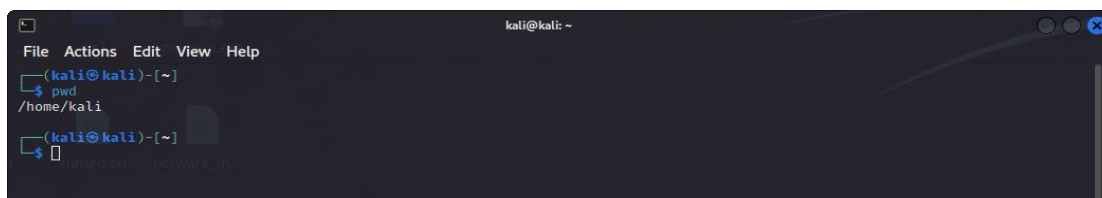
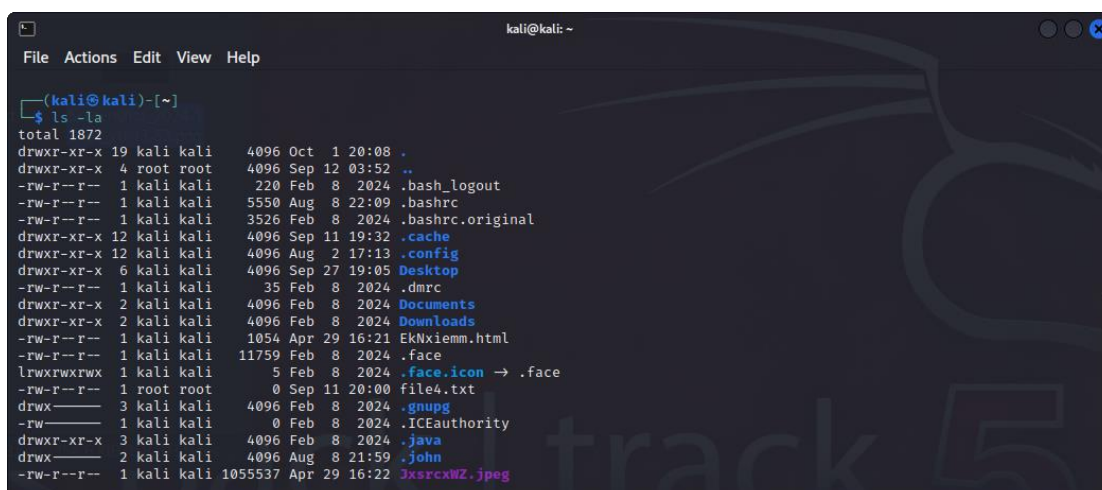

SECTION 1: FILE AND DIRECTORY MANAGEMENT

1. Display the current working directory.



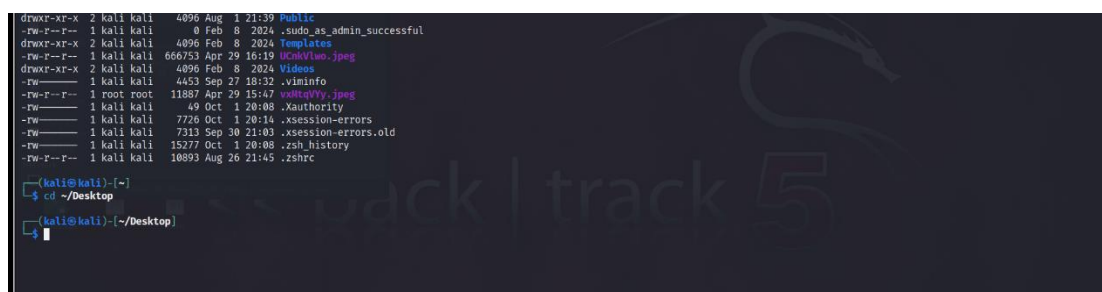
```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ pwd  
/home/kali  
(kali@kali)-[~]  
$
```

