🏴‍☠️ Write-Up: Máquina "Vacaciones"

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

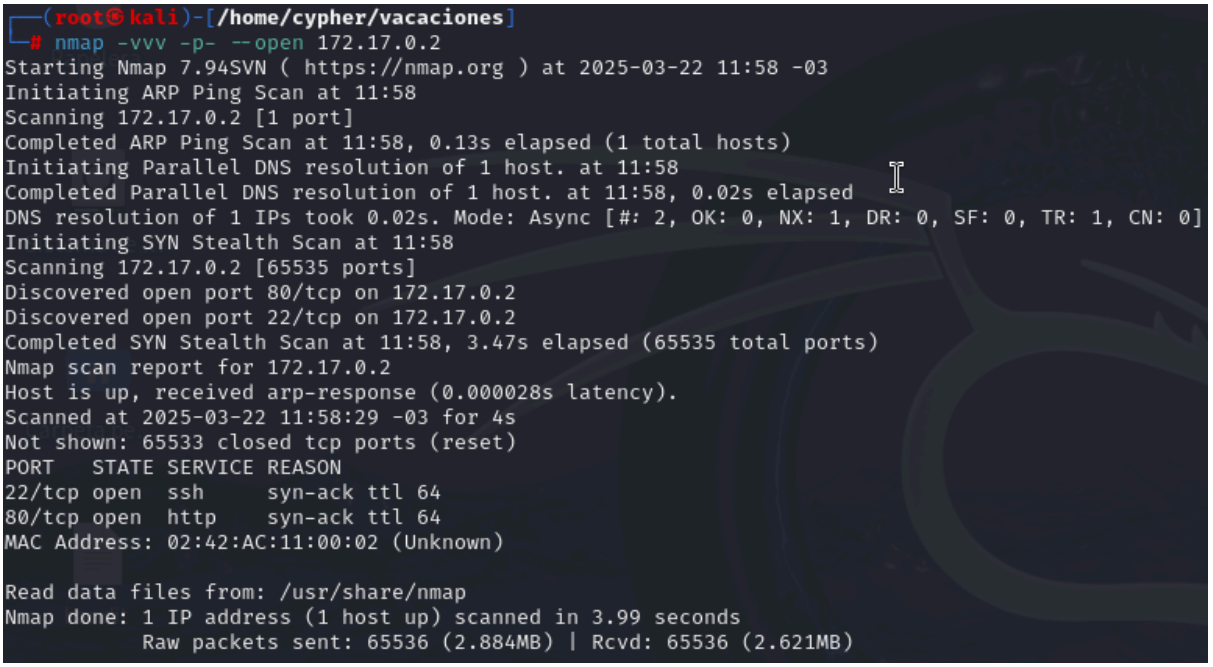
🔎 Metodología de Pentesting

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

Hago un escaneo general a la máquina objetivo, con la finalidad de saber que puertos tiene abiertos.



🎯 2. Escaneo y Enumeración

Ya sabiendo que puertos están abiertos, se hace un escaneo más profundo en esos puertos abiertos encontrados para saber servicios y versiones.

```
┌──(root㉿kali)-[/home/cypher/vacaciones]
└─# nmap -vvv -p 80,22 -sV -sC 172.17.0.2
```

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 41:16:eb:54:64:34:d1:69:ee:dc:d9:21:9c:72:a5:c1 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCzT6jdfo9QUX+9zCmyJQNTcAJXdhXByneCfqA9I7cXPBFGDGgxNAfQdoiqH3EMiTjf+maPlCNyVHGFl+sClQa5sJwdrbWZiJPxfxGkCtWiSrRdKKUKt/7rCMKMOy79
bFRvurgss+57tsglfXkE9FPkZGd3mLruXt5Lyb+8uhFWpW58Df6ZUoSsJi7n0bkXNpEzJAzYHNmRRtv0RsGDFosi/t5KUCMPX67jbM8jsApIVwFIQBTiwzwGQn33G2ZoAJy/NYZ9dkuN2cKM2uItovo25daA+0/SxEfHqA
HGquvoMKSj8pcX3qZVD7cGWlsn9c5QNzHRC2DZUSHrK7UIaG0r
|   256 f0:c4:2b:02:50:3a:49:a7:a2:34:b8:09:61:fd:2c:6d (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMD2Z/ZotorXbs6zP9Sg9XenjSX0HIjYjoEH2cAV7aDoQXZKrssz5AJ98j8b4ntOPGfVehrcRv9X7lKswOea9HM=
|   256 df:e9:46:31:9a:ef:0d:81:31:1f:77:e4:29:f5:c9:88 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIK/0ZadHoPSGKg31xFAhPaX854MMS09s5JgdzqmD3jCl
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
|_http-title: Site doesn't have a title (text/html).
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

