MINISTERE DE L'ENSEIGNEMENT SUPERIEURE ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE DE BEJAIA

Faculté des sciences exactes

Département d'informatique

MEMOIRE DE FIN DE CYCLE

En vue de l'obtention du diplôme de Master professionnel en Informatique

Option : Administration et Sécurité des Réseaux

Thème :

La Sécurité des Réseaux Informatique à Base de Kerberos

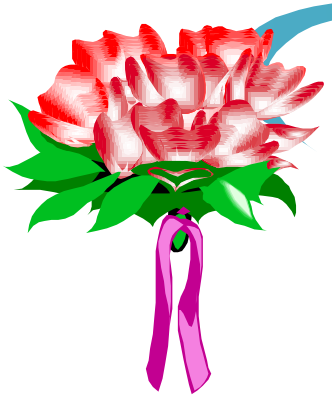
***Présenté par*:**

- BOUFOUDI Siham
- BRAHAMI Nabila

Devant le jury composé de :

Président :	***M*^r^ SADI Mustapha**
***Examinateur 1* :**	**D^r^ ATMANI Mouloud, Docteur, Cerist Bejaïa**
***Examinatrice 2* :**	**M^elle^ MORDJI Zouweyna, Doctorante, université de Bejaïa**
***Encadreur* :**	**D^r^ AMAD Mourad, MCB, université de Bejaïa**
Co-encadreur :	**M^r^ KHENOUS Lachemi, MAA, université de Bejaïa**

Promotion 2014-2015



Remerciements

Au terme de ce travail, nous tenons à remercier **Dieu** le tout puissant de nous avoir donné le courage, la volonté et la patience pour achever ce travail.

Nous avons l'honneur et le plaisir de présenter notre profonde gratitude et nos sincères remerciements à notre encadreur M^{r} AMAD Mourad, pour sa précieuse aide, ses orientations et le temps qu'il nous a accordé pour notre encadrement.

Nous remercions profondément tous les enseignants qui nous ont encouragé et soutenus pendant notre parcoure universitaire.

Nos remerciements les plus sincères et les plus profonds sont adressés au personnel de Département Informatique.

Nos remercions également tous ceux qui ont contribué de prêt ou de loin à l'achèvement de notre Travail.

DEDICACES

Je dédie ce modeste travail à :

Mes très chers parents pour leurs affections.

Mes deux frères NASSIM, EL-HADI.

A toute ma famille.

A ma binôme Nabila et sa famille.

Toute mes amies.

A tous ceux que j'estime beaucoup.

B. Siham

DEDICACES

Je dédie ce modeste travail à :

Mes très chers parents pour leurs affections.

Mes frères et sœurs surtout Malika.

A toute ma famille.

A ma binôme Siham et sa famille.

A B.Mourad qui ma plus soutenue.

A tous ceux que j'estime beaucoup.

B. Nabila

Table des matières

Chapitre III : La sécurité informatique à base du système Kerberos

Chapitre IV : Réalisation

Liste des figures

Liste des figures

Liste des abréviations

A

ACL Access Control List

AES Advanced Encryption Standard

ARPA-net Advanced Research Projects Agency Network

AS Autentication Server

B

BD Data Base

D

DRGB Direction régionale de Bejaia

DNS Domain Name System

DHCP Dynamic Host Configuration Protocol

DoS Deny of Service

DES Data Encryption Standard

DEC Déplômed'EtudesCollègailes

H

HTML HyperTExt Mark-up Language

I

ISO International System Organization

IP Internet Protocol

IBM International Busness Machine

K

KDC Key Distribution Center

L

LAN Local Architecture Network

M

MIT Massachusetts Institute of Technology

MD Message Digest

N

NSA National Security Agency

R

RTC Région Transport Centre

RFC Requests For Comments

S

SHA Secure Hash Algorithm xxx bits

SPOF Single Point Of Failure

T

TGT Ticket-Granting Ticket

TGS. Ticket-Granting Server

TCP/IP Transport Control Protocol / Internet Protocol

W

WINS Windows Internet Name Service

Introduction

Introduction générale

De nos jours les ordinateurs sont de plus en plus omniprésents. Ils contiennent toutes sortes d'informations confidentielles. Il convient donc de tenter de sécuriser ces informations de la façon la plus efficace possible contre toute possibles attaques.

La sécurité informatique a plusieurs objectifs, lies aux types de menaces ainsi qu'aux types de ressources. Néanmoins, les principaux points sont d'empêcher la divulgation des données ainsi que les ressources du réseau, et pour cela la préoccupation actuelle consiste en la mise en place des protocoles sécurisés qui luttent contre les usurpations d'identité ou l'espionnage des données privées.

Parmi ces protocoles, on cite ceux de l'authentification. Ceux-ci sont le procédé par lequel une personne dans un réseau se persuade de l'identité de son interlocuteur. Dans la plupart des cas, cette étape n'est qu'un préalable à la communication réelle, et ce procédé est couplé avec la génération d'une clé de session secrète, que les interlocuteurs peuvent ensuite utiliser pour s'échanger des messages en toute sécurité.

Le protocole d'authentification utilisé au niveau de l'entreprise Sonatrach est RADIUS (Remote Authentication Dial-In User Service) est un protocole d'AAA (Authentication, Authorization and Accounting : identification, autorisation et comptabilité. Dans notre cas, on va se focalier sur l'authentification kerberos, qui est un système dans lequel aucun mot de passe n'est transmis en claire, ce qui constitue une sécurité en soi.

Ainsi, au cours de développement de ce travail de recherche, nous tentons de répondre à la problématique suivante :

- **Qu'est-ce qu'on entend par le protocole Kerberos ?**
- **Quel est son fonctionnement au niveau du réseau ?**
- **Ou peut-on configurer Kerberos dans un système ?**
- **Quelles sont les configurations nécessaires pour réaliser une authentification Kerberos ?**

Au regard des questions que nous avons soulevées dans notre problématique, nous avons provisoirement avancé que :

- Kerberos est un protocole de sécurité complexe au niveau de son fonctionnement.
- L'authentification Kerberos existe dans différents environnements.
- Les paramètres de ce protocole peuvent être initialisés par l'administrateur réseaux.

Pour parvenir à notre objectif, nous avons opté pour une démarche méthodologique qui s'inscrit sur une recherche bibliographique et un travail sur le terrain concrétisé par un stage pratique au niveau de l'entreprise SONATRACH de Bejaia. Ainsi notre travail sera organisé autour de quatre chapitres :

Le premier chapitre vise à présenter brièvement l'entreprise SONATRACH de la wilaya de Bejaia (RDGB).

Le second chapitre concernera la définition de quelques concepts de base de la sécurité des systèmes et réseaux informatiques, et tout ce qui est risques, menaces, services, mécanisme et failles de sécurité.

Le troisième chapitre, est le noyau de notre travail. Ce chapitre est un passage théorique qui détail le protocole d'authentification Kerberos et décrit son fonctionnement ainsi que ses avantages et inconvénients.

Le chapitre quatre, sera consacré à définir l'environnement de travail ainsi les étapes de configurations que nous avons effectués.

Chapitre I

Présentation de l'organisme d'accueil

I.1. Introduction

Afin de nous familiariser avec l'environnement de l'entreprise, nous avons cherché à définir l'activité principale de DRGB (Direction régionale de Bejaïa) et ses divisions ainsi que le rôle de chaque division.

I.2. Historique de la SONATRACH

Afin d'assurer le contrôle et la gestion du secteur naissant dans les années 1950 des hydrocarbures, une Direction de l'Energie et des Carburants a été mise en place en Algérie.

Des indicateurs significatifs d'une évolution peu probable du secteur des hydrocarbures ont été constatés. Après l'indépendance, l'Etat algérien se dota d'un instrument permettant la mise en œuvre d'une politique énergétique en créant le 31-12-1963 par décret n° 63 / 491 la société nationale pour le transport et la canalisation d'hydrocarbures. Cette société a changé de statuts le 22-07-1966 décrets n° 66/292, pour devenir « SONATRACH ».

La volonté de l'Algérie de récupérer ses richesses naturelles et d'assurer pleinement le contrôle de leur exploitation, amena à nationaliser la production des hydrocarbures le 24/02/1971 par la signature d'une ordonnance, définissant le cadre d'activité des sociétés étrangères enAlgérie. Grâce à cette nationalisation, l'entreprise SONATRACH est passée d'une petite entreprise de 33 agents en 1963 à un effectif de 103000 employés la fin des années 1980, et qui compte aujourd'hui 120 000 employés.A l'instar de toute entreprise à travers le monde, la SONATRACH en tant que groupe pétrolier international, s'est tracée des objectifs stratégiques qui reposent essentiellement sur :

- La maîtrise continue de ses métiers de base,
- Le renforcement de ses capacités technologiques,
- Le développement des activités en international,
- Le partenariat en amont et en aval, et la diversification de son portefeuille d'activité.

Les activités de SONATRACH se résument comme suit :

- La recherche et l'exploitation du gisement (*amont*),
- La liquéfaction et la transformation du gaz (*aval*),
- La commercialisation,
- Le transport par canalisation.

I.3. Direction Régionale de Bejaia (DRGB)

Dans ce qui suit nous présenterons la direction régionale de Bejaïa ainsi le rôle de ses services

I.3.1.Présentation

La direction régionale de Bejaïa (DRGB) est l'une des cinq régions de transport des hydrocarbures (TRC) du groupe SONATRACH.

- Elle a pour mission le transport, le stockage et la livraison des hydrocarbures liquides et gazeux.
- Elle est chargée de l'exploitation d'un port pétrolier et d'un gazoduc et deux oléoducs :

- **Oléoduc Haoud El-Hamra vers Bejaïa (OB1) :** installé par la société SOPEG (*Société Pétrolière de Gérance*), cet Oléoduc est le premier pipe-line qui à été installé en Algérie. Il est d'une longueur de 660 km et d'un diamètre de 24 pouces.
- **Oléoduc Béni-Mansour vers Alger (OG1):** il est de longueur de 130 Km et d'un diamètre de 16 pouces.
- **Gazoduc Hassi-R'mel vers Bordj-Menaeil (GG1):**il est d'une longueur de 437 Km et d'un diamètre de 42 pouces, il approvisionne en gaz naturel depuis 1981 toutes les villes et pôles industriels du centre du pays.
- **Port pétrolier :** Est un terminal pétrolier composé de deux postes de chargement à partir d'un parc de pétrole brut composé de 16 bacs, de navires jaugeant jusqu'à 80.000 tonnes au moyen de pompières comportant 10 électropompes de 53.000 chevaux de puissance total.

Ainsi que la gestion des stations de pompage le long des lignes qui sont :

- **SP1 :** station de pompage N°1 à Djamaa (El Oued).
- **SP2 :**station de pompage N°2 à Biskra.
- **SP2 :**station de pompage N°3 à M'Sila.
- **SPM :**station de pompage à Béni Mansour.
- **TRA :**terminal Sidi-Aarcine (Djelfa).
- **TA :**terminal arrivé de Bejaia.
- **SC3:**Station de compression moudjebara (Djelfa).
- **GG1 BM :**terminal de Bordj Menaeil.

I.3.2. Organigramme De DRGB

La figure suivante illustre l'organigramme de la RTC de Bejaïa

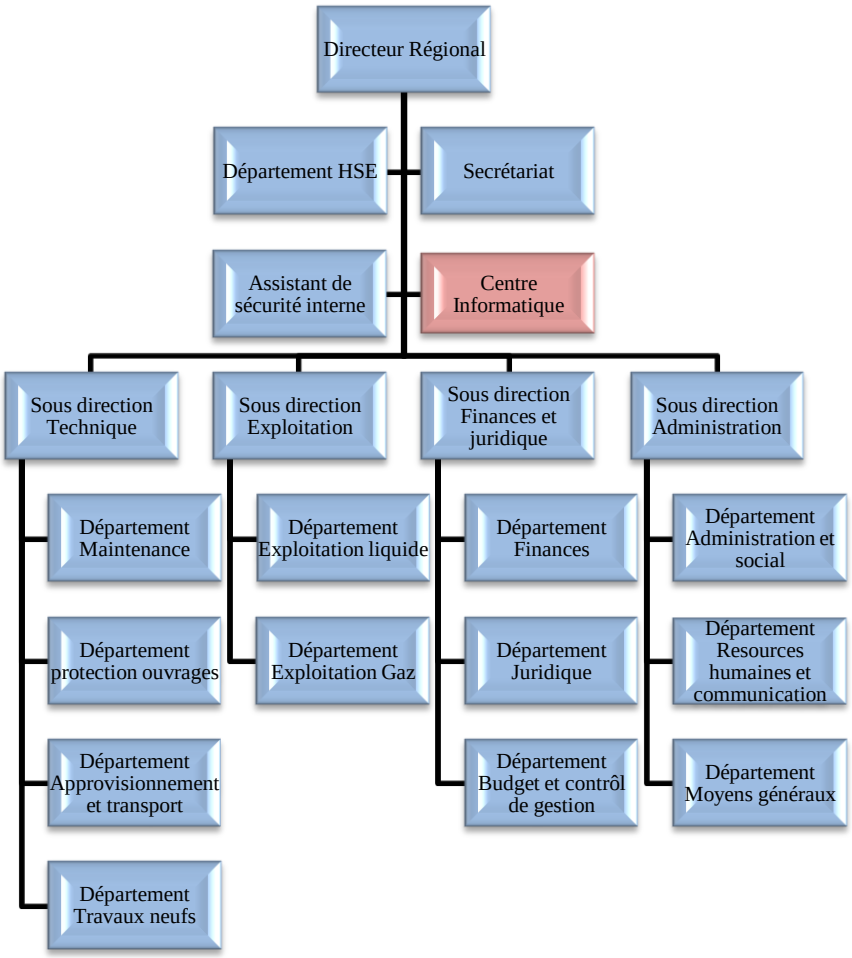


Figure I-1 : Organisation de la RTC.

I.3.3. Rôle de chaque service

Les structures de la direction régionale se présentent comme suit :

- **Direction régionale** : dirigée par un directeur régional et un secrétariat.
- **Secrétariat** : la gestion des courriers.
- **Assistant de sécurité interne** : a pour rôle de gérer les dispositifs de sécurité et la sauvegarde du patrimoine humain et matériel de la RTC.
- **Centre informatique** : il représente le support d'exploitation et le développement des applications informatique pour le compte de la RTC et les autres directions régionales.
- **Sous directiontechnique** : elle a pour mission d'assurer la maintenance et la protection des ouvrages ainsi que l'approvisionnement, l'étude et le suivi de projets de réalisation de travaux neufs. Elle est constituée en quatre départements : maintenance, protection des ouvrages, approvisionnement et transport et département des travaux neufs.

- **Sous directionexploitation** : elle est chargée de l'exploitation des installations de la région, et la maintenance du fonctionnement des trois ouvrages en effectuant des réparations en cas de fuite, de Sabotage ou de panne pour les stations de pompage. Elle comporte deux départements : exploitation liquide et exploitation gaz.
- **Sous directionfinances et juridique** : elle a pour mission d'effectuer la gestion financière, le budget et le contrôle de gestion et de prendre en charge les affaires juridiques de la DRGB. Elle est constituée de trois départements : finances, juridique, budget et contrôle de gestion.
- **Sous directionadministration** : elle a pour mission la gestion des ressources humaines et les moyens généraux. Elle est organisée en trois départements : département administration et social, ressources humaines et communication et moyens généraux.

I.4.Présentation du centre informatique

Le centre informatique est chargé du développement et de l'exploitation des applications informatiques de gestion pour le compte de la direction régionale de Bejaïa (DRGB) et des autres régions.

I.4.1.Organisation structurelle

L'organisation du centre ne cesse de subir des changements et l'évolution rapide de l'informatique pousse le centre à adopter des actions nouvelles à chaque fois afin de subvenir aux nouveaux besoins de l'entreprise.

Pour mener à bien sa mission, le centre informatique s'organise en trois services tels qu'ils sont schématisés dans la Figure I-2:

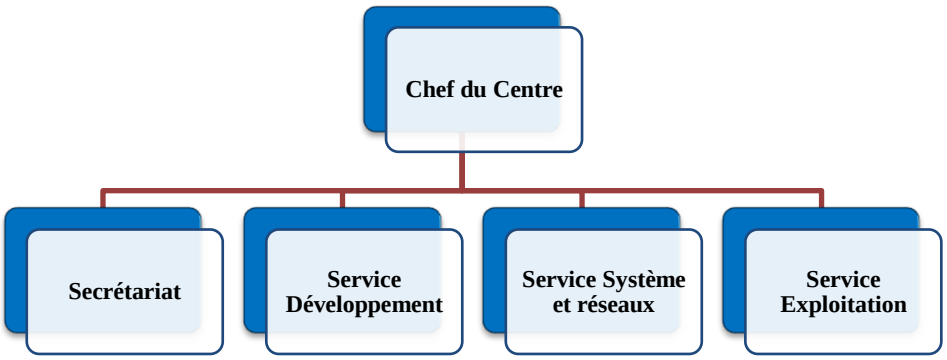


Figure I-2 : Organigramme du centre Informatique

I.4.2.Organisation fonctionnelle

Chaque service a sa propre fonction, on va définir et citer les différentes taches de chacun ci-dessous :

a) Service développement

Chargé d'en bénéficier des nouvelles technologies qu'il acquière tout en optimisant leurs utilisations, ainsi que la prise en charge des besoins des différentes structures de la direction en matière de développement de nouveaux systèmes d'information :

- Etude et analyse ;
- Réalisation d'applications informatique.

Aussi, le service prend en charge les taches de maintenance, ex : manque d'effectif durant la période des congés ou généralement en cas de besoins.

b) Service système et réseaux

Il est chargé d'assurer les tâches suivantes :

- L'administration des serveurs.
- L'administration des bases de données sur les serveurs.
- Installation des logiciels sur serveurs.
- Gestion des performances système et réseau.
- Gestion de la sécurité et des utilisateurs connectes au réseau (droits d'accès).
- Gestion du parc informatique.
- La prise en compte et résolution des pannes.
- Planification et ordonnancement des travaux.
- Sauvegarde et restauration des données.
- Gestion des espaces disques.
- Exploitation (saisie, validation, traitement) des anciennes applications batch pour la DRGB et les autres directions régionales.

c) Service exploitation

Ce service a pour rôle d'exploiter les anciennes applications tournantes sur COBOL, la centralisation des bilans pour la branche transport et la gestion de la paie des temporaires.

I.5.Conclusion

L'étude de l'organisme d'accueil nous a permis d'acquérir des connaissances a propos de monde des entreprise ceci nous a mieux aidé de la conception et du développement de l'application.

Dans le chapitre suivant, nous allons passer à la présentation des notions générale de la sécurité informatique.

Chapitre II

Généralités sur la sécurité informatique

II.1. Introduction

De nos jours, la sécurité informatique est devenue un problème majeur dans la gestion des systèmes informatiques.

En effet, ces derniers ont connu une grande évolution sur les plans d'échange d'informations et d'ouverture sur le monde extérieur. Ils sont donc de plus en plus accessibles, depuis des machines de moins en moins contrôlées.

Ce chapitre sera entamé par la présentation d'un historique sur l'origine de l'utilisation d'Internet, suivi par une définition de la sécurité des systèmes d'informations et des réseaux, en termes de risques et en termes de menaces qu'ils encourent. À partir de l'analyse de ces derniers, il est primordial de rappeler l'importance de la politique de sécurité.

Nous introduisons par la suite les différents services de sécurité que l'ISO a normalisés et les mécanismes imaginés pour rendre ces services plus sécurisé, et les différentes failles de sécurité sur Internet. Puis l'illustration des mécanismes de sécurité les plus importants et la cryptographie.

II.2. Historique

Les premières années de l'apparition d'Internet la circulation des documents ne posait aucun problème de confidentialité et les données traversaient le réseau en clair.

