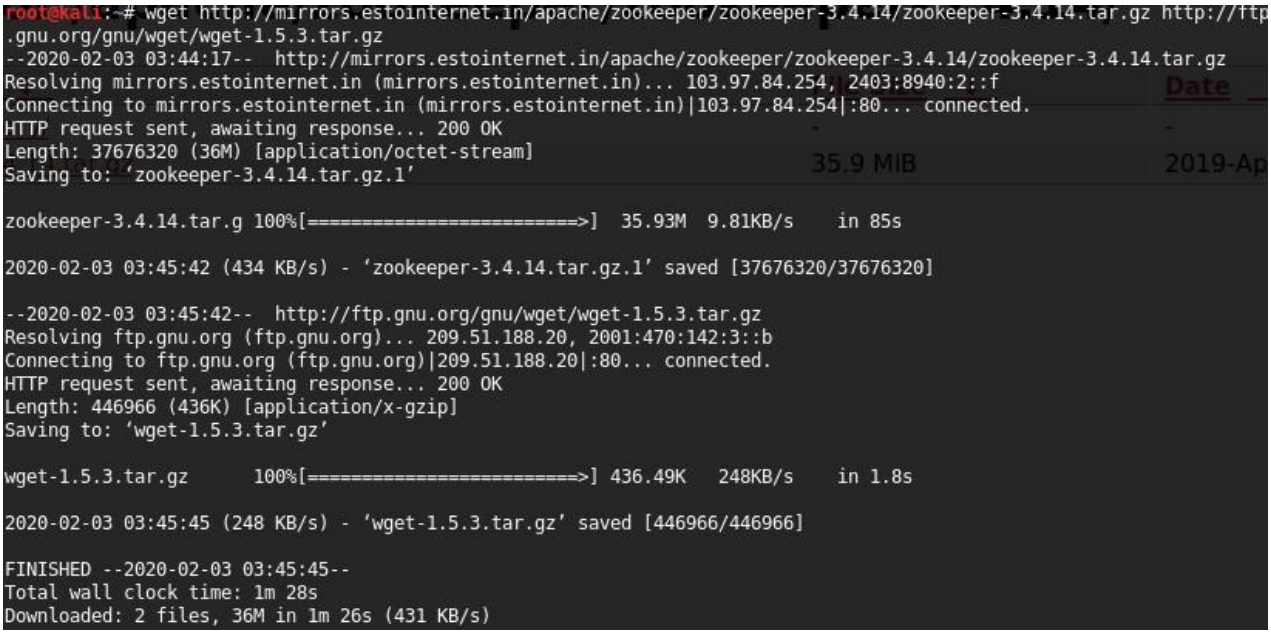
**Output:**


**Example 2**

Download multiple files at a time

**Command:** `wget http://mirrors.estointernet.in/apache/zookeeper/zookeeper3.4.14/zookeeper-3.4.14.tar.gz http://ftp.gnu.org/gnu/wget/wget-1.5.3.tar.gz`

