**Cisco Labs**

**Weekly Report**

**Security Team**

**May 2022 - Week 2**

**Project Description**

As part of our weekly review, the security team at Cisco Labs is responsible for investigating security issues to help keep the organization’s systems secure and protected from internal and external threats.

Recently we have discovered some potential security issues that involve login attempts and employee machines.

Throughout this report, we have documented our process along with screenshots of our findings (queries) while examining the organization’s data in their **employees** and **log\_in\_attempts** tables. We’ll be using SQL to retrieve records from different datasets and investigate the potential security issues.

**Retrieve After Hours Failed Login Attempts**

In this section, our team investigated failed login attempts that were made after business hours (after 6:00pm or 18:00).

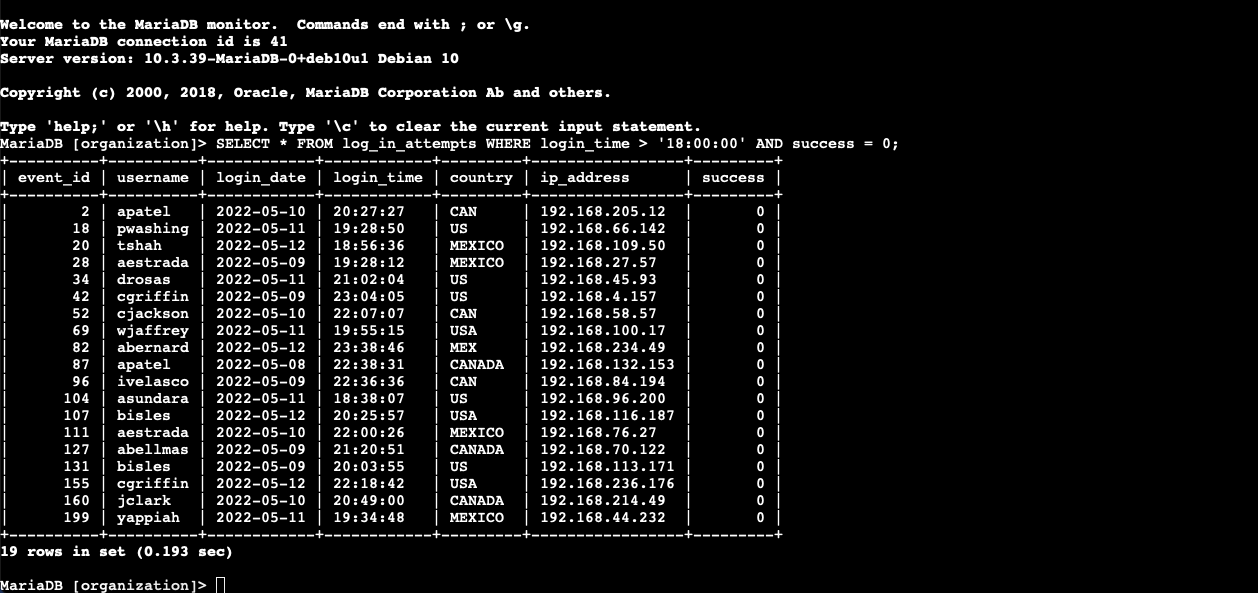
The **login\_time** column in the **log\_in\_attempts** table contains information on when login attempts were made. The success column in the log\_in\_attempts table contains values of TRUE or FALSE to indicate whether the login was successful. MYSQL stores Boolean values as 1 for TRUE, and 0 for FALSE. TRUE = Success, FALSE = Unsuccessful.

Based on the information mentioned above, our SQL query would have to be filtered to retrieve the records that highlight unsuccessful login attempts that were made after 6:00pm and that were also unsuccessful. To do this, we will use the WHERE filter & the AND command.

**SELECT \***

**FROM log\_in\_attempts**

**WHERE login\_time > ‘18:00:00’ AND success = 0;**



From the results shown in the image above, 19 failed login attempts were recorded after 6:00pm.

