FILECEPTION

DESPLIEGUE

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

```
unzip fileception.zip

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

2- Y ahora desplegamos la máquina

```
bash auto_deploy.sh fileception.tar
```

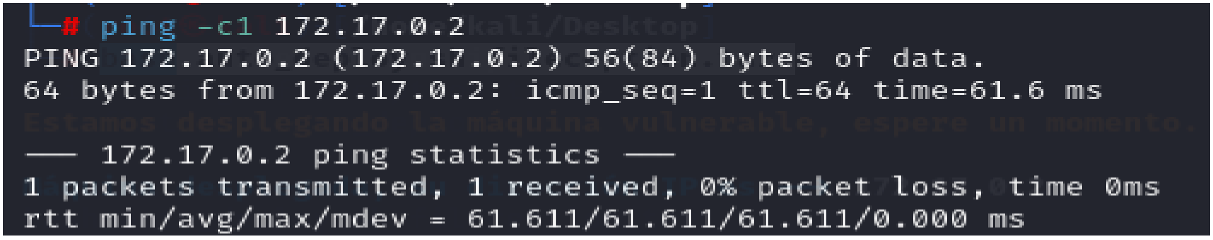
Estamos desplegando la máquina vulnerable, espere un momento.

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=61.6 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 61.611/61.611/61.611/0.000 ms
```

