Google certificate project

SQL-based Security Investigation

Realized by:

Nada Maach

Contents

1 Introduction

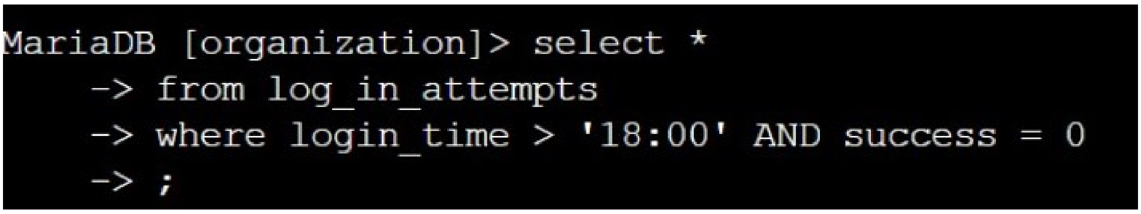
As a security professional in a large organization, one of the key responsibilities is to identify, analyze, and mitigate potential threats. This project demonstrates how SQL can be used to investigate suspicious activities in system logs and employee records.

The objectives of this report are to:

- Detect failed login attempts occurring after business hours.
- Investigate suspicious login activity on specific dates.
- Identify login attempts from outside Mexico.
- Retrieve information about employees in certain departments and locations.
- Exclude specific departments from update operations.

2 Investigating Failed Logins After Business Hours

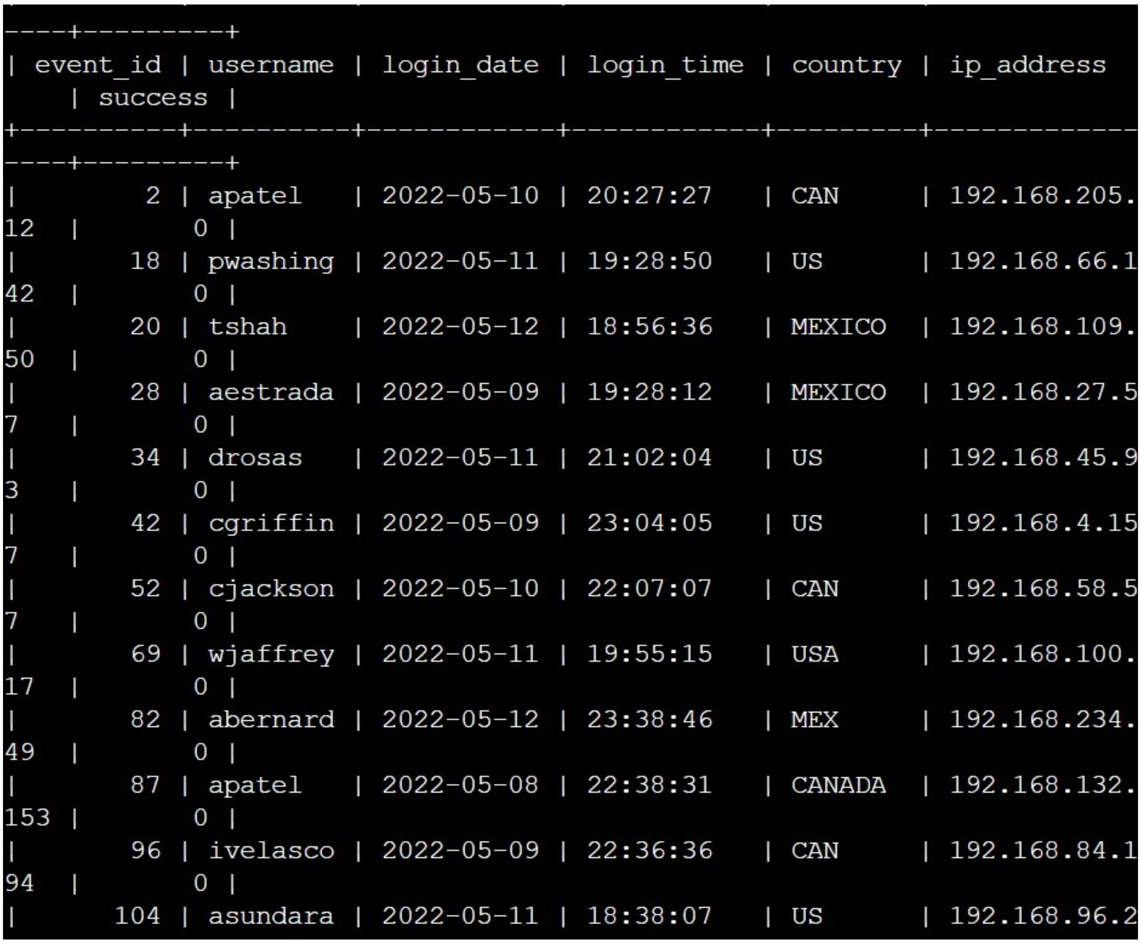
Unauthorized access often occurs outside working hours. We query for failed login attempts (success = 0) that happened after 18:00.



```
MariaDB [organization]> select *
    -> from log_in_attempts
    -> where login_time > '18:00' AND success = 0
    -> ;
```

