Mid Exam

Section 1: File and Directory Management

1. Display the current working directory.

```
┌──(kali㉿kali)-[~]
└─$ pwd
/home/kali
```

2. List all the contents of your current directory, including hidden files.

```
┌──(kali㉿kali)-[~]
└─$ ls -al
total 136
drwx------ 16 kali kali  4096 Sep  9 15:39 .
drwxr-xr-x  3 root root  4096 Aug 21  2023 ..
-rw-r--r--  1 kali kali   220 Aug 21  2023 .bash_logout
-rw-r--r--  1 kali kali  5551 Aug 21  2023 .bashrc
-rw-r--r--  1 kali kali  3526 Aug 21  2023 .bashrc.original
drwxr-xr-x 12 kali kali  4096 Aug 25 06:01 .cache
drwxr-xr-x 15 kali kali  4096 Sep  8 07:00 .config
drwxr-xr-x  4 kali kali  4096 Sep  8 06:06 Desktop
-rw-r--r--  1 kali kali    35 Jul 14 06:40 .dmrc
drwxr-xr-x  2 kali kali  4096 Jul 14 06:37 Documents
drwxr-xr-x  2 kali kali  4096 Jul 14 06:37 Downloads
-rw-r--r--  1 kali kali 11759 Aug 21  2023 .face
lrwxrwxrwx  1 kali kali     5 Aug 21  2023 .face.icon → .face
drwx------  3 kali kali  4096 Jul 14 06:37 .gnupg
-rw-------  1 kali kali     0 Jul 14 06:37 .ICEauthority
drwxr-xr-x  3 kali kali  4096 Aug 21  2023 .java
drwxr-xr-x  4 kali kali  4096 Jul 14 06:37 .local
drwx------  4 kali kali  4096 Jul 14 06:48 .mozilla
drwxr-xr-x  2 kali kali  4096 Jul 14 06:37 Music
drwxr-xr-x  2 kali kali  4096 Jul 14 06:37 Pictures
-rw-r--r--  1 kali kali   807 Aug 21  2023 .profile
drwxr-xr-x  2 kali kali  4096 Jul 14 06:37 Public
-rw-r--r--  1 kali kali     0 Jul 28 05:08 .sudo_as_admin_successful
drwxr-xr-x  2 kali kali  4096 Jul 14 06:37 Templates
-rw-r--r--  1 kali kali    81 Aug 25 05:40 test.sh
drwxr-xr-x  2 kali kali  4096 Jul 14 06:37 Videos
-rw-------  1 kali kali   674 Aug 25 05:47 .viminfo
-rw-------  1 kali kali    49 Sep  9 15:39 .Xauthority
-rw-------  1 kali kali  2287 Sep  9 15:39 .xsession-errors
-rw-------  1 kali kali  2862 Sep  8 05:51 .xsession-errors.old
-rw-------  1 kali kali   859 Sep  8 05:51 .zsh_history
-rw-r--r--  1 kali kali 10868 Aug 21  2023 .zshrc
```

3. Change your directory to the `Desktop`.

```
┌──(kali㉿kali)-[~]
└─$ cd ~/Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$
```

4. Create two directories named `dir1` and `dir2` on the Desktop.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ mkdir dir1 dir2
mkdir: cannot create directory ‘dir1’: File exists
mkdir: cannot create directory ‘dir2’: File exists
```

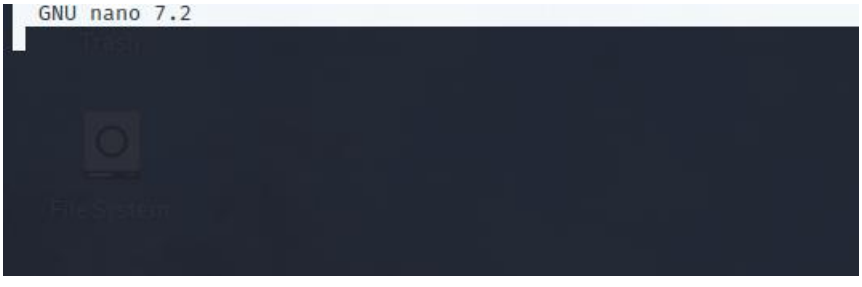
5. Inside `dir1`, create a file named `file1.txt`.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ touch dir1 /file1.txt
touch: cannot touch '/file1.txt': Permission denied
```

