Kali Linux

أوامر في الكالي وادوات

Eng/ Abu Ali
الرازي المجموعة 2 عملي

بسم الله الرحمن الرحيم

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 -la
total 348
drwx------ 19 kali kali   4096 Sep 10 11:15 .
drwxr-xr-x  4 root root   4096 Sep  3 11:38 ..
-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 11 kali kali   4096 Aug 30 04:45 .cache
drwxr-xr-x 14 kali kali   4096 Jul 23 16:07 .config
drwxr-xr-x  5 kali kali   4096 Aug 29 03:54 Desktop
-rw-r--r--  1 kali kali     35 Aug 29 03:23 .dmrc
drwxr-xr-x  2 kali kali   4096 Jul 21 02:10 Documents
drwxr-xr-x  2 kali kali   4096 Jul 21 02:10 Downloads
-rw-r--r--  1 kali kali  11759 Aug 21  2023 .face
lrwxrwxrwx  1 kali kali      5 Aug 21  2023 .face.icon -> .face
drwxr-xr-x  3 kali kali   4096 Aug 30 05:46 fakecall
drwx------  3 kali kali   4096 Jul 21 02:10 .gnupg
-rw-------  1 kali kali      0 Jul 21 02:10 .ICEauthority
drwxr-xr-x  4 kali kali   4096 Aug 15 03:39 .java
drwxr-xr-x  4 kali kali   4096 Jul 21 02:10 .local
drwx------  4 kali kali   4096 Aug 22 04:35 .mozilla
drwxr-xr-x 11 kali kali   4096 Aug 30 04:57 .msf4
drwxr-xr-x  2 kali kali   4096 Jul 21 02:10 Music
drwxr-xr-x  2 kali kali   4096 Jul 21 02:10 Pictures
-rw-r--r--  1 kali kali    807 Aug 21  2023 .profile
drwxr-xr-x  2 kali kali   4096 Jul 21 02:10 Public
-rw-r--r--  1 kali kali      0 Jul 27 14:32 .sudo_as_admin_successful
drwxr-xr-x  2 kali kali   4096 Jul 21 02:10 Templates
drwxr-xr-x  2 kali kali   4096 Jul 21 02:10 Videos
-rw-------  1 kali kali    532 Aug  8 04:43 .viminfo
drwxr-xr-x  2 kali kali   4096 Jul 27 14:27 work
```

3.Change your directory to the `Desktop`.

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

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

```
┌──(kali㉿kali)-[~/Desktop]
└─$ mkdir dir1
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ mkdir dir2
```

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

```
┌──(kali㉿kali)-[~/Desktop/dir1]
└─$ ls
file1.txt
```

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

```
┌──(kali㉿kali)-[~]
└─$ touch Desktop/dir1/file1.txt
```

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

```
┌──(kali㉿kali)-[~]
└─$ nano Desktop/dir1/file1.txt
```

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

```
┌──(kali㉿kali)-[~]
└─$ cp Desktop/dir1/file1.txt  Desktop/dir2/file2.txt
```

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

```
┌──(kali㉿kali)-[~]
└─$ rm Desktop/dir1/file1.txt

┌──(kali㉿kali)-[~]
└─$ ls Desktop/dir1
```

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

```
┌──(kali㉿kali)-[~]
└─$ rmdir Desktop/dir1

┌──(kali㉿kali)-[~]
└─$ ls Desktop
ali  dir2  file2.txt  network_info.txt  network_inf.txt
```

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

```
┌──(kali㉿kali)-[~]
└─$ ifconfig > ~/Desktop network_info.txt
```

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

```
┌──(kali㉿kali)-[~]
└─$ ifconfig > ~/Desktop network_info.txt
```

Section 2: Users and Groups Management:

13.Create a new user with your name.

```
┌──(kali㉿kali)-[~]
└─$ sudo adduser salah
info: Adding user `salah' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `salah' (1007) ...
info: Adding new user `salah' (1007) with group `salah (1007)' ...
info: Creating home directory `/home/salah' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for salah
Enter the new value, or press ENTER for the default
        Full Name []: kali
        Room Number []: kali
        Work Phone []: 77
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
info: Adding new user `salah' to supplemental / extra groups `users' ...
info: Adding user `salah' to group `users' ...
```

14.Set a password for your user.

