NAME:Mukundhan
REG.NO:20BCI0291

Title: Linux Command List Assessment

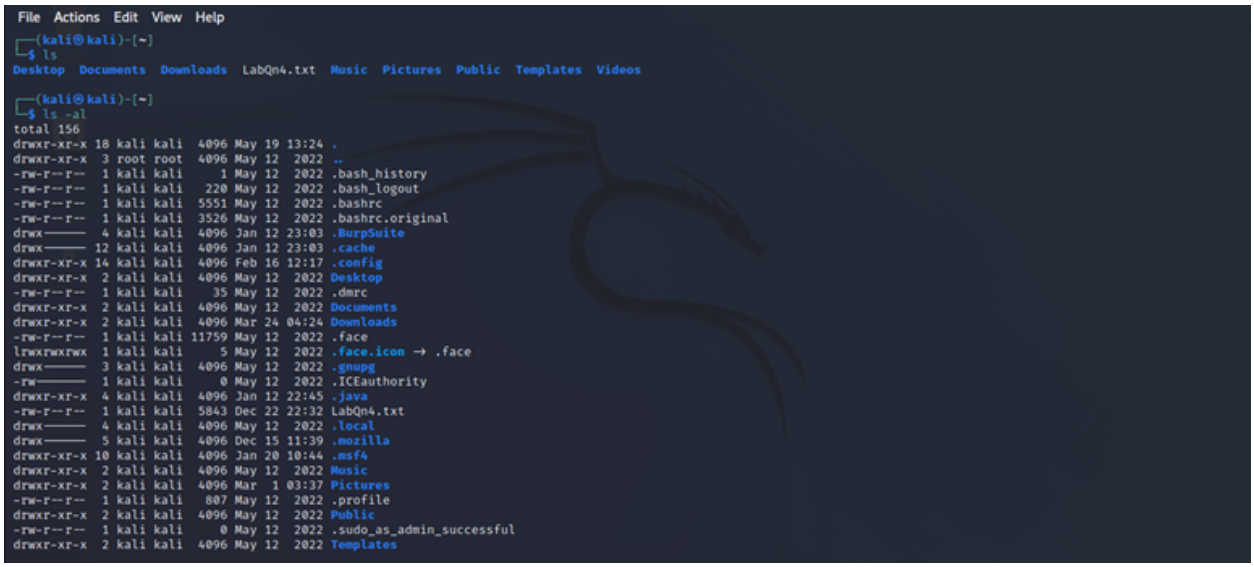
Instructions:-

The following assessment aims to test your understanding and practical knowledge of various Linux commands. Perform the tasks given below using the appropriate commands. Write down the command(s) used to complete each task. You can use any Linux distribution or command-line interface of your choice. Ensure that you provide the correct output or results for each task.

Note: It is recommended to perform this assessment on a Linux machine or virtual environment.

File and Directory Operations:

