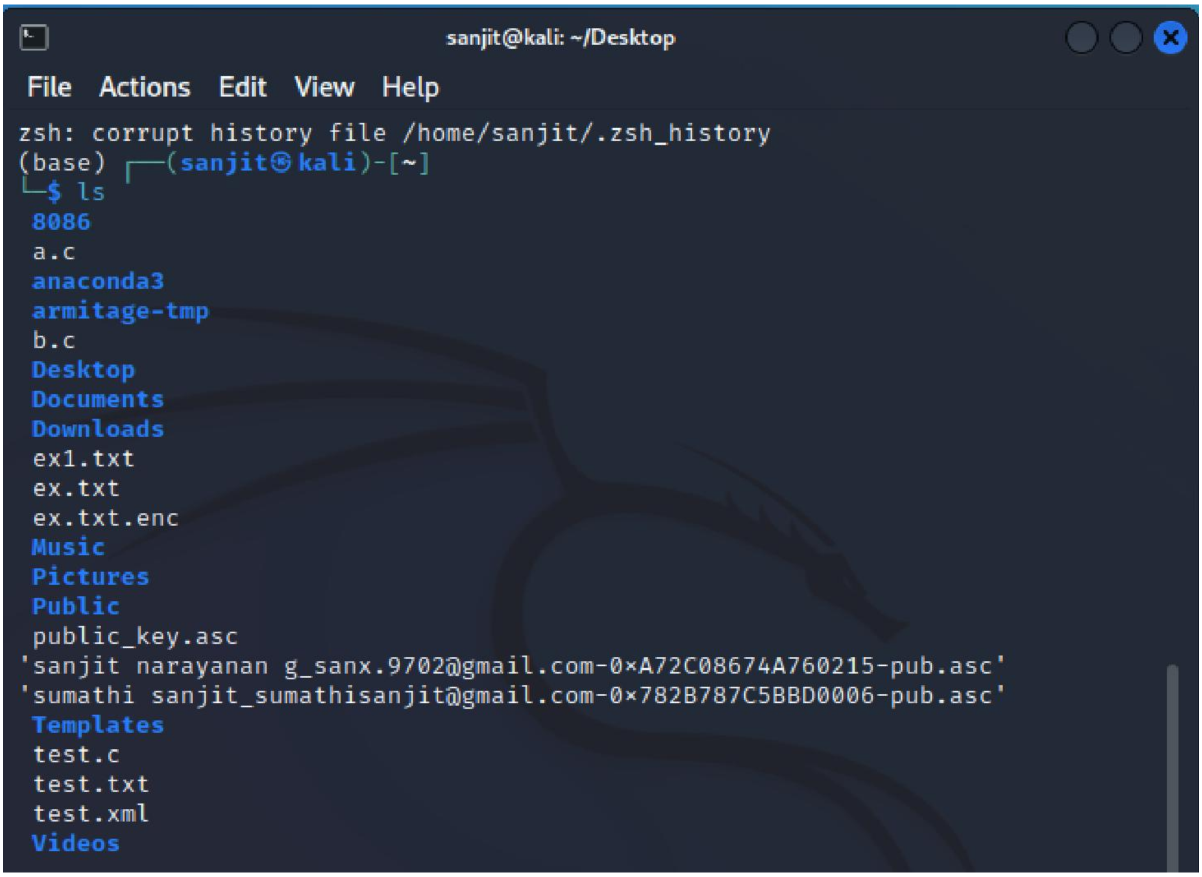
SANJIT NARAYANAN G
20BCE0052
CYBER SECURITY AND ETHICAL HACKING ASSIGNMENT - 1

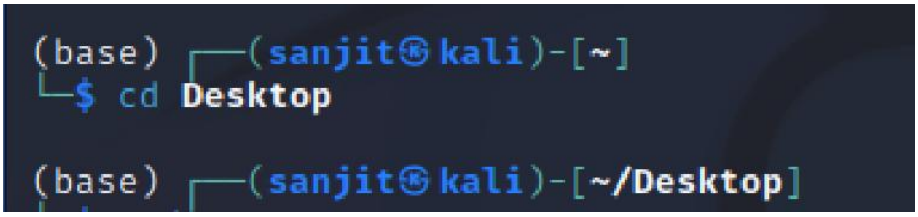
FILE AND DIRECTORY OPERATIONS:

1. LS :



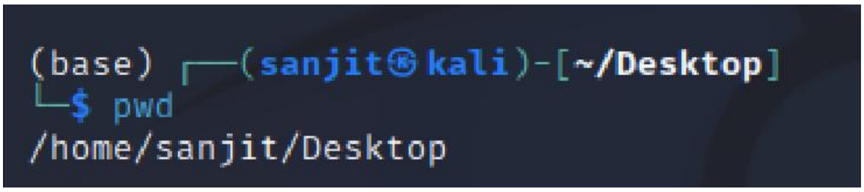
```
zsh: corrupt history file /home/sanjit/.zsh_history
(base) ┌──(sanjit㉿kali)-[~]
└─$ ls
 8086
 a.c
 anaconda3
 armitage-tmp
 b.c
 Desktop
 Documents
 Downloads
 ex1.txt
 ex.txt
 ex.txt.enc
 Music
 Pictures
 Public
 public_key.asc
'sanjit narayanan g_sanx.9702@gmail.com-0×A72C08674A760215-pub.asc'
'sumathi sanjit_sumathisanjit@gmail.com-0×782B787C5BBD0006-pub.asc'
 Templates
 test.c
 test.txt
 test.xml
 Videos
```

2. CD :



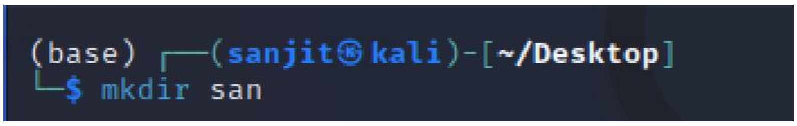
```
(base) ┌──(sanjit㉿kali)-[~]
└─$ cd Desktop

(base) ┌──(sanjit㉿kali)-[~/Desktop]
```

3. PWD :



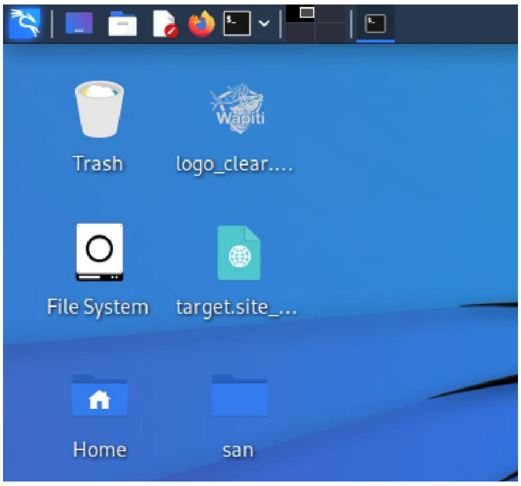
```
(base) ┌──(sanjit㉿kali)-[~/Desktop]
└─$ pwd
/home/sanjit/Desktop
```

4. MKDIR :

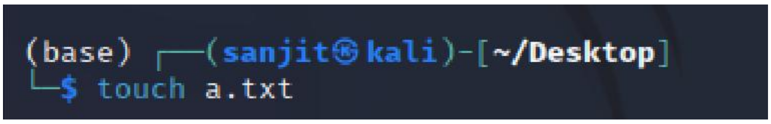


```
(base) ┌──(sanjit㉿kali)-[~/Desktop]
└─$ mkdir san
```

YOU CAN SEE THAT THE DIRECTORY SAN IS CREATED IN DESKTOP :

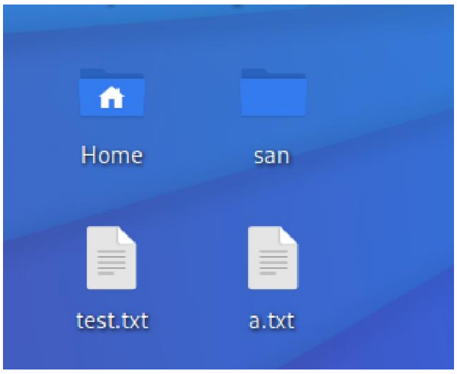


5. CREATE AN EMPTY FILE :

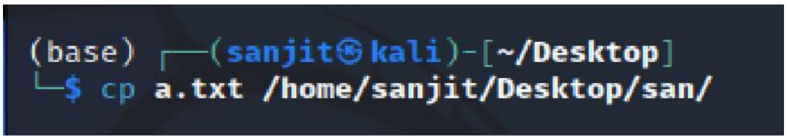


```
(base) ┌──(sanjit㉿kali)-[~/Desktop]
└─$ touch a.txt
```

YOU CAN SEE THAT AN EMPTY FILE NAME a.txt IS CREATED IN DESKTOP :

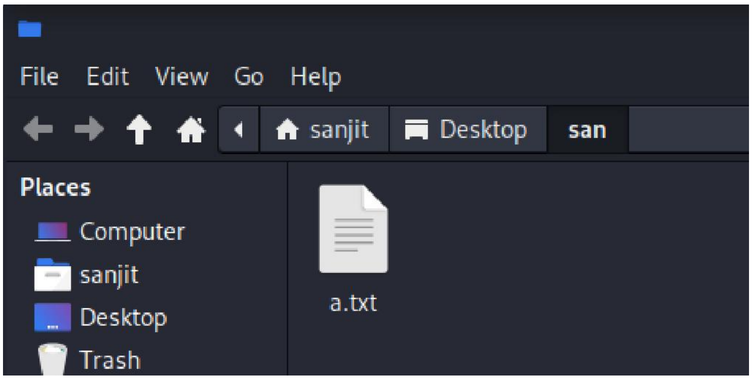


6. COPY FILES AND DIRECTORIES :

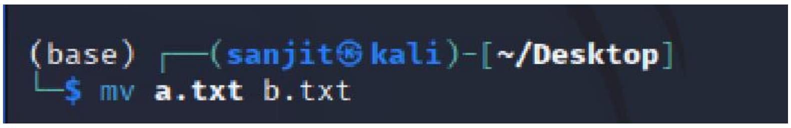


```
(base) ┌──(sanjit㉿kali)-[~/Desktop]
└─$ cp a.txt /home/sanjit/Desktop/san/
```

