h e p i a

Haute école du paysage, d'ingénierie et d'architecture de Genève

Hes·SO GENÈVE

Haute Ecole Spécialisée de Suisse occidentale

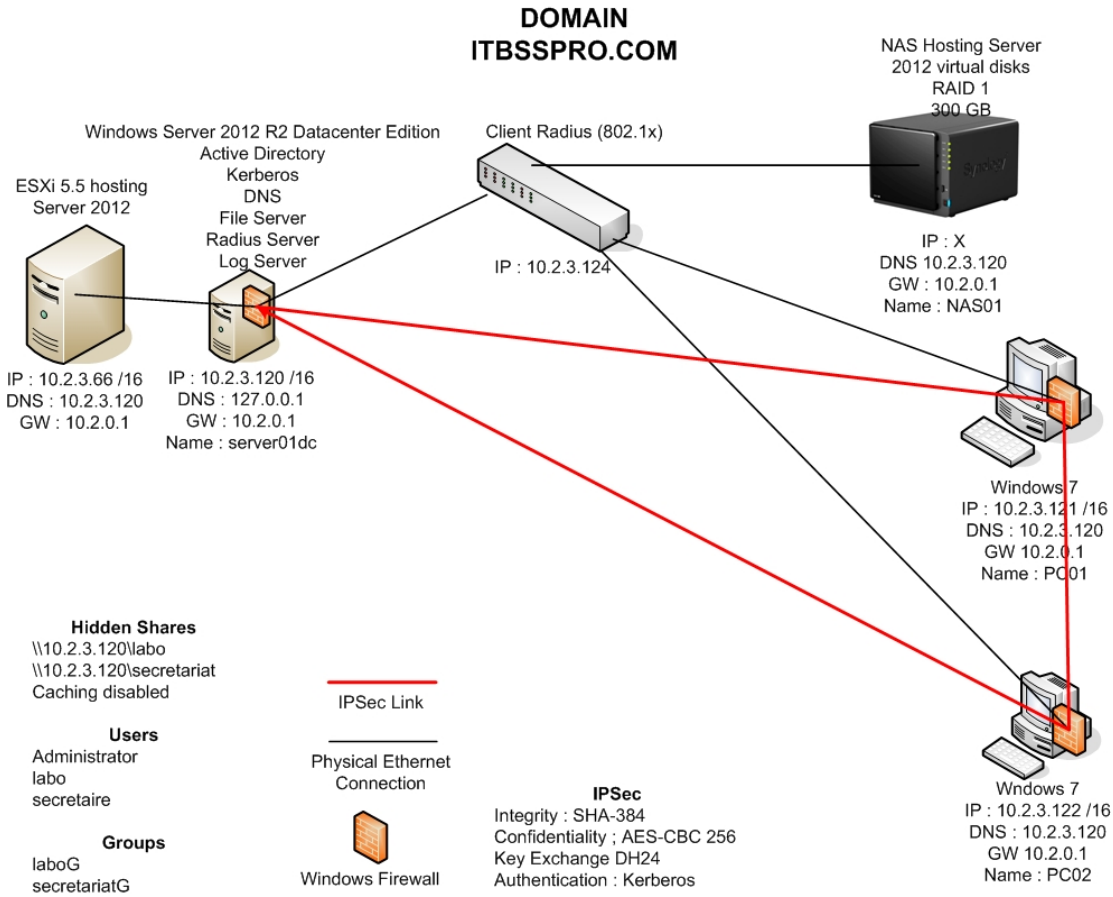
SECURITE DES SYSTEMES D'INFORMATION
INTRANET SECURISE BASE SUR LES PRODUITS MICROSOFT

Jardon-el Hiny Noureddine
Projet de semestre
Hepia 2014
Filière ITI 3

Table of Contents

I/ Introduction

1.1) Schéma



(Figure 1) : Schéma du réseau

1.2) Descriptif

Cette étude, proposée par l'étudiant, concerne la bonne configuration sécuritaire d'un intranet basé sur des produits Microsoft Server 2012 et Windows 7.

Une méthode par raffinements successifs est conseillée incluant les divers tests unitaires.

Cadre du projet :

- Domaine Windows
- Serveur de fichiers
- Authentification 802.1x et avec jeton
- Utilisation de l'hyperviseur ESXi 5.5 pour faciliter les tests (snapshot)

1.3) Travail demandé

Cette étude comprend les étapes suivantes :

1) Recherche des documents utiles (manuel d'installation, best practices, …)

2) Spécification des étapes
   Tenir compte des dépendances
   Analyse des risques
   Validation par le prof.

3) Configuration et tests sur PCs du labo

4) Analyse des résultats avec recommandations pour réalisation en entreprise

1.4) Contexte

Le but de ce projet est la mise en place d'une architecture sécurisée (réseau, serveurs, systèmes de gestion) dans une salle de laboratoire, avec différents équipements. Je vais mettre en place les « Best Practices » en ce qui concerne des notions de sécurité pour un fonctionnement optimal. Un réseau a part sera mis en place pour les tests et les déploiements des systèmes et logiciels. Ce travail sera une simulation en laboratoire et ne représente pas un réseau d'une entreprise existante. Ce travail, développé sur un nombre faibles de machine, aura pour but de montrer et de mettre en place des notions de sécurité et de permettre son intégration dans des réseaux existants plus importants.

1.5) Cahier des charges

Dans ce laboratoire, je vais simuler une société qui demande à pouvoir sécuriser au mieux son infrastructure en interne contre les accès non-autorisés au serveur de fichier, aux données et aux comptes utilisateurs.
Les services demandés par cette société sont les suivants :

- Active directory
- Serveur de fichier
- 2 utilisateurs : labo et secrétaire
- 2 dossiers partagés visible en tant que partage réseau : labo, accessible uniquement par l'utilisateur labo et secrétariat uniquement accessible par l'utilisateur secrétaire (ACL)
- L'administrateur n'a aucun accès à ces dossiers
- Enregistrement des accès sur ces dossiers
- Authentification utilisateur pour l'accès au réseau (802.1x)
- Authentification par certificats (client)
- Certificats récupérable par IIS : http://10.2.3.120/certsrv
- Contrôle d'intégrité et chiffrement des données transmises sur le réseau par IPSec
- IPSec optionnel pour toutes communications (request security)

- IPSec obligatoire pour les connections aux dossiers partagés (require security)
- Gestion centralisée du firewall

1.6) Problématique

Comme nous pouvons le constater aujourd'hui, grâce au partage de connaissances, il devient aisé de monter un serveur ou de mettre en place un réseau ou des services avec de simples fonctionnalités. Nous pouvons mettre en places des infrastructures simples telles que des serveurs web, dns, ftp … chez soi ou en entreprise avec de moins en moins de connaissances. Cela apporte donc des problèmes de sécurité, même si il s'agit d'un intranet comme dans notre cas, aussi bien pour les particuliers que pour les petites entreprises, qui sont à la recherche parfois d'une mise en service rapide pouvant répondre à leurs besoins. Les pirates informatiques en sont bien conscients et profitent de cet essor de services.

Aujourd'hui nombreux sont les problèmes dans le monde de l'informatique, notamment en matière de sécurité. Que se soit pour des raisons financières, un manquement de ressource, de temps ou de connaissance, la sécurité informatique, est un des piliers fondamental pour assurer la pérennité d'une entreprise, mais cet élément reste souvent peu ou mal géré. Un des plus grands challenge est de pouvoir réfléchir aux différents problèmes de sécurité et de pouvoir en limité les conséquences, dû à de mauvaises conceptions ou de configurations. Il convient de noter que de nos jours, les systèmes d'informations deviennent de plus en plus complexes. Nous pouvons constater la présence d'un grand nombre de logiciels, de services, sur un serveur, d'une grande quantité de données, et de logiciels de gestions et de sécurités. Au final, cette complexité augmente le risque de possibilités de failles dans notre système.

En effet, à chaque logiciel d'installé, une faille peut être rajoutée. Il en est de même pour les logiciels de sécurité en eux mêmes. Une mauvaise configuration de ce dernier entrave la sécurité que ce logiciel est censé apporter. Le pire, nous pensons être protégé, mais cela n'est pas le cas. Le risque 0, malgré les moyens mis en place, ne peuvent assurer une sécurité sans failles. Mais il y a certains éléments de bases, en matière de sécurité et de managment qu'il faut prendre en compte. La notion de sécurité est vague. En effet, nous pouvons parler de sécurité physique (contrôle d'accès aux salles serveurs, aux ordinateurs …), de sécurité logique (nécessitant l'utilisation de logiciels, antivirus, firewall…). Il y a également des aspects de gestion des utilisateurs. De manière centralisée, cela facilitera le travail de l'administrateur non seulement pour l'ajout ou la suppression de comptes mais également pour la gestion des accès. Dans le cadre de ce projet, nous nous concentrerons sur les aspects de gestions des utilisateurs, et des ressources en général par le biais de Active Directory .

En effet, de petites failles de sécurité ou de simples mauvaises configurations peuvent avoir des conséquences allant de la simple gène à la fermeture de l'entreprise.

1.7) Les notions abordées seront les suivantes :

- Mise en œuvre d'un système de gestion des utilisateurs (Active Directory)
- Mise en œuvre d'un serveur de fichiers (avec contrôle d'accès)
- Utilisation de certificats pour l'authentification
- Authentification avec 802.1x
- Configuration d'un Switch supportant le 802.1x

Quand nous parlons ici de configuration, il s'agit non seulement de mettre en place les différentes fonctionnalités, mais également de la sécurité. En effet, l'installation et la configuration de base ou simple d'un équipement ou d'un logiciel admet un bon nombre de fonctionnalité avec une sécurité en général peu satisfaisante. Il convient à l'utilisateur de faire le compromis entre fonctionnalités et niveau de sécurité. En effet, une politique de sécurité trop restrictive peut limiter les fonctionnalités offertes.

1.8) Analyse des risques

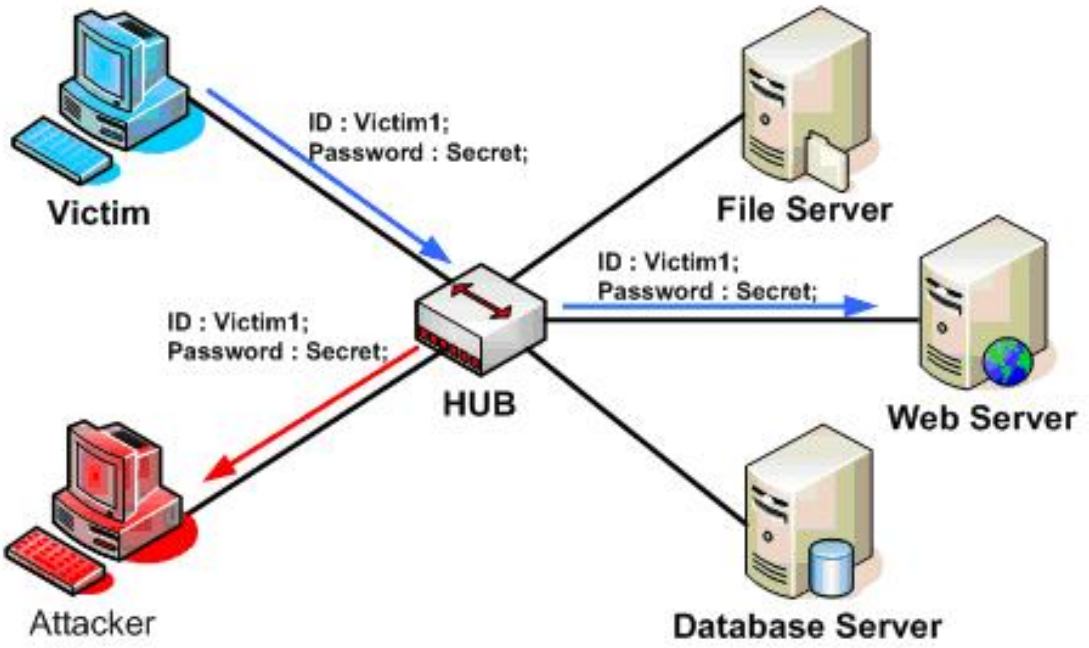
Comme nous l'avons dit précédemment, notre réseau est un intranet. Nous n'avons pas d'accès depuis l'extérieur. Dans notre scénario, nous supposons que notre serveur de fichiers et le contrôleur de domaine, sont hors d'atteintes d'attaques physiques. En effet, celui-ci est situé dans un local protégé dont seuls les administrateurs ont accès.

