# Appliquer des filtres aux requêtes SQL

## Description du projet

[ En tant qu'analyste de sécurité, nous allons analyser et obtenir des informations spécifiques sur les collaborateurs, leurs ordinateurs et les départements auxquels ils appartiennent depuis les bases de données log\_in\_attempts et employees. Bien souvent, l'accès aux données dont nous avons besoin dépendent de plusieurs facteurs. Pour récupérer des informations spécifiques dans une base de données, nous pouvons appliquer des filtres avec plusieurs conditions. Dans ce cas nous avons utilisé les opérateurs AND, OR, LIKE, =, pour créer des filtres plus complexes pour nos requêtes SQL. Nous avons également appliqué un filtre not pour exclure une condition donnée.

]

## Récupérer les tentatives de connexion échouées après les heures d'ouverture

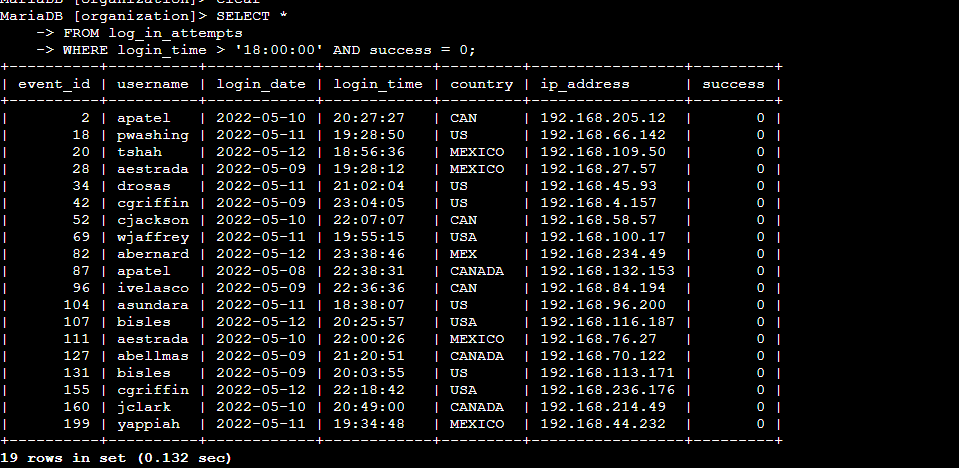
[Pour extraire les tentatives de connexion échouées après l’heure d’ouverture on a utilisé la requête

(SELECT \*

FROM log\_in\_attempts

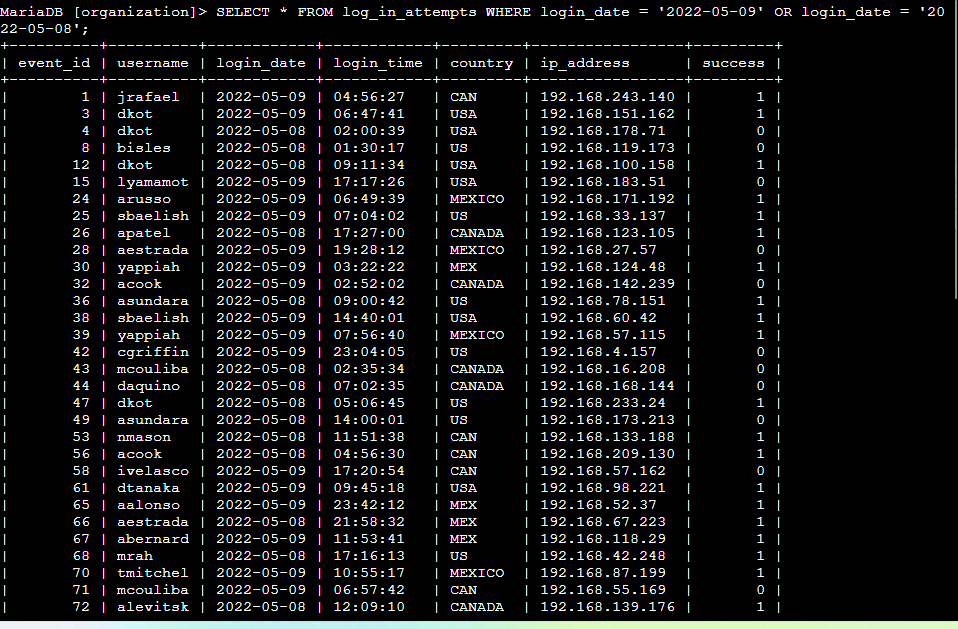
WHERE login\_time > ’18 :00 :00’ AND success = 0;).

Avec cette requête, à travers la ligne SELECT \* nous choisissons toutes les colonnes du tableau log\_in\_attempts comme nous indique cette ligne (FROM log\_in\_attempts) ou’ la colonne login\_time a des heures de connexion supérieur au 18 :00 :00 illustre par (WHERE login\_time > 18 :00 :00) et la colonne succès a échouées (AND success = 0 ;). Nous avons utilisé l’operateur (>) pour indiquer a MariaDB que les lignes a affiches dans la colonne Login\_time doivent être supérieur a 18h.