**Retrieve Login Attempts on Specific Dates**

Our team investigated a suspicious event that occurred on ‘2022-05-09’. We retrieved all login-attempts that occurred on this day and the day before (‘2022-05-08’).

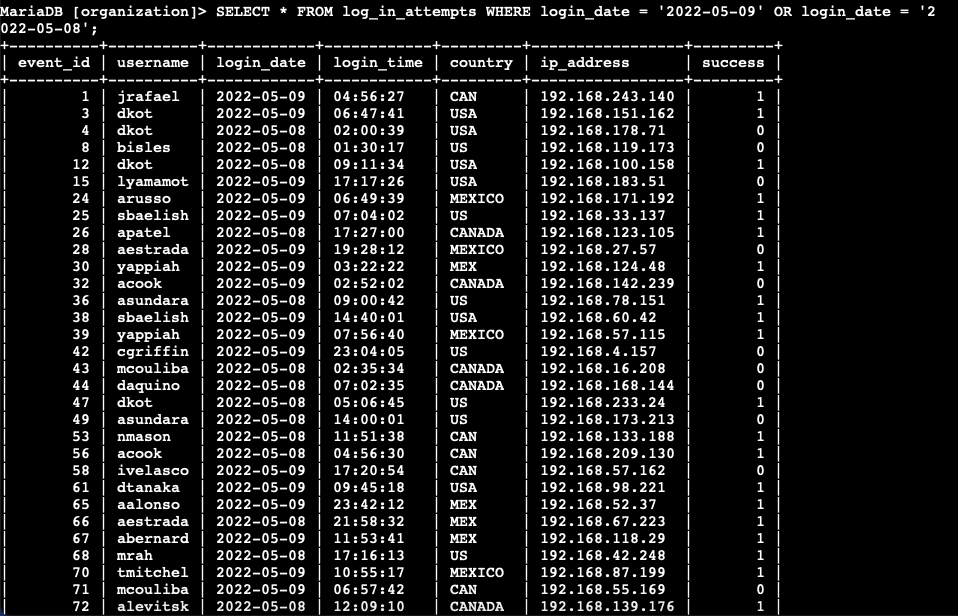
The login\_date column in the log\_in\_attempts table contains information on the dates when login attempts were made.

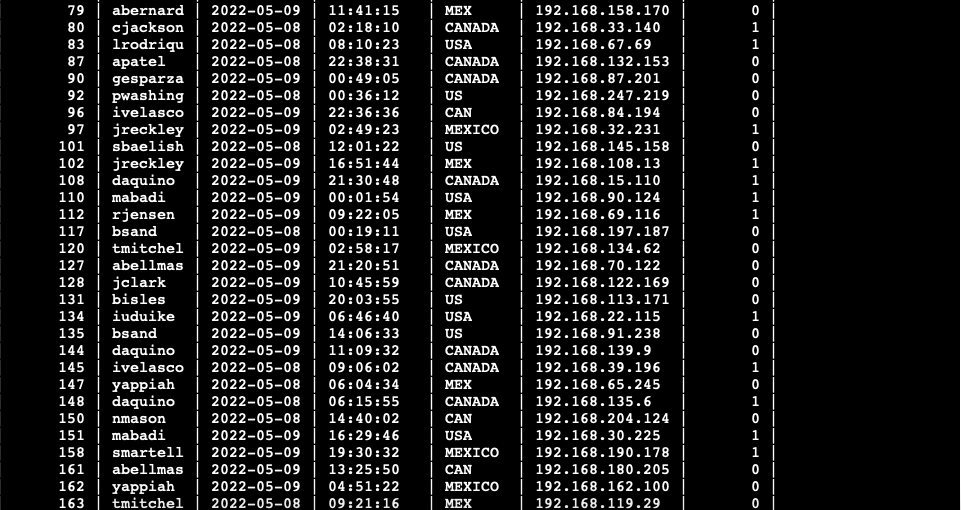
We will use the OR operator to retrieve the failed login attempts on the specified days.