También, se revisa la existencia de directorios interesantes. Pero, no se encontró nada comprometedor.

```
┌──(root㉿kali)-[/home/cypher/vacaciones]
└─# ffuf -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt:FUZZ -u http://172.17.0.2/FUZZ -recursion -recursion-depth 1

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://172.17.0.2/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirbuster/directory-list-lowercase-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
________________________________________________
```

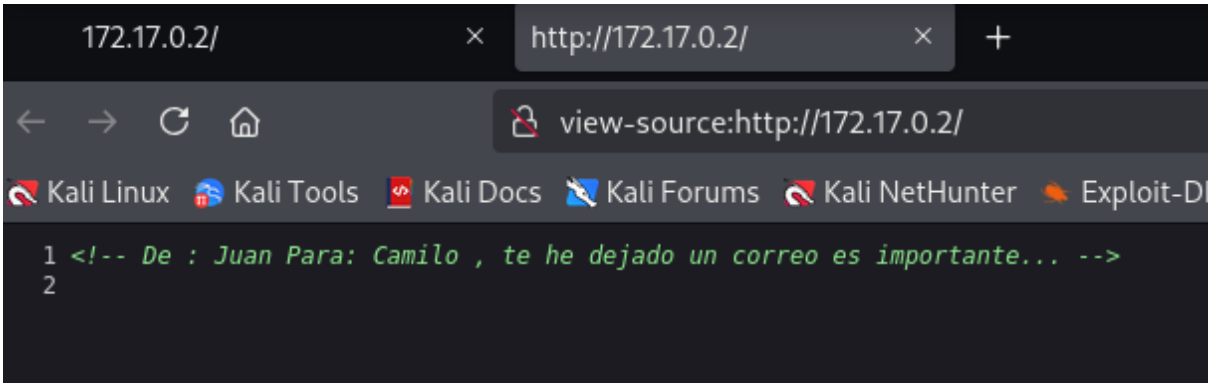
```
#                       [Status: 200, Size: 74, Words: 15, Lines: 2, Duration: 4ms]
# directory-list-lowercase-2.3-medium.txt [Status: 200, Size: 74, Words: 15, Lines: 2, Duration: 5ms]
# Copyright 2007 James Fisher [Status: 200, Size: 74, Words: 15, Lines: 2, Duration: 6ms]
#                       [Status: 200, Size: 74, Words: 15, Lines: 2, Duration: 2ms]
# Priority ordered case insensative list, where entries were found  [Status: 200, Size: 74, Words: 15, Lines: 2, Duration: 3ms]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 74, Words: 15, Lines: 2, Duration: 1ms]
# or send a letter to Creative Commons, 171 Second Street,  [Status: 200, Size: 74, Words: 15, Lines: 2, Duration: 3ms]
# Attribution-Share Alike 3.0 License. To view a copy of this  [Status: 200, Size: 74, Words: 15, Lines: 2, Duration: 6ms]
#                       [Status: 200, Size: 74, Words: 15, Lines: 2, Duration: 8ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/  [Status: 200, Size: 74, Words: 15, Lines: 2, Duration: 10ms]
# This work is licensed under the Creative Commons  [Status: 200, Size: 74, Words: 15, Lines: 2, Duration: 10ms]
# on atleast 2 different hosts [Status: 200, Size: 74, Words: 15, Lines: 2, Duration: 14ms]
#                       [Status: 200, Size: 74, Words: 15, Lines: 2, Duration: 11ms]
                        [Status: 200, Size: 74, Words: 15, Lines: 2, Duration: 16ms]
javascript              [Status: 301, Size: 313, Words: 20, Lines: 10, Duration: 5ms]