YOU CAN SEE THAT a.txt IS PRESENT IN THE SAN DIRECTORY :

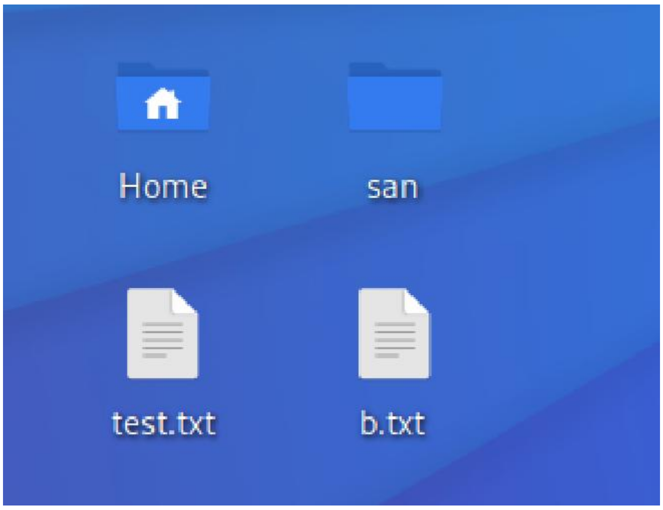


7. MOVE OR RENAME FILES AND DIRECTORIES :

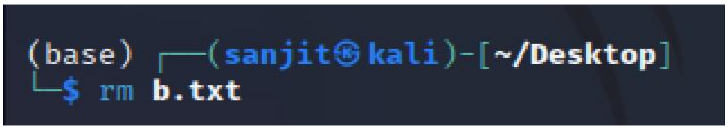


```
(base) ┌──(sanjit㉿kali)-[~/Desktop]
└─$ mv a.txt b.txt
```

YOU CAN SEE THAT a.txt IS BEEN RENAMED/MOVED TO b.txt :

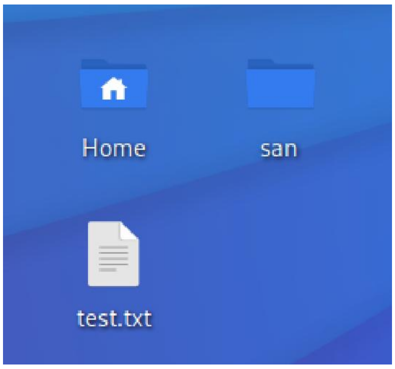


8. REMOVE FILES AND DIRECTORIES :

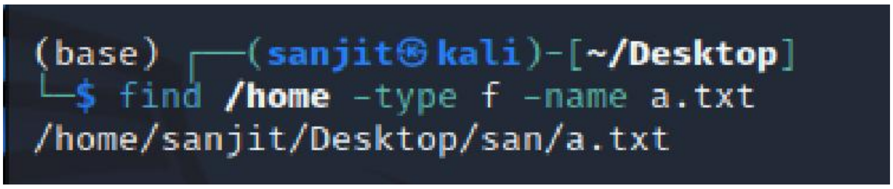


```
(base) ┌──(sanjit㉿kali)-[~/Desktop]
└─$ rm b.txt
```

YOU CAN SEE THAT b.txt HAS BEEN REMOVED :



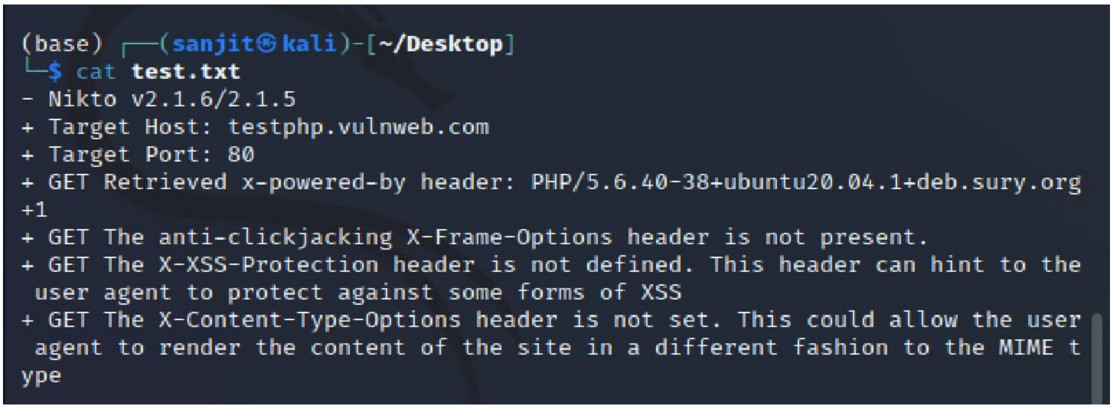
9. SEARCH FOR FILES AND DIRECTORIES :



```
(base) ┌──(sanjit㉿kali)-[~/Desktop]
└─$ find /home -type f -name a.txt
/home/sanjit/Desktop/san/a.txt
```

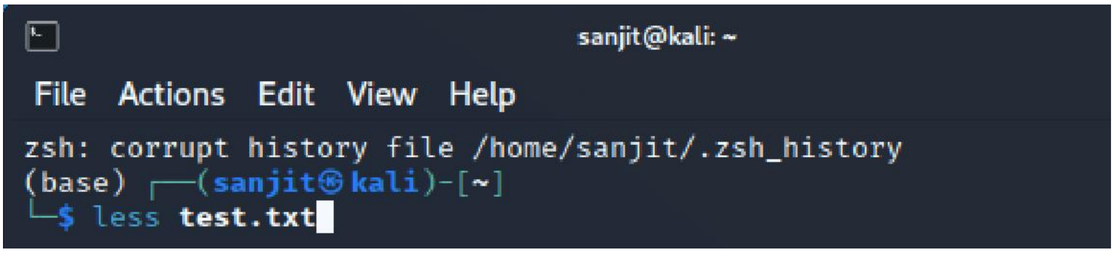
FILE VIEWING AND EDITING:

1. CONCATENATE AND DISPLAY FILE CONTENT :

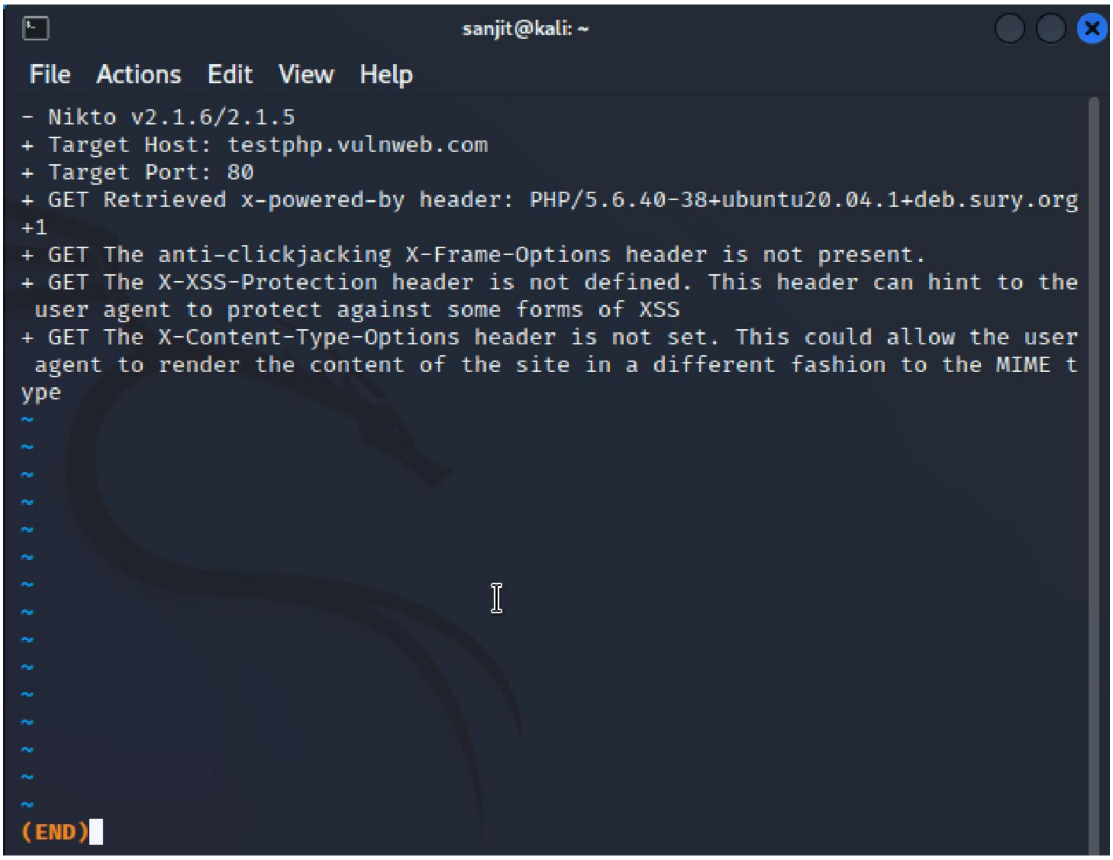


```
(base) ┌──(sanjit㉿kali)-[~/Desktop]
└─$ cat test.txt
- Nikto v2.1.6/2.1.5
+ Target Host: testphp.vulnweb.com
+ Target Port: 80
+ GET Retrieved x-powered-by header: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org
+1
+ GET The anti-clickjacking X-Frame-Options header is not present.
+ GET The X-XSS-Protection 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 t
ype
```