Au début, les protocoles Internet ne sont évolués que pour faire face à l'accroissement du nombre d'utilisateurs, l'ouverture du réseau à un usage commercial a modifié les comportements. Comme des informations confidentielles circulent sur les liaisons, la sécurité des communications est devenue une préoccupation importante des utilisateurs et des entreprises. Tout le monde à se protéger contre une utilisation frauduleuse de leurs données ou contre des intrusions malveillantes dans les systèmes informatiques. La tendance actuelle est de mettre en place des protocoles sécurisés qui luttent contre les usurpations d'identité ou l'espionnage des données privées.

II.3. Risques, Menaces et Politique de sécurité

La sécurité dans un réseau concerne non seulement les éléments physiques (ex :*câbles, modems, routeurs, commutateurs…*), mais aussi les éléments logiques. Le responsable de la sécurité doit analyser l'importance des risques encourus, les menaces potentielles et définir un plan général de protection qu'on appelle politique de sécurité.

II.3.1. Risques

Les risques se mesurent en fonction de deux critères principaux : la **V**ulnérabilité et la **S**ensibilité.

La vulnérabilité : désigne le degré d'exposition aux dangers, elle peut permettre à un attaquant de compromettre des données, déposé aussi un autre utilisateur afin de l'exécution de commandes ou même prendre le contrôle de l'ordinateur affecté**[w1].**

La sensibilité : celle-ci désigne le caractère stratégique d'un composant du réseau. Ce dernier est très sensible vu son caractère et doit être quasi invulnérable. Pour cela, il est primordiale que toutes les mesures de protection soit prises pour le prémunir contre tous les risques

II.3.2. Menaces

Les menaces peuvent être classifiées selon deux catégories : les menaces passives et les menaces actives.

Les menaces passives : ce type de menace consiste essentiellement à copier ou à écouter l'information sur le réseau. Dans ce cas, celui qui prélève une copie n'altère pas l'information en-soi. Il en résulte des difficultés à détecter ce type de malveillance, car elles ne modifient pas l'état du réseau.

Les menaces actives : Elles se traduisent par différents types d'attaques. Parmi ces attaques on distingue :

- le brouillage,
- le déguisement permettant ainsi la modification des données au cours de leur transmission et la modification de l'identité de l'émetteur ou du destinataire,
- l'interposition qui consiste en la création malveillante de messages en émission ou en réception.

Les menaces actives sont de nature à modifier l'état du réseau.

II.3.3. Politique de sécurité

La politique de sécurité nécessite d'abord l'analyse des informations qui circulent ou qui sont stockées en fonction de leur importance et du coût que représenteraient leur perte, et l'analyse des menaces qu'on peut objectivement envisager.

Dans un réseau, il faut définir les mécanismes de protection à mettre en œuvre, on prend par exemple : les outils antivirus, les pare-feu, les patches ou programmes de correction des

systèmes et des applications utilisés…etc., puis définir tous les outils de surveillance allant de l'audit jusqu'au journal historique et la détection des intrusions.

II.4. Services de sécurité

L'ISO a défini un certain nombre de services de sécurité : **A**uthentification, **C**ontrôle d'Accès, **C**onfidentialité et **I**ntégrité de données, **N**on-répudiation.

Pour assurer ces services, différents types de mécanismes sont utilisés, tel que : la *signature numérique, les listes de contrôle d'accès*. Ils diffèrent par leur complexité, leurs coûts, les efforts nécessaires pour leur implantation et leur maintenance **[1].**

II.4.1. Authentification

Le service d'authentification garantit l'identité des correspondants ou des partenaires qui communiquent. On distingue les trois cas d'authentification suivants :

- ***L'authentification de l'entité distante* :** elle garantit que le récepteur est celui souhaité. Son principal objectif est de lutter contre le déguisement, également appelé usurpation d'identité (ou spoofing).
- ***L'authentification de l'origine* :** elle assure que l'émetteur est celui prétendu. Le service est inopérant contre la duplication d'entité.
- ***L'authentification mutuelle* :** elle assure que les deux entités émettrice et réceptrice se contrôlent l'une l'autre.

II.4.2. Contrôle d'accès

Le service de contrôle d'accès empêche l'utilisation non autorisée des ressources accessibles par le réseau. On entend par « utilisation » les modes de : lecture, écriture et création et/ou suppression ; et par ressources : les systèmes d'exploitation, les fichiers, les bases de données et les applications.

Pour contrôler les accès aux ressources, il faut d'abord authentifier les utilisateurs afin de s'assurer de leur identité qui est transportée dans les messages d'initialisation et ensuite établir une liste des droits d'accès associés à chacun.

II.4.3. Confidentialité des données

Garantir la confidentialité des données signifie, empêcher une entité tierce de récupérer ces données et de les exploiter. Seuls les utilisateurs autorisés doivent être en mesure de prendre connaissance du contenu des données. Un message ou un échange de messages à sa confidentialité garantie que tout utilisateur non autorisé qui aurait pu le récupérer ne peut pas l'exploiter.

II.4.4. Intégrité des données

L'intégrité des données assure au récepteur que les données reçues sont celles qui ont été émises. L'intégrité des données peuvent être altéréesde manière accidentelle ou délibérée à la suite d'une fraude active.

Par ailleurs, l'intégrité possède une portée plus ou moins grande, elle varie d'un champ spécifique du message jusqu'à son intégralité. La détection des modifications peut être mise en œuvre uniquement lorsque la communication a lieu en mode non connecté.

II.4.5. Non-répudiation

Consiste en la non-répudiation de l'origine et la non-répudiation de la remise :

La non-répudiation de l'origine : elle fournit au récepteur une preuve empêchant l'émetteur de contester l'envoi d'un message ou le contenu d'un message effectivement reçu.

La non-répudiation de la remise : elle fournit à l'émetteur une preuve empêchant le récepteur de contester la réception d'un message ou le contenu d'un message effectivement émis.

II.5. Failles de sécurité sur Internet

Une faille ou vulnérabilité est une faiblesse dans un système informatique, permettant à un attaquant de porter atteinte à l'intégrité de ce système c'est-à-dire à son fonctionnement normal, à la confidentialité et l'intégrité des données qu'il contient**[w10].**

II.5.1. Méthodes utilisées par les attaquants

Il existe plusieurs méthodes d'attaque, parmi lesquelles on cite :

- **IP spoofing**

Usurpation d'adresse IP, on fait croire que la requête provient d'une machine autorisée. Une bonne configuration du routeur d'entrée permet d'éviter qu'une machine extérieure puisse se faire passer pour une machine interne.

- **DNS spoofing**

Cette technique sert à pousser un serveur de DNS à accepter l'intrus. La solution consiste à séparer le DNS du LAN de celui de l'espace public.

- **Flooding**

Sert à déconnecter quelqu'un à partir de son adresse IP, grâce à un programme appelé flooder. Le flooder envoi des pings à la victime. Un ping sert à calculer à quelle vitesse vous communiquez avec une autre machine via le net. Tout ping génère une réponse. En augmentant le nombre de pings, le serveur déconnectera la victime car elle enverra trop de données en réponseau flood.

- **Smurf**

Smurf ou « attaque par réflexion » est une technique basée sur l'utilisation de serveurs de diffusion (*broadcast*) pour paralyser un réseau**[w2].**

- **Web bug**

Un mail publicitaire est envoyé en HTML, en apparence normal avec une image transparente, difficile à voir en raison de sa taille. Si ce courrier est ouvert pendant la connexion, la requête de téléchargement de l'image vient confirmer la lecture du message et la validité de votre adresse.

- **Hoax (rumeur)**

Un «hoax » est une rumeur que l'on transmet par mail. Ces rumeurs colportent souvent des problèmes de sécurité soit disant découverts par des services officiels ou célèbres. Elles peuvent causer un véritable préjudice à certaines sociétés en encombrant leur réseau. Avant de retransmettre un tel message, il est prudent de vérifier son authenticité.

- **Hacker et Cracker**

Hacker : dans les premières expériences de l'ARPA-net s'y existé une communauté, une culture partagée, de programmeurs expérimentés et de spécialistes des réseaux, Les membres de cette culture ont créé le mot "Hacker". Ces informaticiens sont généralement discrets, anti-autoritaristes et motivés par la curiosité.

Cracker : ce sont principalement des gens qui s'introduisant à distance dans les systèmes informatiques et faire marcher un logiciel qui a besoin d'une licence sans acheter cette dernière, généralement à l'aide d'outils écrit par d'autres et trouvés sur Internet.

II.5.2. Principales attaques

Il existe plusieurs types d'attaques à savoir **:**

- **Virus**

Un virus est un exécutable qui va exécuter des opérations plus ou moins destructrices sur une machine. Sur Internet, les virus peuvent contaminer une machine de plusieurs manières :

• Téléchargement de logiciel puis exécution de celui-ci sans précautions,

• Ouverture sans précautions de documents contenant des macros,

• Pièce jointe de courrier électronique,

• Ouverture d'un courrier au format HTML contenant du JavaScript exploitant une faille de sécurité du logiciel de courrier

• Exploitation d'un bug du logiciel de courrier,

Les virus peuvent être très virulent, mais ils coûtent aussi beaucoup de temps en mise en place d'antivirus et dans la réparation des dégâts causés. On peut malheureusement trouver facilement des logiciels capables de générer des virus et donc permettant à des « amateurs » (aussi appelés crackers) d'étaler leur incompétence.

La meilleure parade est l'utilisation d'un antivirus à jour et d'effectuer les mises à jour des logiciels pour éviter l'exploitation des bugs.

- **Déni de Service (DoS)**

Le but d'une telle attaque est de rendre indisponible durant une certaine période les services ou un réseau complet. Les utilisateurs ne peuvent plus alors accéder aux ressources. Les deux exemples principaux, sont le « ping flood » ou l'envoi massif de courriers électroniques pour saturer une boîte aux lettres (mailbombing). La meilleure parade est le firewall ou la répartition des serveurs sur un réseau sécurisé.

- **Écoute du réseau (sniffer)**

L'écoute du réseau est le fait d'intercepter certaines informations qui transitent sur un réseau local par des logiciels spéciaux, en retranscrivant les trames dans un format plus lisible (Network packetsniffing). C'est l'une des raisons qui font que la topologie en étoile autour d'un hub n'est pas la plus sécurisée, car les trames qui sont émises en «broadcast» sur le réseau

local peuvent être interceptées. De plus, l'utilisateur n'a aucun moyen de savoir qu'un pirate a mis son réseau en écoute.

L'utilisation de switches (*commutateurs*) réduit les possibilités d'écoute mais en inondant le commutateur, celui-ci peut se mettre en mode « HUB » par sécurité. La meilleure parade est l'utilisation de mot de passe non rejouable, de carte à puce ou de calculette à mot de passe.

- **Cheval de Troie**

Un cheval de Troie (*Trojan Horse*) est un type de logiciel malveillant, souvent confondu avec les virus ou autres parasites. Le cheval de Troie est un logiciel en apparence légitime, mais qui contient une malveillance. Le rôle de cheval de Troie est de faire entrer ce parasite sur l'ordinateur et de l'y installer a l'insu de l'utilisateur.

II.6. Mécanismes de Sécurité

Les messages sur un réseau sont toujours des suites de données binaires, ce qui implique la difficulté de la distinction entre l'original et celui qui est dupliqué. Il faut donc adapter les solutions de sécurité au monde électronique.

Il s'agit principalement du chiffrement qui intervient dans presque tous les mécanismes de la signature numérique, des techniques d'utilisation d'identificateur et de mots de passe, de bourrage et de notarisation.

II.6.1. Signature numérique

La signature numérique consiste à utiliser un chiffrement particulier appelé chiffrement irréversible. Celui-ci transforme un message (*long*) en un bloc de données (*de petite taille*) tel qu'il est impossible de reconstruire le message à partir du bloc.

Les algorithmes utilisés sont appelés fonction de hachage ou fonction de condensation. Le bloc est appelé condensé ou signature. Une bonne fonction de hachage doit produire des condensés différents pour des messages différents : si deux messages différents avaient le même condensé, il serait possible pour un utilisateur malveillant de substituer un message à l'autre, tout en conservant le condensé correct. Cela rend la modification du message indétectable.

II.6.2. Mots de passe

Un mot de passe est constitué de lettres minuscules, de lettres majuscules, de caractères spéciaux et de chiffres est techniquement plus difficile à découvrir qu'un mot de passe constitué uniquement de minuscules.

L'utilisation de mots de passe est l'une des briques de base dans la sécurisation d'un système et il doit être difficile à retrouver, même à l'aide d'outils automatisés. La force d'un mot de passe dépend de sa longueur et du nombre de possibilités existantes pour chaque caractère le composant.

II.6.3. Liste de Contrôle d'Accès

Le mécanisme des listes de contrôle d'accès (*ACL, Access Control List*) utilise l'identité authentifiée des entités et des informations fiables pour déterminer leurs droits d'accès au réseau ou aux ressources sur le réseau. De plus, il est susceptible d'enregistrer sous forme de trace d'audit et de répertorier les tentatives d'accès non autorisées.

II.7. Cryptographie

La cryptographie est la science qui utilise les mathématiques pour le cryptage et le décryptage de données. Elle permet ainsi de stocker des informations confidentielles ou de les transmettre sur des réseaux non sécurisés (*tels que l'Internet*), afin qu'aucune personne autre que le destinataire ne puisse les lire. Le mot « Cryptographie » est composé des mots grecs :

- CRYPTO = caché
- GRAPHY = écrire

Il existe de multiples méthodes pour crypter des données et ce sont de plus en plus sophistiquées, et de moins en moins faciles à dépasser. Ces méthodes sont de deux types : par application de calculs simples et par utilisation de calculs plus complexes pour une Cryptographie par clé**[3].**

II.7.1. Cryptographie simple ou Symétrique

La Cryptographie Symétrique est un chiffrement qui utilise une clé secrète partagée entre l'émetteur et le récepteur. Les opérations de l'émetteur et celles du destinataire sont les inverses les unes des autres. Les principaux cryptages simples sont **[4] :**

A) Substitution de caractères

On définit une règle de conversion d'un caractère vers un autre (*décalage de n caractères, table de conversion…*) et on convertit l'ensemble du message vers un message codé. Cette méthode, assez simple à employer, est cependant assez simple à prendre en défaut par analyse statistique du texte (*probabilité d'apparition des lettres dans une langue, étude de la fréquence des doubles lettres,…*), on arrive rapidement à casser le codage

B) Transposition

Au lieu de changer les caractères pour des autres, on change la place des caractères dans le texte en effectuant une lecture verticale du texte et en permutant les colonnes selon un algorithme spécial. Malheureusement, ce cryptage peut aussi être surmonté en essayant plusieurs combinaisons de permutations et en fondant des hypothèses sur le contenu du message.

C) Conversion par XOR

Consiste à appliquer l'opérateur binaire « ou exclusif » (XOR), bit à bit, entre la représentation binaire du message et la représentation binaire de la clé choisie aléatoirement. Plus la longueur de la clé augmente, plus cette méthode n'est incassable, mais elle nécessite un partage des clés entre les parties de l'échange de messages et un stockage de ces clés en mémoire pendant tout le temps de la transaction.

D) DES

Data Encryption Standard, est une méthode de chiffrement utilisant des clés à 56 bits. Il était particulièrement utilisé dans les systèmes Unix.

E) Triple DES ou 3DES

C'est l'application successive de trois passes dans l'algorithme DES avec des clés en principes différentes (mais c'est parfois la même qui soit utilisée selon les implémentations). La longueur de la clé est de 168 bits (3*56 bits). 3DES est en passe de disparaître également, parce qu'il est lent et son niveau de sécurité est peu performant.

F) AES

Advanced Encryption Standard, adopté en 2001 est un algorithme développé par Rijndael, qui consomme peu de mémoire, facile à implémenter et utilise des clés de 128, 192 ou 256 bits. C'est devenu le remplaçant de DES et 3DES. AES est désormais utilisé dans la sécurisation WiFi,

outils de compression, de cryptage de volumes. C'est le seul algorithme autorisé à porter le nom de "AES".

II.7.2. Cryptographie Moderne ou Asymétrique

Les cryptages simples étaient « relativement » aisés à contourner par les crypto-analystes. Il a fallu trouver de nouvelles méthodes de cryptage. Ces nouvelles méthodes de la cryptographie moderne reposent sur une clé contenant deux éléments, l'un est public (*publié dans un annuaire, par exemple*), l'autre est secret (*et jamais transmis*). L'élément public est utilisé Pour chiffrer un message et l'envoyé à un utilisateur.

L'utilisateur est capable de déchiffrer le message en utilisant l'élément secret de sa clé. Lui seul est capable de le faire puisqu'il est le seul à connaître cet élément. En effet, la connaissance de l'élément public de la clé ne permet pas de retrouver l'élément secret.

L'intérêt principal du chiffrement asymétrique est qu'il n'y a pas de clé à transmettre. Par contre, les calculs à effectuer pour chiffrer et déchiffrer sont plutôt longs**[4].**

Les algorithmes asymétriques utilisés sont :

A) RSA

Le cryptage RSA, du nom de ses concepteurs, Ron **R**ivest, Adi **S**hamir et Leonard **A**dleman, est le premier algorithme de chiffrement asymétrique. Le RSA fonctionne à partir de deux nombres premiers, qui doivent être assez grands,On note N = pq. Le nombre N est appelé module RSA. Si deux utilisateurs souhaitent communiqués, ils doivent préparer chacun de son coté un module RSA**[5].**

Le problème ici réside dans la transmission de la clé de cryptage, car celle-ci peut être interceptée par une tiers personne.

B) Diffie-Hellman

Le protocole Diffie-Hellman peut être considéré comme complément au cryptage RSA, car il fournie la possibilité d'échange d'une clé secrète entre deux utilisateurs d'une manière sécurisée.

II.7.3. Fonctions de Hachage

Une fonction de hachage est une application facilement calculable qui convertit un grand ensemble en un plus petit ensemble appelée empreinte de hachage. Il est impossible de la déchiffrer pour revenir à l'ensemble d'origine. Dans ce qui suit on présentera quelques fonctions de hachage qui sont les plus utilisées **[6] :**

A) MD4 et MD5

Message Digest 4 qui génère une empreinte de 128 bits. Cet algorithme est désormais abandonné par une faiblesse de conception et tant la probabilité d'avoir le même résultat pour deux messages différents est important**[2].**

Message Digest 5 améliore MD4, l'empreinte reste sur 128 bits, mais cet algorithme est désormais considéré comme non sûr pour usage cryptographique : une équipe de Chinois a pu démontrer pouvoir reproduire à partir d'une empreinte e1 (*calculée à partir d'un message X*), un nouveau message (Y) capable de produire une empreinte e2 identique à e1. Ce qu'on appelle une collision complète (*dans un contexte peu sécurisé puisque le second message n'a pas été trouvé de manière aléatoire…*)

B) SHA-1

Secure Hash Algorithme -1 est apparu en 1995 sous la coupelle de la NSA, il produit une empreinte de 160 bits mais reste parmi les algorithmes peu sûrs bien qu'il faille une puissance de calcul importante pour permettre une collision qui ne sera trouvée à partir d'un message aléatoire.

C) SHA-2 (aussi appelé SHA-224, SHA-256, SHA-384, SHA-512)

Secure Hash Algorithm xxx bits. Algorithme dérivé de SHA1, publié par la NSA en 2000, les versions 256 et 512 sont répondues et dites sûrs, une étude de 2003 a montré que l'algorithme n'avait pas la fragilité des algorithmes rencontrés sur MD5 et SH1.

II.7.4. Objectifs de la cryptographie

Les objectifs de la cryptographie sont multiples et parmi eux on peut citer :

- ✓ Garantir la confidentialité ;
- ✓ Vérifier l'intégrité des données ;
- ✓ Gérer l'authentification ;
- ✓ Assurer la non-répudiation.