**Output:**

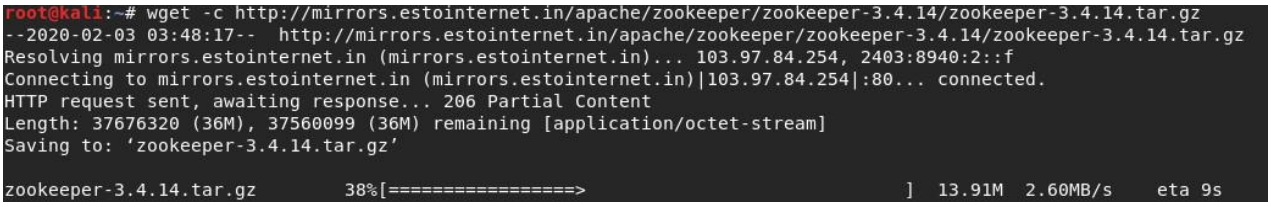


**Example 3**

Resume a file download

**Command:** `wget -c http://mirrors.estointernet.in/apache/zookeeper/zookeeper-3.4.14/zookeeper-3.4.14.tar.gz`

**Output:**

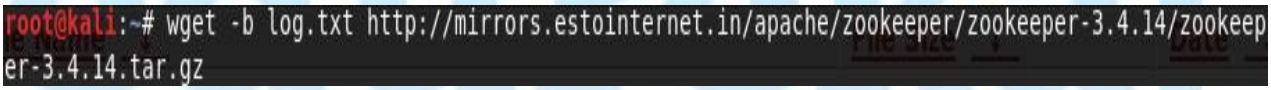



**Example 4**

Download file in the background

**Command:** `wget -b log.txt http://mirrors.estointernet.in/apache/zookeeper/zookeeper-3.4.14/zookeeper-3.4.14.tar.gz`

**Output:**

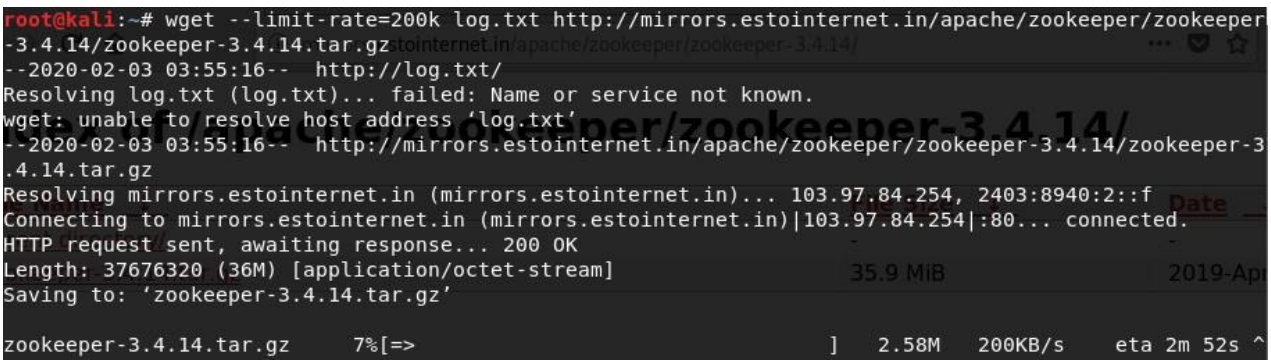



**Example 5**

Limit the download speed

**Command:** `wget --limit-rate=200k log.txt http://mirrors.estointernet.in/apache/zookeeper/zookeeper-3.4.14/zookeeper-3.4.14.tar.gz`

**Output:**



You can find more options for ***wget*** command by running the command: `wget --help`

## Users and User Management

| Command | Description |
|---|---|
| ***who*** | The ***who*** command is used to display user information such as time of last system boot, current run level of the system, list of logged in users, etc. |

**Syntax**

```
who [options] [file | Arg1 Arg2]
```

**Example 1**

**Command:** `who`

**Output:**

```
root@kali:/# who
root     :1           2020-01-27 23:44 (:1)
edureka  :2           2020-01-27 23:59 (:2)
```

**Example 2**

Show the time when the system last booted

**Command:** `who -b -H`

**Output:**

```
root@kali:/# who -b -H
NAME     LINE         TIME                 PID COMMENT
         system boot  2020-01-27 23:42
```

**Example 2**

Show the username of the current user who has invoked this command.

**Command:** `whoami`

**Output:**

```
root@kali:~# whoami
root
```

You can find more options for ***who*** command by running the command: `who --help`

| Command | Description |
|---|---|
| ***adduser*** | The ***adduser*** command is used to add a user to the system |

