PAM Getting started

PAM Getting started

- Introduction
- Quick overview
- PAM videos

Introduction

Why PAM?

Privileged Account Management (from this point forward: PAM), allows you to manage accounts that are necessary to perform scheduled configuration and maintenance tasks, as well as supervening tasks such as the recovery of a hardware or software failure or the restoration of a backup. Due precisely to the need to use these accounts in an unplanned manner, their management must combine security, procedures and flexibility. PAM is the process of determining who has access to what types of information as it creates an integrated view of risk, threats, and controls.

PAM is considered by many analysts and technologists as one of the most important security projects for reducing cyber risk and achieving high-security ROI.

PAM Goals

Reduce the attack surface

- Have an up to date global catalog of accounts and permissions.
- Close the gap between the user and administrator accounts.
- Assign the ownership and responsibilities for each account.
- Complex and rotated passwords.
- Use strong autentication.
- Track accounts ownership and warns when an account loses its last owner.

Minimize the potential impact

- Rectification campaigns to confirm the permissions assigned to each service account.
- Apply dynamic authorization engine (XAML) to grant access to critical resources.

Rapid attack detection

Detection phase

- Exexecution of dangerous commands.
- Usage of dangerous applications.

Response actions

- Drop offending session.
- Lock account.

Notification

- Account owner notification by SMS/Email.
- Creation of a ticket.

Generate and keep legal evidence

- Record privileged account sessions (Screen, KeyBoard, Clipboard, and File transfers).
- Keep encrypted in a secure storage.

Quick overview

Introduction

Once the Jump servers have been installed, following the steps defined on the PAM Jump Server installation page, it will be mandatory to configure the jump servers on the **Soffid Console**, to do that you can visit the Configure PAM session servers page.

Soffid console provides you a powerful tool, **Network discovery** tool. It is able to identify the machines in each defined network and retrieve information about user accounts, also, it can detect system accounts. Visit the Network discovery page for more information.

Once the machines and Accounts, both user and system, have been discovered, the critical accounts must be located in protected storage, the Password Vault. It is important to identify the owner and assign properly those accounts to a specific user or a group of users.

Then it is able to configure workflows or approval processes in order to use these accounts. Some accounts, the real risk accounts, need to request for permission to use them.

All the sessions will be recorded (Screen, KeyBoard, Clipboard, and File transfers).

The ability to configure and manage PAM policies gives Soffid a great power in terms of privileged account management. In this line, it is possible to configure policies based on rules, so when each one of the rules is fulfilled, one or more actions will be triggered according to the configuration. The available actions are to close the session, lock the account, open an issue on a ticketing system and notify the breaking rule. You can find more information by visiting the PAM Rules page and the PAM Policies page.

When you have defined the rules, it is essential to indicate when Soffid has to take in mind them. That can be configured on the Password Vault page, here it is able to indicate the policy for each folder, or none if there is no policy to apply. When you define a policy for a folder, that policy will apply to all accounts hanging from this folder.

Soffid provides you the functionality that allows searching in PAM recording sessions. With that option you can search recording video applying several filters, for instance, you can search all the recordings videos in which the user writes the command "rm" or all the recording videos in which the user write "cat FILE_NAME". For more information visit the

Search in PAM recordings page.

Quick access

Links to functionality on Soffid Console related to the configuration of privileged accounts are provided below:

- PAM Jump Server installation
- Configure PAM session servers
- PAM Rules
- PAM Policies
- Network discovery
- Password Vault
- Accounts
- Search in PAM recordings

Also, you can visit the PAM Deployment procedure:

- Deployment procedure

PAM videos

How works on-screen Keyboard

https://www.youtube.com/embed/OvGXmQT62XU?rel=0