```
┌──(kali㉿kali)-[~]
└─$ sudo passwd salah
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.

```
┌──(kali㉿kali)-[~]
└─$ cat /etc/passwd |grep salah
salah:x:1007:1007:kali,kali,77,:/home/salah:/bin/bash
```

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

```
┌──(kali㉿kali)-[~]
└─$ sudo usermod -aG sudo salah
```

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

```
┌──(kali㉿kali)-[~]
└─$ su salah
Password:
┌──(salah㉿kali)-[/home/kali]
```

18.Create a new group named testgroup.

```
┌──(kali㉿kali)-[~]
└─$ sudo groupadd testgroups
```

19.Add your user to testgroup.

```
┌──(kali㉿kali)-[~]
└─$ sudo usermod -aG testgroups salah
```

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

```
┌──(kali㉿kali)-[~]
└─$ sudo usermod -aG sudo testgroups salah
Usage: usermod [options] LOGIN

Options:
  -a, --append                  append the user to the supplemental GROUPS
                                mentioned by the -G option without removing
                                the user from other groups
  -b, --badname                 allow bad names
  -c, --comment COMMENT         new value of the GECOS field
  -d, --home HOME_DIR           new home directory for the user account
  -e, --expiredate EXPIRE_DATE  set account expiration date to EXPIRE_DATE
  -f, --inactive INACTIVE       set password inactive after expiration
                                to INACTIVE
  -g, --gid GROUP               force use GROUP as new primary group
  -G, --groups GROUPS           new list of supplementary GROUPS
  -h, --help                    display this help message and exit
  -l, --login NEW_LOGIN         new value of the login name
  -L, --lock                    lock the user account
  -m, --move-home               move contents of the home directory to the
                                new location (use only with -d)
  -o, --non-unique              allow using duplicate (non-unique) UID
  -p, --password PASSWORD       use encrypted password for the new password
```

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

```
┌──(kali㉿kali)-[~]
└─$ sudo deluser salah
info: Removing crontab ...
info: Removing user `salah' ...
userdel: user salah is currently used by process 275594
fatal: `/usr/sbin/userdel salah' returned error code 8. Exiting.
```

22.Check if your user still have administrative privileges.

```
┌──(kali㉿kali)-[~]
└─$ sudo -l
Matching Defaults entries for kali on kali:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:

User kali may run the following commands on kali:
    (ALL : ALL) ALL
```

23.Check which groups your user belongs to.

```
┌──(kali㉿kali)-[~]
└─$ groups salah
salah : salah sudo users testgroups
```

Section 2: Users and Groups Management:

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 .**

```
┌──(kali㉿kali)-[~/Desktop]
└─$ chmod 775 /dir2/file2.txt
```

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

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ls -l dir2/file2.txt
-rwxrwxr-x 1 hemeed testgroup 19 Sep 12 03:58 dir2/file2.txt
```

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

```
┌──(kali㉿kali)-[~]
└─$ sudo chown hemeed  ~/Desktop/dir2/file2.txty
```

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

```
┌──(kali㉿kali)-[~]
└─$ ls -l ~/Desktop/dir2/file2.txt
-rwxrwxr-x 1 hemeed testgroup 19 Sep 12 03:58 /home/kali/Desktop/dir2/file2.txt
```

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

```
┌──(kali㉿kali)-[~]
└─$ sudo chown root  ~/Desktop/dir2/file2.txty
```

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

```
┌──(kali㉿kali)-[~]
└─$ sudo chmod a+w  ~/Desktop/dir2/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.

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

Section 4: process Management:

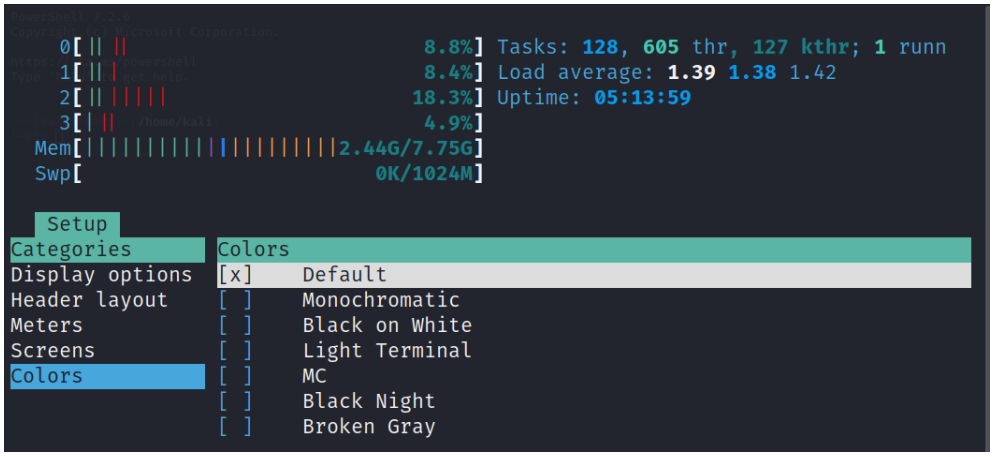
33.Install a system monitor tool that provides an interactive process viewer(htop).

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install htop
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
htop is already the newest version (3.3.0-4).
0 upgraded, 0 newly installed, 0 to remove and 2050 not upgraded.
```

34.Display all running processes.

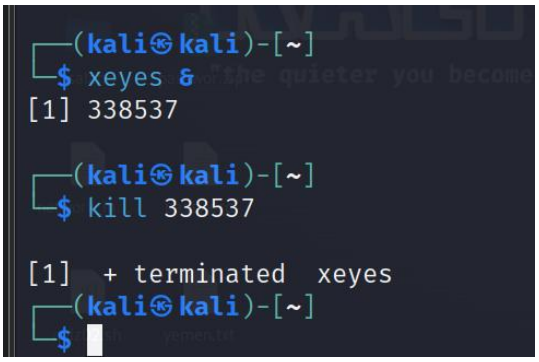
35.Display a tree of all running processes.

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

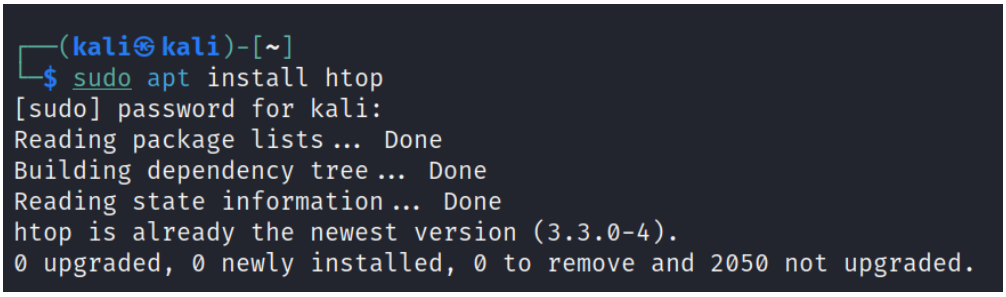


37.Kill a process with a specific PID.

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



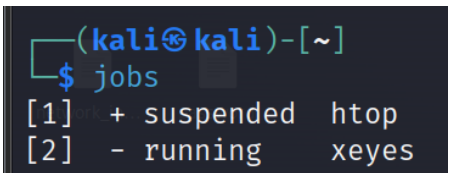
39.Restart the application, then stop it using the interactive process viewer.



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

41.Check how long the system has been running.

42.List all jobs running in the background.



Section 5: Networking Commands:

43.Display the network configuration.

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.222.128  netmask 255.255.255.0  broadcast 192.168.222
.255
        inet6 fe80::484:54cd:ea06:ad6b  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:87:de:de  txqueuelen 1000  (Ethernet)
        RX packets 4780  bytes 994222 (970.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1552  bytes 142243 (138.9 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 3401  bytes 1423416 (1.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3401  bytes 1423416 (1.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

44.Check the IP address of your machine.

```
┌──(kali㉿kali)-[~]
└─$ hostname -I
192.168.222.128
```

45.Test connectivity to an external server.

```
┌──(kali㉿kali)-[~]
└─$ ping example.com
```

46.Display the routing table.

```
┌──(kali㉿kali)-[~]
└─$ ip rout show
default via 192.168.222.2 dev eth0 proto dhcp src 192.168.222.128 metric 1
00
192.168.222.0/24 dev eth0 proto kernel scope link src 192.168.222.128 metr
ic 100
```

47.Check the open ports and active connections.