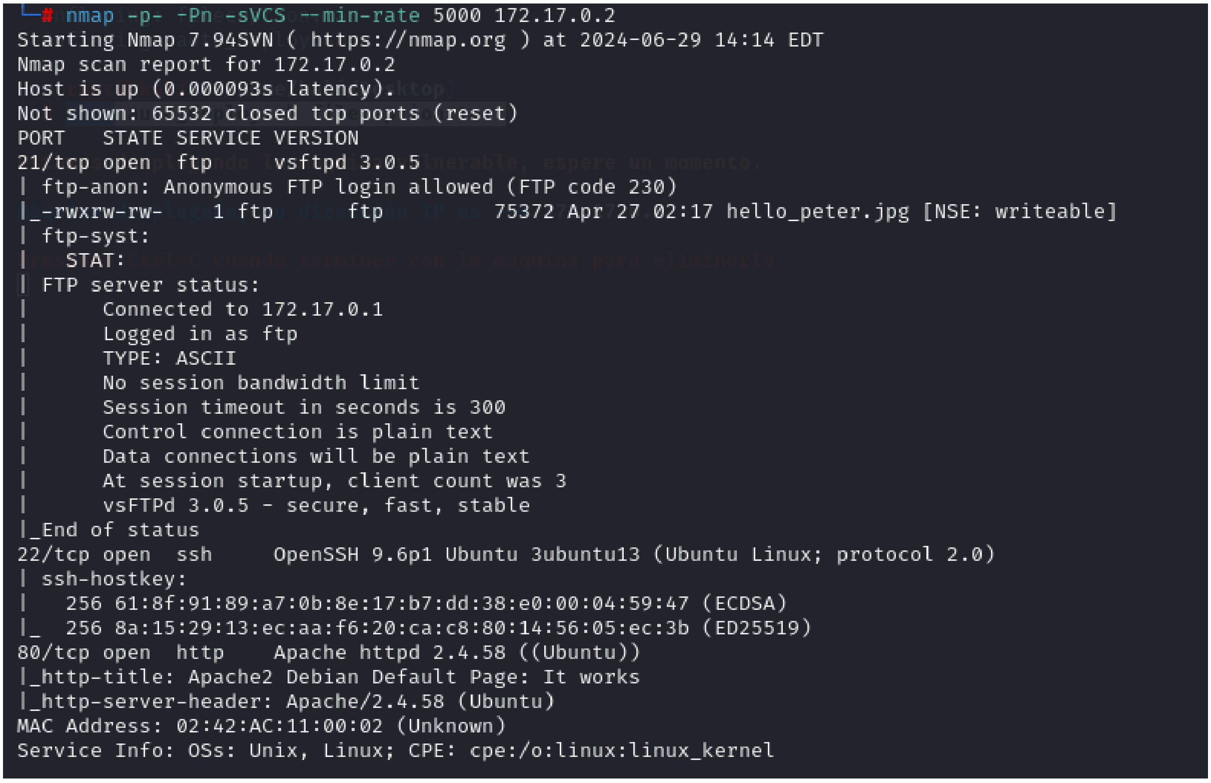
IP DE LA MÁQUINA VÍCTIMA   172.17.0.2

IP DE LA MÁQUINA ATACANTE 192.168.0.26

LINUX- ttl=64

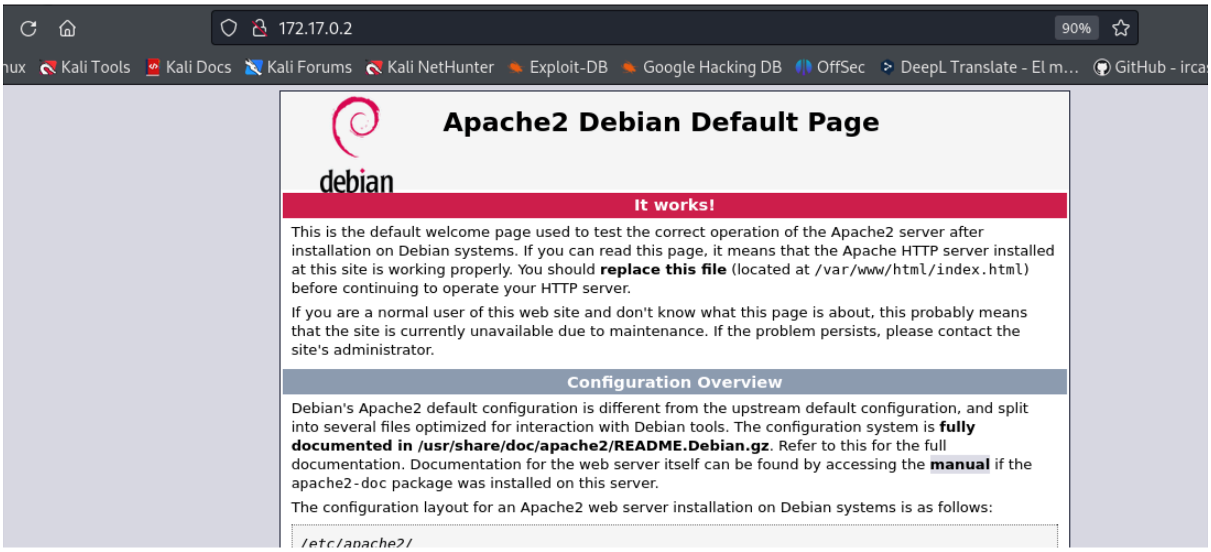
ESCANEO DE PUERTOS

```
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 2024-06-29 14:14 EDT
Nmap scan report for 172.17.0.2
Host is up (0.000093s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rwxrw-rw-    1 ftp      ftp         75372 Apr 27 02:17 hello_peter.jpg [NSE: writeable]
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 172.17.0.1
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.5 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 61:8f:91:89:a7:0b:8e:17:b7:dd:38:e0:00:04:59:47 (ECDSA)
|_  256 8a:15:29:13:ec:aa:f6:20:ca:c8:80:14:56:05:ec:3b (ED25519)
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

PUERTO 80



Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. 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/index.html`) before continuing to operate your HTTP server.

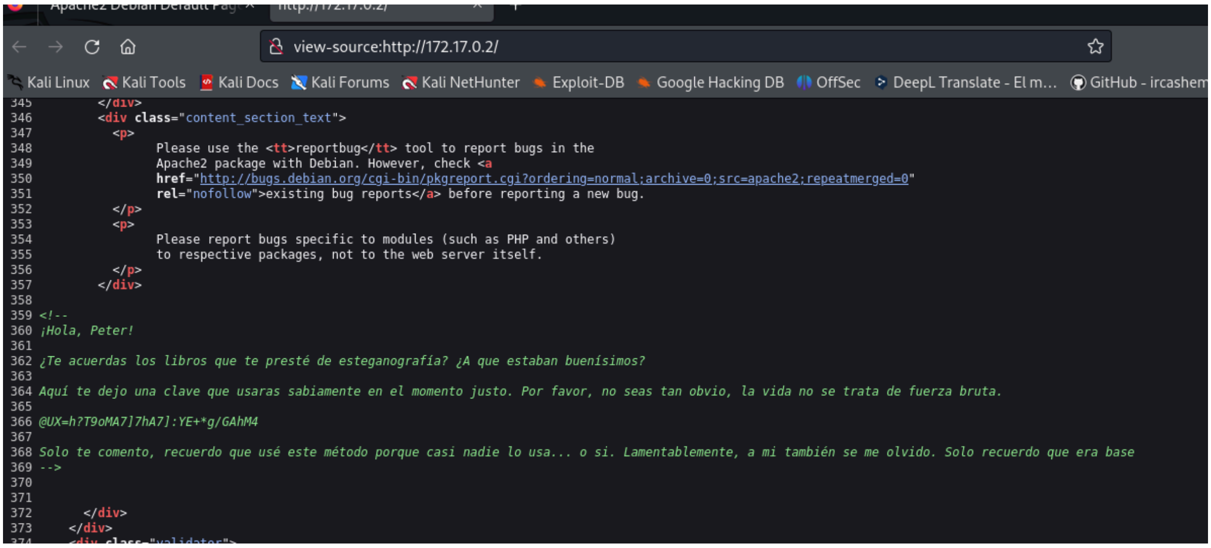
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian 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 **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
```



