

Apply filters to SQL queries

Project description

As a security professional at a large organization, we are investigating security issues to help keep the system secure. Recently, some potential security issues have been discovered involving login attempts and employee machines. We will be examining the organization's data in their **employees** and **log_in_attempts** table using SQL filters to retrieve records from different datasets and investigate the potential security issues.

Retrieve after hours failed login attempts

There has been a potential security incident that occurred after business hours. To investigate this, we are querying the **log_in_attempts** table and reviewing after hours login activity. We will be creating a query that identifies all failed login attempts that occurred after 18:00.

We will be using `SELECT * FROM log_in_attempts WHERE login_time > '18:00'` and `success = 0`. We will be selecting all rows from the **log_in_attempts** table where **login_time** is bigger than 18:00 and where **success** is 0 which means log in did not succeed.

```
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 | 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 (0.002 sec)
```

Retrieve login attempts on specific dates

A suspicious event occurred on 2022-05-09. To investigate this event, we are reviewing all login attempts that occurred on that day and the day before.

We will be using `SELECT * FROM log_in_attempts WHERE login_date = '2022-05-09' OR login_date = '2022-05-08';`. We will be selecting all rows from the `log_in_attempts` table where `login_date` equals to 2022-05-09 or `login_date` equals to 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	2022-05-09	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	1
24	arusso	2022-05-09	06:49:39	MEXICO	192.168.171.192	1
25	sbeelish	2022-05-09	07:04:02	US	192.168.33.137	1
26	spatel	2022-05-08	17:27:05	CANADA	192.168.123.105	1
28	aestrada	2022-05-09	19:11:12	MEXICO	192.168.27.51	0
30	yappiiah	2022-05-09	01:22:22	MEX	192.168.142.148	1
32	accook	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
38	sbeelish	2022-05-09	14:40:01	USA	192.168.60.42	1
39	yappiiah	2022-05-09	07:56:40	MEXICO	192.168.57.115	1
42	cgriffin	2022-05-09	23:04:05	US	192.168.4.157	0
43	mcoulib	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
47	dkot	2022-05-08	05:06:45	US	192.168.233.24	1
49	asundara	2022-05-08	14:00:01	US	192.168.173.213	0
53	nmason	2022-05-08	11:51:38	CAN	192.168.133.188	1
56	acock	2022-05-08	04:16:30	CAN	192.168.209.130	1
58	ivelasco	2022-05-09	17:20:54	CAN	192.168.57.162	0
61	dtanaka	2022-05-09	09:45:18	USA	192.168.98.221	1
65	aalonso	2022-05-09	23:42:12	MEX	192.168.52.37	1
66	aestrada	2022-05-08	21:58:32	MEX	192.168.67.223	1
67	abernard	2022-05-09	11:53:41	MEX	192.168.118.29	1
68	mrah	2022-05-08	17:16:13	US	192.168.42.248	1
70	tmitchel	2022-05-09	10:55:17	MEXICO	192.168.87.199	1
71	mcoulib	2022-05-09	06:57:42	CAN	192.168.55.169	0
72	alevitisk	2022-05-08	12:09:10	CANADA	192.168.139.176	1
79	abernard	2022-05-09	11:41:57	MEX	192.168.158.170	0
80	cjackson	2022-05-08	06:39:10	CANADA	192.168.33.140	1
81	lrodrigu	2022-05-09	06:10:23	USA	192.168.26.165	1
87	spatel	2022-05-08	22:38:31	CANADA	192.168.132.153	0
90	gesparza	2022-05-09	00:49:05	CANADA	192.168.87.201	0
92	pwashing	2022-05-08	00:36:12	US	192.168.247.219	0
96	ivelasco	2022-05-09	22:36:36	CAN	192.168.84.194	0
90	gesparza	2022-05-09	00:49:05	CANADA	192.168.87.201	0
92	pwashing	2022-05-08	00:36:12	US	192.168.247.219	0
96	ivelasco	2022-05-09	22:36:36	CAN	192.168.84.194	0
97	jreckley	2022-05-09	02:49:23	MEXICO	192.168.32.231	1
101	sbeelish	2022-05-08	12:01:22	US	192.168.145.158	0
102	jreckley	2022-05-09	16:51:44	MEX	192.168.108.13	1
108	daquino	2022-05-09	21:30:48	CANADA	192.168.15.110	1
110	mabadi	2022-05-09	00:01:54	USA	192.168.90.124	1
112	rjensen	2022-05-09	09:22:05	MEX	192.168.69.116	1
117	bsand	2022-05-08	00:19:11	USA	192.168.197.187	0
120	tmitchel	2022-05-09	02:58:17	MEXICO	192.168.134.62	0
127	abelimas	2022-05-09	21:20:51	CANADA	192.168.70.122	0
128	jclark	2022-05-09	10:45:59	CANADA	192.168.122.169	0
131	bisles	2022-05-09	20:03:55	US	192.168.113.171	0
134	ludurike	2022-05-09	06:46:40	USA	192.168.22.115	1
135	bsand	2022-05-09	14:06:33	US	192.168.91.238	0
144	daquino	2022-05-09	11:09:32	CANADA	192.168.139.9	0
145	ivelasco	2022-05-08	09:06:102	CANADA	192.168.39.196	1
147	yappiiah	2022-05-08	06:04:134	MEX	192.168.65.245	0
148	daquino	2022-05-08	06:15:55	CANADA	192.168.135.6	1
150	nmason	2022-05-08	14:40:02	CAN	192.168.204.124	0
151	mabadi	2022-05-09	16:29:46	USA	192.168.30.225	1
158	smartell	2022-05-09	19:30:32	MEXICO	192.168.190.178	1
161	abelimas	2022-05-09	13:25:50	CAN	192.168.180.205	0
162	yappiiah	2022-05-09	04:51:22	MEXICO	192.168.162.100	0
163	tmitchel	2022-05-08	09:21:16	MEX	192.168.119.29	0
165	jreckley	2022-05-08	15:28:43	MEXICO	192.168.34.193	0
168	jlansky	2022-05-08	13:25:42	USA	192.168.210.94	1
169	alevitisk	2022-05-08	08:10:43	CANADA	192.168.210.228	0
170	sbeelish	2022-05-09	16:43:18	USA	192.168.65.113	0
172	mabadi	2022-05-08	08:06:50	US	192.168.180.41	1
178	sgilmore	2022-05-08	12:27:22	CAN	192.168.52.216	0
184	alevitisk	2022-05-08	03:09:48	CAN	192.168.33.70	0
186	bisles	2022-05-09	04:29:17	USA	192.168.40.72	0
187	arusso	2022-05-09	00:36:26	MEX	192.168.77.137	0
189	nmason	2022-05-08	05:37:24	CANADA	192.168.168.117	1
190	jsoto	2022-05-09	05:09:21	USA	192.168.25.60	0
191	cjackson	2022-05-08	06:46:07	CANADA	192.168.7.187	0
193	lrodrigu	2022-05-08	07:11:29	US	192.168.125.240	0
197	jsoto	2022-05-08	09:05:09	US	192.168.36.21	0