Figure 1: SQL query to detect failed logins after 18:00

The following figure illustrates a significant number of failed login attempts occurring after 18:00, which strongly suggests the possibility of a malicious attack.

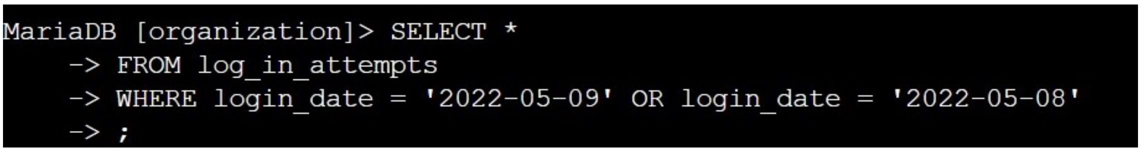


```
----+---------+
| event_id | username | login_date | login_time | country | ip_address
    | success |
+----------+----------+------------+------------+---------+-------------
----+---------+
|        2 | apatel   | 2022-05-10 | 20:27:27   | CAN     | 192.168.205.
12   |       0 |
|       18 | pwashing | 2022-05-11 | 19:28:50   | US      | 192.168.66.1
42   |       0 |
|       20 | tshah    | 2022-05-12 | 18:56:36   | MEXICO  | 192.168.109.
50   |       0 |
|       28 | aestrada | 2022-05-09 | 19:28:12   | MEXICO  | 192.168.27.5
7    |       0 |
|       34 | drosas   | 2022-05-11 | 21:02:04   | US      | 192.168.45.9
3    |       0 |
|       42 | cgriffin | 2022-05-09 | 23:04:05   | US      | 192.168.4.15
7    |       0 |
|       52 | cjackson | 2022-05-10 | 22:07:07   | CAN     | 192.168.58.5
7    |       0 |
|       69 | wjaffrey | 2022-05-11 | 19:55:15   | USA     | 192.168.100.
17   |       0 |
|       82 | abernard | 2022-05-12 | 23:38:46   | MEX     | 192.168.234.
49   |       0 |
|       87 | apatel   | 2022-05-08 | 22:38:31   | CANADA  | 192.168.132.
153  |       0 |
|       96 | ivelasco | 2022-05-09 | 22:36:36   | CAN     | 192.168.84.1
94   |       0 |
|      104 | asundara | 2022-05-11 | 18:38:07   | US      | 192.168.96.2
```