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



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ ls -la  
total 1872  
drwxr-xr-x 19 kali kali 4096 Oct 1 20:08 .  
drwxr-xr-x 4 root root 4096 Sep 12 03:52 ..  
-rw-r--r-- 1 kali kali 220 Feb 8 2024 .bash_logout  
-rw-r--r-- 1 kali kali 5550 Aug 8 22:09 .bashrc  
-rw-r--r-- 1 kali kali 3526 Feb 8 2024 .bashrc.original  
drwxr-xr-x 12 kali kali 4096 Sep 11 19:32 .cache  
drwxr-xr-x 12 kali kali 4096 Aug 2 17:13 .config  
drwxr-xr-x 6 kali kali 4096 Sep 27 19:05 Desktop  
-rw-r--r-- 1 kali kali 35 Feb 8 2024 .dmrc  
drwxr-xr-x 2 kali kali 4096 Feb 8 2024 Documents  
drwxr-xr-x 2 kali kali 4096 Feb 8 2024 Downloads  
-rw-r--r-- 1 kali kali 1054 Apr 29 16:21 EkNxiemm.html  
-rw-r--r-- 1 kali kali 11759 Feb 8 2024 .face  
lrwxrwxrwx 1 kali kali 5 Feb 8 2024 .face.icon -> .face  
-rw-r--r-- 1 root root 0 Sep 11 20:00 file4.txt  
drwx----- 3 kali kali 4096 Feb 8 2024 .gnupg  
-rw----- 1 kali kali 0 Feb 8 2024 .ICEauthority  
drwxr-xr-x 3 kali kali 4096 Feb 8 2024 .java  
drwx----- 2 kali kali 4096 Aug 8 21:59 .john  
-rw-r--r-- 1 kali kali 1055537 Apr 29 16:22 JxsrcxMZ.jpeg
```

3. Change your directory to the `Desktop`.



```
drwxr-xr-x 2 kali kali 4096 Aug 1 21:39 Public  
-rw-r--r-- 1 kali kali 0 Feb 8 2024 .sudo_as_admin_successful  
drwxr-xr-x 2 kali kali 4096 Feb 8 2024 Templates  
-rw-r--r-- 1 kali kali 666753 Apr 29 16:19 Ucmxvise.jpeg  
drwxr-xr-x 2 kali kali 4096 Feb 8 2024 Videos  
-rw----- 1 kali kali 4453 Sep 27 18:32 .viminfo  
-rw-r--r-- 1 root root 11887 Apr 29 15:47 vsMqVvy.jpeg  
-rw----- 1 kali kali 49 Oct 1 20:08 .xauthority  
-rw----- 1 kali kali 7726 Oct 1 20:14 .xsession-errors  
-rw----- 1 kali kali 7313 Sep 30 21:03 .xsession-errors.old  
-rw----- 1 kali kali 15277 Oct 1 20:08 .zsh_history  
-rw-r--r-- 1 kali kali 10893 Aug 26 21:45 .zshrc  
(kali@kali)-[~]  
$ cd ~/Desktop  
(kali@kali)-[~/Desktop]  
$
```

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

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

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

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`.

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

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

```
(kali@kali) ~/Desktop
$ mkdir dir1 dir2
(kali@kali) ~/Desktop
$ touch dir1/file1.txt
(kali@kali) ~/Desktop
$ touch dir2/file2.txt
(kali@kali) ~/Desktop
$ nano dir1/file1.txt
(kali@kali) ~/Desktop
$ cp dir1/file1.txt dir2/file2.txt
(kali@kali) ~/Desktop
$ cd ~
(kali@kali) ~
$ rm Desktop/dir1/file1.txt
(kali@kali) ~
$ cd Desktop
(kali@kali) ~/Desktop
$ rmdir dir1
(kali@kali) ~/Desktop
$
```

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

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