[INFO] Adding a new job to the queue: http://172.17.0.2/javascript/FUZZ

                        [Status: 200, Size: 74, Words: 15, Lines: 2, Duration: 4ms]
server-status           [Status: 403, Size: 275, Words: 20, Lines: 10, Duration: 8ms]
[INFO] Starting queued job on target: http://172.17.0.2/javascript/FUZZ

# directory-list-lowercase-2.3-medium.txt [Status: 403, Size: 275, Words: 20, Lines: 10, Duration: 1ms]
#                       [Status: 403, Size: 275, Words: 20, Lines: 10, Duration: 2ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/  [Status: 403, Size: 275, Words: 20, Lines: 10, Duration: 9ms]
# or send a letter to Creative Commons, 171 Second Street,  [Status: 403, Size: 275, Words: 20, Lines: 10, Duration: 8ms]
                        [Status: 403, Size: 275, Words: 20, Lines: 10, Duration: 9ms]
# Copyright 2007 James Fisher [Status: 403, Size: 275, Words: 20, Lines: 10, Duration: 9ms]
#                       [Status: 403, Size: 275, Words: 20, Lines: 10, Duration: 13ms]
#                       [Status: 403, Size: 275, Words: 20, Lines: 10, Duration: 16ms]
# on atleast 2 different hosts [Status: 403, Size: 275, Words: 20, Lines: 10, Duration: 24ms]
# This work is licensed under the Creative Commons  [Status: 403, Size: 275, Words: 20, Lines: 10, Duration: 27ms]
# Suite 300, San Francisco, California, 94105, USA. [Status: 403, Size: 275, Words: 20, Lines: 10, Duration: 42ms]
# Attribution-Share Alike 3.0 License. To view a copy of this  [Status: 403, Size: 275, Words: 20, Lines: 10, Duration: 43ms]
#                       [Status: 403, Size: 275, Words: 20, Lines: 10, Duration: 43ms]
# Priority ordered case insensative list, where entries were found  [Status: 403, Size: 275, Words: 20, Lines: 10, Duration: 61ms]
                        [Status: 403, Size: 275, Words: 20, Lines: 10, Duration: 75ms]
jquery                  [Status: 301, Size: 320, Words: 20, Lines: 10, Duration: 3ms]
[WARN] Directory found, but recursion depth exceeded. Ignoring: http://172.17.0.2/javascript/jquery/
:: Progress: [207643/207643] :: Job [2/2] :: 2439 req/sec :: Duration: [0:01:17] :: Errors: 0 ::
```