**Syntax**

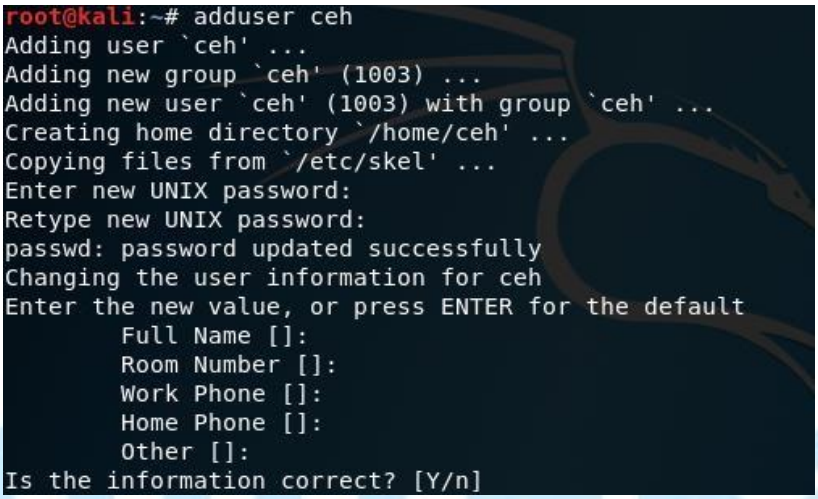
```
adduser [options] <username>
```

**Example 1**

Add a user to the system

**Command:** `adduser ceh`

**Output:**

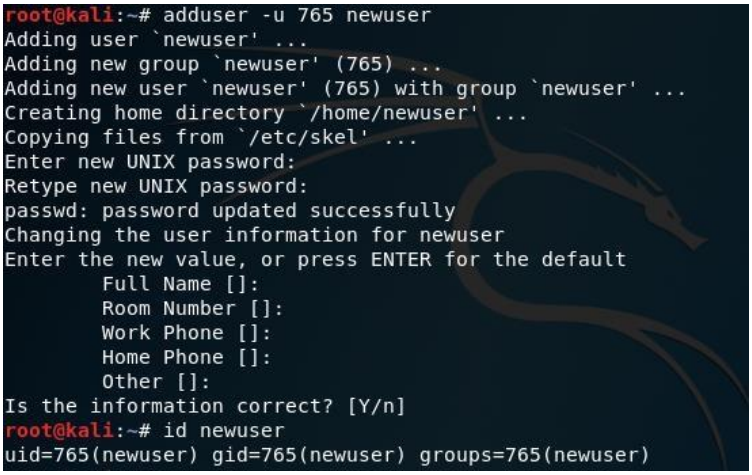



**Example 2**

Add a user to the system with uid 765

**Command:** `adduser -u 765 newuser`

**Output:**




You can find more options for ***adduser*** command by running the command: `adduser --help`

| Command | Description |
|---|---|
| ***addgroup*** | The ***addgroup*** command is used to add a group to the system |

**Syntax**

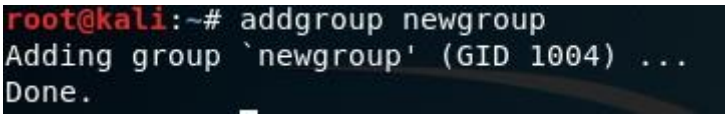
```
addgroup [options] <groupname>
```

**Example**

Add a group to the system

**Command:** `addgroup newgroup`

**Output:**




You can find more options for ***addgroup*** command by running the command: `addgroup --help`

| Command | Description |
|---|---|
| ***passwd*** | The ***passwd*** command is used to change a user's password & manage the user's validity |

**Syntax**

```
passwd [options] [login]
```

**Example 1**

Change password of a user

**Command:** `passwd ceh`

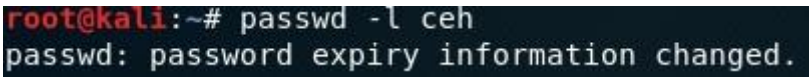
**Output:**


**Example 2**

Disable a user account **Command:**

```
passwd -l ceh
```

**Output:**



**Example 3**

Enable a user account

**Command:** `passwd -u ceh`

**Output:**

```
root@kali:~# passwd -u ceh
passwd: password expiry information changed.
```

**Example 4**

Delete a user account

**Command:** `passwd -d ceh`

**Output:**

```
root@kali:~# passwd -d ceh
passwd: password expiry information changed.
```

You can find more options for ***passwd*** command by running the command: `passwd --help`

| Command | Description |
|---|---|
| ***usermod*** | The ***usermod*** command is used to modify a user account |

**Syntax**

```
usermod [options] [login]
```

**Example 1**

Add a user to a group

**Command:** `usermod -a -G <groupname> <username>`

**Output:**

```
root@kali:~# usermod -a -G edureka edureka
```

**Example 2**

Change the expiry date of a user

**Command:** `usermod -e 2020-12-31 edureka`

**Output:**

```
root@kali:~# usermod -e 2021-12-31 edureka
root@kali:~# chage -l edureka
Last password change                                    : Jan 24, 2020
Password expires                                        : never
Password inactive                                       : never
Account expires                                         : Dec 31, 2021
Minimum number of days between password change          : 0
Maximum number of days between password change          : 99999
Number of days of warning before password expires       : 7
```

**Example 3**

Change the login username of a user

**Command:** `usermod -l new_edureka edureka`

**Output:**

```
root@kali:~# usermod -l new_edureka edureka
```

**Example 4**

Lock user account

**Command:** `usermod -L edureka`

**Output:**

```
root@kali:~# cat /etc/shadow | grep new_edureka
new_edureka:$6$v2s4xMvE$.2tCYTlYX3fgvm1Kcbol.IHWU7GvrPdWTB5xTQwSfeBH.Z3ZkjUyOBQEBsxsovewl
LaT5Y6DSo5sNggD7pCYM/:18285:0:99999:7::18992:
root@kali:~# usermod -L new_edureka
root@kali:~# cat /etc/shadow | grep new_edureka
new_edureka:!$6$v2s4xMvE$.2tCYTlYX3fgvm1Kcbol.IHWU7GvrPdWTB5xTQwSfeBH.Z3ZkjUyOBQEBsxsovew
lLaT5Y6DSo5sNggD7pCYM/:18285:0:99999:7::18992:
```

The exclamatory mark (!) after the username indicates that the user is locked.

