Tutorial 9

IT2562

1. Explain how was authentication done on Linux application before the introduction of Pluggable Authentication Modules.

- Before PAM, every Linux application that needs authentication features will need to develop their own system and associated database.
- Native Linux authentication was not extendable to 3rd party application

2. Where are PAM configuration files located in the file system? How are these configuration files named?

- Every Linux application that needs authentication features will need to develop their own system and associated database

3. Describe the 4 type of PAM interfaces. Is it necessary for a PAM configuration file to define all these interfaces?

- auth — Determines whether the user is who they claim to be, usually by a password, but perhaps by a more sophistcated means, such as biometrics.
- account — Determines whether the user is allowed to access the service, whether their passwords has expired, etc.
- password — This module interface is used for changing user passwords.
- session — Things that should be done before and/or after the user is authenticated. This might include things such as mounting/unmounting the user home directory, logging their login/logout, and restricting/unrestricting the services available to the user.
- **Not necessary** for a PAM configuration file to have definitions for all 4 module interfaces

4. What are PAM authentication modules? Where are they located in the filesystem? How can we find out more information about the usage of these modules in PAM?

- These are binary files developed and compiled by developers
- All located in /usr/lib64/security
- To find out functionality of each PAM module use the ‘man’ command

5. There are control flags used in PAM configuration files together with the modules. Explain briefly these control flags, required, requisite, sufficient and optional.

- required — Module failure results in interface failure result, although PAM will still call all the other modules listed for this interface before denying authentication.
- requisite — Module failure results in immediate denial of authentication.
- sufficient — The module result is ignored if it fails. However, if the result of a module flagged sufficient is successful *and* no previous modules flagged required have failed, then no other module results are required and the interface result is success.
- optional — Whether this module succeeds or fails is only significant if no other modules reference the interface.