```
┌──(kali㉿kali)-[~]
└─$ netstat -tuln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State

┌──(kali㉿kali)-[~]
└─$ ss -tuln
Netid State Recv-Q Send-Q  Local Address:Port   Peer Address:Port Process
```

48.Show the IP address of the host machine and the VM, and verify if they are on the same network.

```
┌──(kali㉿kali)-[~]
└─$ uptime
 10:39:22 up  5:38,  1 user,  load average: 0.03, 0.17, 0.54
```

49.Trace the route to an external server.

```
┌──(kali㉿kali)-[~]
└─$ traceroute 192.168.222.128
traceroute to 192.168.222.128 (192.168.222.128), 30 hops max, 60 byte pack
ets
 1  192.168.222.128 (192.168.222.128)  0.285 ms  0.015 ms  0.010 ms

┌──(kali㉿kali)-[~]
└─$ traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  192.168.222.2 (192.168.222.2)  0.374 ms  0.306 ms  0.184 ms
 2  192.168.222.2 (192.168.222.2)  0.390 ms !H  0.270 ms !H  0.252 ms !H
```

50.Find out the default gateway.

```
┌──(kali㉿kali)-[~]
└─$ sudo ip route | grep defaulte
[sudo] password for kali:
```

51.Check the MAC address of your network interface.

```
┌──(kali㉿kali)-[~]
└─$ ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode D
EFAULT 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 U
P mode DEFAULT group default qlen 1000
    link/ether 00:0c:29:87:de:de brd ff:ff:ff:ff:ff:ff
```

52.Ensure that the VM can access external networks.

```
┌──(kali㉿kali)-[~]
└─$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
From 192.168.222.2 icmp_seq=1 Destination Host Unreachable
From 192.168.222.2 icmp_seq=2 Destination Host Unreachable
From 192.168.222.2 icmp_seq=3 Destination Host Unreachable
From 192.168.222.2 icmp_seq=4 Destination Host Unreachable
From 192.168.222.2 icmp_seq=5 Destination Host Unreachable
From 192.168.222.2 icmp_seq=6 Destination Host Unreachable
From 192.168.222.2 icmp_seq=7 Destination Host Unreachable
```

Section 6: UFW Firewall :

53.Enable the firewall.

```
┌──(kali㉿kali)-[~]
└─$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
From 192.168.222.2 icmp_seq=1 Destination Host Unreachable
From 192.168.222.2 icmp_seq=2 Destination Host Unreachable
From 192.168.222.2 icmp_seq=3 Destination Host Unreachable
From 192.168.222.2 icmp_seq=4 Destination Host Unreachable
From 192.168.222.2 icmp_seq=5 Destination Host Unreachable
From 192.168.222.2 icmp_seq=6 Destination Host Unreachable
From 192.168.222.2 icmp_seq=7 Destination Host Unreachable
```

54.Allow SSH connections through the firewall.

1. Deny all incoming traffic by default.
2. Allow HTTP and HTTPS traffic.
3. Allow port 20
4. Reset the firewall settings.
5. Delete a rule from the firewall.
6. Disable the firewall.
7. View the status of the firewall.
8. Log firewall activity and view it.

Section 7: Searching and System Information:

63.Delete the command history.

```
┌──(kali㉿kali)-[~]
└─$ history -c
```

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

```
┌──(kali㉿kali)-[~/Desktop]
└─$ grep kali /etc/passwd
kali:x:1000:1000:,,,:/home/kali:/usr/bin/zsh
hemeed:x:1005:1005:kali,kali,kali,kali,kali:/home/hemeed:/bin/bash
salah:x:1007:1007:kali,kali,77,:/home/salah:/bin/bash
```

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

```
┌──(kali㉿kali)-[~/Desktop]
└─$ grep kali /etc/group
adm:x:4:kali
dialout:x:20:kali
cdrom:x:24:kali
floppy:x:25:kali
sudo:x:27:kali,salah
audio:x:29:pulse,kali
dip:x:30:kali
video:x:44:kali
plugdev:x:46:kali
users:x:100:kali,ali,moh,hemead,hemeed,salah
netdev:x:106:kali
bluetooth:x:111:kali
scanner:x:117:saned,kali
kali-trusted:x:123:
wireshark:x:140:kali
kali:x:1000:
kaboxer:x:142:kali
```

66.Locate the `passwd` file.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ which passwd
/usr/bin/passwd
```