Nous nous occuperons donc notamment de tous les problèmes de sécurités liés aux ordinateurs des clients, aux accès distants sur le serveur, aux contrôles d'accès sur le réseau, sur les fichiers et à la configuration des comptes et des droits des utilisateurs par le biais de GPOs.

En effet il est important de gérer les comptes efficacement pour éviter que des comptes ne se retrouve avec des droits ou des privilèges trop élevés, éviter que des utilisateurs peuvent se connecter au réseau sans autorisation ou modifier la configuration des ordinateurs. Mettre en place un système afin d'éviter le sniffing des paquets par un chiffrement des données entre le client et le serveur, (eavesdropping, man in the middle) afin d'éviter la fuite d'information.

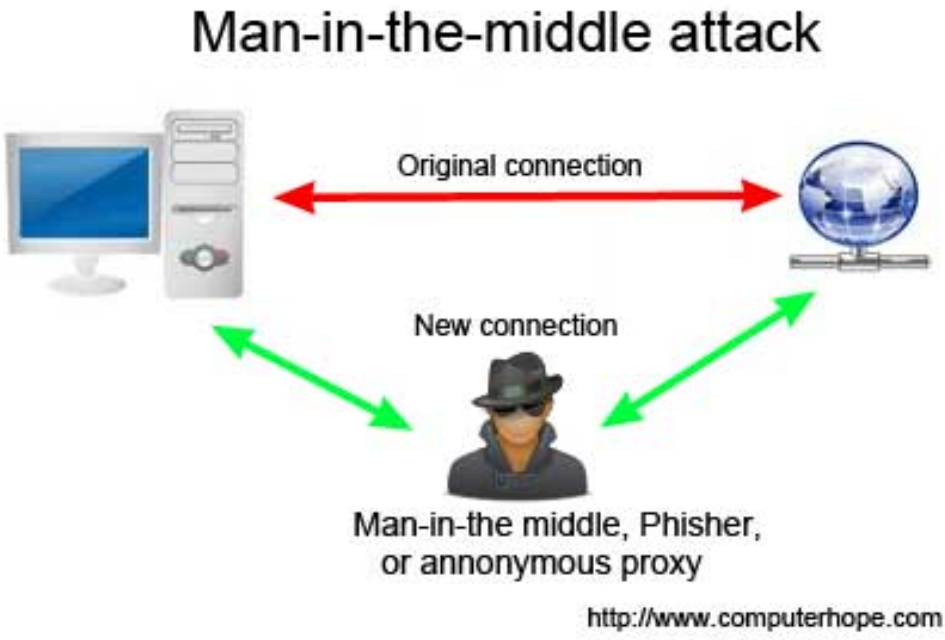
L'eavesdopping consiste à se connecter sur le réseau et d'écouter les différents échanges de paquets entre les machines sans altérer leur contenu. Il est difficile de détecter ce genre d'attaques. Ce genre d'attaques est plus difficile à mettre en œuvre lors de l'utilisation de switch, mais toujours possibles.

Exemple d'eavesdropping :



(Figure 2) : Eavesdropping[1]

Dans le cadre des man-in-the-midde attacks, elles restent sophistiquées et nous pouvons aller de la simple écoute de paquets, à l'interception puis la modification, ou dans l'impersonation afin de remplacer un des protagonistes lors de la communication dans le but de voler des informations tels que des documents, logins, mots de passes…



(Figure 3) : man-in-the-middle attack[2]

[1] https://www.owasp.org/images/4/48/Eavesdropping.jpg
[2] http://www.computerhope.com/jargon/m/maninthemiddleattack.jpg

Nous nous pencherons donc sur les points suivants :

- Administration des comptes utilisateurs
- Monitoring des comptes
- Administration des contrôles d'accès des fichiers et monitoring
- Contrôle d'accès au réseau IP (802.1x) et chiffrement
- Configuration d'un firewall et ouverture des ports

1.9) Matériel nécessaire

Pour ce travail, voici la liste du matériel :

- 1 ordinateur avec ESXi d'installé
- 1 ordinteur avec un client Windows 7
- 1 ordinateur avec un client Windows 8.1
- 1 NAS avec le Datastore de ESXi
- 1 switch netgear GS724T

1.10) Pourquoi un Hyperviseur ?

Pour commencer, nous allons utiliser, pour contenir les serveurs Windows une architecture virtualisée grâce à un hyperviseur : ESXi 5.5. L'hyperviseur nous permettra d'avoir un grand nombre de machines virtuelles en assurant un cout de fonctionnement minimal et un meilleur rendement (électricité). ESXi fait partie de la virtualisation de type 1 assurant performance, économie d'énergie (consolidation des serveurs), sécurité (cloisonnement entre les machines) et possibilités de prendre des snapshots permettant de revenir à un état précédant lors de tests. L'administration se fera à partir d'un client possédant le logiciel vSphere Client 5.5 offrant une connexion sécurisée vers l'hyperviseur en GUI avec SSL. L'installation de ESXi reste aisée. Mais il faut faire attention aux possibles problèmes de compatibilité.

Si cette partie vous intéresse, la procédure d'installation et de configuration détaillée se trouve en annexe.

II/ Windows Server 2012 Datacenter Edition

2.1) Administration et protection des comptes utilisateurs

Dans cette première partie, nous allons nous intéresser aux différents éléments de configurations importants concernant la gestion des comptes et l'audit de ces derniers. Il faut protéger les ordinateurs et les serveurs contre des tentatives de login non autorisées. En effet, en cas de problème, il est important de pouvoir garder une trace des différentes actions liées aux comptes. En effet, sans contrôle nous augmentons les risques d'une attaque qui ne serait que tardivement détectée. Toutes ces données seront stockées dans les logs du serveur.

Grace au fait que nous sommes dans un domaine Windows, il sera plus facile de pouvoir gérer la sécurité et ce, de manière centralisée grâce aux GPOs.
Nous allons mettre en place des règles de sécurités en ce qui concerne les mots de passes et les login des utilisateurs aussi bien sur les postes clients que sur le serveur, pour les comptes locaux et les comptes du domaine.

Il existe toute une myriade d'éléments de configurations pour la protection des comptes utilisateurs, ceux-ci sont heureusement configurables à partir de notre serveur Active Directory.
Nous pouvons prendre exemple d'une société qui souhaite avoir une politique stricte en matière de sécurité sur le contrôle des comptes (notamment sur les mots de passes) afin d'éviter tout login non autorisé :

2.1.1) Eléments de configuration

Des éléments simples tels que :

- Un blocage des comptes après un certains nombres de login (5x)
- Un blocage limité dans le temps (15 min).
- Une possibilité de débloquer le compte automatiquement après 15 minutes.
- Forcer l'utilisation de mots de passes forts.
- Garder un historique des mots de passes pour éviter la réutilisation d'anciens mots de passes.
- Forcer une durée minimale et maximale pour les mots de passes.

2.1.2) Explications

En effet, il est important de pouvoir bloquer les comptes lorsque trop de tentatives ont échouées. Elles peuvent être l'œuvre d'un utilisateur distrait mais également un signe avant coureur d'attaques de type "password guessing", bruteforce, ou dictionary attacks.

Le déblocage du compte pourra se faire manuellement par l'administrateur ou automatiquement après une certaine période (15 minutes).

Il est important en matière de sécurité de forcer l'utilisateur à choisir des mots de passes avec une longueur minimale de caractères. En général, l'utilisation de 7 caractères est suffisante. Dans cette situation, les attaques de type bruteforce ou dictionnary restent dangereuses, mais prendront plus de temps.

Un mot de passe doit en général avoir une « date de validité » forçant ainsi l'utilisateur à changer régulièrement sont mot de passe. Nous pouvons avoir une durée minimum (1 jour) à respecter avant de pouvoir changer un mot de passe ainsi qu'une limite dans le temps (30 jours).

Windows intègre également la possibilité de retenir un historique sécurisé (version hash) des mots de passes pour éviter que l'utilisateur reprenne un ancien mot de passe et grâce au paragraphe précédent, éviter qu'il change souvent de mot de passe (1 jour minimum d'intervalle) pour retourner à un ancien.

Avec la puissance de calcul des ordinateurs d'aujourd'hui, il devient plus rapide de pouvoir pirater un compte utilisateur si il ne respecte pas une certaine complexité dont voici les caractéristiques :

- Ne pas contenir le nom de l'utilisateur
- Au moins 6 caractères
- Doit contenir : majuscules, minuscules chiffres et caractères spéciaux

2.1.3) Tableau de résistance d'attaques

Voici un tableau donnant un exemple de temps nécessaire, pour une attaque bruteforce pour deviner un mot de passe, en fonction de la complexité. Nous observons bien que la complexité est un élément fondamental. La longueur définie du mot de passe est 10 symboles.

Jours	Années	Millénaires
816.94	2.24	0.00
0.08	0.00	0.00
0.00	0.00	0.00
0.00	0.00	0.00

Jours	Années	Millénaires
836'545.75	2'290.34	2.29
83.65	0.23	0.00
3.41	0.01	0.00
0.00	0.00	0.00

Jours	Années	Millénaires
4'857'056.52	13'297.90	13.30
485.71	1.33	0.00
19.82	0.05	0.00
0.01	0.00	0.00

Jours	Années	Millénaires
251'382'207.31	688'246.97	688.25
25'138.22	68.82	0.07
1'026.05	2.81	0.00
0.47	0.00	0.00

(Figure 4) : Tableau de résistance[3]

Légende :

Résistance à une attaque standard
Résistance à une attaque concentrée
Résistance à une attaque Deep Crack
Résistance à une attaque Total Computing Power

[3] http://www.tdeig.ch/ITI2_Secu/CrypToolPresentation-en.pdf

Lorsque nous prenons une machine, nous avons toujours des comptes locaux prédéfinis bien connus, qui sont la cible des attaques. Le compte administrateur ainsi que le compte « invité ». Très souvent le compte administrateur est activé, avec le nom « administrateur » et nous renseigne tout de suite sur le niveau de privilège.

Il est important d'effectuer les changements suivants :

- Changer le nom
- Mettre un mot de passe fort
- Désactiver ces comptes locaux

2.2) Mise en place des politiques d'audit et de surveillance

Nous avons précédemment mis en place un moyen de protéger les comptes utilisateurs, mais avons nous réellement la preuve de son fonctionnement ? Sommes nous vraiment protégé, et avons nous un moyen de vérifier ?
Il est évident qu'une société aimerait pouvoir s'assurer de réellement posséder le contrôle de ses comptes.