2. VIEW FILE CONTENT WITH PAGINATION :

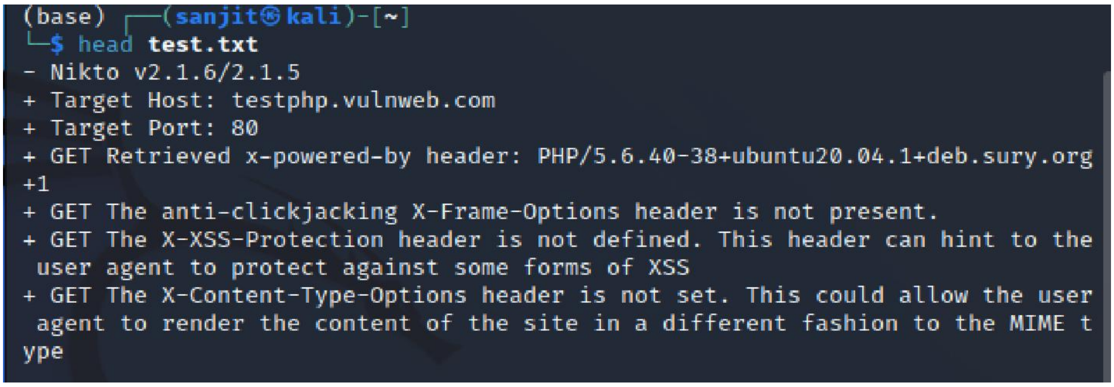


```
zsh: corrupt history file /home/sanjit/.zsh_history
(base) ┌──(sanjit㉿kali)-[~]
└─$ less test.txt
```



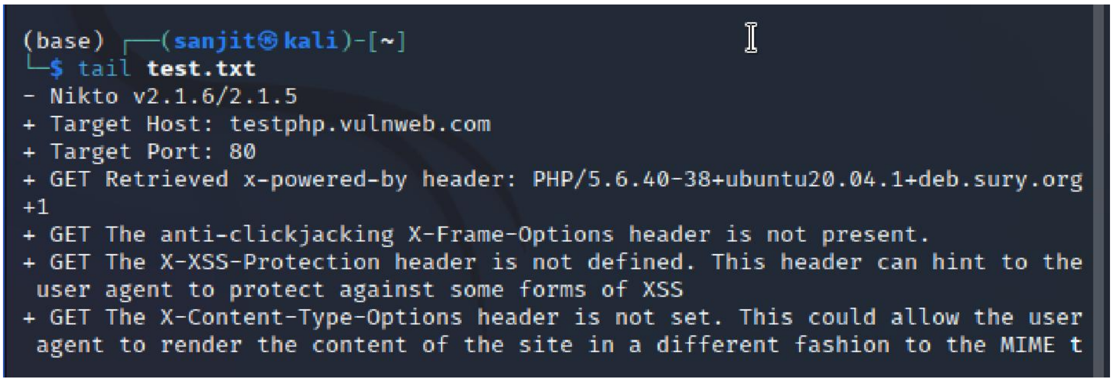
```
- Nikto v2.1.6/2.1.5
+ Target Host: testphp.vulnweb.com
+ Target Port: 80
+ GET Retrieved x-powered-by header: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org
+1
+ GET The anti-clickjacking X-Frame-Options header is not present.
+ GET The X-XSS-Protection header is not defined. This header can hint to the
 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 t
ype
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
(END)
```

3. DISPLAY THE BEGINING OF FILE :



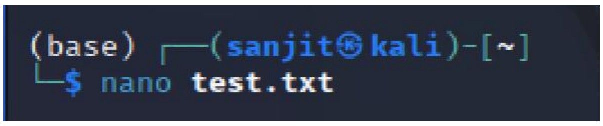
```
(base) ┌──(sanjit㉿kali)-[~]
└─$ head test.txt
- Nikto v2.1.6/2.1.5
+ Target Host: testphp.vulnweb.com
+ Target Port: 80
+ GET Retrieved x-powered-by header: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org
+1
+ GET The anti-clickjacking X-Frame-Options header is not present.
+ GET The X-XSS-Protection header 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 t
ype
```

4. DISPLAY THE END OF FILE :

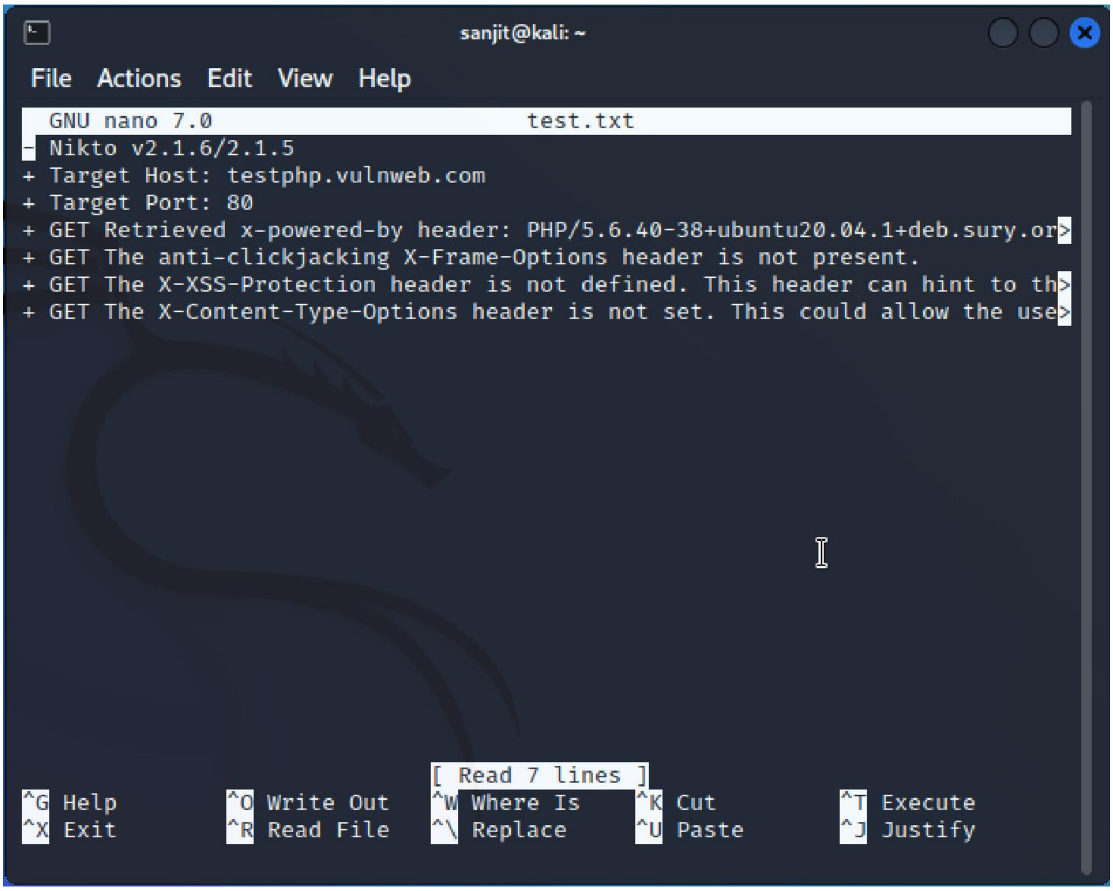


```
(base) ┌──(sanjit㉿kali)-[~]
└─$ tail test.txt
- Nikto v2.1.6/2.1.5
+ Target Host: testphp.vulnweb.com
+ Target Port: 80
+ GET Retrieved x-powered-by header: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org
+1
+ GET The anti-clickjacking X-Frame-Options header is not present.
+ GET The X-XSS-Protection header 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 t
```

5. TEXT EDITOR FOR CREATING AND EDITING FILES :

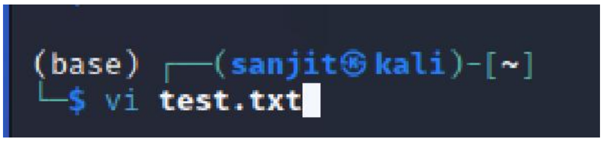


```
(base) ┌──(sanjit㉿kali)-[~]
└─$ nano test.txt
```

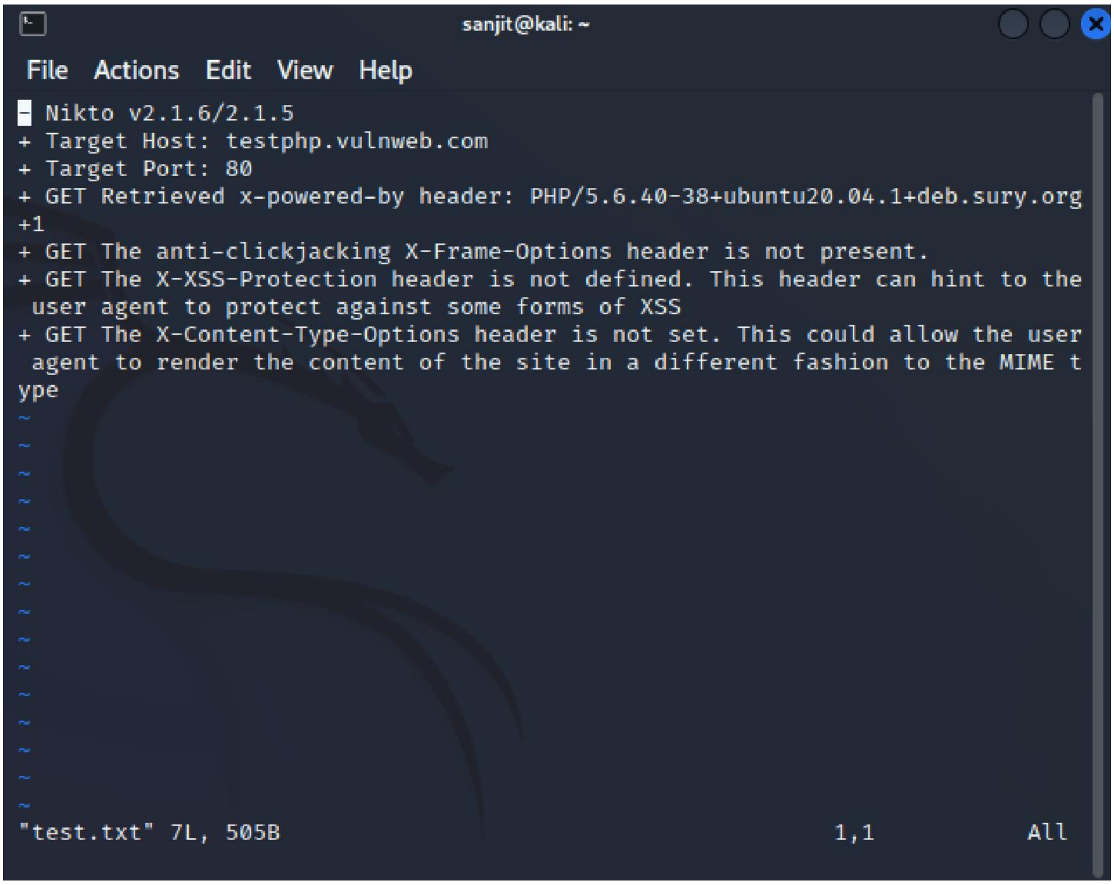


```
  GNU nano 7.0                    test.txt
- Nikto v2.1.6/2.1.5
+ Target Host: testphp.vulnweb.com
+ Target Port: 80
+ GET Retrieved x-powered-by header: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.or>
+ GET The anti-clickjacking X-Frame-Options header is not present.
+ GET The X-XSS-Protection header is not defined. This header can hint to th>
+ GET The X-Content-Type-Options header is not set. This could allow the use>









                              [ Read 7 lines ]
^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify
```

