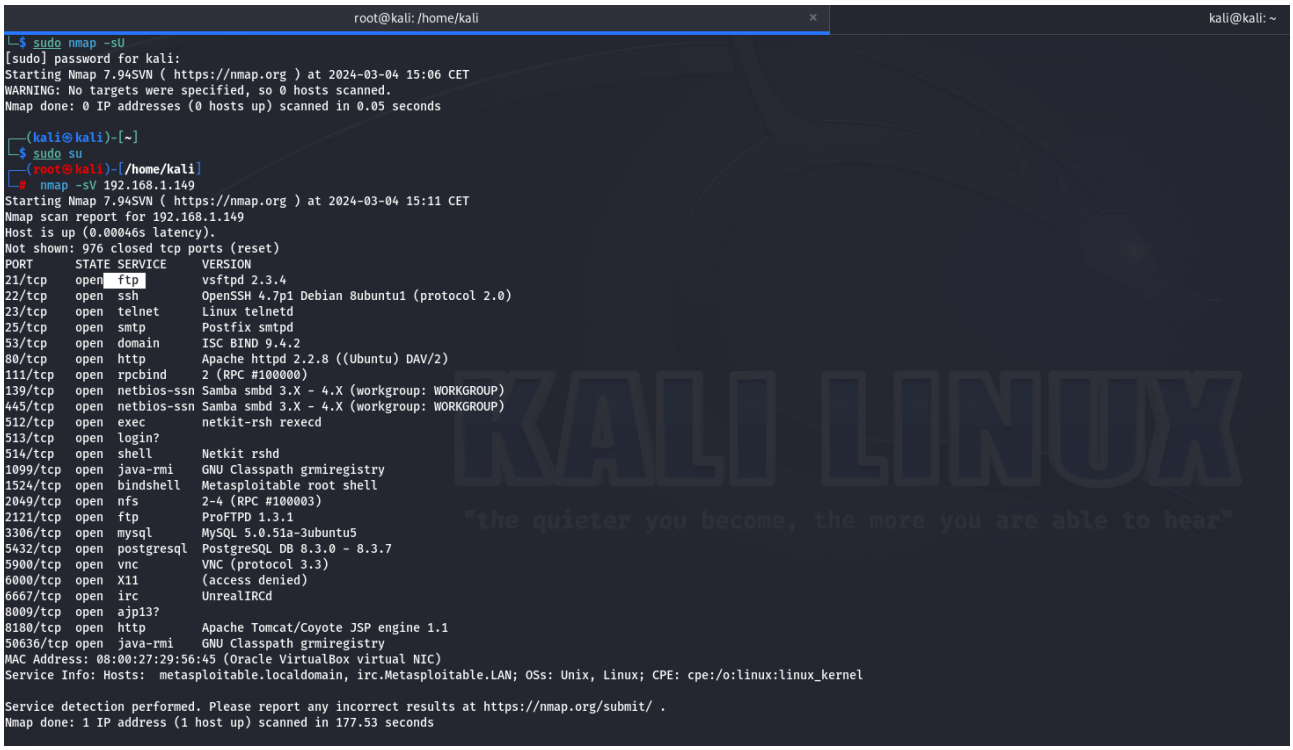
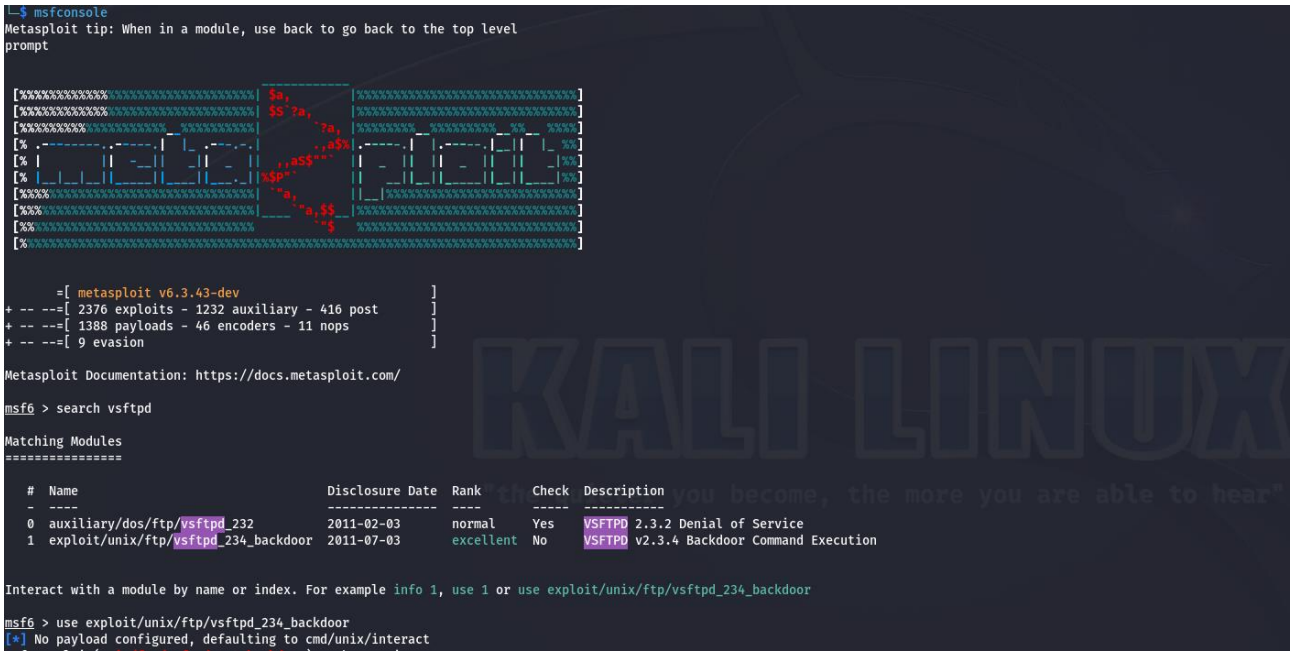
```
┌──(root㉿kali)-[/home/kali]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.150  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fe34:f4be  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:34:f4:be  txqueuelen 1000  (Ethernet)
        RX packets 1594  bytes 112889 (110.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1905  bytes 141485 (138.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 43  bytes 3152 (3.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 43  bytes 3152 (3.