Il est essentiel de pouvoir voir si il y a eu des tentatives de connections qui ont échoués. Nous allons donc mettre en place des politiques d'audit afin de pouvoir inscrire dans les logs, des évènements susceptible de montrer des accès non autorisés, que se soit au niveau des comptes, des accès aux ressources etc.… lorsque nous sommes dans une entreprises, beaucoup de choses peuvent se passer : mauvais login, accès à des ressources non autorisées, création d'utilisateurs ou de groupes. Il est important de pouvoir savoir ce qu'il se passe, et surtout d'en garder une trace.

Des questions sont à se poser :

- Qui s'est connecté sur les machines ?
- Y a-t-il eu des modifications concernant les comptes utilisateurs ?
- A-t-on essayer de se connecter sur un compte préalablement bloquer ?

2.2.1) Eléments de configurations

Voici une liste des différents éléments a prendre en compte :

- Audit account logon events
- Audit account and user account management
- Audit SAM database access
- Audit File Share access

Ces différentes politiques doivent être activées sur toutes les machines du réseau aussi bien pour les tentatives réussies que celles qui ont échoués.

2.2.2) Scénario

Nous pouvons imaginer en cas de problème, la situation suivante : un utilisateur distrait oublie de fermer sa session durant une pause. Il s'ensuit qu'un utilisateur indélicat prend son poste et vole des données. Grace aux politiques d'audit, il sera possible de voir qu'une activité suspecte a eu lieu. L'utilisateur légitime de la machine sera interpellé, mais celui-ci niera toute implication, même d'avoir oublier de verrouiller sa session. Grace au log, nous pouvons voir effectivement que durant ce vol de donnée, ni l'ordinateur ni le serveur de log, n'aura enregistrer une action de verrouillage, de session avant le vol, et même quelles données ont été prises. La responsabilité incombe à l'utilisateur et des sanctions peuvent être prises a son encontre.

2.2.3) Explications

Nous pouvons ici faire en sorte de pouvoir enregistrer toutes tentatives de login, afin de savoir qui s'est connecté, sur quel machine, et quand. Un évènement sera généré à chaque fois que l'ordinateur validera une authentification. Nous pourrons voir pour quel utilisateur, l'authentification aura été effectuée. Des éléments supplémentaire peuvent être logger tels que :

- Logon
- Logoff
- Session lockout
- Access to locked account

La gestion des comptes est également un élément à enregistrer. Un évènement sera générer et enregistrer dans ces conditions :

- Création, modification de comptes ou de groupes
- Suppression, désactivation et activation d'un compte
- Blocage, déblocage
- Changement de SID
- Changement de mot de passe

Il est très important de spécifier une telle politique. En effet grâce à cela nous pouvons garder une trace sur l'activité des comptes d'ordinateurs. Un pirate informatique ou un ancien employé pourrait trouver un moyen de réactiver son compte après avoir quittée la société et donc avoir un accès non autorisé. Il en est de même pour un pirate informatique.

Un cas de problèmes, tels que l'apparition non légitime d'un compte pirate, la réactivation non autorisé d'un compte, seront pris en compte. Dans un environnement avec beaucoup d'utilisateurs, ou les gens ne se connaissent pas, comment savoir si c'est utilisateur est légitime ? Qui a créer ce compte ? Ou qui la réactivé ? Et a quel moment ?
Ce système permettra de répondre à ces questions.

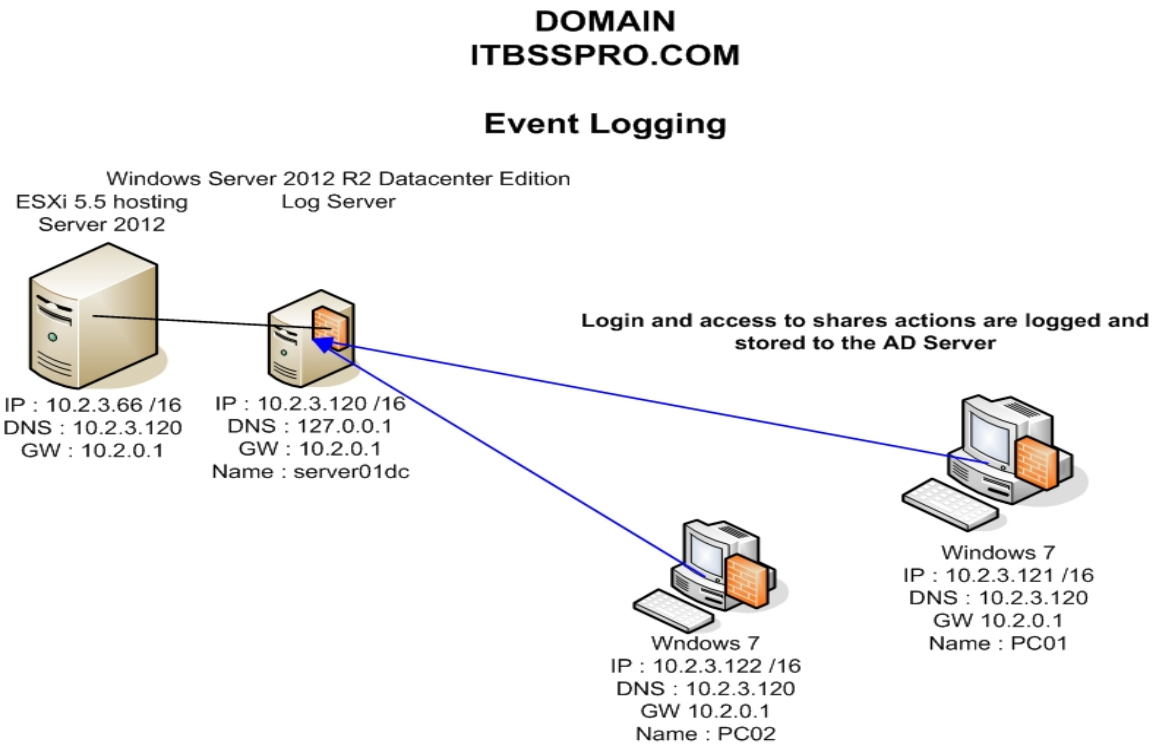
Sur les postes Windows, il existe un fichier très sensible qui enregistre tous les comptes utilisateurs et leurs mots de passes hashés. Il s'agit du SAM (Security Account Management)
Ceci concerne la base de donnée des comptes. Il est important de surveiller ce fichier pour les échecs, afin d'enregistrer les tentatives non autorisé sur un fichier sensible.
Lorsque nous faisons partie d'un domaine, les comptes ne sont pas dans ce fichier, mais dans la base de donnée du contrôleur de domaine. Néanmoins il existe et peut être copié, il peut intéresser un pirate car il existe un administrateur local. Il convient donc de vérifier les accès a ce fichier sensible pour savoir qui a tenter d'accéder à ce fichier, et sur quel machine.

Toujours pour les utilisateurs, mais également pour la protection des accès aux données sur le serveur de fichier, il est important de savoir :

- Qui a accédé à quelle donnée ?
- Quel utilisateur ?
- A partir de quelle machine (nom et IP)
- Quelles ont été les manipulations faites sur ce fichier (suppression, modification…)

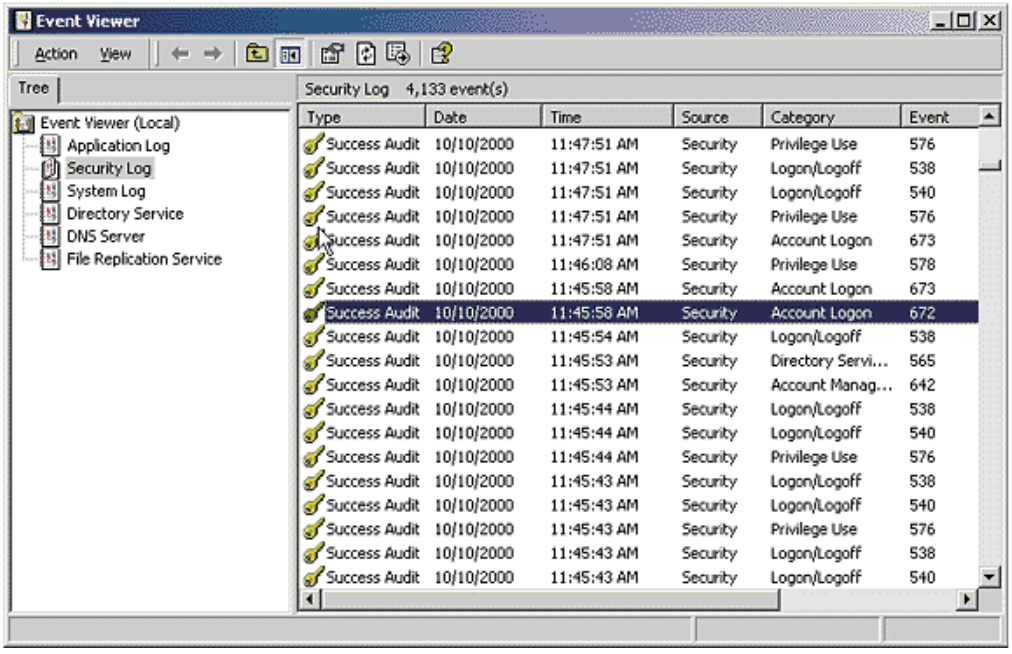
Nous pourrons garder une trace des accès aux fichiers et dossiers partagés. Ce système nécessite la mise en place du partage des dossiers et de règles de contrôle d accès (ACL). Il faut également pour l'élément en question à surveiller, configurer les règles d'audit. A partir de la des enregistrements d'accès seront effectuées dans les logs. Nous pouvons par exemple, pour les utilisateurs classiques spécifier l'enregistrement concernant la lecture, ou la modification d'un fichier.
A partir de la, la société a une preuve écrite, inscrite dans les logs de toute action sur les ressources. Il est difficile pour un utilisateur de nier avoir falsifier, modifier, supprimé ou voler le fichier. Tout est enregistrée.

Voici, à la page suivante, le principe de fonctionnement d'un système le logging. Toutes les machines enverront au contrôleur de domaine des « events » qui seront inscrit dans ses logs, en fonction de la configuration que nous avons vu ci-dessus.



(Figure 5) : Event Logging

Et voici un exemple d'inscription dans les logs d'évènement concernant les logon :



(Figure 6) : Event Logging (logon)[4]

[4] http://technet.microsoft.com/en-us/library/Bb742435.lgeven03_big(l=en-us).gif

2.3) Protection des accès au serveur de fichiers et système de partage et de stockage

Qui a le droit de se logger localement sur le serveur de fichier ? D'effectuer des connections sur le file serveur et d'accéder aux fichiers et dossiers partagés ? A-t-on le droit d'utiliser le lecteur CD, ou une clef USB ? Est-il possible de faire une élévation de privilèges afin d'accéder à certains documents sensible présent sur le serveur ou d'effectuer des changement de configuration?

Cette gestion est importante pour éviter tout vols de données. En effet il faudrait éviter que n'importe quel utilisateur ne puisse se connecter sur n'importe quel système, localement ou à distance, copier, lire, modifier ou supprimer des informations, que se soit sur un partage réseau ou à l'aide de systèmes de stockage amovible.