6. POWERFUL TEXT EDITOR FOR EXPERIENCED USERS :



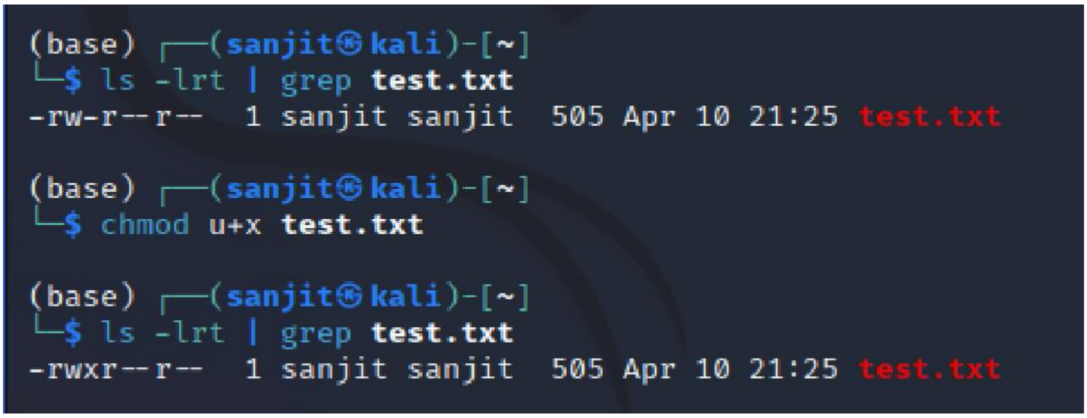
```
(base) ┌──(sanjit㉿kali)-[~]
└─$ vi test.txt
```



```
- Nikto v2.1.6/2.1.5
+ Target Host: testphp.vulnweb.com
+ Target Port: 80
+ GET Retrieved x-powered-by header: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org
+1
+ 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 t
ype
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"test.txt" 7L, 505B                                           1,1           All
```

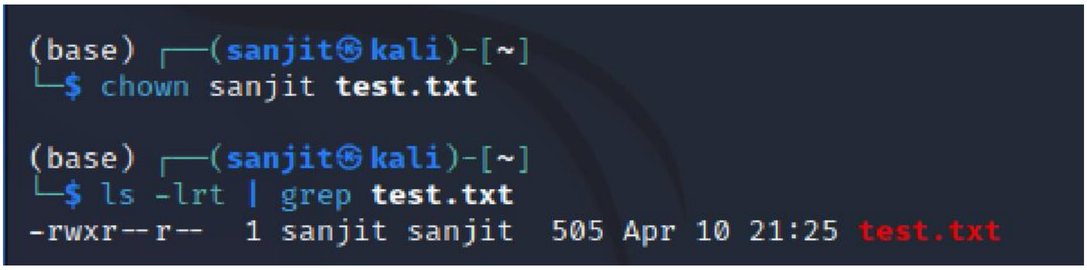
FILE PERMISSION :

1. CHANGE FILE PERMISSION :



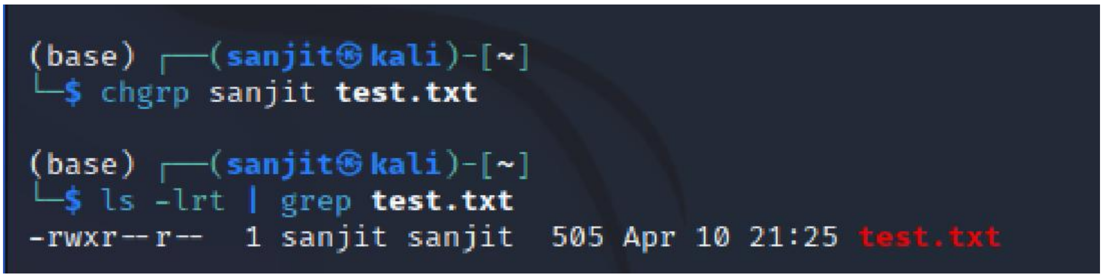
```
(base) ┌──(sanjit㉿kali)-[~]
└─$ ls -lrt | grep test.txt
-rw-r--r--  1 sanjit sanjit  505 Apr 10 21:25 test.txt

(base) ┌──(sanjit㉿kali)-[~]
└─$ chmod u+x test.txt

(base) ┌──(sanjit㉿kali)-[~]
└─$ ls -lrt | grep test.txt
-rwxr--r--  1 sanjit sanjit  505 Apr 10 21:25 test.txt
```

2. CHANGE FILE OWNER :



```
(base) ┌──(sanjit㉿kali)-[~]
└─$ chown sanjit test.txt

(base) ┌──(sanjit㉿kali)-[~]
└─$ ls -lrt | grep test.txt
-rwxr--r--  1 sanjit sanjit  505 Apr 10 21:25 test.txt
```

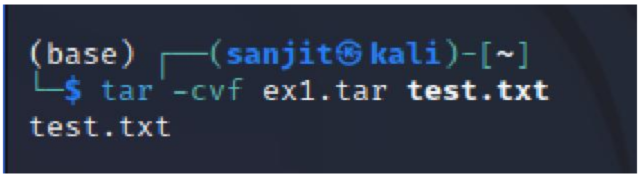
3. CHANGE FILE GROUP :



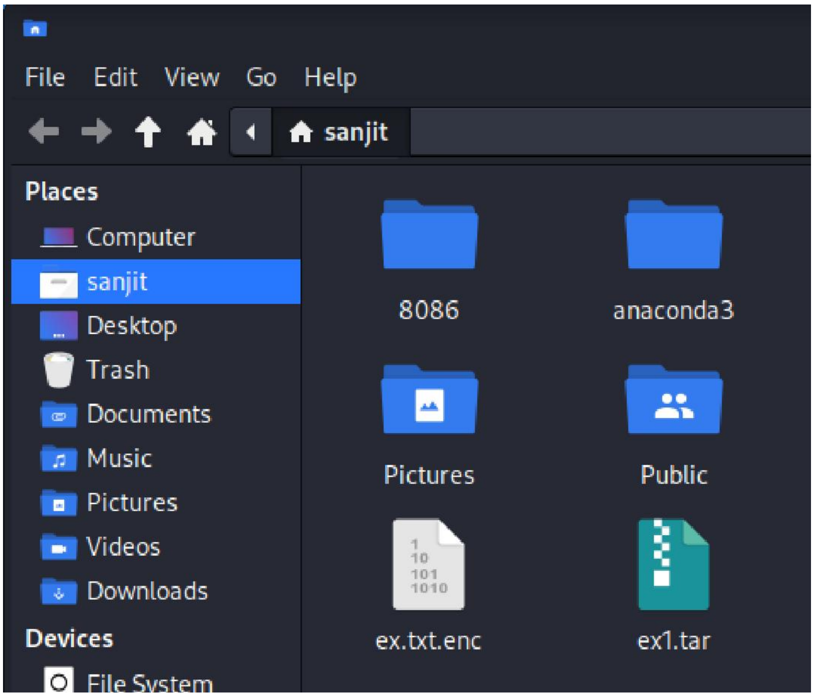
```
(base) ┌──(sanjit㉿kali)-[~]
└─$ chgrp sanjit test.txt

(base) ┌──(sanjit㉿kali)-[~]
└─$ ls -lrt | grep test.txt
-rwxr--r--  1 sanjit sanjit  505 Apr 10 21:25 test.txt
```

FILE COMPRESSION AND ARCHIVING :

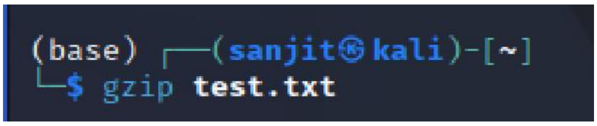
1. ARCHIVE FILES :



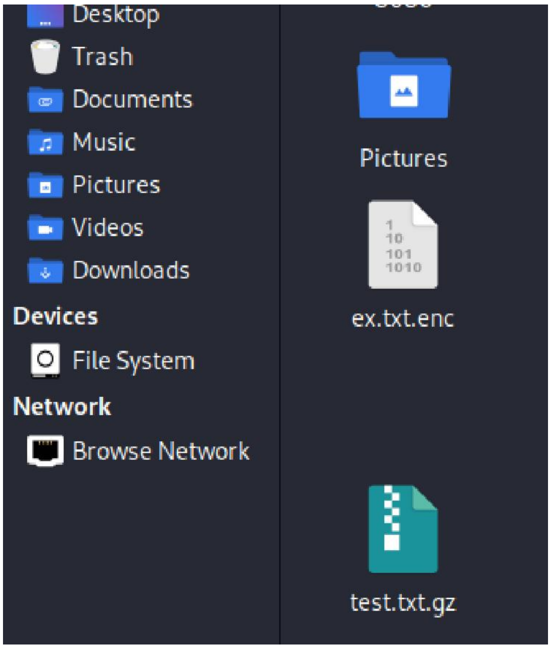
```
(base) ┌──(sanjit㉿kali)-[~]
└─$ tar -cvf ex1.tar test.txt
test.txt
```