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Settare gli ip Kali linux con 192.168.1.150 e metasploitable con ip a 192.168.1.149.

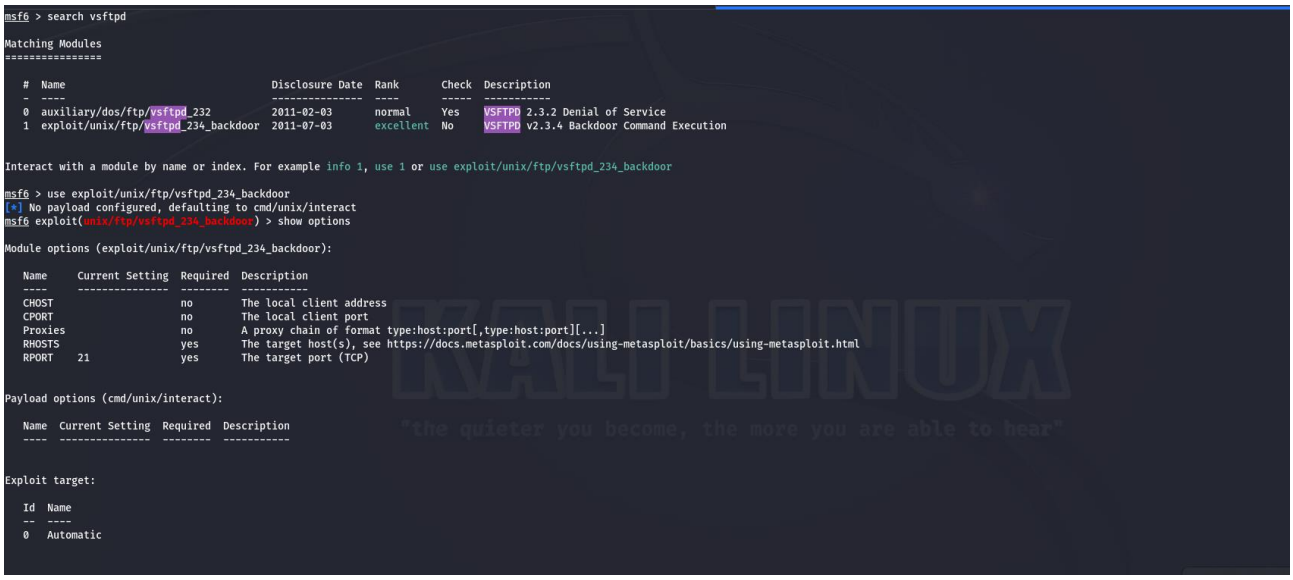
```
5 packets transmitted, 5 received, 0% packet loss, time 4031ms
rtt min/avg/max/mdev = 0.260/0.322/0.411/0.060 ms
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:29:56:45
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe29:5645/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1891 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1682 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:146675 (143.2 KB)  TX bytes:114516 (111.8 KB)
