

Master 2 SeCReTS  
Sécurité applicative  
**TP : Kerberos**

18 décembre 2018

Première partie  
**Généralités**

**1 Objectifs du TP**

L'objectif de ce TP est d'installer et configurer un serveur Kerberos et de déployer plusieurs services kerbérisés. En particulier, on utilisera Kerberos pour ouvrir une session locale et à distance sur une machine, s'authentifier sur un proxy et sur un serveur HTTP ou encore administrer des machines virtuelles en s'authentifiant via kerberos.

Ces manipulations se feront à l'aide de machines virtuelles et éventuellement de conteneurs LXC.

**2 Pré-requis**

Pour cette première partie, vous pouvez utiliser directement la machine virtuelle gateway1 ou créer un conteneur lxc sur celle-ci. Si vous faites le choix d'utiliser lxc, votre conteneur devra porter le nom kdc.secrets.com et être connecté à un bridge interne à gateway1. Ce conteneur devra être accessible depuis client1 (règles de routage + iptables).

### 3 Utilisation de lxc (facultatif)

Créez un réseau interne à gateway1 (bridge) nommé dmz-services. L'ip portée par le bridge sera 10.1.4.254 avec comme masque de sous réseau 255.255.255.0. Rendez cette configuration statique.

```
# /etc/systemd/network/dmz-services.netdev
[NetDev]
Name=dmz-services
Kind=bridge

# /etc/systemd/network/dmz-services.network
[Match]
Name=dmz-services

[Network]
Address=10.1.4.254/24
ConfigureWithoutCarrier=yes
```

Pour ceux qui ne disposent pas d'un accès internet, décompresser l'archive lxc-ubuntu-2018.tgz dans le repertoire /var/cache/lxc de gateway1 (tar xzvf /root/lxc-ubuntu-2018.tgz -C /var/cache/lxc/).

Ensuite, vous allez créer un conteneur ubuntu minimal avec la commande suivante :

```
$ lxc-create -n kdc.secrets.com -t ubuntu
```

Editez la configuration de votre conteneur pour définir statiquement son adresse IP. La configuration du conteneur se trouve dans /var/lib/lxc/kdc.secrets.com/config. Il doit notamment figurer les lignes suivantes :

```
lxc.net.0.type = veth
lxc.net.0.link = dmz-services
lxc.net.0.flags = up
lxc.net.0.ipv4.address = 10.0.4.11/24
lxc.net.0.ipv4.gateway = 10.0.4.254
```

Editez également la configuration ssh afin de permettre les connexions en root avec mot de passe. /var/lib/lxc/kdc.secrets.com/rootfs/etc/ssh/sshd\_config :

```
PermitRootLogin yes
```

Vous pouvez ensuite démarrer le conteneur (lxc-start -n kdc.secrets.com -d) puis vous connecter au conteneur en ssh et continuer la suite du TP (ssh root@10.1.4.11).

## Deuxième partie

# Manipulations de base

## 1 Installation du serveur

Installez les packages *krb5-kdc* et *krb5-admin-server* sur gateway1 (ou le conteneur kdc.secrets.com) en utilisant apt ou en prenant ceux présent dans *~/deb-kerberos*.

Si vous travaillez directement sur gateway1, rajoutez un alias IP sur l'interface intnet1.

```
# /etc/systemd/network/enp0s3.network
```

```
[Match]
```

```
Name=enp0s3
```

```
[Network]
```

```
Address=10.1.1.1/24
```

```
Address=10.1.1.11/24
```

Renseignez celle-ci dans **serveur DNS** sous le nom kdc.secrets.com, à défaut le fichier */etc/hosts*. Profitez en pour rajouter les entrées DNS pour client1.secrets.com et gateway1.secrets.com si ce n'est pas déjà fait. Si vous n'avez pas de serveur DNS, le fichier */etc/hosts* sur client1 et gateway1 doit ressembler à ça :

```
# /etc/hosts
```

```
127.0.0.1      localhost
```

```
10.1.1.1      gateway1.secrets.com gateway1
```

```
10.1.1.2      client1.secrets.com client1
```

```
10.1.1.11     kdc.secrets.com kdc
```

```
ou
```

```
10.1.4.11     kdc.secrets.com kdc
```