Trop souvent un administrateur à le pouvoir de tout faire, mais dans les grandes sociétés, les administrateurs n'ont pas accès aux documents sensibles pour éviter des vols d'informations. Nous règlerons dans ce cas, les ACL des fichiers/dossiers, et les accès aux partages.

2.3.1) Configuration des partages et ACL

Configuration des partages :

- Deux dossiers partagés, un par groupe.
- Accès aux partages et aux informations que par les membres d'un même groupe
- Ces dossiers partagés sont invisibles sur le réseau grâce a l'utilisation du « $ » a la fin du partage. Si on ne connaît pas le chemin du dossier partagé, alors on ne peut pas s'y connecter.
- Les administrateurs ont les accès aux partages refusés.
- Les mises en caches des documents sont interdites afin d'assurer l'intégrité des documents et que en cas de changement de configuration des ACL, cela soit tout de suite pris en compte.

Configuration des ACLs

- Les administrateurs n'ont aucun accès aux dossiers
- Les utilisateurs peuvent créer, modifier, supprimer… les informations dans leurs partages.
- Les utilisateurs ne peuvent pas voir ou modifier les attributs et les permissions, faire un changement de propriétaire.

Nous assurons ici un confinement des informations et des comptes.

Encore une fois, en utilisant les GPO, nous allons contrôler certains des accès aux systèmes et aux fichiers. Nous allons voir certains éléments de configurations permettant de déployer ces politiques à partir du serveur Active Directory.

2.3.2) Contrôle des moyens de connections sur les machines

Voici quelques éléments à voir :

- Allow logon localy : pour le serveur, seul les administrateurs sont autorisés. Pour les postes clients, les administrateurs et les utilisateurs du domaine sont autorisés.

- Access this computer from network : nous avons un serveur de fichier, il est donc important de laisser les administrateurs et les utilisateurs du domaine, la possibilité de se connecter sur le serveur.

- Deny logon through RDP : Nous n'autorisons aucun accès a distance sur les machines avec RDP.

- Do not allow enumeration of SAM Database and shares : nous interdisons à tous les utilisateurs anonymes de pouvoir lister les ressources enregistrer sur le contrôleur de domaines tels que les partages.

- Do not display user info when session is locked and do not display last username. Cela nous permettra d'éviter qu'un pirate recense les noms des utilisateurs.

Nous venons de limiter les possibilités de login sur les machines, en fonction des risques de sécurités. En effet un utilisateur lambda ne doit pas pouvoir se connecter physiquement sur un serveur de fichier ou à distance en utilisant RDP.

2.3.3) Empêcher la copie de données

Les sociétés sont en général très sensibles au vol d'informations. Mais que pouvons nous faire contre cela ? Pouvons nous empêcher un utilisateur lambda d'insérer une clef USB dans une machine pour voler des informations, ou de propager un virus par le biais de cette clef ? La réponse est oui. On refuse catégoriquement l'utilisation du floppy, du lecteur CD et de clefs USB à tout le personnel.

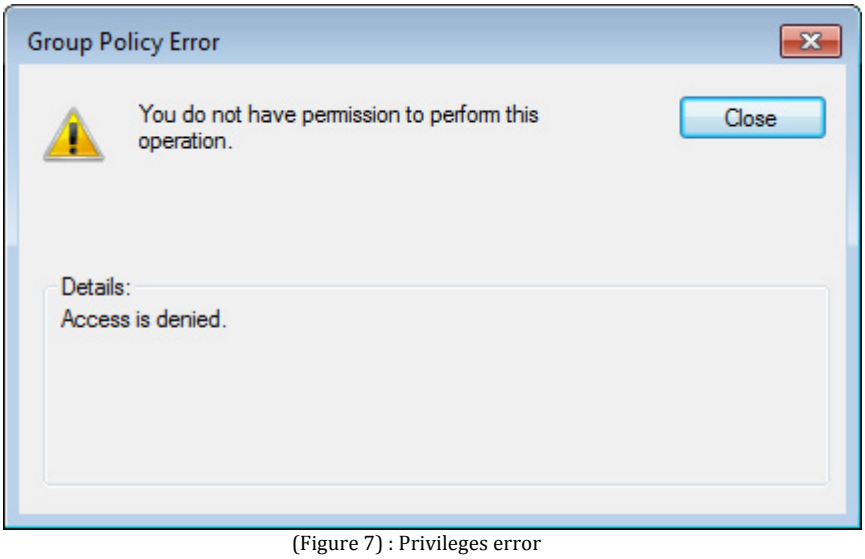
Voici les éléments importants:

- Floppy drives : deny execute, read, write
- CD and DVD : deny execute, read, write
- Removalbe disks : deny execute, read, write
- All removale storage : deny execute, read, write

Ces politiques configurable dans les GPO permet de spécifier un blocage total de tous les lecteurs amovibles et d'éviter par le biais de ce matériel une copie non autorisée. Nous pouvons bien sur spécifier des exceptions pour le directeur par exemple.

2.3.4) Empêcher l'élévation de privilèges

Mais maintenant que la plupart de ces politiques sont spécifiés pour les utilisateurs, qu'en est il des administrateurs ? Nous pouvons imaginer que les administrateurs n'ont pas ce genre de limitations. Cela voudrait-il dire que en cas d'élévation de privilège, un simple utilisateur lambda pourrait outrepasser ces règles ? Oui cela est possible. C'est pourquoi nous devons empêcher sur les machines clients les élévations de privilèges :
UAC : Behavior of the elevation prompt for standard users : automaticaly deny elevation requests
Toute demande d'élévation est impossible sur les postes clients.
Grace à cette politique, nous empêchons à toutes personnes l'accès à une élévation de privilèges lorsque un programme ou une fonction système nous demande des droits d'administrateurs pour effectuer des modifications.



(Figure 7) : Privileges error

2.4) Gestion des connexions entre les serveurs et les clients

Lorsque nous sommes dans un réseau d'entreprise, il est difficile de pouvoir gérer efficacement les communications. Toutes nos communications sont elles légitimes ? Est-il possible qu'un pirate se connecte sur notre réseau dans le but de voler des données ? Comment pouvons nous être sur que nous communiquons bien avec la bonne personne ? Avec le bon serveur ? Pouvons nous mettre en place des moyens d'authentification des participants ? En effet, il peut y avoir beaucoup d'utilisateurs ou de machines connectées. Parois même sans que nous sachions véritablement qui s'est connecté au réseau. Plusieurs méthodes peuvent être mise en place afin de limiter ces problèmes. Nous parlerons ici des méthodes « intégrées » de Windows pour assurer une protection des communications par le biais du chiffrement, de la signature et de l'authentification des connections et des protagonistes (fonctionnalités natives + IPSEC + Kerberos) ainsi que de l'accès au réseau par le biais d'une autorité d'authentification d'accès : RADIUS.

2.4.1) Signature et chiffrement natif

Windows intègre heureusement pour tous les membres du domaine deux fonctionnalités activées par défaut :

- Digitally sign communications
- Digitally encrypt or sign secure channel

Ces politiques forcent les ordinateurs et serveurs du réseau appartement au domaine à signer les paquets SMB (par exemple) et chiffrer les sessions de communications. Ils ne pourront pas communiquer ensemble si cette politique n'est pas respectée. Cela permettra d'éviter des attaques telles que le man-in-the-middle (dans le cadre de modification de données) ou « server or user impersonation ». En effet, un pirate pourrait intercepter ou modifier des paquets SMB ou impersonifier un système afin d'avoir accès aux ressources du serveur.
Lors de l'établissement de telles sessions, les informations des comptes utilisateurs et d'ordinateurs sont utilisées. Cela nous permettra d'assurer l'intégrité des données échangées, le chiffrement et l'authentification de l'utilisateur et du poste client.

Voici donc ce que nous offre Windows dans le cadre de la protection des communications. Il est évident que ceci n'est pas suffisant. Il est nécessaire de pouvoir assurer une communication complètement sécurisée. Nous allons donc aborder IPSec afin de pouvoir protéger nos communications internes avec Kerberos comme système pour l'authentification.

2.4.2) Kerberos

Fonctionnement :

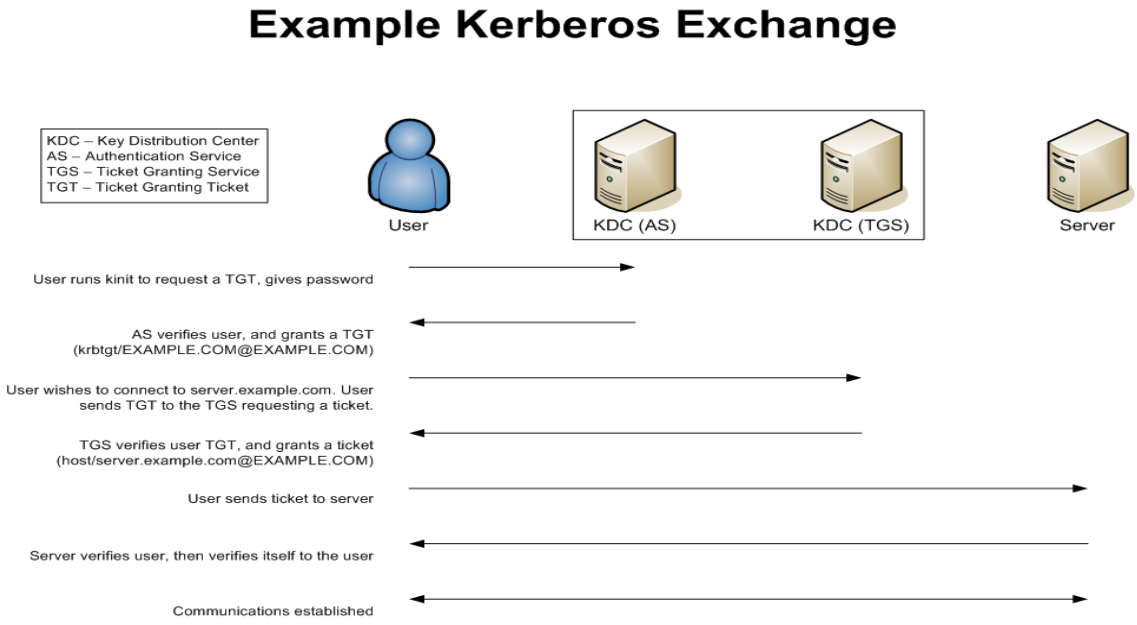
Le protocole Kerberos repose sur un système de cryptographie à base de clés secrètes (clés symétriques ou clés privées). Kerberos partage avec chaque client du réseau une clé secrète permettant de prouver l'identité de l'entité.

Le principe de fonctionnement de Kerberos repose sur la notion de tickets.

- Afin d'obtenir l'autorisation d'accès à un service, un utilisateur distant doit envoyer son identifiant au serveur d'authentification.
- Le serveur d'authentification vérifie que l'identifiant existe et envoie un ticket initial au client distant, chiffré avec la clé associée au client. Le ticket initial contient :
    - une clé de session, faisant office de mot de passe temporaire pour chiffrer les communications suivantes ;
    - un ticket d'accès au service de délivrement de ticket.
- Le client distant déchiffre le ticket initial avec sa clé et obtient ainsi un ticket et une clé de session.

Grâce à son ticket et sa clé de session, le client distant peut envoyer une requête chiffrée au service de délivrement de ticket, afin de demander l'accès à un service.