6. Inside `dir2`, create a file named `file2.txt`.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ touch dir2 /file2.txt
touch: cannot touch '/file2.txt': Permission denied
```

7. **Using nano or vim Write the numbers 1 to 9 into `file1.txt`.**



8. **From the home directory Copy the contents of `file1.txt` into `file2.txt`.**

```
┌──(kali㉿kali)-[~/Desktop]
└─$ cp file1.txt file2.xtx
cp: cannot stat 'file1.txt': No such file or directory
```

9. From the home directory, delete `file1.txt` inside `dir1`.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ rm file1.txt
rm: cannot remove 'file1.txt': No such file or directory
```

10. Remove the directory `dir1` from the Desktop.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ rm dir1
rm: cannot remove 'dir1': Is a directory
```

11. **Redirect the output of the network configuration command to a file named `network_info.txt` on the Desktop.**

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.199.137  netmask 255.255.255.0  broadcast 192.168.199.255
        inet6 fe80::7481:9d35:9541:6581  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:8b:de:d5  txqueuelen 1000  (Ethernet)
        RX packets 115  bytes 7365 (7.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 25  bytes 3220 (3.1 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 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
```

12. **Open the Desktop folder and show all files with detailed information.**

```
┌──(kali㉿kali)-[~/Desktop]
└─$ cd ~/Desktop ls -al
cd: too many arguments
```

Section 2: Users and Groups Management

1. Create a new user with your name.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo useradd ahmed_saad
[sudo] password for kali:
```

2. Set a password for your user.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo passwd ahmed7733
passwd: user 'ahmed7733' does not exist
```

3. Open the file that contains user information and verify that your user has been added.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo cat /ect/passwd
cat: /ect/passwd: No such file or directory
```

4. Add your user to the file that gives administrative privileges.

```
  GNU nano 7.2
#
# 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"

# This fixes CVE-2005-4890 and possibly breaks some versions of kdesu
# (#1011624, https://bugs.kde.org/show_bug.cgi?id=452532)
Defaults        use_pty

# This preserves proxy settings from user environments of root
# equivalent users (group sudo)
#Defaults:%sudo env_keep += "http_proxy https_proxy ftp_proxy all_proxy no_proxy"

# This allows running arbitrary commands, but so does ALL, and it means
# different sudoers have their choice of editor respected.
#Defaults:%sudo env_keep += "EDITOR"

# Completely harmless preservation of a user preference.
#Defaults:%sudo env_keep += "GREP_COLOR"

# While you shouldn't normally run git as root, you need to with etckeeper
#Defaults:%sudo env_keep += "GIT_AUTHOR_* GIT_COMMITTER_*"

# Per-user preferences; root won't have sensible values for them.
#Defaults:%sudo env_keep += "EMAIL DEBEMAIL DEBFULLNAME"

# "sudo scp" or "sudo rsync" should be able to use your SSH agent.
#Defaults:%sudo env_keep += "SSH_AGENT_PID SSH_AUTH_SOCK"

# Ditto for GPG agent
#Defaults:%sudo env_keep += "GPG_AGENT_INFO"

# Host alias specification

# User alias specification

# Cmnd alias specification


^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute       ^C
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify       ^/
```

5. Switch to your user and confirm the user identity.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ su - your_username
su: user your_username does not exist or the user entry does not contain all the required fields
```

6. Create a new group named `testgroup`.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo groupadd testgroup
```

7. Add your user to `testgroup`.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ gpasswd -a ahmed testgroup
gpasswd: user 'ahmed' does not exist
```

8. Add the group `testgroup` to the file that gives administrative privileges.

```
This file MUST be edited with the 'visudo' command as

Please consider adding local content in /etc/sudoers.
directly modifying this file.

See the man page for details on how to write a sudoer

efaults        env_reset
efaults        mail_badpass
efaults        secure_path="/usr/local/sbin:/usr/local

This fixes CVE-2005-4890 and possibly breaks some ver
(#1011624, https://bugs.kde.org/show_bug.cgi?id=45253
efaults        use_pty

This preserves proxy settings from user environments
equivalent users (group sudo)
Defaults:%sudo env_keep += "http_proxy https_proxy ftp

This allows running arbitrary commands, but so does A
different sudoers have their choice of editor respect
Defaults:%sudo env_keep += "EDITOR"

Completely harmless preservation of a user preference
Defaults:%sudo env_keep += "GREP_COLOR"

While you shouldn't normally run git as root, you nee
Defaults:%sudo env_keep += "GIT_AUTHOR_* GIT_COMMITTER
```