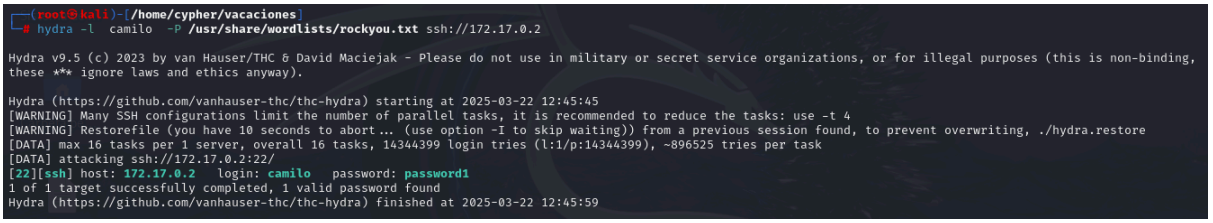
Un escaneo con Nikto para no pasar por alguna vulnerabilidad o información comprometedora en la web.

Revisé el código de la web, y está ese comentario. Se puede deducir que hay un usuario “juan” y un usuario “camilo”. No tengo sus contraseñas, pero son usuarios candidatos para aplicar fuerza bruta en SSH.

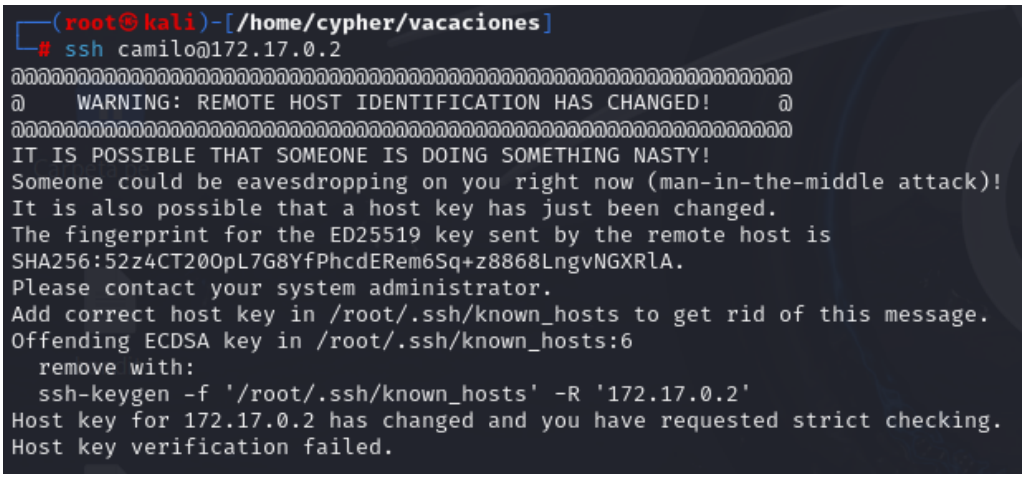


💥 3. Explotación de Vulnerabilidades

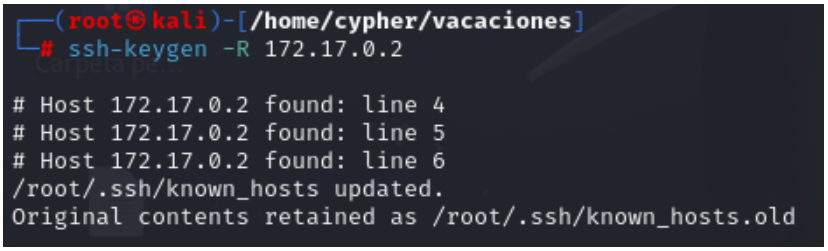
Teniendo el usuario “camilo”, apliqué fuerza bruta con hydra en el servicio SSH para encontrar alguna contraseña.



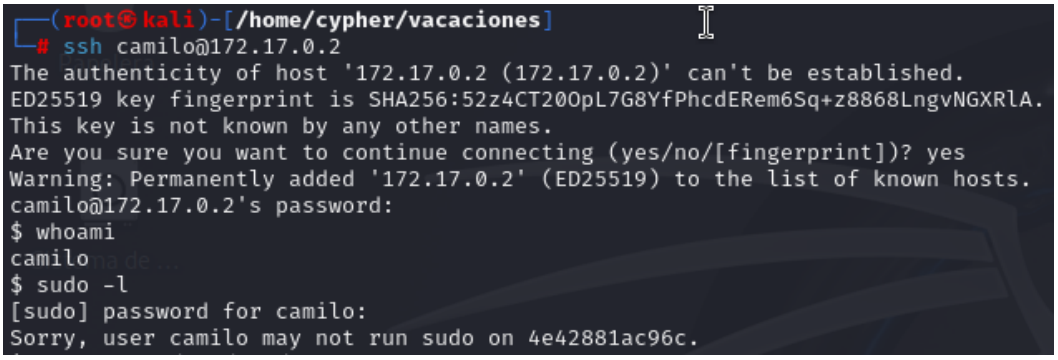
Al ya tener un usuario y contraseña, intenté ingresar por hydra, pero me salió un error, ya que las máquinas de Dockerlabs me suelen salir con IP similares o iguales. Pero buscando en internet encontré que se puede solucionar super fácil.



Con ese comando lo arreglé en un segundo.



Ahora si, volviendo a intentar, se tiene un acceso exitoso por SSH.