Dans quels fichiers se trouvent respectivement la configuration du serveur et du client Kerberos? Aidez vous des pages de manuel et de la documentation présente dans le répertoire */usr/share/doc/* ainsi que de la commande *dpkg*.

```
# Configuration du KDC
```

```
/etc/krb5kdc/kdc.conf
```

```
# Configuration du client
```

```
/etc/krb5.conf
```

Éditez la configuration du KDC pour définir le royaume SECRETS.COM et initialisez la base du KDC.

```
# /etc/krb5kdc/kdc.conf
[kdcdefaults]
    kdc_ports = 750,88

[realms]
    SECRETS.COM = {
        database_name = /var/lib/krb5kdc/principal
        admin_keytab = FILE:/etc/krb5kdc/kadm5.keytab
        acl_file = /etc/krb5kdc/kadm5.acl
        key_stash_file = /etc/krb5kdc/stash
        kdc_ports = 750,88
        max_life = 10h 0m 0s
        max_renewable_life = 7d 0h 0m 0s
        master_key_type = des3-hmac-sha1
        #supported_encetypes = aes256-cts:normal aes128-cts:normal
        default_principal_flags = +preauth
    }

# Initialisation de la base du KDC
kdb5_util create -s -r SECRETS.COM
```

En vous aidant toujours de la documentation, créez les principaux Kerberos suivant :

- host/kdc.secrets.com@SECRETS.COM
- host/client1.secrets.com@SECRETS.COM
- host/gateway1.secrets.com@SECRETS.COM
- alice@SECRETS.COM
- bob@SECRETS.COM
- bob/admin@SECRETS.COM

A quoi correspondent ces principaux ?

```
# kadmin.local -r SECRETS.COM
addprinc -randkey host/kdc.secrets.com@SECRETS.COM
addprinc -randkey host/gateway1.secrets.com@SECRETS.COM
addprinc -randkey host/client1.secrets.com@SECRETS.COM
addprinc alice@SECRETS.COM
addprinc bob@SECRETS.COM
addprinc bob/admin@SECRETS.COM
```

Après avoir créé la configuration cliente, ajouter ensuite le principal host/gateway1.secrets.com à la keytab de la machine virtuelle gateway1 (et host/kdc.secrets.com à la keytab du conteneur kdc.secrets.com si vous utilisez lxc) puis démarrez le KDC et ajoutez le au démarrage de la machine (ou du conteneur).

```
# /etc/krb5.conf
[libdefaults]
dns_lookup_realm = false
dns_lookup_kdc = false
default_realm = SECRETS.COM

[realms]
SECRETS.COM = {
    kdc = kdc.secrets.com:88
    admin_server = kdc.secrets.com
}

[domain_realm]
.secrets.com = SECRETS.COM
secrets.com = SECRETS.COM
```

```
ktadd host/kdc.secrets.com@SECRETS.COM
```

```
# systemctl enable krb5-kdc
# systemctl start krb5-kdc
```

Comment peut on valider que le KDC est bien démarré ?

```
systemctl status krb5-kdc
netstat -lnup
```

Qu'elle commande permet de lister le contenu d'une keytab ou d'un cache de ticket ? A l'aide de l'outil `kinit`, validez que les principaux des utilisateurs sont bien fonctionnels puis configurez la politique de mots de passe suivante pour l'utilisateur `alice` :

- longueur minimum : 5 caractères
- historique de mots de passe : 3
- nombre maximum d'erreur d'authentification : 5
- verrouillage du compte de 60 secondes
- 2 classes de caractères minimum
- changement de mot de passe tous les 60 jours

```
# klist -kt /etc/krb5.keytab
# kinit bob@SECRETS.COM
# klist
# kadmin.local -r SECRETS.COM
addpol -minlength 5 -history 3 -maxfailure 5 -minclasses 2 -lockoutduration 60
-maxlife "60 days" users
modify_principal -policy users alice
```