67.**Locate the shadow file and open it.**

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo cat /etc/shadow
[sudo] password for kali:
root:*:19590:0:99999:7:::
daemon:*:19590:0:99999:7:::
bin:*:19590:0:99999:7:::
sys:*:19590:0:99999:7:::
sync:*:19590:0:99999:7:::
games:*:19590:0:99999:7:::
man:*:19590:0:99999:7:::
lp:*:19590:0:99999:7:::
mail:*:19590:0:99999:7:::
news:*:19590:0:99999:7:::
uucp:*:19590:0:99999:7:::
proxy:*:19590:0:99999:7:::
```

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

```
┌──(kali㉿kali)-[~/Desktop]
└─$ find /etc -type f -name "*.conf"
/etc/ts.conf
/etc/smartd.conf
/etc/freetds/freetds.conf
/etc/plymouth/plymouthd.conf
/etc/resolv.conf
/etc/sensors3.conf
/etc/udev/udev.conf
/etc/udev/iocost.conf
/etc/avahi/avahi-daemon.conf
/etc/john/john-mail.conf
/etc/john/john.conf
/etc/nginx/snippets/fastcgi-php.conf
/etc/nginx/snippets/snakeoil.conf
/etc/nginx/fastcgi.conf
/etc/nginx/nginx.conf
/etc/snmp/snmp.conf
```

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

```
┌──(kali㉿kali)-[~/Desktop]
└─$ grep -r "var" /var/log
grep: /var/log/vmware-vmsvc-root.1.log: Permission denied
/var/log/Xorg.1.log.old:[ 20944.964] (==) Log file: "/var/log/Xorg.1.log",
 Time: Wed Sep 25 10:49:39 2024
grep: /var/log/boot.log: Permission denied
grep: /var/log/private: Permission denied
/var/log/fontconfig.log:/var/cache/fontconfig: cleaning cache directory
grep: /var/log/boot.log.2: Permission denied
/var/log/Xorg.0.log:[ 19178.364] (==) Log file: "/var/log/Xorg.0.log", Tim
e: Wed Sep 25 10:20:13 2024
grep: /var/log/btmp: Permission denied
grep: /var/log/boot.log.1: Permission denied
grep: /var/log/speech-dispatcher: Permission denied
grep: /var/log/vmware-vmsvc-root.2.log: Permission denied
/var/log/dpkg.log.1:2023-08-21 16:27:02 install libefivar1:amd64 <none> 37
-6
/var/log/dpkg.log.1:2023-08-21 16:27:02 status half-installed libefivar1:a
md64 37-6
/var/log/dpkg.log.1:2023-08-21 16:27:02 status unpacked libefivar1:amd64 3
7-6
```

70.View the system’s kernel version.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ uname -r
6.3.0-kali1-amd64
```

71.Display the system’s memory usage.

```
└─$ free -h
               total        used        free      shared  buff/cache   availabl
e
Mem:           7.7Gi       922Mi       5.0Gi       5.9Mi       2.1Gi       6.8G
i
Swap:          1.0Gi          0B       1.0Gi
```

72.Show the system’s disk usage.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            3.9G     0  3.9G   0% /dev
tmpfs           794M  1.3M  793M   1% /run
/dev/sda1        79G   15G   60G  21% /
tmpfs           3.9G     0  3.9G   0% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           794M  116K  794M   1% /run/user/1000
```

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

```
┌──(kali㉿kali)-[~/Desktop]
└─$ uptime
 12:17:10 up  7:12,  1 user,  load average: 0.24, 0.18, 0.18
```

74.**Display the current logged-in users.**

```
┌──(kali㉿kali)-[~/Desktop]
└─$ who
kali     tty7         2024-09-25 10:20 (:0)
```

75.Check the identity of the current user.

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

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

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo less /var/log/auth.log
/var/log/auth.log: No such file or directory
```

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

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

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

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo usermod -L salah
```

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

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo chsh -s /bin/bash salah
```

80.Display the system's boot messages.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ grep kali /etc/passwd
kali:x:1000:1000:,,,:/home/kali:/usr/bin/zsh
hemeed:x:1005:1005:kali,kali,kali,kali,kali:/home/hemeed:/bin/bash
salah:x:1007:1007:kali,kali,77,:/home/salah:/bin/bash
```