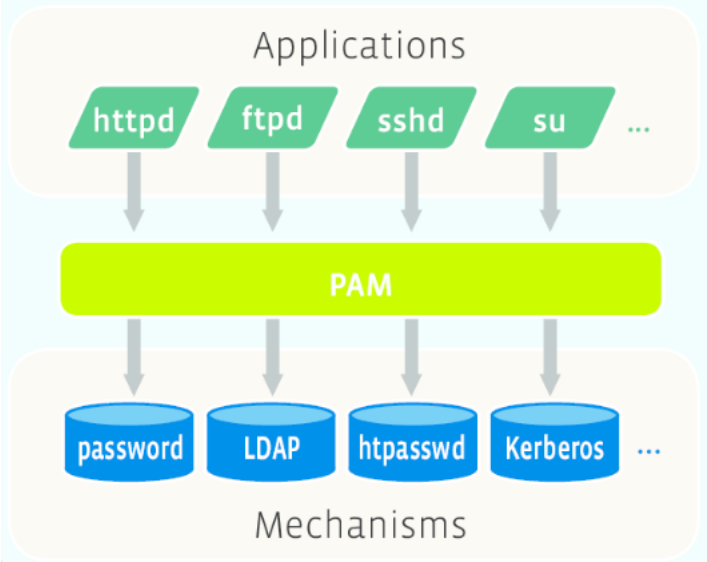
Responsable du cours (ARIR81/M1-APP-RS) : Yousfi Souheib

TP3 : Authentification SSH avec OpenLDAP

Introduction

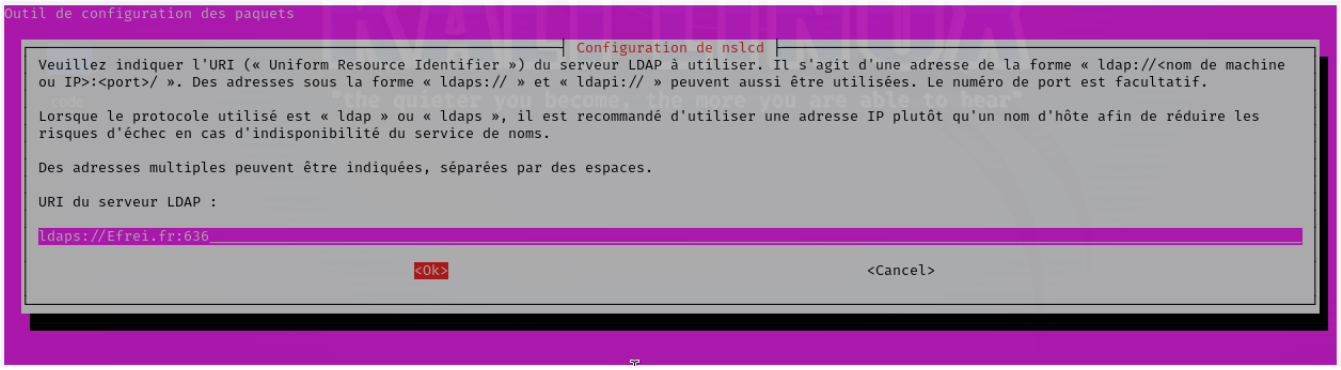
Dans ce troisième TP, nous visons à simplifier et centraliser la gestion des identités au moyen de LDAP, offrant aux utilisateurs la commodité d'utiliser un unique jeu d'identifiants pour se connecter à une variété de services, y compris SSH, et, dans les TP à venir, Apache et VPN. Pour y parvenir, nous allons exploiter les Pluggable Authentication Modules (PAM), un pilier des systèmes de type Unix, conçu pour centraliser et sécuriser l'authentification pour une multitude d'applications et de services. Ce TP est une opportunité pour vous de comprendre et d'implémenter des mécanismes d'authentification modernes et efficaces, essentiels dans le paysage technologique actuel.

