INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES CENTRE VAL DE LOIRE

Département Sécurité et Technologies Informatiques

Cryptograhie – TD7

Jérémy Briffaut <jeremy.briffaut@insa-cvl.fr>

Jean-Christophe Deneuville <jean-christophe.deneuville@insa-cvl.fr>

Lundi 1er octobre 2018

Exercice 1 Préparation

Récupérer les images serveur et client kerberos dans `/usr2/Images_Briffaut`

1. Mettre la mémoire de ces machines à 256Mo
2. Lancer le client et le serveur

Exercice 2 Fixer la configuration

Étapes à réaliser en tant que root (mot de passe azerty) sur les machines :

Serveur	Client
`#hostname server`	`#hostname client`
`#domainname exemplekrb.com`	`#domainname exemplekrb.com`
`#vim /etc/hosts` (fixer l'IP du client)	`#vim /etc/hosts` (fixer l'IP du serveur)
`#/etc/init.d/iptables stop`	`#/etc/init.d/iptables stop`
`#/etc/init.d/nfs restart`	

Exercice 3 Prise en main de kerberos (à réaliser sur le serveur)

Récupérer un ticket kerberos pour le principal admin/admin (mot de passe azerty) : `kinit admin/admin`.

Lister les tickets disponibles : `klist -e`

1. Quel est le type de ce ticket ?
2. Quel est le chiffrement utilisé ?
3. À qui appartient ce ticket ?
4. Quel est sa durée ?

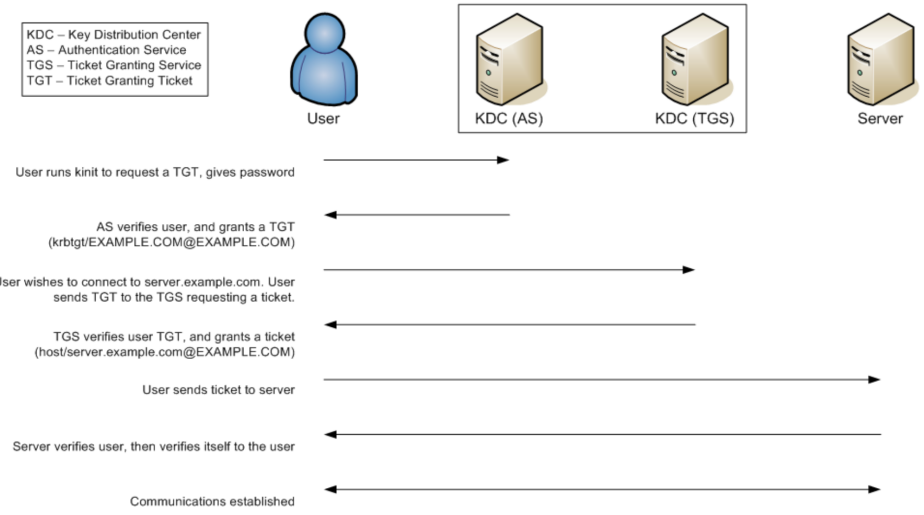
Lancer `wireshark` sur le serveur (écouter l'interface ethernet) et **le conserver jusqu'à la fin du TD !**

Exercice 4 Prise en main de kerberos (à réaliser sur le client)

Connectez-vous à l'interface d'administration de kerberos : `kadmin admin/admin`.

1. Quels sont les différentes actions possibles ? (commande `help`)
2. Lister les principaux disponibles : `listprincs`
3. Quels sont les différents types de principaux ?
4. Ajouter un principal : `addprinc user` puis `quit`.
5. Analyser les requêtes capturées par `wireshark`. Quel est le type des paquets kerberos envoyés par le client ?

6. Récupérer un ticket pour votre nouvel utilisateur :
   1. `kdestroy`
   2. `kinit user`
   3. `klist -e`
7. À quoi sert la commande `kdestroy` ?
8. Analyser les requêtes capturées par wireshark. Quel est le type des paquets kerberos envoyés par le client ? Quel est le type des requêtes et des réponses envoyées ?



Exercice 5 Configuration de NFSv4

Sur le serveur, entrez la commande : `mount --bind /home /export/home`. À quoi sert cette commande ?

Sur le client (correction d'un bug de fedora 8) :

— Éditer le fichier `/etc/sysconfig/nfs`, décommenter la ligne `SECURE_NFS=yes`

— Créer un lien vers une bibliothèque manquante : `ln -s /usr/lib/libgssapi_krb5.so.2 /usr/lib/libgssapi_krb5.so`

— Démarrer le service NFS et un service manquant :

  — `/etc/init.d/nfs start`

  — `rpc.gssd`

Exercice 6 Utilisation de NFSv4 (sur le client)

Monter le partage NFS : `mount server:/ /mnt/nfs -t nfs4 -o sec=krb5`

1. Analyser les réquêtes capturer par wireshark :
   a) Quel est le type des paquets kerberos envoyés par le client ?
   b) Quel est le type des requêtes et des réponses envoyées ?
2. Sur le serveur, analyser le fichier `/var/log/krb5kdc.log`

Exercice 7 Partie supplémentaire

1. Configurer le client pour autoriser la connexion via kerberos (pam).
2. Configurer le client pour automonter la partition NFS dans `/home` (`automount` ou `/etc/fstab`)