Figure 2: Result: SQL query to detect failed logins after 18:00

3 Retrieve Login Attempts on Specific Dates

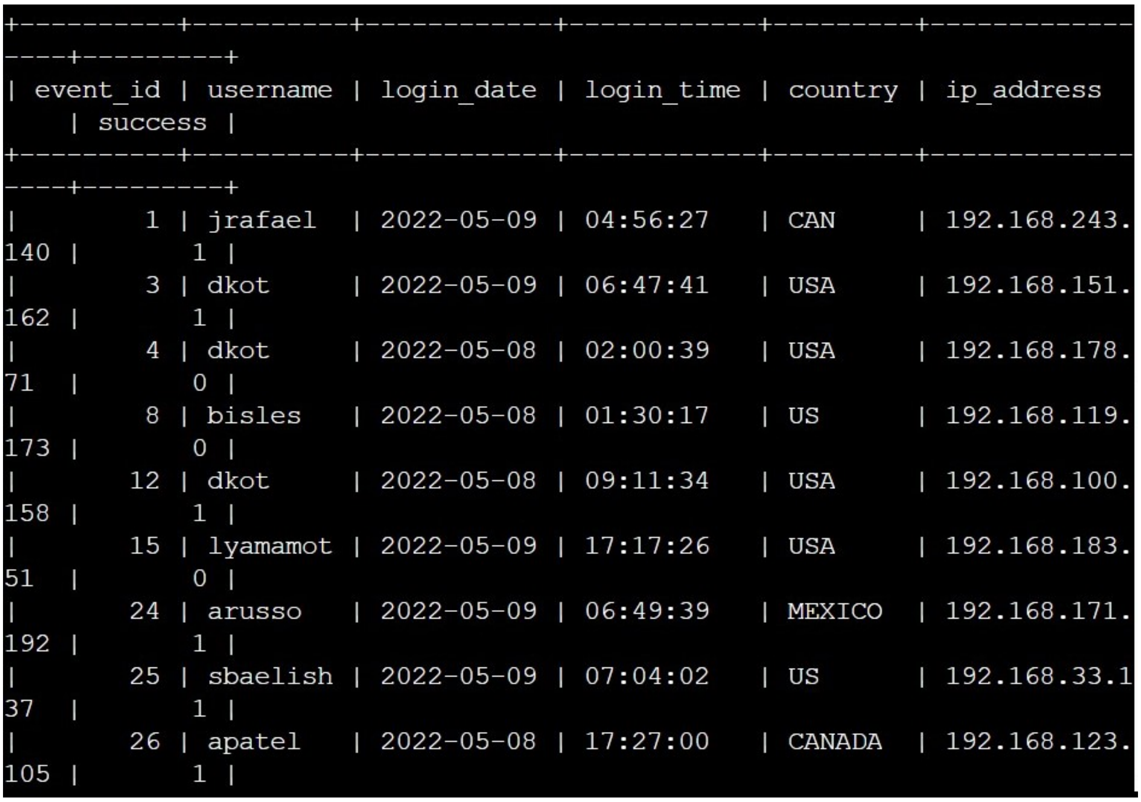
To investigate an incident, we extract all login attempts on `2022-05-09` and the day before.



```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE login_date = '2022-05-09' OR login_date = '2022-05-08'
    -> ;
```

Figure 3: SQL query for suspicious dates

In the context of an incident investigation, we analyze login dates to identify unusual activity. As shown in the following figure, multiple login attempts from different IP addresses were recorded, warranting further investigation.