L'avantage de ce système est qu'il permet une authentification mutuelle permettant d'authentifier les deux parties communicants.
L'authentification proposée par le serveur Kerberos a une durée limitée dans le temps, ce qui évite des attaques de type « replay attacks ».



(Figure 8) : Kerberos Exchange[5]

[5] http://community.igniterealtime.org/servlet/JiveServlet/download/1060-8-1605/Example+Kerberos+Exchange.png

2.4.3) Utilisation du pare-feu Windows avancé

Le pare-feu Windows fait parti du système de protection intégré des systèmes Microsoft. Il se trouve activé par défaut. Ce qui est intéressant, c'est que lorsque nous activons des services, tels que la réplication des informations entre contrôleur de domaines, partage de fichiers, ou autre, le trafic est automatiquement autorisé car des règles d'exceptions se mettent en place automatiquement à notre insu.

Bien sur cela représente également un problème de sécurité. Dans le cadre ou certains services systèmes sont activés à notre insu (par un hacker, par une application…) ou autre, le trafic est automatiquement autorisé. Un logiciel malveillant s'installe ? De forte chance il y a que le système laisse passer le trafic. Il est évident que dans le cadre de ce travail, seul des services Microsoft ont été utilisés, il est donc fort possible qu'il soit normal que ces fonctionnalités soient automatiquement autorisées à travers le firewall. Mais qu'en est-il de programmes tiers ? Aurons nous une alerte qu'un programme inconnu tente d'établir une connexion ? Ceci reste à voir, d'autant que ce pare-feu contrôle aussi bien le trafic entrant que sortant.

Dans cette partie, nous n'allons pas traiter tout de suite les éléments concernant le trafic entrant ou sortant mais plutôt la mise en place de règles de communications, déployables sur les machines également par le biais de GPO :

- Activation du firewall
- Connection Security Rules
- IPSec

Nous allons gérer ici qui a le droit de se connecter sur les systèmes, à partir de quels prérequis, les connections se voient refusé ou autorisé.

Microsoft appel cela : « Connection Security Rules »

Nous allons créer une règle que Microsoft appel : l'isolation. Grace à cela nous pouvons restreindre les communications selon certains critères. Il est évident que nous voulons refuser à un utilisateur lambda de simplement brancher sa machine en réseau puis de pouvoir commencer à se connecter aux autres machines. C'est pour cela nous allons demander à ce que le trafic entre toutes les machines soit authentifier si possible. Cela s'appel : « request security ».
Ce que nous appelons ici authentification du trafic est lié, à l'algorithme d'authentification que nous allons utiliser dans la configuration IPSec que nous allons voir au point suivant.

2.4.4) Utilisation de IPSecurity avec le pare-feu Windows

Il est important de noter que Microsoft a intégré IPSec dans le module du pare-feu. Cette version d'IPSec est d'ailleurs amélioré et prend en charge un plus grand nombre d'algorithmes.

2.4.4.1) Niveau de sécurité à implémenter

Dans ce travail, nous utiliserons IPsec pour toutes les communications entre les machines. Il est important de noter que nous allons rendre l'utilisation de IPSec optionnelle pour toutes les communications sauf pour les connections aux dossiers partagés, par le biais des politiques de sécurité pour toutes les machines du domaine.

Une société qui nécessite un niveau de protection important en ce qui concerne la confidentialité des données et l'intégrité de ces dernières doit s'assurer que tous les systèmes communiquant répondent à un certain niveau de sécurité. En effet si les ordinateurs ne peuvent négocié les paramètres de sécurité IPSec pour le partage des données, ils ne répondent donc pas au prérequis fixer par la société, et représente donc un risque qu'une machine commence à échanger des données de manière non sécurisées, ou dans le cadre d'un pirate intercepte des données non sécurisées.

Les protocoles utilisés seront Ah et ESP afin de garantir un maximum de protection. AH nous permettra de vérifier l'intégrité des données et l'authentification des systèmes communicants, mais n'offre pas de système cryptographique. Il est donc important de rajouter ESP dans un mode transport. Dans ce mode, il n'y a pas d'authentification des systèmes mais offre une intégrité partielle des données et un service de chiffrement.

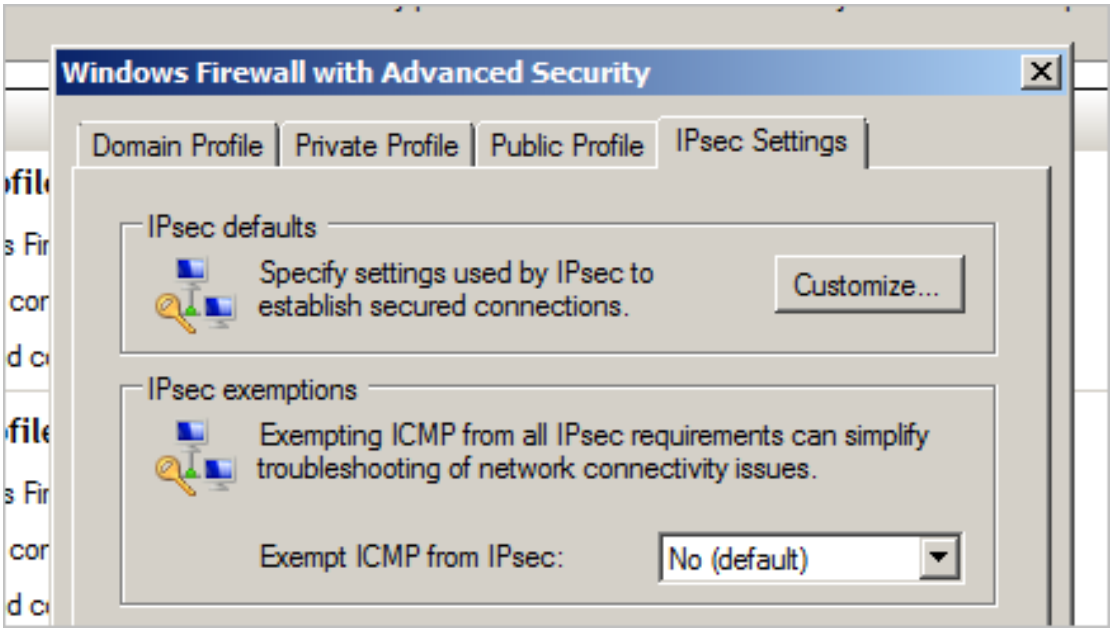
2.4.4.2) Configuration IPSec

Ces deux protocoles sont complémentaires et seront donc utilisés conjointement. Les algorithmes suivants seront utilisés pour l'échange des clefs et la protection des données :

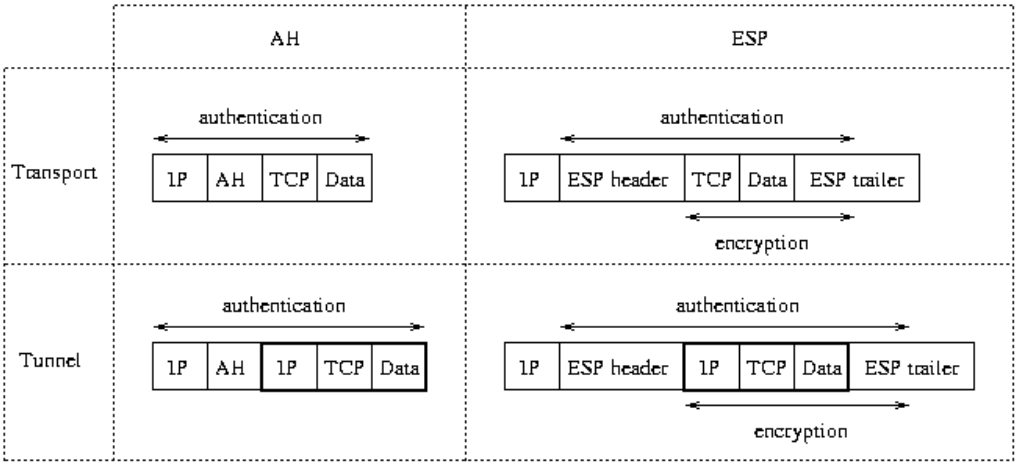
- Intégrité : SHA-384 (intégrité)
- Chiffrement : AEC-CBC 256
- Echange des clefs : DH24
- Authentification : Kerberos V5 basé sur les comptes ordinateurs ou utilisateurs

Une nouvelle clef sera créée après 100 Mbytes ou 60 minutes afin de pouvoir limiter les interceptions de clefs et les replay attacks. Nous aurons également d'activé, le PFS (Perfect Forward Secrecy) qui garantit que la découverte par un adversaire de la clé privée d'un correspondant à long terme ne compromet pas la confidentialité des communications passées. Ces algorithmes sont dits "ressources intensive" et peuvent créer des ralentissements au niveau CPU.

Voici l'intégration de IPSec dans le pare-feu Windows :



Format des trames (seul le mode transport nous intéresse):



(Figure 9) : format des trames IPSec[6]

[6] http://wwwconference.org/proceedings/www9/249/ipsec1.gif

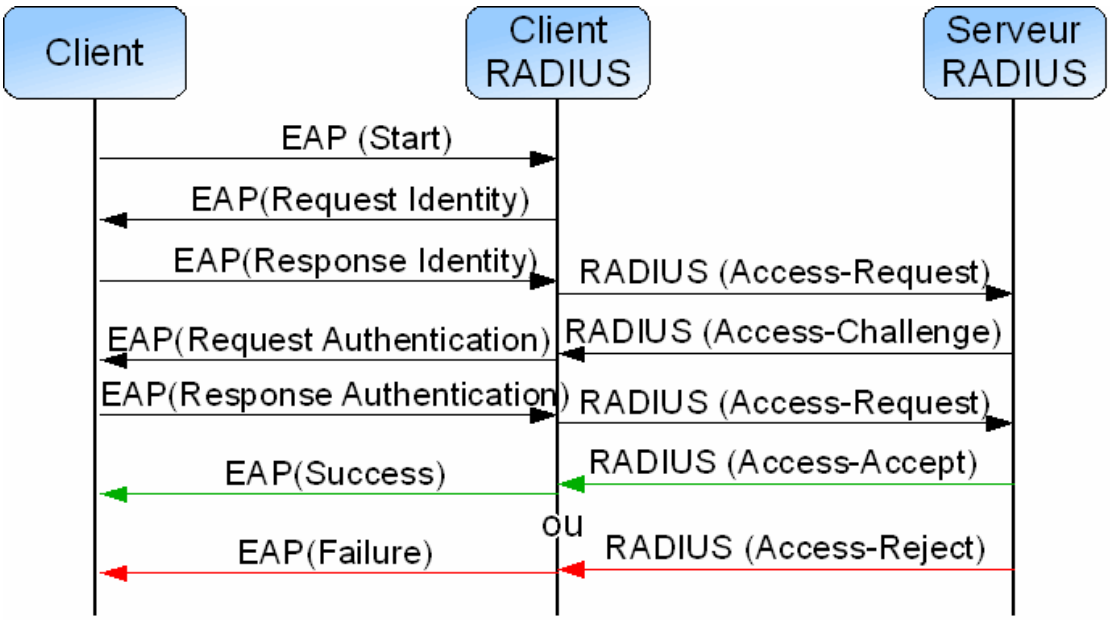
2.4.5) Radius

Comme mécanisme de protection pour l'accès au réseau, j'ai décidé d'implémenter RADIUS avec l'utilisation de certificats comme moyen d'authentification. Jusque là nous avons protégé les accès aux ressources du serveur mais nous devons mettre en place une protection plus « proche » de l'utilisateur, donc au niveau du switch. Bien qu'il existe d'autres éléments de sécurités tels que le : Port-Security. Un utilisateur non authentifié, n'aura aucun accès au réseau et donc aucun contact avec le serveur ou les autres clients.

