LPIC-2 TRAINING COURSE

Topic 211: Pluggable Authentication Modules

What is PAM

- **Modules provide dynamic authorization for application and services**
- **4 groups for independent management**
  - **Account modules**: check that a account is valid
  - **Authentication modules**: verify account's identity
  - **Password modules**: reponsible for updating password
  - **Session modules**: define actions that are performed at the beginning and end of session
- **Modules are stored in /lib/security**

PAM Configuration

- ***/etc/pam.conf* or files in */etc/pam.d/***
  - ***/etc/pam.conf***
    `servicename type control module-path module-arguments`
  - ***/etc/pam.conf/<servicename>***
    `type control module-path module-arguments`
- **Fileds meaning:**
  - **servicename**: name of the application involed (***login***, ***ssh***, ***passwd***…)
  - **type**: task to be perfomed (***account***, ***auth***, ***password***, ***session***)
  - **control:** what should do in case authentication fails (***requisite, required, sufficent, optional, include***)
  - **module-path:** path to PAM module
  - **module-arguments:** module specific arguments

Example: */etc/pam.d/login*

```
# Perform password authentication and allow accounts without a password
auth required pam_unix.so nullok

# Check password validity and continue processing other PAM's even if
# this test fails. Access will only be granted if a 'required' PAM,
# that follows this ‘sufficent' one, succeeds.
account sufficent pam_ldap.so
account required pam_unix.so

# Log the user name and session type to syslog at both the start and
# the end of the session.
session required pam_unix.so

# Allow the user to change empty passwords (nullok), perform some
# additional checks (obscure) before a password change is accepted and
# enforce that a password has a minimum (min=4) length of 4 and a
# maximum (max=8) length of 8 characters.
password required pam_unix.so nullok obscure min=4 max=8
```

Thank You !

BACKUP SLIDES