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

TP2 : Architectures et Infrastructures sécurisées d'entreprise

Introduction

Ce deuxième TP est axé sur l'expérience pratique et comment on assure une communication chiffrée entre le client LDAP et le serveur LDAP. Lorsque l'on utilise l'authentification simple, le mot de passe est transmis en clair au serveur. Il est donc crucial de sécuriser le canal de communication en utilisant le TLS (Transport Layer Security). La sécurisation dans notre cas de figure s'appuie sur l'activation de l'accès ldaps.

1. Création des certificats.
2. Configuration du client.
3. Comparaison ldap et ldaps.

Création des clés et des certificats :

Les certificats générés seront enregistrés sous le dossier /home/kali/Desktop/Cert. La commande openssl permet de générer une clé privée ainsi qu'un certificat à partir de cette clé. Dans notre cas de figure, nous générons une clé et un certificat auto-signé à partir de cette clé.

```
┌──(kali㉿kali)-[~/Desktop/Cert]
└─$ sudo openssl genpkey -algorithm RSA -out server-key.pem
...+++++
.................................+++++
```

```
┌──(kali㉿kali)-[~/Desktop/Cert]
└─$ sudo openssl req -new -key server-key.pem -out server-csr.pem
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:France
Locality Name (eg, city) []:Paris
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Efrei
Organizational Unit Name (eg, section) []:RS
Common Name (e.g. server FQDN or YOUR name) []:Efrei.fr
Email Address []:serveur@efrei.fr

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

```
┌──(kali㉿kali)-[~/Desktop/Cert]
└─$ sudo openssl x509 -req -in server-csr.pem -signkey server-key.pem -out server-cert.pem
Signature ok
subject=C = FR, ST = France, L = Paris, O = Efrei, OU = RS, CN = Efrei.fr, emailAddress = serveur@efrei.fr
Getting Private key
```

Le serveur ldap doit avoir accès aux certificats et à la clé du serveur. Nous mettons les droits restrictifs pour Openldap :

```
┌──(kali㉿kali)-[~/Desktop/Cert]
└─$ sudo chown openldap:openldap server-cert.pem

┌──(kali㉿kali)-[~/Desktop/Cert]
└─$ sudo chown openldap:openldap server-key.pem

┌──(kali㉿kali)-[~/Desktop/Cert]
└─$ sudo chmod 400 server-key.pem
```

La configuration de slapd pour qu'il trouve le certificat se fait via un fichier LDIF. Le fichier cert.ldif informe slapd qu'il y aura une modification (changetype : modify) sur la racine config pour la déclaration des certificats et de la clé du serveur.

```
┌──(kali㉿kali)-[~/Desktop/Cert]
└─$ cat cert.ldif
dn: cn=config
changetype: modify
replace: olcTLSCACertificateFile
olcTLSCACertificateFile: /home/kali/Desktop/Cert/server-cert.pem
-
replace: olcTLSCertificateFile
olcTLSCertificateFile: /home/kali/Desktop/Cert/server-cert.pem
-
replace: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /home/kali/Desktop/Cert/server-key.pem
-
replace: olcTLSVerifyClient
olcTLSVerifyClient: never
```

Pour exécuter ces changements, la commande ldapmodify est utilisée. En effet, la configuration du serveur ne peut être modifiée que par l'utilisateur root du système. La solution réside dans le protocole ldapi : utilise un unix socket au lieu du réseau et qui permet de déléguer l'authentification au système Linux. Essayons d'effectuer cette modification avec la commande ci-après. Il est important de noter, on exécute la commande avec sudo.

```
┌──(kali㉿kali)-[~/Desktop/Cert]
└─$ sudo ldapmodify -QY EXTERNAL -H ldapi:/// -f cert.ldif
modifying entry "cn=config"

┌──(kali㉿kali)-[~/Desktop/Cert]
└─$ cat /etc/ldap/slapd.d/cn=config.ldif
cat: '/etc/ldap/slapd.d/cn=config.ldif': Permission denied

┌──(kali㉿kali)-[~/Desktop/Cert]
└─$ sudo !!