ls: List files and directories



cd: Change directory

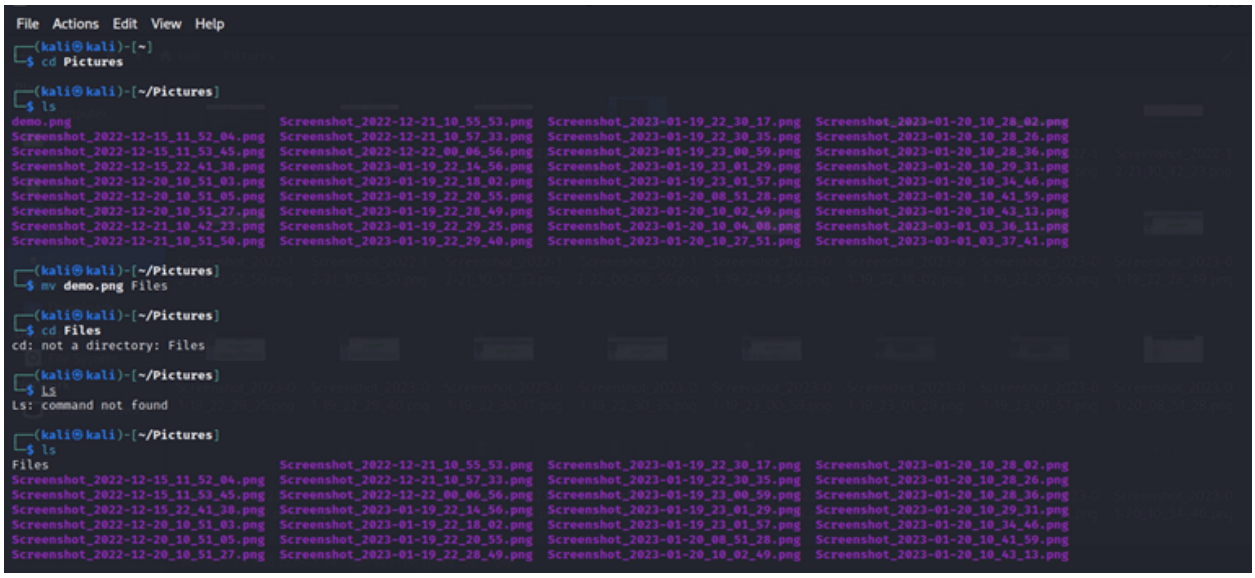
pwd: Print working directory

mkdir: Make directory

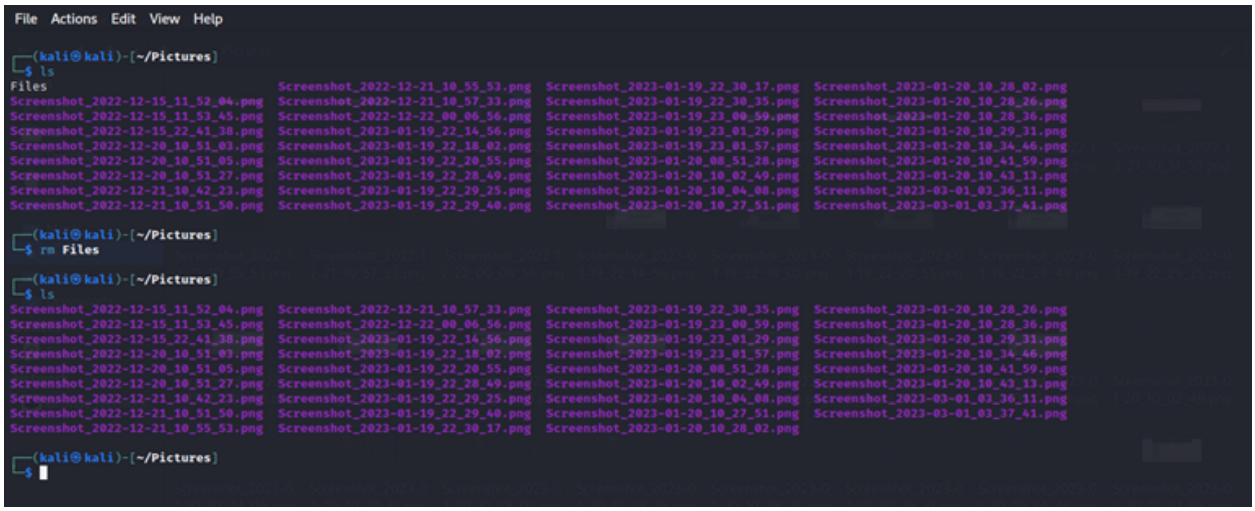
touch: Create an empty file

cp: Copy files and directories

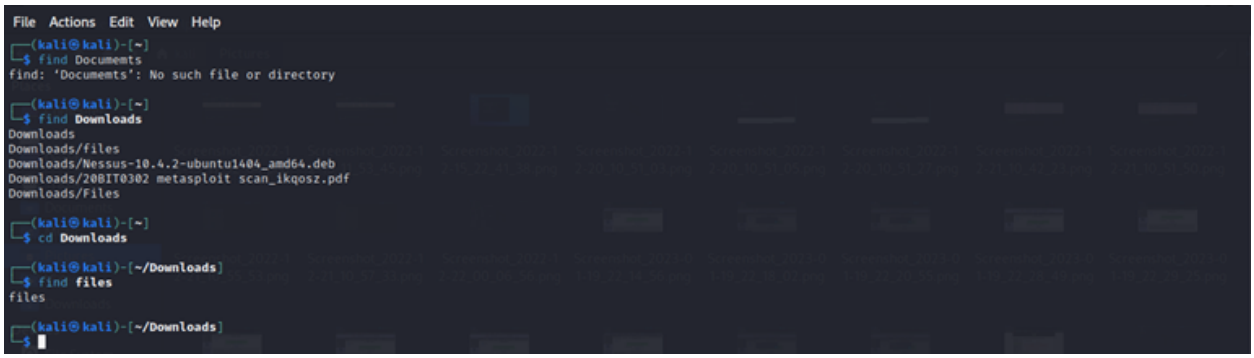
mv: Move or rename files and directories



rm: Remove files and directories



find: Search for files and directories



File Viewing and Editing:

cat: Concatenate and display file content

less: View file content with pagination

```
File  Actions  Edit  View  Help
- Nikto v2.1.6/2.1.5
+ Target Host: 192.168.50.129
+ Target Port: 80
+ GET Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ GET The anti-clickjacking X-Frame-Options header is not present.
+ GET The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ GET The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ GET Uncommon header 'tcn' found, with contents: list
+ GET Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15.
 The following alternatives for 'index' were found: index.php
+ HEAD Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ ZXSTAXFW Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: TRACE HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ GET /phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-3268: GET /doc/: Directory indexing found.
+ OSVDB-48: GET /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-12184: GET /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY str
ings.
+ OSVDB-12184: GET /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY str
ings.
+ OSVDB-12184: GET /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY str
ings.
+ OSVDB-12184: GET /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY str
ings.
+ OSVDB-3092: GET /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ GET Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec  9 12:24:00 2008
+ OSVDB-3092: GET /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3268: GET /test/: Directory indexing found.
+ OSVDB-3092: GET /test/: This might be interesting...
+ OSVDB-3233: GET /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information.
+ OSVDB-3268: GET /icons/: Directory indexing found.
+ OSVDB-3233: GET /icons/README: Apache default file found.
+ GET /phpMyAdmin/: phpMyAdmin directory found
+ OSVDB-3092: GET /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
LabQn4.txt
```

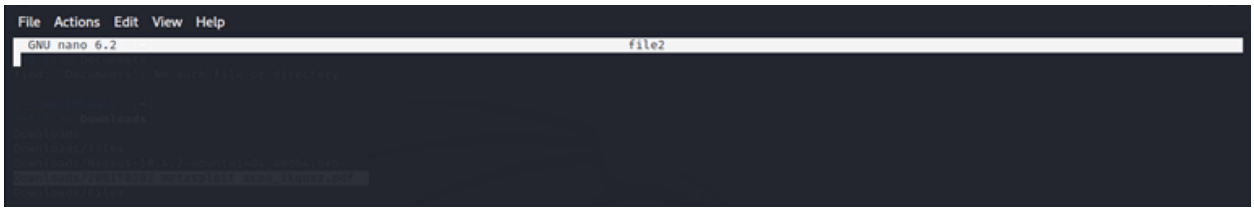
head: Display the beginning of a file

```
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ head -- LabQn4.txt
- Nikto v2.1.6/2.1.5
+ Target Host: 192.168.50.129
+ Target Port: 80
+ GET Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ GET The anti-clickjacking X-Frame-Options header is not present.
+ GET The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ GET The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ GET Uncommon header 'tcn' found, with contents: list
+ GET Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15.
 The following alternatives for 'index' were found: index.php
+ HEAD Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.

┌──(kali㉿kali)-[~]
└─$
```

tail: Display the end of a file

```
┌──(kali㉿kali)-[~]
└─$ tail -- LabQn4.txt
+ OSVDB-12184: GET /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY str
ings.
+ OSVDB-12184: GET /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY str
ings.
+ OSVDB-3092: GET /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ GET Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec  9 12:24:00 2008
+ OSVDB-3092: GET /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3268: GET /test/: Directory indexing found.
+ OSVDB-3092: GET /test/: This might be interesting...
+ OSVDB-3233: GET /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information.
+ OSVDB-3268: GET /icons/: Directory indexing found.
+ OSVDB-3233: GET /icons/README: Apache default file found.

┌──(kali㉿kali)-[~]
└─$
```