```
(kali@kali) ~/Desktop
$ ifconfig > network_info.txt
(kali@kali) ~/Desktop
$ ls -ls
total 4104
drwxr-xr-x  5 kali kali   4096 Oct  1 20:26 .
drwxr-xr-x 19 kali kali   4096 Oct  1 20:08 ..
-rw-r--r--  1 kali kali    25 Sep 12 04:34 ahmed.txt
drwxr-xr-x  2 kali kali   4096 Oct  1 20:23 dir2
-rwxr-xr--  1 ahmed ahmed    0 Sep 12 03:57 file2.txt
-rwxr-xr--  1 kali kali    36 Sep 11 20:25 file.txt
-rwxrw-rw-  1 kali kali 1114193 Aug  8 21:46 'Linux Files and Directories Management.png'
-rwxrw-rw-  1 kali kali  993106 Aug  8 21:46 'Linux Networking Commands .png'
drwxr-xr-x  2 kali kali   4096 Oct  1 20:29 mobile
-rw-r--r--  1 kali kali    721 Oct  1 20:31 network_info.txt
-rw-r--r--  1 kali kali    43 Sep 27 19:05 oo.sh
-rw-r--r--  1 root root   80841 Apr 29 16:15 payload.apk
-rw-r--r--  1 root root    7382 Apr 29 15:36 payload.exe
-rwxrw-rw-  1 kali kali 1053494 Aug  8 21:46 'Process Management.png'
drwxr-xr-x  3 kali kali   4096 Sep 11 20:34 project
-rwxrw-rw-  1 kali kali   834466 Aug  8 21:46 'Users and Groups Management.png'
(kali@kali) ~/Desktop
$
```

Section 2: Users and Groups Management

13. Create a new user with your name.

14. Set a password for your user.

```
kali@kali: ~/Desktop
$ sudo useradd anas
$ sudo passwd anas
New password:
Retype new password:
passwd: password updated successfully
$
```

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

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

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

```
kali@kali: ~/Desktop
$ sudo useradd anas
$ sudo passwd anas
New password:
Retype new password:
passwd: password updated successfully
$ sudo cat /etc/passwd | grep anas
anas:x:1004:1005::/home/anas:/bin/sh
$ sudo nano /etc/sudoers
$ su - anas
Password:
su: warning: cannot change directory to /home/anas: No such file or directory
$
```

18. Create a new group named `testgroup`.

19. Add your user to `testgroup`.

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

21. Remove your user from the file that gives administrative privileges.

```
kali@kali: ~/Desktop
$ sudo groupadd testgroup
$ sudo nano /etc/sudoers
$ sudo nano /etc/sudoers
$
```

SECTION 3: PERMISSIONS AND OWNERSHIP

24. 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 .

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

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

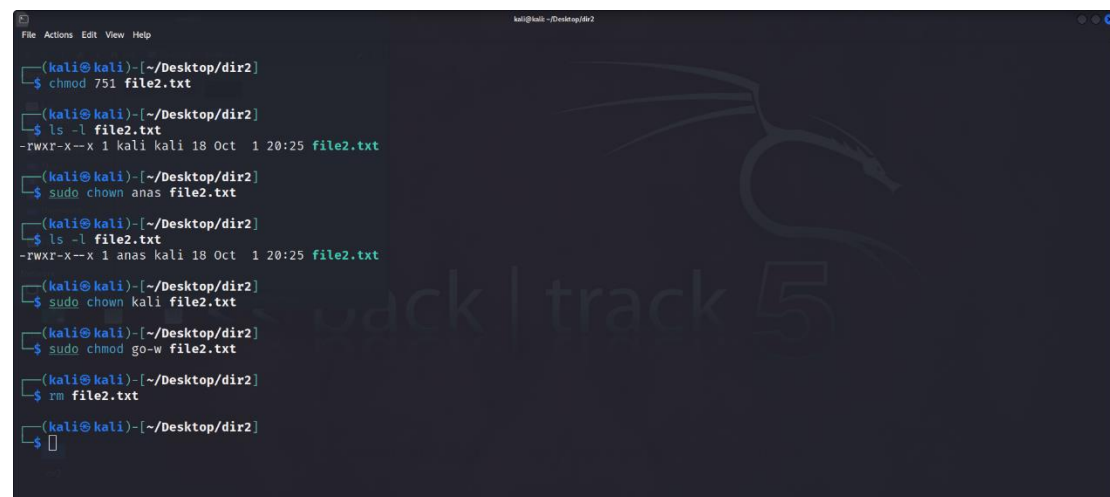
27. verify the ownership of `file2.txt`.

28. Change back the ownership of a file `file2.txt`

29. Grant write permission to everyone for `file2.txt`

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

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