75 rows in set (0.002 sec)

Retrieve login attempts outside of Mexico

There has been suspicious activity with login attempts, but the team has determined that this activity didn't originate in Mexico. We will be investigating login attempts that occurred outside of Mexico.

We will be using `SELECT * FROM log_in_attempts WHERE NOT country LIKE 'MEX%';`. We will be selecting all rows from the `log_in_attempts` table where the `country` column does not contain values of both `MEX` and `MEXICO`. So, we used `'MEX%'` and which is used with the `LIKE` function with the `WHERE` function.

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	0			
4	dkot	2022-05-09	02:00:39	USA	192.168.178.71	0			
5	jrafael	2022-05-11	03:05:59	CANADA	192.168.86.232	0			
7	erab	2022-05-11	01:45:14	CAN	192.168.170.243	1			
8	erab	2022-05-11	01:45:14	US	192.168.170.243	0			
10	jrafael	2022-05-12	09:33:19	CANADA	192.168.220.221	0			
11	sgilmore	2022-05-11	10:16:29	CANADA	192.168.140.81	0			
12	dkot	2022-05-09	09:11:34	USA	192.168.100.158	1			
13	mrah	2022-05-11	09:29:34	USA	192.168.246.135	1			
14	shaelish	2022-05-10	10:20:18	US	192.168.16.99	1			
15	lynnamot	2022-05-11	01:21:51	US	192.168.172.151	0			
16	louiehui	2022-05-11	06:44:22	CAN	192.168.172.189	1			
17	pawashing	2022-05-11	02:13:30	USA	192.168.81.89	1			
18	pawashing	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	ludmilla	2022-05-11	17:50:00	US	192.168.131.447	1			
25	ludmilla	2022-05-11	17:50:00	US	192.168.131.447	1			
26	spatel	2022-05-10	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	02:52:02	US	192.168.72.59	1			
34	drosario	2022-05-11	20:13:04	US	192.168.172.159	0			
36	lunadura	2022-05-08	09:00:42	US	192.168.78.151	1			
37	erab	2022-05-10	06:03:41	CANADA	192.168.152.148	0			
38	shaelish	2022-05-09	14:40:01	USA	192.168.60.42	1			
41	spatel	2022-05-10	17:39:42	CANADA	192.168.46.207	0			
42	cgriffin	2022-05-09	23:00:05	US	192.168.4.157	0			
43	lrodriguez	2022-05-08	03:54:08	CANADA	192.168.172.208	0			
44	daquino	2022-05-08	07:02:35	CANADA	192.168.160.144	0			
45	dtanaka	2022-05-11	10:12:54	US	192.168.223.157	1			
46	erab	2022-05-11	11:29:27	CAN	192.168.24.12	0			
47	dkot	2022-05-09	05:06:45	US	192.168.233.24	1			
48	asundara	2022-05-08	04:40:03	USA	192.168.172.159	1			
49	lunadura	2022-05-08	04:40:03	US	192.168.172.159	0			
50	jclarke	2022-05-10	10:48:02	CANADA	192.168.174.117	0			
51	jrafael	2022-05-10	22:14:01	CANADA	192.168.148.115	1			
52	cjackson	2022-05-10	22:07:07	CAN	192.168.58.57	0			