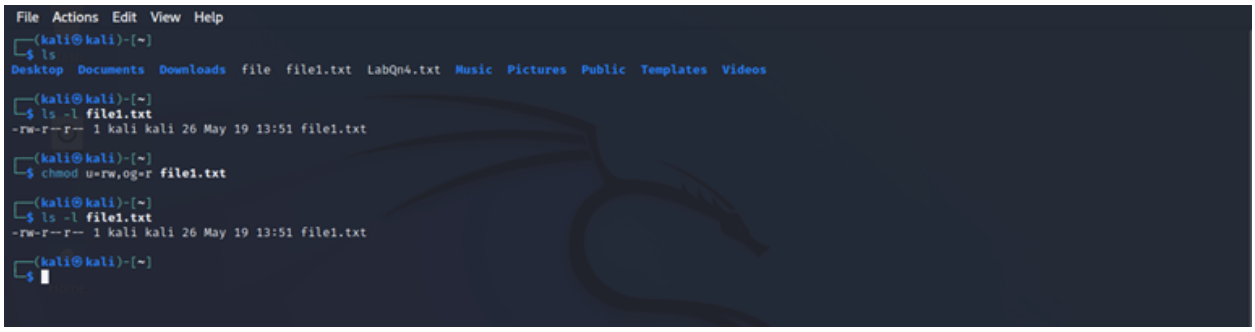
nano: Text editor for creating and editing files



vi/vim: Powerful text editor for experienced users

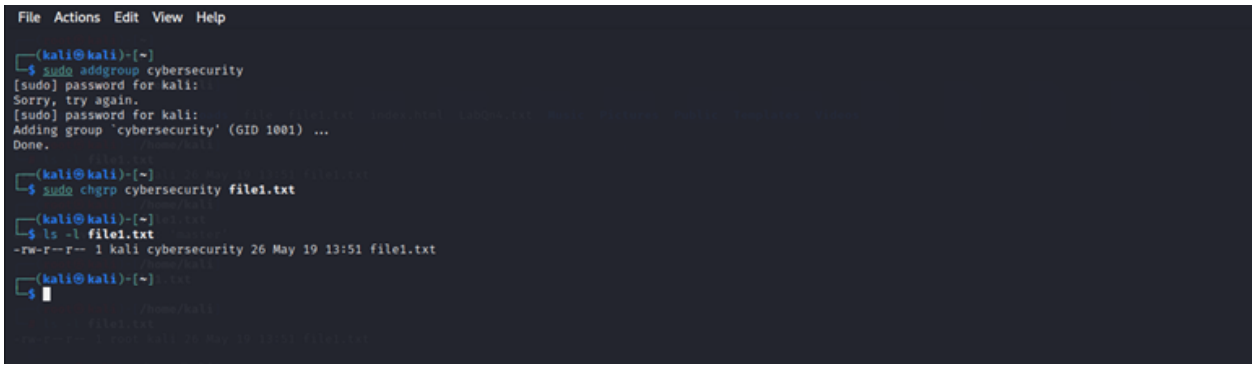
File Permissions:

chmod: Change file permissions



chown: Change file owner

chgrp: Change file group



D

File Compression and Archiving:

tar: Archive files

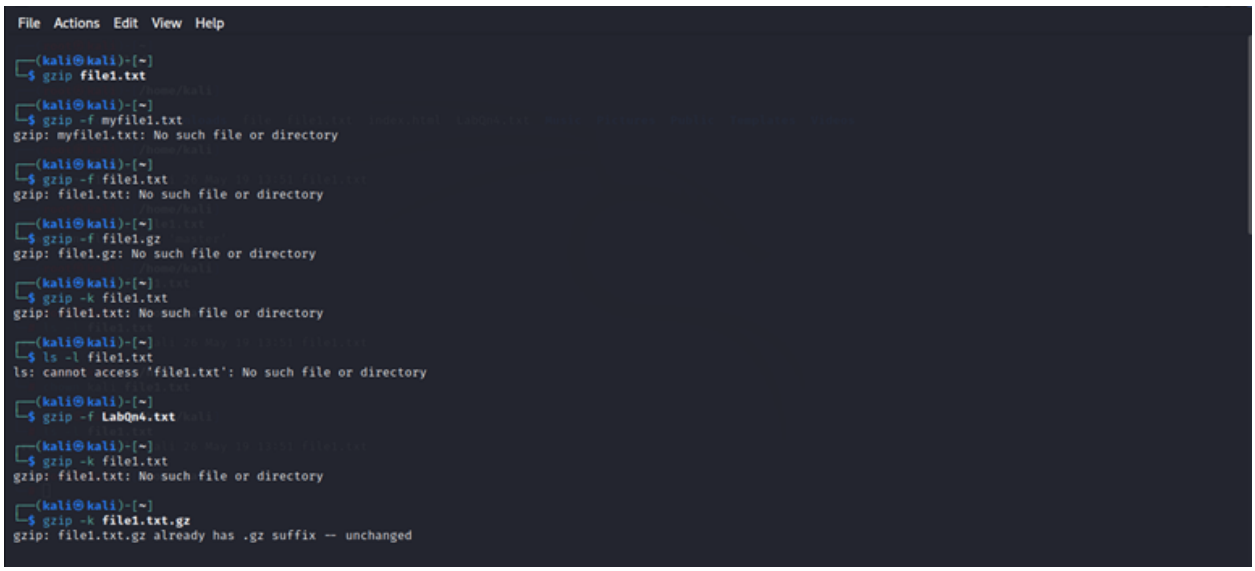
Commands:

- tar cvf f.tar*
- tar xvf f.tar
- tar tvf f.tar

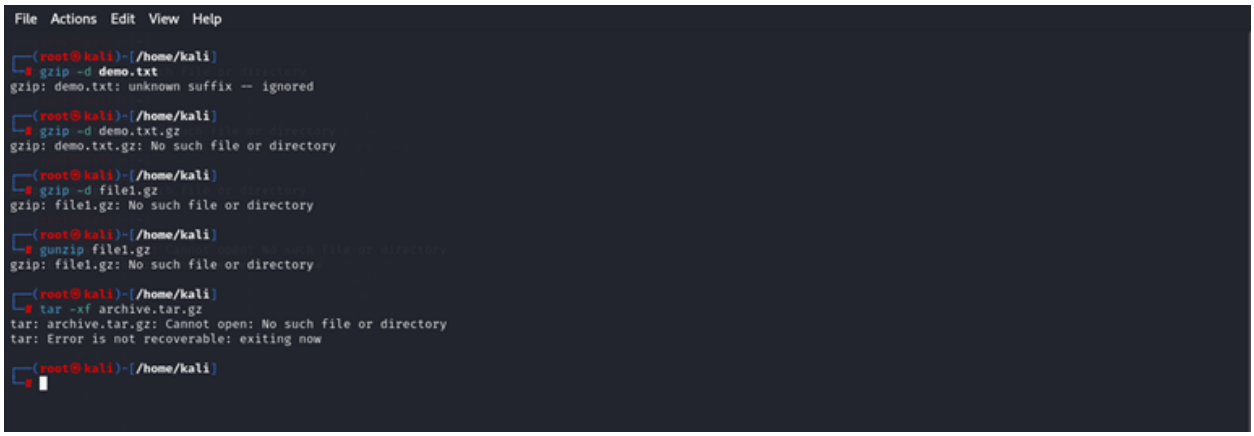
```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ tar xvf f.tar
Desktop/
Documents/
Documents/Penetration/
Documents/testing/
Downloads/
Downloads/files
Downloads/Nessus-10.4.2-ubuntu1404_amd64.deb
Downloads/20BIT0302 .pdf
Downloads/Files
file
file1.txt
index.html
LabQn4.txt
Music/
Pictures/
Pictures/Screenshot_2022-12-21_10_51_50.png
Pictures/Screenshot_2023-01-20_10_04_08.png
Pictures/Screenshot_2023-01-20_10_28_02.png
Pictures/Screenshot_2022-12-21_10_55_53.png
Pictures/Screenshot_2023-01-20_10_02_49.png
Pictures/Screenshot_2023-01-19_22_14_56.png
Pictures/Screenshot_2023-03-01_03_36_11.png
Pictures/Screenshot_2023-01-20_10_28_26.png
Pictures/Screenshot_2022-12-15_11_52_04.png
Pictures/Screenshot_2022-12-21_10_42_23.png
Pictures/Screenshot_2023-01-20_10_34_46.png
Pictures/Screenshot_2023-01-20_08_51_28.png
Pictures/Screenshot_2023-01-20_10_43_13.png
Pictures/Screenshot_2023-01-19_22_18_02.png
Pictures/Screenshot_2023-01-20_10_41_59.png
Pictures/Screenshot_2023-01-19_22_28_49.png
Pictures/Screenshot_2022-12-20_10_51_05.png
Pictures/Screenshot_2023-01-20_10_27_51.png
```

```
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ tar tvf f.tar
drwxr-xr-x kali/kali         0 2022-05-12 12:19 Desktop/
drwxr-xr-x kali/kali         0 2023-05-19 13:32 Documents/
drwxr-xr-x kali/kali         0 2023-05-19 13:32 Documents/Penetration/
drwxr-xr-x kali/kali         0 2023-05-19 13:32 Documents/testing/
drwxr-xr-x kali/kali         0 2023-05-19 13:57 Downloads/
-rw------- kali/kali   4079120 2023-05-19 13:39 Downloads/files
-rwxr-xr-x kali/kali  58913086 2023-02-16 11:52 Downloads/Nessus-10.4.2-ubuntu1404_amd64.deb
-rw-r--r-- kali/kali     74986 2023-03-24 04:23 Downloads/20BIT0302 .pdf
-rw------- kali/kali   4079120 2021-12-30 02:25 Downloads/Files
-rw-r--r-- kali/kali         2 2023-05-19 14:11 file
-rw-r--r-- kali/cybersecurity 26 2023-05-19 13:51 file1.txt
-rw-r--r-- kali/kali     50674 2023-05-19 14:51 index.html
-rw-r--r-- kali/kali      5843 2022-12-22 22:32 LabQn4.txt
drwxr-xr-x kali/kali         0 2022-05-12 12:19 Music/
drwxr-xr-x kali/kali         0 2023-05-19 13:47 Pictures/
-rw-r--r-- kali/kali    186553 2022-12-21 10:51 Pictures/Screenshot_2022-12-21_10_51_50.png
-rw-r--r-- kali/kali    164579 2023-01-20 10:04 Pictures/Screenshot_2023-01-20_10_04_08.png
-rw-r--r-- kali/kali    126538 2023-01-20 10:28 Pictures/Screenshot_2023-01-20_10_28_02.png
-rw-r--r-- kali/kali    203809 2022-12-21 10:56 Pictures/Screenshot_2022-12-21_10_55_53.png
-rw-r--r-- kali/kali    105780 2023-01-20 10:02 Pictures/Screenshot_2023-01-20_10_02_49.png
-rw-r--r-- kali/kali    148675 2023-01-19 22:15 Pictures/Screenshot_2023-01-19_22_14_56.png
-rw-r--r-- kali/kali    129243 2023-03-01 03:36 Pictures/Screenshot_2023-03-01_03_36_11.png
-rw-r--r-- kali/kali    132316 2023-01-20 10:28 Pictures/Screenshot_2023-01-20_10_28_26.png
-rw-r--r-- kali/kali    139293 2022-12-15 11:52 Pictures/Screenshot_2022-12-15_11_52_04.png
-rw-r--r-- kali/kali    184916 2022-12-21 10:42 Pictures/Screenshot_2022-12-21_10_42_23.png
-rw-r--r-- kali/kali    178667 2023-01-20 10:34 Pictures/Screenshot_2023-01-20_10_34_46.png
-rw-r--r-- kali/kali    138635 2023-01-20 08:51 Pictures/Screenshot_2023-01-20_08_51_28.png
-rw-r--r-- kali/kali    124645 2023-01-20 10:43 Pictures/Screenshot_2023-01-20_10_43_13.png
-rw-r--r-- kali/kali    124916 2023-01-19 22:18 Pictures/Screenshot_2023-01-19_22_18_02.png
-rw-r--r-- kali/kali    137102 2023-01-20 10:42 Pictures/Screenshot_2023-01-20_10_41_59.png
-rw-r--r-- kali/kali    146222 2023-01-19 22:28 Pictures/Screenshot_2023-01-19_22_28_49.png
-rw-r--r-- kali/kali    154371 2022-12-20 10:51 Pictures/Screenshot_2022-12-20_10_51_05.png
```

