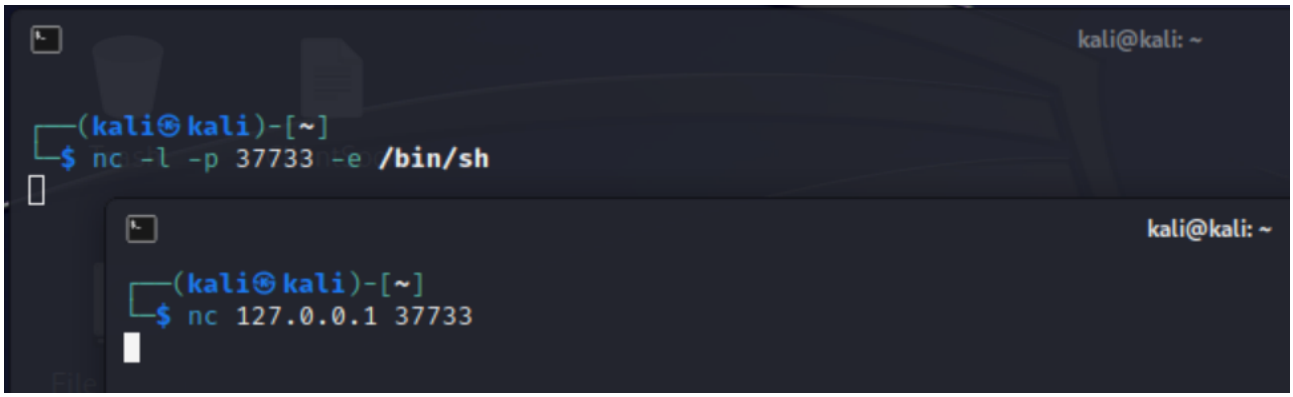
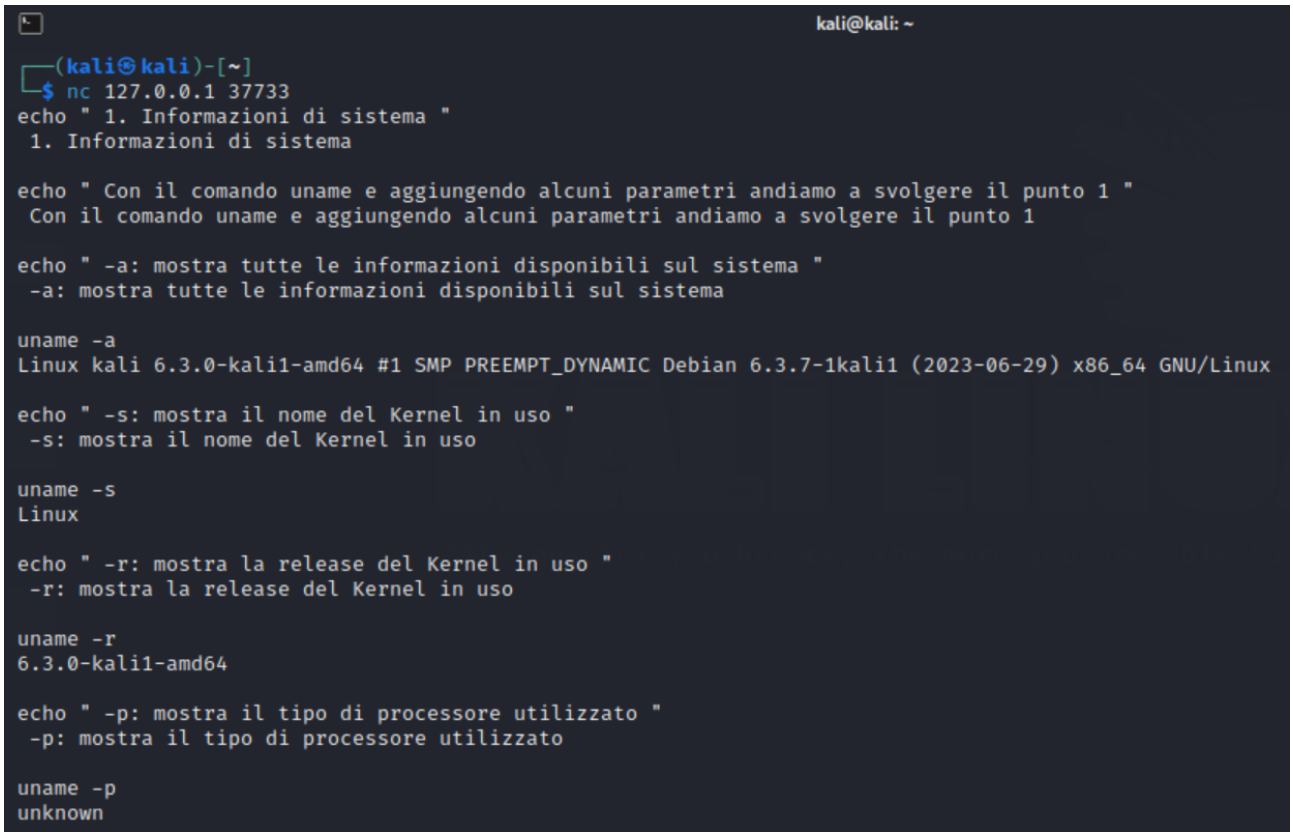
Sulla Macchina Kali Linux lanciamo il comando netcat con le opzioni -l per il listening e meno p per la porta poi -e per far eseguire qualcosa (in questo caso una shell da mettere a disposizione dell'attaccante)