Configuration :

- Le serveur AD est le serveur Radius
- Le Switch Netgear est le client Radius
- Authentification par certificat client uniquement (EAP-TLS)
- Login autorisé de 8h à 20h
- Service NPS de Microsoft

Le service NPS (Network Policy Server) nous permet de mettre en place les politiques de connexions. Nous pouvons par exemple y spécifier quelles sont les heures de connexions autorisées, quel mécanisme d'authentification, à partir de quel client RADIUS la demande d'authentification peut se faire etc…
La configuration complète du service NPS se trouve sur ce site :
http://blog.meigh.eu/2013/01/16/-email-post-.aspx



(Figure 10) : mécanisme[7]

[7] http://www-igm.univ-mlv.fr/~dr/XPOSE2007/jgauth02_RADIUS/img/connect.png

Délivrance du certificat

Par souci de simplicité dans se laboratoire, la délivrance de certificat se fait par le biais du serveur : http://10.2.3.120/certsrv. Il serait possible de mettre en place un système de délivrance automatique mais cela n'est pas utile dans notre cas.

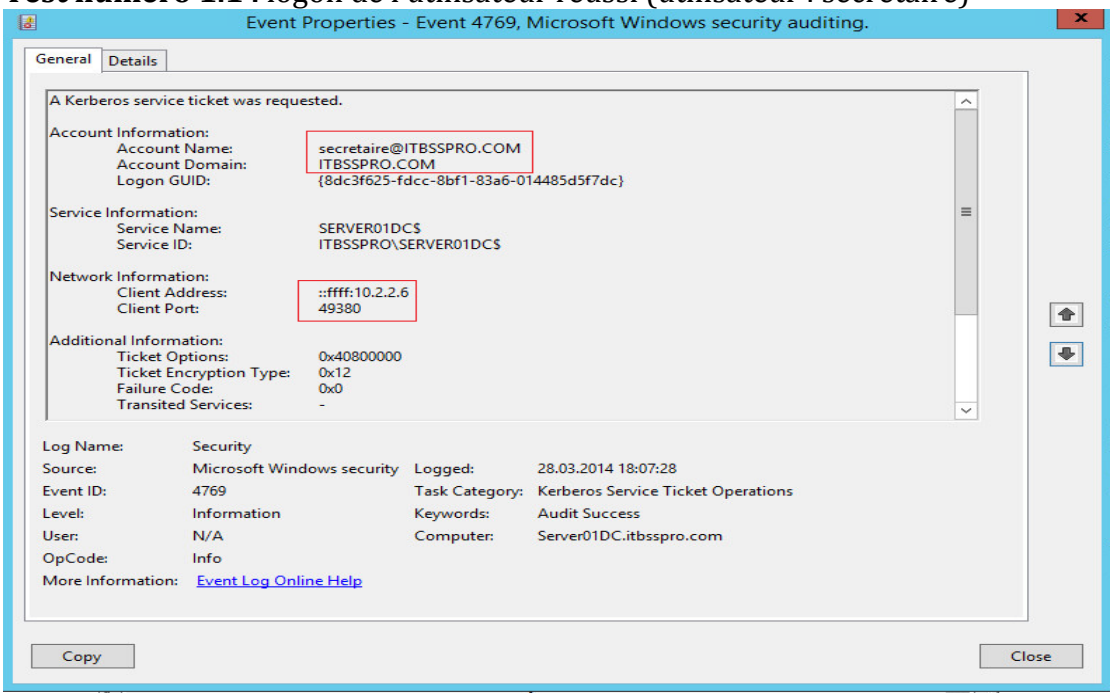
Pour rentrer sur le site, il faut etre un utilisateur autorisé (authentification par username-password). Le certificat sera crée en fonction de ces informations. L'utilisateur n'a plus qu'à installer le certificat puis l'utiliser lors de la demande de connextion.

III/ Test

Maintenant que nous avons pu mettre en place nos différentes politiques de sécurité, il est important de pouvoir tester si tout est correct, par le biais des informations enregistrées dans les logs de type « sécurité » du serveur. Nous allons voir :

1. Tests d'authentification de l'utilisateur (vérification logs)
   1.1. Login
   1.2. Logoff
   1.3. Echec
2. Test d'accès au partage (vérification logs)
   2.1. Réussi
   2.2. Echec
3. Que se passe-il si nous désactivons un compte utilisateur
4. Que se passe-il si nous désactivons un compte machine
5. Que se passe-t-il si un client n'a pas la bonne configuration IPsec/Firewall
6. Quels sont les ports du serveur visible pour un ordinateur hors domaine (Firewall OFF)?
7. Quels sont les ports du serveur visible, avec Firewall, pour un ordinateur hors domaine ? (Firewall ON, Any incoming traffic allowed)
8. Quels sont les ports du serveur visible, avec Firewall, pour un ordinateur hors domaine ? (Firewall ON)
9. Est-il possible de lire un CD ?
10. L'élévation de privilège est-elle possible ?

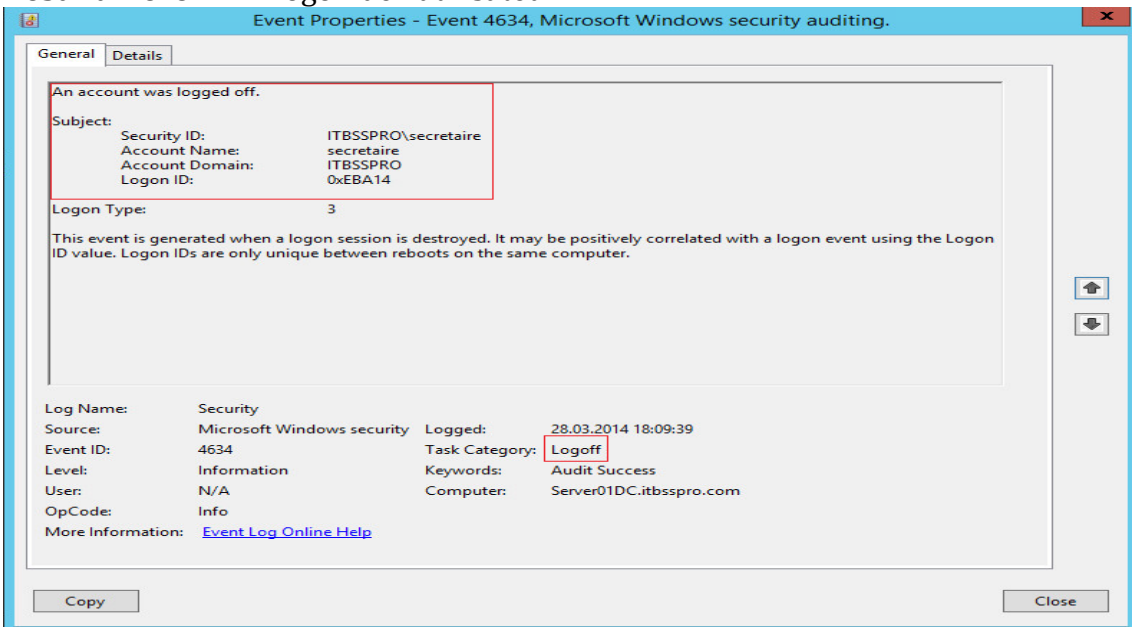
Test numéro 1.1 : logon de l'utilisateur réussi (utilisateur : secrétaire)



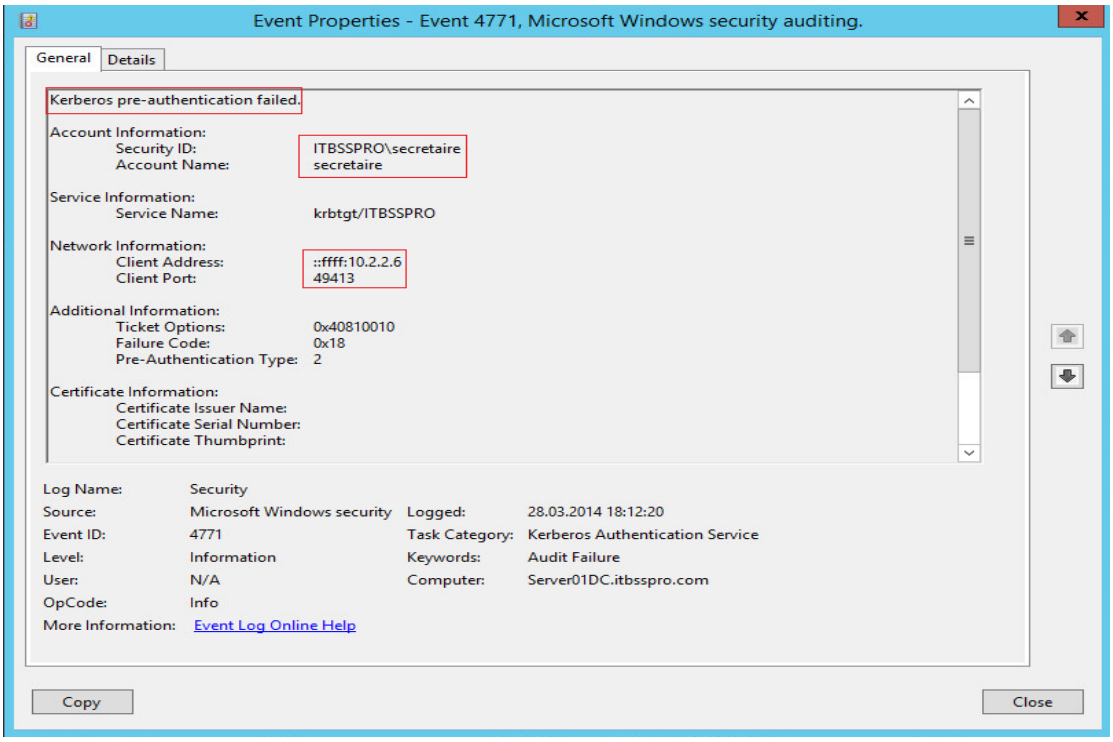
<u>Informations importantes :</u>

- Nom d'utilisateur
- Adresse IP de l'ordinateur

Test numéro 1.2 : Logoff de l'utilisateur



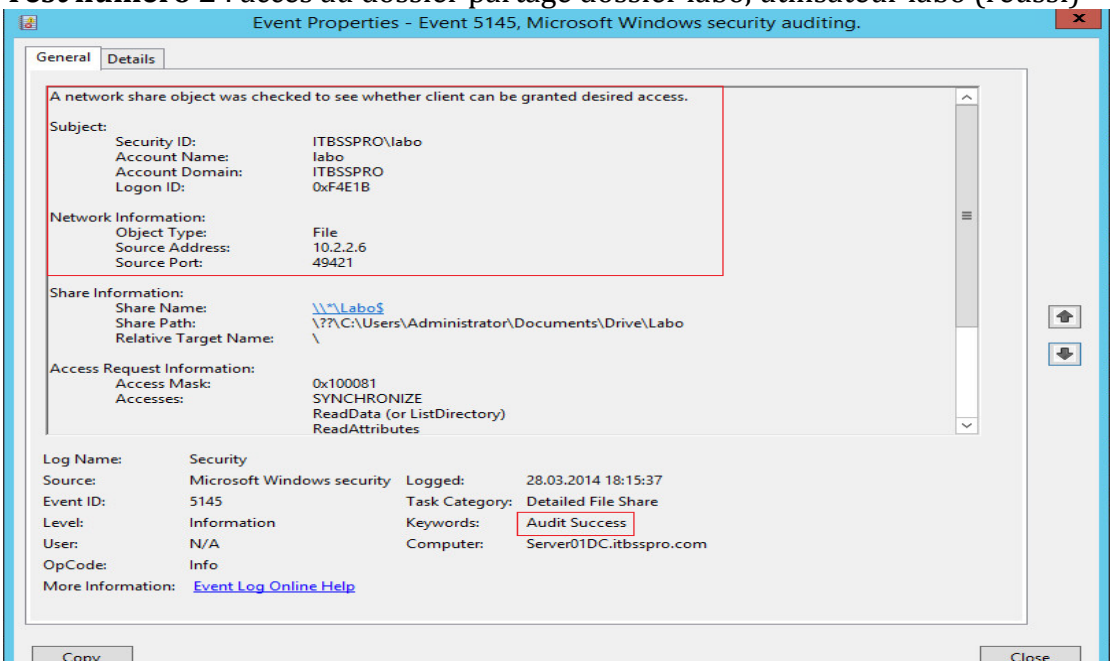
Test numéro 1.3 : Echec de l'authentification