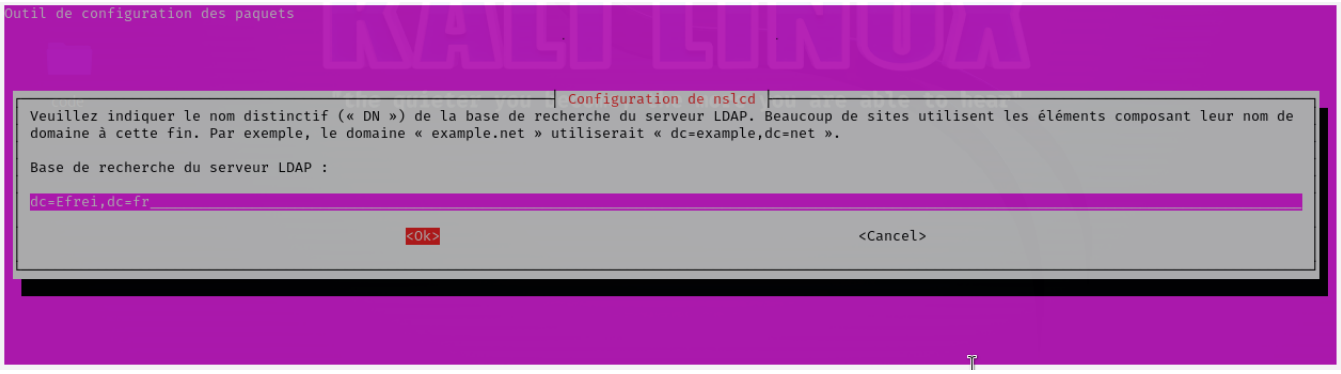


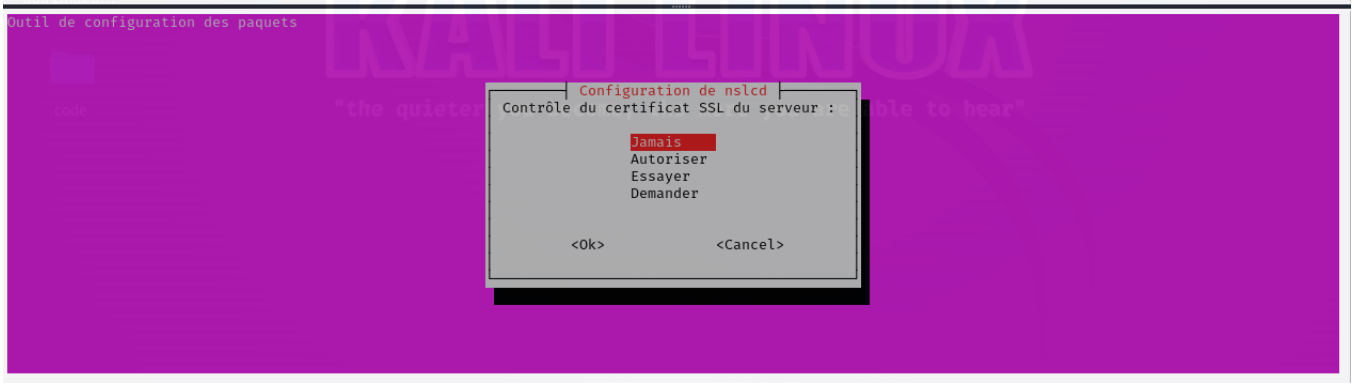
Configuration du PAM

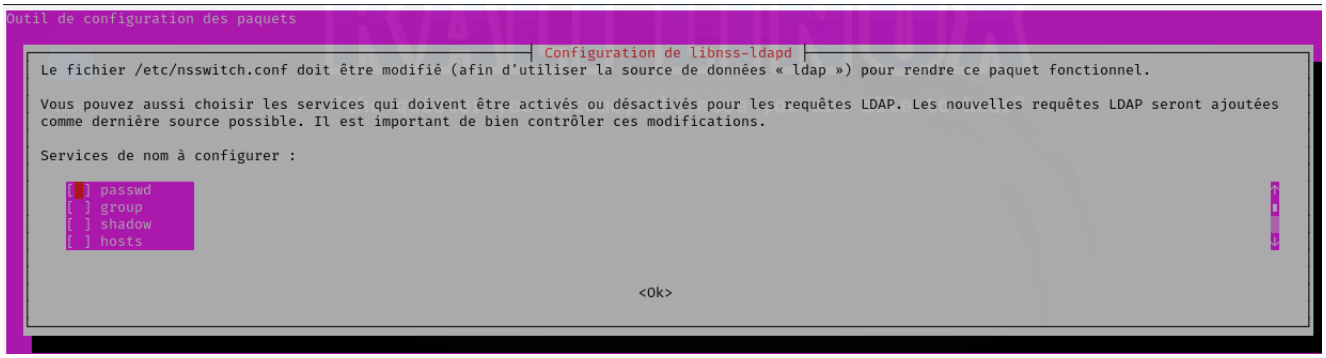
La première étape consiste à installer le package libnss-ldapd, en veillant à suivre les configurations spécifiques du serveur OpenLDAP. Parallèlement, d'autres packages tels que libpam-ldapd, nscd, nslcd, et nslcd-utils seront également installés. L'intégration de ces packages dans le système PAM d'un système Linux permet la configuration de services et d'applications pour authentifier les utilisateurs en utilisant les informations stockées sur un serveur LDAP.

```
pierre@Efrei:~$ sudo apt-get install libnss-ldapd
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  libpam-ldapd nscd nslcd nslcd-utils
Paquets suggérés :
  kstart
Les paquets suivants seront ENLEVÉS :
  libnss-ldap
Les NOUVEAUX paquets suivants seront installés :
  libnss-ldapd libpam-ldapd nscd nslcd nslcd-utils
0 mis à jour, 5 nouvellement installés, 1 à enlever et 2 non mis à jour.
Il est nécessaire de prendre 299 ko dans les archives.
Après cette opération, 1 019 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n]
```