```
(kali@kali)-[~/Desktop/dir2]
$ chmod 751 file2.txt

(kali@kali)-[~/Desktop/dir2]
$ ls -l file2.txt
-rwxr-x--x 1 kali kali 18 Oct 1 20:25 file2.txt

(kali@kali)-[~/Desktop/dir2]
$ sudo chown anas file2.txt

(kali@kali)-[~/Desktop/dir2]
$ ls -l file2.txt
-rwxr-x--x 1 anas kali 18 Oct 1 20:25 file2.txt

(kali@kali)-[~/Desktop/dir2]
$ sudo chown kali file2.txt

(kali@kali)-[~/Desktop/dir2]
$ sudo chmod go-w file2.txt

(kali@kali)-[~/Desktop/dir2]
$ rm file2.txt

(kali@kali)-[~/Desktop/dir2]
$
```

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

chmod -R 755 project/

SECTION 4: PROCESS MANAGEMENT

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

sudo apt install htop

34. Display all running processes.

```
(kali@kali)~/Desktop/dir2
$ ps aux
```

USER	PID	%CPU	%MEM	VSZ	RSS	TTY	STAT	START	TIME	COMMAND
root	1	0.0	0.1	166168	11232	?	Ss	20:07	0:00	/sbin/init splash
root	2	0.0	0.0	0	0	?	S	20:07	0:00	[kthreadd]
root	3	0.0	0.0	0	0	?	I<	20:07	0:00	[rcu_gp]
root	4	0.0	0.0	0	0	?	I<	20:07	0:00	[rcu_par_gp]
root	6	0.0	0.0	0	0	?	I<	20:07	0:00	[kworker/0:0H-events_highpri]
root	9	0.0	0.0	0	0	?	I<	20:07	0:00	[mm_percpu_wq]
root	10	0.0	0.0	0	0	?	S	20:07	0:00	[rcu_tasks_kthre]
root	11	0.0	0.0	0	0	?	S	20:07	0:00	[rcu_tasks_rude_]
root	12	0.0	0.0	0	0	?	S	20:07	0:00	[rcu_tasks_trace]
root	13	0.0	0.0	0	0	?	S	20:07	0:00	[ksoftirqd/0]
root	14	0.0	0.0	0	0	?	S	20:07	0:00	[rcu_preempt]

35. Display a tree of all running processes.

```
(kali@kali)~/Desktop/dir2
$ pstree
```

```
systemd--ModemManager--2*[{ModemManager}]
systemd--NetworkManager--2*[{NetworkManager}]
systemd--agetty
systemd--colord--2*[{colord}]
systemd--cron
systemd--dbus-daemon
systemd--haveged
systemd--lightdm--Xorg--{Xorg}
systemd--lightdm--xfce4-session--Thunar--2*[{Thunar}]
systemd--lightdm--xfce4-session--agent--2*[{agent}]
systemd--lightdm--xfce4-session--applet.py
systemd--lightdm--xfce4-session--blueman-applet--3*[{blueman-applet}]
systemd--lightdm--xfce4-session--light-locker--3*[{light-locker}]
systemd--lightdm--xfce4-session--nm-applet--3*[{nm-applet}]
systemd--lightdm--xfce4-session--polkit-gnome-au--2*[{polkit-gnome-au}]
systemd--lightdm--xfce4-session--ssh-agent
systemd--lightdm--xfce4-session--xfce4-notifyd--2*[{xfce4-notifyd}]
systemd--lightdm--xfce4-session--xfce4-panel--panel-1-whisker--2*[{panel-1-whisker}]
systemd--lightdm--xfce4-session--xfce4-panel--panel-13-clipgr--2*[{panel-13-clipgr}]
systemd--lightdm--xfce4-session--xfce4-panel--panel-14-sysstr--2*[{panel-14-sysstr}]
systemd--lightdm--xfce4-session--xfce4-panel--panel-15-genmon--2*[{panel-15-genmon}]
systemd--lightdm--xfce4-session--xfce4-panel--panel-16-pulsea--2*[{panel-16-pulsea}]
systemd--lightdm--xfce4-session--xfce4-panel--panel-17-notifi--2*[{panel-17-notifi}]
systemd--lightdm--xfce4-session--xfce4-panel--panel-18-power--2*[{panel-18-power-}]
systemd--lightdm--xfce4-session--xfce4-panel--panel-22-action--2*[{panel-22-action}]
systemd--lightdm--xfce4-session--2*[{xfce4-panel}]
```

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

htop

37. Kill a process with a specific PID.