Informations importantes :

- Echec
- Nom d'utilisateur
- Adresse IP de l'ordinateur

Test numéro 2 : accès au dossier partagé dossier labo, utilisateur labo (réussi)

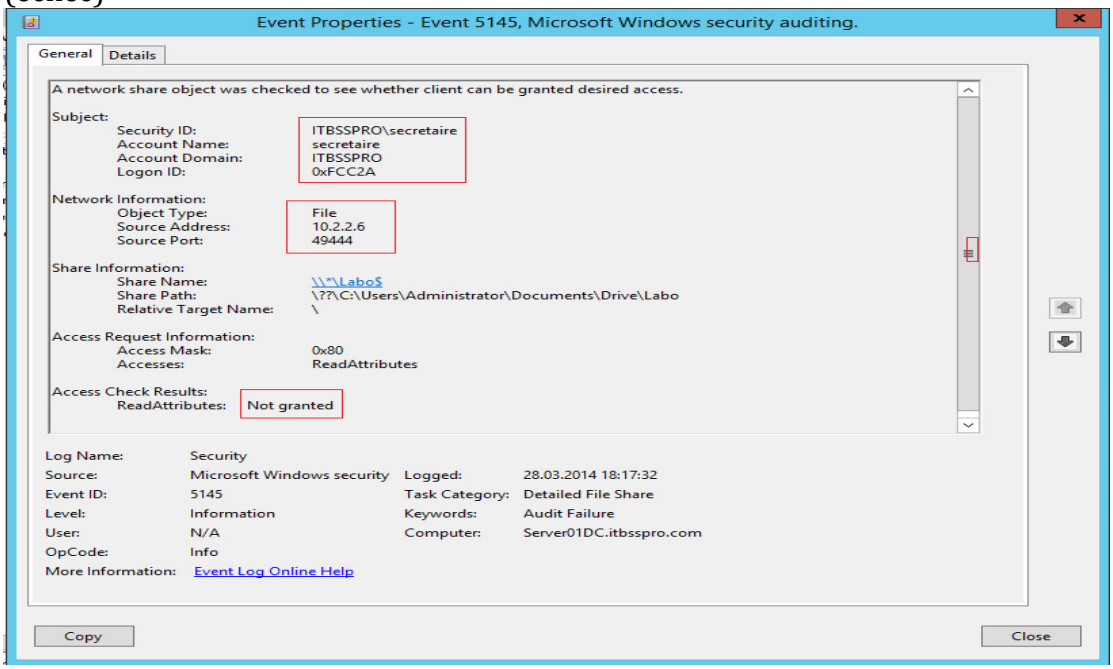


Informations importantes :

- Réussie
- Nom d'utilisateur

- IP source
- Quel dossier partagé est accédé

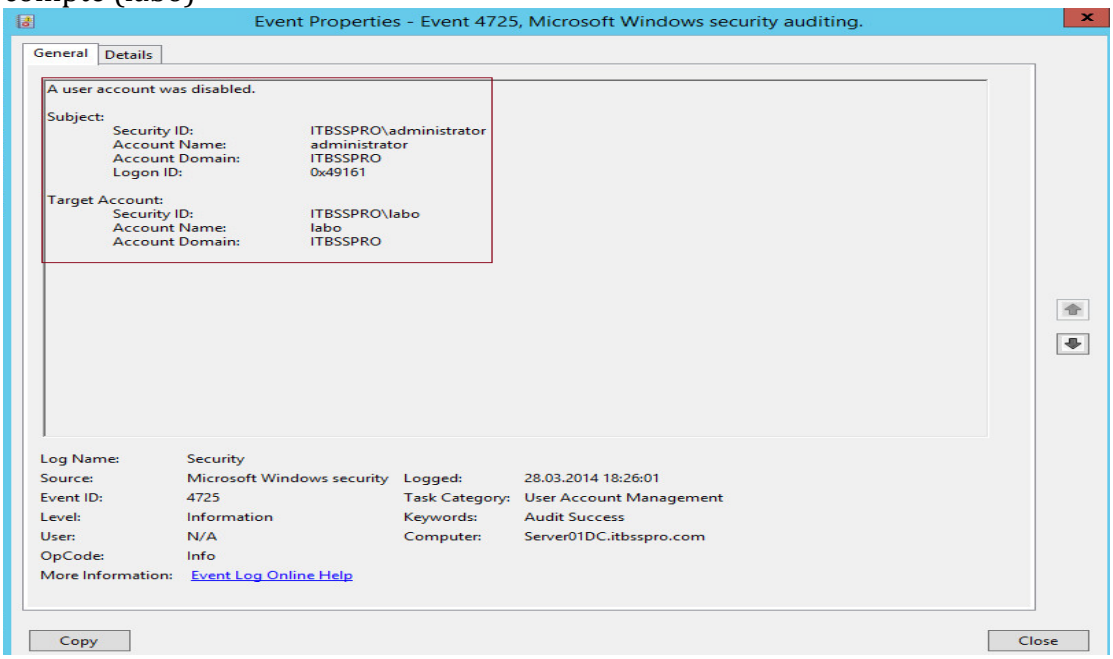
Test Numéro 2.2 : accès au dossier partager dossier labo, utilisateur secrétaire (échec)



Informations importantes :

- Echec
- Utilisateur
- IP source
- Quel dossier partagé on tente d'accéder

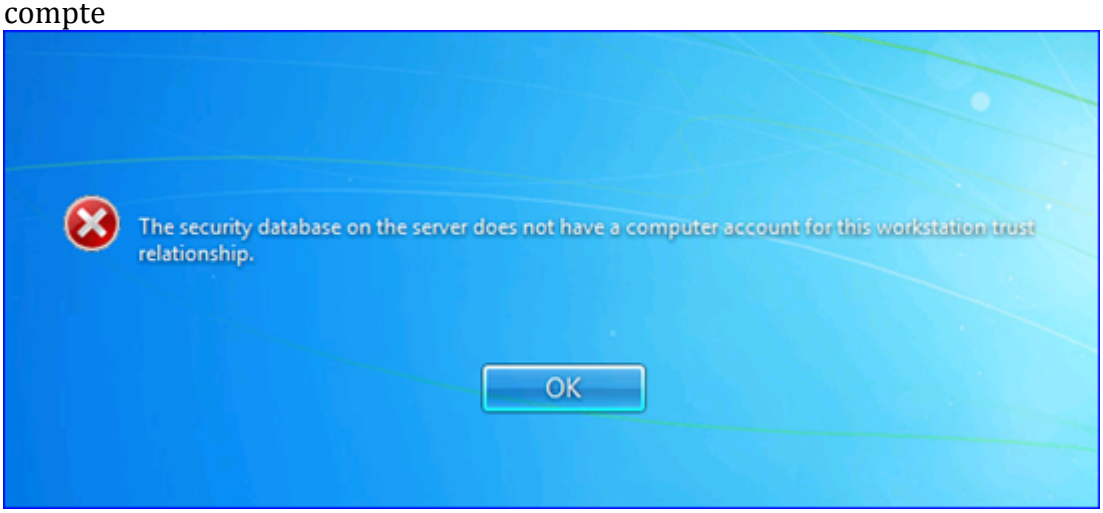
Test numéro 3 : désactivation d'un compte utilisateur puis utilisation de ce compte (labo)



Informations importantes :

- Quel compte a été désactivé (labo)
- Par qui : administrator
- Message sur poste client : « this user account was disabled »

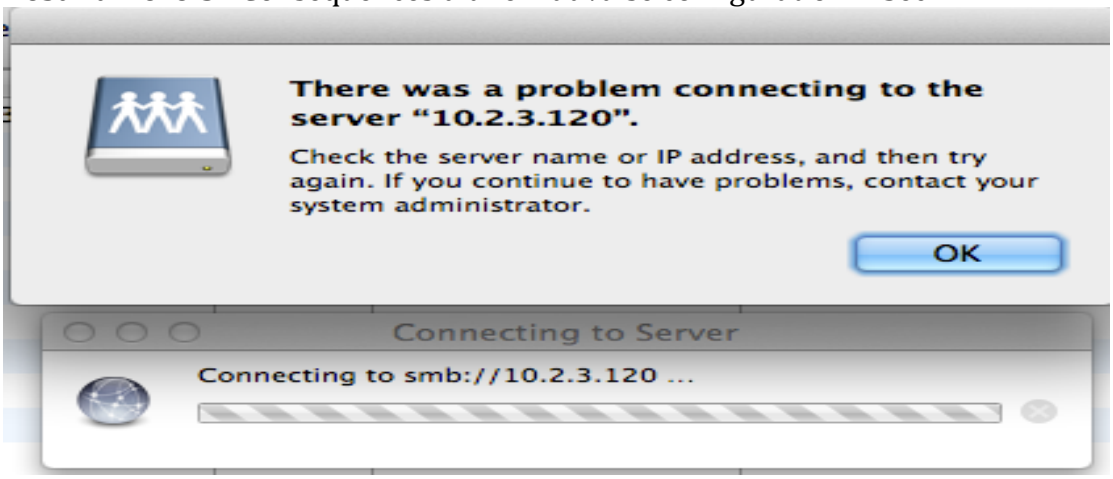
Test numéro 4 : désactivation d'un compte machine puis utilisation de ce compte



Information importante :

