Chapitre 2 : Kerberos

Objectifs :

Ce chapitre présente la sécurité Kerberos. Elle apporte la sécurité des transactions réseaux et l'authentification unique (SSO).

Après avoir étudié le protocole, l'étudiant apprend concrètement comment mettre en œuvre Kerberos. Il apprend d'abord son installation, son administration et son utilisation.

Contenu

- Présentation de Kerberos.
- Le protocole Kerberos.
- L'exploitation.
- L'utilisation de services « kerbérisés ».
- Ateliers.

1. Présentation de Kerberos

1.1.La théorie

Kerberos est un protocole cryptographique dont le rôle essentiel est l'authentification d'entités dialoguant en réseau. Généralement on l'utilise aussi pour chiffrer les transactions réseaux. Il peut être une solution globale à la sécurité réseau. À partir du moment où un utilisateur s'est authentifié, il accède sous son identité à l'ensemble des services compatibles Kerberos. On parle de SSO (Single Sign Once) : l'utilisateur ne s'authentifie qu'une seule fois. Kerberos ne se charge que de l'authentification. Le droit d'accéder ou non à un service n'est pas de son ressort. Le protocole Kerberos a été développé au MIT dans le cadre du projet Athena (comme X-Window). Kerberos, contrairement à SSH ou SSL n'utilise pas la cryptologie à clé publique mais uniquement les méthodes de chiffrement classiques symétriques. Elle impose l'usage d'un serveur d'authentification, le KDC (Key Distribution Center).

1.2.Les applications prenant en charge Kerberos

Au début, pour qu'une application puisse utiliser Kerberos, il fallait modifier son code. Cette opération était appelée parfois « kerbérisation ». Actuellement, il suffit que l'application intègre l'API de sécurité réseau GSSAPI pour qu'elle soit de fait compatible Kerberos. L'implémentation Cyrus du protocole SASL utilisé notamment dans les logiciels de messagerie et LDAP prend en charge GSSAPI. Ainsi ces applications sont compatibles Kerberos.

Les applications Unix suivantes prennent en charge Kerberos

- Telnet

- Ftp
- Les R-commandes (rsh, rcp)
- SSH
- Web (Apache avec le module mod_auth_kerb, Firefox)
- Samba
- NFSv4
- PostgreSQL
- Les applications gérant le courrier électronique (Postfix, Cyrus Imap…)
- Thunderbird
- OpenLDAP

Remarque

Beaucoup d'autres systèmes ou applications prennent en charge Kerberos en dehors des systèmes Unix : Windows 2000 et les versions ultérieures, MacOsX, VMWare ESX Server, Cisco, Oracle ainsi que les applications Java.

1.3. Les particularités des distributions

Lors de l'élaboration de Kerberos, les États-Unis interdisaient l'exportation de logiciels de cryptographie. C'est pourquoi la distribution de référence, celle du MIT, n'a été disponible qu'aux USA. La plupart des distributions Linux ont utilisé la version Heimdal, provenant de Suède. Actuellement, les restrictions légales ont disparu. RedHat utilise toujours la version Kerberos du MIT. Debian offre le choix entre la version Heimdal et celle du MIT. Les anciennes versions SUSE utilisent la version Heimdal et les récentes celle du MIT.

Remarque :

Les systèmes Windows 2000 et suivants utilisent Kerberos en s'appuyant sur un code source différent du MIT et sur des normes différentes des systèmes Unix. Leur API, même si elle s'inspire de GSSAPI n'est pas compatible. Tout cela ne simplifie pas l'interopérabilité entre systèmes Unix et Windows.

1.4. Le protocole Kerberos

1.4.1. La théorie

Kerberos est un protocole cryptographique servant à l'authentification et au chiffrement de transactions réseau. Actuellement c'est la version 5 du protocole Kerberos qui est utilisée. Elle est normalisée par les instances d'Internet. Des applications utilisent encore la version 4. Le protocole se divise en deux phases :

- La connexion d'un utilisateur.

- L'utilisateur, via un logiciel client « kerbérisé », accède à un service.