**SELECT \***

**FROM log\_in\_attempts**

**WHERE login\_date = ‘2022-05-09’ OR ‘2022-05-08’;**







75 login attempts were made on these two days.

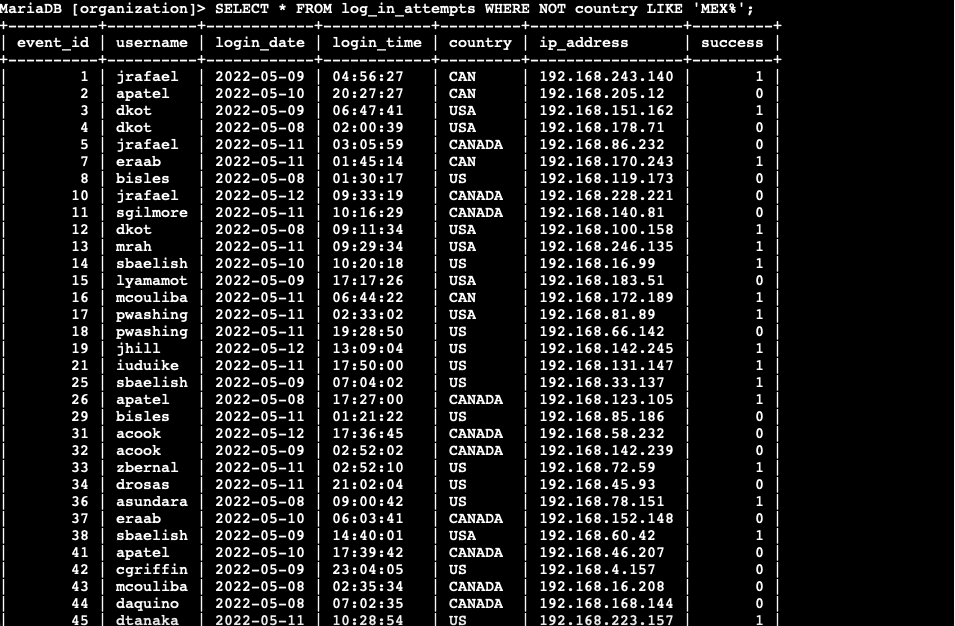
**Retrieve Login Attempts Outside of Mexico**

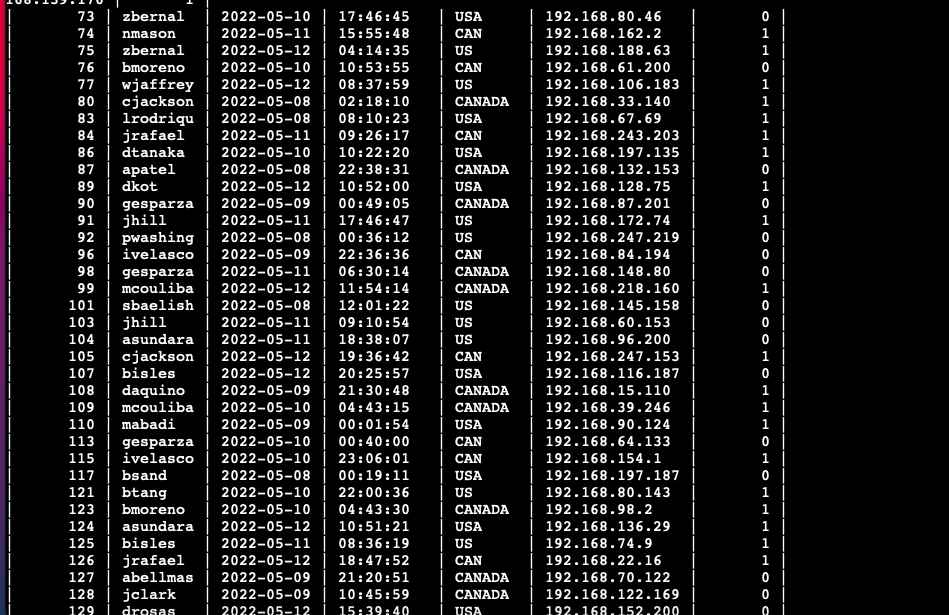
Our next step involved investigating logins that did not originate in Mexico. The country field includes entries with ‘MEX’ and ‘MEXICO’. To retrieve login attempts that did not originate in Mexico, you should use the NOT and LIKE operators and the matching pattern ‘MEX%’.