II.8. Conclusion

Ce chapitre a permet la présentation des composants de la sécurité informatique, les usages qui ont induit à sa création, les différentes formes de menacesà la sécurité de l'information, ainsi que les mesures qui ont été prisent pour y remédier. Ceci pour permettre à mieux cerner le sujet de notre étude et de présenter l'un des protocoles qui sert à préserver la sécurité d'un réseau et de l'information qui y circule. Le chapitre prochain sera dédié à la présentation de ce protocole nommé « Kerberos ».

Chapitre III

La sécurité informatique à base de Kerberos

III.1. Introduction

Le chapitre précédent s'est basé sur la présentation des éléments constituent l'origine même de la sécurité informatique et les termes liés à celle-ci.

À présent, cette partie sera focalisée sur le protocole d'authentification Kerberos, en commençant par sa définition, les notions essentielles à connaître pour mieux comprendre son fonctionnement et ses étapes d'authentification, mais avant ça, un bref aperçu sur son historique et son fondement s'imposent.

III.2. Historique

Vers la fin des années 70, deux chercheurs Roger Needham et Michael Schroeder, ont défini une plateforme sécurisée permettant d'authentifier les utilisateurs. Ils ont mis en place deux protocoles dont l'un utilise des clés privées de cryptage, et l'autre utilise des clés publiques de cryptage**[7].**

L'objectif de ce protocole est de permettre à deux utilisateurs d'établir une connexion sécurisée fiable. La sécurité viendra du fait qu'à la fin du protocole, les deux utilisateurs devront partager une clé secrète, afin d'échanger des informations d'une façon sécurisée. Ce protocole sera donc sûr, si, il est possible de garantir que seuls ces utilisateurs connaissent leur clé secrète**[w3].**

Le protocole d'authentification Kerberos est fondé sur les clés privées de cryptage. Kerberos a vu le jour dans les années 1980, au sein du projet "Athena", un projet de recherche conjoint entre le MIT, DEC et IBM. Il s'agit d'un système conçu pour assurer une authentification fiable entre différents nœuds d'un réseau non sécurisé, garantissant la confidentialité des échanges.

Vers la fin des années 80, la première version publique est publiée, sous le nom de Kerberos 4, vue que les trois premières ont étaient que des versions de développement.

La version 5 est destinée à corriger certaines limites de la version précédente**[2].**

III. 3. Définition de Kerberos

Kerberos vient de la mythologie grecque (Cerbère) et correspond au nom du chien à trois têtes gardien des portes de l'enfer. Il porte bien son nom puisqu'il est chargé d'authentifier, d'autoriser et de surveiller les utilisateurs voulant accéder aux ressources et services de réseau. Il agit d'un chien en garde contre les intrus sur les services réseau**[w4].**

Il s'agit d'un protocole sécurisé, où il ne transmet jamais de mot de passe en clair sur le réseau. Il transmet des messages cryptés à durée de vie limitée, qui repose sur un mécanisme de clés secrètes et l'utilisation de tickets**[9].**

En effet, sa fiabilité et son extensibilité lui ont servi d'être choisi par Microsoft pour devenir le protocole d'authentification des réseaux utilisant le système Windows**[10].**

III. 4. Tickets de Kerberos

Le concept d'un Ticket est utilisé comme marque qui prouve l'identité d'un utilisateur, en effet, les tickets sont des documents numériques qui stockent des clés de session. Ils sont publiés pendant une session de *login*et alors peut être employé au lieu des mots de passe pour tous services. Au cours de l'authentification, le client reçoit deux tickets:

–**Un ticket de ticket-octroi(TGT) :** agit en tant que identificateur global pour un utilisateur et une clé de session.

–**Un ticket de service :** authentifie un utilisateur à un service particulier.Ces tickets incluent le groupe date/heure qui indique une expiration. Ce temps d'expiration peut être placé par des administrateurs de Kerberos selon le service.

III.5. Serveurs de Kerberos

Afin d'accomplir l'authentification sûre, Kerberos emploie un tiers de confiance connu comme centre de distribution de clés (le KDC), qui est constitué de deux composants, typiquement intégrés dans un serveur simple:

- ✓ ***Un serveur d'authentification :*** il effectue l'authentification de l'utilisateur, il contient une base de données qui inclue les clés secrètes des utilisateurs et services.
- ✓ ***Un serveur de Ticket-octroi(TGS):*** qui accorde des tickets aux utilisateurs**[w5].**

III.6. Termes liées à Kerberos

L'utilisation de Kerberos fait appel à un vocabulaire dont les principaux termes sont énumérés comme suit :

Principal: Triplet <primary name, instance, realm>.

- ✓ Primaryname : nom d'utilisateur ou du service ;
- ✓ Instance : rôle/groupe du primary ;
- ✓ Realm : domaine d'administration associé à au moins un serveur Kerberos qui stocke la 'master BD' du site/domaine.

Client : Entité pouvant obtenir un ticket (*utilisateur/hôte*).

Service : Programme/ordinateur accédé sur un réseau.

TGT : Ticket particulier permettant au détenteur d'obtenir d'autres tickets pour le même domaine**[11].**

Royaume : le domaine administratif qui englobe les clients Kerberos et les serveurs est appelé un royaume. Chaque domaine Kerberos a au moins un serveur Kerberos, zéro ou plusieurs serveurs esclaves Kerberos, et un certain nombre de clients. La base de données de ce domaine est stockée sur le serveur Kerberos.

KDC (*Key Distribution Center*) : Base de Données des clients et des serveurs ainsi que des clés privées associées.

Le service d'octroi de tickets (TGS) et le serveur d'authentification (AS) sont généralement désignés collectivement comme la distribution de clés Center (KDC)**[13].**

III.7. Principe de fonctionnement de Kerberos

Dans l'authentification via Kerberos trois acteurs se présentent:

- ❖ Le client qui souhaite s'authentifier auprès d'un serveur;
- ❖ Le serveur qui doit s'assurer de l'authenticité de client ;
- ❖ Un tiers de confiance, le KDC.

Chacun de ces trois acteurs possède une clé secrète. Ainsi, ces acteurs partagent leurs clés secrètes avec le tiers de confiance (*c'est-à-dire le KDC*), donc le KDC connaît toutes les clés secrètes des entités de son royaume de confiance Kerberos (*realm*). En réalité, chaque acteur ne connaît qu'une seule clé, mais un ensemble de clés de différents types leur permettant d'utiliser différents formats et algorithmes (*MD5/DES, SHA-1/AES, etc.*).

Les clés secrètes sont des clés ayant une durée de vie importante (*de quelques semaines à l'infini pour les clés n'expirant jamais*).

Il existed'autres clés dites clés de sessions partagées entre deux acteurs. Ces clés sont négociées durant l'authentification d'un client et elles possèdent une durée de vie bien plus courte (*quelques heures au maximum*), les tickets générés par les KDC sont transmis aux clients. Elles sont conservées par les clients afin de les présenter par la suite aux KDC ou aux serveurs qui serviront à convaincre une entité de l'identité d'une autre entité. Il crée également des clés de session qui sont données à deux participants et qui servent à chiffrer les données entre ces deux participants.

III.8. Etapes de l'authentification de Kerberos

L'authentification d'un client auprès d'un serveur va s'opérer en trois échanges auprès de trois services distincts **[10] :**

III.8.1. Obtention d'un Ticket TGT

Cette étape est l'authentification du client auprès de service d'Authentification :

- **Construction du TGT**

Lorsqu'unutilisateur souhaite s'authentifier sur son domaine Kerberos. Il dispose pour cela d'un nom d'utilisateur et d'un mot de passe. Donc il effectue une requête de TGT auprès de service d'Authentification (AS) en lui indiquant le nom d'utilisateur. L'AS reçoit cette demande, et commence alors la construction d'un TGT. Il crée une clé de cryptage symétrique aléatoire, et compose un ticket contenant :

- La date d'émission du ticket ;
- La durée de vie du ticket ;
- La clé de cryptage créée.

Ce service d'authentification dispose de sa propre clé de cryptage , il s'en sert pour crypter le ticket, qu'on appelle désormais le TGT (*Ticket-Granting Ticket*). Seul ce service Kerberos sera donc en mesure de lire les informations.

- **Réception du TGT**

Le client reçoit à travers le réseau un TGT (*crypté avec le mot de passe de KDC*) et la clé de session (*cryptée avec le mot de passe de l'utilisateur*).

L'utilisateur, qui a entré son mot de passe sur sa machine locale, peut alors décrypter la clé de session. Il se trouve maintenant en présence :

– **d'une clé de session** : elle lui servira pour communiquer de manière sécurisée avec le KDC (*pour les futures demandes de tickets au TGS*) ;

– **d'un TGT :** il prouve qu'il s'est bien adressé au KDC et a obtenu une clé de session (*l'utilisateur présentera ce TGT au TGS*).

III.8.2. Acquisition d'un ticket de service

Cette étape est l'Authentification du client auprès de service TGS :

➢ **Construction de l'authentificateur**

Une fois le client a obtenu un TGT et une clé de session, il peut s'adresser au service TGS du KDC afin d'utiliser un des services Kerbérisés (*par exemple, un service Telnet, c'est à dire un Telnet ou il n'aura pas à saisir de mot de passe*). Le client va alors composer un authentificateur. En effet, le TGT ayant pu être intercepté par n'importe qui, il faut pouvoir prouver son identité.

Cet authentificateur est composé du nom de l'utilisateur, de l'adresse de sa machine, et de l'heure courante. Il crypte ceci avec la clé de session (*qu'il est le seul à connaître*), et joint ceci au TGT. Il rajoute enfin, en clair, son nom d'utilisateur, son adresse, et bien sûr le nom du service auquel il souhaite accéder.

➢ **Authentification du client**

Le service TGS du KDC reçoit les informations, et commence par décrypter le TGT, qui a été crypté avec la clé de KDC, et si le décryptage réussit, cela prouve l'authenticité du client. Dans ce TGT, figure la clé de session avec laquelle le client a crypté l'authentificateur, il peut alors le décrypter. Si ce décryptage réussit, c'est que le client qui s'adresse à lui est bien celui qu'il prétend d'être. Par ailleurs, le KDC effectue des vérifications sur les dates et durées de vie, pour s'assurer qu'il ne s'agit pas de tickets ou authentificateurs périmés.

➢ **Création du ticket de service**

Une fois le client considéré comme authentifie, le KDC crée aléatoirement une nouvelle clé de session. Celle-ci servira pour crypter les communications entre le client et le service auquel il souhaite accéder. Il faut donc que cette clé parvienne au client et au service. Voici donc la composition du ticket :

– Le nom et l'adresse de l'utilisateur pour lequel le ticket a été créé,

- Le nom du service que l'utilisateur a demandé d'utiliser,
- La date d'émission et la durée de vie du ticket,
- La clé de session nouvellement créée pour les communications entre le client et le service.

Pour que le service ciblé soit le seul à pouvoir accéder à ces informations, ce ticket est crypté avec son mot de passe stocké dans la base de données de KDC. Il suffira donc que le client donne ce ticket crypté au service pour qu'il puisse en extraire la clé de session.

➢ **Réception du ticket de service**

Le KDC transmet ce ticket de service et cette clé de session cryptée à l'utilisateur. Comme celui-ci connait la clé de session utilisée entre lui-même et le KDC, il peut décrypter la clé de session qu'il utilisera avec le service ciblé.

III.8.3. Authentification auprès d'un service

Cette étape est l'Authentification du client auprès de service souhaite avoir accès :

➢ **Construction de l'authentificateur**

Le client crée un authentificateur, comportant son nom, son adresse et sa date d'émission. Il crypte ces informations avec la clé de session créée déjà par le KDC, cela servira pour les communications entre ce client et ce service. Il envoie alors l'authentificateur crypté et le ticket au service ciblé.

➢ **Authentification du client**

Le service reçoit le ticket, qu'il est le seul à pouvoir décrypter. En effet, il connaît son propre mot de passe, avec lequel le KDC avait crypté le ticket. Il en extrait alors les informations qui s'y trouvent, dont la clé de session à utiliser avec le client qui vient de se connecter. Une première vérification consiste à s'assurer que le nom de service figurant dans ce ticket soit bien celui du service adressé. Si c'est le cas, c'est que le ticket émane bien du KDC. Il effectue alors les vérifications de concordance entre la date, l'authentificateur et le ticket. Le service a alors l'assurance que le client qui s'est connecté est bien celui auquel le ticket a été délivré par le KDC.

➢ **Authentification du service**

Le service peut s'authentifier auprès du client. Comme il est le seul à disposer de la clé de session, il va crypter une information connue du client, pour que celui-ci vérifie sa valeur.

L'utilisateur réceptionne ce paquet crypté, le décrypte, et doit y lire la même valeur. Si c'est bien le cas, le client considère qu'il s'adresse effectivement au service demandé, et il dispose maintenant d'une clé de cryptage, en commun avec lui.

III.9. Exemple illustrant l'authentification Kerberos

Les étapes de l'authentification dans le modèle de Kerberos sont présentées de façon détaillée dans la Figure III-1 :

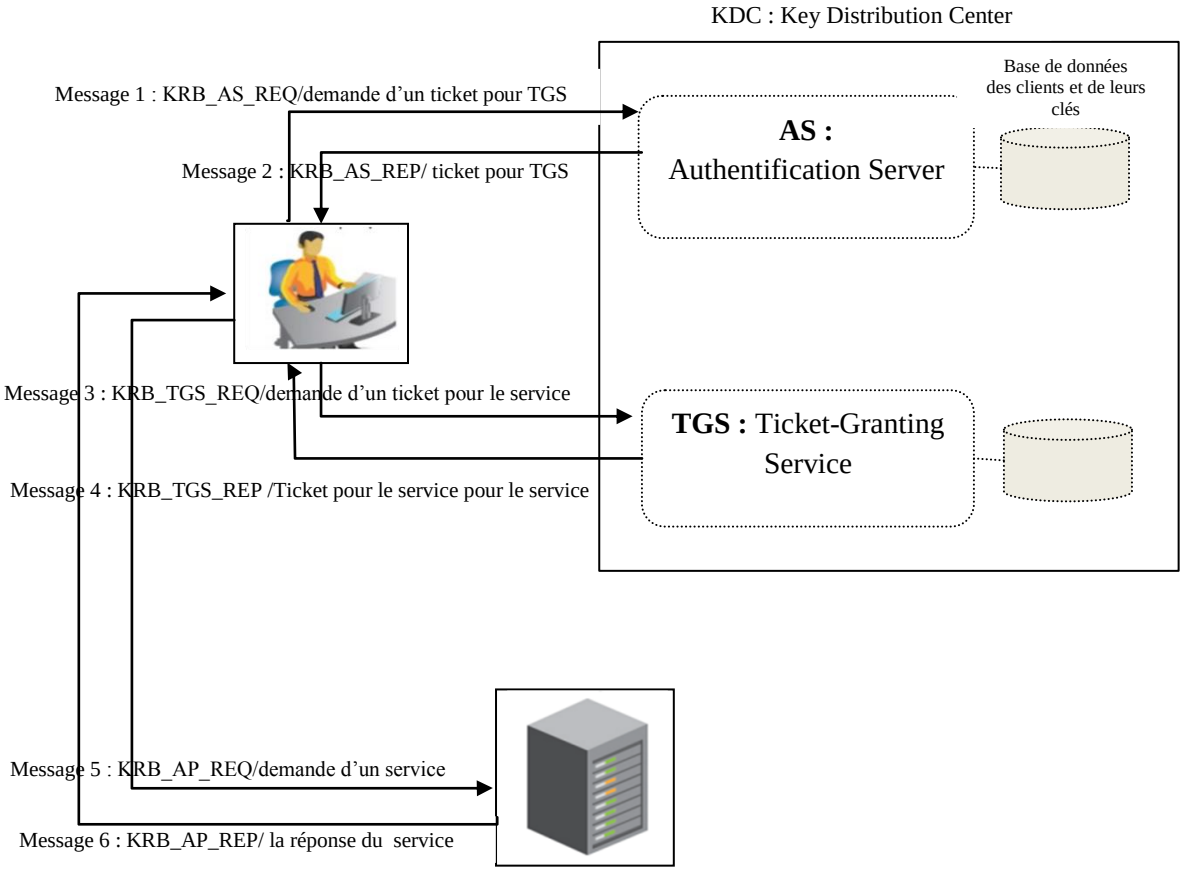


Figure III-1: exemple d'authentification dans kerberos

Kerberos de telle sort que:

- ✓ Le client envoie au serveur d'authentification le message 1 « KRB AS REQ » : où il précise son nom et demande un ticket qui va le présenter ensuite au TGS afin de contacter le destinataire.
- ✓ Le serveur d'authentification lui répond avec le message 2 « KRB AS REP » : Le serveur d'authentification cherche le client dans sa base de données. S'il le trouve, il

engendre une clé de session qui devra être utilisée entre le client et le TGS. Cette clé est chiffrée avec la clé secrète du client : c'est la première partie du message. Ensuite, il crée un ticket pour le client afin qu'il puisse s'authentifier auprès du TGS, ce ticket est chiffré avec la clé secrète du TGS. Le client ne pourra pas le déchiffrer mais pourra le présenter tel quel est à chaque requête au TGS. Dans ce cas particulier, le ticket est appelé TGT.

- ✓ Ensuite, avec le message 3 « KRB TGS REQ » le client s'authentifie auprès de TGS et demande le ticket de service qu'il souhaite avoir accès. Pour cela, le client fourni au TGS d'une part le nom du serveur qu'il souhaite contacter, d'autre part le ticket TGT et un identificateur qui possède des informations crypté avec la clé de session cet identificateur est vérifiable à partir du ticket par le TGS.
- ✓ Grâce à sa clé secrète, le TGS déchiffre le ticket, et récupère la clé de session et peut ainsi déchiffrer l'identificateur.

  Il compare le contenu de l'identificateur avec les informations contenues dans le ticket et si tout concorde (*le client est authentifiée*), il peut engendrer une clé de session (*qui sera utilisée entre le client et le service souhaité à avoir accès*) qu'il chiffre avec la clé de session et un nouveau ticket que le client devra présenter au service. Ces deux derniers seront la réponse de TGS au client contenant dans le message 4 « KRB TGS REP ». Après réception de ce message et déchiffrement, le client dispose donc en plus de la clé de session et de TGT (*qu'il conserve jusqu'à expiration du ticket pour dialoguer avec TGS*) déjà obtenue par le AS, d'une nouvelle clé de session et d'un nouveau ticket qu'il pourra utiliser avec service à accéder.
- ✓ Le message 5« KRB AP REQ » correspond à la demande de service souhaité par le client, il s'authentifier auprès de ce service de la même manière qu'avec le TGS (*message 3(KRB TGS REQ)*).
- ✓ Et le message 6« KRB AP REP » correspond à la réponse à la demande.

  De son coté, le service accédé s'authentifier en prouvant qu'il a pu déchiffrer le ticket reçu par le client et donc, il possède la clé de session.Pour cela, il faut qu'il renvoie une information vérifiable par le client et chiffrée avec cette clé. Pour éviter les attaques de type «replay ». En vérifiant cela, le client est maintenant sûr de l'identité de service et dispose d'une clé de session utilisable pour chiffrer les communications entre les deux.

III.10. Environnement de Kerberos

Il y'a deux environnements distincts dont le Kerberos est intégré:

- **Environnement d'Unix/Linux** utilisant KDCs légèrement modifié et il est basé sur une des distributions ouvertes populaires de source de Kerberos.
- **Environnement de Windows** utilisant l'annuaire actif**[12].**

Actuellement, il n'y a aucune intégration entre les deux environnements pour l'authentification de Kerberos.

Dans l'environnement Windows, Kerberos est intégré dans le système, alors que dans Linux l'administrateur doit initialiser les paramètres de configuration de Kerberos avant d'établir la connexion entre le serveur et les clients.