Il est possible d'effectuer des ajustements manuels sur les fichiers de configuration.

Par exemple, l'ajout du certificat de l'autorité de certification dans le fichier nslcd.conf et une vérification minutieuse des informations saisies. En ce qui concerne la séquence de recherche, elle est définie dans le fichier nsswitch.conf. Ce dernier sert de fichier de configuration pour les bases de données systèmes (■ System Databases ■) et le service de noms (■ Name Service Switch ■), lesquels jouent un rôle clé dans l'identification et la récupération des comptes utilisateurs :

```
pierre@Efrei:/etc/ldap/ssl$ sudo nano /etc/nslcd.conf
pierre@Efrei:/etc/ldap/ssl$ sudo cat /etc/nslcd.conf
# /etc/nslcd.conf
# nslcd configuration file. See nslcd.conf(5)
# for details.

# The user and group nslcd should run as.
uid nslcd
gid nslcd

# The location at which the LDAP server(s) should be reachable.
uri ldaps://Efrei.fr:636

# The search base that will be used for all queries.
base dc=Efrei,dc=fr

# The LDAP protocol version to use.
#ldap_version 3

# The DN to bind with for normal lookups.
#binddn cn=annonymous,dc=example,dc=net
#bindpw secret

# The DN used for password modifications by root.
#rootpwmoddn cn=admin,dc=example,dc=com

# SSL options
#ssl off
tls_reqcert never
tls_cacertfile /etc/ldap/ssl/cert.pem

# The search scope.
#scope sub
```

```
pierre@Efrei:~$ sudo cat /etc/nsswitch.conf
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

passwd:         ldap files systemd
group:          ldap files systemd
shadow:         ldap files
gshadow:        files

hosts:          files dns
networks:       files

protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

netgroup:       nis
```

Et puis, nous testons la véracité des informations :

```
pierre@Efrei:/etc/ldap/ssl$ ldapsearch -H ldaps://Efrei.fr:636 -b 'dc=Efrei,dc=fr' -x uid=pierre.dupont -LLL
dn: uid=pierre.dupont,ou=users,dc=Efrei,dc=fr
objectClass: person
objectClass: top
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
uidNumber: 3002
gidNumber: 3002
homeDirectory: /home/pierre
loginShell: /bin/bash
uid: pierre.dupont
sn: dupont
cn: pierre dupont
mail:: cGllcnJlLmR1cG9udEBlZnJlaS5mciA=
```

Je remarque que l'email n'est pas bien rempli. J'en profite pour rappeler la mise à jour d'une entrée ldap sur le serveur et son résultat sur la machine cliente :

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ ldapmodify -W -D 'cn=admin,dc=Efrei,dc=fr'
Enter LDAP Password:
dn: uid=pierre.dupont,ou=users,dc=Efrei,dc=fr
changetype:modify
replace: mail
mail: pierre.dupont@efrei.fr

modifying entry "uid=pierre.dupont,ou=users,dc=Efrei,dc=fr"

^C
┌──(kali㉿kali)-[~]
└─$
```

```
pierre@Efrei:~$ ldapsearch -H ldaps://Efrei.fr:636 -b 'dc=Efrei,dc=fr' -x uid=pierre.dupont -LLL
dn: uid=pierre.dupont,ou=users,dc=Efrei,dc=fr
objectClass: person
objectClass: top
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
uidNumber: 3002
gidNumber: 3002
homeDirectory: /home/pierre
loginShell: /bin/bash
uid: pierre.dupont
sn: dupont
cn: pierre dupont
mail: pierre.dupont@efrei.fr
```

Ensuite, nous procéderons à la vérification de l'intégration des informations relatives aux utilisateurs et aux groupes dans les fichiers passwd et group.