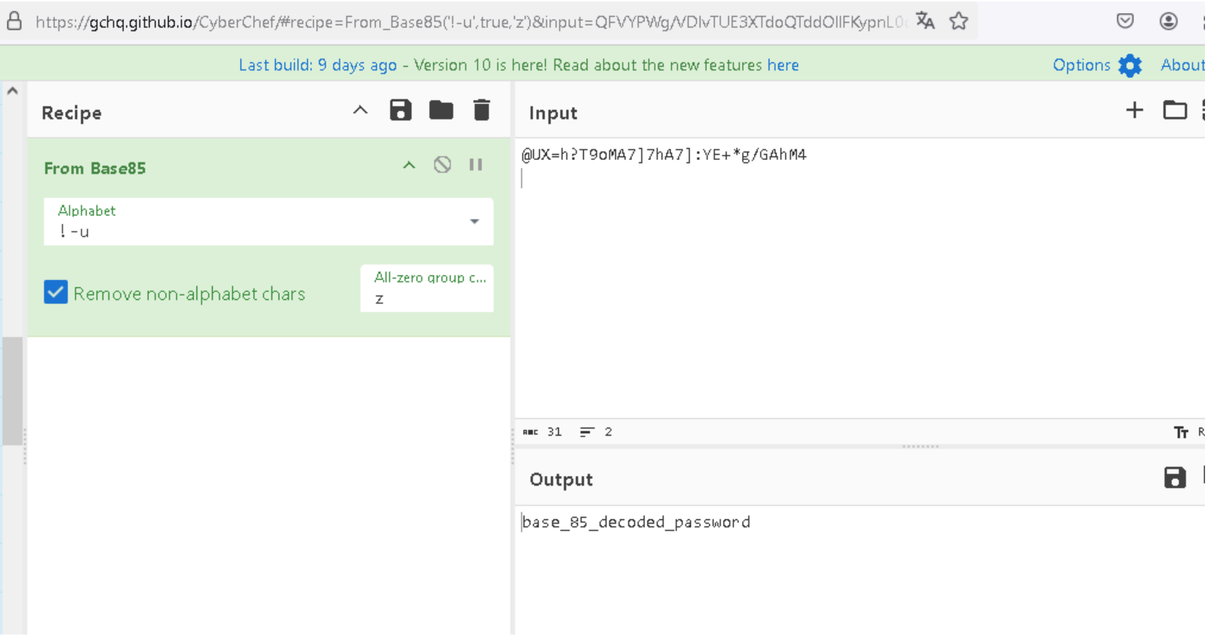
view-source:http://172.17.0.2/

```
        </div>
        <div class="content_section_text">
          <p>
                Please use the <tt>reportbug</tt> tool to report bugs in the
                Apache2 package with Debian. However, check <a
                href="http://bugs.debian.org/cgi-bin/pkgreport.cgi?ordering=normal;archive=0;src=apache2;repeatmerged=0"
                rel="nofollow">existing bug reports</a> before reporting a new bug.
          </p>
          <p>
                Please report bugs specific to modules (such as PHP and others)
                to respective packages, not to the web server itself.
          </p>
        </div>

<!--
¡Hola, Peter!

¿Te acuerdas los libros que te presté de esteganografía? ¿A que estaban buenísimos?

Aquí te dejo una clave que usaras sabiamente en el momento justo. Por favor, no seas tan obvio, la vida no se trata de fuerza bruta.

@UX=h?T9oMA7]7hA7]:YE+*g/GAhM4

Solo te comento, recuerdo que usé este método porque casi nadie lo usa... o si. Lamentablemente, a mi también se me olvido. Solo recuerdo que era base
-->


      </div>
    </div>
    <div class="validator">
```