III.11. Authentification de Kerberos avec active directory

Kerberos est une partie intégrante de l'Active Directory d'annuaire de Windows. Les contrôleurs de domaine sont les centres de distribution des clés de Kerberos, et les clients systèmes emploient le protocole de Kerberos pour authentifier des utilisateurs avec les serveurs de contrôleur de domaine**[13].**

III.12. Avantages de Kerberos

Kerberos est un protocole conçu pour être sûr même lorsqu' il est exécuté sur un réseau peu sûr.

-Les transmissions sont chiffrées avec une clé secrète appropriée, l'attaquant ne peut pas avoir un ticket valide pour gagner l'accès non autorisé à un service sans compromettre une clé de cryptage.

-Kerberos protège également contre les attaques de rejeu, où l'attaquant écoute les communications légitimes de Kerberos et les retransmettre.

- Les tickets Kerberos peuvent contenir les adresses IP liés à la partie authentifiée pour empêcher de rejouer des adresses différentes.

-Kerberos se sert du chiffrement symétrique au lieu de la clé publique de chiffrage, ce qui le rend efficace.

-Les mots de passe ne sont jamais envoyés sur le réseau en texte brut où les pirates peuvent capturer et contrôler les paquets réseau à la recherche de l'identifiant del'utilisateur et un mot de passe**[w6**].

-Kerberos utilise l'horodatage et des informations de durée de vie pour sécuriser les communications au sein du réseau**[w7].**

-Diminue le risque d'attaque par des paquets mal formés (*débordement de buffer*).

-Diminue le nombre de bugs d'implémentation**[14].**

-Kerberos garantit l'intégrité des données, leur confidentialité, la non répudiation et l'authentification mutuelle des clients services**[15].**

III.13. Inconvénients de Kerberos

Il n'y a pas de système parfait et il s'agit d'être bien conscient des limitations de ce système. Les grandes lignes des faiblesses du système Kerberos sont:

-Tous les services du réseau doivent être « Kerberisé », c'est-à-dire compatible avec le protocole Kerberos. Les services doivent être capables de comprendre le système de ticket, sinon aucune authentification ne sera possible.

-Il faut que toutes les machines du réseau soient synchronisées, sinon l'utilisation des timestamp et la durée de vie des tickets risquent d'être faussées et plus aucune authentification ne sera possible.

-Kerberos introduit un SPOF (Single Point Of Failure) dans le réseau. Si le serveur Kerberos tombe, il n'y aura plus aucun accès aux différents services du réseau. La machine serveur de Kerberos doit être parfaitement sure.

- Si l'AS de Kerberos est compromis, un attaquant pourra accéder à tous les services avec un unique login.

-Kerberos chiffre uniquement la phase d'authentification, il ne chiffre pas les données qui seront transmises lors de la session**[w5].**

III.14. Conclusion

A travers ce chapitre, on a pu appréhender la notion du protocole Kerberos, son langage utilisé et sa procédure d'authentification ainsi que son authentification avec Active directory. Quelques avantages et inconvénients ont été soulignés. Mais ceci reste toujours dans le cadre théorique et de prise de connaissance. C'est ainsi que le chapitre à venir fera office de pratique pour mettre en avant les notions acquises durant ce travail.

Chapitre IV

Réalisation

IV.1. Introduction

Le présent chapitre concerne la partie pratique de notre travail, qui s'est déroulée au sein du centre informatique de la SONATRACH, plus précisément au"service systèmes et réseau". Après une collecte d'information approfondie, et renseignement sur le protocole de sécurité de l'entreprise. On a su que cette entreprise sécurise son réseau avec le protocole d'authentification RADIUS.

Notre thèmes de réalisation étant Kerberos,nous allons rester dans ce contexte, ainsi notre travail sera présenter de la manièresuivante :

- Présentation de l'environnement de travail ;
- La réalisation de l'authentification sur linux et sur Windows, où on détaillera les configurations effectuées.

IV.2. Environnement de travail

Pour la réalisation de ce travail, nous avons opté pour l'utilisation de la VMware Workstation, et la réalisation avec Windows Server 2008.

IV.2.1. VMware Workstation

VMware Workstationest un outil indispensable qui constitue pour, les développeurs, testeurs et autres professionnels de l'informatique du monde entier, un puissant logiciel de création et d'utilisation de machines virtuelles. Son utilitéconsiste à faire fonctionner sur un seul ordinateur plusieurs systèmes d'exploitation, comme si ces derniers fonctionnaient sur des ordinateurs distincts, comme: Windows, Linux, Solaris…

VMware Workstation est une technologie éprouvéequi vise les intérêts suivant :

- l'utilisation optimale des ressources
- l'installation, déploiement et migration facile des machines virtuelles
- l'économie sur le matériel

-l'installation, tests, développements, cassage et possibilité de recommencer sans casser le système d'exploitation hôte.

IV.2.2. Windows Server 2008

Windows Server 2008 permet aux professionnels de l'informatique d'accroître la flexibilité et la fiabilité de leur infrastructure de serveur. Elle constitue également, pour lesdéveloppeurs, une plateforme Web et d'applications plus solide pour la création d'applications et de services connectés.

IV.3. Réalisation

Pour rester dans le cadre de notre projet, et après avoir constaté que l'entreprise Sonatrach utilise le protocole d'authentification RADIUS, nous avons suggéré de réaliser l'étude de l'authentificationKerberos sur Linux et sur Windows. Donc on va présenter l'étude de l'authentification Kerberos dans deux environnements : environnement linux et environnement Windows.

IV.3.1. Environnement Linux

Avant de procéder à l'installation de Kerberos sous Linux, il est important de définir quelques commandes et fichiers utilisés durant celle-ci.

➢ Fichiers et commandes

- **/etc/krb5.conf :** C'est le fichier (ASCII) qui permet de définir, pour un système donné, les différents domaines Kerberos disponibles. Pour chacun d'eux, on spécifie le KDC, le domaine, etc...Il précise également les comportements par défaut des clients et serveurs qui s'exécutent sur le système.
- **/etc/krb5.keytab :**Ce fichier (binaire) contient les clés de cryptage des services Kerbérisés. C'est là qu'un tel service récupère sa clé de décryptage pour pouvoir lire les tickets que lui présenteront les clients. Ce fichier est généré par le KDC, qui a créé la clé.
- **Kinit :** C'est la commande qui permet d'obtenir un TGT auprès du KDC. L'utilisateur fournit son nom et son mot de passe, et il reçoit le ticket. Puis il ne lui sera plus nécessaire de les saisir lorsqu'il s'adressera à un des services Kerbérisés du domaine.
- **Klist :** C'est la commande qui permet de lister les tickets en possession de l'utilisateur. Cela comprend le TGT comme les tickets de service, et le fait qu'ils soient périmés ou non.
- **Kdestroy :** Cette commande sert à vider le cache qui contient tous les tickets acquis, y compris les TGT.
- **Kadmin :** Utilisée par un administrateur, cette commande sert à administrer les KDCs à distance. kadmin.local offre les mêmes services, mais s'exécute en local sur le KDC.
- **Ktutil :** Cette commande est utilisée pour manipuler les clés des services Kerbérisés. Elle permet notamment d'ajouter des clés du KDC dans le fichier krb5.keytab.

- **Installation du serveur Kerberos sous Linux**

Avant de commencerl'authentification Kerberos sous Linux,nous devant installer et configurer le serveur **DNS** (Domain Name System) ainsi le serveur du temps **NTP**(protocole de synchronisation de réseau). Car, si les horloges du serveur et du client diffèrent de plus de cinq minutes, les clients ne pourront pas s'authentifier sur le serveur **[w9]**.

Cette synchronisation de l'horloge est nécessaire pour empêcher un agresseur d'utiliser un ancien authentificateur pour se déguiser en un utilisateur valide.

- **Installer et configurer le KDC Kerberos**.

1. Dans cette première partie, nous allons utiliser les paquets Debian fournis par la commande "**apt-get**". Et nous enchainerons avec le lancement de la commande suivante :

```
# apt-cache search krb5
```

Nousobtenons une grande quantité de modules, mais si nous nous attardons sur ceux qui commencent par "krb5-" nous obtenons:

```
# apt-cache search krb5
krb5-config - Configuration files for Kerberos Version 5
krb5-auth-dialog - tray applet for reauthenticatingkerberos tickets
krb5-admin-server - MIT Kerberos master server (kadmind)
krb5-kdc-ldap - MIT Kerberos key server (KDC) LDAP plugin
krb5-kdc - MIT Kerberos key server (KDC)
krb5-multidev - Development files for MIT Kerberos without Heimdal conflict
krb5-pkinit - PKINIT plugin for MIT Kerberos
krb5-user - Basic programs to authenticate using MIT Kerberos
krb5-doc - Documentation pour MIT Kerberos
krb5-clients - Secure replacements for ftp, telnet and rsh using MIT Kerberos
krb5-ftpd - Secure FTP server supporting MIT Kerberos
krb5-rsh-server - Secure replacements for rshd and rlogind using MIT Kerberos
krb5-telnetd - Secure telnet server supporting MIT Kerberos
```

Dans la liste on peut remarquer les paquets suivants :

- krb5-admin-server : permet d'installer notre admin-server.
- krb5-config : permet d'obtenir les fichiers de configuration pour Kerberos 5.
- krb5-kdc : permet d'installer le KDC.

- krb5-user : permet d'obtenir les commandes pour une authentification basique en utilisant Kerberos.

2. En second lieu nous exécutons donc la commande pour installer ces quatre paquets :

```
# apt-get install krb5-admin-server krb5-config krb5-kdc krb5-user
```

Lors de l'installation du paquet par apt-get, il nous est demandé le nom du royaume (realm) Kerberos par défaut. Il nous est ensuite demandé le nom du serveur Kerberos duroyaume choisit précédemment, ainsi que le nom du serveur d'administration. Nous avons précisé "server-kdc", le nom de notre station.

3. Maintenant, nous affectons une adresse à la station déjà créée à l'aide de cette commande :

```
# cat /etc/hosts
```

➢ **Configuration du royaume Kerberos**

Dans cette deuxième partie nous procéderons à la configuration du royaume,voici le contenu de notre fichier /etc/krb5.conf :

```
# cat /etc/krb5.conf
[libdefaults]
default_realm = ESSAI
....
[realms]
ESSAI = {
kdc = server-kdc
admin_server = server-kdc
}
```

Ce qui permet de préciser à la librairie Kerberos de notre machine les informations sur :

- le royaume par défaut.
- l'adresse du KDC et du serveur **admin** de notre Kerberos.

Le contenu de notre fichier "/etc/krb5kdc/kdc.conf " correspondant à la configuration du KDC.Ce fichier contient :

- Les informations sur les bases de données Kerberos, des Keytab et des ACL.
- Les ports du KDC.

- Les informations sur les encodages supportés et sur les durées de vie des tickets.

Maintenant que la configuration est effectuée, nous allons maintenant créer la base de données "database_name" avec l'outil "kdb5_util". Nous choisissons "test" comme mot de passe du KDC.

```
# kdb5_util -r ESSAI create –s
```

La commande kadmin.local nous permet ainsi de nous connecter en local sur l'admin-server et de pouvoir créer des politiques, des principals...

```
# kadmin.local
```

- **Création des policy**

- La création de policy se fait avec la commande suivante :

```
add_policy -minlength 12 -maxlife "60 days" admin
```

Cette commande va créer la politique longueur minimale de mot de passe de 12 caractères et d'une durée de vie de 60 jours pour admin.

- La liste des policy pour un user se fait avec : get_policy<user>

- **Création de comptes**

Nous allons maintenant ajouter plusieurs comptes : « hello/admin@ESSAI »et « world@ESSAI », On va donc ajouter ces principales avec ces commandes :

```
kadmin.local: add_principal -policy admin hello/admin@ESSAI
kadmin.local: add_principal -policy users world@ESSAI
```

- **Création des ACLs**

Pour créer des ACLs, nous devons créer le fichier "kadm5.acl" dans /etc/krb5kdc/kadm5.acl (selon la directive acl_file de notre fichier /etc/krb5kdc/kdc.conf).

La syntaxe est la suivante : Kerberos_principal permissions [target_principal] [restrictions]

Soit notre fichier kdadm5.acl :

```
# cat /etc/krb5kdc/kadmin.acl
hello/admin@ESSAI *
```

Pour pouvoir utiliser "kadmin" en distant, nous devons créer les keytab pour les deux utilisateurs kadmin/admin et kadmin/changepw :

```
kadmin.local: ktaddkadmin/admin kadmin/changepw
Entry for principal kadmin/admin with kvno 5, encryption type AES-256 CTS … added to keytab
WRFILE:/etc/krb5.keytab.
Entry for principal kadmin/admin with kvno 5, encryption type ArcFour...HMAC/md5 added to keytab
WRFILE:/etc/krb5.keytab.
Entry for principal kadmin/admin with kvno 5, encryption type Triple DES... added to keytab
WRFILE:/etc/krb5.keytab.
Entry for principal kadmin/admin with kvno 5, encryption type DES cbc … CRC-32 added to keytab
WRFILE:/etc/krb5.keytab.
Entry for principal kadmin/changepw with kvno 4, encryption type AES-256 CTS … added to keytab
WRFILE:/etc/krb5.keytab.
Entry for principal kadmin/changepw with kvno 4, encryption type ArcFour … added to keytab
WRFILE:/etc/krb5.keytab.
Entry for principal kadmin/changepw with kvno 4, encryption type Triple DES ... added to keytab
WRFILE:/etc/krb5.keytab.
Entry for principal kadmin/changepw with kvno 4, encryption type DES cbc … CRC-32 added to keytab
WRFILE:/etc/krb5.keytab.
```

Maintenant que tout est configuré, nous pouvons donc démarrer krb5kdc et kadmind pour pouvoir utiliser kadmin en local et en distant.

```
# krb5kdc
# kadmind
```

Ou :

```
# /etc/init.d/krb5-kdc start
# /etc/init.d/krb5-admin-server start
```

- **Utilisation de kinit et klist**

Nous allons maintenant utiliser deux commandes :

- kinit : qui va initialiser une connexion Kerberos

- klist : qui va montrer les sessions Kerberos

```
# kinitworld@ESSAI
Password for world@ESSAI:
# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: world@ESSAI
Valid starting Expires Service principal
05/04/15 18:35:45 05/05/15 04:35:45 krbtgt/ESSAi@ESSAI
renew until 05/05/15 18:35:49
```

IV.3.2. Environnement Windows

A présent, on passe à la réalisation sur l'environnement Windows server 2008. Pour ce faire, on doit tout d'abord installer certains services nécessaires au fonctionnement de cette partie de réalisation.

Avons tout installation, nous allons commencer d'abord par fixer une adresse IP et un Masque de sous réseau ainsi l'adresse de serveur DNS et WINS a notre serveur

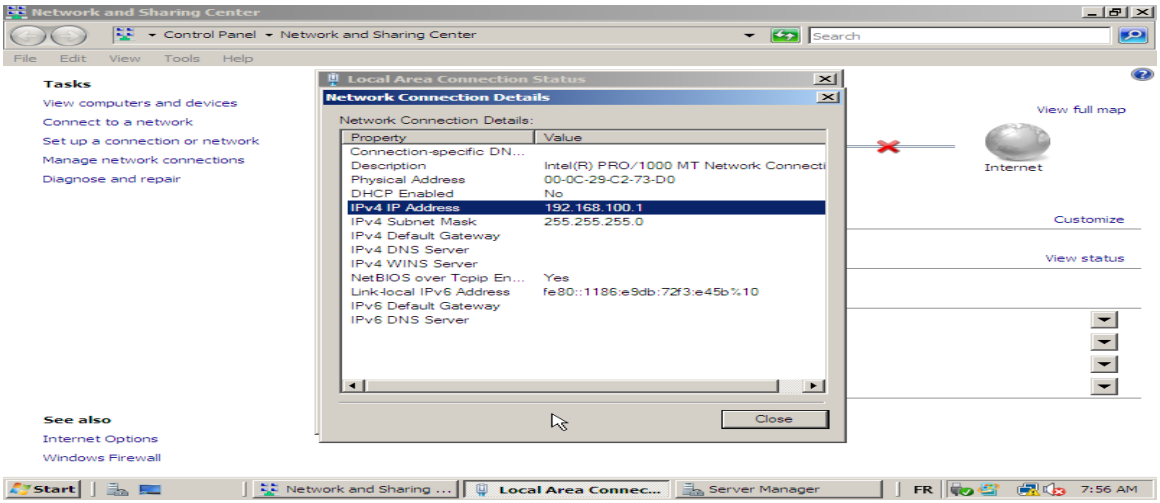


Figure IV-1 :Fixer les adresses au serveur

Puis l'installation des services nécessaires on commence tout d'abord par le DHCP.

➢ DHCP

Le DHCP (Dynamic Host Configuration Protocol) est un protocole réseau qui a pour but de simplifier l'administration d'un réseau. Le protocole DHCP offre un moyen de centraliser la configuration des machines du réseau, en mettant à disposition un serveur au sein d'un réseau local.

Le serveur fournit aux machines clientes leurs paramètres TCP/IP :

- L'adresse IP ;
- Le masque de sous réseau ;
- La passerelle par défaut ;
- L'adresse des serveurs de noms (NetBIOS/WINS ou DNS) ;
- Le type de nœud NetBIOS ;
- Le nom de domaine Internet

Ainsi le protocole DHCP permet à un ordinateur qui se connecte au sein d'un réseau d'obtenir dynamiquement sa configuration tout en évitant les conflits d'adresses. Il évite également la reconfiguration des ordinateurs portables lors d'un changement de réseau.

L'administrateur peut facilement avoir un œil sur son réseau, et connaître les adresses allouées aux clients DHCP. Ces adresses sont allouées par un mécanisme de bail. Le temps d'expiration du bail peut être fixe ou illimité.

Une machine conserve son bail jusqu'à son expiration et essaiera de le renouveler avec la même adresse si possible.

1- Puis pour lancer lesétapes d'installations, on clique sur **Add Role**, qui se trouve dans « Server Manager »

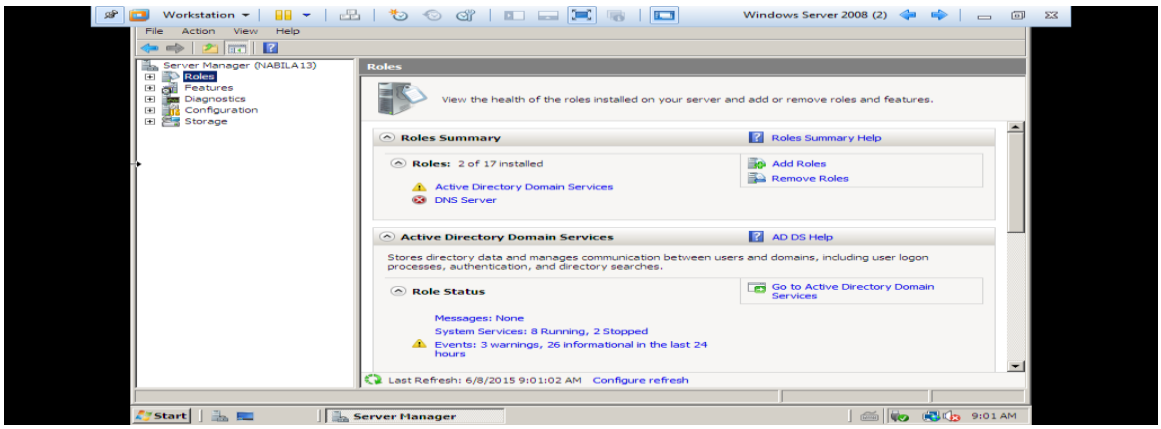


Figure IV-2 : Add Role pour installer le service DHCP

2- Ensuite, on nous demande de configurer les étendues d'adresse IP qui seront distribuées par le serveur.

