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

Sprint 1 : Architectures et Infrastructures sécurisées d'entreprise

Objectif

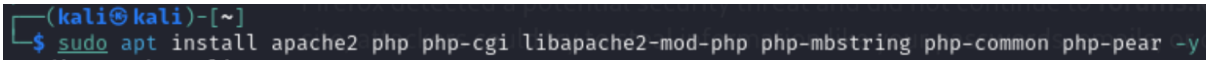
Á la fin de ce travail, en ayant accès au web ou en ligne de commande, vous devez :

1. Être capable d'installer et configurer un serveur OpenLDAP.
2. Connaître les principaux composants de OpenLDAP (slapd, fichier de configuration, etc.)
3. Connaître l'existence des commandes de maintenance de OpenLDAP (slapcat, slapadd, etc.)
4. Être capable d'utiliser les commandes usuelles de OpenLDAP (ldapsearch, ldapadd, ldapmodify, ldapdelete, etc.)
5. Être capable de décrire des objets dans le format LDIF, exemple de objectClass :
   (a) top : Cette classe est la super classe de toutes les autres classes. Elle est généralement utilisée comme classe parente pour toutes les autres classes.
   (b) organizationalUnit : Utilisée pour représenter une unité organisationnelle dans une structure d'organisation.
   (c) person : Utilisée pour définir des entrées représentant des personnes. Elle peut être utilisée pour stocker des informations telles que le nom, le prénom, l'email, etc.
   (d) organizationalPerson : Une sous-classe de 'person' qui étend les attributs autorisés pour les entrées représentant des personnes dans une organisation.
   (e) inetOrgPerson : Inclut les attributs supplémentaires pour stocker des informations spécifiques à Internet, tels que l'adresse email, le numéro de téléphone, @ip ....
   (f) posixAccount : Utilisée pour représenter un compte d'utilisateur compatible avec les systèmes Unix POSIX.
   (g) posixGroup : Utilisée pour représenter un groupe compatible avec les systèmes Unix POSIX.
   (h) organizationalRole : Utilisée pour représenter un rôle organisationnel, tel qu'un poste ou une fonction au sein de l'organisation.
   (i) device : Utilisée pour représenter des périphériques ou des équipements informatiques tels que des imprimantes, des routeurs, etc.
6. Être capable d'effectuer des recherches et d'écrire un filtre LDAP.
7. Être capable de connaître l'importance du protocole ldaps et l'utilisation des certificats pour l'authentification. La vérification se fait via Wireshark.

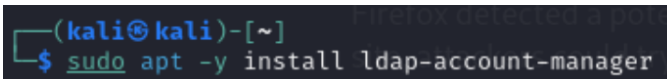
Résultat attendu pour le sprint 1

Un rapport qui comprend :

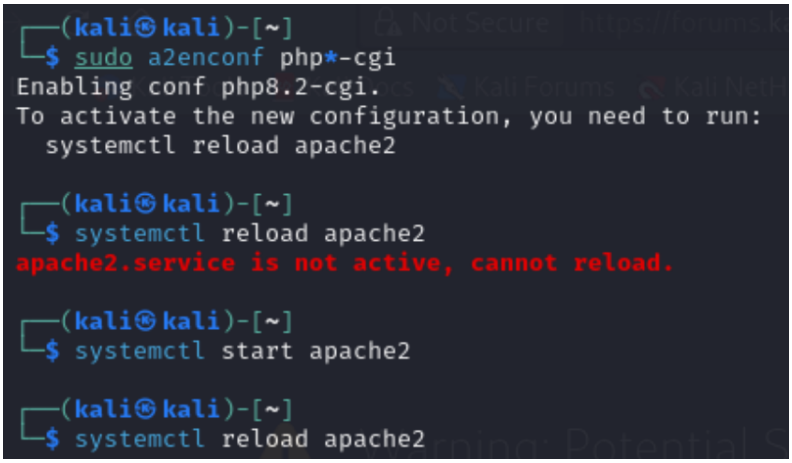
1. Une marche à suivre permettant l'installation et la configuration de OpenLDAP, en s'appuyant sur les captures d'écran des différentes étapes.
   (a) En mode classique (vous vous appuyez sur les captures du TP1 et TP2).
   (b) En mode graphique en installant le ldap Account Manager.
      i. Installation des packages reliés au web :