gzip: Compress files



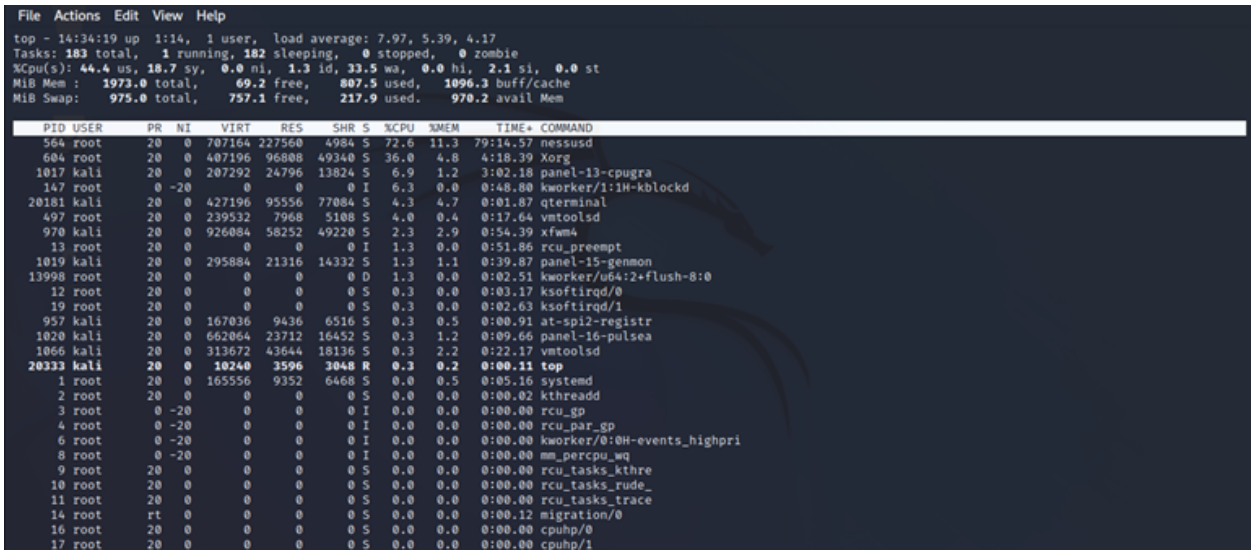
unzip: Extract files from a ZIP archive



Process Management:

ps: List running processes

top: Display real-time system information and processes



kill: Terminate processes

bg: Run processes in the background

fg: Bring background processes to the foreground

System Information:

uname: Print system information

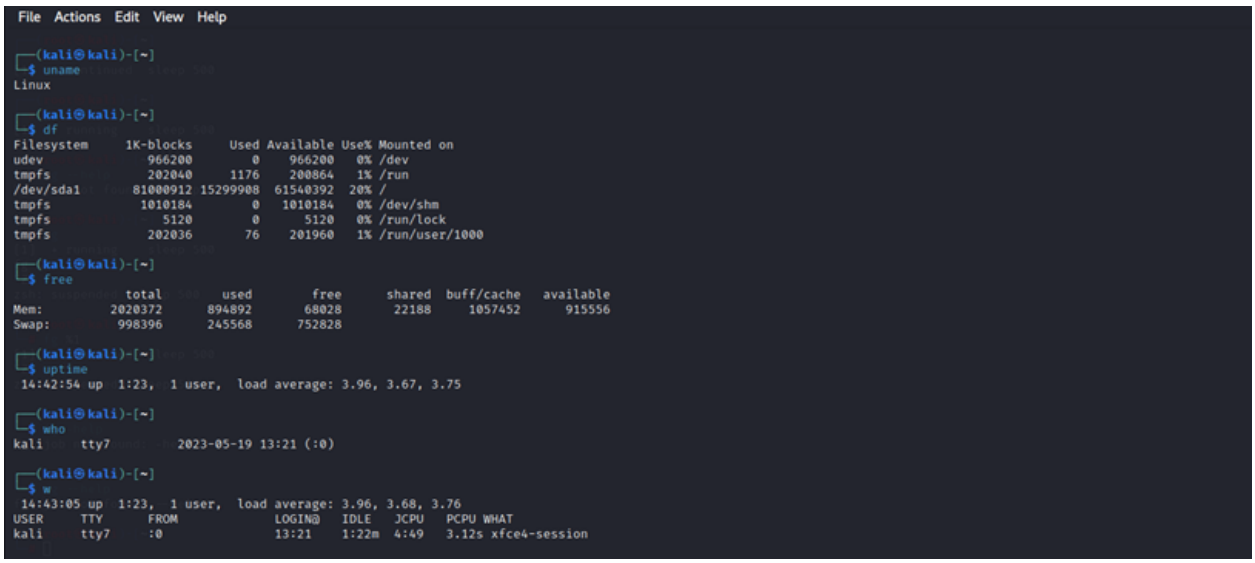
df: Display disk space usage

free: Display memory usage

uptime: Show system uptime

who: Display logged-in users

w: Display logged-in users and their activities



Networking:

ifconfig: Configure network interfaces

```
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.50.128  netmask 255.255.255.0  broadcast 192.168.50.255
        inet6 fe80::20c:29ff:feb1:d154  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:b1:d1:54  txqueuelen 1000  (Ethernet)
        RX packets 177  bytes 12888 (12.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2218  bytes 194314 (189.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(kali㉿kali)-[~]
└─$
```