┌──(kali㉿kali)-[~/Desktop/Cert]
└─$ sudo cat /etc/ldap/slapd.d/cn=config.ldif
# AUTO-GENERATED FILE - DO NOT EDIT!! Use ldapmodify.
# CRC32 7b16692e
dn: cn=config
objectClass: olcGlobal
cn: config
olcArgsFile: /var/run/slapd/slapd.args
olcLogLevel: none
olcPidFile: /var/run/slapd/slapd.pid
olcToolThreads: 1
structuralObjectClass: olcGlobal
entryUUID: 940b9d1c-5914-103e-86b5-21be3e1b4165
creatorsName: cn=config
createTimestamp: 20240206082214Z
olcTLSCACertificateFile: /home/kali/Desktop/Cert/server-cert.pem
olcTLSCertificateFile: /home/kali/Desktop/Cert/server-cert.pem
olcTLSCertificateKeyFile: /home/kali/Desktop/Cert/server-key.pem
olcTLSVerifyClient: never
entryCSN: 20240209121402.141486Z#000000#000#000000
modifiersName: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
modifyTimestamp: 20240209121402Z
```

Finalement, le fichier /etc/default/slapd est modifié pour lui ajouter la méthode d'accès ldaps et de redémarrer le service :

```
┌──(kali㉿kali)-[~/Desktop/Cert]
└─$ cat /etc/default/slapd | grep "SLAPD_SERVICES"
# SLAPD_SERVICES="ldap://127.0.0.1:389/ ldaps:/// ldapi:///"
SLAPD_SERVICES="ldap:/// ldapi:/// ldaps:///"

┌──(kali㉿kali)-[~/Desktop/Cert]
└─$ sudo service slapd restart
```

Le serveur en mode secure :) est maintenant en écoute sous le port 636 :

```
┌──(kali㉿kali)-[~/Desktop/Cert]
└─$ sudo netstat -laptun | grep slapd
tcp        0      0 0.0.0.0:389             0.0.0.0:*               LISTEN      53214/slapd
tcp        0      0 0.0.0.0:636             0.0.0.0:*               LISTEN      53214/slapd
tcp6       0      0 :::389                  :::*                    LISTEN      53214/slapd
tcp6       0      0 :::636                  :::*                    LISTEN      53214/slapd
```

```
┌──(kali㉿kali)-[~/Desktop/Cert]
└─$ ps -ef | grep slap
openldap   53214       1  0 07:18 ?        00:00:00 /usr/sbin/slapd -h ldap:/// ldapi:/// ldaps:/// -g openldap -u openldap
-F /etc/ldap/slapd.d
kali       54417    4835  0 07:22 pts/2    00:00:00 grep --color=auto slap
```

Configuration du client :

Vérification de l'authentification des différents clients :

```
┌──(kali㉿kali)-[~/Desktop/Cert]
└─$ ldapwhoami -x -D "uid=pierre.dupont,ou=users,dc=Efrei,dc=fr" -W
Enter LDAP Password:
dn:uid=pierre.dupont,ou=users,dc=Efrei,dc=fr

┌──(kali㉿kali)-[~/Desktop/Cert]
└─$ ldapwhoami -x -D "uid=souheib.yousfi,ou=users,dc=Efrei,dc=fr" -W
Enter LDAP Password:
dn:uid=souheib.yousfi,ou=users,dc=Efrei,dc=fr
```

On passe à la machine cliente d'un des utilisateurs de notre annuaire, par exemple pierre, et intégrons l'adresse de notre serveur (La configuration de la machine du client a été faite dans le TP1) :

```
┌──(kali㉿kali)-[~/Desktop/Cert]
└─$ hostname -I
192.168.56.20

┌──(kali㉿kali)-[~/Desktop/Cert]
└─$
```

```
pierre@Efrei:~$ getent hosts
127.0.0.1       localhost
127.0.1.1       ubuntu.myguest.virtualbox.org ubuntu
192.168.56.20   Efrei.fr
127.0.0.1       ip6-localhost ip6-loopback
pierre@Efrei:~$
```

Connexion non sécurisée :

La première étape est de vérifier que la machine cliente peut accéder au serveur ldap par la commande ldapsearch.

Vérifions tout d'abord le contenu de notre annuaire sur la machine cliente :