Usuario peter y contraseña @UX=h?T9oMA7]7hA7]:YE+*g/GAhM4

Nos vamos a https://gchq.github.io/CyberChef/. En input ponemos la cadena a analizar

le damos a la barita mágica y tenemos base_85_decoded_password



https://gchq.github.io/CyberChef/#recipe=From_Base85('!-u',true,'z')&input=QFVYPWg/VDlvTUE3XTdoQTddOllFKypnL0

Last build: 9 days ago - Version 10 is here! Read about the new features here

Recipe

From Base85

Alphabet: !-u

☑ Remove non-alphabet chars

All-zero group c...: z

Input

```
@UX=h?T9oMA7]7hA7]:YE+*g/GAhM4
```

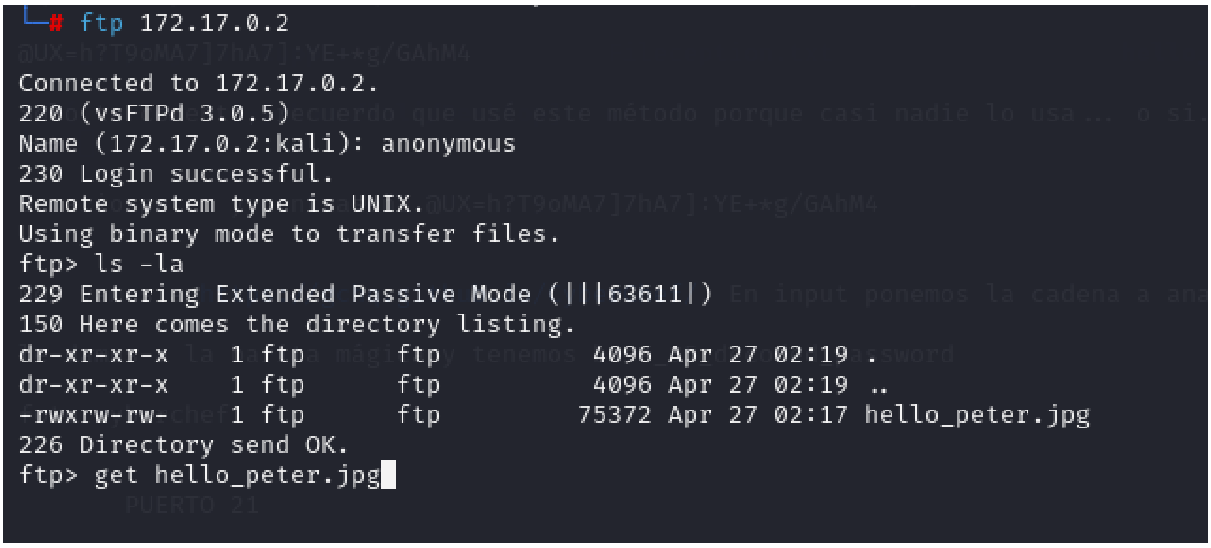
31 2

Output

```
base_85_decoded_password
```

PUERTO 21

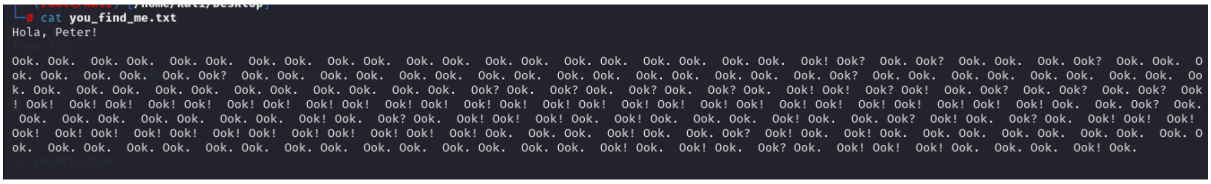
Accedemos al puerto 21, listamos y nos descargamos el .jpg



```
└─# ftp 172.17.0.2
Connected to 172.17.0.2.
220 (vsFTPd 3.0.5)
Name (172.17.0.2:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (|||63611|)
150 Here comes the directory listing.
dr-xr-xr-x    1 ftp      ftp          4096 Apr 27 02:19 .
dr-xr-xr-x    1 ftp      ftp          4096 Apr 27 02:19 ..
-rwxrw-rw-    1 ftp      ftp         75372 Apr 27 02:17 hello_peter.jpg
226 Directory send OK.
ftp> get hello_peter.jpg
```