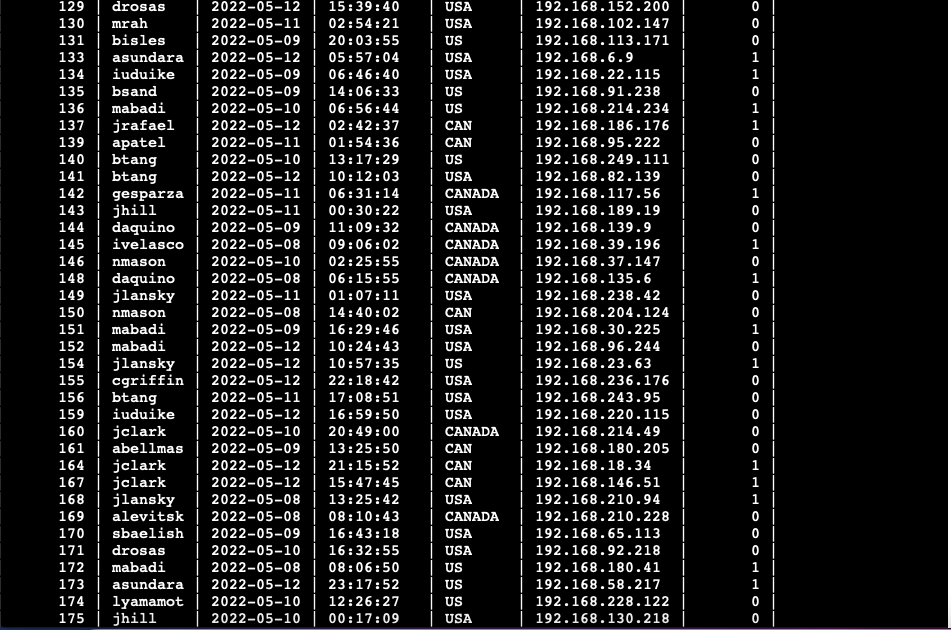
**SELECT \*  
FROM log\_in\_attempts**

**WHERE NOT country LIKE ‘Mex%’;**

The NOT Operator is used to filter out records by the column that does not match the criteria listed after the LIKE operator. The LIKE operator is used along with wildcard characters (%) when searching for a specified pattern in a column. For example, some records pertaining to Mexico may have ‘Mex’ or ‘Mexico’ as values in the country column. To ensure that both results are retrieved, we use the wildcard character (%) along with the LIKE operator.





****

****

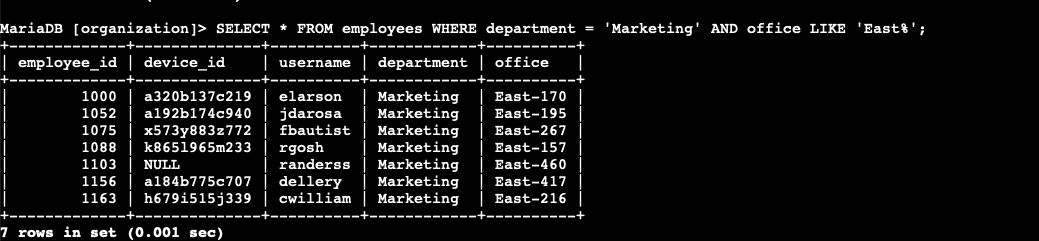
144 login attempts were made outside of Mexico.

**Retrieve Employees in Marketing**

Our team is updating employee machines, and you need to obtain the information about employees in the ‘Marketing’ department who are located in all offices in the East Building (such as ‘East-170’ or ‘East-320’).

