Apply filters to SQL queries

Project description

My company is attempting to increase the security of their system. My responsibility is to ensure the security of the system, look into any potential security concerns, and upgrade employee computers as necessary. Examples of how I carried out security-related tasks using SQL and filters are shown in the steps that follow.

Retrieve after hours failed login attempts

After business hours (after 18:00), there was a possible security incident. All failed after-hours login attempts must be looked into.

The SQL query I made to look for failed login attempts that happened outside business hours is shown in the following code.

```
MariaDB [organization]> clear
MariaDB [organization]> SELECT *
    ->
    -> FROM log_in_attempts
    ->
    -> WHERE login_time > '18:00' AND success = FALSE;+----------+----------+------
-----+------------+---------+----------------+---------+
| event_id | username | login_date | login_time | country | ip_address      | succe
s |
+----------+----------+------------+------------+---------+-----------------+------
--+
|        2 | apatel   | 2022-05-10 | 20:27:27   | CAN     | 192.168.205.12  |
0 |
|       18 | pwashing | 2022-05-11 | 19:28:50   | US      | 192.168.66.142  |
0 |
|       20 | tshah    | 2022-05-12 | 18:56:36   | MEXICO  | 192.168.109.50  |
0 |
|       28 | aestrada | 2022-05-09 | 19:28:12   | MEXICO  | 192.168.27.57   |
0 |
|       34 | drosas   | 2022-05-11 | 21:02:04   | US      | 192.168.45.93   |
0 |
|       42 | cgriffin | 2022-05-09 | 23:04:05   | US      | 192.168.4.157   |
0 |
|       52 | cjackson | 2022-05-10 | 22:07:07   | CAN     | 192.168.58.57   |
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     | 192.168.84.194  |
0 |
```

The screenshot's first section is my query, while the second section is some of the results. This query searches for unsuccessful login attempts that took place after 18:00. I started by choosing every piece of information in the `log_in_attempts` table. Then, I filtered my findings to output only login attempts that took place after 18:00 and failed using a `WHERE` clause and an `AND` operator. The first restriction, `login_time > '18:00'`, excludes login attempts made after that time. The second criterion, `success = FALSE`, excludes out unsuccessful login attempts.

Retrieve login attempts on specific dates

On 2022-05-09, a suspicious occurrence took place. It is necessary to look into any login activity that took place on 2022-05-09 or the day prior.

The code that follows shows how I built a SQL query to search for login attempts that took place on particular dates.

```
MariaDB [organization]> SELECT *
    ->
    -> FROM log_in_attempts
    ->
    -> WHERE login_date = '2022-05-09' OR login_date = '2022-05-08';
+----------+----------+------------+------------+---------+----------------+-------
--+
| event_id | username | login_date | login_time | country | ip_address     | succes
s |
+----------+----------+------------+------------+---------+----------------+-------
--+
|        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      | 192.168.33.137  |
1 |
|       26 | apatel   | 2022-05-08 | 17:27:00   | CANADA  | 192.168.123.105 |
1 |
|       28 | aestrada | 2022-05-09 | 19:28:12   | MEXICO  | 192.168.27.57   |
0 |
|       30 | yappiah  | 2022-05-09 | 03:22:22   | MEX     | 192.168.124.48  |
```

My query is shown in the first part of the screenshot, and some of the output is shown in the second. This search finds all attempts to log in that took place on either 2022-05-09 or 2022-05-08. I began by choosing all of the information from the `log_in_attempts` table. Then, I filtered my findings using a `WHERE` clause and an `OR` operator to only show login attempts that happened on either 2022-05-09 or 2022-05-08. Logins made on or after 2022-05-09 are excluded by the first criterion, `login_date = '2022-05-09'`. With the second condition, which reads "`login_date = '2022-05-08'`," only logins made on May 8, 2022 are considered.

