Apply filters to SQL queries

Project description

This project required me to query an organization's DB, filtering through data and applying SQL concepts and syntax in a cyber-security setting.

Retrieve after-hours failed login attempts

← Activity: Filter with AND, OR, and NOT

```
clear
MariaDB [organization]> SELECT *
   -> FROM log in attempts
      WHERE login time > '18:00' AND success = '0';
 event id | username | login date | login time | country | ip address
 uccess
                     2022-05-10 | 20:27:27
                                                         192.168.205.12
            apatel
                                                 CAN
     0
            pwashing | 2022-05-11 | 19:28:50
                                                 US
                                                         192.168.66.142
     0
                     2022-05-12 18:56:36
                                                 MEXICO
                                                         192.168.109.50
            tshah
       20
     0
                       2022-05-09 | 19:28:12
                                                         192.168.27.57
                                                 MEXICO
       28
            aestrada
                     2022-05-11 | 21:02:04
                                                 US
                                                         192.168.45.93
       34
            drosas
     0
       42
            cgriffin | 2022-05-09 | 23:04:05
                                               US
                                                         192.168.4.157
     0
                       2022-05-10 | 22:07:07
                                                 CAN
                                                          192.168.58.57
       52
            cjackson
     0
            wjaffrey 2022-05-11 19:55:15
                                                          192.168.100.17
       69
                                                 USA
     0
            abernard | 2022-05-12 | 23:38:46
                                                 MEX
                                                          192.168.234.49
       82
     0
            apatel
                     2022-05-08 | 22:38:31
                                                 CANADA
                                                         192.168.132.153
       87
            ivelasco | 2022-05-09 | 22:36:36
                                                          192.168.84.194
                                                 CAN
            asundara | 2022-05-11 | 18:38:07
                                                 US
                                                          192.168.96.200
            bisles
                       2022-05-12 | 20:25:57
                                                 USA
                                                           192.168.116.187
      107
```

Retrieve login attempts on specific dates

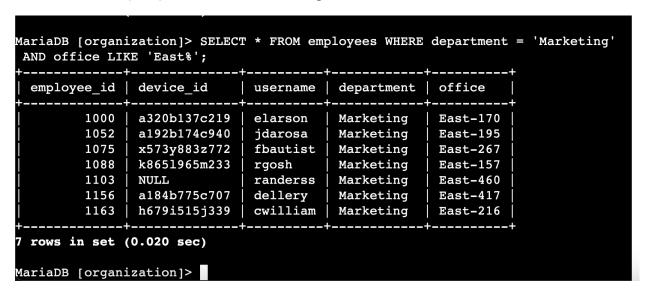
← Activity: Filter with AND, OR, and NOT

```
19 rows in set (0.032 sec)
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
success
                     2022-05-09 | 04:56:27
                                                         | 192.168.243.140 |
            jrafael
                                               CAN
                     2022-05-09 | 06:47:41
                                                         | 192.168.151.162 |
            dkot
                                                USA
                     2022-05-08 | 02:00:39
                                                         | 192.168.178.71 |
            dkot
                                                 USA
                     2022-05-08 | 01:30:17
                                                US
                                                         | 192.168.119.173 |
            bisles
     0
                     2022-05-08 | 09:11:34
                                                         192.168.100.158
            dkot
                                                 USA
       12
           | lyamamot | 2022-05-09 | 17:17:26
                                                         | 192.168.183.51 |
                                               USA
       15
     0
                     2022-05-09 | 06:49:39
                                                         | 192.168.171.192 |
            arusso
                                               MEXICO
       24
            sbaelish | 2022-05-09 | 07:04:02
                                               US
                                                         192.168.33.137
       25
                     2022-05-08 | 17:27:00
                                               CANADA
                                                         | 192.168.123.105 |
           apatel
       26
       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
```

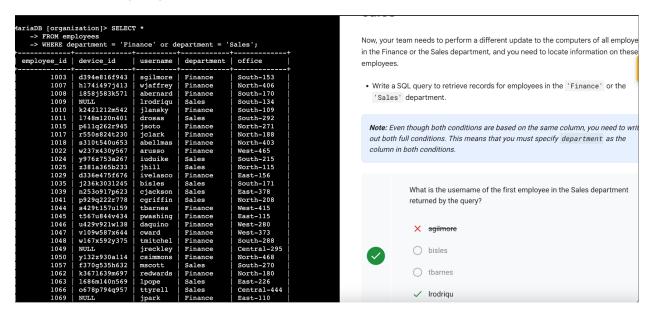
Retrieve login attempts outside of Mexico

```
MariaDB [organization]> SELECT *
   -> FROM log in attempts
   -> WHERE NOT country LIKE 'MEX%';
 event_id | username | login_date | login_time | country | ip_address
success
                     2022-05-09 | 04:56:27
                                              CAN
                                                       192.168.243.140
        1 | jrafael
            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
                                                       192.168.178.71
            dkot
                      2022-05-08 | 02:00:39
                                               USA
     0
                     2022-05-11 | 03:05:59
                                                       192.168.86.232
          jrafael
                                              CANADA
     0
                     2022-05-11 | 01:45:14
                                               CAN
                                                       192.168.170.243
            eraab
     1
            bisles
                     2022-05-08 | 01:30:17
                                               US
                                                       192.168.119.173
     0
                      2022-05-12 | 09:33:19
                                               CANADA
                                                       192.168.228.221
          jrafael
     0
          | sgilmore | 2022-05-11 | 10:16:29
                                                       192.168.140.81
                                              CANADA
     0
                      2022-05-08 | 09:11:34
                                               USA
                                                       192.168.100.158
       12
            dkot
                     2022-05-11 | 09:29:34
                                               USA
                                                       | 192.168.246.135 |
            mrah
```

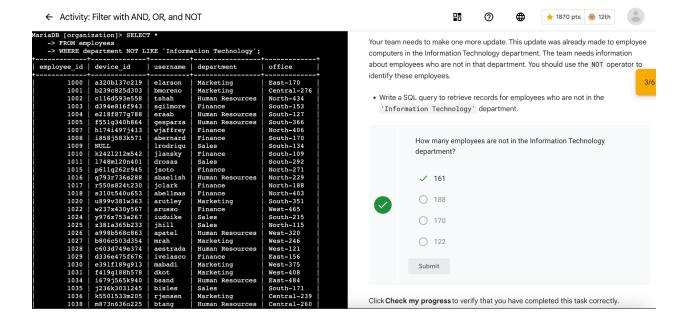
Retrieve employees in Marketing



Retrieve employees in Finance or Sales



Retrieve all employees not in IT



Summary

As part of a security investigation and system update task, the objective was to extract specific employee-related information, machine data, and departmental details from the database. The process involved filtering data based on several criteria. First, identifying failed login attempts after business hours; second, retrieving login attempts on specified dates; third, obtaining logins not originating in Mexico; fourth, gathering details of employees in the Marketing department; fifth, acquiring information on employees within Finance or Sales departments. Lastly, retrieving data on employees not belonging to the Information Technology department was also part of the task.