## 2 Configuration de kadmind

A quel endroit se trouve le fichier d'acl permettant l'administration distante du KDC ? Autorisez les principaux dont l'instance est `admin` à administrer le KDC.

```
# /var/lib/lxc/kdc.secrets.com/rootfs/etc/krb5kdc/kadm5.acl
/admin@SECRETS.COM *
```

Après avoir redémarré le service kadmin, connectez vous à distance depuis `client1` et le principal `bob/admin` pour ajouter la keytab `host/client1.secrets.com`.

```
# kadmin -r SECRETS.COM -p bob/admin@SECRETS.COM  
ktadd host/client1.secrets.com@SECRETS.COM
```

```
# klist -kt /etc/krb5.keytab
```

## 3 Authentification Kerberos locale et à distance

### 3.1 A distance via ssh

Créez le compte unix de l'administrateur bob dans le conteneur kdc sans lui attribuer de mot de passe puis configurez ssh pour accepter l'authentification via GSSAPI.

```
useradd -m -s /bin/bash bob
```

```
# /etc/ssh/sshd_config  
GSSAPIAuthentication yes
```

```
systemctl restart ssh
```

### 3.2 Localement via la pam krb5

```
apt-get install libpam-krb5
```

```
lxc-console -n kdc.secrets.com (ctrl + a q pour sortir)
```

## Troisième partie

# Kerberisation des services

## 1 Proxy Squid

Générez une keytab pour le service squid puis, en vous aidant des commentaires présents dans son fichier de configuration, paramétrez le proxy pour :

- Autoriser tout le monde à accéder au domaine cea.fr et tous ses sous-domaines
- Autoriser les utilisateurs authentifié (via Kerberos) à surfer sur internet
- Interdire tout le reste

```
# kadmin -r SECRETS.COM -p bob/admin@SECRETS.COM
addprinc -randkey HTTP/proxy.secrets.com@SECRETS.COM
ktadd -k /etc/squid/proxy.keytab HTTP/proxy.secrets.com@SECRETS.COM

# systemctl edit squid
[Service]
Environment=KRB5_KTNAME="/etc/squid/squid.keytab"

# /etc/squid/squid.conf
auth_param negotiate program /usr/lib/squid/negotiate_kerberos_auth -d -s
    HTTP/proxy.secrets.com@SECRETS.COM
auth_param negotiate children 20 startup=0 idle=1
auth_param negotiate keep_alive on
acl KRB5_AUTH proxy_auth REQUIRED
acl CEA dstdomain .cea.fr cea.fr
allow client CEA
allow client KRB5_AUTH
deny all
# systemctl restart squid
```

## 2 Serveur apache

Après avoir généré une keytab pour le service apache, paramétrez le serveur apache pour n'autoriser que les utilisateurs authentifié à accéder aux pages web.

```
<Directory /var/www/>
AuthType Kerberos
AuthName "Zone KERB"
KrbMethodNegotiate On
KrbMethodK5Passwd Off
KrbAuthRealms SECRETS.COM
KrbServiceName HTTP
Krb5KeyTab /etc/apache2/httpd.keytab
require valid-user
Options Indexes FollowSymLinks MultiViews
AllowOverride None
Order allow,deny
allow from all
</Directory>
```

### 3 Hyperviseur libvirt

Après avoir généré une keytab pour le service libvirt (libvirt/hypervisor.secrets.com), paramétrez le serveur libvirt pour autoriser l'authentification via kerberos.

### 4 Relation d'approbation

Créez un second serveur Kerberos qui gèrera le domaine SRVEXT.SECRETS.COM et effectuez les opérations suivantes :

- Supprimer le principal du proxy squid du KDC de SECRETS.COM
- Recréez le sur le KDC de SRVEXT.SECRETS.COM
- Établissez une relation d'approbation qui approuve SECRETS.COM sur SRVEXT.SECRETS.COM

Sans oublier d'adapter la configuration des clients, validez ensuite le bon fonctionnement de la relation d'approbation.