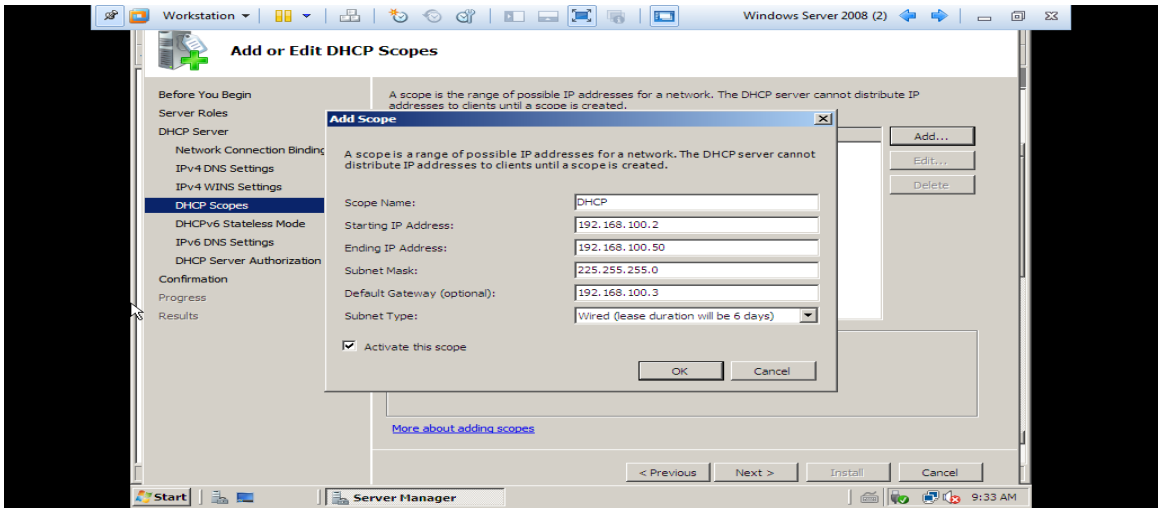


Figure IV-3 : Fixer la plage d'adresses pondant l'installation de service DHCP

3- Patientez quelques minutes pendant l'installation, puis fermez la fenêtre.

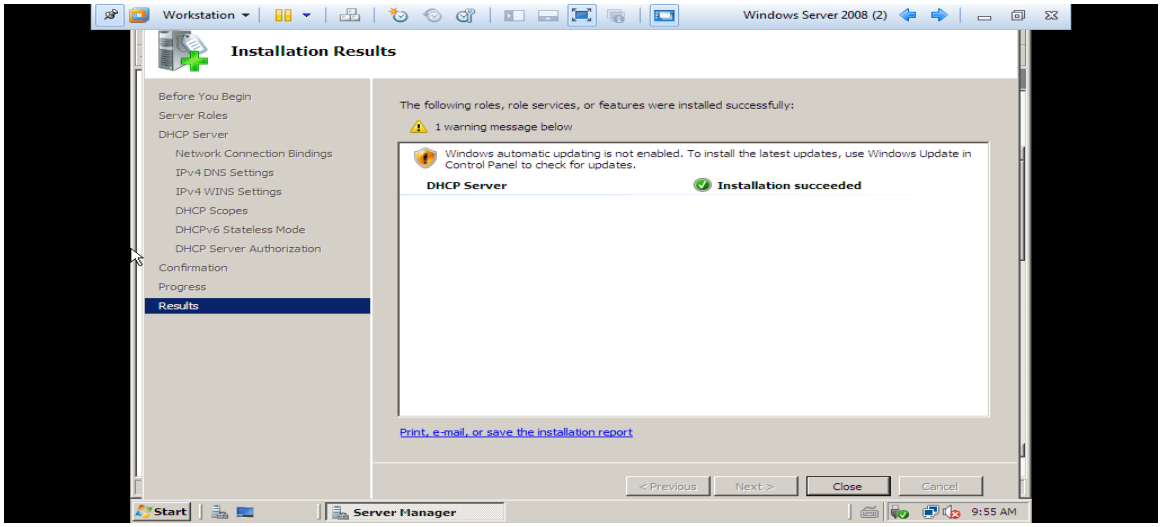


Figure IV-4 : Service DHCP installé

L'installation de DHCP est à présent terminée. Maintenant on doit installer le DNS.

➢ DNS

Domain Name System ou système de nom de domaine, est un service permettant d'établir uneconcordance entre des adresses IP et des noms de machines. La base de données est accessible avec un mécanisme client-serveur.

1- Pour l'installation de DNS, nous allons commencer d'abord par cliquer sur **AddRole**, qui se trouve dans « Server Manager »

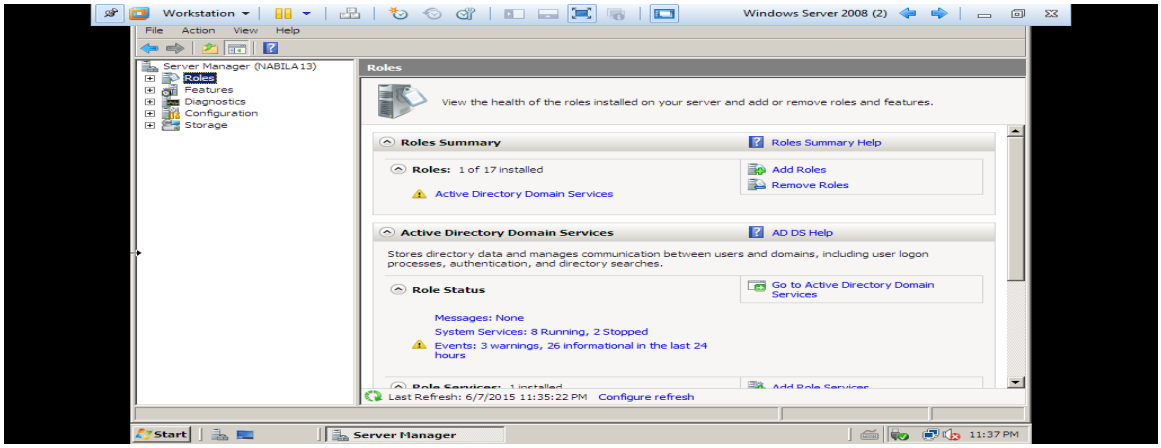


Figure IV-5 : Add Role pour installer le service DNS

2- Cliquez sur « installer », et patientez pendant l'installation

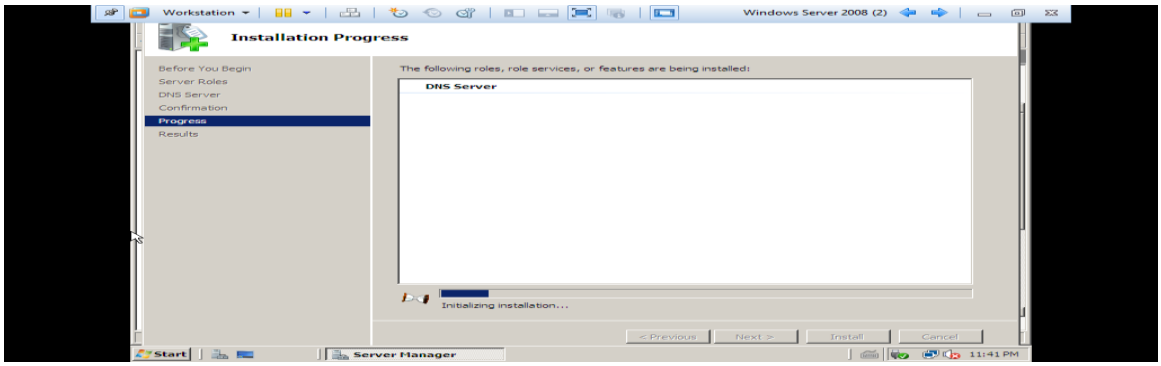


Figure IV-6 : progression d'installation de service DNS

3- Puis, on clique sur configurer pour configurer notre domaine

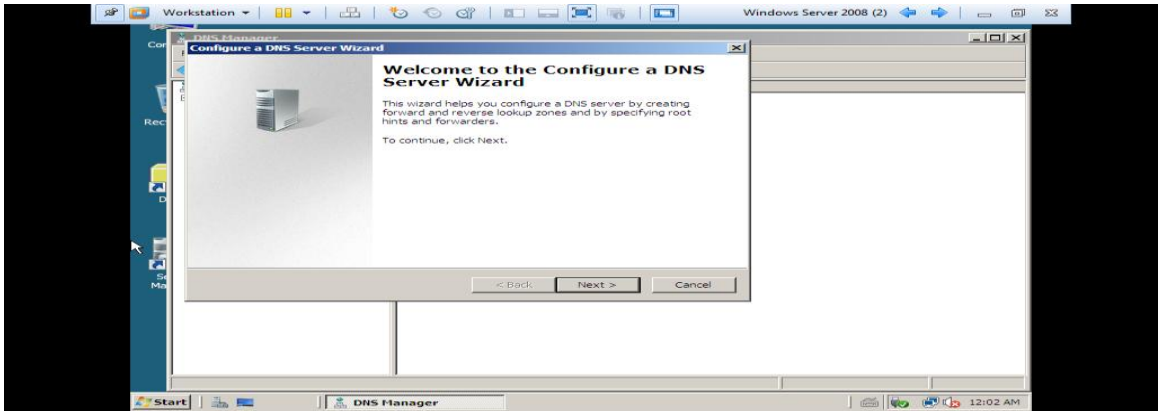


Figure IV-7 : Configuration de serveur DNS

4- Par la suite on spécifie le nom de Domaine

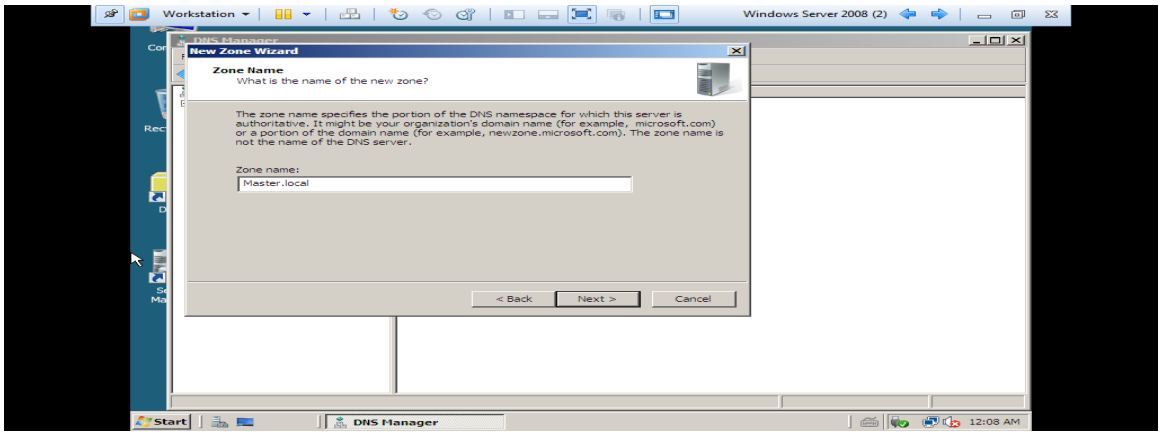


Figure IV-8 : spécifier le nom de domaine

5- Pour finir, nous allons configurer les adresses des DNS public sur lesquels notre serveur ira chercher les noms de site internet (exemple google.com).

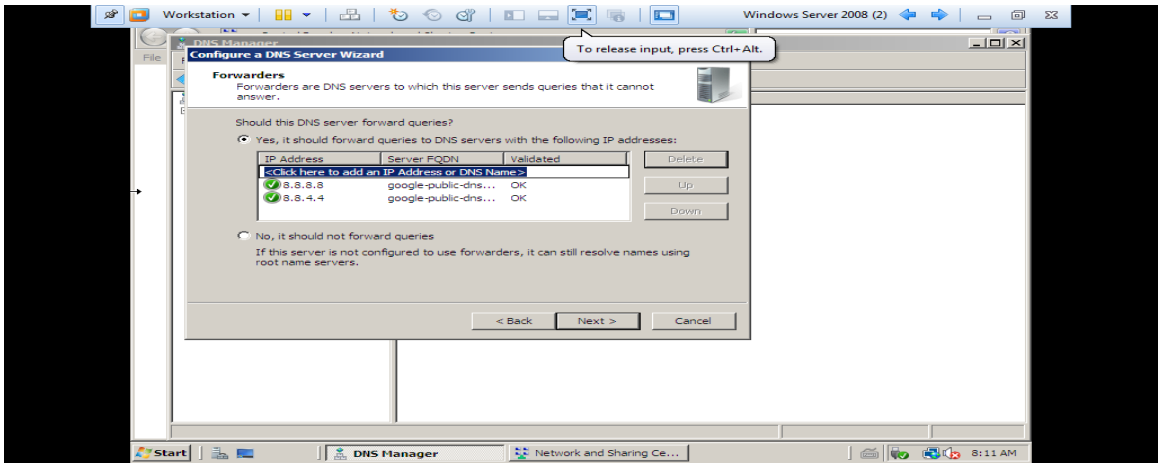


Figure IV-9 : configuration des DNS public

➢ Active directory

Active Directory (AD) est un annuaire introduit par Windows 2000 Server. Son implémentationpermet de centraliser des informations relatives aux utilisateurs et aux ressources d'une entreprise enfournissant des mécanismes d'identification et d'authentification tout en sécurisant l'accès aux données.

Pour configurer active Directory on install le service Active Directory à partir de Server Roles :

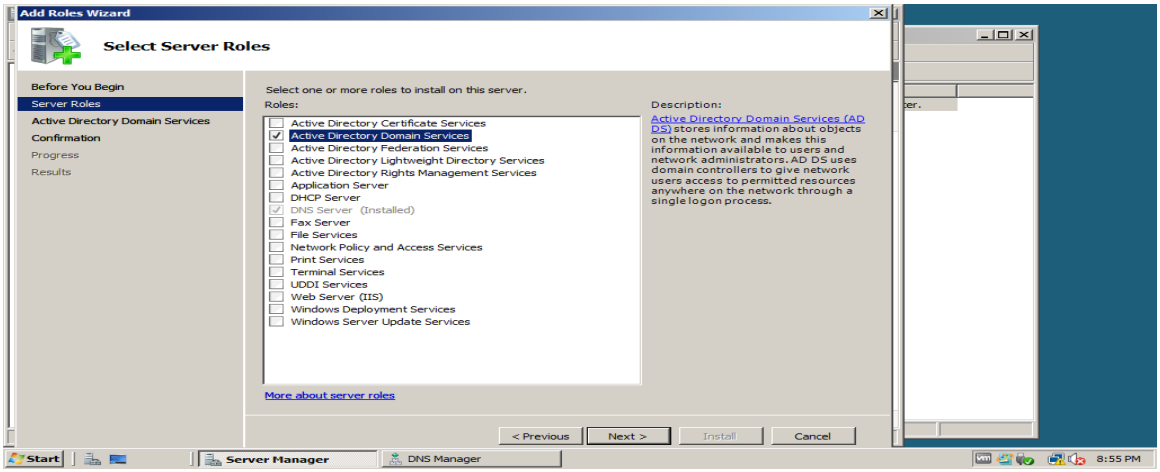


Figure IV-10 : installation de service Active Directory

1- Une fois le service, est installé on passe à la configuration de domaine Active Directory en cliquant sur **Dcpomo.exe** dans le Server Manager :

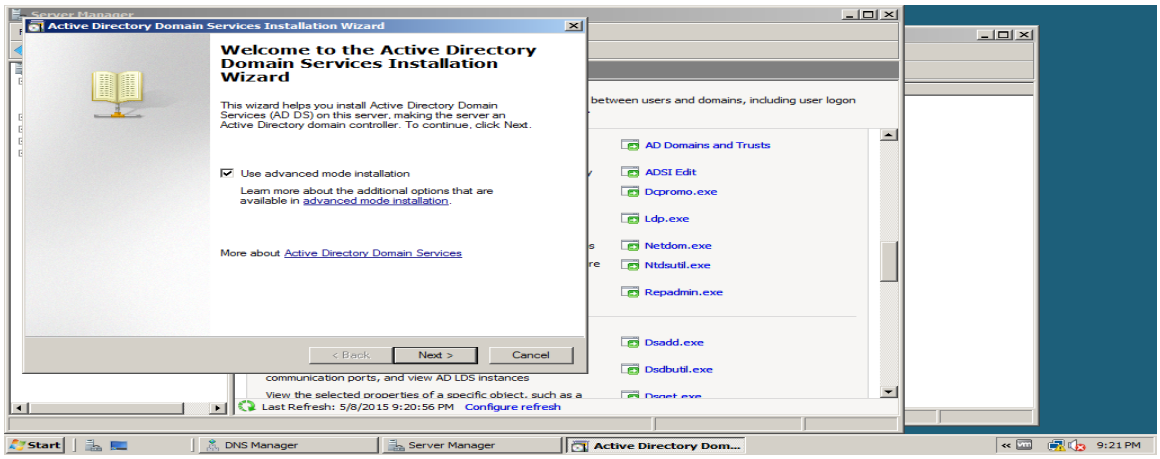


Figure IV-11 : le lancement de Dcpromo .exe

2- On poursuit l'installation jusqu'à la fin

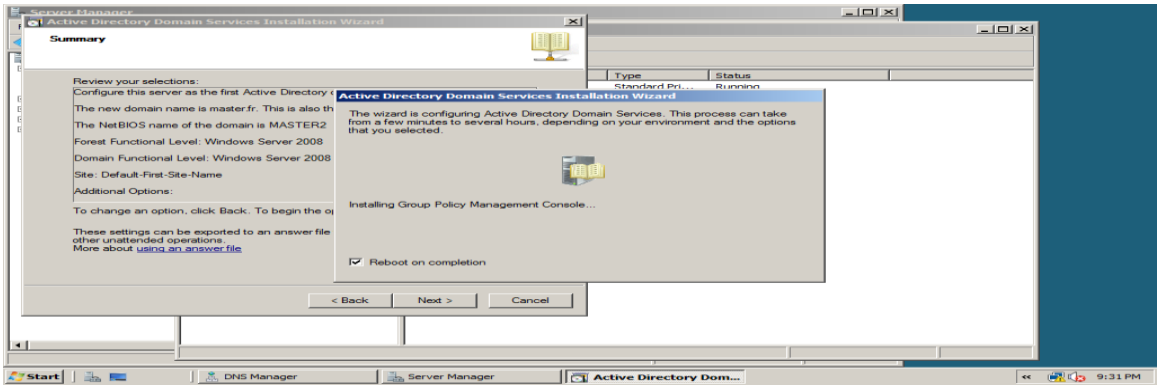


Figure IV-12 : progression de l'installation de Domaine Active Directory

➢ Serveur de fichiers

Un serveur de fichiers fournit un emplacement central sur le réseau où sont stocker les ressources (fichiers) et les partager avec des utilisateurs de ce réseau.

Lorsque les utilisateurs ont besoin d'un fichier important qui doit être accessible pour un grand nombre de personnes, ils peuvent accéder à distance au fichier situé sur le serveur de fichiers.