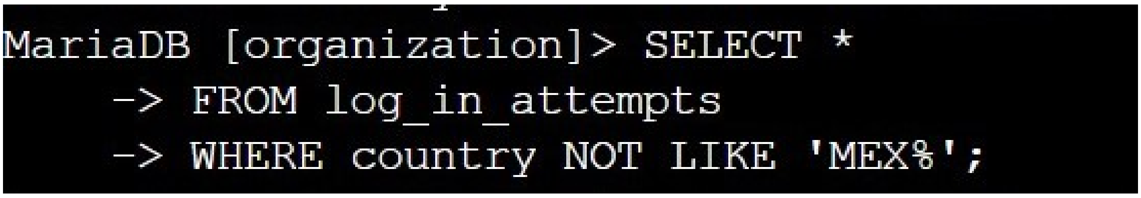


```
+----------+----------+------------+------------+---------+-------------
----+---------+
| event_id | username | login_date | login_time | country | ip_address
    | success |
+----------+----------+------------+------------+---------+-------------
----+---------+
|        1 | jrafael  | 2022-05-09 | 04:56:27   | CAN     | 192.168.243.
140 |       1 |
|        3 | dkot     | 2022-05-09 | 06:47:41   | USA     | 192.168.151.
162 |       1 |
|        4 | dkot     | 2022-05-08 | 02:00:39   | USA     | 192.168.178.
71  |       0 |
|        8 | bisles   | 2022-05-08 | 01:30:17   | US      | 192.168.119.
173 |       0 |
|       12 | dkot     | 2022-05-08 | 09:11:34   | USA     | 192.168.100.
158 |       1 |
|       15 | lyamamot | 2022-05-09 | 17:17:26   | USA     | 192.168.183.
51  |       0 |
|       24 | arusso   | 2022-05-09 | 06:49:39   | MEXICO  | 192.168.171.
192 |       1 |
|       25 | sbaelish | 2022-05-09 | 07:04:02   | US      | 192.168.33.1
37  |       1 |
|       26 | apatel   | 2022-05-08 | 17:27:00   | CANADA  | 192.168.123.
105 |       1 |
```

Figure 4: Result: SQL query for suspicious dates

4 Retrieve Login Attempts Outside of Mexico

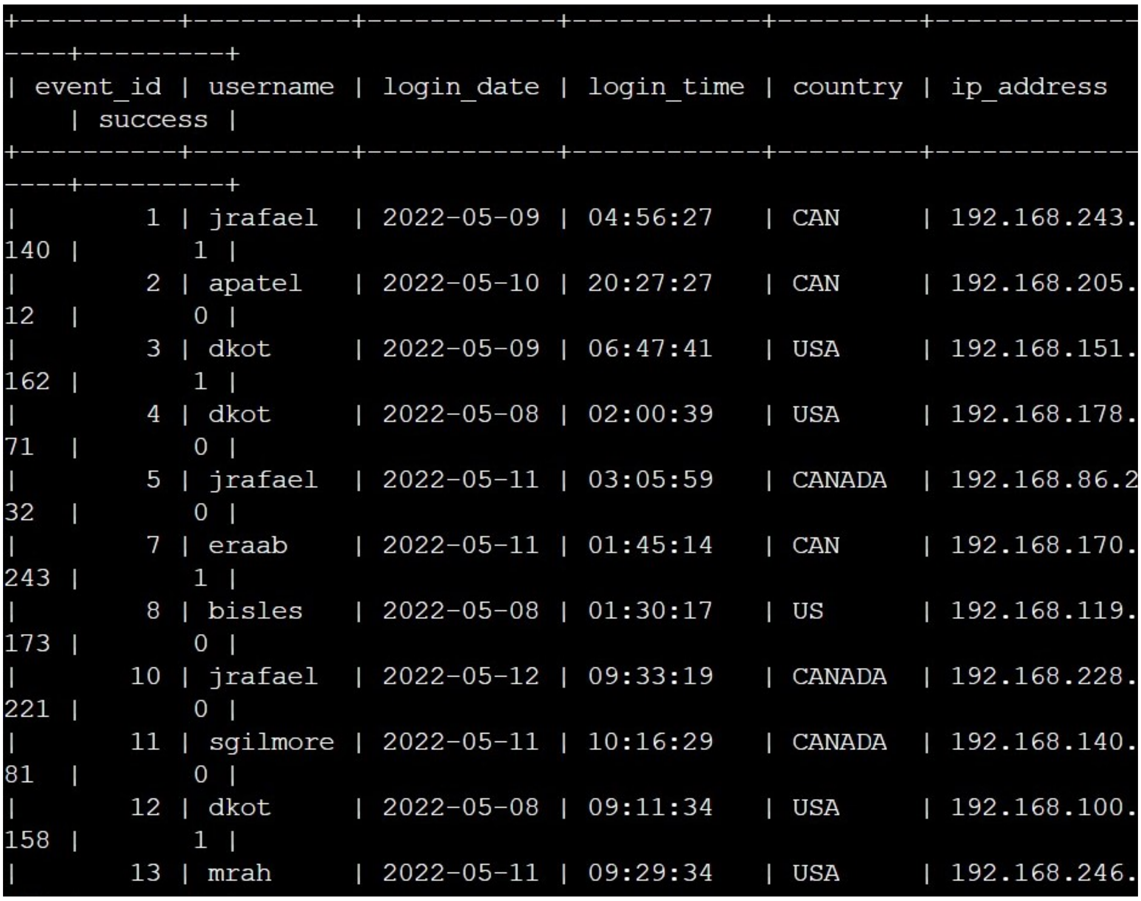
Attackers often connect from unexpected locations. The following query filters out all logins not originating from Mexico:



```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE country NOT LIKE 'MEX%';
```