9. **Remove your user from the file that gives administrative privileges.**

```
┌──(kali㉿kali)-[~/Desktop]
└─$ gpasswd -d ahmed testgroup
gpasswd: Permission denied.
```

10. **Check if your user still have administrative privileges.**

```
┌──(kali㉿kali)-[~/Desktop]
└─$ grops ahmed
grops: error: can't open file 'ahmed'
```

11. Check which groups your user belongs to.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ grops

```

Section 3: Permissions and Ownership

1. **Set the permissions of `file2.txt` on the Desktop to allow the owner to read, write, and execute; the group to read and execute; and others to read .**

```
┌──(kali㉿kali)-[~/Desktop]
└─$ chmod 754 ~/Desktop/file2.txt
chmod: cannot access '/home/kali/Desktop/file2.txt': No such file or directory
```

2. Check the permissions of `file2.txt` to verify the change.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ls -l ~/Desktop/file2.txt
ls: cannot access '/home/kali/Desktop/file2.txt': No such file or directory
```

3. Change the ownership of `file2.txt` to your user.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo chown your_username ~/Desktop/file2.txt
chown: invalid user: ‘your_username’
```

4. verify the ownership of `file2.txt`.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ls -l ~/Desktop/file2.txt
ls: cannot access '/home/kali/Desktop/file2.txt': No such file or directory
```

5. **Change back the ownership of a file `file2.txt` .**

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo chown original_owner ~/Desktop/file2.txt
chown: invalid user: ‘original_owner’
```

6. **Grant write permission to everyone for `file2.txt`.**

```
┌──(kali㉿kali)-[~/Desktop]
└─$ chmod a+w ~/Desktop /file2.txt
chmod: cannot access '/file2.txt': No such file or directory
```

7. **Remove the write permission for the group and others for `file2.txt`.**

```
┌──(kali㉿kali)-[~/Desktop]
└─$ chmod go-w ~/Desktop /file2.txt
chmod: cannot access '/file2.txt': No such file or directory
```

8. **Delete `file2.txt` after making the necessary ownership and permission changes.**

```
┌──(kali㉿kali)-[~/Desktop]
└─$ rm ~/Desktop /file2.txt
rm: cannot remove '/home/kali/Desktop': Is a directory
rm: cannot remove '/file2.txt': No such file or directory
```

9. **What command would you use to recursively change the permissions of all files and directories inside a folder named `project` to `755`.**

```
┌──(kali㉿kali)-[~/Desktop]
└─$ chmod -R 755 ~/project
chmod: cannot access '/home/kali/project': No such file or directory
```

Section 4: Process Management

1. **Install a system monitor tool that provides an interactive process viewer(htop).**

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo dnf install htop
sudo: dnf: command not found
```

2. Display all running processes.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ 'ps aux'
ps aux: command not found
```

3. Display a tree of all running processes.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ 'pstree'
systemd─┬─ModemManager───3*[{ModemManager}]
        ├─NetworkManager───3*[{NetworkManager}]
        ├─agetty
        ├─colord───3*[{colord}]
        ├─cron
        ├─dbus-daemon
        ├─haveged
        ├─lightdm─┬─Xorg───{Xorg}
        │         ├─lightdm─┬─xfce4-session─┬─Thunar───3*[{Thunar}]
        │         │         │               ├─agent───3*[{agent}]
        │         │         │               ├─blueman-applet───4*[{blueman-applet}]
        │         │         │               ├─light-locker───4*[{light-locker}]
        │         │         │               ├─nm-applet───4*[{nm-applet}]
        │         │         │               ├─polkit-gnome-au───3*[{polkit-gnome-au}]
        │         │         │               ├─ssh-agent
        │         │         │               ├─xfce4-panel─┬─panel-1-whisker───3*[{panel-1-whisker}]
        │         │         │               │            ├─panel-13-cpugra───3*[{panel-13-cpugra}]
        │         │         │               │            ├─panel-14-systra───3*[{panel-14-systra}]
        │         │         │               │            ├─panel-15-genmon───3*[{panel-15-genmon}]
        │         │         │               │            ├─panel-16-pulsea───3*[{panel-16-pulsea}]
        │         │         │               │            ├─panel-17-notifi───3*[{panel-17-notifi}]
        │         │         │               │            ├─panel-18-power-───3*[{panel-18-power-}]
        │         │         │               │            ├─panel-22-action───3*[{panel-22-action}]
        │         │         │               │            └─3*[{xfce4-panel}]
        │         │         │               ├─xfce4-power-man───3*[{xfce4-power-man}]
        │         │         │               ├─xfdesktop───3*[{xfdesktop}]
        │         │         │               ├─xfsettingsd───3*[{xfsettingsd}]
        │         │         │               ├─xfwm4───12*[{xfwm4}]
        │         │         │               ├─xiccd───3*[{xiccd}]
        │         │         │               └─3*[{xfce4-session}]
        │         │         └─3*[{lightdm}]
        │         └─3*[{lightdm}]
        ├─polkitd───3*[{polkitd}]
        ├─qterminal─┬─zsh─┬─grops
        │           │     └─pstree
        │           └─2*[{qterminal}]
        ├─rtkit-daemon───2*[{rtkit-daemon}]
        ├─systemd─┬─(sd-pam)
        │         ├─at-spi-bus-laun─┬─dbus-daemon
        │         │                 └─4*[{at-spi-bus-laun}]
        │         ├─at-spi2-registr───3*[{at-spi2-registr}]
```