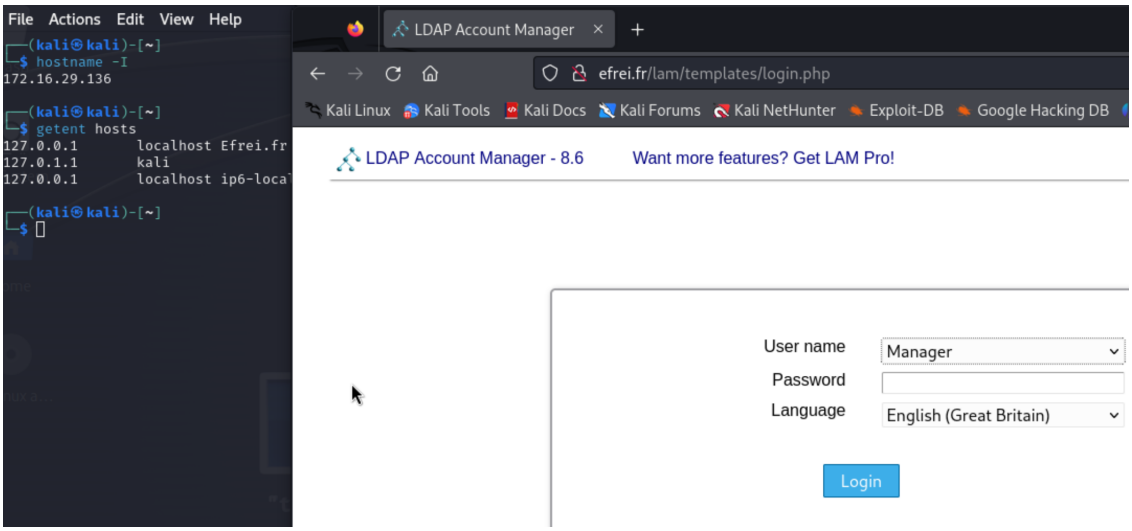
      ii. Installation de LAM :



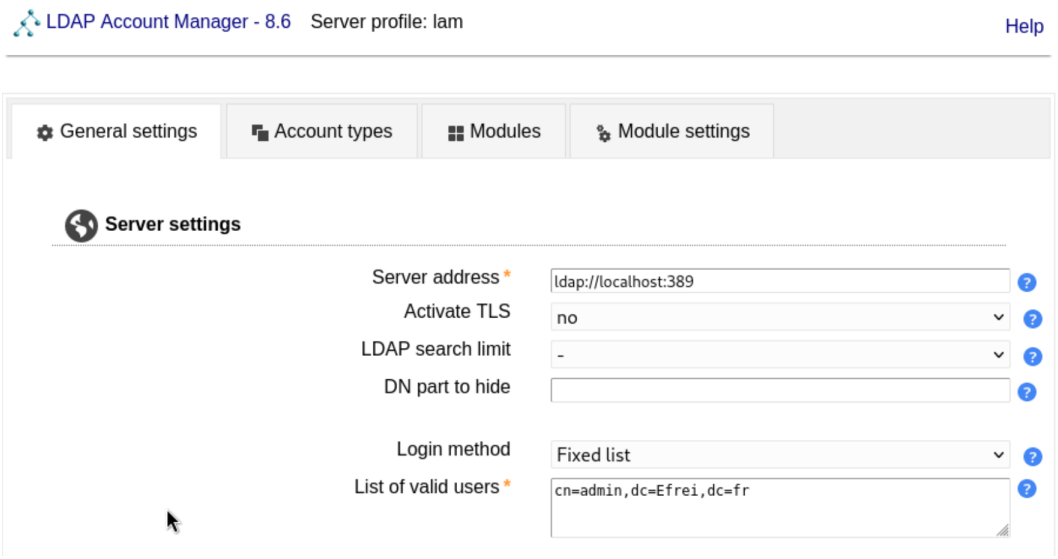
      iii. Activation de Apache :



      iv. Lancement de LAM :



v. Modification des informations par défaut du serveur :



vi. Faites les modifications nécessaires pour obtenir un résultat qui ressemble au réseau de notre DIT du TP1 :