L'authentification de l'utilisateur se matérialise concrètement par l'obtention d'un ticket. Après sa connexion, l'utilisateur détient un ticket appelé TGT (Ticket Granting Ticket) lui permettant ultérieurement d'obtenir des tickets pour chacun des services qu'il veut utiliser. Le ticket est l'objet que l'utilisateur transmet pour s'identifier. Il contient des informations le concernant et il est chiffré avec la clé de son correspondant. De son point de vue, le ticket est une donnée opaque.

1.4.2. Le protocole

- **Obtention du TGT**

L'utilisateur Pierre désire se connecter. Il envoie au service AS (Authentication Server) du KDC une requête en clair (AS_REQ) contenant son nom (son principal) ainsi que celui du serveur pour obtenir le ticket TGT. Celui-ci lui permettra ensuite de demander des tickets de services. Le serveur lui renvoie sa réponse (AS_REP). Elle contient le TGT ainsi qu'une clé de session (Kses_as) destinée à être utilisée dans les échanges ultérieurs avec le serveur. L'ensemble de ces informations est chiffré avec la clé de l'utilisateur (Kpierre). Le client, après déchiffrement, mémorise la clé de session et le TGT dans un tampon d'accréditation (credential cache).

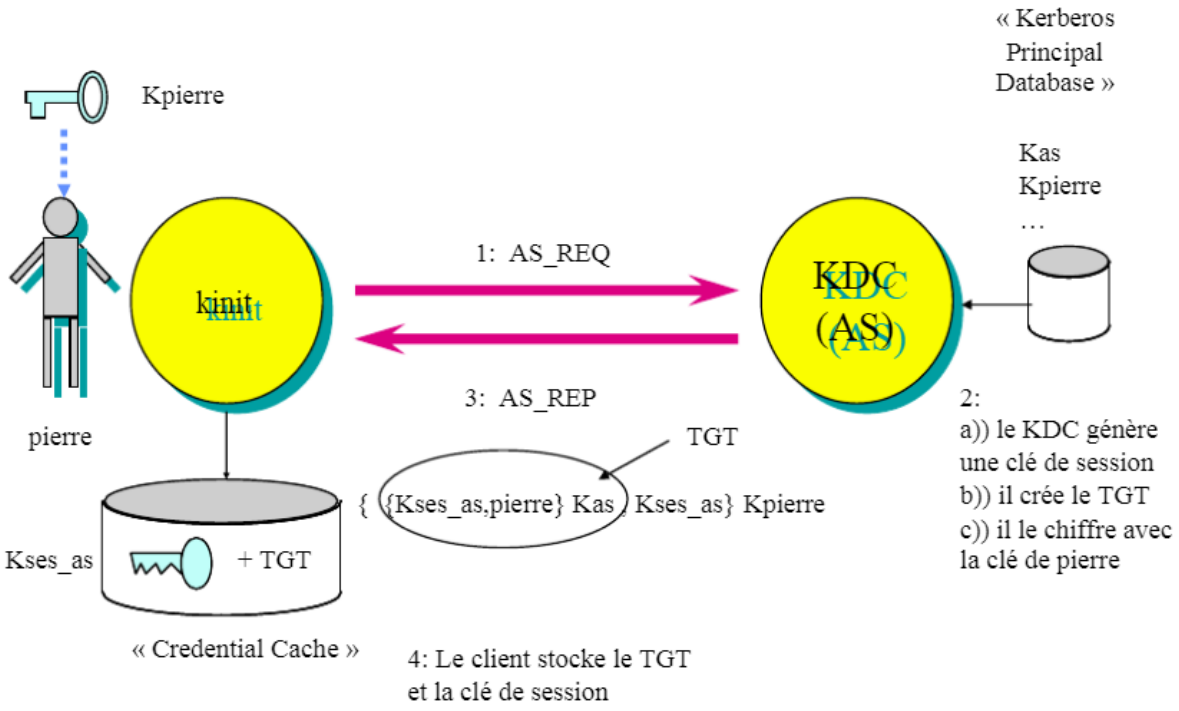

Fig. Obtention du TGT

Le TGT est chiffré avec la clé du service AS (Kas). Il contient les données suivantes :

- Une copie de la clé de session (Kses_as).
- Le nom (le principal) du client.

- L'adresse IP du client.
- Un horodatage.
- La durée de vie du ticket.