Retrieve login attempts outside of Mexico

I think there is a problem with the login attempts that took place outside of Mexico after looking into the company's data on login attempts. These login attempts need to be looked into.

The SQL query I made to look for login attempts outside of Mexico is shown in the following code.

```
MariaDB [organization]> SELECT *
    ->
    -> FROM log_in_attempts
    ->
    -> WHERE NOT country LIKE 'MEX%';
+----------+----------+------------+------------+---------+----------------+-------
--+
| event_id | username | login_date | login_time | country | ip_address     | succes
s |
+----------+----------+------------+------------+---------+----------------+-------
--+
|        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  | 192.168.86.232  |
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     | 192.168.246.135 |
1 |
```

My query is shown in the first part of the screenshot, and some of the output is shown in the second. This search retrieves all attempts at login made outside of Mexico. I began by choosing all of the information from the `log_in_attempts` table. I then applied a `WHERE` clause with a `NOT` to exclude all nations besides Mexico. Because the dataset refers to Mexico as `MEX` and `MEXICO`, I used `LIKE` with `MEX%` as the pattern to match. When combined with `LIKE`, the percentage symbol (`%`) stands in for any amount of arbitrary characters.

Retrieve employees in Marketing

A few Marketing department employees' PCs need to be updated, according to my team. I need to find out which employee machines need updating in order to achieve this.
The code that follows shows how I built a SQL query to search for employee computers from staff members in the East building's Marketing department.

```
MariaDB [organization]> SELECT *
    ->
    -> FROM employees;
+-------------+-------------+----------+-----------------------+-------------+
| 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   |
|        1006 | g329h357i597 | alevitsk | Information Technology | East-320    |
|        1007 | h174i497j413 | wjaffrey | Finance               | North-406   |
|        1008 | i858j583k571 | abernard | Finance               | South-170   |
|        1009 | NULL         | lrodriqu | Sales                 | South-134   |
|        1010 | k2421212m542 | jlansky  | Finance               | South-109   |
|        1011 | l748m120n401 | drosas   | Sales                 | South-292   |
|        1012 | m756n668o146 | nmason   | Information Technology | North-160   |
|        1013 | n205o559p243 | zbernal  | Information Technology | South-229   |
|        1014 | NULL         | asundara | Information Technology | West-219    |
|        1015 | p611q262r945 | jsoto    | Finance               | North-271   |
|        1016 | q793r736s288 | sbaelish | Human Resources       | North-229   |
|        1017 | r550s824t230 | jclark   | Finance               | North-188   |
|        1018 | s310t540u653 | abellmas | Finance               | North-403   |
|        1019 | t815u205v470 | mcouliba | Information Technology | North-108   |
|        1020 | u899v381w363 | arutley  | Marketing             | South-351   |
|        1021 | v200w121x977 | smartell | Information Technology | South-138   |
|        1022 | w237x430y567 | arusso   | Finance               | West-465    |
|        1023 | x253y759z103 | aalonso  | Information Technology | West-393    |
|        1024 | y976z753a267 | iuduike  | Sales                 | South-215   |
|        1025 | z381a365b233 | jhill    | Sales                 | North-115   |
|        1026 | a998b568c863 | apatel   | Human Resources       | West-320    |
```

My query is shown in the first part of the screenshot, and some of the output is shown in the second. This search produces a list of every worker in the East building's Marketing division. I began by choosing all of the information from the `employees` table. Then, to find workers who are employed by the Marketing division and the East building, I utilized a `WHERE` clause with an `AND`. Because the information in the `office` column refers to the East building with the given office number, I used `LIKE` with `East%` as the pattern to match. The first filter for personnel in the Marketing department is the component of the condition that reads `department =`

'Marketing'. The office LIKE 'East%' component of the second condition filters for workers in the East building.

Retrieve employees in Finance or Sales

Additionally, the equipment used by staff members in the sales and finance divisions needs to be upgraded. I can only receive personnel data from these two departments because I need a different security update.

