M2-ESECURE Rezo
TP3: LDAP - Mail

Pierre Blondeau
Pierre.Blondeau@unicaen.fr

03/10/2012

1 Introduction

L'objectif de ce TP est de vous faire construire une infrastructure de messagerie basée sur un annuaire LDAP.

ATTENTION 1 : Au cours de ce tp lorsque vous rencontrerez le caractère "\" dans un fichier de configuration ou une ligne de commande, il s'agit uniquement d'un symbole signifiant que la "phrase" est trop longue pour être mise sur une seul ligne dans ce sujet.

ATTENTION 2 : Après chaque modification des fichiers de configuration, il faudra redémarrer ou recharger la configuration des services modifiés. Par exemple pour dovecot `/etc/init.d/dovecot restart`.

2 Marionnet

Pour ce TP, nous allons utiliser un réseau très simple avec une machine et un bridge. Configurer les machines avec les adresses IPs définis en cours et modifier le fichier /etc/hosts pour joindre les autres machines avec leurs noms de la forme NOM.info.

3 Annuaire LDAP

3.1 Installation et Configuration

Pour l'installation, rien de plus simple : `slapd` pour le serveur ldap et `ldap-utils` pour les outils.

```
apt-get install slapd ldap-utils
```

Lors de l'installation debian configure le serveur ldap avec les informations du système. Pour modifier cette configuration nous utiliserons les outils de debian :

```
dpkg-reconfigure slapd
```

L'interface va vous proposer de configurer le serveur slapd :

```
Voulez vous omettre la configuration d'OpenLDAP            -> non
Nom de domaine                                             -> NOM.info
Nom d'entité                                               -> NOM.info
2 x Mot de passe                                           -> ...
Format de base de données                                  -> HDB
Faut-il supprimer la base de données à la purge du paquets -> non
Faut il déplacer l'ancienne base de données                -> oui
Faut il autoriser le protocle LdapV2                       -> non
```

Dans des conditions réelles d'utilisation, pour plus de sécurité, il faudrait créer différents utilisateurs et ajouter des ACL qui leurs permettent de lire ou d'écrire dans certains champs en fonction de leurs besoins. Par exemple, si on utilise un CMS, il est intéressant de lui permettre de modifier le mot de passe de connexion sans pour autant lui donner tous les privilèges du compte `admin`.

3.2 Création d'utilisateurs

Nous allons maintenant créer les utilisateurs de notre annuaire. Pour cela, nous allons utiliser un fichier au format `ldif` et la commande `ldapadd`, exemple :

```
dn: ou=People,dc=NOM,dc=info
ou: People
objectClass: organizationalUnit

dn: uid=pierre,ou=People,dc=NOM,dc=info
uid: pierre
cn: Pierre BLONDEAU
sn: BLONDEAU
mail: pierre@NOM.info
userPassword: pierrepassword
telephoneNumber: 0000
roomNumber: 0000
initials: PB
objectClass: inetOrgPerson

dn: uid=NOM,ou=People,dc=NOM,dc=info
uid: NOM
cn: Prenom NOM
sn: NOM
mail: NOM@NOM.info
userPassword: NOMpassword
telephoneNumber: 0000
roomNumber: 0000
initials: IT
objectClass: inetOrgPerson
```

Ajoutez votre propre compte et celui de plusieurs de vos camarades en modifiant le NOM.

```
ldapadd -h localhost -x -D "cn=admin,dc=NOM,dc=info" \
    -w password -f utilisateur.ldiff
```

Vérifiez le résultat avec `ldapsearch`. Vous pourriez également le faire avec des outils graphiques comme luma, JXplorer ou GQ.

```
ldapsearch -h localhost -x -D "cn=admin,dc=NOM,dc=info" \
    -b "dc=NOM,dc=info" -w password -LLL
```

3.3 Modification des utilisateurs

Nous allons maintenant découvrir l'outil `ldapmodify`. Voici la structure d'un fichier :

```
dn: uid=pierre,ou=People,dc=NOM,dc=info
changetype: modify
replace: telephoneNumber
telephoneNumber: 7343
-
replace: roomNumber
roomNumber: 406
-
add: title
title: ASR
-
delete: initials
```

Modifiez les numéros de téléphone par des numéros aléatoires et les numéros de salle par la salle de TP. Ajoutez vous le titre d'"ETUDIANT" et supprimez les initiales de tous les utilisateurs.

```
ldapmodify -h localhost -x -D "cn=admin,dc=NOM,dc=info" \
    -w password -f utilisateur.lmodif
```

Vérifiez le résultat.