```
(kali@kali)~/Desktop/dir2
$ xeyes 6
[1] 13038

(kali@kali)~/Desktop/dir2
$ kill 13038

[1] + terminated xeyes
(kali@kali)~/Desktop/dir2
$
```

38. Start an application and stop it using a command that kills processes by name(exeyes). 39. Restart the application, then stop it using the interactive process viewer.

```
(kali@kali)~[/Desktop/dir2]
$ xeyes &
[1] 13455

(kali@kali)~[/Desktop/dir2]
$ pkill xeyes
[1] + terminated xeyes

(kali@kali)~[/Desktop/dir2]
$
```

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

```
(kali@kali)~[/Desktop/dir2]
$ xeyes &
[1] 13949

(kali@kali)~[/Desktop/dir2]
$ fg
[1] + running xeyes

(kali@kali)~[/Desktop/dir2]
$
```

41. Check how long the system has been running.

42. List all jobs running in the background.

```
(kali@kali)~[/Desktop/dir2]
$ uptime
20:55:33 up 48 min, 1 user, load average: 0.22, 0.17, 0.18

(kali@kali)~[/Desktop/dir2]
$ jobs
```

SECTION 5: NETWORKING COMMANDS

43. Display the network configuration.

```
(kali@kali)~[/Desktop/dir2]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    ether 00:0c:29:49:98:af txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 117 bytes 20845 (20.3 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 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 32 bytes 2096 (2.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 32 bytes 2096 (2.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)~[/Desktop/dir2]
$
```

45. Test connectivity to an external server.

ping -c 4 google.com

46. Display the routing table.

47. Check the open ports and active connections.

```
kali@kali: ~/Desktop/dir2
(kali@kali)-[~/Desktop/dir2]
$ route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
192.168.75.0 0.0.0.0 255.255.255.0 U 100 0 0 eth0

(kali@kali)-[~/Desktop/dir2]
$ netstat -tuln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address Foreign Address State

(kali@kali)-[~/Desktop/dir2]
$
```

49. Trace the route to an external server.

traceroute google.com

50. Find out the default gateway.

ip route | grep default

51. Check the MAC address of your network interface.

```
(kali@kali)-[~/Desktop/dir2]
$ ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT group default qlen 1000
   link/ether 00:0c:29:49:98:af brd ff:ff:ff:ff:ff:ff

(kali@kali)-[~/Desktop/dir2]
$
```

52. Ensure that the VM can access external networks.

ping

SECTION 6: UFW FIREWALL

53. Enable the firewall.

sudo ufw enable

54. Allow SSH connections through the firewall.

sudo ufw allow ssh

55. Deny all incoming traffic by default.

sudo ufw default deny incoming

56. Allow HTTP and HTTPS traffic.

sudo ufw allow http

sudo ufw allow https

57. Allow port 20

sudo ufw allow 20

58. Reset the firewall settings.

sudo ufw reset

59. Delete a rule from the firewall.

sudo ufw delete allow ssh

60. Disable the firewall.

sudo ufw disable

61. View the status of the firewall.

sudo ufw status

62. Log firewall activity and view it.

sudo ufw logging on

cat /var/log/ufw.log

SECTION 7: SEARCHING AND SYSTEM INFORMATION

63. Delete the command history.

history -c

64. Search for a kali in the `/etc/passwd` file.

65. Search for a kali in the `/etc/group` file.