SELECT \*   
FROM employees

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

****

7 computers need to be updated as per the results shown above.

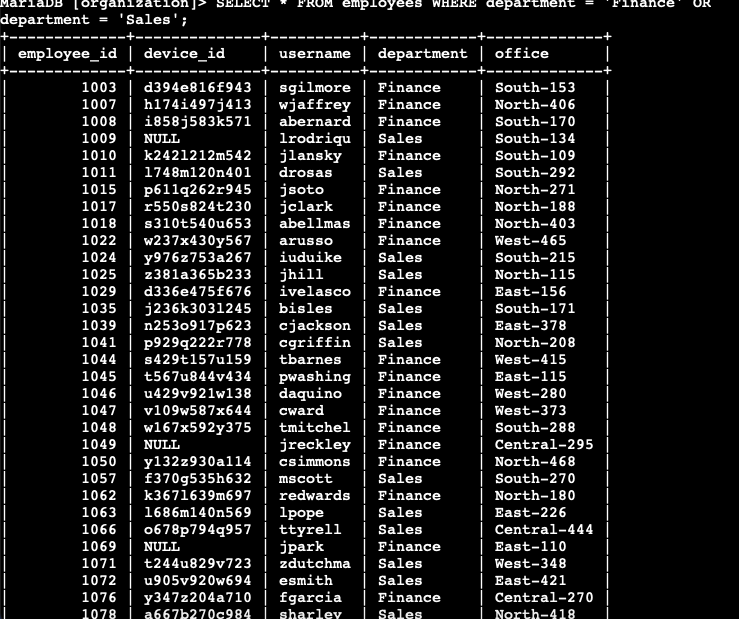
**Retrieve Employees in Finance or Sales**

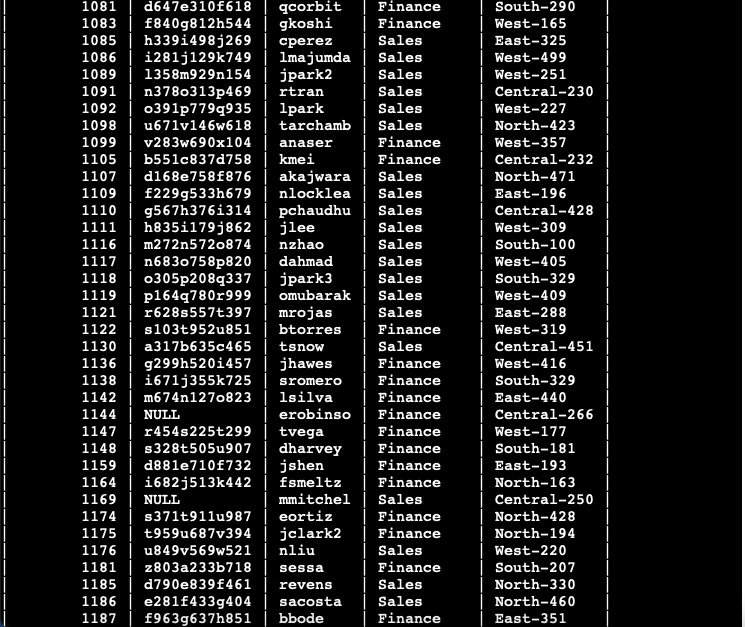
Our team also needs to perform a different update to the computers of all employees in the Finance or Sales department, and we need to locate information on these employees.