Figure 5: SQL query for non-Mexico logins

The following results reveal multiple login attempts originating from unusual geographic locations, indicating activity that requires further investigation.

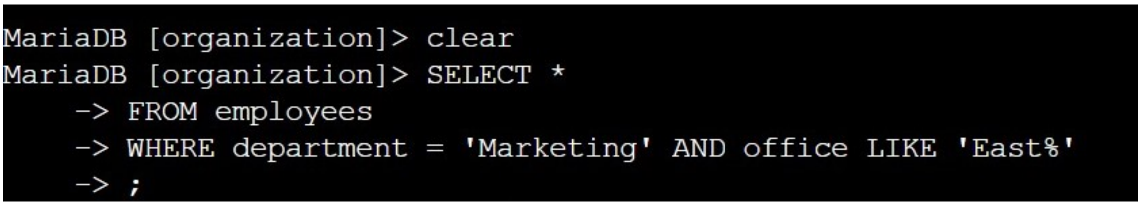


```
+----------+----------+------------+------------+---------+------------
----+---------+
| event_id | username | login_date | login_time | country | ip_address
    | success |
+----------+----------+------------+------------+---------+------------
----+---------+
|        1 | jrafael  | 2022-05-09 | 04:56:27   | CAN     | 192.168.243.
140 |       1 |
|        2 | apatel   | 2022-05-10 | 20:27:27   | CAN     | 192.168.205.
12  |       0 |
|        3 | dkot     | 2022-05-09 | 06:47:41   | USA     | 192.168.151.
162 |       1 |
|        4 | dkot     | 2022-05-08 | 02:00:39   | USA     | 192.168.178.
71  |       0 |
|        5 | jrafael  | 2022-05-11 | 03:05:59   | CANADA  | 192.168.86.2
32  |       0 |
|        7 | eraab    | 2022-05-11 | 01:45:14   | CAN     | 192.168.170.
243 |       1 |
|        8 | bisles   | 2022-05-08 | 01:30:17   | US      | 192.168.119.
173 |       0 |
|       10 | jrafael  | 2022-05-12 | 09:33:19   | CANADA  | 192.168.228.
221 |       0 |
|       11 | sgilmore | 2022-05-11 | 10:16:29   | CANADA  | 192.168.140.
81  |       0 |
|       12 | dkot     | 2022-05-08 | 09:11:34   | USA     | 192.168.100.
158 |       1 |
|       13 | mrah     | 2022-05-11 | 09:29:34   | USA     | 192.168.246.
```