```
kali@kali: ~/Desktop/dir2
$ grep kali /etc/passwd
kali:x:1000:1000:kali,,,:/home/kali:/usr/bin/zsh

(kali@kali)~[~/Desktop/dir2]
$ grep kali /etc/group
adm:x:4:kali
dialout:x:20:kali
cdrom:x:24:kali
floppy:x:25:kali
sudo:x:27:kali
audio:x:29:pulse,kali
dip:x:30:kali
video:x:44:kali
plugdev:x:46:kali
netdev:x:109:kali
debian-tor:x:115:kali
wireshark:x:125:kali
bluetooth:x:129:kali
vboxsf:x:130:kali
kali-trusted:x:137:
scanner:x:144:saned,kali
kali:x:1000:
kaboxer:x:154:kali

(kali@kali)~[~/Desktop/dir2]
$
```

66. Locate the `passwd` file.

```
kali@kali: ~/Desktop/dir2
$ locate passwd
/etc/passwd
/etc/passwd-
/etc/alternatives/vncpasswd
```

67. Locate the shadow file and open it.

```
kali@kali: ~/Desktop/dir2
$ locate shadow
/etc/gshadow
/etc/gshadow-
```

```
kali@kali: ~/Desktop/dir2
$ sudo cat /etc/shadow
[sudo] password for kali:
root:!:19761:0:99999:7:::
```

68. Search for all configuration files in the `/etc` directory.

```
kali@kali: ~/Desktop/dir2
$ find /etc -type f -name "*.conf"
/etc/opensc/opensc.conf
/etc/tightvncserver.conf
/etc/speech-dispatcher/clients/emacs.conf
/etc/speech-dispatcher/modules/espeak.conf
```

69. Search recursively for a specific word in the `/var/log` directory.

70. View the system's kernel version.

71. Display the system's memory usage.

72. Show the system's disk usage.

```
kali@kali: ~/Desktop/dir2
(kali@kali)~$ sudo grep -r "specific_word" /var/log
/var/log/auth.log:Oct  1 21:16:32 kali sudo:    kali : TTY=pts/0 ; PWD=/home/kali/Desktop/dir2 ; USER=root ; COMMAND=/usr/bin/grep -r specific_w
ord /var/log
grep: /var/log/journal/77a26db45fda4d88b7f079b299117424/user-1000.journal: binary file matches

(kali@kali)~$ uname -r
5.16.0-kali7-amd64

(kali@kali)~$ free -h
              total        used        free      shared  buff/cache   available
Mem:           7.7Gi        859Mi        6.2Gi         25Mi         741Mi        6.6Gi
Swap:          974Mi           0B         974Mi

(kali@kali)~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            3.9G   0    3.9G   0% /dev
tmpfs           793M  1.2M  791M   1% /run
/dev/sda1       63G   27G   33G   45% /
tmpfs           3.9G   0    3.9G   0% /dev/shm
tmpfs           5.0M   0    5.0M   0% /run/lock
tmpfs           793M  84K   793M   1% /run/user/1000

(kali@kali)~$
```

73. Check the system's uptime and load average.

74. Display the current logged-in users.

75. Check the identity of the current user.

```
kali@kali: ~/Desktop/dir2
(kali@kali)~$ uptime
21:18:14 up 1:11, 1 user, load average: 0.20, 0.24, 0.20

(kali@kali)~$ who
kali          tty7                2024-10-01 20:08 (:0)

(kali@kali)~$ whoami
kali

(kali@kali)~$
```

76. View the `/var/log/auth.log` file.