          Base address:0xd020 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:446 errors:0 dropped:0 overruns:0 frame:0
          TX packets:446 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:176269 (172.1 KB)  TX bytes:176269 (172.1 KB)

msfadmin@metasploitable:~$ _
```



Effettuare scansione delle porte di metasploitable con nmap eseguendo il comando sopra riportato.

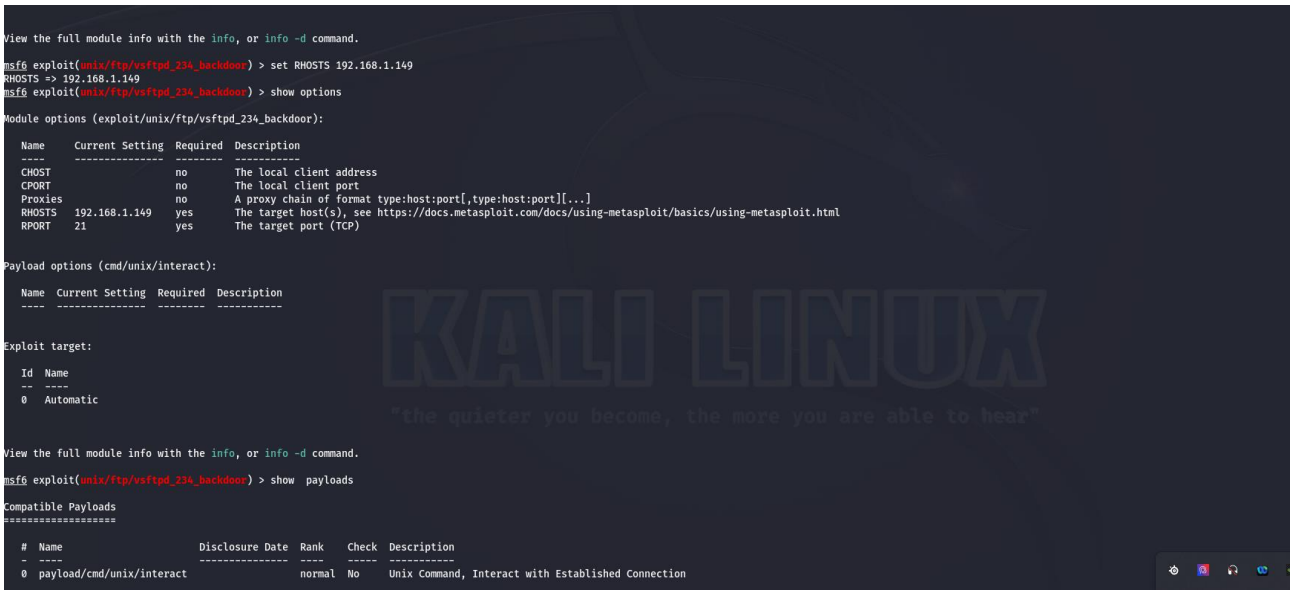


Eseguire il comando msfconsole e successivamente digitare search vsftp.

