Apply filters to SQL queries

Project description

In this project, I used SQL queries to simulate an analyst on a cyber security team who recently discovered some potential security issues that involve login attempts and employee machines. I used SQL queries to examine the data of employees and their log in attempts to discover the potential security vulnerabilities.

Retrieve after hours failed login attempts

```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE login_time > '18:00' AND success = 0;
```

After discovering that there was a potential security incident that occured after business hours (18:00). I used SQL to query the log_in_attempts table to identify all failed login attempts that occurred after 18:00 and where the success was False which is represented by 0 here (where 1 is True). The query yielded this table :

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 (0.097 sec)
```

Retrieve login attempts on specific dates

There was a suspicious event that occurred on 2022-05-09. To investigate it, I looked at activity that happened on 2022-05-09 or on the day prior to it.

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

Here I used the OR operator to show the login attempts done on both days. I created a SQL query to filter out the dates.

Retrieve login attempts outside of Mexico

After looking at the data on login attempts,it is believed that there is an issue with the login attempts that occurred outside of Mexico. To investigate these login attempts, I will create a SQL query that filters out Mexico from the table.

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

My input shows that I used the NOT operator to filter out countries that do not start with MEX since the dataset can represent it as MEX or MEXICO. This is the output.

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

Retrieve employees in Marketing and in East Building

The team wants to update certain computers for employees in Marketing department. They are located in East building. I created a SQL query with the following input to filter it out.

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

I filtered it out by department and I used the LIKE with East% as the pattern to match any office that

starts with East. This was the output :

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

Summary

In this project, I applied filets for SQL queries using operators like AND, OR, NOT as well as LIKE and the % wildcard to be specific with my filter. The SQL queries helped me get specific information on login attempts and employee machines.