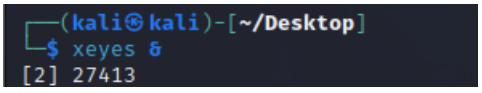
4. Open the interactive process viewer and identify a process by its PID.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ htop
Command 'htop' not found, but can be installed with:
sudo apt install htop
Do you want to install it? (N/y)
```

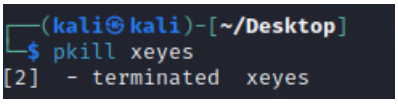
5. **Kill a process with a specific PID.**

```
┌──(kali㉿kali)-[~/Desktop]
└─$ kill pid
kill: illegal pid: pid
```

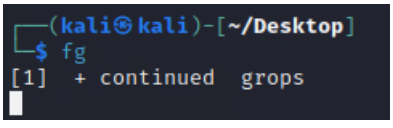
6. **Start an application and stop it using a command that kills processes by name(exeyes).**



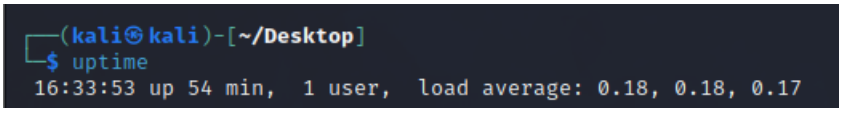
7. Restart the application, then stop it using the interactive process viewer.



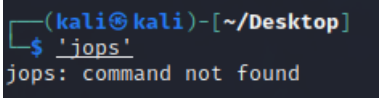
8. **Run a command in the background, then bring it to the foreground(exeyes).**



9. Check how long the system has been running.



10. List all jobs running in the background.



Section 5: Networking Commands

1. Display the network configuration.
2. Check the IP address of your machine.
3. Test connectivity to an external server.
4. Display the routing table.
5. **Check the open ports and active connections.**
6. Show the IP address of the host machine and the VM, and verify if they are on the same network.
7. Trace the route to an external server.
8. Find out the default gateway.
9. Check the MAC address of your network interface.
10. Ensure that the VM can access external networks.

Section 6: UFW Firewall

1. Enable the firewall.
2. Allow SSH connections through the firewall.
3. Deny all incoming traffic by default.
4. Allow HTTP and HTTPS traffic.

5. Allow port 20
6. Reset the firewall settings.
7. Delete a rule from the firewall.
8. Disable the firewall.
9. View the status of the firewall.
10. Log firewall activity and view it.

Section 7: Searching and System Information

1. Delete the command history.
2. **Search for a kali in the `/etc/passwd` file.**
3. **Search for a kali in the `/etc/group` file.**
4. Locate the `passwd` file.
5. **Locate the shadow file and open it.**
6. Search for all configuration files in the `/etc` directory.
7. Search recursively for a specific word in the `/var/log` directory.
8. View the system’s kernel version.
9. Display the system’s memory usage.
10. Show the system’s disk usage.
11. Check the system's uptime and load average.
12. **Display the current logged-in users.**
13. Check the identity of the current user.
14. View the `/var/log/auth.log` file.
15. Shred the `auth.log` file securely.
16. How do you lock a user account to prevent them from logging in.
17. What command would you use to change a user's default shell.
18. Display the system's boot messages.