1 . Informazioni di sistema



```
echo " -i: mostra informazioni sulla piattaforma hardware "
 -i: mostra informazioni sulla piattaforma hardware

uname -i
unknown

echo " -o: mostra il sistema operativo in uso "
 -o: mostra il sistema operativo in uso

uname -o
GNU/Linux

echo " -n: mostra l'hostaname del computer sulla rete "
 -n: mostra l'hostaname del computer sulla rete

uname -n
kali

echo " -m: mostra il nome dell'hardware utilizzato dalla macchina "
 -m: mostra il nome dell'hardware utilizzato dalla macchina

uname -m
x86_64
```

2 . Esplorazione del file system

```
pwd
/home/kali
cd ../..
pwd
/
tree
```

```
49076 directories, 514394 files
```

3 . Processi in esecuzione

```
echo " 3. Processi in esecuzione "
 3. Processi in esecuzione

echo " Con il comando ps andiamo a vedere i processi in esecuzione "
 Con il comando ps andiamo a vedere i processi in esecuzione

ps -f
UID          PID    PPID  C STIME TTY          TIME CMD
kali        1859    1856  0 14:12 pts/0    00:00:00 /usr/bin/zsh
kali        9364    1859  0 14:27 pts/0    00:00:00 sh
kali       23048    9364  0 14:56 pts/0    00:00:00 ps -f
```

4 . Risorse di rete

```
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.148  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fecb:7ef5  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:cb:7e:f5  txqueuelen 1000  (Ethernet)
        RX packets 7705  bytes 900554 (879.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 94  bytes 22584 (22.0 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 4352  bytes 40791165 (38.9 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4352  bytes 40791165 (38.9 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

5 . Utenti e Autorizzazioni

```
┌──(kali㉿kali)-[~]
└─$ nc 127.0.0.1 37733
groups
kali adm dialout cdrom floppy sudo audio dip video plugdev users netdev bluetooth scanner wireshark kaboxer vboxsf
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)
id -Gn
kali adm dialout cdrom floppy sudo audio dip video plugdev users netdev bluetooth scanner wireshark kaboxer vboxsf
cat /etc/passwd
```

```
cat /etc/passwd | ls -l
total 488
drwxr-xr-x  2 kali kali   4096 Dec  9 04:41 Desktop
drwxr-xr-x  2 kali kali   4096 Nov 11 15:11 Documents
drwxr-xr-x  2 kali kali   4096 Nov 11 15:11 Downloads
d--x--x--x 13 kali kali   4096 Dec 16 04:59 gameshell
d--x--x--x 13 kali kali   4096 Dec 16 05:26 gameshell.1
d--x--x--x 13 kali kali   4096 Dec 16 09:02 gameshell.2
-rwxr-xr-x  1 kali kali 246320 Dec 17 20:32 gameshell-save.sh
-rw-r--r--  1 kali kali 203144 Nov 30 14:02 gameshell.sh
drwxr-xr-x  2 kali kali   4096 Nov 11 15:11 Music
drwxr-xr-x  2 kali kali   4096 Nov 11 15:11 Pictures
drwxr-xr-x  2 kali kali   4096 Nov 11 15:11 Public
drwxr-xr-x  2 kali kali   4096 Nov 11 15:11 Templates
drwxr-xr-x  2 kali kali   4096 Nov 11 15:11 Videos
```

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
man:x:6:12:man:/var/cache/man:/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
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/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:nobody:/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:100:107::/nonexistent:/usr/sbin/nologin
tss:x:101:109:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:x:102:65534::/var/lib/strongswan:/usr/sbin/nologin
tcpdump:x:103:110::/nonexistent:/usr/sbin/nologin
usbmux:x:104:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/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:108:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
pulse:x:109:114:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
lightdm:x:110:116:Light Display Manager:/var/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/chroot:/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
geoclue:x:118:126::/var/lib/geoclue:/usr/sbin/nologin
Debian-snmp:x:119:127::/var/lib/snmp:/bin/false
sslh:x:120:128::/nonexistent:/usr/sbin/nologin
ntpsec:x:121:131::/nonexistent:/usr/sbin/nologin
redsocks:x:122:132::/var/run/redsocks:/usr/sbin/nologin
rwhod:x:123:65534::/var/spool/rwho:/usr/sbin/nologin
_gophish:x:124:134::/var/lib/gophish:/usr/sbin/nologin
iodine:x:125:65534::/run/iodine:/usr/sbin/nologin
miredo:x:126:65534::/var/run/miredo:/usr/sbin/nologin
statd:x:127:65534::/var/lib/nfs:/usr/sbin/nologin
redis:x:128:135::/var/lib/redis:/usr/sbin/nologin
postgres:x:129:136:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mosquitto:x:130:138::/var/lib/mosquitto:/usr/sbin/nologin
inetsim:x:131:139::/var/lib/inetsim:/usr/sbin/nologin
_gvm:x:132:141::/var/lib/openvas:/usr/sbin/nologin
kali:x:1000:1000:,,,:/home/kali:/usr/bin/zsh