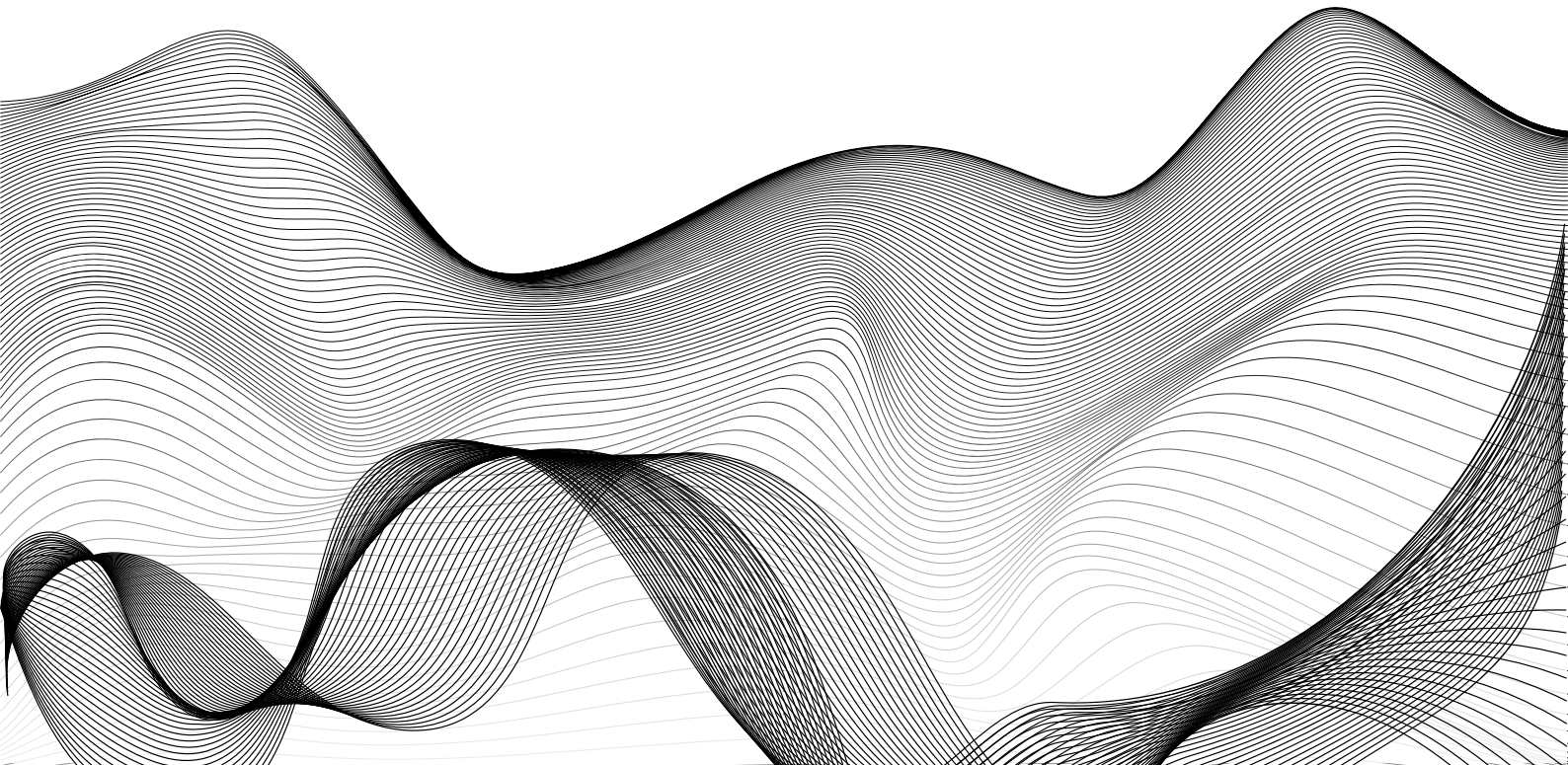
ELEONORA
VIOLA

DATASHIELDS

HACKING CON METASPLOIT

S7/L1



Per questo esercizio in primo luogo modifico l'indirizzo IP della Metasploitable e della Kali Linux,

```
iface eth1 inet static
address 192.168.1.149
netmask 255.255.255.0
network 192.168.1.149
broadcast 192.168.1.255
gateway 192.168.1.1
```

```
auto eth1
iface eth1 inet static
address 192.168.1.150/24
netmask 255.255.255.0
```