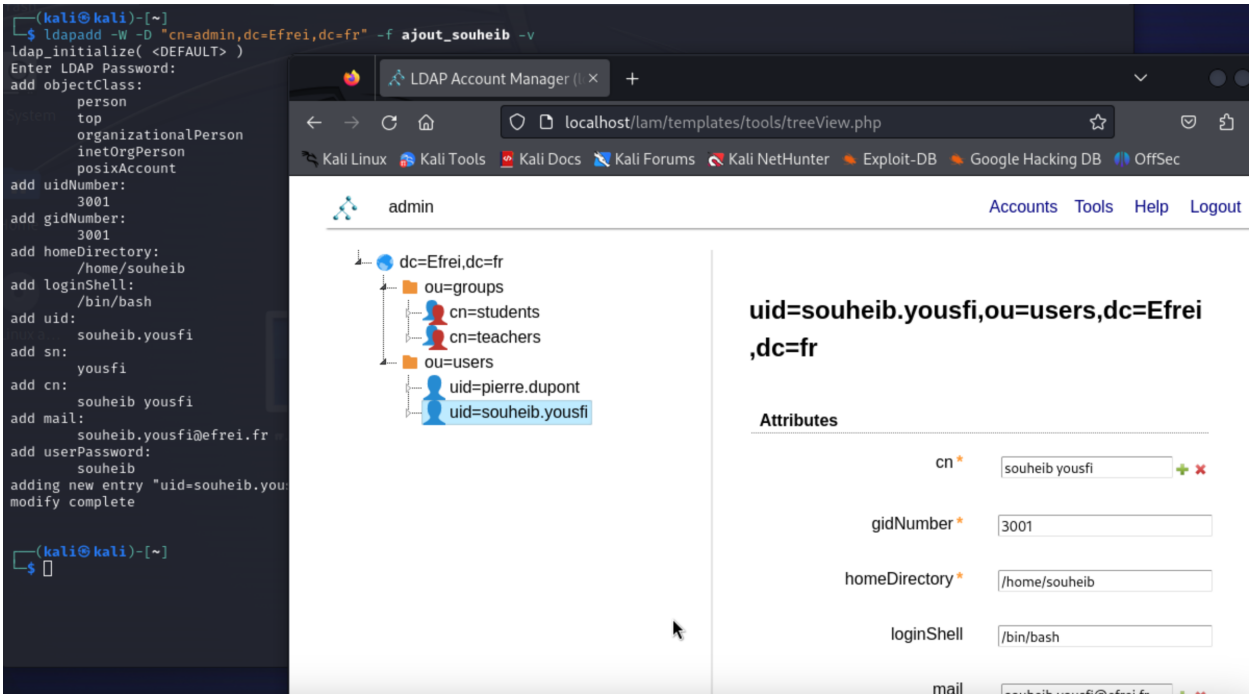


FIGURE 1 – Résultat du LAM

2. DIT :
   L'exécution des commandes sur le terminal s'applique aussi sur le serveur LAM, comme indiqué dans la figure 1. On lance par exemple le LDIF sur le terminal et en actualisant le LAM on s'aperçoit de la mise à jour.
   En s'appuyant sur le DIT du premier TP, faites les modifications nécessaires pour obtenir le DIT de la figure 2. C'est recommandé de faire des MAJ sur les informations existantes du DIT du premier TP, en s'appuyant sur vos informations personnelles.
   Chaque groupe d'étudiants est amené à créer une arborescence propre à lui, composée de tous les membres de ce groupe. Les informations nom, prénom, email, groupe, password, adresse postale de tous les utilisateurs doivent exister.