Con steghide intentamos extraer información del jpg

cat you_find_me.txt



```
└─# cat you_find_me.txt
Hola, Peter!

Ook. Ook.  Ook. Ook.  Ook. Ook.  Ook. Ook.  Ook. Ook.  Ook. Ook.  Ook. Ook.  Ook. Ook.  Ook. Ook.  Ook. Ook.  Ook! Ook?  Ook. Ook?  Ook. Ook.  Ook. Ook?  Ook. Ook.  O
ok. Ook.  Ook. Ook.  Ook. Ook?  Ook. Ook.  Ook. Ook.  Ook. Ook.  Ook. Ook.  Ook. Ook.  Ook. Ook.  Ook. Ook.  Ook. Ook?  Ook. Ook.  Ook. Ook.  Ook. Ook.  Ook. Ook.  Oo
k. Ook.  Ook. Ook.  Ook. Ook.  Ook. Ook.  Ook. Ook.  Ook. Ook.  Ook? Ook.  Ook? Ook.  Ook? Ook.  Ook? Ook.  Ook! Ook!  Ook? Ook!  Ook. Ook?  Ook. Ook?  Ook. Ook?  Ook
! Ook!  Ook! Ook!  Ook! Ook!  Ook! Ook!  Ook! Ook!  Ook! Ook!  Ook! Ook!  Ook! Ook!  Ook! Ook!  Ook! Ook!  Ook! Ook!  Ook! Ook!  Ook! Ook!  Ook! Ook.  Ook. Ook?  Ook.
 Ook.  Ook. Ook.  Ook. Ook.  Ook. Ook.  Ook! Ook.  Ook? Ook.  Ook! Ook!  Ook! Ook.  Ook! Ook.  Ook. Ook.  Ook! Ook.  Ook. Ook?  Ook! Ook.  Ook? Ook.  Ook! Ook!  Ook!
Ook!  Ook! Ook!  Ook! Ook!  Ook! Ook!  Ook! Ook!  Ook! Ook!  Ook! Ook.  Ook. Ook.  Ook! Ook.  Ook. Ook?  Ook! Ook.  Ook! Ook.  Ook. Ook.  Ook. Ook.  Ook. Ook.  Ook. O
ok.  Ook. Ook.  Ook. Ook.  Ook. Ook.  Ook. Ook.  Ook. Ook.  Ook. Ook.  Ook. Ook.  Ook! Ook.  Ook! Ook.  Ook? Ook.  Ook! Ook!  Ook! Ook.  Ook. Ook.  Ook! Ook.
```

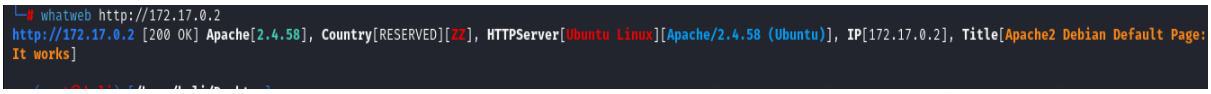
Es el lenguaje de programación Ook!, que es un lenguaje esotérico diseñado como una broma. Está basado en comandos simples usando sólo las palabras "Ook." y "Ook!", y su sintaxis está inspirada en el estilo de los orangutanes.

