QUERIES:

This database allows us to select all the connections from the network table that are classified as SQL Injection attacks:

For example:

- This query selects all columns from the network and joins them with the attacks table on the attack_id column. It then filters the result set to include only those records where the attack type is 'SQL Injection'.

```
MariaDB [Project]> SELECT *
    -> FROM network n
    -> JOIN attacks a ON n.attack_id = a.attack_id
    -> WHERE a.attack_type = 'SQL Injection';
+------------+----------+---------------+-----------+-------------+-------------+-----------+---------------+--------------+
| network_id | duration | protocol_type | attack_id | host_id_src | host_id_dst | attack_id | attack_type   | attack_level |
+------------+----------+---------------+-----------+-------------+-------------+-----------+---------------+--------------+
|          2 |      150 | UDP           |         2 |           5 |          22 |         2 | SQL Injection |            8 |
+------------+----------+---------------+-----------+-------------+-------------+-----------+---------------+--------------+
1 row in set (0.113 sec)
```

This database also allows us to identify suspicious patterns:

For example:

- Query to identify network connections exhibiting suspicious patterns, such as a high volume of traffic originating from a single source.

```
MariaDB [Project]> SELECT host_id_src, SUM(duration) AS total_duration
    -> FROM network
    -> GROUP BY host_id_src
    -> HAVING total_duration > 50;
+-------------+----------------+
| host_id_src | total_duration |
+-------------+----------------+
|           2 |            300 |
|           5 |            150 |
|          35 |            500 |
+-------------+----------------+
3 rows in set (0.044 sec)
```