Análise de Consultas SQL para Investigação de Segurança

Descrição do Projeto

Neste projeto, explorei a aplicação de consultas SQL para investigar potenciais incidentes de segurança em um ambiente corporativo simulado. Através da análise de dados de tentativas de login e informações de funcionários, demonstrei a capacidade de filtrar e extrair informações cruciais para a identificação de atividades suspeitas e a manutenção da segurança do sistema. O foco principal foi a utilização de operadores lógicos (AND, OR, NOT) e a cláusula LIKE para refinar as buscas em grandes conjuntos de dados, simulando cenários reais de cibersegurança.

Consulta de tentativas de login com falha após o expediente

Para investigar um possível incidente de segurança que ocorreu após o horário comercial, foi necessário identificar todas as tentativas de login com falha que aconteceram depois das 18:00. A consulta SQL utilizada para este propósito filtrou a tabela `log_in_attempts` com base na coluna `login_time` (maior que '18:00') e na coluna `success` (igual a `false` ou `0`).

```
SELECT *
FROM log_in_attempts
WHERE login_time > '18:00' AND success = FALSE;
```

```
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     | success |
+----------+----------+------------+------------+---------+----------------+---------+
|        2 | apatel   | 2022-05-10 | 20:27:27   | CAN     | 192.168.205.12 |       0 |
|       18 | pwashing | 2022-05-11 | 19:28:50   | US      | 192.168.66.142 |       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 |
|      104 | asundara | 2022-05-11 | 18:38:07   | US      | 192.168.96.200 |       0 |
|      107 | bisles   | 2022-05-12 | 20:25:57   | USA     | 192.168.116.187|       0 |
|      111 | aestrada | 2022-05-10 | 22:00:26   | MEXICO  | 192.168.76.27  |       0 |
|      127 | abellmas | 2022-05-09 | 21:20:51   | CANADA  | 192.168.70.122 |       0 |
|      131 | bisles   | 2022-05-09 | 20:03:55   | US      | 192.168.113.171|       0 |
|      155 | cgriffin | 2022-05-12 | 22:18:42   | USA     | 192.168.236.176|       0 |
|      160 | jclark   | 2022-05-10 | 20:49:00   | CANADA  | 192.168.214.49 |       0 |
|      199 | yappiah  | 2022-05-11 | 19:34:48   | MEXICO  | 192.168.44.232 |       0 |
+----------+----------+------------+------------+---------+----------------+---------+
19 rows in set (0.001 sec)
```

Consulta de tentativas de login em datas específicas

Para investigar um evento suspeito ocorrido em 2022-05-09, foi necessário analisar todas as tentativas de login que aconteceram nesse dia e no dia anterior. A consulta SQL utilizada filtrou a tabela `log_in_attempts` para incluir registros onde a `login_date` fosse '2022-05-09' ou '2022-05-08'.

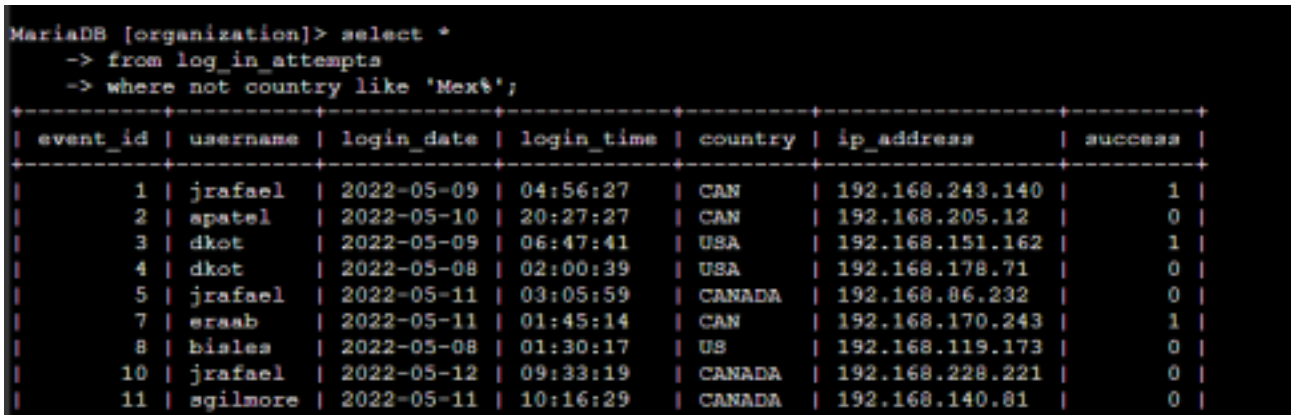
```sql
SELECT *
FROM log_in_attempts
WHERE login_date = '2022-05-09' OR login_date = '2022-05-08';
```

```
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 |
+----------+----------+------------+------------+---------+----------------+---------+
|        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 |       1 |
|       32 | acook    | 2022-05-09 | 02:52:02   | CANADA  | 192.168.142.239|       0 |
|       36 | asundara | 2022-05-08 | 09:00:42   | US      | 192.168.78.151 |       1 |
```