Nos vamos a https://www.dcode.fr/ook-language

9h889h23hhss2

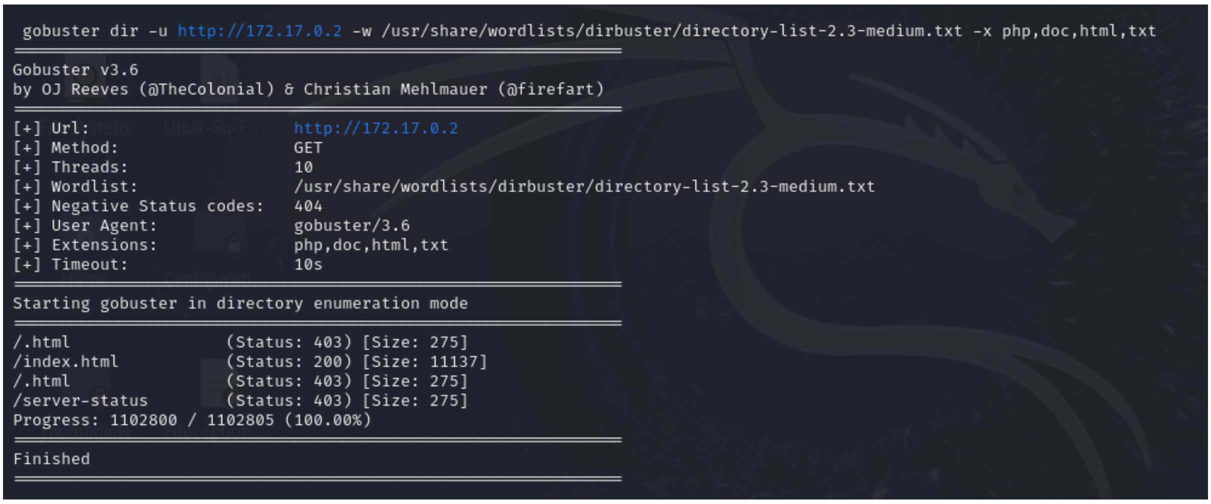
ENUMERACIÓN

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][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.58 (Ubuntu)], IP[172.17.0.2], Title[Apache2 Debian Default Page:
It works]
```

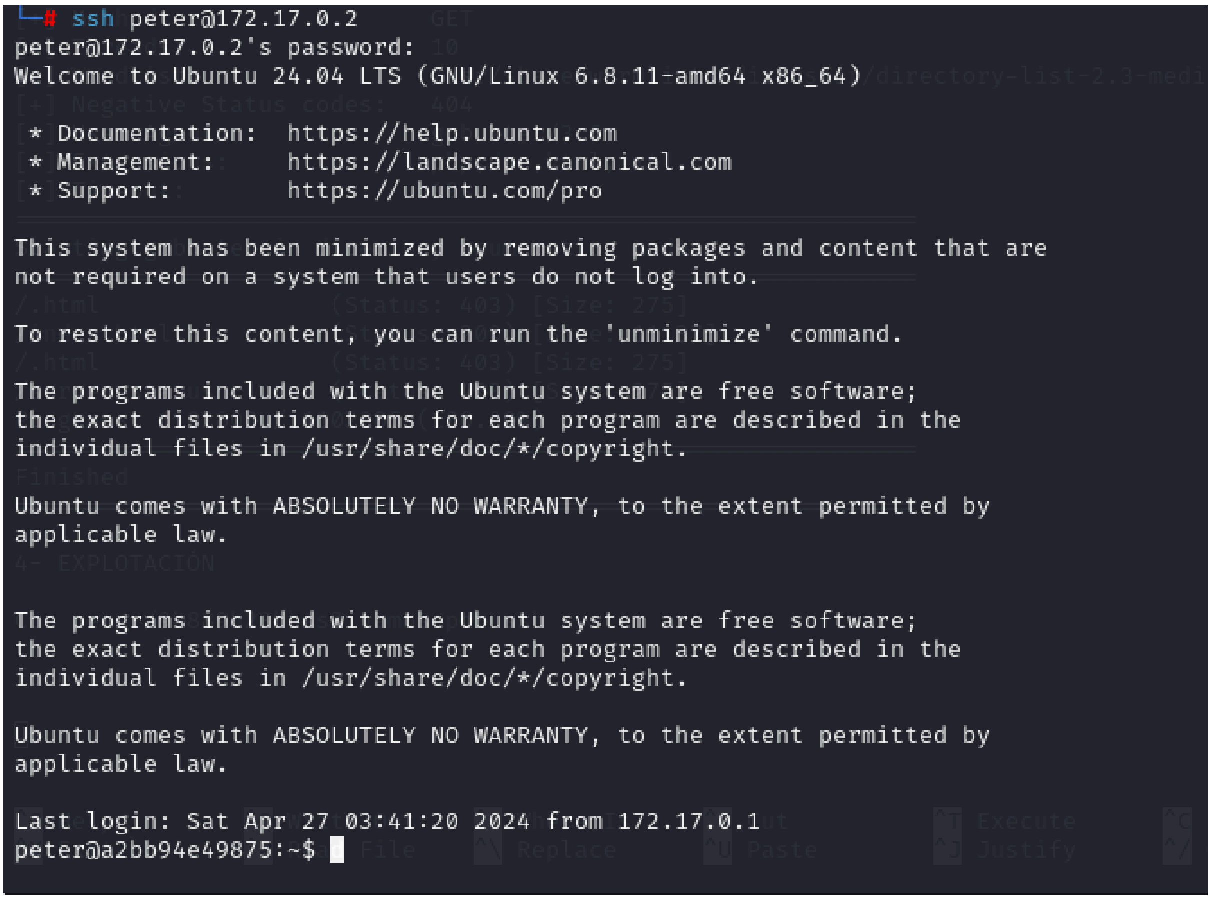
gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html,txt



