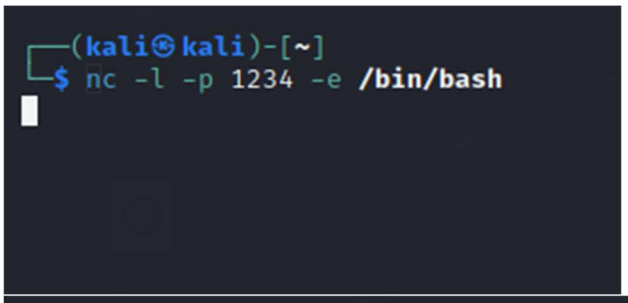
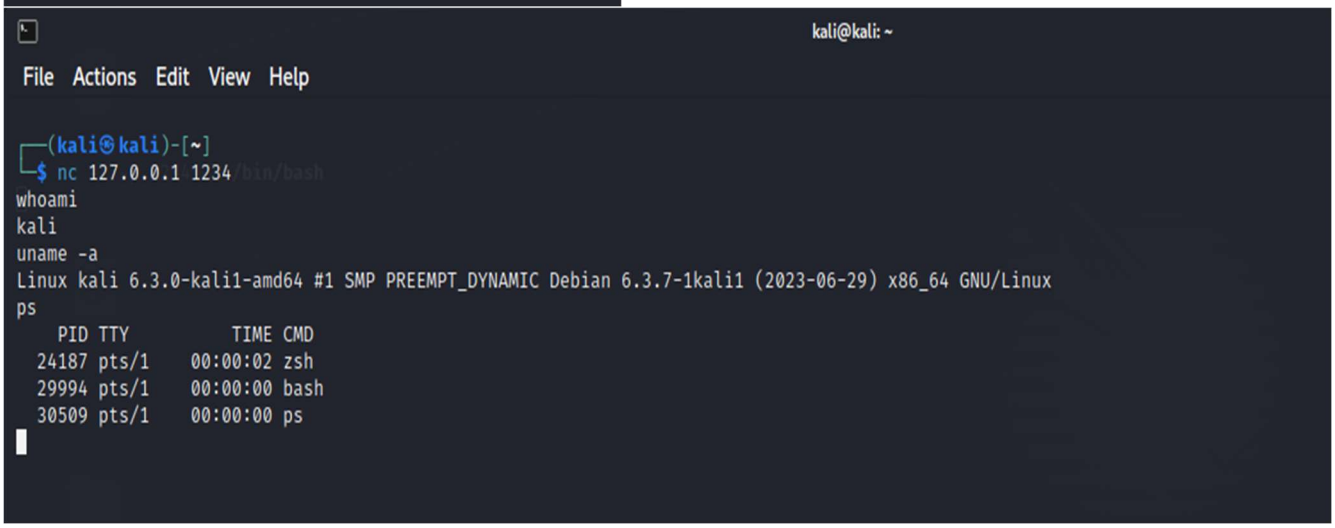
Facciamo un esercizio di "discovering" nel sistema operativo Linux, usando i comandi visti fino ad ora.

L'obiettivo è ottenere informazioni sensibili e identificare i processi in esecuzione esplorando il sistema operativo.

Proseguiamo per step al fine di estrapolare le seguenti informazioni:

1. Informazioni di sistema
2. Esplorazione del file system
3. Processi in esecuzione
4. Risorse di rete
5.Utenti e autorizzazioni





1-3

2

```
ls
area.py
client_server_2.py
client_server.py
Desktop
Documents
dos
Downloads
gameshell
gameshell.1
gameshell.2
gameshell-save.sh
gameshell.sh
gameshell.sh.1
gameshell.sh.2
gameshell.sh.3
gameshell.sh-save.2
gioco
gioco.c
Music
nano.120583.save
nano.2378.save
nano.3839.save
Pictures
pippo
pluto
Public
studenti
Templates
tmp
Videos
windows
```

```
dir
area.py              gameshell.1          gioco             pluto
client_server_2.py   gameshell.2          gioco.c           Public
client_server.py     gameshell-save.sh    Music             studenti
Desktop              gameshell.sh         nano.120583.save  Templates
Documents            gameshell.sh.1       nano.2378.save    tmp
dos                  gameshell.sh.2       nano.3839.save    Videos
Downloads            gameshell.sh.3       Pictures          windows
gameshell            gameshell.sh-save.2  pippo
```

```
cd tmp
ls
risultati.doc
```

4

```
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.86.109  netmask 255.255.255.0  broadcast 192.168.86.255
        inet6 fe80::a00:27ff:fecb:7ef5  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:cb:7e:f5  txqueuelen 1000  (Ethernet)
        RX packets 270  bytes 17968 (17.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 245  bytes 62976 (61.5 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 64  bytes 4847 (4.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 64  bytes 4847 (4.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
id
uid=1000(kali) gid=1000(kali) groups=1000(kali),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),100(users),106(netdev),111(bluetooth),117(scanner),140(wireshark),142(kaboxer),143(vboxsf)
```