1- Pour l'installation de Serveur de fichier, nous allons cocher les services souhaités

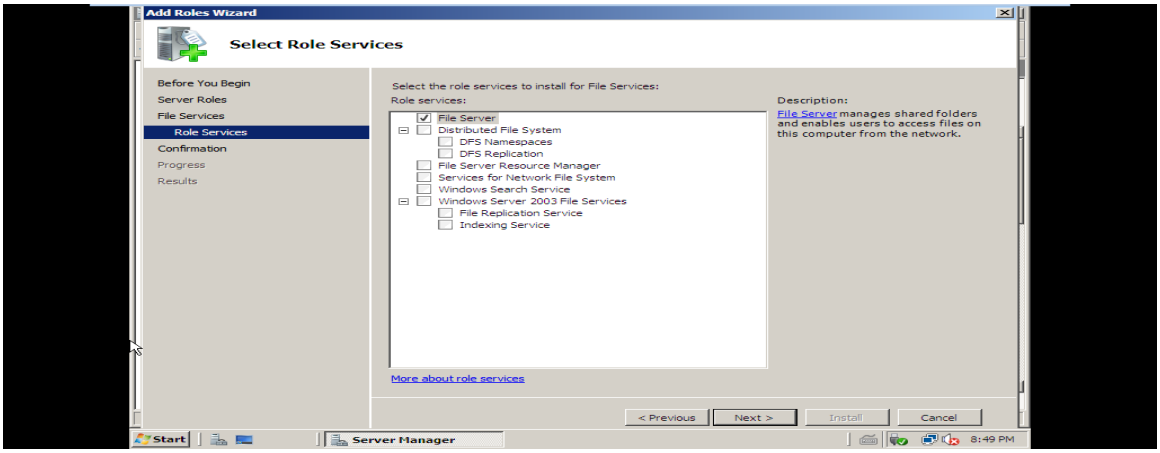


Figure IV-13 : installation de serveur de fichiers

2- On clique sur installer pour terminer

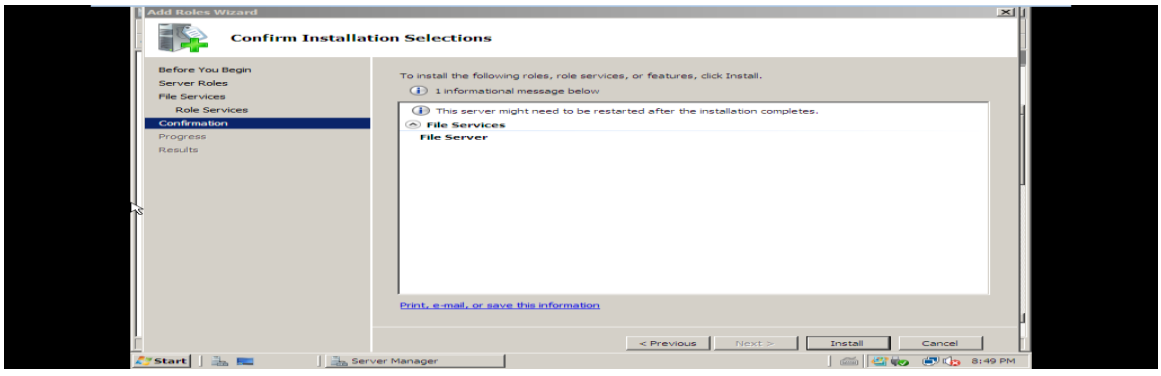


Figure IV-14 : Progression de l'installation de serveur de fichiers

IV.3.3. Création et configuration du royaume Kerberos

Pour créer et configurer notre protocole kerberos, on procède respectivement à :

- la création d'une approbation pour le royaume Kerberos,
- on associe chaque utilisateur ou groupe à ce royaume
- on procède à l'activation du centre de distribution des clés (le KDC)
- on spécifier les informations pour les mots de passe et les tickets de kerberos

- et pour finir on choisi le type de chiffrement à utilisé et limiter l'accès en attribuant des permissions selon le besoin.

➢ Création d'une approbation

Pour commencer on doit crée une approbation de confiance entre un domaine Active Directory et un royaume Kerberos

1. Lancement de l'approbation de confiance

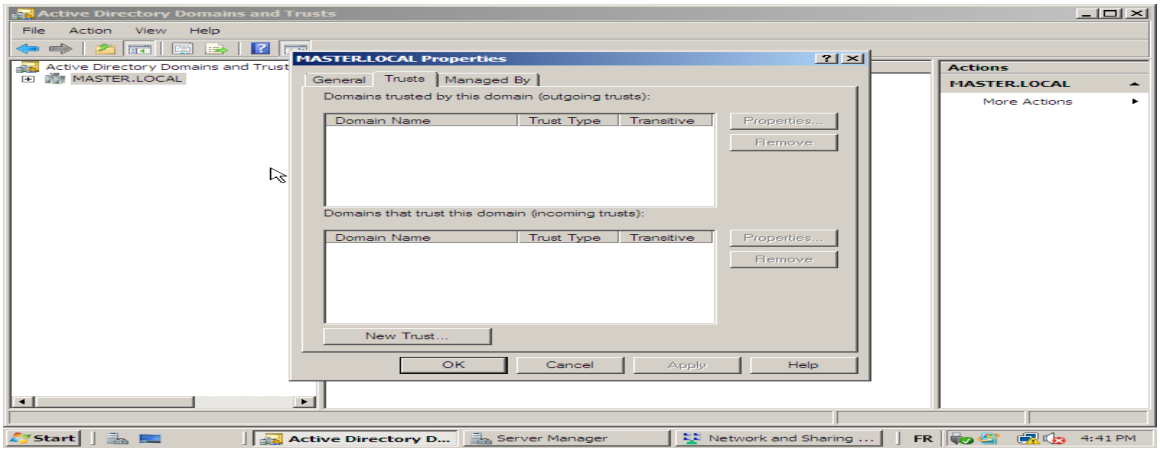


Figure IV-15 : Création d'une approbation

2. Création d'une nouvelle approbation de confiance

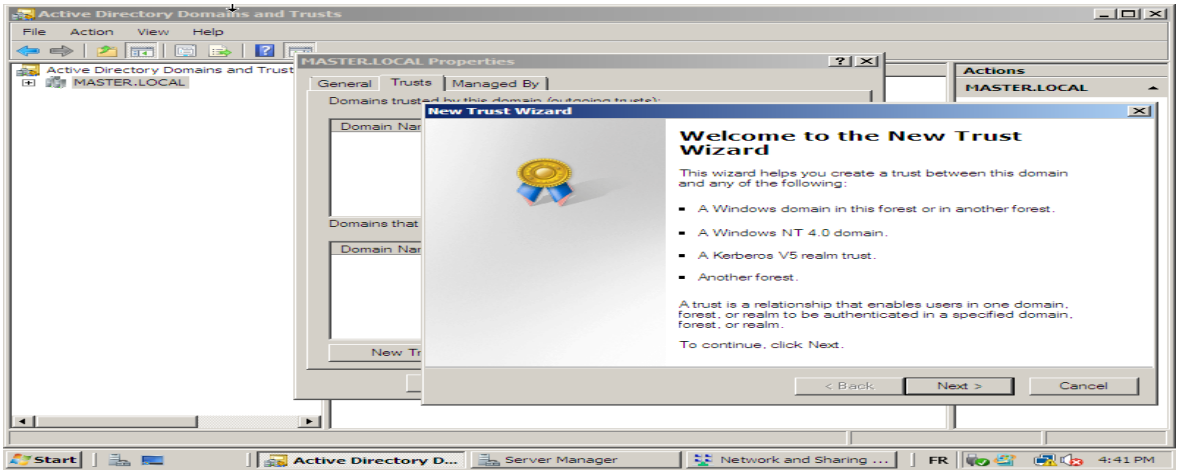


Figure IV-16 : installation d'une nouvelle approbation

3. On choisi l'approbation de confiance entre le domaine Active Directory et le royaume Kerberos :

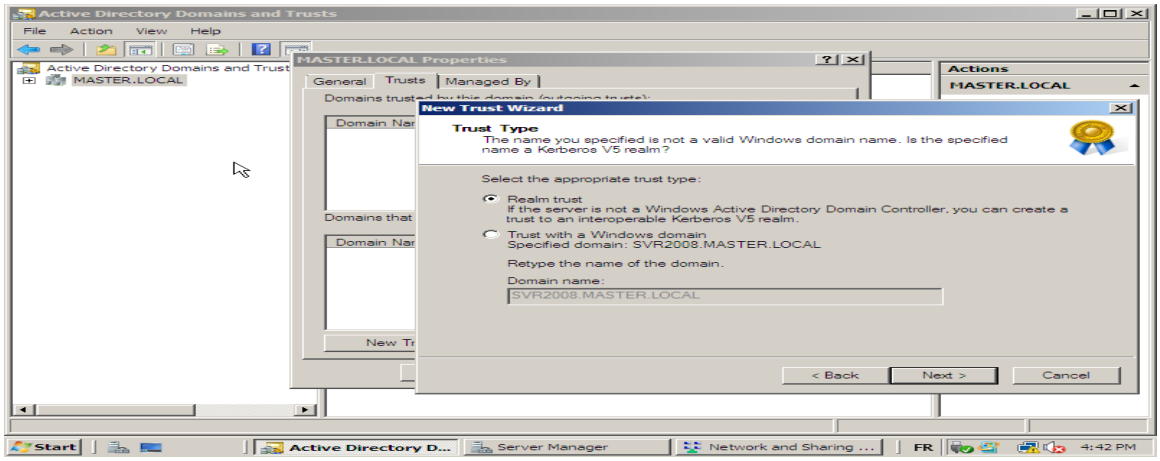


Figure IV-17 : Type de l'approbation

4. Ensuite on choisit la transitivité de l'approbation avec notre royaume kerberos :

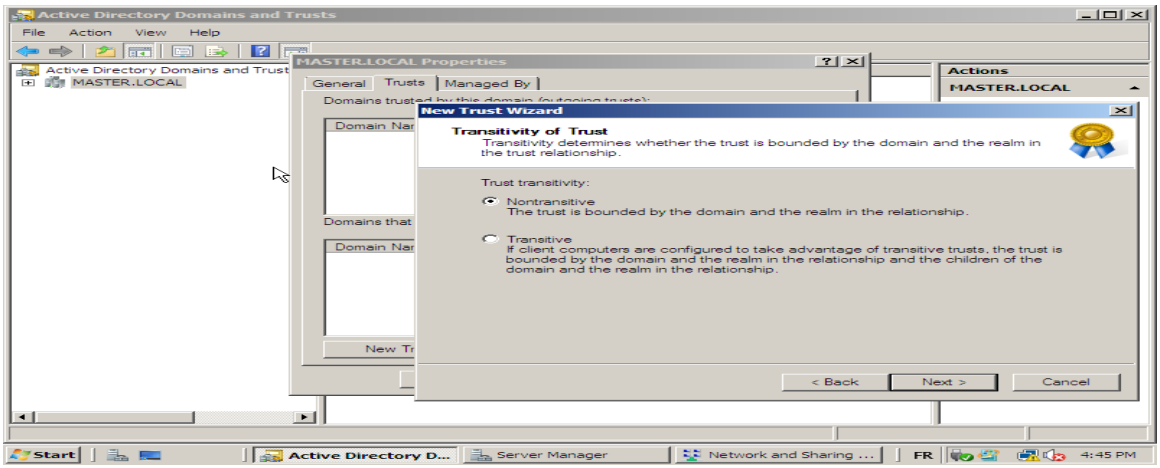


Figure IV-18 : sélectionner la transitivité de l'approbation

5. L'étape suivante consiste à spécifier la direction de l'approbation. Dans les deux sens, pour que le client sache qu'il s'adresse bien au AS et que le AS puisse authentifier à son tour le client :

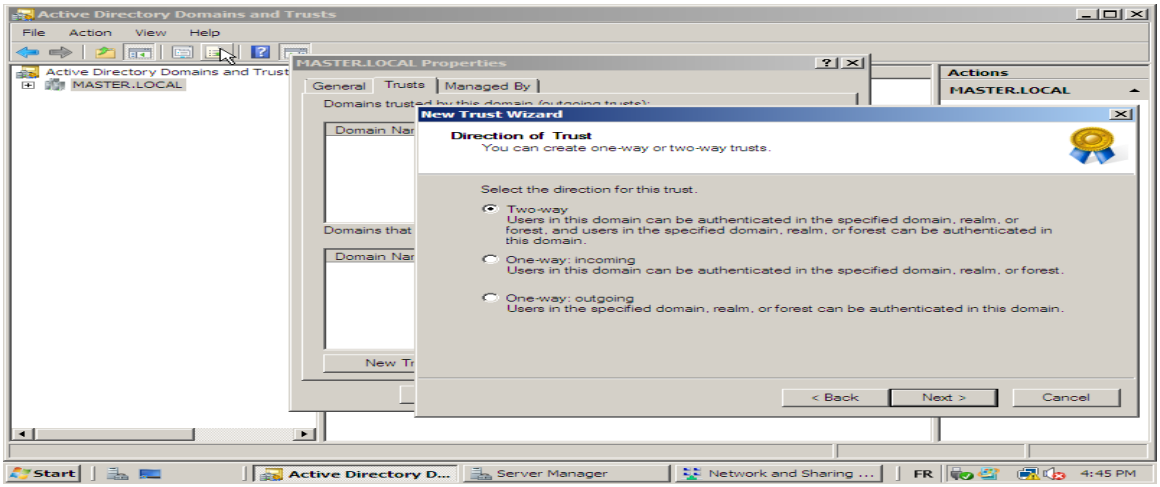


Figure IV-19 : sélectionner la direction de l'approbation

6. L'attribution des mots de passe pour cette approbation :

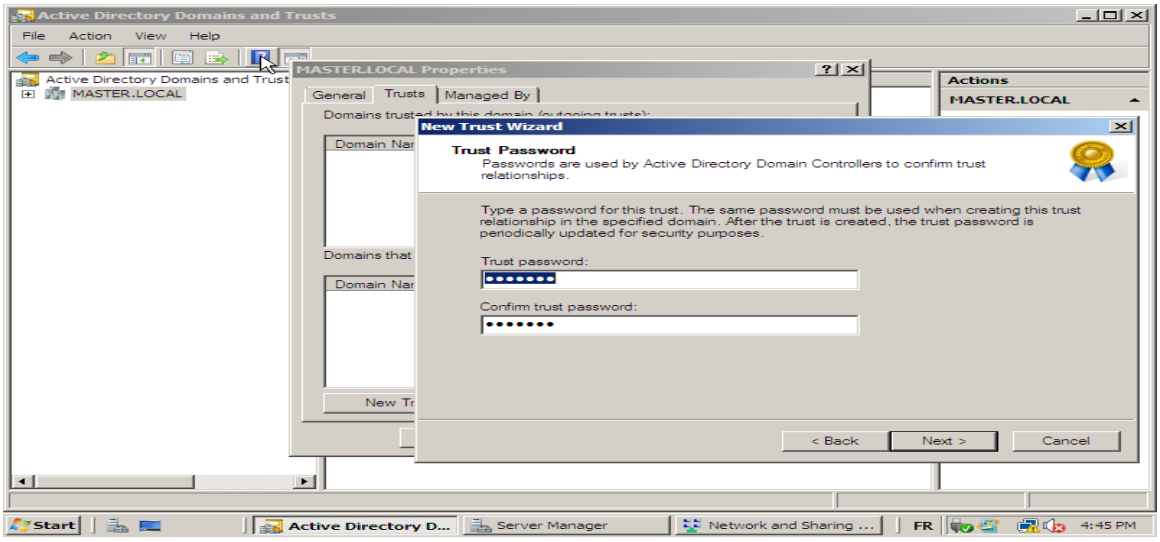


Figure IV-20 : création de mot de passe pour l'approbation

7. On aura le résultat de la fenêtre ci-dessous, donc l'approbation du royaume kerberos a été créée :

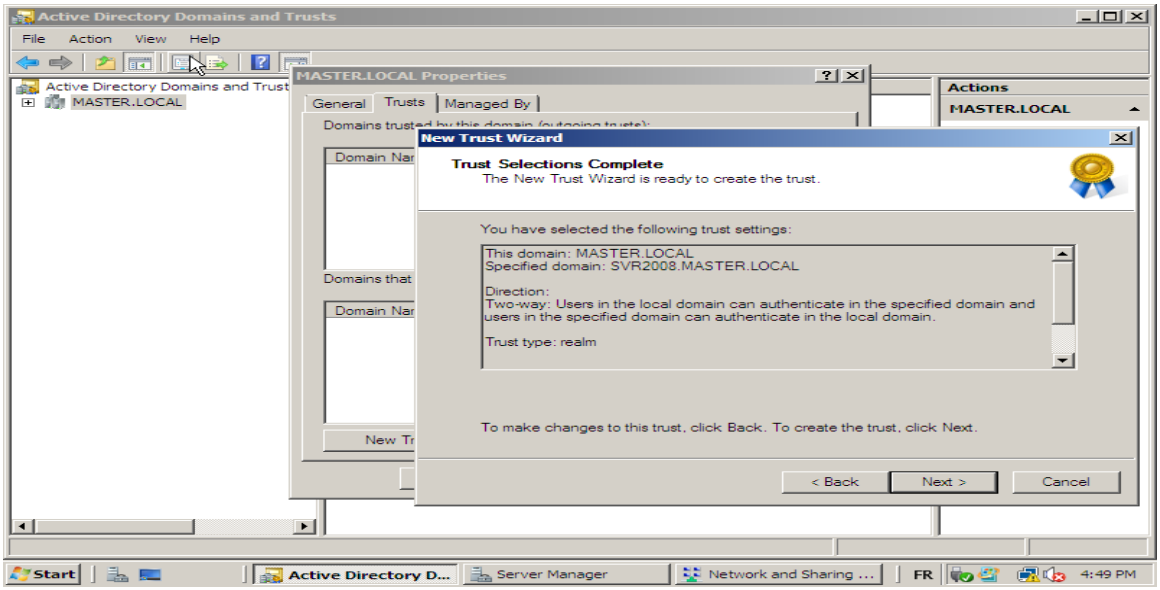


Figure IV-21 : fin de la création de l'approbation

8. Une fois l'approbation est créée on associe chaque groupe ou utilisateur à cette approbation :

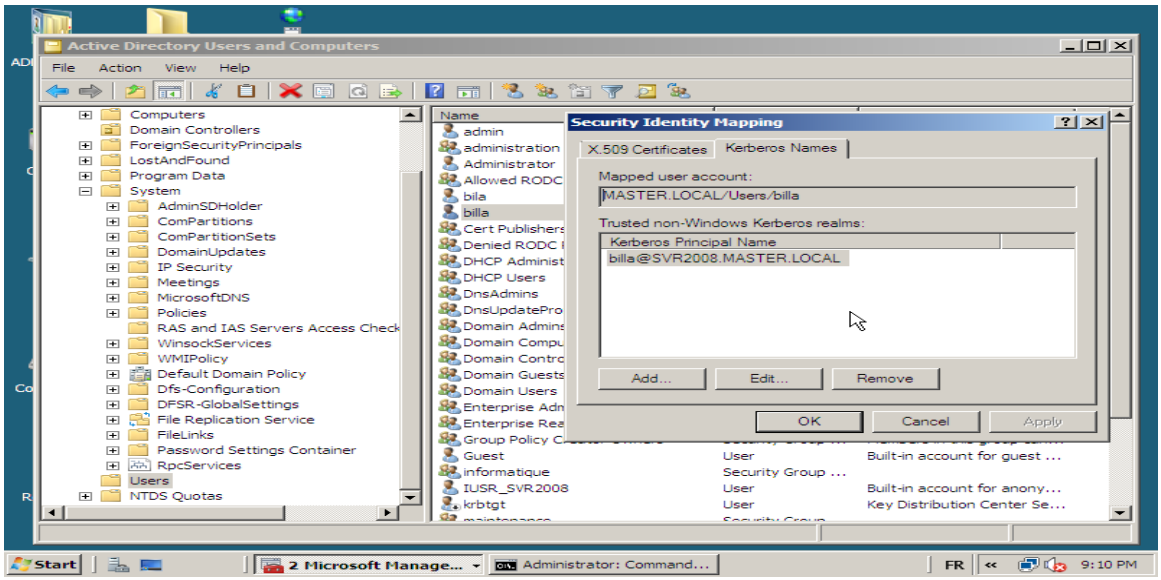


Figure IV-22 : associer les comptes a l'approbation créée

➢ Centre de distribution de clés (KDC)

Le centre de distribution de clés Kerberos qui se trouve dans system service doit être activé, donc on procédé à son activation :

1. Activation du KDC

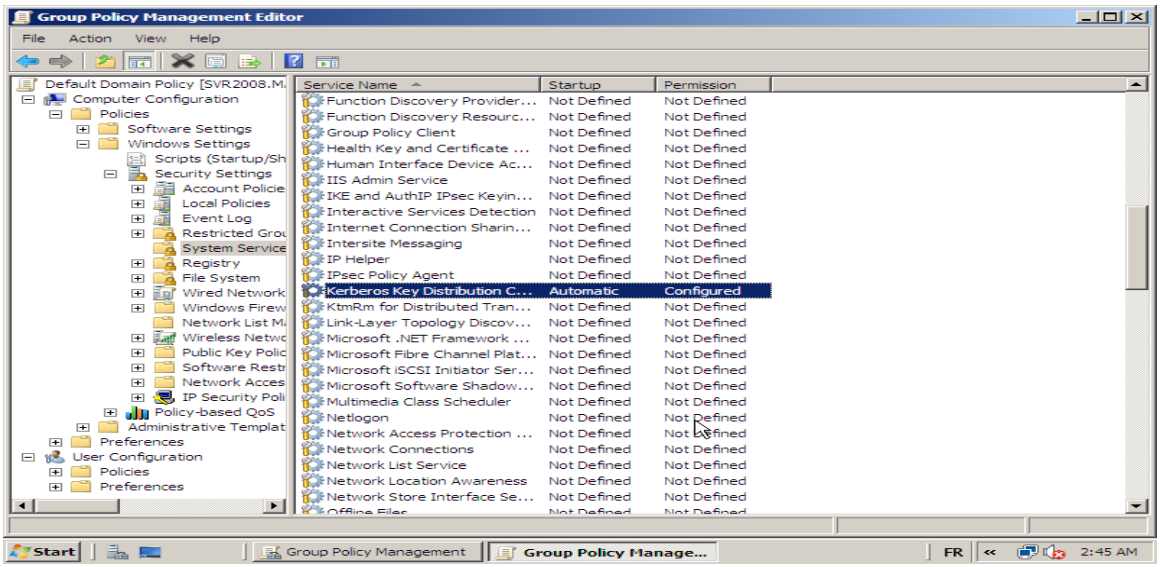


Figure IV-23 : Activation de Centre Distribution De Clés

La commande ksetup permet de vérifier que le domaine de royaume kerberos (realm) a bien été créé, donc on effectue la vérification.