**Example 5**

Unlock user account

**Command:** `usermod -U edureka` **Output:**

```
root@kali:~# cat /etc/shadow | grep new_edureka
new_edureka:!$6$v2s4xMvE$.2tCYTlYX3fgvm1Kcbol.IHWU7GvrPdWTB5xTQwSfeBH.Z3ZkjUyOBQEBsxsovew
lLaT5Y6DSo5sNggD7pCYM/:18285:0:99999:7::18992:
root@kali:~# usermod -U new_edureka
root@kali:~# cat /etc/shadow | grep new_edureka
new_edureka:$6$v2s4xMvE$.2tCYTlYX3fgvm1Kcbol.IHWU7GvrPdWTB5xTQwSfeBH.Z3ZkjUyOBQEBsxsovewl
LaT5Y6DSo5sNggD7pCYM/:18285:0:99999:7::18992:
```

You can find more options for ***usermod*** command by running the command: `usermod --help`

| Command | Description |
|---|---|
| ***groupmod*** | The ***groupmod*** command is used to modify a group in the system |

**Syntax**

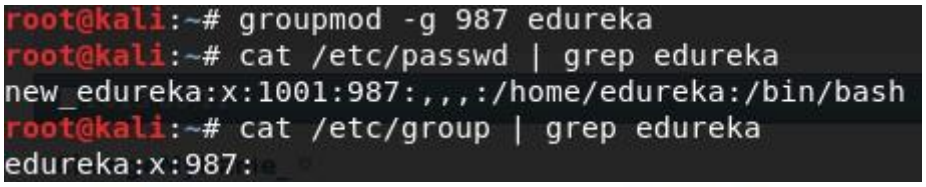
```
groupmod [options] <groupname>
```

**Example 1**

Change the GID of a group

**Command:** `groupmod -g 987 edureka`

**Output:**

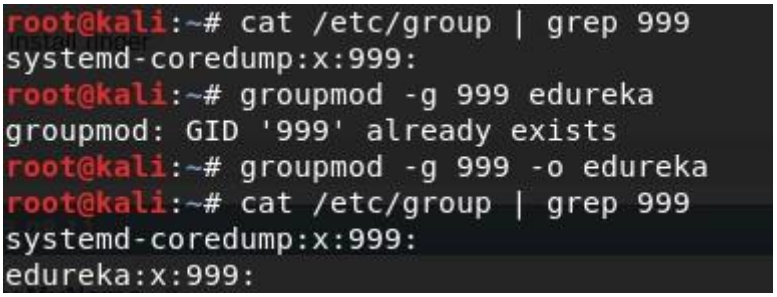



**Example 2**

Assign an existing GID to another group

**Command:** `groupmod -g 999 -o edureka`

**Output:**




| Command | Description |
|---|---|
| ***deluser*** | The ***deluser*** command is used to delete a user or group from the system |

**Syntax**

```
deluser [options] [login]
```

**Example**

Remove a user from a group

**Command:** `deluser <username> <groupname>`
**Output:**

```
root@kali:~# deluser edu edureka
Removing user `edu' from group `edureka' ...
Done.
root@kali:~#
```

You can find more options for ***deluser*** command by running the command: `deluser --help`

| Command | Description |
|---|---|
| ***id*** | The ***id*** command is used to get the information about the user and the group |

**Syntax**

```
id [options] [user]
```

**Example**

Print the user and group information

**Command:** `id`

**Output:**

```
root@kali:~# id
uid=0(root) gid=0(root) groups=0(root)
```

## Process Management

| Command | Description |
|---|---|
| ***ps*** | The ***ps*** command is used to fetch information about the active processes |

**Syntax**

```
ps [options]
```

**Example 1**

List the running processes.

**Command:** `ps`

**Output:**

```
root@kali:~# ps
  PID TTY          TIME CMD
 1478 pts/0    00:00:00 bash
 1723 pts/0    00:00:00 ps
root@kali:~#
```

**Example 2**

Display full information about the running processes.

**Command:** `ps -f`

**Output:**

```
root@kali:~# ps -f
UID          PID  PPID  C STIME TTY          TIME CMD
root        1478  1471  0 06:13 pts/0    00:00:00 bash
root        1733  1478  0 06:25 pts/0    00:00:00 ps -f
root@kali:~#
```

**Example 2**

Display process in BSD format.