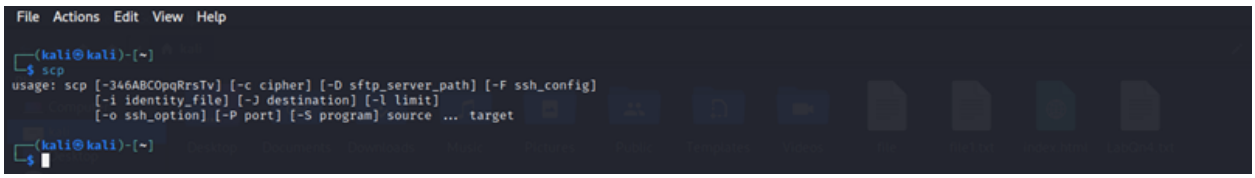
ping: Send ICMP echo requests to a network host

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ ping 192.168.50.129
PING 192.168.50.129 (192.168.50.129) 56(84) bytes of data.
64 bytes from 192.168.50.129: icmp_seq=1 ttl=64 time=3.49 ms
64 bytes from 192.168.50.129: icmp_seq=2 ttl=64 time=0.645 ms
64 bytes from 192.168.50.129: icmp_seq=3 ttl=64 time=0.898 ms
64 bytes from 192.168.50.129: icmp_seq=4 ttl=64 time=0.735 ms
64 bytes from 192.168.50.129: icmp_seq=5 ttl=64 time=0.732 ms
64 bytes from 192.168.50.129: icmp_seq=6 ttl=64 time=0.646 ms
64 bytes from 192.168.50.129: icmp_seq=7 ttl=64 time=0.660 ms
64 bytes from 192.168.50.129: icmp_seq=8 ttl=64 time=1.50 ms
64 bytes from 192.168.50.129: icmp_seq=9 ttl=64 time=1.81 ms
64 bytes from 192.168.50.129: icmp_seq=10 ttl=64 time=0.674 ms
64 bytes from 192.168.50.129: icmp_seq=11 ttl=64 time=0.759 ms
64 bytes from 192.168.50.129: icmp_seq=12 ttl=64 time=0.725 ms
64 bytes from 192.168.50.129: icmp_seq=13 ttl=64 time=0.735 ms
64 bytes from 192.168.50.129: icmp_seq=14 ttl=64 time=0.695 ms
64 bytes from 192.168.50.129: icmp_seq=15 ttl=64 time=0.691 ms
64 bytes from 192.168.50.129: icmp_seq=16 ttl=64 time=0.778 ms
64 bytes from 192.168.50.129: icmp_seq=17 ttl=64 time=1.80 ms
64 bytes from 192.168.50.129: icmp_seq=18 ttl=64 time=8.23 ms
64 bytes from 192.168.50.129: icmp_seq=19 ttl=64 time=0.743 ms
64 bytes from 192.168.50.129: icmp_seq=20 ttl=64 time=0.757 ms
64 bytes from 192.168.50.129: icmp_seq=21 ttl=64 time=0.725 ms
64 bytes from 192.168.50.129: icmp_seq=22 ttl=64 time=5.47 ms
64 bytes from 192.168.50.129: icmp_seq=23 ttl=64 time=1.02 ms
64 bytes from 192.168.50.129: icmp_seq=24 ttl=64 time=0.968 ms
64 bytes from 192.168.50.129: icmp_seq=25 ttl=64 time=0.672 ms
64 bytes from 192.168.50.129: icmp_seq=26 ttl=64 time=0.723 ms
64 bytes from 192.168.50.129: icmp_seq=27 ttl=64 time=1.40 ms
64 bytes from 192.168.50.129: icmp_seq=28 ttl=64 time=0.802 ms
64 bytes from 192.168.50.129: icmp_seq=29 ttl=64 time=1.19 ms
64 bytes from 192.168.50.129: icmp_seq=30 ttl=64 time=0.697 ms
64 bytes from 192.168.50.129: icmp_seq=31 ttl=64 time=0.722 ms
64 bytes from 192.168.50.129: icmp_seq=32 ttl=64 time=0.985 ms
```

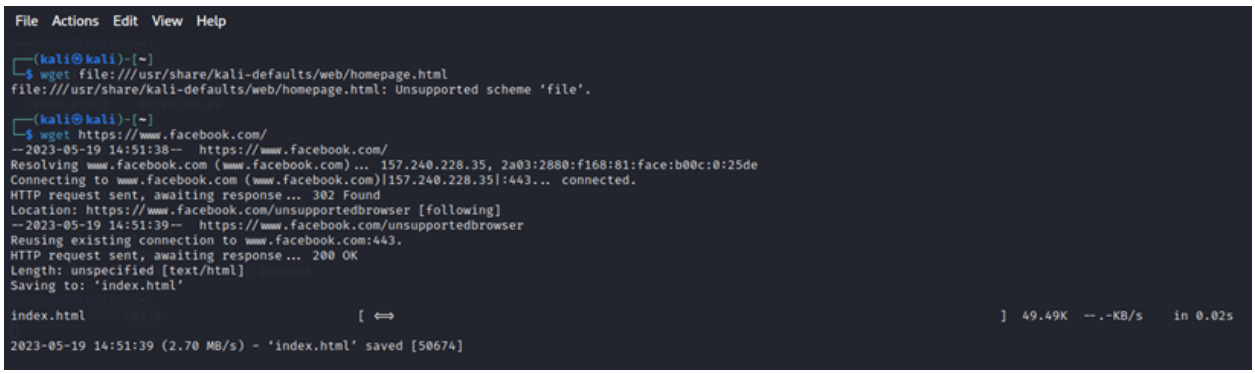
ssh: Securely connect to a remote system

```
┌──(kali㉿kali)-[~]
└─$ ssh
usage: ssh [-46AaCfGgKkMNnqsTtVvXxYy] [-B bind_interface]
           [-b bind_address] [-c cipher_spec] [-D [bind_address:]port]
           [-E log_file] [-e escape_char] [-F configfile] [-I pkcs11]
           [-i identity_file] [-J [user@]host[:port]] [-L address]
           [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
           [-Q query_option] [-R address] [-S ctl_path] [-W host:port]
           [-w local_tun[:remote_tun]] destination [command [argument ...]]