5

```
ls -l
total 1152
-rw-r--r--  1 kali kali   1211 Dec  1 13:29 area.py
-rw-r--r--  1 kali kali    481 Dec  9 13:10 client_server_2.py
-rw-r--r--  1 kali kali    548 Dec 13 08:50 client_server.py
drwxr-xr-x  2 kali kali   4096 Oct 27 16:13 Desktop
drwxr-xr-x  2 kali kali   4096 Oct 27 16:13 Documents
drwxr-xr-x  2 kali kali   4096 Nov 21 18:47 dos
drwxr-xr-x  2 kali kali   4096 Oct 27 16:13 Downloads
d--x--x--x 13 kali kali   4096 Dec 16 11:11 gameshell
d--x--x--x 13 kali kali   4096 Dec 16 14:28 gameshell.1
drwxr-xr-x 13 kali kali   4096 Dec 17 09:29 gameshell.2
-rwxr-xr-x  1 kali kali 231215 Dec 18 09:20 gameshell-save.sh
-rw-r--r--  1 kali kali 203144 Nov 30 20:02 gameshell.sh
-rw-r--r--  1 kali kali 203144 Nov 30 20:02 gameshell.sh.1
-rw-r--r--  1 kali kali 203144 Nov 30 20:02 gameshell.sh.2
d--x--x--x 13 kali kali   4096 Dec 16 11:26 gameshell.sh.3
-rwxr-xr-x  1 kali kali 219228 Dec 16 11:30 gameshell.sh-save.2
-rwxr-xr-x  1 kali kali  16064 Nov 28 20:41 gioco
-rw-r--r--  1 kali kali   1734 Nov 28 20:40 gioco.c
drwxr-xr-x  2 kali kali   4096 Oct 27 16:13 Music
-rw-------  1 kali kali      1 Dec  9 13:13 nano.120583.save
-rw-------  1 root root      1 Oct 27 20:13 nano.2378.save
-rw-------  1 root root     81 Oct 27 20:09 nano.3839.save
drwxr-xr-x  2 kali kali   4096 Oct 27 16:13 Pictures
-rw-r--r--  1 kali kali      0 Nov 21 21:06 pippo
-rw-r--r--  1 kali kali      0 Nov 21 20:43 pluto
drwxr-xr-x  2 kali kali   4096 Oct 27 16:13 Public
drwxr-xr-x  5 kali kali   4096 Nov 21 18:48 studenti
drwxr-xr-x  2 kali kali   4096 Oct 27 16:13 Templates
drwxr-xr-x  2 kali kali   4096 Nov 21 18:50 tmp
drwxr-xr-x  2 kali kali   4096 Oct 27 16:13 Videos
drwxr-xr-x  2 kali kali   4096 Nov 21 18:47 windows
```

```
ls -all
total 1352
drwx------ 25 kali kali   4096 Dec 19 19:52 .
drwxr-xr-x  3 root root   4096 Aug 21 20:59 ..
-rw-r--r--  1 kali kali   1211 Dec  1 13:29 area.py
-rw-r--r--  1 kali kali    220 Aug 21 20:59 .bash_logout
-rw-r--r--  1 kali kali   5551 Aug 21 20:59 .bashrc
-rw-r--r--  1 kali kali   3526 Aug 21 20:59 .bashrc.original
drwx------  7 kali kali   4096 Dec 14 08:25 .BurpSuite
drwxr-xr-x 11 kali kali   4096 Nov 21 20:59 .cache
-rw-r--r--  1 kali kali    481 Dec  9 13:10 client_server_2.py
-rw-r--r--  1 kali kali    548 Dec 13 08:50 client_server.py
drwxr-xr-x 16 kali kali   4096 Dec 12 20:54 .config
drwxr-xr-x  2 kali kali   4096 Oct 27 16:13 Desktop
-rw-r--r--  1 kali kali     35 Oct 27 16:13 .dmrc
drwxr-xr-x  2 kali kali   4096 Oct 27 16:13 Documents
drwxr-xr-x  2 kali kali   4096 Nov 21 18:47 dos
drwxr-xr-x  2 kali kali   4096 Oct 27 16:13 Downloads
-rw-r--r--  1 kali kali  11759 Aug 21 20:59 .face
lrwxrwxrwx  1 kali kali      5 Aug 21 20:59 .face.icon → .face
d--x--x--x 13 kali kali   4096 Dec 16 11:11 gameshell
d--x--x--x 13 kali kali   4096 Dec 16 14:28 gameshell.1
drwxr-xr-x 13 kali kali   4096 Dec 17 09:29 gameshell.2
-rwxr-xr-x  1 kali kali 231215 Dec 18 09:20 gameshell-save.sh
-rw-r--r--  1 kali kali 203144 Nov 30 20:02 gameshell.sh
-rw-r--r--  1 kali kali 203144 Nov 30 20:02 gameshell.sh.1
-rw-r--r--  1 kali kali 203144 Nov 30 20:02 gameshell.sh.2
d--x--x--x 13 kali kali   4096 Dec 16 11:26 gameshell.sh.3
-rwxr-xr-x  1 kali kali 219228 Dec 16 11:30 gameshell.sh-save.2
-rwxr-xr-x  1 kali kali  16064 Nov 28 20:41 gioco
-rw-r--r--  1 kali kali   1734 Nov 28 20:40 gioco.c
drwx------  3 kali kali   4096 Oct 27 16:13 .gnupg
```

```
groups
kali adm dialout cdrom floppy sudo audio dip video plugdev users netdev bluetooth scanner wireshark kaboxer vboxsf
```