

SQL filtering versus Linux filtering

Previously, you explored the Linux commands that allow you to filter for specific information contained within files or directories. And, more recently, you examined how SQL helps you efficiently filter for the information you need. In this reading, you'll explore differences between the two tools as they relate to filtering. You'll also learn that one way to access SQL is through the Linux command line.

Accessing SQL

There are many interfaces for accessing SQL and many different versions of SQL. One way to access SQL is through the Linux command line.

To access SQL from Linux, you need to type in a command for the version of SQL that you want to use. For example, if you want to access SQLite, you can enter the command *sqlite3* in the command line.

After this, any commands typed in the command line will be directed to SQL instead of Linux commands.

Differences between Linux and SQL filtering

Although both Linux and SQL allow you to filter through data, there are some differences that affect which one you should choose.

Structure

SQL offers a lot more structure than Linux, which is more free-form and not as tidy.

For example, if you wanted to access a log of employee log-in attempts, SQL would have each record separated into columns. Linux would print the data as a line of text without this organization. As a result, selecting a specific column to analyze would be easier and more efficient in SQL.

In terms of structure, SQL provides results that are more easily readable and that can be adjusted more quickly than when using Linux.

Joining tables

Some security-related decisions require information from different tables. SQL allows the analyst to join multiple tables together when returning data. Linux doesn't have that same functionality; it doesn't allow data to be connected to other information on your computer. This is more restrictive for an analyst going through security logs.

Best uses

As a security analyst, it's important to understand when you can use which tool. Although SQL has a more organized structure and allows you to join tables, this doesn't mean that there aren't situations that would require you to filter data in Linux.

A lot of data used in cybersecurity will be stored in a database format that works with SQL. However, other logs might be in a format that is not compatible with SQL. For instance, if the data is stored in a text file, you cannot search through it with SQL. In those cases, it is useful to know how to filter in Linux.

Key takeaways

To work with SQL, you can access it from multiple different interfaces, such as the Linux command line. Both SQL and Linux allow you to filter for specific data, but SQL offers the advantages of structuring the data and allowing you to join data from multiple tables.

Revision #1

Created 9 July 2023 15:19:37 by naruzkurai

Updated 9 July 2023 15:20:28 by naruzkurai