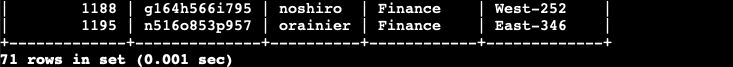
**SELECT \***

**FROM employees**

**WHERE department = ‘Finance’ OR department = ‘Sales’;**





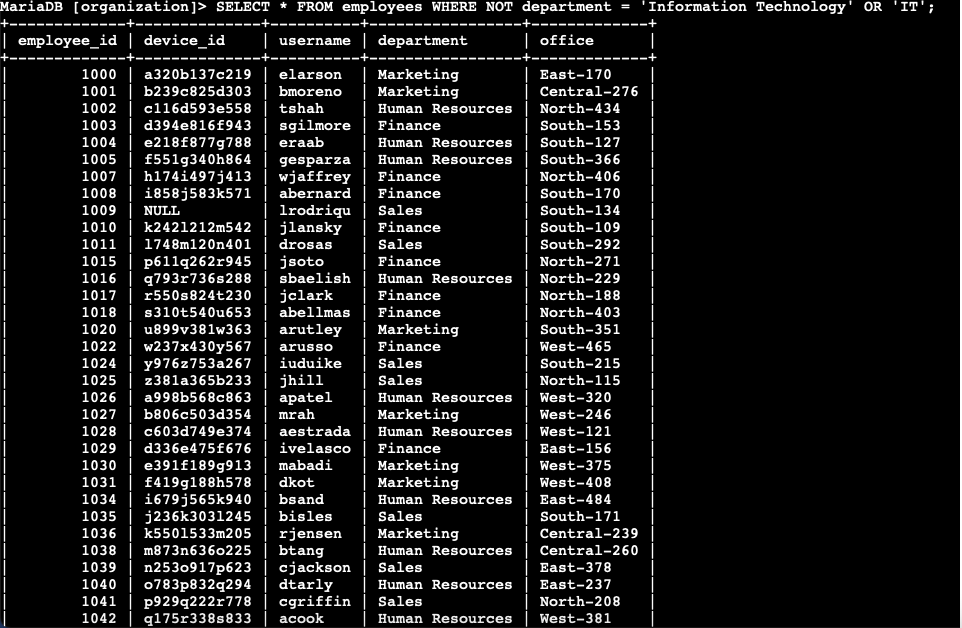
****

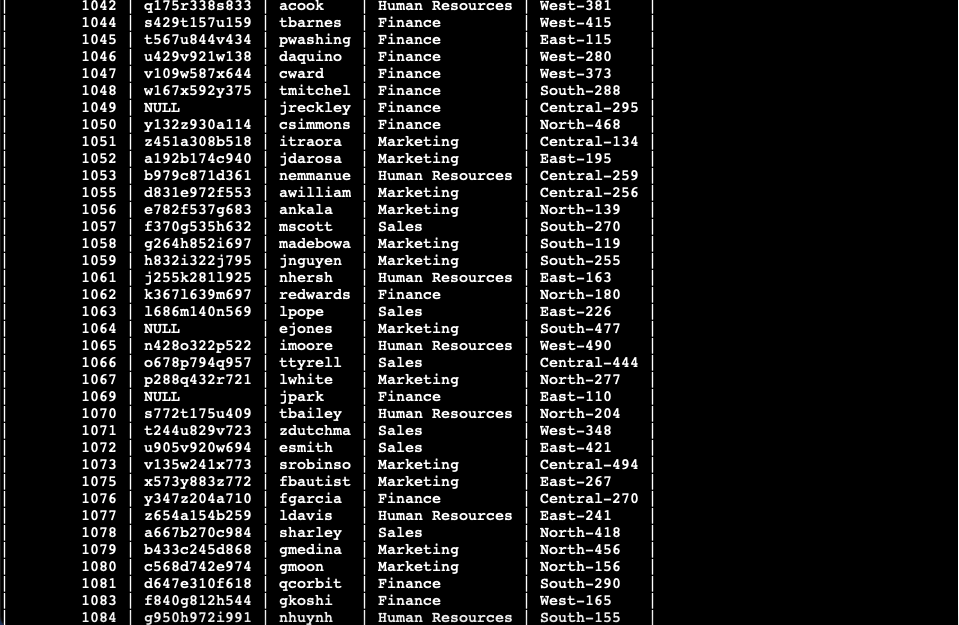
**Retrieve Employees not in IT**

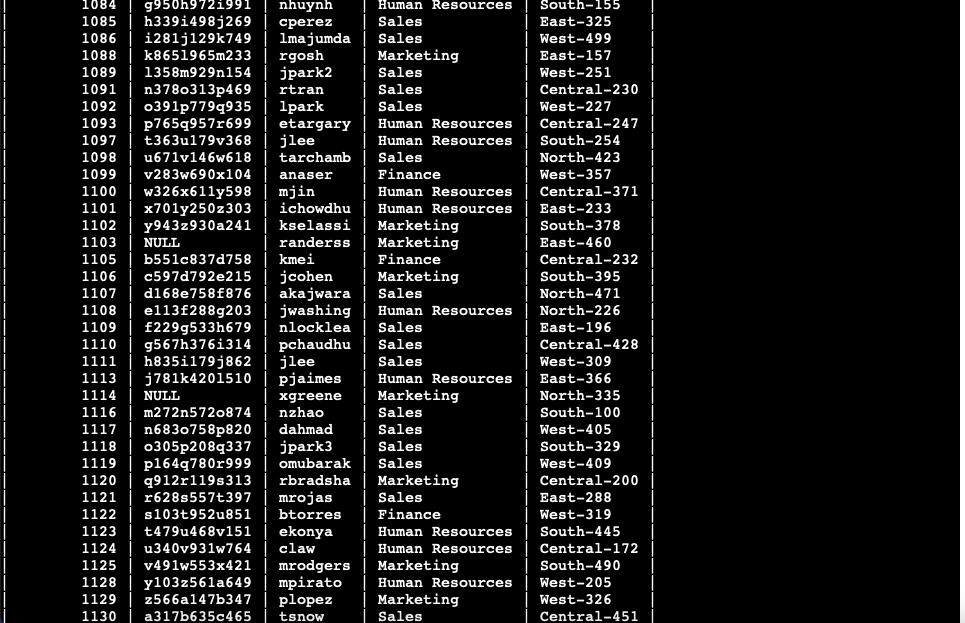