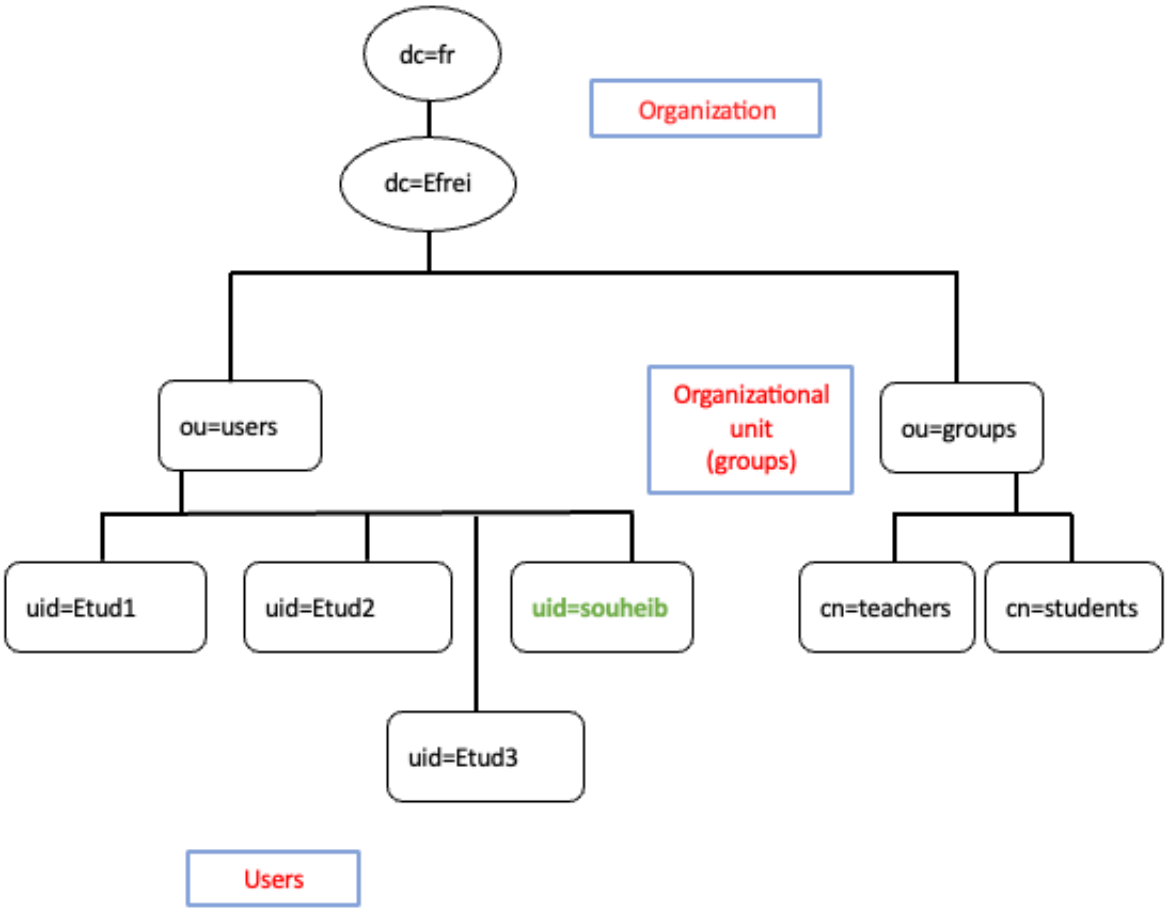


FIGURE 2 – DIT personnel

3. Testez la connexion LDAPS sur un utilisateur de votre choix avec le serveur Openldap en s'appuyant sur Wireshark. N'oubliez pas de commenter vos captures écran.

♣ S.Y. ♣
Bon travail