Remarque :

L'ensemble des messages est horodaté et les tickets ont une durée de vie limitée. Ceci afin d'éviter des attaques de type Replay. Des écarts importants d'horloge entre les ordinateurs sont interdits (par défaut de l'ordre de 5 mn). L'usage d'un système de synchronisation comme NTP est indispensable.

Le protocole

- **L'obtention d'un ticket de service**

Quand le client désire accéder à un service, il en fait la demande au serveur KDC par une requête TGS. Celle-ci contient le nom (le principal) du service demandé, le TGT et une donnée d'authentification (authenticator). Elle contient le nom (le principal) et un horodatage, le tout chiffré avec la clé de session (Kses_as) obtenue à l'étape précédente.

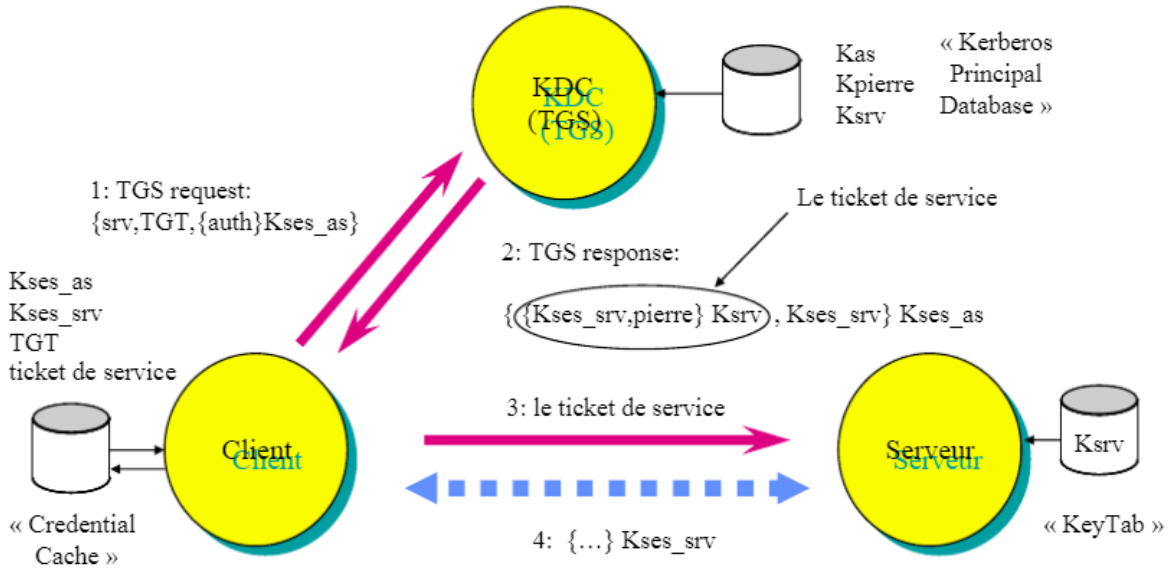

Fig. Accès à un service

Le serveur répond par une réponse TGS qui contient les éléments suivants :

- Le ticket de service.
- Une clé de session pour le service (Kses_srv).
- Le nom (le principal) du service.
- Une durée de vie pour le ticket.

Le tout chiffré avec la clé de service AS (kses_as).

- Le ticket de service est chiffré avec la clé du service (Ksrv). Il contient les données suivantes :

- Une copie de la clé de session pour le service (Kses_srv).
- Le nom (le principal) du client.
- L'adresse IP du client.
- Un horodatage.
- La durée de vie du ticket.

Ensuite, le client s'authentifie auprès du serveur offrant le service demandé en lui envoyant le ticket de service. Le serveur déchiffre le ticket et obtient une copie de la clé de session (Kses_srv). Cette clé de chiffrement symétrique lui sert ensuite pour dialoguer de manière confidentielle avec le client.

Remarque

Le protocole Kerberos ne décrit pas dans le détail ces dernières étapes (transmission du ticket de service et réponse du serveur). Elles sont spécifiques pour chaque application.

1.4.2. Principals et Realm

Dans une infrastructure Kerberos, chaque utilisateur et chaque service possède un nom, appelé « principal ». Un principal peut avoir une « instance » qui le qualifie.