144 rows in set (0.001 sec)

Retrieve employees in Marketing

We want to perform security updates on specific employee machines in the Marketing department. We are responsible for getting information on these employee machines and will need to query the **employees** table. We will be identifying all employees in the Marketing department for all offices in the East building.

We will be using `SELECT * FROM employees WHERE department = 'Marketing' AND office LIKE 'East%';`. We will be selecting all rows from the employees table where the department column is Marketing and the office column contains East by using `LIKE 'East%'`.

MariaDB [organization]> SELECT * FROM employees WHERE department = '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)

Retrieve employees in Finance or Sales

We need to perform a different security update on machines for employees in the Sales and Finance departments. We are trying to identify all employees in the Sales or Finance departments.

We will be using `SELECT * FROM employees WHERE department = 'Sales' OR department = 'Finance';`. We will be selecting all rows from the employees table where the department column is Sales or the department column is Finance.

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	lrodrigu	Sales	South-134
1010	k242l212m542	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	k367l1639m697	redwards	Finance	North-180
1063	l686m140n569	lpopo	Sales	East-226
1066	o678p794q957	ttyrell	Sales	Central-444
1069	NULL	jpark	Finance	East-110
1071	t244u829v723	zdutchma	Sales	West-348
1072	u905v920w694	esmith	Sales	East-421
1076	y347z204a710	fgarcia	Finance	Central-270
1078	a667b270c984	sharley	Sales	North-418
1081	d647e310f618	qcorbit	Finance	South-290
1083	f840g812h544	gkoshi	Finance	West-165
1085	h339i498j269	cperez	Sales	East-325
1086	i281j129k749	lmajumda	Sales	West-499
1089	l358m929n154	jpark2	Sales	West-251

Retrieve all employees not in IT

We need one more update to employee machines. The employees who are in the Information Technology department already have this update, but employees in all other departments need it. We will be identifying all employees not in the IT department.

We will be using `SELECT * FROM employees WHERE NOT department = 'Information Technology';`. We will be selecting all rows from the employees table where the department column is not information technology using the `WHERE NOT`.

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	lrodrigu	Sales	South-134
1010	k242l212m542	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
1034	i679j565k940	bsand	Human Resources	East-484
1035	j236k303l245	bisles	Sales	South-171
1036	k550l1533m205	rzjensen	Marketing	Central-239
1038	m873n636o225	btang	Human Resources	Central-260
1039	n253o917p623	cjackson	Sales	East-378
1040	o783p832q294	dtarly	Human Resources	East-237
1041	p929q222r778	cgriffin	Sales	North-208
1042	q175r338s833	acook	Human Resources	West-381
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

Summary

As a security professional at a large organization, we made sure we investigated security issues to help keep the system secure. We found failed log in attempts that occurred after business hours 18:00 to find suspicious login activity. We also retrieved log in attempts that occurred on 2022-05-09 or 2022-05-08 to identify suspicious login attempts for the suspicious event. We also found log in attempts that do not originate from Mexico. We identified these activities using the `log_in_attempts` table.

After that, we retrieved employees in Marketing who are in the East building, employees in the Finance or Sales department, and employees that are not in the IT department using the

employees table. For the SQL query, we used the SELECT, WHERE, function with the filter AND, OR, NOT, LIKE, and %.