Superusers

by Sophia Tutorial

WHAT'S COVERED

This tutorial explores the importance of separating out superuser and regular accounts in two parts:

1. Reasons For Superusers
2. Superuser Administration

1. Reasons For Superusers

The principle of least privileges is an important element to consider when it comes to setting up security in any information system. Whether it is through Windows, Linux, or a database, a “superuser” account is viewed as a role that comes with unrestricted access to all commands, functions, and resources within a system. A superuser can bypass all permission checks, and access all types of powerful operations, including everything in the database, things that touch the underlying system, and enabling extensions. Superuser roles in a database have the ability to create databases and roles, or completely remove them. If the superuser role is misused on purpose or even by accident, it can create significant damage.

Most of the security protection measures are handled around the perimeter of an information system. However, superuser roles and accounts are already on the inside. For example, if an individual had temporary access to the superuser role in a database, they could create additional roles to which they could connect, causing further damage. Even if the superuser role that an individual had been using was removed, they could have backdoors through these other roles. They could even remove evidence of their activity within the system. For example, an intruder with a superuser role could create orders within a system and have items that they did not purchase sent to them. Once the order had been sent out, they could delete the order and any related data so that the system had no indication of that order.

2. Superuser Administration

In the last tutorial, we explored SQL injections, wherein individuals can potentially drop a table or even a database. However, they can only do so if the role that the application was logging into had that permission. As such, any roles that a user of an application will interface with should only be given the necessary privileges to complete their tasks. In some organizations, superuser roles and accounts are shared among various users, such as database administrators. By doing this, though, the audit trail becoming a lot more difficult to track.

Policies need to be put in place to help provision, segregate and monitor various risks. For example, the superuser role should be strictly limited to a number of individuals. You can temporarily increase the

privileges of individuals when needed, without granting them full superuser privileges around the clock. You can also work on separating the privileges of users and force them to use certain accounts depending on when they need certain privileges. You may have separate accounts/roles that have the ability to update and query data, while other accounts/roles can only query data if that role doesn't need to make changes. All permissions should be granted to the user or role, they should not be automatically given.

It can also be important to change out the superuser password on a regular basis so that even if the account is compromised, it is limited. Some organizations may even change the password after each use of the role to keep it safe.

SUMMARY

Separating out superuser roles and regular accounts is important, as superuser roles should only be used when absolutely needed.

Source: Authored by Vincent Tran