PAM exercise

Jens Schønberg

April 2022

1 Exercise 1. See around in pam.d

Look inside the /etc/pam.d directory, for instance at sudo,su and sshd. Valid controllers are:

- required - failure if not loaded, after all revocation.
- requsite - same as required, but direct termination
- sufficient - valid if no other failures
- optional - failure only means something if it's the only one
- include - load in config
- substract - like include, but compartmentarize the include.

standard modules are

- account - used by system for service differential, also restrict/permit services based on system attributes
- auth - prompts for authentication, through authentication authorization is granted
- password - only used to change password
- session - setup before opening/closing, such as logging data or performing before/after session-based information

2 Exercise 2. Restrict SSH edit for root

Open up the /etc/pam.d/sshd

add in auth required pami_listfile.so\onerr=succeed item=user sense=deny file=/etc/ssh/deniedusers then in /etc/sshd, make deniedusers, edit it and write in 'root' or the users you wish to restrict.

Now chmod the file you wish to strict to remove other rights, now sshd user will be denied edit rights when trying to auth

3 Exercise 2. Revove SSH root login via PAM