2. Confirmation de création du royaume "realm"

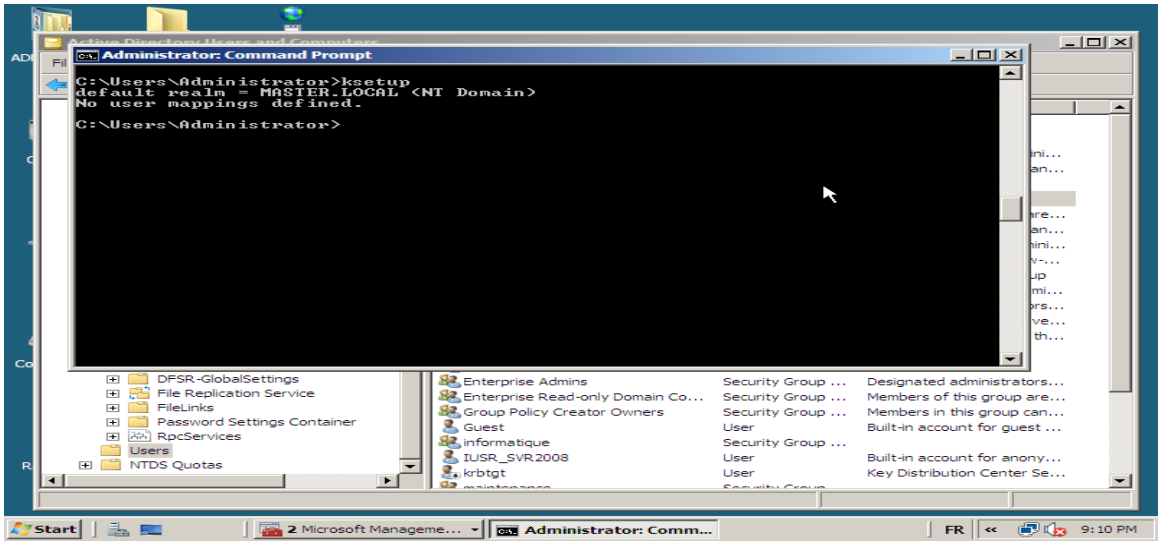


Figure IV-24 : test de la commande ksetup

➢ Délégation de groupe

Pour contrôler notre domaine avec l'utilisation unique de Kerberos, on choisit le type de délégation qu'on veut appliquer dans le système : *(dans notre cas : use Kerberosonly)*

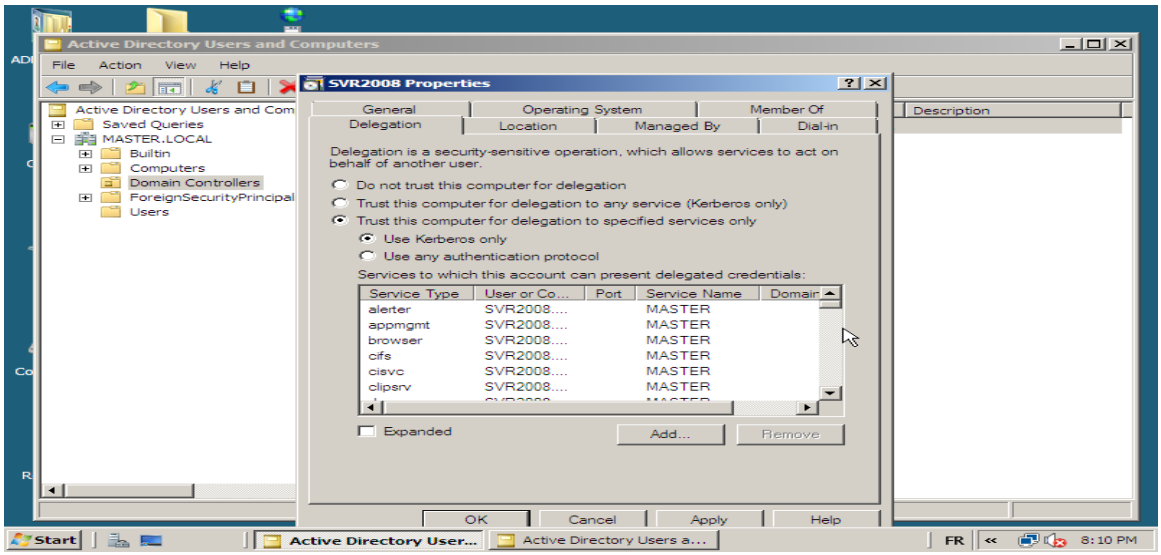


Figure IV-25 : spécifier la délégation de groupe pour le domaincontrollers

Une fois le domaine de KDC est crée, on spécifie les informations concernant les mots de passes et tickets de Kerberos :

Dans active Directory Users and Computers on fait apparaitre l'utilisateur « krbtgt »

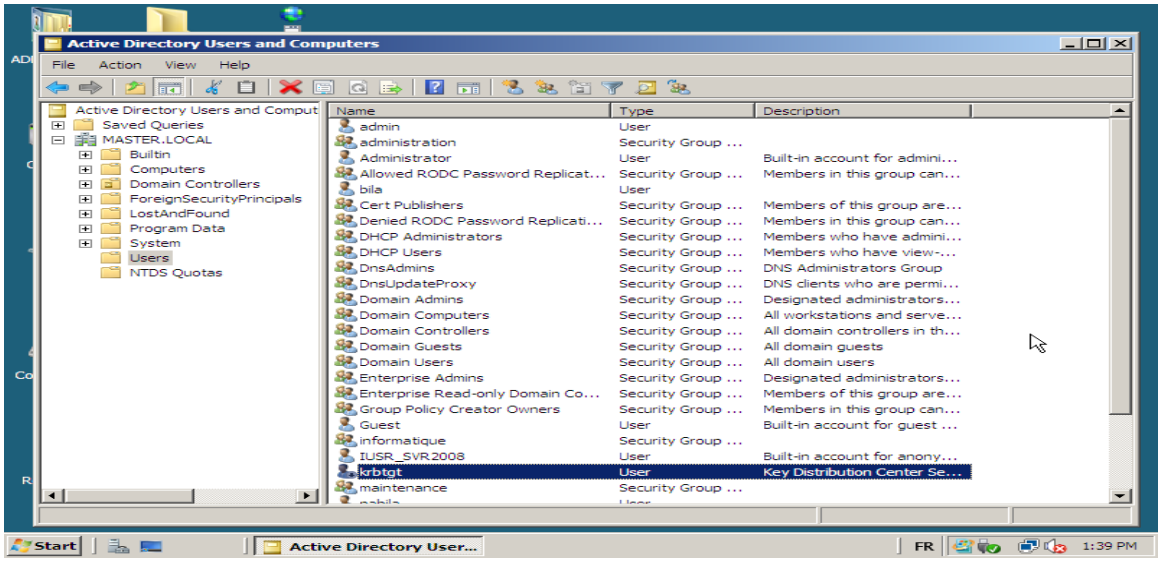


Figure IV-26 : faire apparaitre le krbtgt

Par la suite on enchaine avec la spécification des informations concernant les mots de passes et tickets de Kerberos, ceci ce fait dans Groupe Policy Management.

➢ Groupe policy management

1. On accéde au Groupe Policy Management :

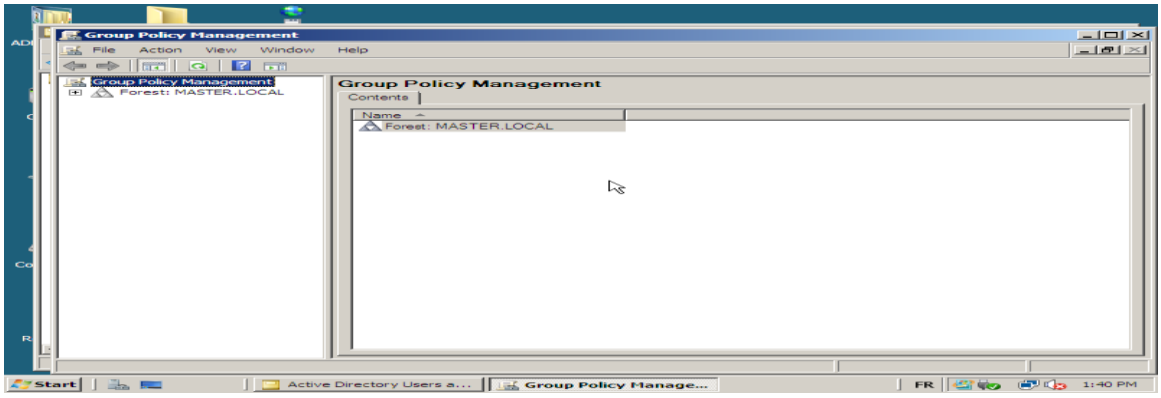


Figure IV-27 : Groupe Policy Management

2. La fenêtre qui suit montre le Default Domain Policy

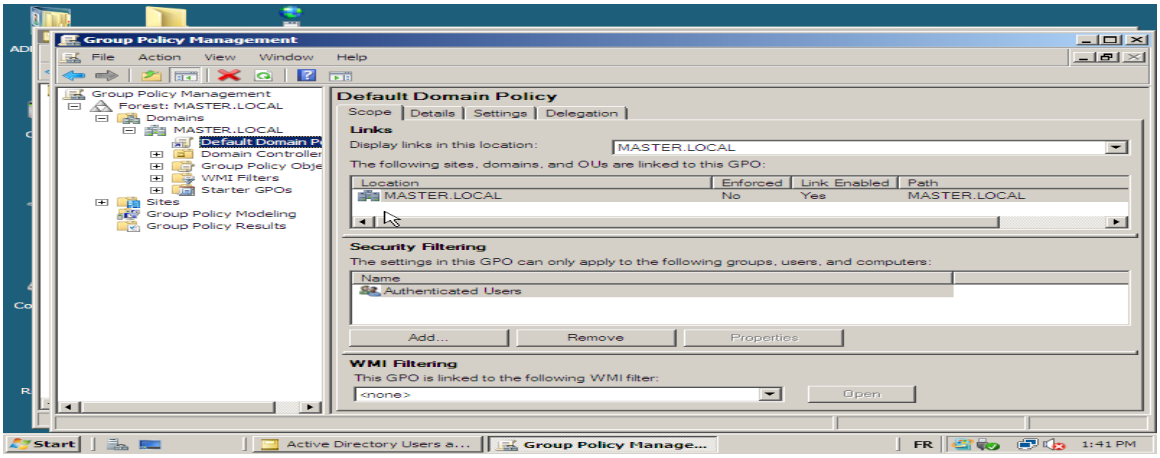


Figure IV-28 : Default Domain Policy

3. Dans l'arborescence on clique sur Edit pour éditer le Default Domain Policy :

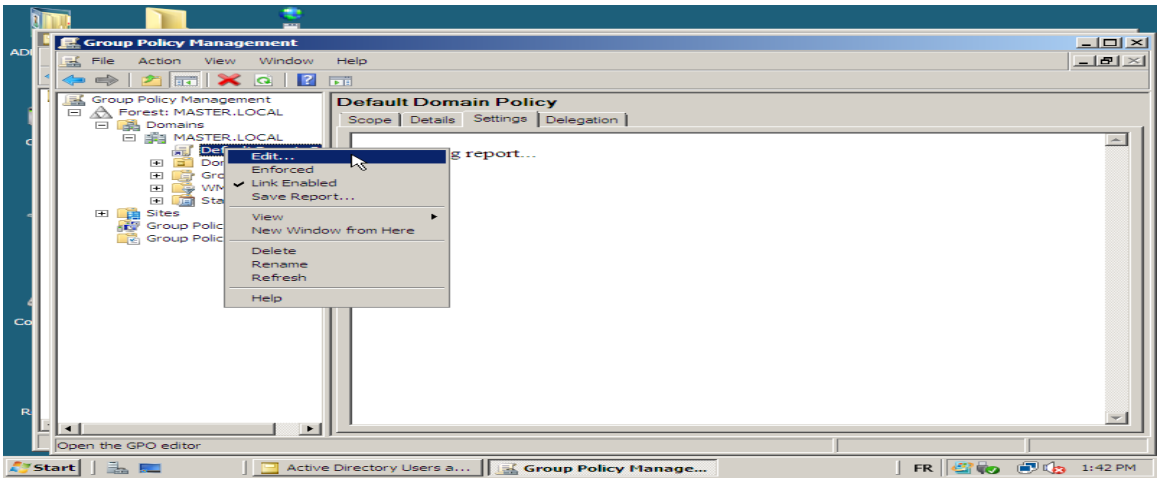


Figure IV-29 : éditer le Default Domain Policy

4. Donc la fenêtre Groupe Policy Management Editor va s'afficher :

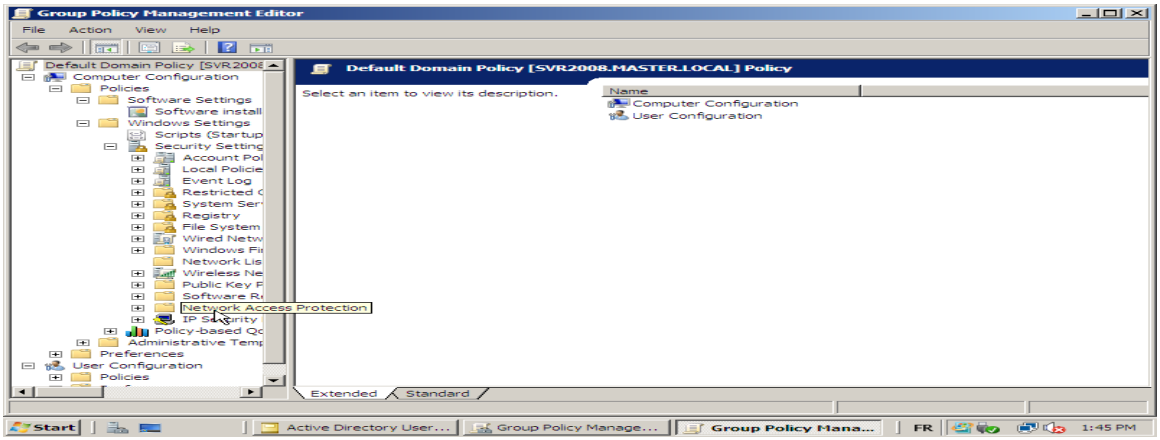


Figure IV-30 : Groupe Policy Management Editor

C’est ce qui va nous permettre de spécifier les informations propres aux mots de passe et tickets Kerberos :

✓ **Password Policy contient :**

- La mémorisation des mots de passe ;
- Les durées de vie minimale et maximale des mots de passe ;
- La longueur des mots de passe

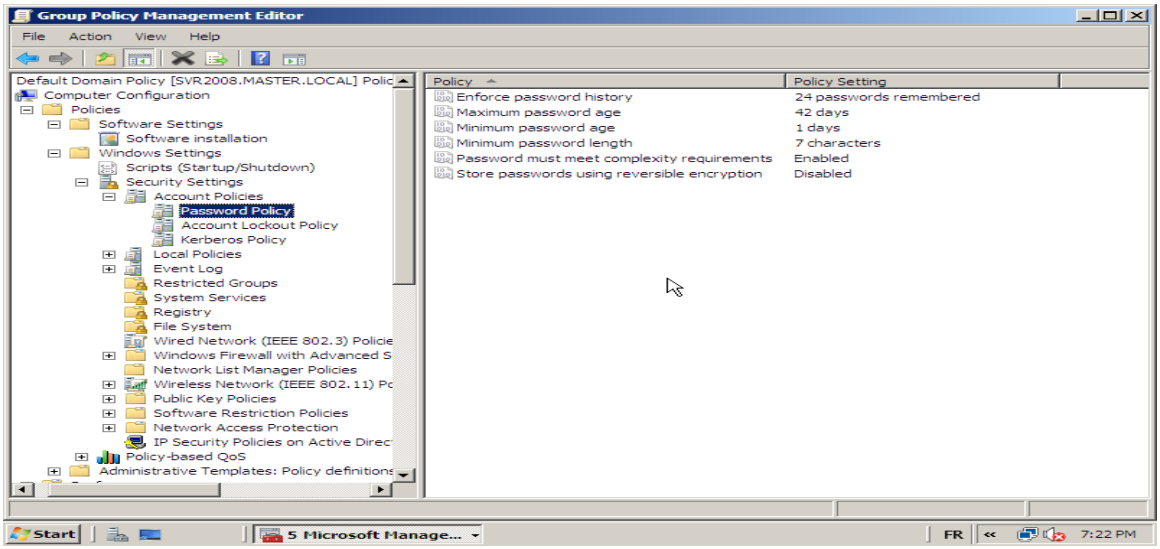


Figure IV-31 : Password Policy

✓ **Account Lockout Policy contient :**

- Le Compte Durée de verrouillage ;
- Le Seuil de verrouillage du compte ;
- Réinitialiser le compte Seuil de verrouillage Après

