Using SQL Filters to retrieve records

Employees Login Attempts

Project description

As a Security Analyst at a large organization, I was responsible for identifying and investigating suspicious login activity within the company's internal systems. This project involved analyzing data from the organization's `employees` and `log_in_attempts` tables using SQL queries to detect potential security threats.
Here i will be using the SQL operators `AND`, `OR`, `NOT`, `WHERE`, `LIKE`

Retrieve, after hours of failed login attempts

So I am investigating a failed login attempts after business hours, office hour ends at '18:00', I used these queries below:

```
SELECT *
FROM log_in_attempts
WHERE login_time > '18:00' AND success = 0;
```

and i got the output:

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

which indicates that there were 19 failed login attempts after 18:00

Retrieve login attempts on specific dates

Am retrieving all login attempts on ‘2022-05-09’ and ‘2022-05-08, so I will be using my “OR” operator. So I used these queries below:

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

and my output indicates this:

username	login_date	login_time
jrafael	2022-05-09	04:56:27
apatel	2022-05-10	20:27:27
dkot	2022-05-09	06:47:41
dkot	2022-05-08	02:00:39
jrafael	2022-05-11	03:05:59
arutley	2022-05-12	17:00:59
eraab	2022-05-11	01:45:14
bisles	2022-05-08	01:30:17
yappiah	2022-05-11	13:47:29
jrafael	2022-05-12	09:33:19
sgilmore	2022-05-11	10:16:29
dkot	2022-05-08	09:11:34
mrah	2022-05-11	09:29:34
sbaelish	2022-05-10	10:20:18
lyamamot	2022-05-09	17:17:26
mcouliba	2022-05-11	06:44:22
pwashing	2022-05-11	02:33:02
pwashing	2022-05-11	19:28:50
jhill	2022-05-12	13:09:04
tshah	2022-05-12	18:56:36
iuduike	2022-05-11	17:50:00
rjensen	2022-05-11	00:59:26
yappiah	2022-05-10	18:11:53
arusso	2022-05-09	06:49:39
sbaelish	2022-05-09	07:04:02
apatel	2022-05-08	17:27:00
aalonso	2022-05-10	01:55:35
aestrada	2022-05-09	19:28:12
bisles	2022-05-11	01:21:22
yappiah	2022-05-09	03:22:22
acook	2022-05-12	17:36:45
acook	2022-05-09	02:52:02
zbernal	2022-05-11	02:52:10
drosas	2022-05-11	21:02:04
tshah	2022-05-10	15:26:08

Retrieve login attempts outside of Mexico

Here I am retrieving login attempts that did not originate from Mexico. In this query, I used the ‘LIKE’, ‘NOT’ and %, I used the % symbol here because it acts as a wildcard character and it will NOT return countries that start with MEX (‘MEX%’). So the queries I used were:

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

and the output that came out were

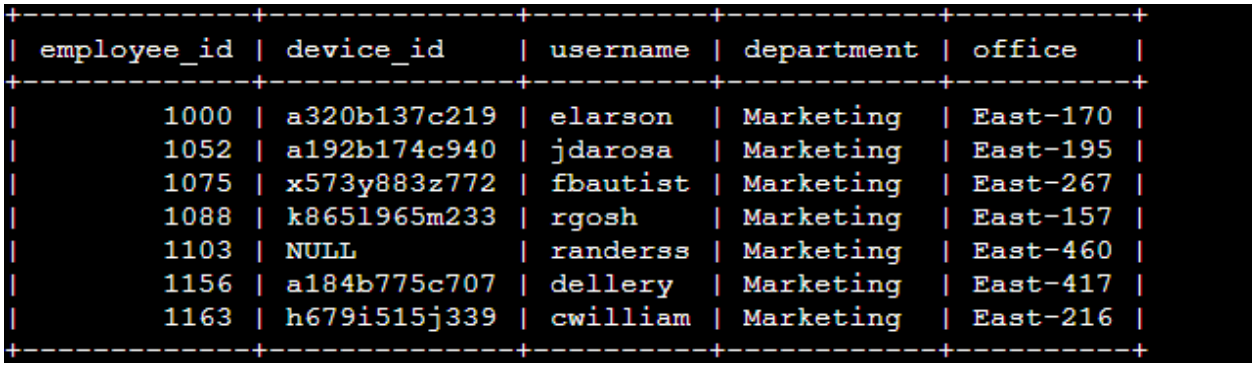
event_id	username	login_date	login_time	country	ip_address	success
1	jrafael	2022-05-09	04:56:27	CAN	192.168.243.140	1
2	apatel	2022-05-10	20:27:27	CAN	192.168.205.12	0
3	dkot	2022-05-09	06:47:41	USA	192.168.151.162	1
4	dkot	2022-05-08	02:00:39	USA	192.168.178.71	0
5	jrafael	2022-05-11	03:05:59	CANADA	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
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
14	sbaelish	2022-05-10	10:20:18	US	192.168.16.99	1
15	lyamamot	2022-05-09	17:17:26	USA	192.168.183.51	0
16	mcouliba	2022-05-11	06:44:22	CAN	192.168.172.189	1
17	pwashing	2022-05-11	02:33:02	USA	192.168.81.89	1
18	pwashing	2022-05-11	19:28:50	US	192.168.66.142	0
19	jhill	2022-05-12	13:09:04	US	192.168.142.245	1
21	iuduike	2022-05-11	17:50:00	US	192.168.131.147	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
29	bisles	2022-05-11	01:21:22	US	192.168.85.186	0
31	acook	2022-05-12	17:36:45	CANADA	192.168.58.232	0
32	acook	2022-05-09	02:52:02	CANADA	192.168.142.239	0
33	zbernal	2022-05-11	02:52:10	US	192.168.72.59	1
34	drosas	2022-05-11	21:02:04	US	192.168.45.93	0
36	asundara	2022-05-08	09:00:42	US	192.168.78.151	1
37	eraab	2022-05-10	06:03:41	CANADA	192.168.152.148	0
38	sbaelish	2022-05-09	14:40:01	USA	192.168.60.42	1
41	apatel	2022-05-10	17:39:42	CANADA	192.168.46.207	0
42	cgriffin	2022-05-09	23:04:05	US	192.168.4.157	0
43	mcouliba	2022-05-08	02:35:34	CANADA	192.168.16.208	0
44	daquino	2022-05-08	07:02:35	CANADA	192.168.168.144	0
45	dtanaka	2022-05-11	10:28:54	US	192.168.223.157	1
46	eraab	2022-05-11	11:29:27	CAN	192.168.24.12	0
47	dkot	2022-05-08	05:06:45	US	192.168.233.24	1
48	asundara	2022-05-11	03:18:45	USA	192.168.72.10	1

Retrieve employees in Marketing

I want to retrieve employees information in marketing department in the office East 170 and 320, so I will run a SQL query, I created a query using the operator “AND”, “LIKE” and % to get the information for employees in marketing department,
So I used these queries below:

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

and the output gave me this :



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

which indicates that there were 7 offices in the East 170 - 320

Retrieve employees in Finance or Sales

I want to perform an update in this department (sales and finance), which I need to retrieve the record of the employees in this department, so I used the operator `OR`, So the queries I used were:

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

I got the output below:

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
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
1063	l686m140n569	lpope	Sales	East-226

Retrieve all employees not in IT

I want to retrieve employees information who are not in the Information Technology (IT) Department, so I used the operator ‘NOT which I used these queries:

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

and the output gave me:

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
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
1063	l686m140n569	lpope	Sales	East-226
1066	o678p794q957	ttyrell	Sales	Central-444
1069	NULL	jpark	Finance	East-110

Summary

As a Security Analyst in a large organization, I conducted an investigation into potential security threats by analyzing login activity and employee data. This involved querying and filtering information from the `employees` and `log_in_attempts` tables using SQL.

Using SQL logical operators such as `AND`, `OR`, and `NOT`, I performed a series of targeted queries to uncover patterns and anomalies. Key tasks included:

- Retrieving **failed login attempts outside business hours**, which may indicate unauthorized access.
- Extracting **login attempts on specific dates** to support incident tracking.
- Identifying **login activity outside of Mexico**, pointing to potential location-based threats.

- Filtering **employees in the Marketing department** to narrow down internal access investigations.
- Isolating **employees in Finance and Sales**, while excluding those in IT, to focus on departments most at risk.