```
pierre@Efrei:~$ getent passwd | grep pierre.dupont
pierre.dupont:*:3002:3002:pierre dupont:/home/pierre:/bin/bash
pierre:x:1001:1001:pierre dupont,,,:/home/pierre:/bin/bash
pierre@Efrei:~$ getent passwd | grep souheib
souheib.yousfi:*:3001:3001:souheib yousfi:/home/souheib:/bin/bash
pierre@Efrei:~$ getent group | grep teacher
teachers:*:3001:
pierre@Efrei:~$ getent group | grep student
students:*:3002:
```

Gestion de l'accès SSH : Autorisation pour les enseignants et interdiction pour les étudiants :)

Nous mettons l'accent sur la gestion de l'accès SSH, en ciblant particulièrement les enseignants. Notre démarche initiale consiste à garantir que tous les utilisateurs bénéficient d'un accès SSH, avant de limiter cet accès aux seuls enseignants. :

```
ubuntu@Efrei:~$ ssh pierre.dupont@localhost
pierre.dupont@localhost's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-100-generic aarch64)
```

```
pierre.dupont@Efrei:/$ exit
logout
Connection to localhost closed.
ubuntu@Efrei:~$ ssh souheib.yousfi@localhost
souheib.yousfi@localhost's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-100-generic aarch64)
```

Pour restreindre l'accès SSH exclusivement aux enseignants, il est nécessaire de mettre à jour la directive AllowGroups dans le fichier /etc/ssh/sshd_config, en y spécifiant le groupe ayant le droit d'accéder via SSH.

```
ubuntu@Efrei:~$ cat /etc/ssh/sshd_config | grep AllowGroups
AllowGroups teachers
```

Il est également nécessaire d'ajouter la ligne auth required pam_group.so au fichier /etc/-pam.d/sshd pour assurer la vérification de l'appartenance à un groupe spécifique. Le module par_group.so appartient à l'ensemble des modules PAM et est utilisé pour gérer les vérifications d'appartenance à des groupes lors de l'ouverture de sessions par les utilisateurs.

```
pierre@Efrei:~$ sudo cat  /etc/pam.d/sshd | grep 'auth required'
auth required pam_group.so
```

Pour finaliser la configuration, il est nécessaire de redémarrer le service.

Par la suite, nous procédons à la vérification de l'authentification pour les différents utilisateurs :

```
pierre@Efrei:~$ ssh pierre.dupont@localhost
pierre.dupont@localhost's password:
Permission denied, please try again.
pierre.dupont@localhost's password:

pierre@Efrei:~$ ssh souheib.yousfi@localhost
souheib.yousfi@localhost's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-100-generic aarch64)
```

Pour déterminer l'emplacement du module en fonction de votre système, exécutez la commande locate pam_group.so. Ensuite, il faut inclure dans votre rapport une brève description de quelques modules présents dans le répertoire /security/, avec une extension .so, qui sont typiquement localisés dans /usr/lib.
Pour l'utilisateur autorisé en SSH, il se peut que le répertoire personnel, tel que /home/souheib, ne soit pas présent. Pour remédier à cela, le module pam_mkhomedir.so est conçu pour créer automatiquement ce répertoire à la première connexion de l'utilisateur, si celui-ci n'existe pas déjà. Pour activer cette fonctionnalité, insérez la ligne correspondante dans le fichier /etc/-pam.d/sshd.

```
ubuntu@Efrei:~$ head -3 /etc/pam.d/sshd
# PAM configuration for the Secure Shell service
session required pam_mkhomedir.so
auth required pam_group.so
```

Connectez vous en ssh et vérifiez la présence de /home/souheib :

```
souheib.yousfi@Efrei:~$ ls /home/
souheib/ ubuntu/
```

♣ S.Y. ♣
Bon travail