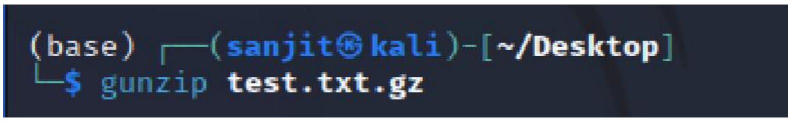
2. COMPRESS FILES :



```
(base) ┌──(sanjit㉿kali)-[~]
└─$ gzip test.txt
```

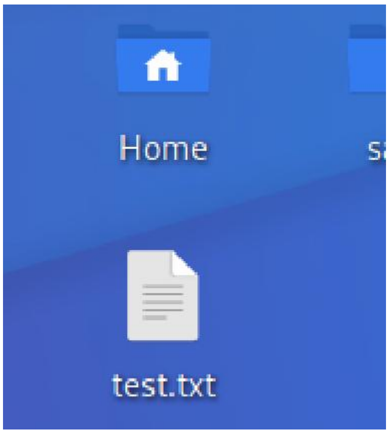


3. EXTRACT FILES FROM A ZIP-ARCHIVE :



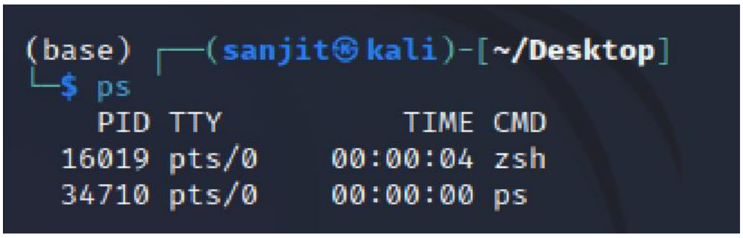
```
(base) ┌──(sanjit㉿kali)-[~/Desktop]
└─$ gunzip test.txt.gz
```

YOU CAN VIEW THE UN-ZIPPED FILE :



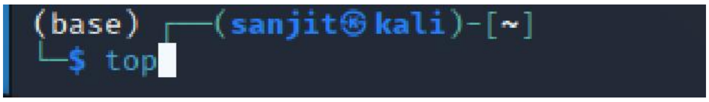
PROCESS MANAGEMENT :

1. LIST THE RUNNING PROCESS :

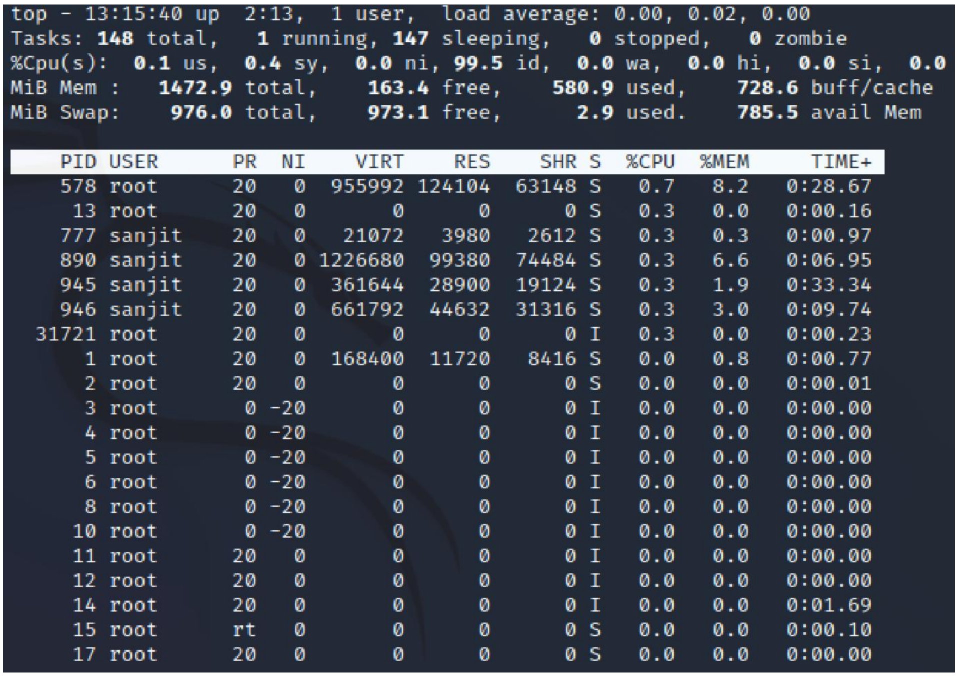


```
(base) ┌──(sanjit㉿kali)-[~/Desktop]
└─$ ps
    PID TTY          TIME CMD
  16019 pts/0    00:00:04 zsh
  34710 pts/0    00:00:00 ps
```

2. DISPLAY REAL TIME SYSTEM INFORMATION AND PROCESSES :

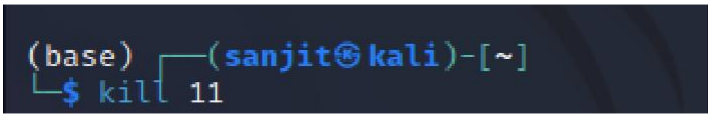


```
(base) ┌──(sanjit㉿kali)-[~]
└─$ top
```



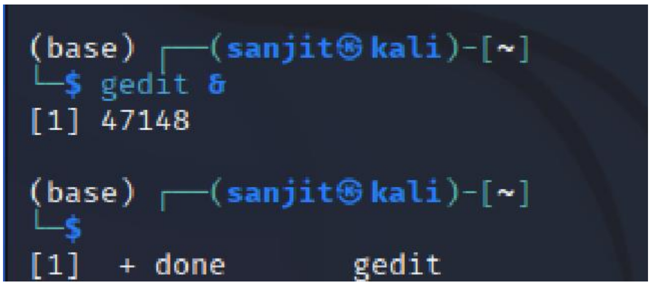
```
top - 13:15:40 up  2:13,  1 user,  load average: 0.00, 0.02, 0.00
Tasks: 148 total,   1 running, 147 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.1 us,  0.4 sy,  0.0 ni, 99.5 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0
MiB Mem :   1472.9 total,    163.4 free,    580.9 used,    728.6 buff/cache
MiB Swap:    976.0 total,    973.1 free,      2.9 used.    785.5 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+
    578 root      20   0  955992 124104  63148 S   0.7   8.2   0:28.67
     13 root      20   0       0      0      0 S   0.3   0.0   0:00.16
    777 sanjit    20   0   21072   3980   2612 S   0.3   0.3   0:00.97
    890 sanjit    20   0 1226680  99380  74484 S   0.3   6.6   0:06.95
    945 sanjit    20   0  361644  28900  19124 S   0.3   1.9   0:33.34
    946 sanjit    20   0  661792  44632  31316 S   0.3   3.0   0:09.74
  31721 root      20   0       0      0      0 I   0.3   0.0   0:00.23
      1 root      20   0  168400  11720   8416 S   0.0   0.8   0:00.77
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.01
      3 root       0 -20       0      0      0 I   0.0   0.0   0:00.00
      4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00
      5 root       0 -20       0      0      0 I   0.0   0.0   0:00.00
      6 root       0 -20       0      0      0 I   0.0   0.0   0:00.00
      8 root       0 -20       0      0      0 I   0.0   0.0   0:00.00
     10 root       0 -20       0      0      0 I   0.0   0.0   0:00.00
     11 root      20   0       0      0      0 I   0.0   0.0   0:00.00
     12 root      20   0       0      0      0 I   0.0   0.0   0:00.00
     14 root      20   0       0      0      0 I   0.0   0.0   0:01.69
     15 root      rt   0       0      0      0 S   0.0   0.0   0:00.10
     17 root      20   0       0      0      0 S   0.0   0.0   0:00.00
```

3. TO KILL A PROCESS :



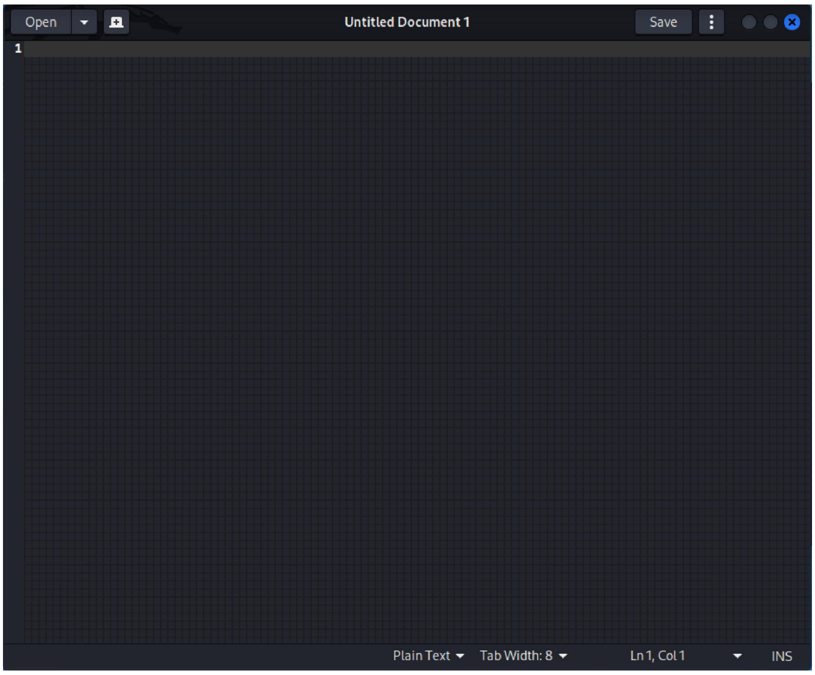
```
(base) ┌──(sanjit㉿kali)-[~]
└─$ kill 11
```