The code that follows shows how I built a SQL query to look for employee machines from workers in the sales or finance divisions.

```
MariaDB [organization]> SELECT *
    ->
    -> FROM employees
    ->
    -> WHERE department = 'Finance' OR department = 'Sales';
+-------------+--------------+----------+------------+-------------+
| 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 | k2421212m542 | jlansky  | Finance    | South-109   |
|        1011 | 1748m120n401 | 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 | j236k3031245 | 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    |
|        1046 | u429v921w138 | daquino  | Finance    | West-280    |
|        1047 | v109w587x644 | cward    | Finance    | West-373    |
|        1048 | w167x592y375 | tmitchel | Finance    | South-288   |
|        1049 | NULL         | jreckley | Finance    | Central-295 |
|        1050 | y132z930a114 | csimmons | Finance    | North-468   |
|        1057 | f370g535h632 | mscott   | Sales      | South-270   |
|        1062 | k3671639m697 | redwards | Finance    | North-180   |
```

My query is shown in the first part of the screenshot, and some of the output is shown in the second. All personnel in the sales and finance departments are returned by this query. I began by choosing all of the information from the employees table. I then used an OR and a WHERE clause to select for workers in the finance and sales divisions. Because I wanted every employee in either department, I utilized the OR operator rather than the AND operator. Employees from the Finance department are filtered according to the first condition, department = 'Finance'. Furthermore, department = 'Sales' in the second criteria excludes personnel from the Sales department.

Retrieve all employees not in IT

My group still needs to change the security settings for those who work outside the information technology division. I must first gather information on these employees before I can make the upgrade.

The example below shows how I built a SQL query to look for employee computers from people who weren't in the IT department.

```
MariaDB [organization]> SELECT *
    ->
    -> FROM employees
    ->
    -> WHERE NOT department = 'Information Technology';
+-------------+-------------+----------+-----------------+-------------+
| 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   |
|        1008 | i858j583k571 | abernard | Finance         | South-170   |
|        1009 | NULL         | lrodriqu | Sales           | South-134   |
|        1010 | k2421212m542 | jlansky  | Finance         | South-109   |
|        1011 | l748m120n401 | drosas   | Sales           | South-292   |
|        1015 | p611q262r945 | jsoto    | Finance         | North-271   |
|        1016 | q793r736s288 | sbaelish | Human Resources | North-229   |
|        1017 | r550s824t230 | jclark   | Finance         | North-188   |
|        1018 | s310t540u653 | abellmas | Finance         | North-403   |
|        1020 | u899v381w363 | arutley  | Marketing       | South-351   |
|        1022 | w237x430y567 | arusso   | Finance         | West-465    |
|        1024 | y976z753a267 | iuduike  | Sales           | South-215   |
|        1025 | z381a365b233 | jhill    | Sales           | North-115   |
|        1026 | a998b568c863 | apatel   | Human Resources | West-320    |
|        1027 | b806c503d354 | mrah     | Marketing       | West-246    |
|        1028 | c603d749e374 | aestrada | Human Resources | West-121    |
|        1029 | d336e475f676 | ivelasco | Finance         | East-156    |
|        1030 | e391f189g913 | mabadi   | Marketing       | West-375    |
|        1031 | f419g188h578 | dkot     | Marketing       | West-408    |
```

My query is shown in the first part of the screenshot, and some of the output is shown in the second. All employees who are not in the information technology department are returned by the query. I began by choosing all of the information from the `employees` table. Then, to filter out workers who weren't in this department, I used a `WHERE` clause with `NOT`.

Summary

To obtain detailed information on login attempts and employee workstations, I used filters to SQL queries. Employees and `log_in_attempts` are the two tables I used. I filtered for the precise data required for each task using the `AND`, `OR`, and `NOT` operators. In order to search for trends, I also used `LIKE` and the wildcard percentage sign (`%`).