To retrieve employees not in Information Technology, the SQL command goes as follows:

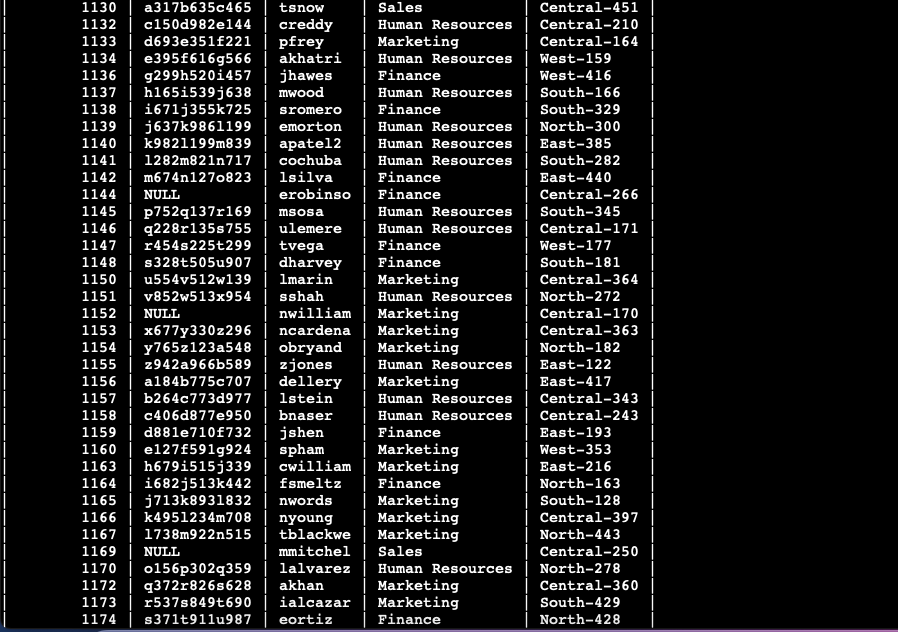
SELECT \*   
FROM employees

WHERE NOT department = ‘Information Technology’ OR ‘IT’;











161 employees are not working in IT throughout the entire organization.

**End of Report**