Figure 6: Result: SQL query for non-Mexico logins

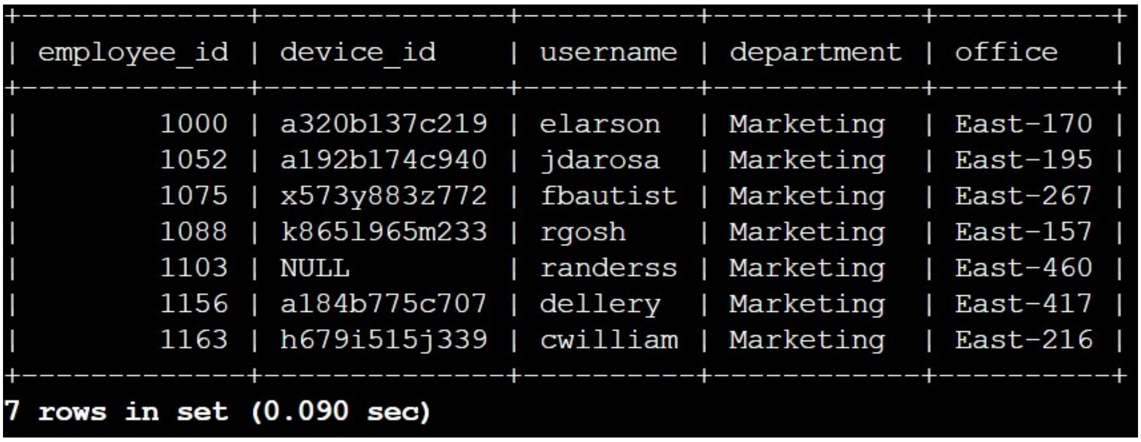
5 Retrieve Employees in Marketing

Employees in Marketing located in the East building require system updates.



```
MariaDB [organization]> clear
MariaDB [organization]> SELECT *
    -> FROM employees
    -> WHERE department = 'Marketing' AND office LIKE 'East%'
    -> ;
```

Figure 7: SQL query for Marketing employees in East building

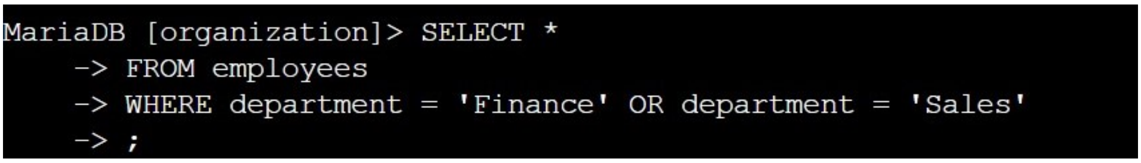


```
+-------------+--------------+----------+------------+----------+
| employee_id | device_id    | username | department | office   |
+-------------+--------------+----------+------------+----------+
|        1000 | a320b137c219 | elarson  | Marketing  | East-170 |
|        1052 | a192b174c940 | jdarosa  | Marketing  | East-195 |
|        1075 | x573y883z772 | fbautist | Marketing  | East-267 |
|        1088 | k8651965m233 | rgosh    | Marketing  | East-157 |
|        1103 | NULL         | randerss | Marketing  | East-460 |
|        1156 | a184b775c707 | dellery  | Marketing  | East-417 |
|        1163 | h679i515j339 | cwilliam | Marketing  | East-216 |
+-------------+--------------+----------+------------+----------+
7 rows in set (0.090 sec)
```