**Command:** `ps aux`

**Output:**

```
root@kali:~# ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.1 182016  8956 ?        Ss   Feb02   0:09 /sbin/init
root           2  0.0  0.0      0     0 ?        S    Feb02   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   Feb02   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   Feb02   0:00 [rcu_par_gp]
root           6  0.0  0.0      0     0 ?        I<   Feb02   0:00 [kworker/0:0H-kblockd]
root           8  0.0  0.0      0     0 ?        I<   Feb02   0:00 [mm_percpu_wq]
root           9  0.0  0.0      0     0 ?        S    Feb02   0:00 [ksoftirqd/0]
root          10  0.0  0.0      0     0 ?        I    Feb02   0:06 [rcu_sched]
root          11  0.0  0.0      0     0 ?        I    Feb02   0:00 [rcu_bh]
root          12  0.0  0.0      0     0 ?        S    Feb02   0:00 [migration/0]
root          14  0.0  0.0      0     0 ?        S    Feb02   0:00 [cpuhp/0]
root          15  0.0  0.0      0     0 ?        S    Feb02   0:00 [cpuhp/1]
root          16  0.0  0.0      0     0 ?        S    Feb02   0:00 [migration/1]
root          17  0.0  0.0      0     0 ?        S    Feb02   0:00 [ksoftirqd/1]
root          19  0.0  0.0      0     0 ?        I<   Feb02   0:00 [kworker/1:0H-kblockd]
root          20  0.0  0.0      0     0 ?        S    Feb02   0:00 [cpuhp/2]
root          21  0.0  0.0      0     0 ?        S    Feb02   0:00 [migration/2]
root          22  0.0  0.0      0     0 ?        S    Feb02   0:00 [ksoftirqd/2]
root          24  0.0  0.0      0     0 ?        I<   Feb02   0:00 [kworker/2:0H-kblockd]
root          25  0.0  0.0      0     0 ?        S    Feb02   0:00 [cpuhp/3]
root          26  0.0  0.0      0     0 ?        S    Feb02   0:00 [migration/3]
```

**Example 3**

Display process running as root.

**Command:** `ps -U root -u root`

**Output:**

```
root@kali:~# ps -U root -u root
  PID TTY          TIME CMD
    1 ?        00:00:09 systemd
    2 ?        00:00:00 kthreadd
    3 ?        00:00:00 rcu_gp
    4 ?        00:00:00 rcu_par_gp
    6 ?        00:00:00 kworker/0:0H-kblockd
    8 ?        00:00:00 mm_percpu_wq
    9 ?        00:00:00 ksoftirqd/0
   10 ?        00:00:06 rcu_sched
   11 ?        00:00:00 rcu_bh
   12 ?        00:00:00 migration/0
   14 ?        00:00:00 cpuhp/0
   15 ?        00:00:00 cpuhp/1
   16 ?        00:00:00 migration/1
   17 ?        00:00:00 ksoftirqd/1
   19 ?        00:00:00 kworker/1:0H-kblockd
   20 ?        00:00:00 cpuhp/2
   21 ?        00:00:00 migration/2
   22 ?        00:00:00 ksoftirqd/2
   24 ?        00:00:00 kworker/2:0H-kblockd
   25 ?        00:00:00 cpuhp/3
   26 ?        00:00:00 migration/3
   27 ?        00:00:02 ksoftirqd/3
```

**Example 4**

Display process in a tree format.

**Command:** `ps -e --forest`

**Output:**

```
root@kali:~# ps -e --forest
  PID TTY          TIME CMD
    2 ?        00:00:00 kthreadd
    3 ?        00:00:00  \_ rcu_gp
    4 ?        00:00:00  \_ rcu_par_gp
    6 ?        00:00:00  \_ kworker/0:0H-kblockd
    8 ?        00:00:00  \_ mm_percpu_wq
    9 ?        00:00:00  \_ ksoftirqd/0
   10 ?        00:00:06  \_ rcu_sched
   11 ?        00:00:00  \_ rcu_bh
   12 ?        00:00:00  \_ migration/0
   14 ?        00:00:00  \_ cpuhp/0
   15 ?        00:00:00  \_ cpuhp/1
   16 ?        00:00:00  \_ migration/1
   17 ?        00:00:00  \_ ksoftirqd/1
   19 ?        00:00:00  \_ kworker/1:0H-kblockd
   20 ?        00:00:00  \_ cpuhp/2
   21 ?        00:00:00  \_ migration/2
   22 ?        00:00:00  \_ ksoftirqd/2
   24 ?        00:00:00  \_ kworker/2:0H-kblockd
   25 ?        00:00:00  \_ cpuhp/3
   26 ?        00:00:00  \_ migration/3
   27 ?        00:00:02  \_ ksoftirqd/3
   29 ?        00:00:00  \_ kworker/3:0H-kblockd
```