4 Installation du logiciel IMAP et POP3

Vous utiliserez le logiciel dovecot comme Mail Delivery Agent. Nous allons commencer par créer un nouvel utilisateur :

```
groupadd -g 5000 vmail
useradd -g vmail -u 5000 vmail -d /home/vmail -m
```

Puis installer dovecot avec le support de IMAP et de POP :

```
apt-get install dovecot-imapd dovecot-pop3d
```

4.1 Configuration de Dovecot

Nous allons maintenant configurer dovecot. On commence par modifier le fichier /etc/dovecot/dovecot.conf

```
protocols = imap pop3
listen = *
disable_plaintext_auth = no
log_timestamp = "%Y-%m-%d %H:%M:%S "
login_greeting = NumETU Mail Serveur.
mail_location = maildir:/home/vmail/%d/%n/Maildir:\
    INBOX=/home/vmail/%d/%n/Maildir:\
    INDEX=/home/vmail/%d/%n/Maildir/tmp/index
mail_uid = vmail
mail_gid = vmail
mail_privileged_group = vmail
protocol imap {
  imap_client_workarounds = outlook-idle delay-newmail
}

protocol pop3 {
  pop3_uidl_format = %08Xu%08Xv
  pop3_client_workarounds = outlook-no-nuls
}
protocol lda {
  postmaster_address = NOM@NOM.info
  auth_socket_path = /var/run/dovecot/auth-master
}
auth default {
  mechanisms = plain login
  passdb ldap {
    args = /etc/dovecot/dovecot-ldap.conf
  }
  userdb ldap {
    args = /etc/dovecot/dovecot-ldap.conf
  }
  user = root
  socket listen {
    master {
      path = /var/run/dovecot/auth-master
      mode = 0600
      user = vmail
      group = vmail
    }
    client {
      path = /var/spool/postfix/private/auth
      mode = 0660
      user = postfix
      group = postfix
    }
  }
}
```

ATTENTION : Respectez les espaces devant les "{"
ATTENTION : Vous spécifiez à dovecot qu'il propose une socket client pour l'authentification SMTP de postfix. Seulement, postfix n'est pas encore installé. Pour que votre serveur dovecot démarre correctement, installez postfix comme indiqué en début de partie 5 et revenez pour la suite.

4.2 Couplage avec l'annuaire LDAP

On indique ensuite à dovecot comment il doit utiliser le serveur LDAP en éditant le fichier /etc/dovecot/dovecot-ldap.conf

```
hosts = 127.0.0.1
auth_bind = yes
ldap_version = 3
base = ou=People,dc=NOM,dc=info
user_filter = (&(objectClass=inetOrgPerson)(mail=%u))
pass_attrs = mail=user,userPassword=password
pass_filter = (&(objectClass=inetOrgPerson)(mail=%u))
```

4.3 Savez vous parler IMAP ?

Vous pouvez tester le comportement de votre logiciel IMAP en vous connectant directement dessus depuis une console du serveur ou depuis le poste client :

```
telnet localhost 143
ou
telnet 192.168.56.2 143
...
a00 LOGIN username password
...
a01 LIST * *
...
a02 LOGOUT
```

5 Installation du logiciel SMTP

Vous avez des boîtes, vous pouvez vous connecter dessus. Maintenant, il faut pouvoir leur transférer des messages. C'est le rôle du Mail Transport Agent. L'un des plus utilisé est postfix :

```
apt-get install postfix postfix-ldap
```

L'interface va vous proposer de configurer le serveur postfix :

```
Configuration type du serveur de messagerie  -> Site internet
Nom de courrier                              -> NOM.info
```

Si vous êtes en train de configurer dovecot, vous pouvez y retourner.

5.1 Configuration de Postfix

Nous allons maintenant configurer Postfix. On commence avec le fichier /etc/postfix/main.cf

```
smtpd_banner = $myhostname ESMTP $mail_name (Debian/GNU)
biff = no
append_dot_mydomain = no
readme_directory = no
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_use_tls=yes
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache
myhostname = NOM.info
alias_maps = hash:/etc/aliases
```

```
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = localhost
relayhost =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
virtual_mailbox_domains = NOM.info
virtual_mailbox_maps = ldap:/etc/postfix/ldap-accounts.cf
virtual_alias_maps = ldap:/etc/postfix/ldap-accounts.cf
virtual_mailbox_base = /home/vmail
dovecot_destination_recipient_limit = 1
virtual_transport = dovecot
virtual_uid_maps = static:vmail
virtual_gid_maps = static:vmail
```

5.2 Couplage avec le logiciel IMAP

C'est dovecot qui va faire le Mail Delivery Agent pour postfix. C'est à dire déposer les messages dans la boîte des destinataires de messages locaux. Il faut donc ajouter à la fin du fichier /etc/postfix/master.cf la ligne :

```
# Dovecot LDA
dovecot   unix  -       n       n       -       -       pipe
  flags=DRhu user=vmail:vmail argv=/usr/lib/dovecot/deliver -d $recipient
```