```
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:              php,doc,html,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 275]
/index.html           (Status: 200) [Size: 11137]
/.html                (Status: 403) [Size: 275]
/server-status        (Status: 403) [Size: 275]
Progress: 1102800 / 1102805 (100.00%)
===============================================================
Finished
===============================================================
```

EXPLOTACIÓN

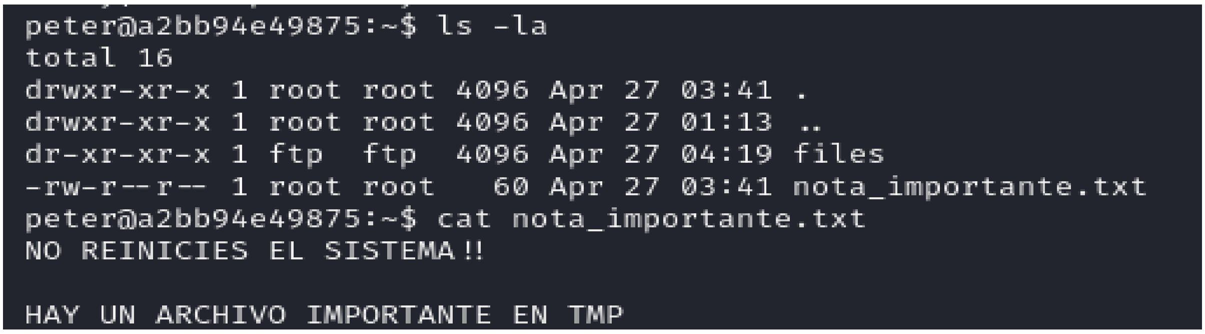
Con peter/9h889h23hhss2 vamos por ssh



```
└─# ssh peter@172.17.0.2
peter@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.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Sat Apr 27 03:41:20 2024 from 172.17.0.1
peter@a2bb94e49875:~$ 
```

ESCALADA DE PRIVILEGIOS

Listamos y nos encontramos con nota importante



```
peter@a2bb94e49875:~$ ls -la
total 16
drwxr-xr-x 1 root root 4096 Apr 27 03:41 .
drwxr-xr-x 1 root root 4096 Apr 27 01:13 ..
dr-xr-xr-x 1 ftp  ftp  4096 Apr 27 04:19 files
-rw-r--r-- 1 root root   60 Apr 27 03:41 nota_importante.txt
peter@a2bb94e49875:~$ cat nota_importante.txt
NO REINICIES EL SISTEMA!!

HAY UN ARCHIVO IMPORTANTE EN TMP
```

Vamos a /tmp

Tenemos dos archivos

```
peter@a2bb94e49875:/tmp$ ls -la
total 28
drwxrwxrwt 1 root   root   4096 Jun 30 20:43 .
drwxr-xr-x 1 root   root   4096 Jun 30 20:43 ..
-rw-r--r-- 1 ubuntu ubuntu 14558 Apr 27 03:38 importante_octopus.odt
-rw-r--r-- 1 root   root     114 Apr 27 02:20 recuerdos_del_sysadmin.txt
```

```
peter@a2bb94e49875:/tmp$ cat recuerdos_del_sysadmin.txt

Cuando era niño recuerdo que, a los videos, para pasarlos de

flv a mp4, solo cambiaba la extensión. Que iluso.
```

Nos traemos a nuestro kali el otro archivo