Figure 8: SQL query for Marketing employees in East building

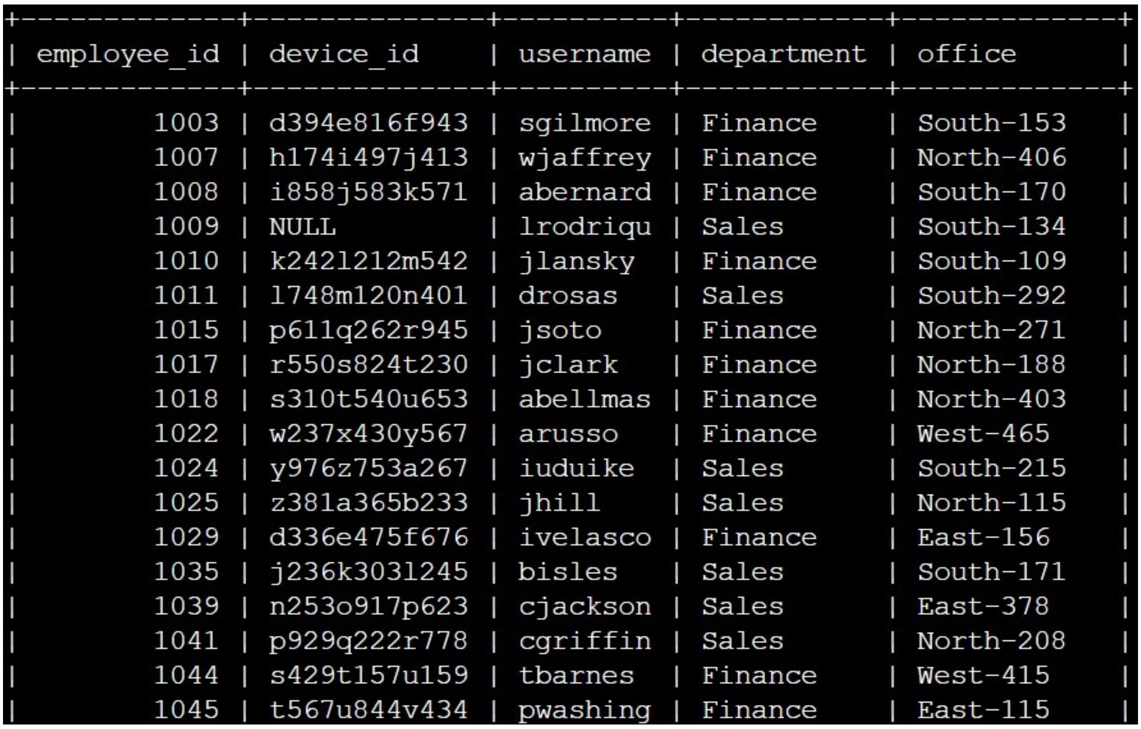
6 Retrieve Employees in Finance or Sales

Updates are also required for Finance and Sales departments.



```
MariaDB [organization]> SELECT *
    -> FROM employees
    -> WHERE department = 'Finance' OR department = 'Sales'
    -> ;
```

Figure 9: SQL query for Finance or Sales employees

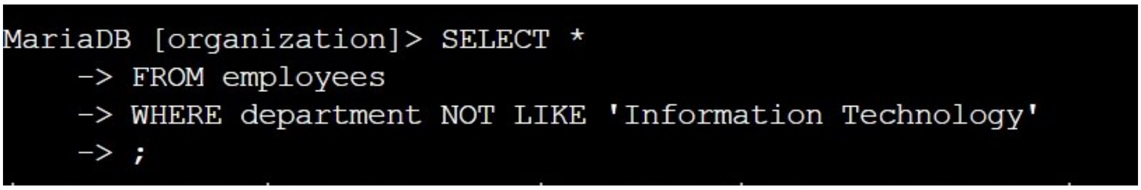


```
+-------------+--------------+----------+------------+-------------+
| employee_id | device_id    | username | department | office      |
+-------------+--------------+----------+------------+-------------+
|        1003 | d394e816f943 | sgilmore | Finance    | South-153   |
|        1007 | h174i497j413 | wjaffrey | Finance    | North-406   |
|        1008 | i858j583k571 | abernard | Finance    | South-170   |
|        1009 | NULL         | lrodriqu | Sales      | South-134   |
|        1010 | k242l212m542 | jlansky  | Finance    | South-109   |
|        1011 | l748m120n401 | drosas   | Sales      | South-292   |
|        1015 | p611q262r945 | jsoto    | Finance    | North-271   |
|        1017 | r550s824t230 | jclark   | Finance    | North-188   |
|        1018 | s310t540u653 | abellmas | Finance    | North-403   |
|        1022 | w237x430y567 | arusso   | Finance    | West-465    |
|        1024 | y976z753a267 | iuduike  | Sales      | South-215   |
|        1025 | z381a365b233 | jhill    | Sales      | North-115   |
|        1029 | d336e475f676 | ivelasco | Finance    | East-156    |
|        1035 | j236k303l245 | bisles   | Sales      | South-171   |
|        1039 | n253o917p623 | cjackson | Sales      | East-378    |
|        1041 | p929q222r778 | cgriffin | Sales      | North-208   |
|        1044 | s429t157u159 | tbarnes  | Finance    | West-415    |
|        1045 | t567u844v434 | pwashing | Finance    | East-115    |
```