 ]

## Récupérer les tentatives de connexion à des dates spécifiques

[ Pour visualiser ses tentatives de connexion entre le 08/05/2022 et le 09/05/2022 on a utilisé la requête SELECT \* FROM log\_in\_attempts WHERE login\_date = ‘2022-05-09’ OR login\_date = ‘2022-05-08’ ;

Pour chacune des parties de cette requête, SELECT \* fais le choix de toutes les colonnes, FROM log\_in\_attempts indique dans quel tableau qui est dans notre cas actuelle le tableau log\_in\_attempts ; WHERE login\_date = ‘2022-05-09’ OR login\_date = ‘2022-05-08’ sur quelles colonnes faire le filtre des dates spécifier entre les cotes ; OR est le principale filtre utilise ici. Il indique que la règle de filtrage peut s’appliquer soit aux login\_date effectués le 2022-05-09 ou le 2022-05-08. ]

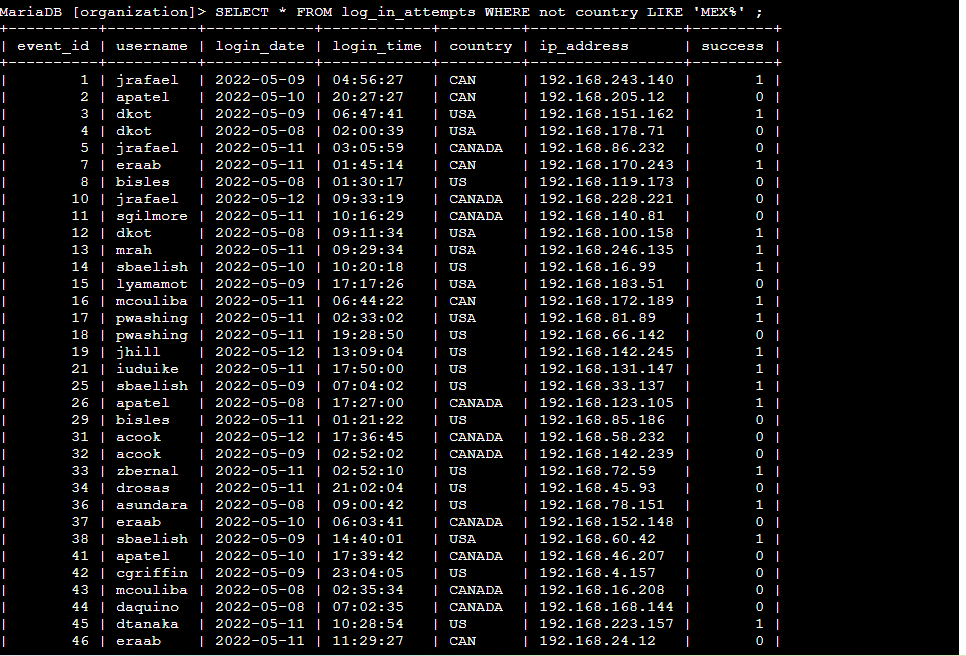
## Récupérer les tentatives de connexion en dehors du Mexique

[ SELECT \*

FROM log\_in\_attempts

WHERE not country LIKE 'MEX%';

Sur cette requête les deux premières lignes conduisent aux mêmes effets décrits aux étapes précédentes. La troisième ligne qui est WHERE not country LIKE ‘MEX%’ ; nous demandons à notre base de données de trier à partir de la colonne country et d’afficher les pays autres que le MEX dans sa colonne ; Pour cela not et LIKE sont les filtres pour dire pas comme le pays MEX%. Le caractère pourcentage indique à la base de données d’applique le filtre aux lignes présentent dans la colonne country ayant pour racine de chaine de caractère MEX.

]

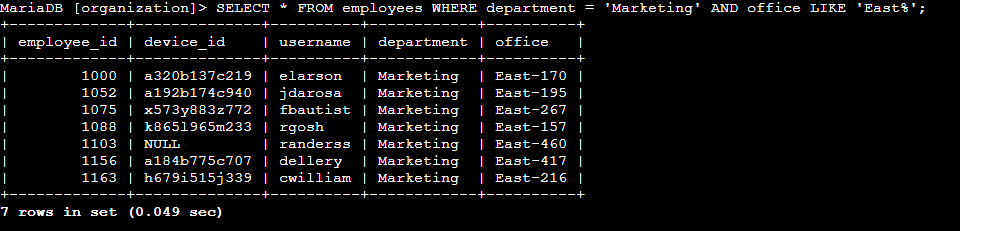
## Récupérer les employés du Marketing

[ SELECT \*

FROM employees

WHERE department = 'Marketing' AND office LIKE 'East%’;

Cette requête extrait les employés du département Marketing dont les bureaux sont à L’Est pour des mise à jour de sécurité dans leurs ordinateurs. Alors la requête est faite en trois étapes principales, à savoir : la ligne SELECT \* demande à la base de données MariaDB d’afficher toutes les colonnes, la ligne FROM employees indique de quelle table extraire toutes les colonnes de la requête ligne 1 et la troisième indique sur quelle colonne appliquée les filtres égale (=), et (AND), ressemblant a (LIKE) dans les colonnes departement et office.

