Compte rendue Kerberos

- Contexte

Kerberos est un protocole d'authentification réseau qui repose sur un mécanisme de clés secrètes et l'utilisation de tickets et non de mot de passe en clair, évitant ainsi le risque d'interception frauduleuse des mots de passe des utilisateurs. Il porte relativement bien son nom puisqu'il est chargé d'authentifier, d'autoriser et de surveiller les utilisateurs voulant accéder aux ressources et services de votre réseau. Il agit en chien de garde contre les intrus sur vos services réseau.

Afin de réaliser correctement l'authentification des différents protocoles principaux (un protocole est une entité présente dur le réseau définit par un identifiant unique), le protocole Kerberos fais appel à 3 acteurs différents :

- Le client : Utilisateur ou programme ayant besoin d'un service (ftp, mai l, web, etc) fourni par un serveur distant.
- Le serveur d'application : Il fourni le service demandé par le client aprè s que celui-ci se soit authentifié.
- Le serveur de distribution des clés KDC(Key Distribution Center) : Il per met
  l'authentification de tous les clients sur le réseau dont il a la responsabi lité

Kerberos se décompose en trois sous protocoles

- Service d'authentification : permet d'authentifier les clients
- Le service de délivrement de TGS : permet de fournir l'authentification auprès des serveurs d'application
- Service d'authentification Client / Serveur qui permet d'établir une communication sécurisée entre le client et le serveur d'applications

L'authentification Kerberos repose sur le principe que chaque client d'un rése au donné doit s'identifier sur un serveur global.Le client doit présenter au ser veur un ticket d'authentification que lui a préalablement fourni ce dernier.Tout client muni de ce ticket est considéré comme authentifié
sécurisation du réseau puisque aucune données d'authentification non chiffré e ne circule sur celui-ci.

Nous souhaitons crée une AD sur un parc informatique composer de 1 pc

sous Windows et 2 sur Ubuntu servers. Pour cela nous devons utiliser le protocole Kerberos couplet à LDAP.

192.168.100.23 192.168.100.25
192.168.100.27

- Tutoriel d’installation

Les informations utiles avant de commencer sont :

Pré-requis :

1 Windows serveur

2 Ubuntu

- Windows serveur domaine = fred.lan
- Nom complet du pc Windows serveur = rami.fred.lan
- Adresse ip de la première machine Ubuntu = 192.168.100.25

Une fois le domaine crée sur Windows server 2008 ont passé sur le premier Ubuntu.

On commence par mettre à jour Ubuntu avec :

- **Sudo apt-get update**

- **Sudo apt-get upgrade**

Pour la résolution de nom de domaine

- **/etc/resolv.conf**
- **Nameserver 192.168.100.23 (l'adresse IP de notre windows server)**
- **Search fred.lan (notre nom de domaine**
-

Nous allons maintenant passer l'IP de l'Ubuntu en statique :

- **Sudo nano /etc/network/interfaces** (afin de modifier le fichier interfaces)
- Apres INET supprimer le DHCP et remplacer par **STATIC**
- Ensuite il faut attribuer les IP du pc pour cela tapé à la suite :

  address 192.168.100.25

  netmask 255.255.255.0

  gateway 192.168.100.1

  dns-nameservers 192.168.100.23

Avant de passer à la suite ont redémarre le réseau

- **Sudo /etc/init.d/networking reload**
- **Sudo /etc/init.d/networking restart**
- **Sudo nano /etc/hosts**
- **A la suite du nom de votre machine taper .fred.lan**
- A la fin de cette page taper a la suite :

#DC Primaire

192.168.100.23 rami.fred.lan rami

- **Sudo apt-get install ntpdate**
- **Sudo nano /etc/default/ntpdate**
- Sur la ligne «NTPSERVERS= ‘’**192.168.100.23**‘’ » taper l’IP de windows server
- Sur la ligne << NTPOPTIONS=’’**-u**‘’>>

On ajuste le l’heure avec :

- **/usr/sbin/ntpdate-debian**

Installation de krberos :

- **Apt-get install krb5-user**
- Royaume par défaut : **fred.lan**
- Noms d’hôtes dans le royaume **: rami.fred.lan**
- Serveur administratif du royaume **: rami.fred.lan**

- Mode Opératoire

Ensuite on modifie le fichier krb5.conf :

- **Nano /etc/krb5.conf**
- **On remplace par :**

[libdefaults]

ticket_lifetime = 24000

default_realm = FRED.LAN

fowardable = true

proxiable = true

dns_fallback = no

#default_tkt_enctypes = des3-hmac-sha1 des-cbc-crc

#default_tgs_enctypes = des3-hmac-sha1 des-cbc-crc

[realms]

FRED.LAN = {

kdc = rami.fred.lan

default_domain = FRED.LAN

}

[domain_realm]

.fred.lan = RAMI.FRED.LAN

fred.lan = RAMI.FRED.LAN

[login]

krb4_convert = true

krb4_get-tickets = false

On crée maintenant un ticket de kerberos :

- **Sudo kinit –V Administrateur@FRED.LAN**

Et on vérifie :

- **Klist**

Si tous se passe bien Krbgt/FRED.LAN@FRED devrais répondre

On Install samba winbind

- **apt-get install samba winbind**

Et on modifie le fichier smb.conf

- **nano /etc/samba/smb.conf**

[global]

security = ADS

realm = FRED.LAN

workgroup = FRED

winbind separator = +

idmap uid = 10000 - 20000

idmap gid = 10000 - 20000

winbind enum users = yes

winbind enum groups = yes

template homedir = /home/%D%U

template shell = /bin/bash

client use spnego = yes

winbind use default domain = no

domain master = no

local master = no

preferred master = no

os level = 0

On tape **testparm** pour tester le paramètre saisi et enfin ont rejoint l'ad avec :

- **net ads join -U Administrateur -S rami.fred.lan**
- **il faudra saisir le mot de passe de l'Administrateur Windows server**

Si tous se passe bien Il vous sera indiqué que la machine ubuntu a bien rejoint le Domain.

Code oublier

Sudo apt-get install libpam-winbind libnss-winbind

Installer webmin

Syncroniser user samba

Lier l'ad « groupe user »

Copier le user administrateur et cree le meme que celui de ubuntu

Suivre tuto a partir du 7.

https://doc.ubuntu-fr.org/tutoriel/comment_ajouter_machine_ubuntu_dans_domaine_active_directory

« Attention fichier pam a modifier pas remplacer »