5.3 Couplage avec l'annuaire LDAP

Pour que le serveur puisse tester que les adresses existent vraiment, il doit pouvoir faire des requêtes dans LDAP. Il faut créer le fichier /etc/postfix/ldap-accounts.cf

```
server_host = localhost
port = 389
version = 3
search_base = ou=People,dc=NOM,dc=info
query_filter = (mail=%s)
result_attribute = mail
```

5.4 Savez vous parler SMTP ?

Comme pour IMAP, vous pouvez tester votre logiciel de transport de courrier en vous connectant directement dessus depuis une console du serveur. Les commandes suivantes devraient vous aider à comprendre le protocole et à le parler partiellement. Les réponses du serveur SMTP ne sont pas toutes transcrites ici. Si vous ne respectez pas le protocole, le code de retour vous l'indiquera par un numéro et un commentaire.

```
$ telnet IP 25
Trying IP...
Connected to IP.
Escape character is '^]'.
220 server ESMTP
EHLO NOM.info
MAIL FROM: <NOM1@NOM.info>
RCPT TO: <NOM2@NOM.info>
DATA

From: une adresse
To: une autre adresse
Subject: un sujet
Date: une date

La ligne vide est obligatoire.
Pour terminer la session, on met
```

```
un point "." seul.
.
```

6 Avec un client de messagerie

Sur le poste client, configurer un Mail User Agent comme Thunderbird ou Evolution pour vous connecter sur le serveur de mail et faire des tests.

7 Installation d'un webmail

Pour utiliser un webmail, il faut installer un serveur web et une base de données.

```
apt-get install apache2 php5 mysql-server php5-mysql
```

Il faut ensuite télécharger l'application du webmail. Nous installerons Roundcube. Téléchargez le dans /usr/src, décompressez le avec tar zxvf et lisez le fichier INSTALL pour l'installer. Vérifiez que vous pouvez envoyer et recevoir des mails après l'installation.

8 Sécurisation du serveur

8.1 Chiffrement des mots de passe

Lorsque vous consultez le serveur LDAP avec le compte admin, vous pouvez voir les mots de passe en claire. Utiliser l'outil slappasswd pour chiffrer votre mot de passe, puis l'outil ldapmodify pour modifier votre mot de passe dans l'annuaire.

Comment dovecot fait il pour se connecter une fois le mot de passe chiffré ?

8.2 Configuration SSL

L'utilisation du transport SSL permet d'obtenir 2 choses :
– La sécurisation de la phase d'authentification
– La protection des messages
Évidemment, la protection des messages n'est valable que pour ceux échangés entre les utilisateurs du même serveur. Ce n'est pas valable pour les messages qui sont reçu ou émis vers des serveurs tiers.

8.2.1 Génération d'un certificat

Nous allons maintenant générer des certificats serveurs auto-signés.

```
openssl req -new -x509 -days 3650 -nodes -out /etc/ssl/certs/tp.cert -keyout /etc/ssl/private/tp.key
```

8.2.2 Utilisation du certificat généré

Configurez dovecot pour fait du IMAPS et du POPS, postfix pour faire du SMTPS et apache pour faire du HTTPS

8.2.3 Test des logiciels

Comme pour les parties « en clair » des protocoles HTTP, IMAP et SMTP, vous pouvez tester vos serveurs sécurisés « à la main ». La seule différence c'est que vous n'utilisez pas la commande `telnet` pour vous connecter mais la commande `openssl`.

```
openssl s_client -host localhost -port 443 # HTTPS
openssl s_client -host localhost -port 465 # SMTPS
openssl s_client -host localhost -port 993 # IMAPS
openssl s_client -host localhost -port 995 # POPS
```

8.3 Système de limitation de spam (facultatif)

Mettez en place de systèmes comme SPF ou DKIM.

8.4 Acl LDAP (facultatif)

Interdisez l'accès anonyme à votre annuaire. Créez un utilisateur qui permet à dovecot, postfix et roundcube d'authentifier les utilisateurs.

8.5 Antivirus et Antispam (facultatif)

Pour ceux qui ont le temps, vous pourrez essayer de mettre en place un antivirus (ClamAV) et un antispam (SpamAssassin ou dspam).

8.5.1 Test de l'installation

Les logiciels antivirus et antispam sont normalement configurés pour répondre de manière positive en utilisant tous leurs tests lorsqu'on leur envoie des messages contenant une chaîne particulière.

Pour l'antispam, cette chaîne est le *GTUBE (Generic Test for Unsolicited Bulk Email)*. Envoyez un message contenant la chaîne de caractères suivante :

```
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X
```

Pour l'antivirus, il s'agit du fichier *EICAR*[1] *Standard Anti-Virus Test File* qui peut aussi se présenter sous une simple chaîne de caractère dans votre message de test :

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

1. European Institute for Computer Antivirus Research