┌──(kali㉿kali)-[~]
└─$ ssh --version
unknown option -- -
usage: ssh [-46AaCfGgKkMNnqsTtVvXxYy] [-B bind_interface]
           [-b bind_address] [-c cipher_spec] [-D [bind_address:]port]
           [-E log_file] [-e escape_char] [-F configfile] [-I pkcs11]
           [-i identity_file] [-J [user@]host[:port]] [-L address]
           [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
           [-Q query_option] [-R address] [-S ctl_path] [-W host:port]
           [-w local_tun[:remote_tun]] destination [command [argument ...]]

┌──(kali㉿kali)-[~]
└─$
```

scp: Securely copy files between systems



wget: Download files from the web



System Administration:

sudo: Execute commands with superuser privileges

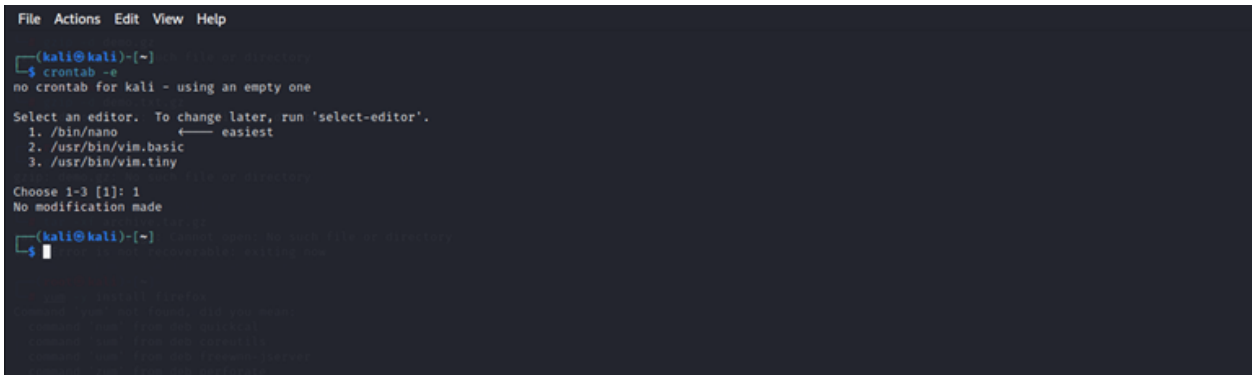
apt-get: Package management for Debian-based distributions

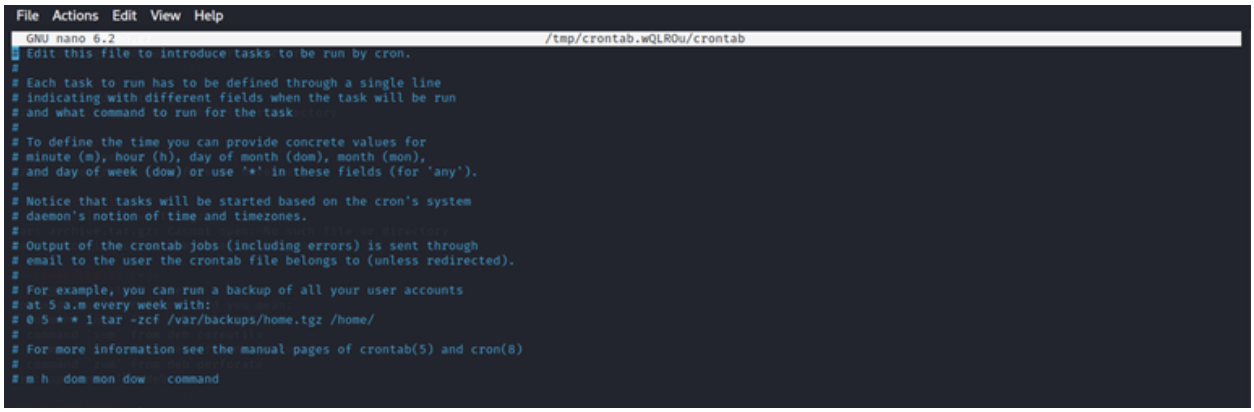
```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ apt-get
apt 2.4.5 (amd64)
Usage: apt-get [options] command
       apt-get [options] install|remove pkg1 [pkg2 ...]
       apt-get [options] source pkg1 [pkg2 ...]

apt-get is a command line interface for retrieval of packages
and information about them from authenticated sources and
for installation, upgrade and removal of packages together
with their dependencies.

Most used commands:
  update - Retrieve new lists of packages
  upgrade - Perform an upgrade
  install - Install new packages (pkg is libc6 not libc6.deb)
  reinstall - Reinstall packages (pkg is libc6 not libc6.deb)
  remove - Remove packages
  purge - Remove packages and config files
  autoremove - Remove automatically all unused packages
  dist-upgrade - Distribution upgrade, see apt-get(8)
  dselect-upgrade - Follow dselect selections
  build-dep - Configure build-dependencies for source packages
  satisfy - Satisfy dependency strings
  clean - Erase downloaded archive files
  autoclean - Erase old downloaded archive files
  check - Verify that there are no broken dependencies
  source - Download source archives
  download - Download the binary package into the current directory
  changelog - Download and display the changelog for the given package

