

Découverte de PAM et conception d'une configuration

Phase 1 – Recherche documentaire

Question 1 : Qu'est-ce que PAM et à quoi sert-il dans Linux ?

Question 2 : Quelle est la différence entre un module PAM et une application PAM-aware ?

Question 3 : Quels sont les types de directives qu'on trouve dans les fichiers PAM (*auth*, *account*, *password*, *session*) ? Donnez un exemple de module pour chacun.

Question 4 : Que représente le control flag (*required*, *requisite*, *sufficient*, *optional*) ? Expliquez la conséquence de chaque mot-clé.

Question 5 : Donnez trois modules PAM courants et décrivez leur rôle.

Question 6 : À quoi ressemble un fichier dans `/etc/pam.d/` ? Recherchez un exemple réel.

Question 7 : Pourquoi PAM renvoie-t-il un code de succès ou d'échec à l'application cliente (C, Python, etc.) ?

Phase 2 – Étude et écriture d’un fichier PAM pour un programme C

Contexte

Un programme C appelé `authformation` demande un nom d'utilisateur et un mot de passe, puis vérifie ces informations via PAM avant d'afficher : *“Connexion réussie”* ou *“Échec d’authentification”*.

programme C

```
#include <security/pam_appl.h>
#include <security/pam_misc.h>
#include <stdio.h>

int main() {
    pam_handle_t *pamh = NULL;
    struct pam_conv conv = { misc_conv, NULL };
    int retval = pam_start("authformation", NULL, &conv, &pamh);

    if (retval == PAM_SUCCESS)
        retval = pam_authenticate(pamh, 0);

    if (retval == PAM_SUCCESS)
        printf("Connexion réussie\n");
    else
        printf("Échec d’authentification\n");

    pam_end(pamh, retval);
    return (retval == PAM_SUCCESS ? 0 : 1);
}
```

Travail demandé

Vous devez rédiger le fichier de configuration PAM correspondant :

`/etc/pam.d/authformation`

Le programme doit :

- utiliser le mot de passe local (`pam_unix.so`);
- bloquer après 3 échecs pendant 60 secondes (`pam_tally2.so`);
- charger les variables d’environnement (`pam_env.so`);
- journaliser la session (`pam_lastlog.so`).

Question 8 : Complétez chaque ligne avec le module approprié et ses options.

```
# /etc/pam.d/authformation

auth      required  -----
auth      required  -----
account   required  -----
session   optional  -----
session   required  -----
```

Question 9 : Expliquez le rôle de chaque directive dans ce tableau.

Ligne	Type	Control	Module	Rôle / Description
1	auth	required		
2	auth	required		
3	account	required		
4	session	optional		
5	session	required		

Question 10 : Expliquez ce qui se passe si un module échoue (selon son *control flag*).

Question 11 : En quelques lignes, décrivez le rôle global de ce fichier dans le système PAM.

Ressources suggérées

- François Goffinet — <https://linux.goffinet.org/administration/securite-locale/pluggable-authentication-modules-pam/>
- Stéphane Robert — <https://blog.stephane-robert.info/docs/securiser/durcissement/pam/>