```
scp peter@172.17.0.2:/tmp/importante_octopus.odt /home/kali/Desktop

peter@172.17.0.2's password:
importante_octopus.odt
```

Como el primer archivo nos habla de la posibilidad de cambiar la extensión de archivos, con el comando mv, vamos probando el comportamiento y la información obtenida con varias extensiones, hasta que al cambiar a formato

.zip

```
mv importante_octopus.odt importante_octopus.zip
```

Ahora, con unzip

```
 unzip importante_octopus.zip
Archive:  importante_octopus.zip
   creating: Configurations2/accelerator/
   creating: Configurations2/floater/
   creating: Configurations2/images/Bitmaps/
   creating: Configurations2/menubar/
   creating: Configurations2/popupmenu/
   creating: Configurations2/progressbar/
   creating: Configurations2/statusbar/
   creating: Configurations2/toolbar/
   creating: Configurations2/toolpanel/
  inflating: META-INF/manifest.xml
 extracting: Thumbnails/thumbnail.png
  inflating: content.xml
  inflating: leerme.xml
  inflating: manifest.rdf
  inflating: meta.xml
 extracting: mimetype
  inflating: settings.xml
  inflating: styles.xml
```

```
cat leerme.xml
```

Decirle a Peter que me pase el odt de mis anécdotas, en caso de que se me

olviden mis credenciales de administrador... Él no sabe de Esteganografía,

nunca se imaginaría esto.

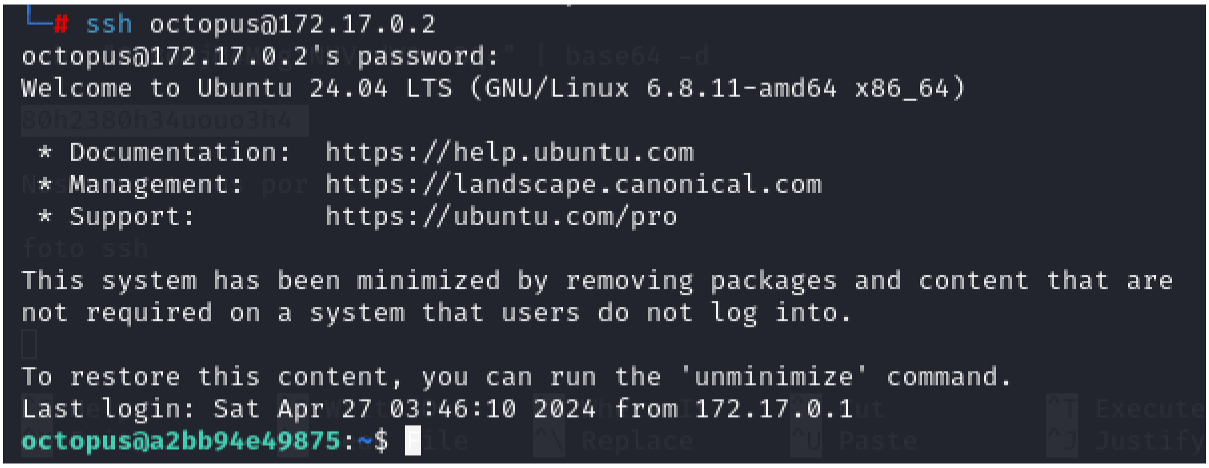
usuario: octopus
password: ODBoMjM4MGgzNHVvdW8zaDQ=

Tenemos usuario y contraseña; esta parece estar codificada en base64

```
echo "ODBoMjM4MGgzNHVvdW8zaDQ=" | base64 -d
```

```
80h2380h34uouo3h4
```

Nos conectamos por ssh



```
└─# ssh octopus@172.17.0.2
octopus@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: Sat Apr 27 03:46:10 2024 from 172.17.0.1
octopus@a2bb94e49875:~$
```

Buscamos permisos sudo

```
octopus@a2bb94e49875:~$ sudo -l

Matching Defaults entries for octopus on a2bb94e49875:
	env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
use_pty

User octopus may run the following commands on a2bb94e49875:
	(ALL) NOPASSWD: ALL
	(ALL : ALL) ALL

octopus@a2bb94e49875:~$ sudo su

[sudo] password for octopus:
root@a2bb94e49875:/home/octopus# whoami
root
root@a2bb94e49875:/home/octopus#
```