4. RUN PROCESS IN THE BACKGROUND :



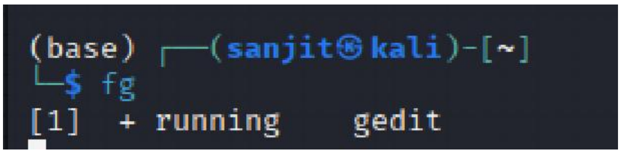
```
(base) ┌──(sanjit㉿kali)-[~]
└─$ gedit &
[1] 47148

(base) ┌──(sanjit㉿kali)-[~]
└─$
[1]  + done        gedit
```

YOU CAN SEE THAT THE EDITOR IS OPENED IN BACKGROUND :



Plain Text   Tab Width: 8   Ln 1, Col 1   INS

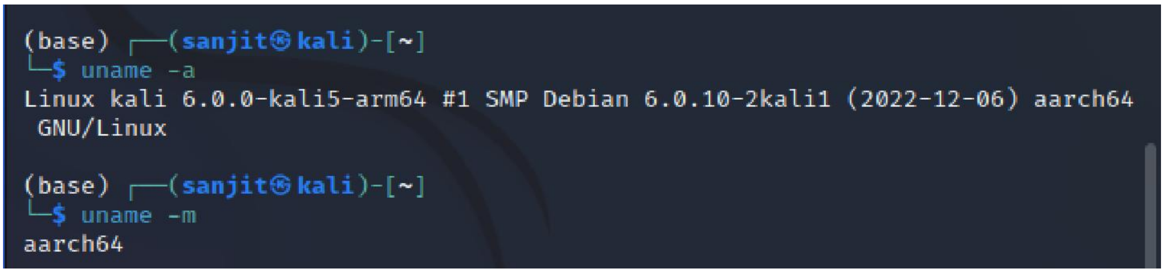
5. BRING BACKGROUNG RUNNING PROCESS TO FRONT :



```
(base) ┌──(sanjit㉿kali)-[~]
└─$ fg
[1]  + running     gedit
```

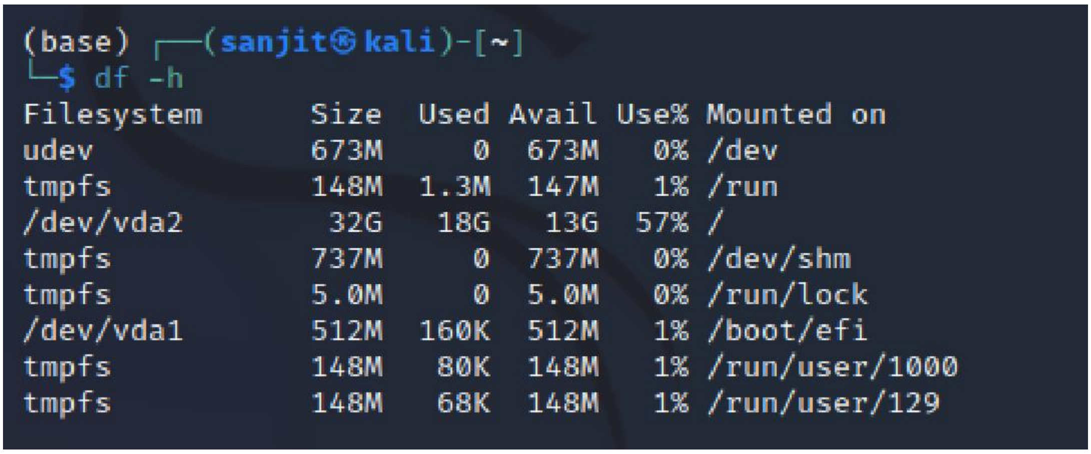
SYSTEM INFORMATION :

1. PRINT SYSTEM INFORMATION :



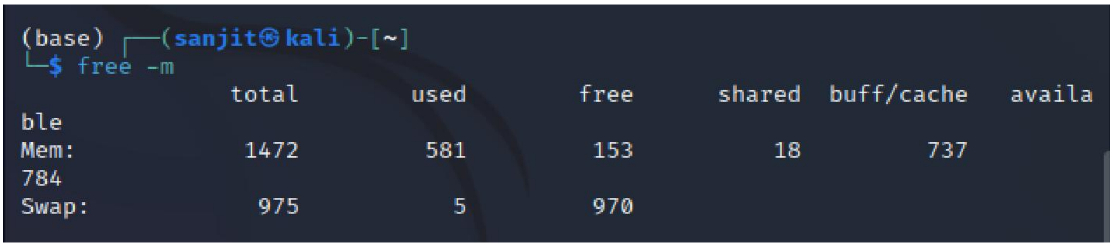
```
(base) ┌──(sanjit㉿kali)-[~]
└─$ uname -a
Linux kali 6.0.0-kali5-arm64 #1 SMP Debian 6.0.10-2kali1 (2022-12-06) aarch64
 GNU/Linux

(base) ┌──(sanjit㉿kali)-[~]
└─$ uname -m
aarch64
```

2. DISPLAY DISK SPACE USAGE :



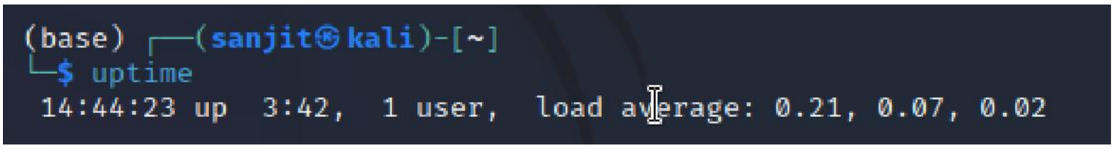
```
(base) ┌──(sanjit㉿kali)-[~]
└─$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            673M     0  673M   0% /dev
tmpfs           148M  1.3M  147M   1% /run
/dev/vda2        32G   18G   13G  57% /
tmpfs           737M     0  737M   0% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
/dev/vda1       512M  160K  512M   1% /boot/efi
tmpfs           148M   80K  148M   1% /run/user/1000
tmpfs           148M   68K  148M   1% /run/user/129
```

3. DISPLAY MEMORY USAGE :



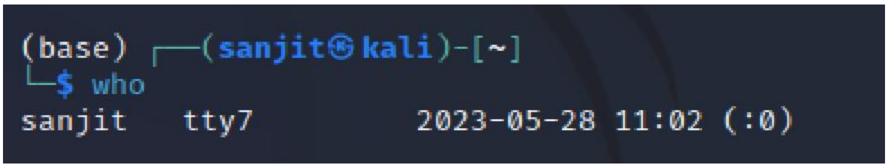
```
(base) ┌──(sanjit㉿kali)-[~]
└─$ free -m
               total        used        free      shared  buff/cache   availa
ble
Mem:            1472         581         153          18         737
784
Swap:            975           5         970
```

4. SHOW SYSTEM UPTIME:



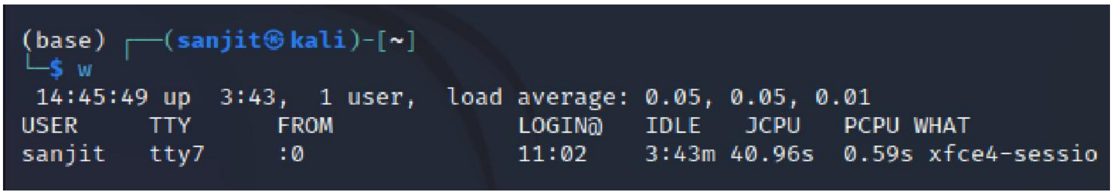
```
(base) ┌──(sanjit㉿kali)-[~]
└─$ uptime
 14:44:23 up  3:42,  1 user,  load average: 0.21, 0.07, 0.02
```

5. DISPLAY LOGGED IN USERS :



```
(base) ┌──(sanjit㉿kali)-[~]
└─$ who
sanjit   tty7         2023-05-28 11:02 (:0)
```

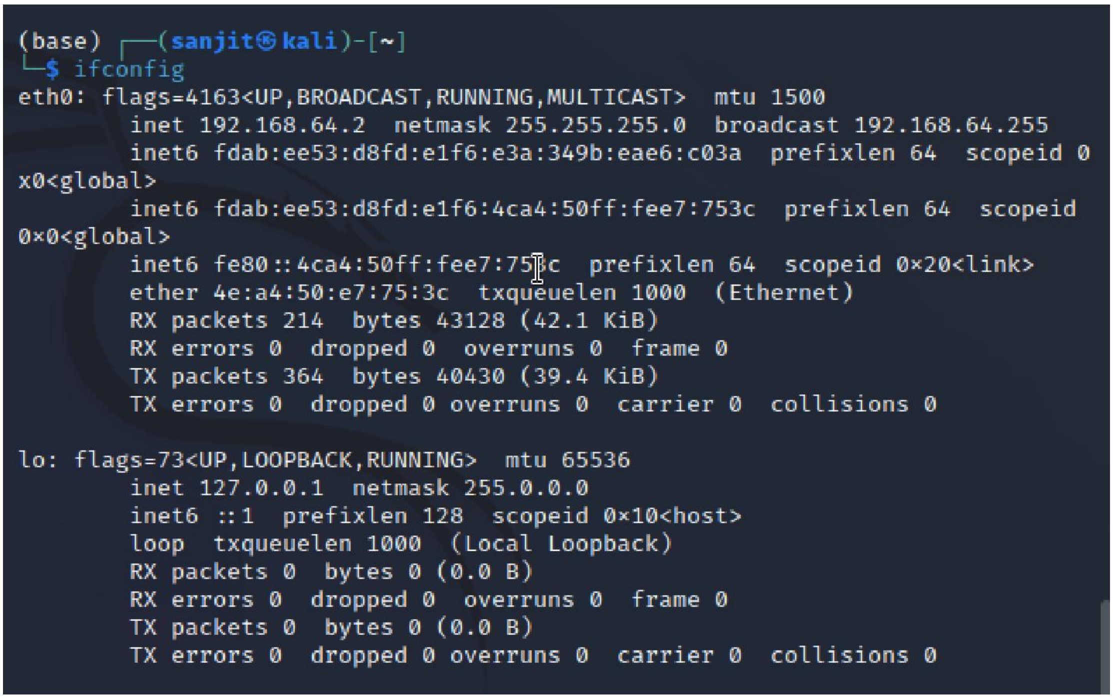
6. DISPLAY LOGGED IN USERS AND THEIR ACTIVITIES :



```
(base) ┌──(sanjit㉿kali)-[~]
└─$ w
 14:45:49 up  3:43,  1 user,  load average: 0.05, 0.05, 0.01
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
sanjit   tty7     :0               11:02    3:43m 40.96s  0.59s xfce4-sessio
```