]

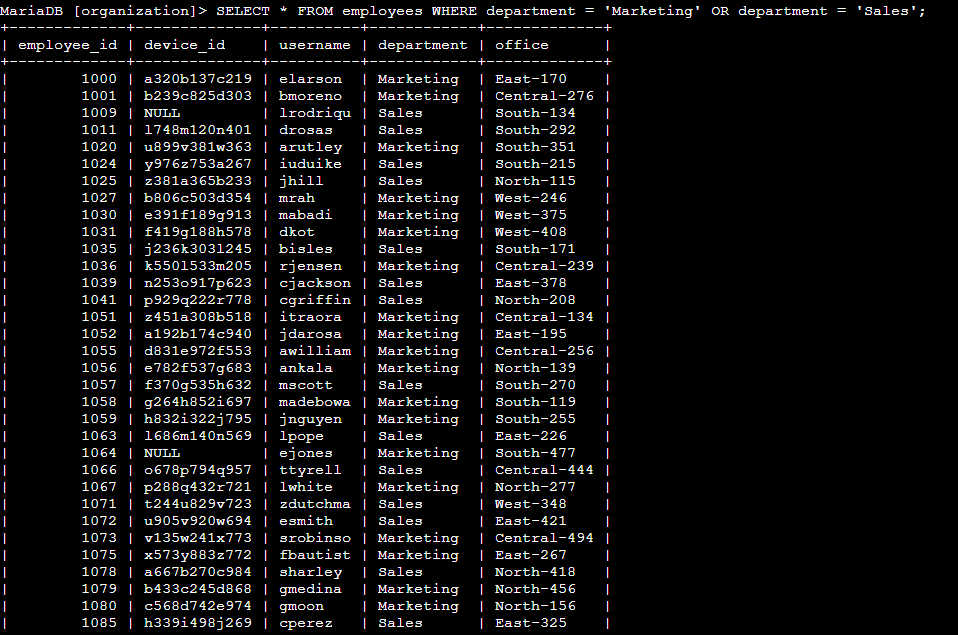
## Récupérer les employés des services finances (Finance) ou commerciaux (Sales)

[ SELECT \*

FROM employees

WHERE department = 'Marketing' OR department = 'Sales';

Pour cette étape aux niveaux de la ligne trois de la requête nous avons utilisé deux filtres, à savoir le filtre d’égalité (=) qui permet d’afficher les lignes de la colonne department ou c’est marque Marketing. La requête ne s’arrête pas là, par la suite on utilise le filtre OR qui demande aussi à la base de données d’afficher les lignes de la colonne department où sont marquées Sales.

]

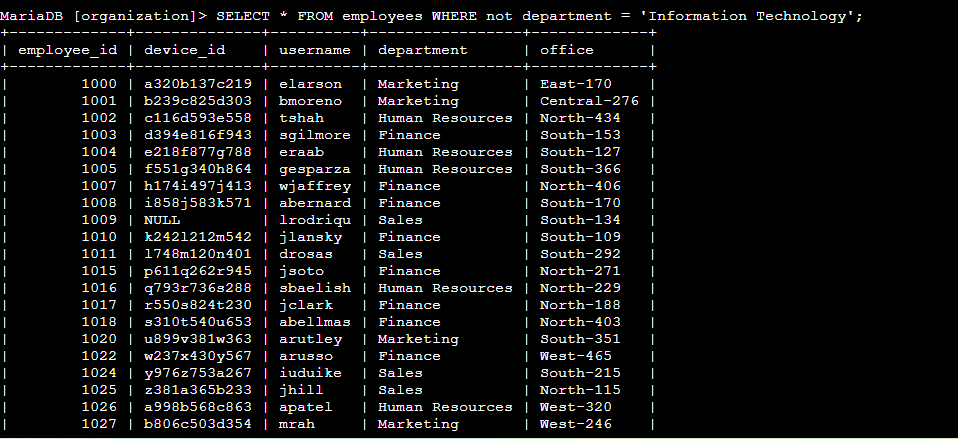
## Récupérer tous les employés qui ne sont pas dans l'informatique (IT)

[ SELECT \*

FROM employees

WHERE not department = 'Information Technology';

A cette étape, la ligne trois de la requête nous avons utilisé deux filtres à savoir le filtre (not) qui permet de ne pas afficher les lignes de la colonne department ou sont marquées Information Technology ; qui son tour est illustre par le filtre égalité (=).

]

## Synthèse

[Au cours de cet atelier on a effectué :

Une récupération de toutes les tentatives de connexion ayant échoué après les horaires d'ouverture ;

On a récupéré toutes les tentatives de connexion effectuées à certaines dates ;

Récupérer toutes les connexions qui ne proviennent pas du Mexique ;

Recueillir des informations sur certains collaborateurs du département marketing ;

Recueillir des informations sur les collaborateurs du département financier/commercial ;

Recueillir des informations sur les collaborateurs extérieurs au département informatique ; Ce qui nous a permis d’analyse et d’identifier les potentiels menaces et vulnérabilités auxquels note structure pouvais faire face.

]