Un domaine d'authentification Kerberos est appelé « Realm ». Un principal pleinement qualifié intègre le nom du Realm dont il fait partie.

1.4.3. Kerberos et le DNS

Pour un fonctionnement correct et à grande échelle de Kerberos, l'utilisation du DNS est conseillée. En effet, Kerberos peut utiliser le DNS comme service de résolution. Grâce a lui (via les enregistrements SRV), un service peut connaître le Realm auquel appartient un poste ou un domaine et quels sont les KDC qui le servent. Ainsi la configuration individuelle des clients n'est plus nécessaire.

1.5.Le savoir concret

Le protocole Kerberos 5

88/udp,

88/tcp Le service d'obtention de ticket.

749/tcp Le service kadmin (MIT et Heimdal).

754/tcp Le service de propagation de la base principale sur les KDC esclaves.

4444/udp La conversion de tickets krb5 en krb4.

Le protocole Kerberos

751/udp,

751/tcp Le service d'administration.

752/udp Le service de changement de mot de passe.

761/tcp Le service de changement de mot de passe.

Le protocole Kerberos 4

750/udp,

750/tcp Le service d'obtention de ticket.

464/udp L'ancien service de changement de mot de passe.

1.5.1. Les « principals »

Syntaxe

composant[/composant][/composant]…@Realm Syntaxe Générique (Krb5)

nom_de_l_utilisateur[/instance]@Realm Utilisateur

service/FQDN@Realm Service

nom[.instance]@Realm Syntaxe Kerberos 4

Exemples

pierre@DNS.ORG L'utilisateur pierre

paul/admin@DNS.ORG L'administrateur paul

host/venus.dns.org@DNS.ORG Les services de base de Venus

nfs/venus.dns.org@DNS.ORG Le service NFS de venus

Remarques :

- ✓ Les services de base intègrent telnet et les commandes remote (R-commandes).
- ✓ La gestion de Kerberos est simplifiée si les Realms correspondent aux domaines DNS.

L'exploitation

La théorie

Les étapes de la mise en œuvre de Kerberos

1. Faire les choix d'organisation.
   Choisir un nom pour le Realm.
   Déterminer le rôle de chaque ordinateur :
   - Serveur maître (KDC), il abrite la base de données Kerberos et les services AS, TGS et le service d'administration distante.
   - Serveur esclave (KDC secondaire), il contient une copie de la base de données Kerberos ainsi que les services AS et TGS.
   - Serveur abritant un service (SS).
   - Poste client.
   - Choisir le ou les administrateurs.
2. Synchroniser les horloges de tous les postes (KDCs, serveurs, client). Cette synchronisation est faite habituellement grâce à NTP.

3. Configurer le serveur Kerberos maître.

Spécifier le Realm d'appartenance et les KDC.

- Créer la base de données Kerberos.
- Créer le compte d'administration.
- Créer et installer les clés pour effectuer l'administration distance.
- Donner aux administrateurs les droits (les ACL) de gestion des principals.
- Démarrer les services : serveurs de tickets (AS et TGS) et administration distante.

4. Pour chaque ordinateur membre du Realm.
   Configurer le Realm d'appartenance et les adresses des KDC.
5. Pour chaque service.
   - Créer un principal identifiant le service.
   - Créer et installer les clés du service

Important : l'installation des clés doit être effectuée à partir du serveur abritant le service. L'outil d'administration à distance copiera un jeu de clés dans une base de données locale appelée « Keytab » et le double des clés sur le KDC.

6. Pour chaque utilisateur
   - Créer un principal identifiant l'utilisateur.
   - Saisir un mot de passe. La clé de l'utilisateur en dérivera et sera stockée dans la base de données Kerberos. Le mot de passe devra être mémorisé par l'utilisateur. Il servira de double de la clé.

Remarques :

- ✓ Dans la démarche présentée nous avons supposé que notre Realm était isolé. Dans une structure importante il est possible d'avoir plusieurs Realms. Dans ce cas, on configure des authentifications croisées.
- ✓ Les postes clients peuvent ne pas être configurés si l'on utilise les enregistrements SRV du DNS.