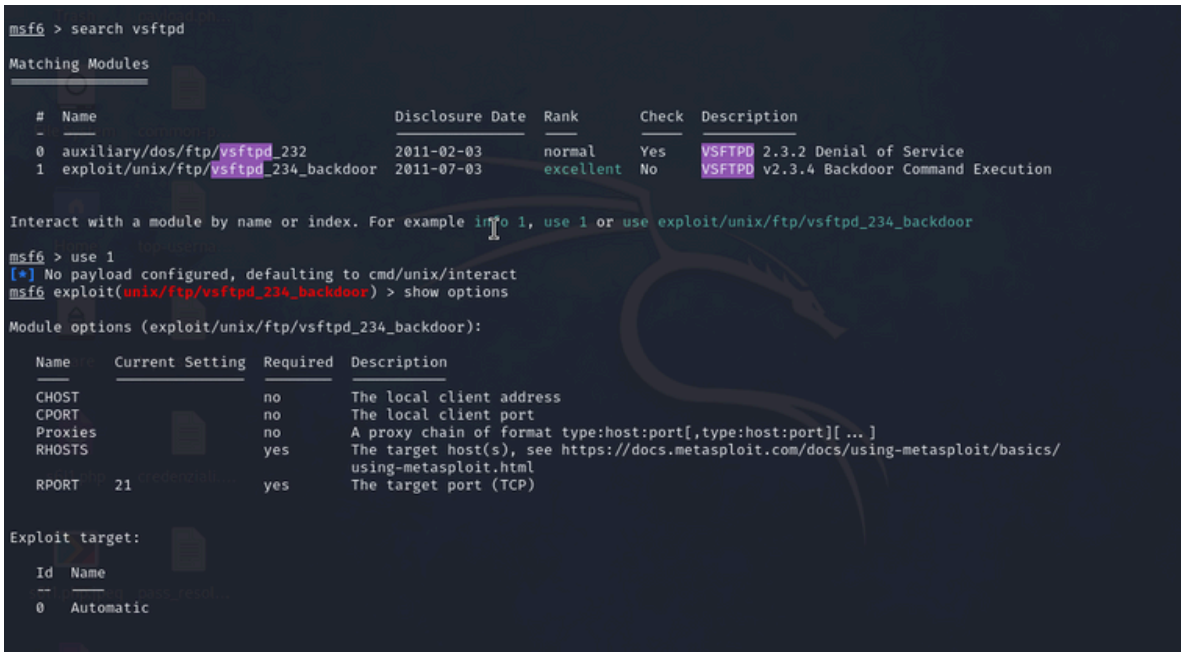
Procedo dunque con il ping per verificare che sia tutto connesso.

```
┌──(kali㉿kali)-[~]
└─$ ping -c4 meta
PING meta (192.168.1.149) 56(84) bytes of data.
64 bytes from meta (192.168.1.149): icmp_seq=1 ttl=64 time=0.573 ms
64 bytes from meta (192.168.1.149): icmp_seq=2 ttl=64 time=0.768 ms
64 bytes from meta (192.168.1.149): icmp_seq=3 ttl=64 time=1.54 ms
64 bytes from meta (192.168.1.149): icmp_seq=4 ttl=64 time=2.10 ms

── meta ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3058ms
rtt min/avg/max/mdev = 0.573/1.244/2.099/0.611 ms
```

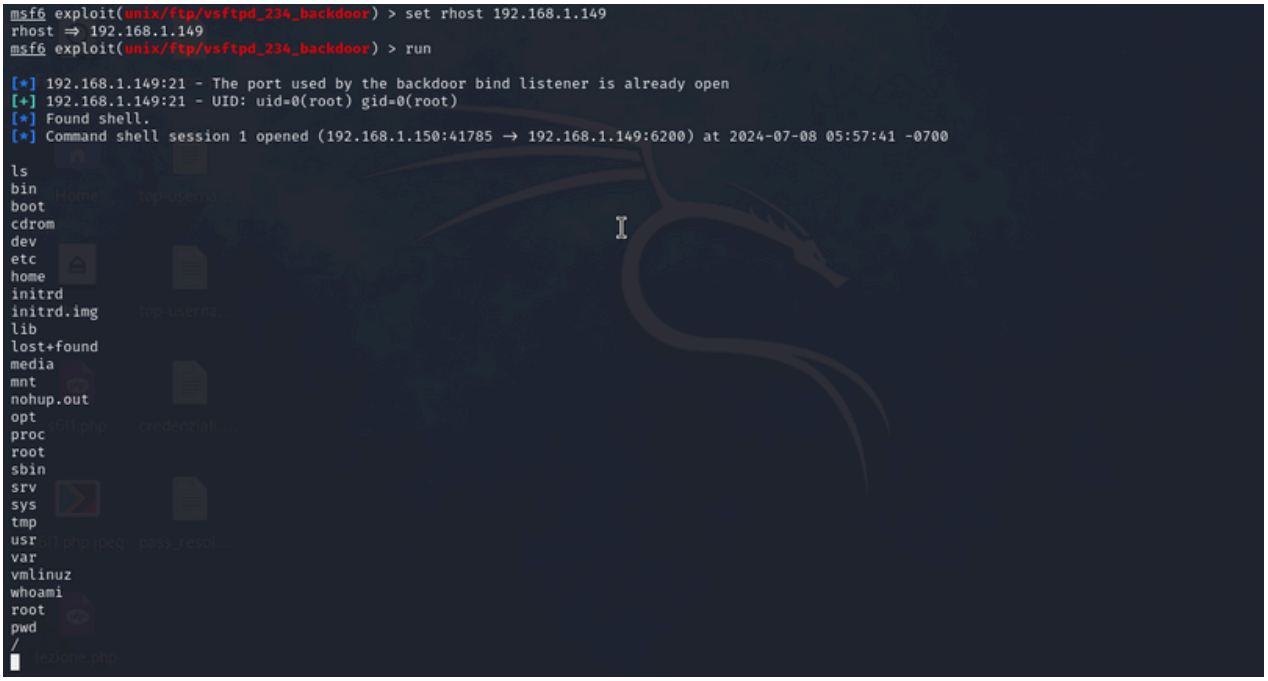
Successivamente accedo alla **msfconsole**

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Use the analyze command to suggest runnable modules for
hosts

                https://metasploit.com


       =[ metasploit v6.4.15-dev                          ]
+ -- --=[ 2433 exploits - 1251 auxiliary - 428 post       ]
+ -- --=[ 1471 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]
```

Cerco vsftpd, seleziono il modulo **unix/ftp/vsftpd_234_backdoor** e guardo le opzioni.



Uso il comando RHOST per mettere l'ip di meta e mando l'exploit con **run**.



In questo modo sono dentro metasploitable e posso creare la cartella **test_metasploit**