**Example 5**

Display process in the format pid, ppid and command

**Command:** `ps -eo pid,ppid,cmd`

**Output:**


**Example 6**

Display the process name of a pid

**Command:** `ps -p 6666 -o comm=`

**Output:**


**Example 7**

Display the process execution time

**Command:** `ps -eo pid,comm,etime`

**Output:**

```
root@kali:~# ps -eo pid,comm,etime
  PID COMMAND                 ELAPSED
    1 systemd                 08:52:34
    2 kthreadd                08:52:34
    3 rcu_gp                  08:52:34
    4 rcu_par_gp              08:52:34
    6 kworker/0:0H-kb         08:52:34
    8 mm_percpu_wq            08:52:34
    9 ksoftirqd/0             08:52:34
   10 rcu_sched               08:52:34
   11 rcu_bh                  08:52:34
   12 migration/0             08:52:34
   14 cpuhp/0                 08:52:34
   15 cpuhp/1                 08:52:34
   16 migration/1             08:52:34
   17 ksoftirqd/1             08:52:34
   19 kworker/1:0H-kb         08:52:34
   20 cpuhp/2                 08:52:34
   21 migration/2             08:52:34
   22 ksoftirqd/2             08:52:34
   24 kworker/2:0H-kb         08:52:34
   25 cpuhp/3                 08:52:34
   26 migration/3             08:52:34
```

**Example 7**

Display all the threads of a process.

**Command:** `ps -eLF`

**Output:**

```
root@kali:~# ps -eLF
UID          PID  PPID   LWP  C NLWP    SZ   RSS PSR STIME TTY          TIME CMD
root           1     0     1  0    1 45504  8980   2 Feb02 ?        00:00:10 /sbin/init
root           2     0     2  0    1     0     0   2 Feb02 ?        00:00:00 [kthreadd]
root           3     2     3  0    1     0     0   0 Feb02 ?        00:00:00 [rcu_gp]
root           4     2     4  0    1     0     0   0 Feb02 ?        00:00:00 [rcu_par_gp]
root           6     2     6  0    1     0     0   0 Feb02 ?        00:00:00 [kworker/0:0H-kblockd]
root           8     2     8  0    1     0     0   0 Feb02 ?        00:00:00 [mm_percpu_wq]
root           9     2     9  0    1     0     0   0 Feb02 ?        00:00:00 [ksoftirqd/0]
root          10     2    10  0    1     0     0   1 Feb02 ?        00:00:10 [rcu_sched]
root          11     2    11  0    1     0     0   0 Feb02 ?        00:00:00 [rcu_bh]
root          12     2    12  0    1     0     0   0 Feb02 ?        00:00:00 [migration/0]
root          14     2    14  0    1     0     0   0 Feb02 ?        00:00:00 [cpuhp/0]
root          15     2    15  0    1     0     0   1 Feb02 ?        00:00:00 [cpuhp/1]
root          16     2    16  0    1     0     0   1 Feb02 ?        00:00:00 [migration/1]
root          17     2    17  0    1     0     0   1 Feb02 ?        00:00:00 [ksoftirqd/1]
root          19     2    19  0    1     0     0   1 Feb02 ?        00:00:00 [kworker/1:0H-kblockd]
root          20     2    20  0    1     0     0   2 Feb02 ?        00:00:00 [cpuhp/2]
root          21     2    21  0    1     0     0   2 Feb02 ?        00:00:00 [migration/2]
root          22     2    22  0    1     0     0   2 Feb02 ?        00:00:00 [ksoftirqd/2]
root          24     2    24  0    1     0     0   2 Feb02 ?        00:00:00 [kworker/2:0H-kblockd]
root          25     2    25  0    1     0     0   3 Feb02 ?        00:00:00 [cpuhp/3]
root          26     2    26  0    1     0     0   3 Feb02 ?        00:00:00 [migration/3]
```

You can find more options for ***ps*** command by running the command: `ps --help`

| Command | Description |
|---|---|
| ***kill*** | The ***kill*** command is used to terminate a process |