Figure 10: SQL query for Finance or Sales employees

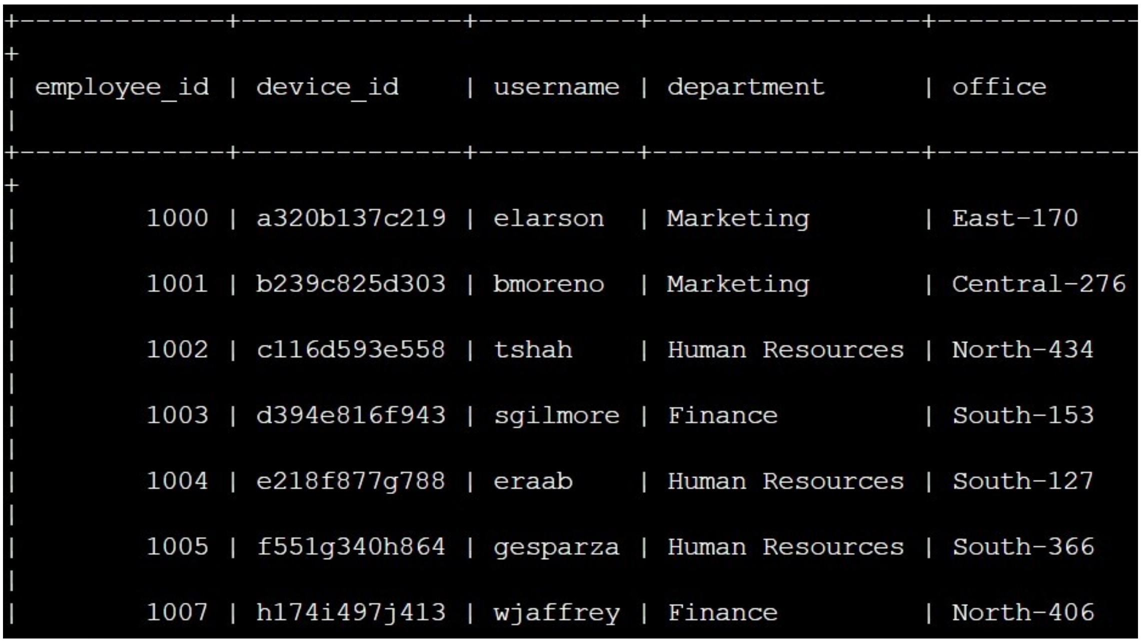
7 Retrieve Employees Not in IT

Since IT department computers are already updated, we exclude them from the next query.
Example result:



```
MariaDB [organization]> SELECT *
    -> FROM employees
    -> WHERE department NOT LIKE 'Information Technology'
    -> ;
```

Figure 11: SQL query for employees not in IT



```
+-------------+--------------+----------+-----------------+------------
+
| employee_id | device_id    | username | department      | office
|
+-------------+--------------+----------+-----------------+------------
+
|        1000 | a320b137c219 | elarson  | Marketing       | East-170
|
|        1001 | b239c825d303 | bmoreno  | Marketing       | Central-276
|
|        1002 | c116d593e558 | tshah    | Human Resources | North-434
|
|        1003 | d394e816f943 | sgilmore | Finance         | South-153
|
|        1004 | e218f877g788 | eraab    | Human Resources | South-127
|
|        1005 | f551g340h864 | gesparza | Human Resources | South-366
|
|        1007 | h174i497j413 | wjaffrey | Finance         | North-406
```

Figure 12: Result: SQL query for employees not in IT

8 Summary

This investigation demonstrated the use of SQL for cybersecurity monitoring and response:

- Detected suspicious failed logins outside normal working hours.
- Identified login attempts on incident-related dates.
- Highlighted login activity from outside Mexico.
- Extracted employee details for targeted security updates.
- Ensured efficient exclusion of already-updated IT systems.

SQL is a powerful tool for incident investigation, log analysis, and enforcing security policies across enterprise environments.