Devolutions

Glossary of Common Privileged Access Management (PAM) Terms

IT CAN ALSO CREATE RISKS AND CUSTOMER SERVICE ISSUES

When I started working at Devolutions a long time ago (it's been five years — time flies when you're having fun!), I thought my language skills were pretty good. I mean, I'm fluent in English and French, and I have a strong grasp of Hebrew (????!) and Spanish (hola!).

But then one of my colleagues asked me, "Do you speak PAM?" — and I had no idea what they meant. I figured it was some fictional language, like Shyriiwook.

But guess what? Speaking PAM is even more useful than speaking Shyriiwook (my apologies to all of the Wookies out there), because pretty much everyone is talking about PAM these days.

Now, I know that many of you are technical wizards who know all about PAM. I mean, if you were a Jeopardy! contestant and the category was "Privileged Access Management", you would have all the answers and force your fellow contestants to leave the stage in shame.

But then, some of the folks who visit our blog are business users and not technical users. Plus, sometimes even the ultra-geeks among us could use a refresher, right? And so, I thought it would be helpful to put together a little glossary of common PAM terms (in alphabetical order):

Account Brokering: The action to initiate a session using a well-known protocol (SSH, RDP, VNC, X11, etc.) and inject the credentials on behalf of the user at that time. Account brokering inserts credentials on the back end, which means that end users never see passwords in the first place — but they can still access necessary accounts to complete their day-to-day work.

Break-Glass Scenarios: Any method that is established to provide emergency access to a secure information system. As a result, in the event of a critical error or abnormal end, users without privileged access can gain access to key systems to correct the problem.

Firecall Account: Accounts created to facilitate emergency access to a secure system. Firecall (a.k.a. administrator accounts) are sometimes accessed by users without privileged accounts, so they can gain access to key systems when problems arise (see ***Break-Glass Scenarios***).

Least-Privileged Account: A user account with a minimal number of privileges needed to perform daily operations.

Privilege: The authority to make administrative or elevated changes to a network or computer, and to see sensitive information.

Privileged Account: An account that has elevated privileges. It can be shared with many users but represents one application, system, service, or administrator. There are multiple types of privileged accounts (see ***System Accounts***, ***Shared Accounts***, and ***Service Accounts***).

Service Accounts: Allows remote (i.e., software-to-software) interactions with other systems, or to run specific services.

Shared Accounts: Accounts shared between multiple users for software maintenance and installation purposes. They often feature "fire call" or "break-glass" accounts, which provide temporary access to a secure information system in case of critical error or emergency situations (see ***Break-Glass Scenarios***).

System Accounts: A built-in account used by admins to access applications and systems, such as root on Unix/Linux systems or Administrator on Windows systems.

Privileged Business Users: Users who have access to sensitive data and information assets, such as HR records, payroll details, financial information, the company's intellectual property, etc.

Privileged IT Users: Users who have access to IT infrastructure supporting the business.

Privileged Users: Users who have been granted privileged access. There are multiple types of privileged users (see ***Privileged Business Users*** and ***Privileged IT Users***).

User Account: A standard account that represents one human user with standard privileges (usually linked to an Active Directory profile).

And there you go! If you already speak fluent PAM, then you can share this glossary with your less geeky colleagues and clients/customers, so that they'll know what you're talking about. This can improve efficiency and security, which is definitely a good thing — or as Chewbacca would say in elegant and lyrical Shriwook: oooaoowhrrrcraaohuanraaoahoowhhhhhhhggg!