**Syntax**

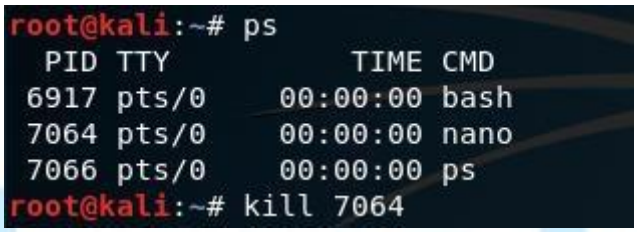
```
kill [options] <pid>
```

**Example 1**

Kill a process

**Command:** `kill 7064`

**Output:**

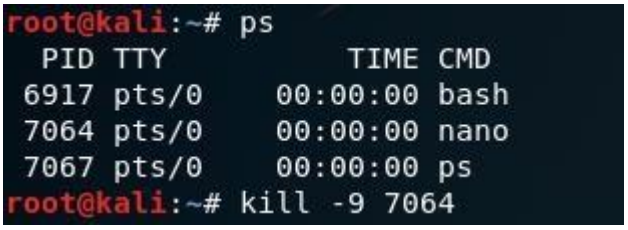



**Example 2**

Force kill a process

**Command:** `kill -9 7064`

**Output:**




You can find more options for ***kill*** command by running the command: `kill --help`

| Command | Description |
|---|---|
| ***lsof*** | The ***lsof*** command is used to list open files |

**Syntax**

```
lsof [options] [names]
```

**Example 1**

List all the files opened by root

**Command:** `lsof -u root`

**Output:**

```
root@kali:~# lsof -u root
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/130/gvfs
      Output information may be incomplete.
COMMAND    PID USER   FD      TYPE             DEVICE  SIZE/OFF       NODE NAME
systemd      1 root  cwd       DIR                8,1     36864          2 /
systemd      1 root  rtd       DIR                8,1     36864          2 /
systemd      1 root  txt       REG                8,1   1476920    1182354 /usr/lib/systemd/systemd
systemd      1 root  mem       REG                8,1   1325424    1180465 /usr/lib/x86_64-linux-gnu/
libm-2.29.so
systemd      1 root  mem       REG                8,1    149704    1185892 /usr/lib/x86_64-linux-gnu/
libudev.so.1.6.12
systemd      1 root  mem       REG                8,1    137424    1184729 /usr/lib/x86_64-linux-gnu/
libgpg-error.so.0.25.0
systemd      1 root  mem       REG                8,1     43304    1185009 /usr/lib/x86_64-linux-gnu/
libjson-c.so.3.0.1
systemd      1 root  mem       REG                8,1     34904    1184071 /usr/lib/x86_64-linux-gnu/
libargon2.so.1
systemd      1 root  mem       REG                8,1    432664    1184376 /usr/lib/x86_64-linux-gnu/
libdevmapper.so.1.02.1
systemd      1 root  mem       REG                8,1     30776    1185941 /usr/lib/x86_64-linux-gnu/
libuuid.so.1.3.0
systemd      1 root  mem       REG                8,1     18832    1184101 /usr/lib/x86_64-linux-gnu/
libattr.so.1.1.0
systemd      1 root  mem       REG                8,1     22880    1184231 /usr/lib/x86_64-linux-gnu/
```

**Example 2**

List all the files opened by a process.

**Command:** `lsof -c gdm3`

**Output:**

```
root@kali:~# lsof -c gdm3
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/130/gvfs
      Output information may be incomplete.
COMMAND  PID USER   FD      TYPE             DEVICE SIZE/OFF    NODE NAME
gdm3    1846 root  cwd       DIR                8,1     36864       2 /
gdm3    1846 root  rtd       DIR                8,1     36864       2 /
gdm3    1846 root  txt       REG                8,1    428416 1061962 /usr/sbin/gdm3
gdm3    1846 root  mem       REG                8,1     51696 1180471 /usr/lib/x86_64-linux-gnu/libnss
_files-2.29.so
gdm3    1846 root  mem       REG                8,1    337024 1703954 /usr/lib/locale/aa_DJ.utf8/LC_CT
YPE
gdm3    1846 root  mem       REG                8,1   2586242 1703953 /usr/lib/locale/aa_DJ.utf8/LC_CO
LLATE
gdm3    1846 root  mem       REG                8,1     30776 1185941 /usr/lib/x86_64-linux-gnu/libuui
d.so.1.3.0
gdm3    1846 root  mem       REG                8,1    137424 1184729 /usr/lib/x86_64-linux-gnu/libgpg
-error.so.0.25.0
gdm3    1846 root  mem       REG                8,1    343008 1184166 /usr/lib/x86_64-linux-gnu/libblk
id.so.1.1.0
gdm3    1846 root  mem       REG                8,1   1168056 1184624 /usr/lib/x86_64-linux-gnu/libgcr
ypt.so.20.2.4
gdm3    1846 root  mem       REG                8,1    121184 1185134 /usr/lib/x86_64-linux-gnu/liblz4
.so.1.8.3
```