🔐 4. Escalada de Privilegios y Post-explotación

Reviso con métodos simples la existencia de alguna vulnerabilidad para escalar privilegios. Pero no logré encontrar nada interesante.

```
$ getcap -r / 2>/dev/null
$  find / -perm -4000 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/gpasswd
/usr/bin/chfn
/usr/bin/sudo
/bin/su
/bin/umount
/bin/mount
```

```
$ find / -name 'correo' 2>/dev/null
$
$ find / -name 'mail' 2>/dev/null
/var/mail
/var/spool/mail
$ pwd
/home/camilo
$ cd ..
$ cd ..
$ cd var/mail
$ ls
camilo
```

Buscando archivos en la máquina, encontré un correo.txt y al abrirlo me da una contraseña que puede servir para iniciar sesión en otro usuario. Recordando que antes encontramos los usuarios “juan” y “camilo”. También tiene sentido, ya que en el comentario de la web dice que Juan le dejó un correo a Camilo.

```
$ cd camilo
$ ls
correo.txt
$ cat correo.txt
Hola Camilo,

Me voy de vacaciones y no he terminado el trabajo que me dio el jefe. Por si acaso lo pide, aquí tienes la contraseña: 2k84dicb
```

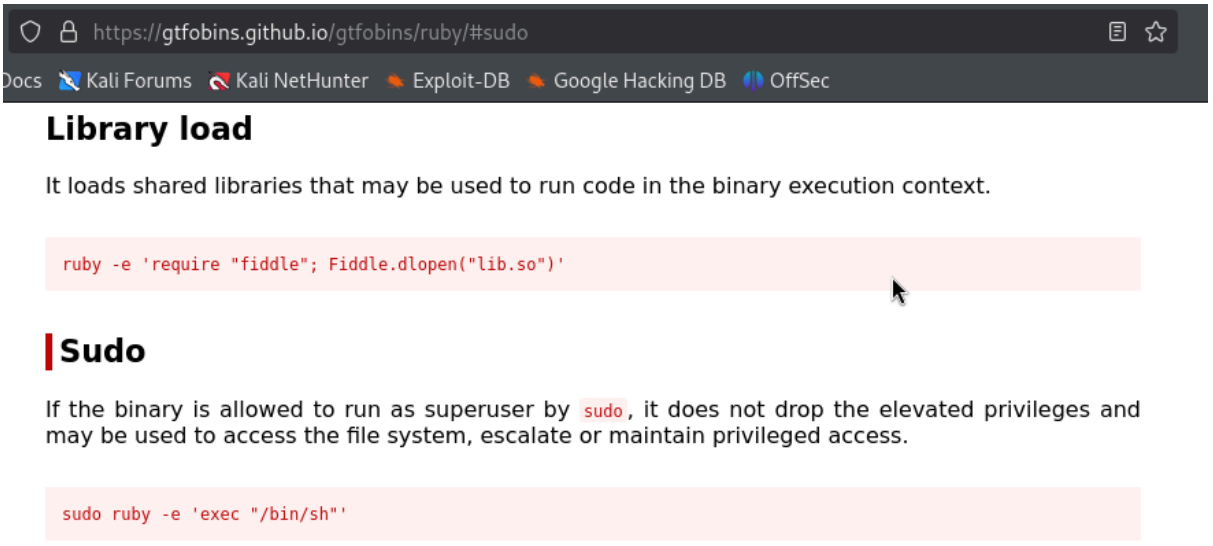
```
$ su juan
Password:
$ whoami
juan
```

Se logró ingresar al usuario “juan” usando la contraseña encontrada en correo.txt. Ahora, busco posibles vulnerabilidades para escalar privilegios con ese usuario.

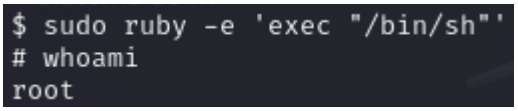
```
$ getcap -r / 2>/dev/null
$ sudo -l
Matching Defaults entries for juan on 4e42881ac96c:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User juan may run the following commands on 4e42881ac96c:
    (ALL) NOPASSWD: /usr/bin/ruby
```

Buscando en GTFOBins el archivo encontrado anteriormente, me arroja que un comando puede servir para explotarlo y obtener la escalada de privilegios.



Finalmente, al ingresar el comando encontrado en GTFOBins se logra tener privilegios root.



🏆 Banderas y Resultados

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