See apt-get(8) for more information about the available commands.
Configuration options and syntax is detailed in apt.conf(5).
Information about how to configure sources can be found in sources.list(5).
Package and version choices can be expressed via apt_preferences(5).
```

systemctl: Manage system services

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ systemctl
  UNIT                                                                    LOAD   ACTIVE SUB       DESCRIPTION                                                  >
  proc-sys-fs-binfmt_misc.automount                                       loaded active waiting   Arbitrary Executable File Formats File System Automount>
  sys-devices-pci0000:00-0000:00:07.1-ata2-host1-target1:0:0-1:0:0:0-block-sr0.device loaded active plugged   VMware_Virtual_IDE_CDROM_Drive
  sys-devices-pci0000:00-0000:00:10.0-host2-target2:0:0-2:0:0:0-block-sda-sda1.device loaded active plugged   VMware_Virtual_S 1
  sys-devices-pci0000:00-0000:00:10.0-host2-target2:0:0-2:0:0:0-block-sda-sda2.device loaded active plugged   VMware_Virtual_S 2
  sys-devices-pci0000:00-0000:00:10.0-host2-target2:0:0-2:0:0:0-block-sda-sda5.device loaded active plugged   VMware_Virtual_S 5
  sys-devices-pci0000:00-0000:00:10.0-host2-target2:0:0-2:0:0:0-block-sda.device      loaded active plugged   VMware_Virtual_S
  sys-devices-pci0000:00-0000:00:11.0-0000:02:01.0-net-eth0.device                    loaded active plugged   82545EM Gigabit Ethernet Controller (Copper) (PRO/1000 >
  sys-devices-pci0000:00-0000:00:11.0-0000:02:02.0-sound-card0-controlC0.device       loaded active plugged   /sys/devices/pci0000:00/0000:00:11.0/0000:02:02.0/sound>
  sys-devices-platform-serial8250-tty-ttyS2.device                                    loaded active plugged   /sys/devices/platform/serial8250/tty/ttyS2
  sys-devices-platform-serial8250-tty-ttyS3.device                                    loaded active plugged   /sys/devices/platform/serial8250/tty/ttyS3
  sys-devices-pnp0-00:06-tty-ttyS0.device                                             loaded active plugged   /sys/devices/pnp0/00:06/tty/ttyS0
  sys-devices-pnp0-00:07-tty-ttyS1.device                                             loaded active plugged   /sys/devices/pnp0/00:07/tty/ttyS1
  sys-devices-virtual-misc-rfkill.device                                              loaded active plugged   /sys/devices/virtual/misc/rfkill
  sys-module-configfs.device                                                          loaded active plugged   /sys/module/configfs
  sys-module-fuse.device                                                              loaded active plugged   /sys/module/fuse
  sys-subsystem-net-devices-eth0.device                                               loaded active plugged   82545EM Gigabit Ethernet Controller (Copper) (PRO/1000 >
  -.mount                                                                             loaded active mounted   Root Mount
  dev-hugepages.mount                                                                 loaded active mounted   Huge Pages File System
  dev-mqueue.mount                                                                    loaded active mounted   POSIX Message Queue File System
  run-credentials-systemd\x2dsysusers.service.mount                                   loaded active mounted   /run/credentials/systemd-sysusers.service
  run-rpc_pipefs.mount                                                                loaded active mounted   RPC Pipe File System
  run-user-1000-gvfs.mount                                                            loaded active mounted   /run/user/1000/gvfs
  run-user-1000.mount                                                                 loaded active mounted   /run/user/1000
  run-vmblock\x2dfuse.mount                                                           loaded active mounted   VMware vmblock fuse mount
  sys-fs-fuse-connections.mount                                                       loaded active mounted   FUSE Control File System
  sys-kernel-config.mount                                                             loaded active mounted   Kernel Configuration File System
  sys-kernel-debug.mount                                                              loaded active mounted   Kernel Debug File System
  sys-kernel-tracing.mount                                                            loaded active mounted   Kernel Trace File System                     >
  systemd-ask-password-plymouth.path                                                  loaded active waiting   Forward Password Requests to Plymouth Directory Watch
  systemd-ask-password-wall.path                                                      loaded active waiting   Forward Password Requests to Wall Directory Watch   >
  init.scope                                                                          loaded active running   System and Service Manager
  session-2.scope                                                                     loaded active running   Session 2 of User kali                       >
```

crontab: Schedule recurring tasks





useradd: Add a new user

```
File  Actions  Edit  View  Help
└─$ useradd
Usage: useradd [options] LOGIN
       useradd -D
       useradd -D [options]

Options:
      --badnames                do not check for bad names
  -b, --base-dir BASE_DIR       base directory for the home directory of the
                                new account
      --btrfs-subvolume-home    use BTRFS subvolume for home directory
  -c, --comment COMMENT         GECOS field of the new account
  -d, --home-dir HOME_DIR       home directory of the new account
  -D, --defaults                print or change default useradd configuration
  -e, --expiredate EXPIRE_DATE  expiration date of the new account
  -f, --inactive INACTIVE       password inactivity period of the new account
  -g, --gid GROUP               name or ID of the primary group of the new
                                account
  -G, --groups GROUPS           list of supplementary groups of the new
                                account
  -h, --help                    display this help message and exit
  -k, --skel SKEL_DIR           use this alternative skeleton directory
  -K, --key KEY=VALUE           override /etc/login.defs defaults
  -l, --no-log-init             do not add the user to the lastlog and
                                faillog databases
  -m, --create-home             create the user's home directory
  -M, --no-create-home          do not create the user's home directory
  -N, --no-user-group           do not create a group with the same name as
                                the user
  -o, --non-unique              allow to create users with duplicate
                                (non-unique) UID
  -p, --password PASSWORD       encrypted password of the new account
  -r, --system                  create a system account
  -R, --root CHROOT_DIR         directory to chroot into
  -P, --prefix PREFIX_DIR       prefix directory where are located the /etc/* files
  -s, --shell SHELL             login shell of the new account
```

passwd: Change user password

```
┌──(kali㉿kali)-[~]
└─$ passwd
Changing password for kali.
Current password:
```

Ensure that you provide the correct command(s) used to accomplish each task. Write your answers below each task.

Once you have completed the assessment, review your answers and verify that the output or results are correct.

Make this in doucement format and send them with images