**Example 3**

List all the files opened by a particular process using its PID

**Command:** `lsof -p 6666`

**Output:**

```
root@kali:~# lsof -p 6666
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/130/gvfs
      Output information may be incomplete.
COMMAND    PID USER   FD      TYPE DEVICE SIZE/OFF NODE NAME
kworker/3 6666 root  cwd       DIR    8,1    36864    2 /
kworker/3 6666 root  rtd       DIR    8,1    36864    2 /
kworker/3 6666 root  txt   unknown                     /proc/6666/exe
```

**Example 5**

List all the files opened by network connections

**Command:** `lsof -i`

**Output:**

```
root@kali:~# lsof -i
COMMAND    PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
dhclient 1893 root    6u  IPv4  43696      0t0  UDP *:bootpc
```

You can find more options for ***lsof*** command by running the command: `lsof --help`

## Service Management

| Command | Description |
|---|---|
| *service* | The ***service*** command is used to manage services |

**Syntax**

```
service script command [options]
```

**Example 1**

Start a service

**Command:** `service apache2 start`

**Output:**

```
root@kali:~# service apache2 start
```

**Example 2**

Restart a service

**Command:** `service apache2 restart`

**Output:**

```
root@kali:~# service apache2 restart
```

**Example 3**

Check the status of a service

**Command:** `service apache2 status`

**Output:**

```
root@kali:~# service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset:
   Active: active (running) since Fri 2020-01-10 06:41:05 EST; 1min 23s ago
  Process: 3462 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCE
 Main PID: 3466 (apache2)
    Tasks: 7 (limit: 4679)
   Memory: 13.2M
   CGroup: /system.slice/apache2.service
           ├─3466 /usr/sbin/apache2 -k start
           ├─3467 /usr/sbin/apache2 -k start
           ├─3468 /usr/sbin/apache2 -k start
           ├─3469 /usr/sbin/apache2 -k start
           ├─3470 /usr/sbin/apache2 -k start
           ├─3471 /usr/sbin/apache2 -k start
           └─3472 /usr/sbin/apache2 -k start

Jan 10 06:41:05 kali systemd[1]: Starting The Apache HTTP Server...
Jan 10 06:41:05 kali apachectl[3462]: AH00558: apache2: Could not reliably deter
Jan 10 06:41:05 kali systemd[1]: Started The Apache HTTP Server.
```

**Example 4**

Stop a service

**Command:** `service apache2 stop`

**Output:**

```
root@kali:~# service apache2 stop
```

You can find more options for ***service*** command by running the command: `service --help`

| Command | Description |
|---|---|
| ***Systemctl*** | The ***systemctl*** command is used to control the system and service manager |

**Syntax**

```
systemctl [options] command [unit]
```

**Example 1**

Start a service

**Command:** `systemctl start apache2`

**Output:**

```
root@kali:~# systemctl start apache2
```

**Example 2**

Stop a service

**Command:** `systemctl stop apache2`

**Output:**

```
root@kali:~# systemctl stop apache2
```

**Example 3**

Check the status of a service

**Command:** `systemctl status apache2`

**Output:**

```
root@kali:~# systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset:
   Active: inactive (dead)

Jan 10 06:43:35 kali apachectl[3531]: AH00558: apache2: Could not reliably deter
Jan 10 06:43:35 kali systemd[1]: apache2.service: Succeeded.
Jan 10 06:43:35 kali systemd[1]: Stopped The Apache HTTP Server.
Jan 10 06:44:54 kali systemd[1]: Starting The Apache HTTP Server...
Jan 10 06:44:54 kali apachectl[3539]: AH00558: apache2: Could not reliably deter
Jan 10 06:44:54 kali systemd[1]: Started The Apache HTTP Server.
Jan 10 06:45:45 kali systemd[1]: Stopping The Apache HTTP Server...
Jan 10 06:45:45 kali apachectl[3557]: AH00558: apache2: Could not reliably deter
Jan 10 06:45:45 kali systemd[1]: apache2.service: Succeeded.
Jan 10 06:45:45 kali systemd[1]: Stopped The Apache HTTP Server.
lines 1-14/14 (END)
```

**Example 4**

Enable a service

**Command:** `systemctl enable apache2`

**Output:**

```
root@kali:~# systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /lib/system
d/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable apache2
```

**Example 5**

Disable a service

**Command:** `systemctl disable apache2`

**Output:**

```
root@kali:~# systemctl disable apache2
Synchronizing state of apache2.service with SysV service script with /lib/system
d/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable apache2
Removed /etc/systemd/system/multi-user.target.wants/apache2.service.
```

You can find more options for ***systemctl*** command by running the command: `systemctl --help`

edureka!

© Brain4ce Education Solutions Pvt. Ltd.