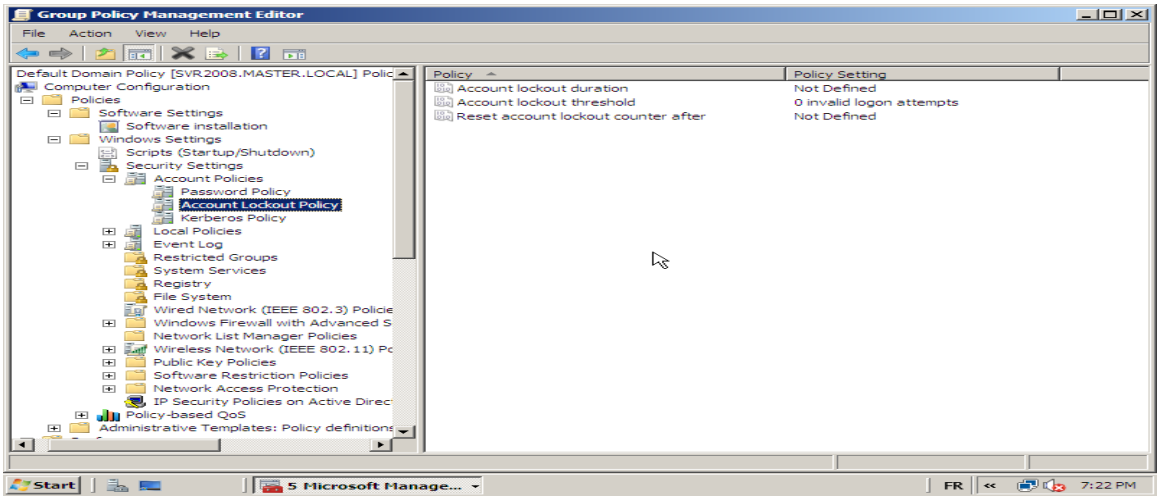


Figure IV-32 : Account Lockout Policy

✓ **Kerberos Policy contient :**

- la durée de vie des tickets de service ;
- la durée de vie maximale des tickets des utilisateurs et tickets des utilisateurs renewal ;
- la durée de synchronisation de temps entre les clients

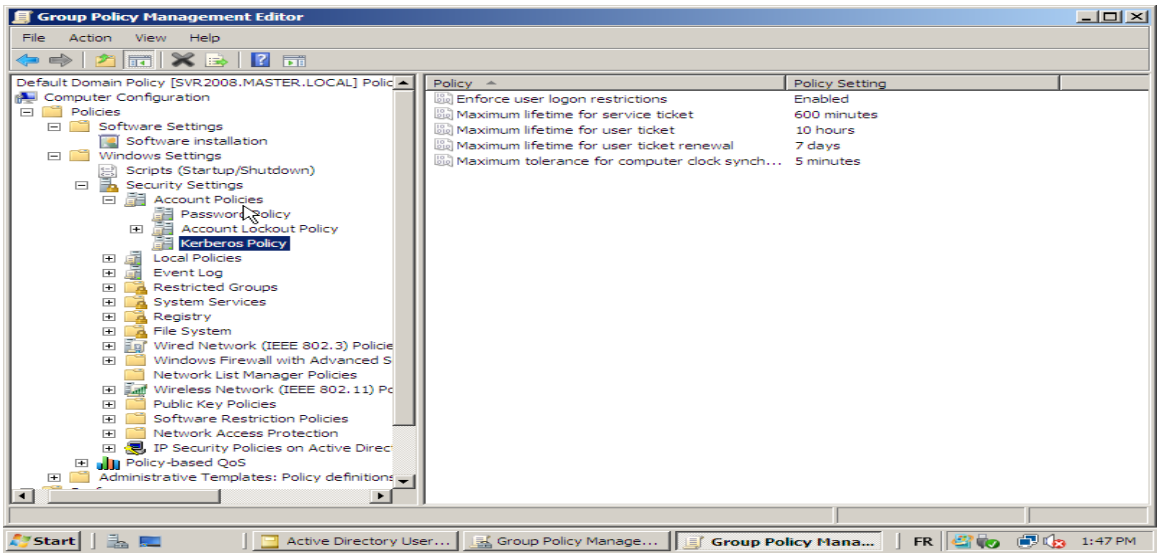


Figure IV-33 : Kerberos Policy

Par la suite on passe aux comptes des utilisateurs pour choisir le type de chiffrement à utilisé avec Kerberos :

1. Chiffrement des donnés pour un utilisateur

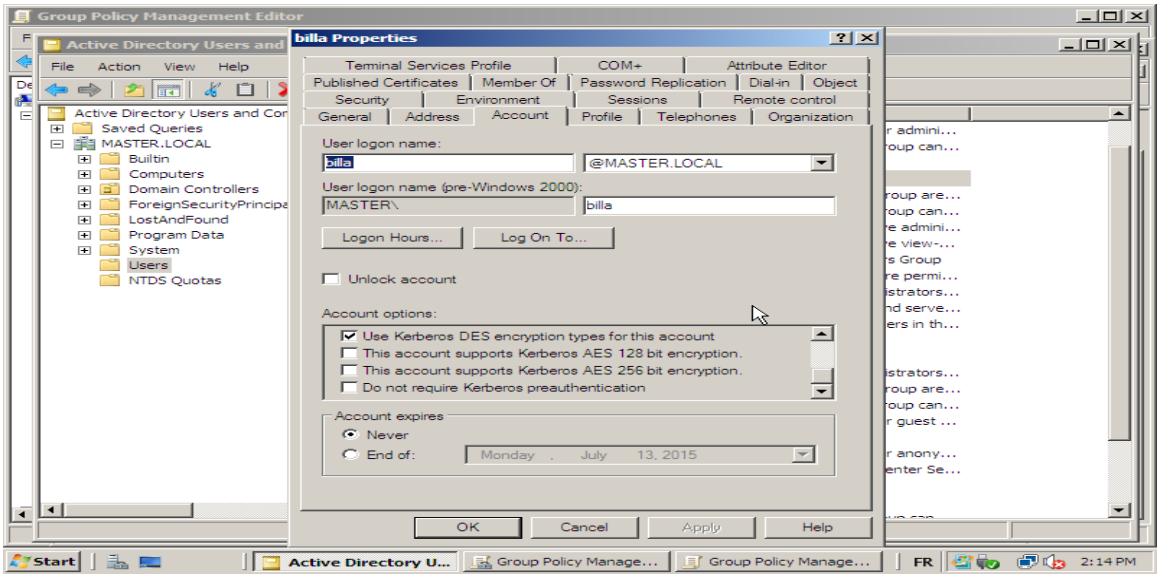


Figure IV-34 : choix de chiffrement à utiliser avec Kerberos

Ainsi pour sécuriser l'accès des utilisateurs au serveur l'administrateur de réseau, on spécifier pour chaque groupe ou utilisateur un certain nombre de permissions dans l'anglet Security :

2. Définition des autorisations aux utilisateurs

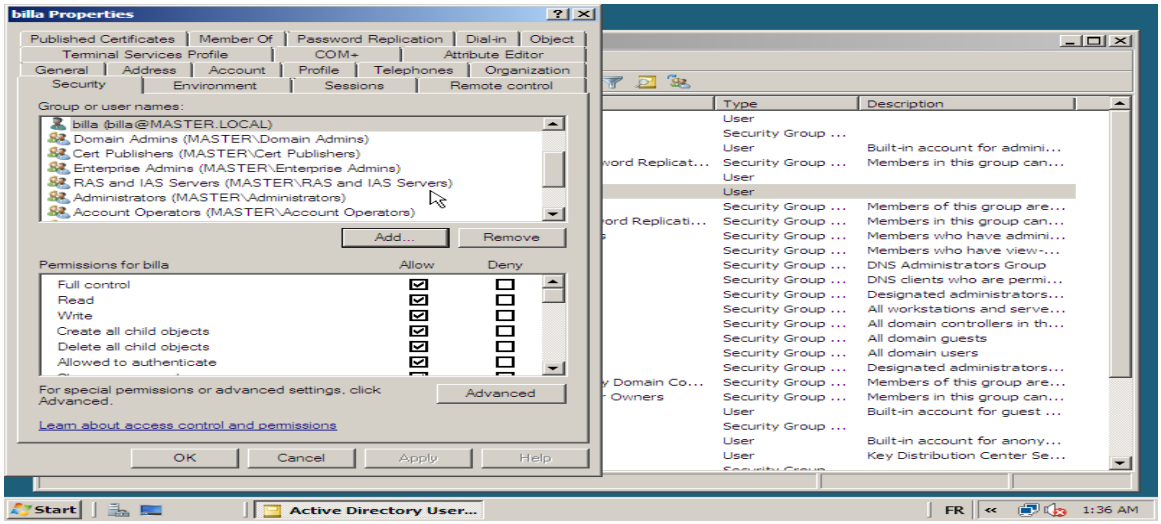


Figure IV-35 : Spécifier les permissions pour les comptes utilisateurs

Aussi on spécifié pour les données qui se trouvent dans le serveur des permissions nécessaires selon les besoins :

3. Définition des permissions pour les données

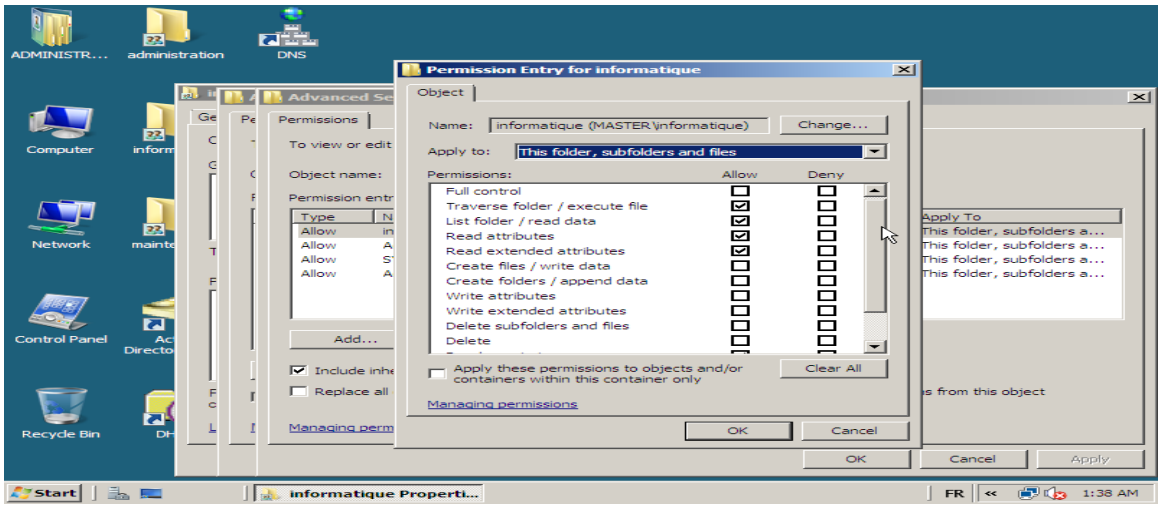


Figure IV-36 : Spécifier les permissions pour les dossiers et fichiers partagés dans le réseau

La configuration de kerberos étant terminé, on peut visualiser les tickets kerberos des clients en exécutant la commande "klist"

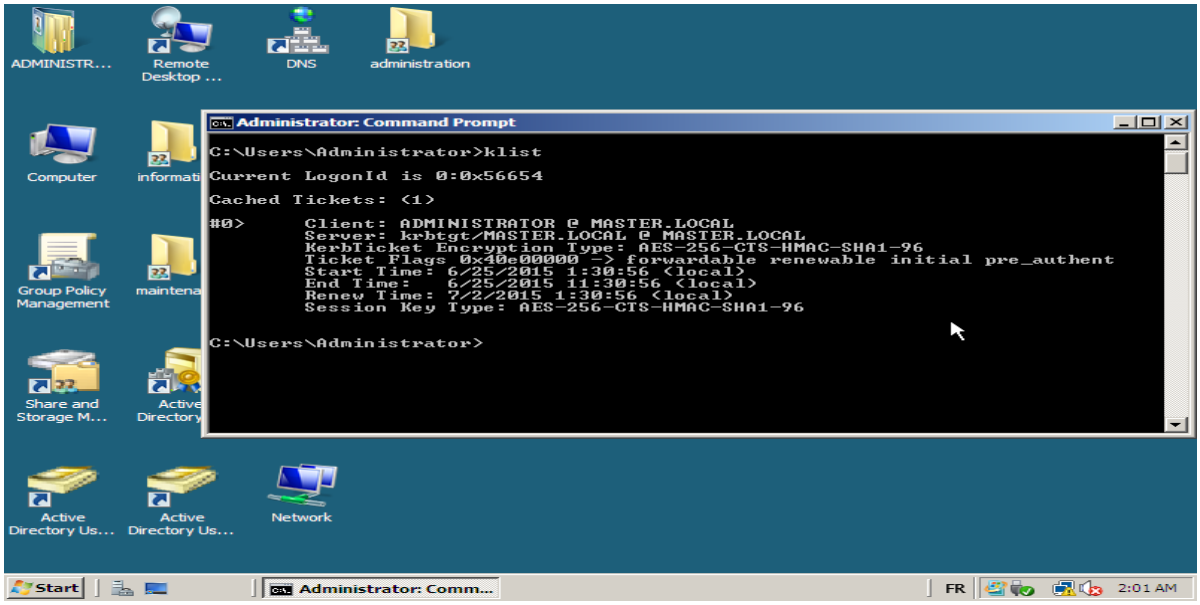


Figure IV-37 : test de la commande Klist

IV.4. Conclusion

A travers ce chapitre nous avons pu mettre en pratique nos connaissances acquises tout au long de ce stage. Hormis le manque de documentation sur la pratique, et la maitrise du protocole Kerberos. Cependant, nous avons pu découvrir et accéder au monde des machines virtuelles, et de découvrir leur fonctionnement et leurs avantages. Nous avons pu consacrer cette partie à illustrer les différentes étapes et la démarche à suivre pour la réalisation de la configuration de protocole Kerberos sous Linux et sous Windows server 2008.

La contrainte de temps ne nous a pas laissé l'opportunité d'effectuer une authentification par une connexion au serveur à distance.

Conclusion

De nos jours, la sécurité informatique est quasi-indispensable pour le bon fonctionnement d'un réseau, aucune entreprise ne peut prétendre vouloir mettre en place une infrastructure réseau, quel que soit sa taille, sans envisager une politique de sécurité. Cette politique consiste à mettre en place des protocoles visant à sauvegarder ses infrastructures et son patrimoine. Notre travail concerne l'un de ces protocoles : le protocole d'authentification Kerberos.

Nous avons commencé notre projet par la présentation de l'entreprise Sonatrach dans laquelle nous avons effectué un stage pratique. Ensuite, nous avons entamé le second chapitre par la présentation des généralités sur la sécurité des systèmes et réseaux informatiques, ce qui nous a permis d'approfondir nos connaissances et d'en savoir plus sur ses concepts. Puis, dans le troisième chapitre, nous avons présenté le protocole Kerberos, après on a défini son environnement technique.Ceci pour finir avec un quatrième chapitre dans lequel ont consigné tous les étapes de notre pratique.

Au terme de ce travail, nous pouvant conclure que Kerberos est un protocole de sécurité qui est fondé sur l'utilisation de clé privé, en son sein aucune transmission de mot de passe en claire n'est jamais effectuée. L'authentification Kerberos se fait dans les deux sens, le client s'authentifie en décryptant le TGT, et le server l'authentifie à travers sa requête pour le TGS.

Mais il en résulte que ce protocole en lui seul ne permet pas de garantir la sécurité des données d'une entité, car l'existence de certains attaques comme le « replay » qui permet de rejoué ce protocole le rend inefficient. En outre, sans la synchronisation du temps dans le réseau,un intrus pourra avoir accès aux services avec un ancien ticket, ce qui constitue une menace actif.

En guise de perspectives, nous envisageons de comparer en termes de performances les systèmes Kerberos avec d'autres systèmes similaires

Bibliographie

[1]: Orsel J. **:** *« Les services de sécurité »*, Édition de l'Information d'entreprise, 1994 , page 122 .

[2]: Kohl J., Neuman C. : *« Information Security Management Handbook »***,** RFC 1510, September 1993.

[3]: Laurent M. : **«** *Introduction à la cryptographie »*, édition CENT, Paris , 1987 .

[4]: Bertrand G. : *« Besoins, architecture, fonctionnement, nouveautés de la version 5, implémentations, perspectives »,* Mémoire de probatoire –CNAM, 2003.

[5]: Nitaj A. : *« cryptanalyse de RSA »,* Laboratoire de Mathématiques Nicolas Oresme Université de Caen, France, Version du 28 juin 2009.

[6]: Chabot Ch. : *« Fonction de hachage et signature électronique »,* mémoire en Master professionnelle option Administration des Réseaux et de bases de données, université de limoges, XLIM-DMI, 123.

[7]: Clément D., Julien V. : *« KerberosCross- platformauthentication andsingle sign- on »*,Exposés de nouvelles technologies des réseaux, Ecole d'ingénieur en Informatique et Réseaux de l'université de Marne- la-Vallée.Septembre 2003 – Février 2004.

[8]: Rivest R. : *« The MD4 Message-Digest Algorithm»*, RFC 1320, April 1992.

[9]: Shankar R. **: «** *Guide d'administration système : Services de sécurité, Référence »*, E23285 Août 2011.

[10]: Perrin Ph. , Lopitaux F. *: « Etude de compatibilité de systèmes Kerberos » :* Projet d'Administration de Réseaux, Option Réseaux et Systèmes Répartis, E.N.S.E.I.R.B, Mars 2002.

[11]: Varrette S. : *« Comprendre et mettre en place une architecture Kerberos »,* Version 0.2, Avril 2004.

[12]: Stephen C. : *« Kerberos, Recommended Practices for Deploying & Using Kerberos in Mixed Environments »*, édition MIT Kerberos Consortium, 2008.

[13]: Yarlagadda S. : « *Kerberos authentication made easy on OpenVMS »,* OpenVMS Technical Journal V18.

[14]: Gambs S. : *« Kerberos »* d'après un cours de Frédéric Tronel,13 janvier 2015.

[15]: Tung B. *: « Kerberos »* édition illustrée, réimprimée ,1999 .

Webgraphie

[w1]: Http://fr.wingwit.com/reseaux/network-security/75703.html#.VTYgGFDw_Mw

[w2]: Http://www.commentcamarche.net/contents/43-attaque-par-reflexion-smurf

[w3]: Http://www.fil.univ-lille1.fr/~hym/e/svl-07/needham-schroeder.html

[w4]: Http://www.devensys.com/blog/kerberos-principe-de-fonctionnement(1&2)

[w5]: Http://www.devensys.com/blog/kerberos-principe-de-fonctionnement

[w6]: Http://guiartic.com/fr/ordinateurs/reseaux-informatiques/quels-sont-les-avantages-de-lauthentification-kerberos.php

[w7]: Http://www.famsci.com/quels-sont-les-avantages-de-l-authentification-kerberos.html

[w8]: Http://www.devensys.com/blog/kerberos-principe-de-fonctionnement

[w9]: Http://www.eecis.udel.edu/~ntp

[w10]: Http://www.ylescop.free.fr/mrim/cours/securite.pdf

Résumé

L'authentification est un composant essentiel dans la sécurité des systèmes d'information. Si de nombreux protocoles d'authentification coexistent, Kerberos s'est largement imposé ces dernières années comme protocole d'authentification sur les réseaux locaux, en particulier avec son adoption comme service principal d'authentification dans les environnements Active Directory.

Ce travail a deux objectifs. Le premier est de rappeler quelques notions de base sur la sécurité ainsi sur le protocole Kerberos. Le second est de tester un LAB qui réalise une communication sécurisée entre un serveur et des clients.

Mots clé : Securité des réseaux, Authentification, Kerberos

Abstract

The authentication is an essential component in the information system security. If many authentication protocols coexist, Kerberos is largely imposed itself these last years as an authentication protocol on the local area networks in particular with its adoption like a principle service of authentication in the Activates Directory environments.

This project has two objectives; the first is to recall some basics concepts on the security on Kerberos protocol. The second is to test a LAB which carries out a communication made safe between a server and clients.

Key words: Network security, Authentication, Kerberos,