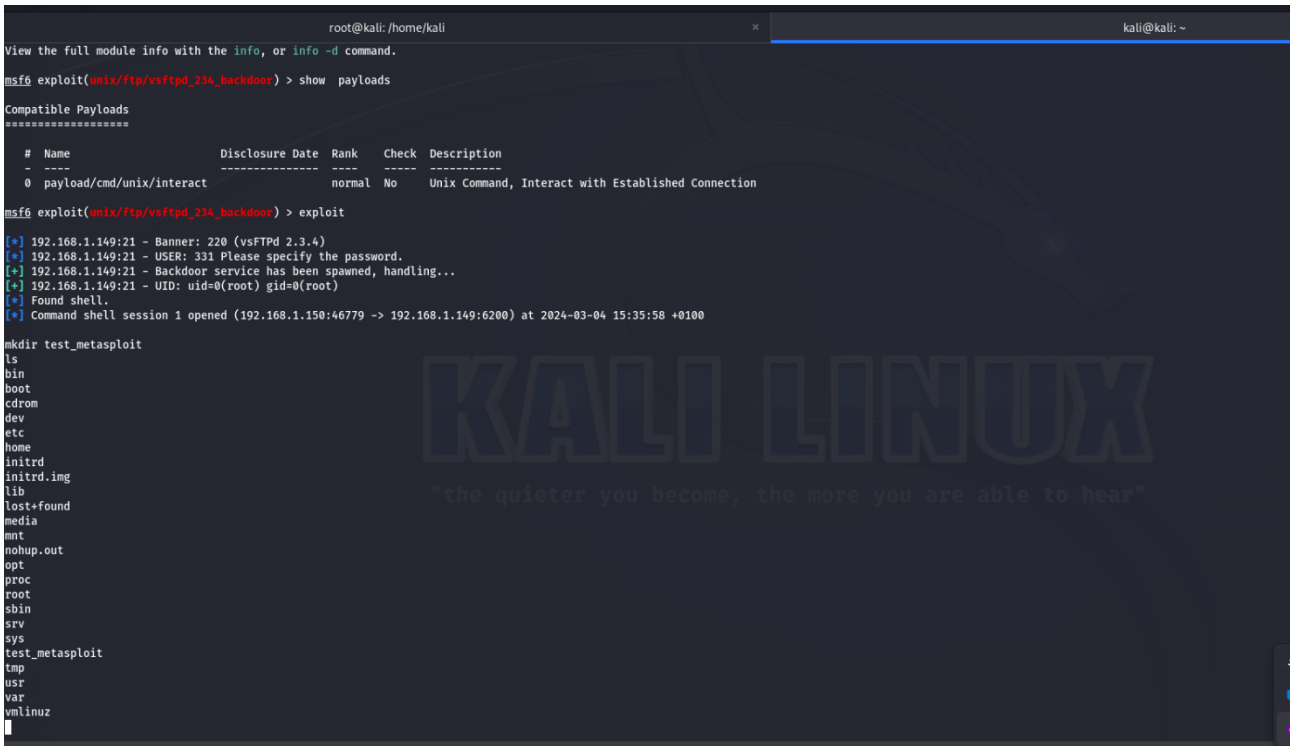


Scegliere exploit/unix/... mettendo il nome del modulo con davanti il comando use.

Digitare il comando set RHOSTS e l'ip di metasploitable.



Controllare che sia stato settato con il comando show options



Creo la directory in metasploit su metasploit