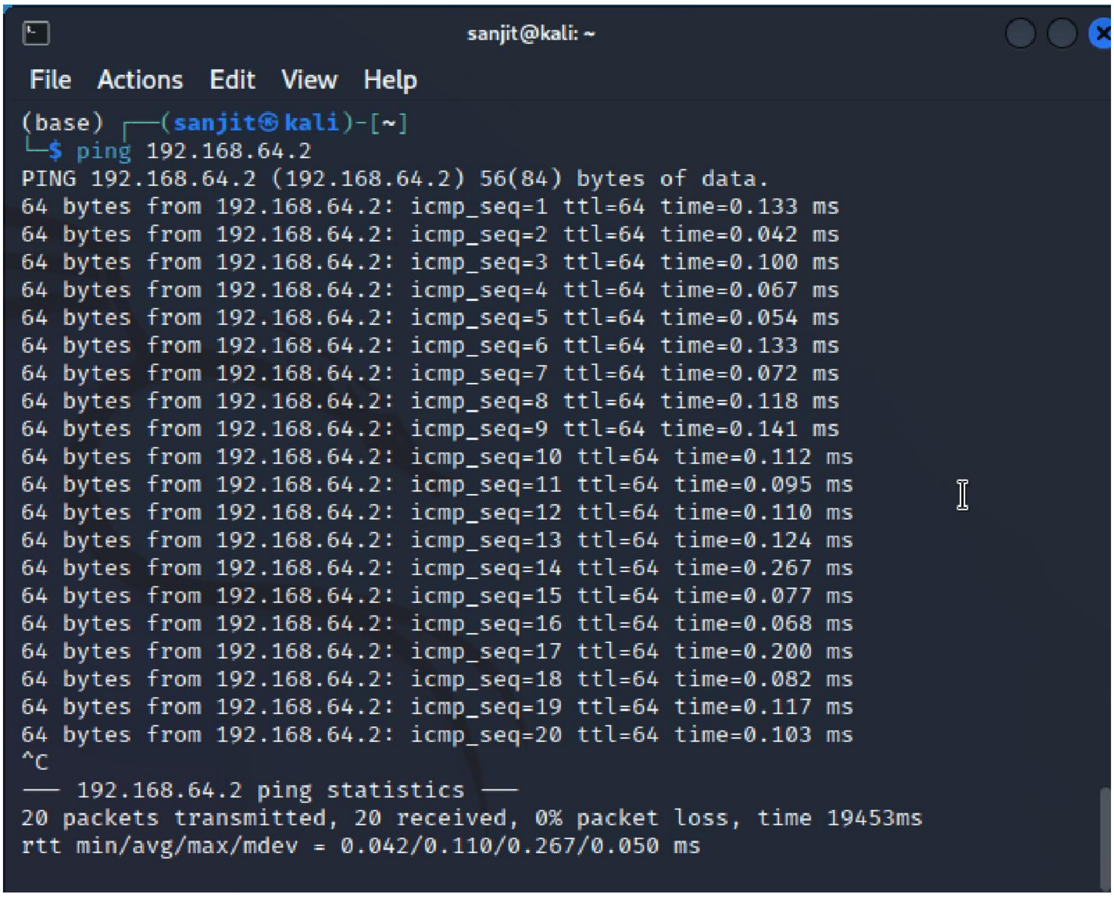
NETWORKING :

1. CONFIGURE NETWORK INTERFACES :



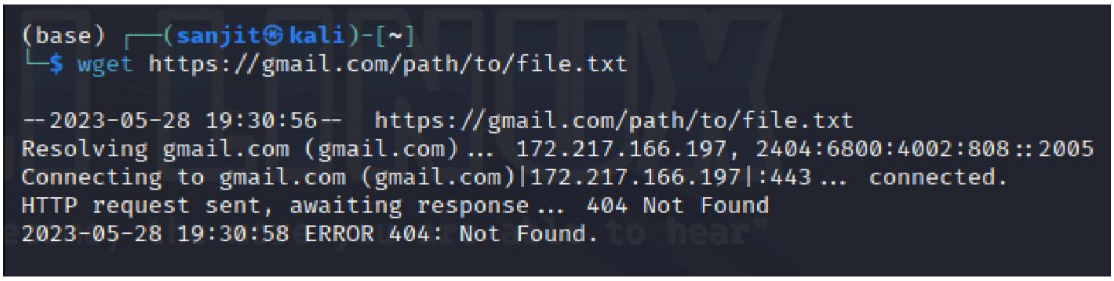
```
(base) ┌──(sanjit㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.64.2  netmask 255.255.255.0  broadcast 192.168.64.255
        inet6 fdab:ee53:d8fd:e1f6:e3a:349b:eae6:c03a  prefixlen 64  scopeid 0
x0<global>
        inet6 fdab:ee53:d8fd:e1f6:4ca4:50ff:fee7:753c  prefixlen 64  scopeid
0×0<global>
        inet6 fe80::4ca4:50ff:fee7:753c  prefixlen 64  scopeid 0×20<link>
        ether 4e:a4:50:e7:75:3c  txqueuelen 1000  (Ethernet)
        RX packets 214  bytes 43128 (42.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 364  bytes 40430 (39.4 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 0×10<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
```

2. SEND ICMP REQUEST TO A NETWORK HOST :



```
(base) ┌──(sanjit㉿kali)-[~]
└─$ ping 192.168.64.2
PING 192.168.64.2 (192.168.64.2) 56(84) bytes of data.
64 bytes from 192.168.64.2: icmp_seq=1 ttl=64 time=0.133 ms
64 bytes from 192.168.64.2: icmp_seq=2 ttl=64 time=0.042 ms
64 bytes from 192.168.64.2: icmp_seq=3 ttl=64 time=0.100 ms
64 bytes from 192.168.64.2: icmp_seq=4 ttl=64 time=0.067 ms
64 bytes from 192.168.64.2: icmp_seq=5 ttl=64 time=0.054 ms
64 bytes from 192.168.64.2: icmp_seq=6 ttl=64 time=0.133 ms
64 bytes from 192.168.64.2: icmp_seq=7 ttl=64 time=0.072 ms
64 bytes from 192.168.64.2: icmp_seq=8 ttl=64 time=0.118 ms
64 bytes from 192.168.64.2: icmp_seq=9 ttl=64 time=0.141 ms
64 bytes from 192.168.64.2: icmp_seq=10 ttl=64 time=0.112 ms
64 bytes from 192.168.64.2: icmp_seq=11 ttl=64 time=0.095 ms
64 bytes from 192.168.64.2: icmp_seq=12 ttl=64 time=0.110 ms
64 bytes from 192.168.64.2: icmp_seq=13 ttl=64 time=0.124 ms
64 bytes from 192.168.64.2: icmp_seq=14 ttl=64 time=0.267 ms
64 bytes from 192.168.64.2: icmp_seq=15 ttl=64 time=0.077 ms
64 bytes from 192.168.64.2: icmp_seq=16 ttl=64 time=0.068 ms
64 bytes from 192.168.64.2: icmp_seq=17 ttl=64 time=0.200 ms
64 bytes from 192.168.64.2: icmp_seq=18 ttl=64 time=0.082 ms
64 bytes from 192.168.64.2: icmp_seq=19 ttl=64 time=0.117 ms
64 bytes from 192.168.64.2: icmp_seq=20 ttl=64 time=0.103 ms
^C
── 192.168.64.2 ping statistics ──
20 packets transmitted, 20 received, 0% packet loss, time 19453ms
rtt min/avg/max/mdev = 0.042/0.110/0.267/0.050 ms
```

3. DOWNLOAD FILES FROM THE WEB:

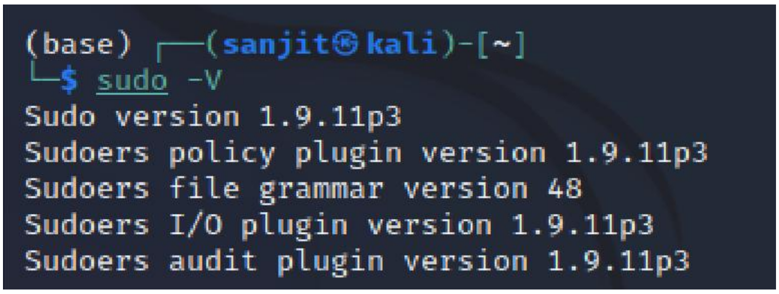


```
(base) ┌──(sanjit㉿kali)-[~]
└─$ wget https://gmail.com/path/to/file.txt

--2023-05-28 19:30:56--  https://gmail.com/path/to/file.txt
Resolving gmail.com (gmail.com)... 172.217.166.197, 2404:6800:4002:808::2005
Connecting to gmail.com (gmail.com)|172.217.166.197|:443... connected.
HTTP request sent, awaiting response... 404 Not Found
2023-05-28 19:30:58 ERROR 404: Not Found.
```

you can use real-world websites to download data from the website.