```
pierre@Efrei:~$ sudo slapcat
[sudo] password for pierre:
dn: dc=Efrei,dc=fr
objectClass: top
objectClass: dcObject
objectClass: organization
o: Efrei
dc: Efrei
structuralObjectClass: organization
entryUUID: 9ea4e8c2-5ad7-103e-897e-df3f05cf963d
creatorsName: cn=admin,dc=Efrei,dc=fr
```

Puis, testons la connexion non sécurisé sur la machine serveur :

```
pierre@Efrei:~/Desktop/cert$ ldapsearch -x -H ldap://192.168.56.20:389 -b 'dc=Efrei,dc=fr' '(sn=yousfi)' -LLL
dn: uid=souheib.yousfi,ou=users,dc=Efrei,dc=fr
objectClass: person
objectClass: top
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
uidNumber: 6001
gidNumber: 6001
homeDirectory: /home/souheib
loginShell: /bin/bash
uid: souheib.yousfi
sn: yousfi
cn: souheib yousfi
mail: souheib.yousfi@efrei.fr
mail: souheib.yousfi@efrei.net
```

Connexion sécurisée :

Il faut d'abord vérifier la connexion avec le serveur et de lui demander son certificat. La commande openssl s_client permet d'établir une connexion sécurisée avec le serveur, et afficher son certificat.

```
pierre@Efrei:~/Desktop/cert$ openssl s_client -showcerts -connect Efrei.fr:636 | head -n 2
depth=0 C = FR, ST = France, L = Paris, O = Efrei, OU = RS, CN = Efrei.fr, emailAddress = serveur@efrei.fr
verify error:num=18:self-signed certificate
verify return:1
depth=0 C = FR, ST = France, L = Paris, O = Efrei, OU = RS, CN = Efrei.fr, emailAddress = serveur@efrei.fr
verify return:1
CONNECTED(00000003)
```

Le certificat est ensuite envoyé par le serveur au biais de la commande scp :

```
┌──(kali㉿kali)-[~/Desktop/Cert]
└─$ sudo scp server-cert.pem pierre@192.168.56.15:/home/pierre/Desktop/cert/
pierre@192.168.56.15's password:
server-cert.pem                                               100% 1281   804.7KB/s   00:00
```

Ensuite, le fichier ldap.conf doit être modifié pour accepter l'accès en ldaps et ajouter le path du certificat. L'appel de la commande ldapsearch maintenant présente l'annuaire en accès sécurisé.

```
pierre@Efrei:~/Desktop/cert$ cat /etc/ldap/ldap.conf
#
# LDAP Defaults
#

# See ldap.conf(5) for details
# This file should be world readable but not world writable.

#BASE   dc=example,dc=com
#URI    ldap://ldap.example.com ldap://ldap-master.example.com:666
BASE    dc=Efrei,dc=fr
URI     ldaps://Efrei.fr:636
#SIZELIMIT      12
#TIMELIMIT      15
#DEREF          never

# TLS certificates (needed for GnuTLS)
#TLS_CACERT     /etc/ssl/certs/ca-certificates.crt
TLS_CACERT /home/pierre/Desktop/cert/server-cert.pem
```

```
pierre@Efrei:~/Desktop/cert$ ldapsearch -x -H ldaps://Efrei.fr:636 -b "dc=Efrei,dc=fr" "(sn=dupont)" -LLL
dn: uid=pierre.dupont,ou=users,dc=Efrei,dc=fr
objectClass: person
objectClass: top
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
uidNumber: 6002
gidNumber: 6002
homeDirectory: /home/pierre
loginShell: /bin/bash
uid: pierre.dupont
sn: dupont
cn: pierre dupont
mail: pierre.dupont@efrei.fr
```

Comparaison ldap et ldaps :

Caractéristique	LDAP	LDAPS
Chiffrement des données	Non chiffré	Chiffrement SSL/TLS des données
Intégrité des données	Aucune intégrité assurée pendant le transit	Intégrité assurée par SSL/TLS
Authentification du serveur	Non authentifié	Authentification du serveur par certificat SSL/TLS
Port par défaut	389 (non sécurisé)	636 (sécurisé)
Configuration côté serveur	Configuration standard	Configuration d'un certificat SSL/TLS
Exemples d'utilisation	Accés à l'annuaire	Accés à des données sensibles

♣ S.Y. ♣
Bon travail