Consulta de tentativas de login fora do México

Houve atividade suspeita com tentativas de login, mas a equipe determinou que essa atividade não se originou no México. Para investigar as tentativas de login que ocorreram fora do México, a seguinte consulta SQL foi utilizada. Ela emprega o operador `NOT LIKE` para excluir registros onde o campo `country` começa com 'Mex' (abrangendo 'MEX' e 'MEXICO').

```
SELECT *
FROM log_in_attempts
WHERE NOT country LIKE 'Mex%';
```



```
MariaDB [organization]> select *
    -> from log_in_attempts
    -> where not country like 'Mex%';
+----------+----------+------------+------------+---------+-----------------+---------+
| 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  | 192.168.86.232  |       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 |
```

Consultas de funcionários em Marketing

Para realizar atualizações de segurança em máquinas específicas de funcionários do departamento de Marketing, foi necessário obter informações sobre esses funcionários. A consulta SQL abaixo filtrou a tabela `employees` para identificar todos os funcionários do departamento de Marketing em todos os escritórios do edifício East. O operador `LIKE` foi usado para o campo `office` para incluir todos os escritórios que começam com 'East-'.

```
SELECT *
FROM employees
WHERE department LIKE 'Marketing' AND office LIKE 'East-%';
```

```
MariaDB [organization]> select *
    -> from employees
    -> where department like 'Marketing' and office like 'East-%';
+-------------+-------------+----------+------------+----------+
| 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 (0.002 sec)
```

Consultas de funcionários em Finanças ou Vendas

Para uma atualização de segurança diferente, foi necessário identificar funcionários dos departamentos de Vendas ou Finanças. A consulta SQL a seguir utilizou o operador `OR` para selecionar registros da tabela `employees` onde o `department` é 'Finance' ou 'Sales'.

```sql
SELECT *
FROM employees
WHERE department LIKE 'Finance' OR department LIKE 'Sales';
```

```
MariaDB [organization]> select *
    -> from employees
    -> where department like 'Finance' or department like '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 | 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   |
```

Consulta de todos os funcionários que não estão na TI

Para uma atualização de segurança que não se aplicava ao departamento de Tecnologia da Informação, foi necessário identificar todos os funcionários que não estavam na TI. A consulta SQL abaixo utilizou o operador `NOT LIKE` para excluir funcionários do departamento de 'Information Technology' da tabela `employees`.

```
SELECT *
FROM employees
WHERE NOT department LIKE 'Information Technology';
```

```
MariaDB [organization]> select *
    -> from employees
    -> where not department like '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   |
```

Resumo

Este projeto demonstrou a aplicação prática de consultas SQL para fins de cibersegurança, especificamente na investigação de incidentes e na gestão de dados de funcionários. As consultas desenvolvidas abordaram cenários comuns, como a identificação de tentativas de login suspeitas e a segmentação de funcionários para atualizações de segurança. A utilização eficaz de operadores como AND, OR, NOT e LIKE é fundamental para a análise de grandes volumes de dados e para a tomada de decisões informadas em segurança da informação.