```
kali@kali: ~/Desktop/dir2
(kali@kali)~$ sudo cat /var/log/auth.log
Sep 26 19:45:50 kali lightdm: pam_unix(lightdm-greeter:session): session opened for user lightdm(uid=138) by (uid=0)
Sep 26 19:45:50 kali systemd-logind[570]: New session c1 of user lightdm.
Sep 26 19:45:50 kali systemd: pam_unix(systemd-user:session): session opened for user lightdm(uid=138) by (uid=0)
Sep 26 19:46:26 kali lightdm: gkr-pam: unable to locate daemon control file
Sep 26 19:46:26 kali lightdm: gkr-pam: stashed password to try later in open session
Sep 26 19:46:27 kali lightdm: pam_unix(lightdm-greeter:session): session closed for user lightdm
Sep 26 19:46:27 kali systemd-logind[570]: Removed session c1.
Sep 26 19:46:27 kali lightdm: pam_unix(lightdm-session): session opened for user kali(uid=1000) by (uid=0)
```

77. Shred the `auth.log` file securely.

78. How do you lock a user account to prevent them from logging in.

```
(kali@kali)-[~/Desktop/dir2]
$ sudo shred -u /var/log/auth.log
shred: /var/log/auth.log: failed to open for writing: No such file or directory

(kali@kali)-[~/Desktop/dir2]
$ sudo passwd -l anas
passwd: password changed.
```

79. What command would you use to change a user's default shell.

chsh -s /bin/bash username

80. Display the system's boot messages.

```
0.000000] BIOS-e820: [mem 0x00000000bfefff00-0x00000000bfefffff] ACPI NVS
0.000000] BIOS-e820: [mem 0x00000000bfff0000-0x00000000bfffffff] usable
0.000000] BIOS-e820: [mem 0x00000000f0000000-0x00000000f7ffffff] reserved
0.000000] BIOS-e820: [mem 0x00000000fec00000-0x00000000fec0ffff] reserved
0.000000] BIOS-e820: [mem 0x00000000fee00000-0x00000000fee0ffff] reserved
0.000000] BIOS-e820: [mem 0x00000000fffe0000-0x00000000ffffffff] reserved
0.000000] BIOS-e820: [mem 0x0000000100000000-0x000000023fffffff] usable
0.000000] NX (Execute Disable) protection: active
0.000000] SMBIOS 2.7 present.
0.000000] DMI: VMware, Inc. VMware Virtual Platform/440BX Desktop Reference Platform, BIOS 6.00 11/12/2020
0.000000] vmware: hypercall mode: 0x02
0.000000] Hypervisor detected: VMware
0.000000] vmware: TSC freq read from hypervisor : 1991.999 MHz
0.000000] vmware: Host bus clock speed read from hypervisor : 66000000 Hz
0.000000] vmware: using clock offset of 17966500760 ns
0.000011] tsc: Detected 1991.999 MHz processor
0.000908] e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
0.000911] e820: remove [mem 0x000a0000-0x000fffff] usable
0.000914] last_pfn = 0x240000 max_arch_pfn = 0x400000000
0.000931] x86/PAT: Configuration [0-7]: WB WC UC- UC WB WP UC- WT
0.000939] e820: update [mem 0xc0000000-0xffffffff] usable ==> reserved
0.000944] last_pfn = 0xc0000 max_arch_pfn = 0x400000000
0.007859] found SMP MP-table at [mem 0x000f6a70-0x000f6a7f]
0.007875] Using GB pages for direct mapping
0.008049] RAMDISK: [mem 0x2f8f3000-0x33c70fff]
0.008054] ACPI: Early table checksum verification disabled
0.008056] ACPI: RSDP 0x000000000000f6a0 000024 (v02 PTLTD )
0.008059] ACPI: XSDT 0x00000000bfeea65b 00005c (v01 INTEL 440BX 06040000 VMW 01324272)
0.008064] ACPI: FACP 0x00000000bfeefe73 0000f4 (v04 INTEL 440BX 06040000 PTL 000f4240)
```