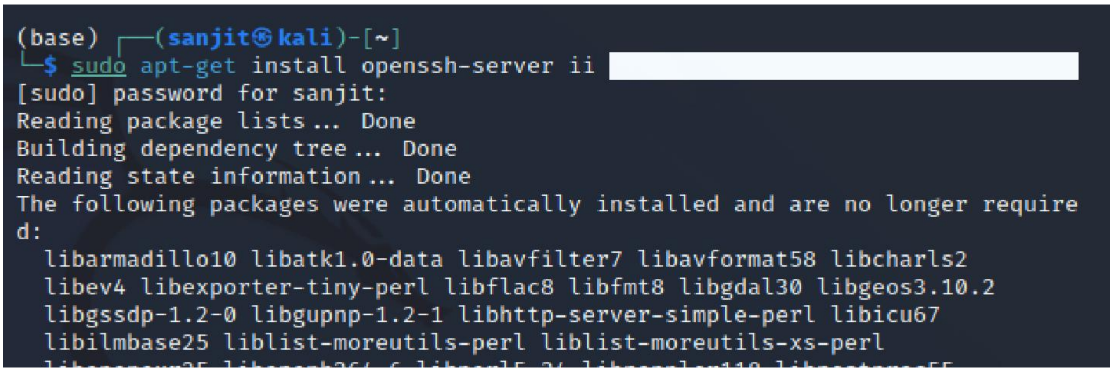
SYSTEM ADMINISTRATION :

1. EXECUTE COMMANDS WITH SUPERUSER PRIVILIGES :



```
(base) ┌──(sanjit㉿kali)-[~]
└─$ sudo -V
Sudo version 1.9.11p3
Sudoers policy plugin version 1.9.11p3
Sudoers file grammar version 48
Sudoers I/O plugin version 1.9.11p3
Sudoers audit plugin version 1.9.11p3
```

2. PACKAGE MANAGEMENT FOR DEBIAN-BASED DISTRIBUTIONS :



```
(base) ┌──(sanjit㉿kali)-[~]
└─$ sudo apt-get install openssh-server ii
[sudo] password for sanjit:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following packages were automatically installed and are no longer require
d:
  libarmadillo10 libatk1.0-data libavfilter7 libavformat58 libcharls2
  libev4 libexporter-tiny-perl libflac8 libfmt8 libgdal30 libgeos3.10.2
  libgssdp-1.2-0 libgupnp-1.2-1 libhttp-server-simple-perl libicu67
  libilmbase25 liblist-moreutils-perl liblist-moreutils-xs-perl
```

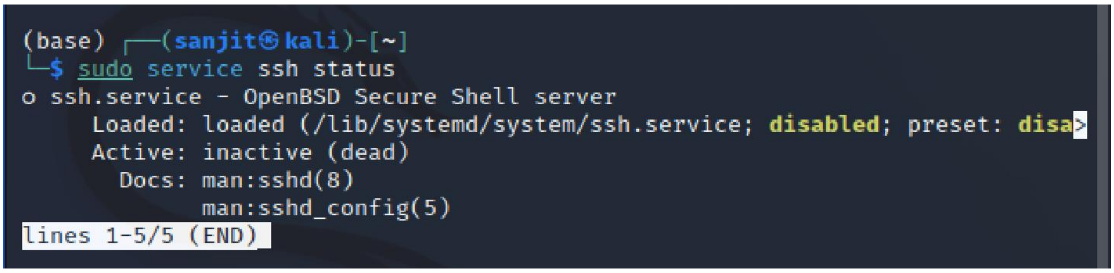
3. PACKAGE MANAGEMENT FOR RED HAT-BASED DISTRIBUTIONS:

COMMAND :
yum command_name

EXAMPLE : to print the repository list
yum repolist

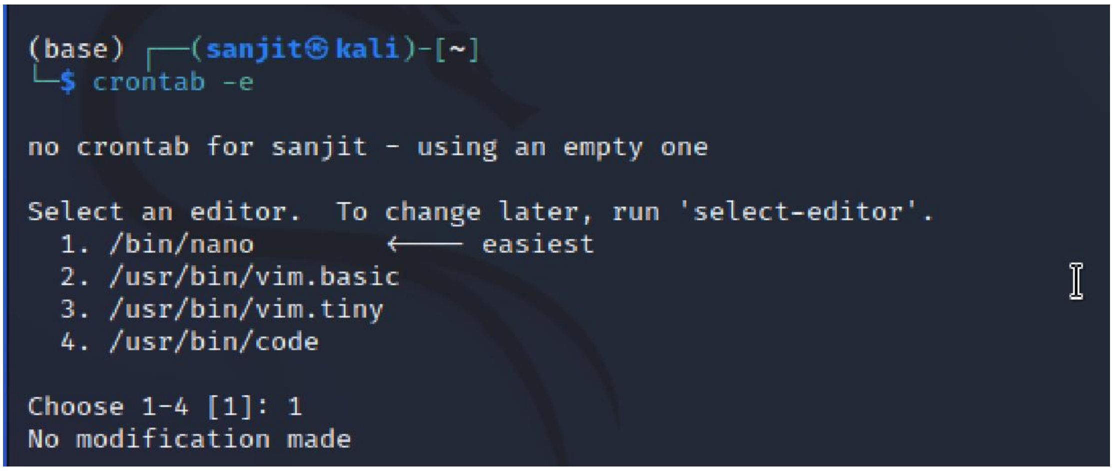
Note: yum is outdated and not supported in current versions of kali-linux.

4. MANAGE SYSTEM SERVICES:



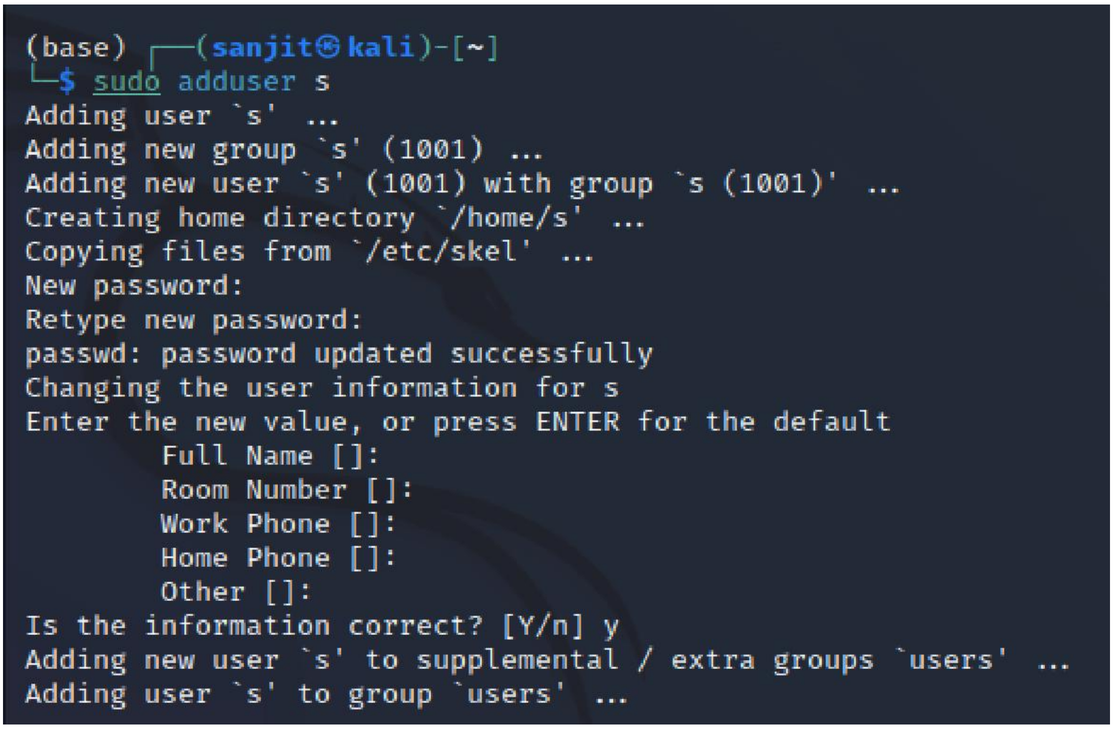
```
(base) ┌──(sanjit㉿kali)-[~]
└─$ sudo service ssh status
o ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; disabled; preset: disa>
     Active: inactive (dead)
       Docs: man:sshd(8)
             man:sshd_config(5)
lines 1-5/5 (END)
```

5. SCHEDULE RECURRING TASKS:



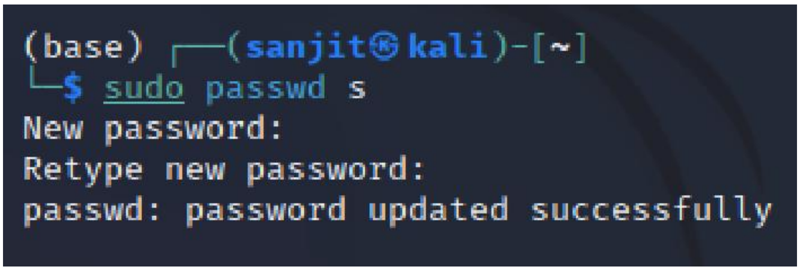
```
(base) ┌──(sanjit㉿kali)-[~]
└─$ crontab -e

no crontab for sanjit - using an empty one

Select an editor.  To change later, run 'select-editor'.
  1. /bin/nano        ←—— easiest
  2. /usr/bin/vim.basic
  3. /usr/bin/vim.tiny
  4. /usr/bin/code

Choose 1-4 [1]: 1
No modification made
```

6. ADD NEW USER :



```
(base) ┌──(sanjit㉿kali)-[~]
└─$ sudo adduser s
Adding user `s' ...
Adding new group `s' (1001) ...
Adding new user `s' (1001) with group `s (1001)' ...
Creating home directory `/home/s' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for s
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
Adding new user `s' to supplemental / extra groups `users' ...
Adding user `s' to group `users' ...
```

7. CHANGE PASSWORD FOR AN USER :



```
(base) ┌──(sanjit㉿kali)-[~]
└─$ sudo passwd s
New password:
Retype new password:
passwd: password updated successfully
```