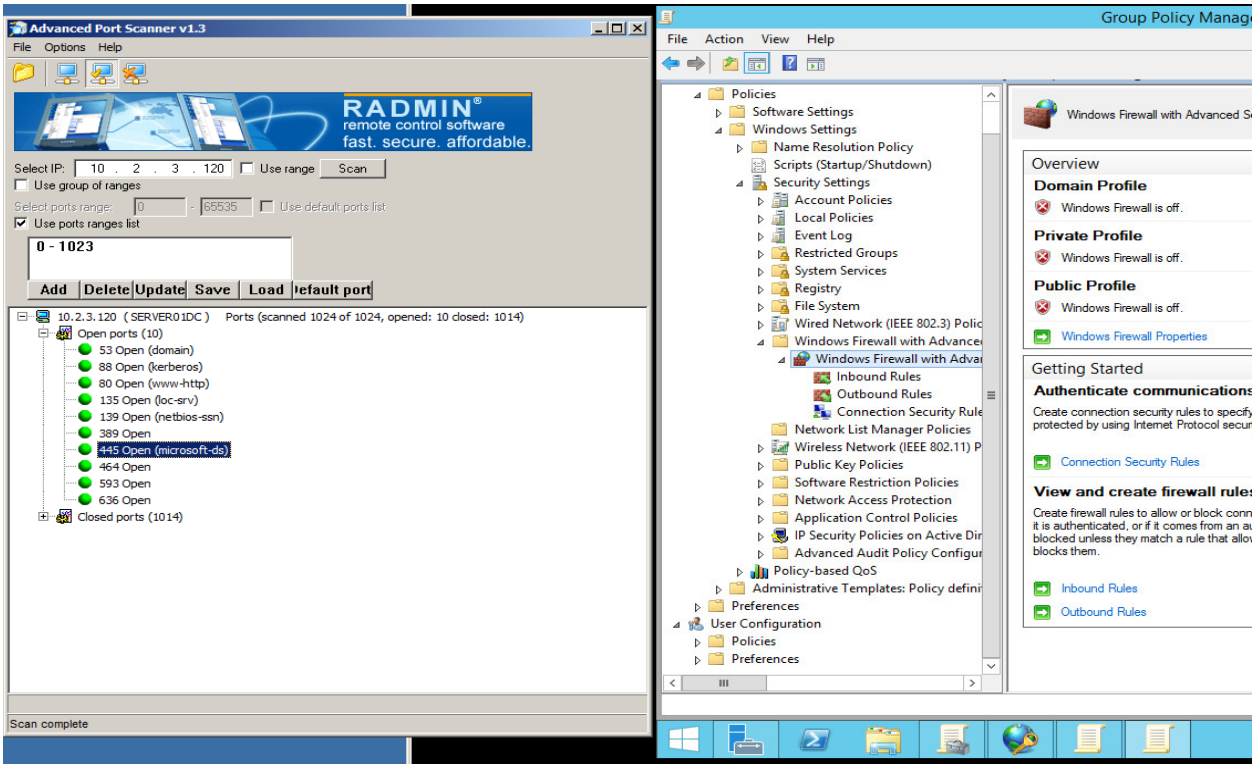
- Le poste client est averti que le compte machine n'existe pas sur le serveur. Aucun utilisateur peut se logger en utilisant la machine. Même un administrateur.

Test numéro 5 : Conséquences d'une mauvaise configuration IPSec



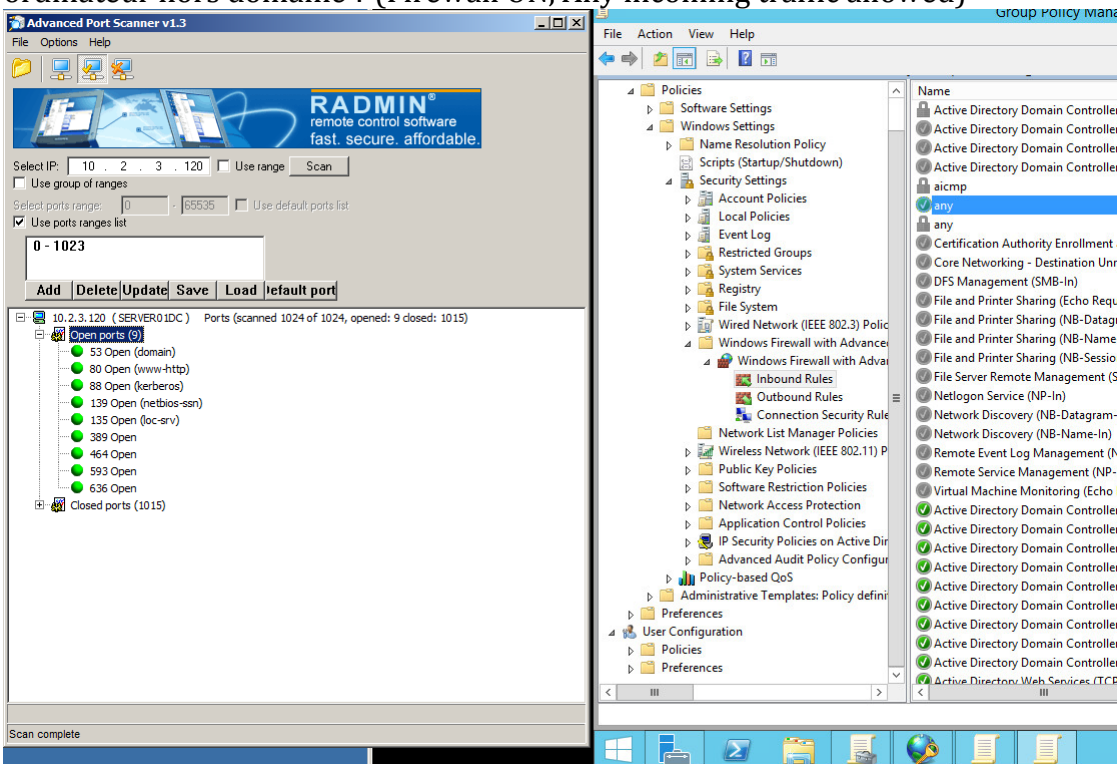
Cet ordinateur ne faisant pas parti du domaine il lui est impossible de se connecter aux partages.

Test numéro 6 : Quels sont les ports du serveur visible pour un ordinateur hors domaine (Firewall OFF) ?



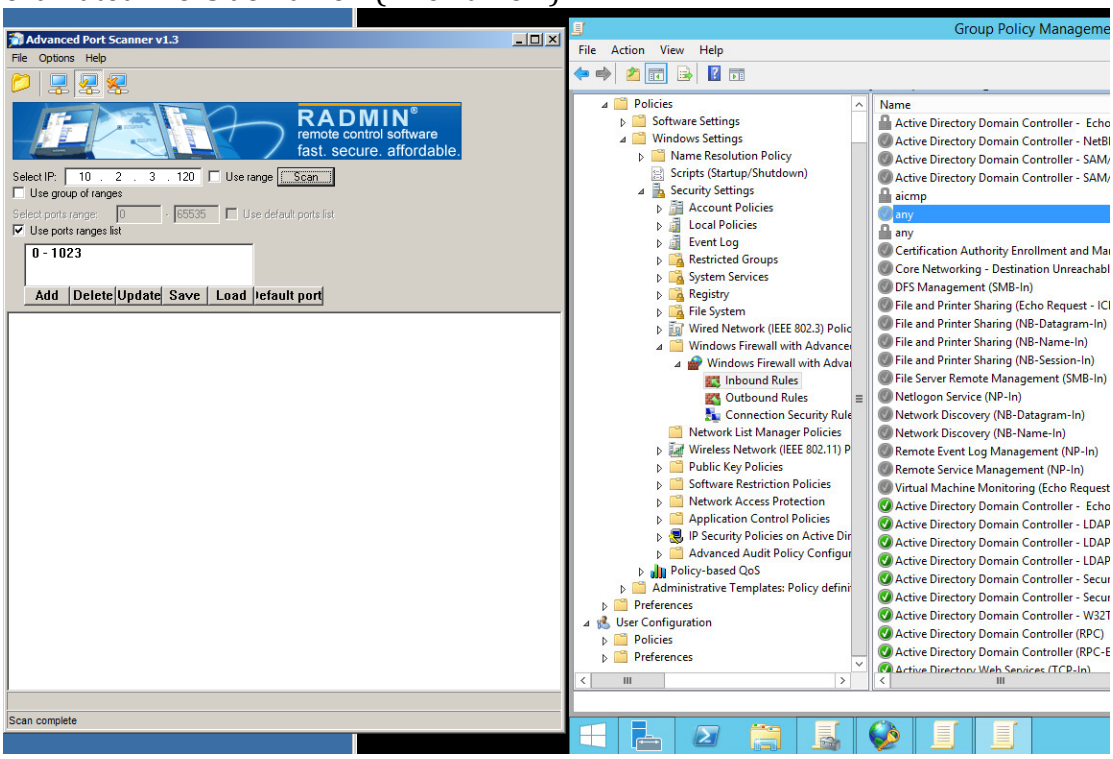
Remarque : on observe que le port pour le SMB est ouvert : 445

Test numéro 7 : Quels sont les ports du serveur visible, avec Firewall, pour un ordinateur hors domaine ? (Firewall ON, Any incoming traffic allowed)

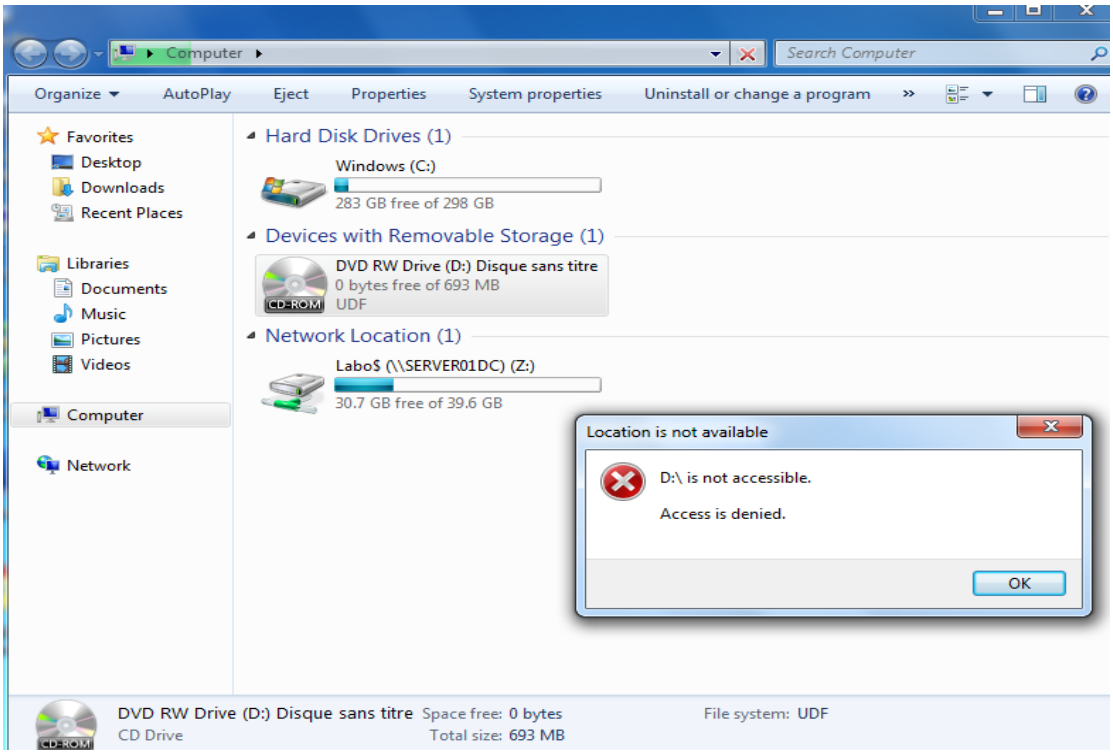


Dans cette situation, le firewall laisse entrer tout le trafic, mais à une exception. Le port SMB n'est plus visible car celui ci nécessite une utilisation d'IPSec pour l'être.

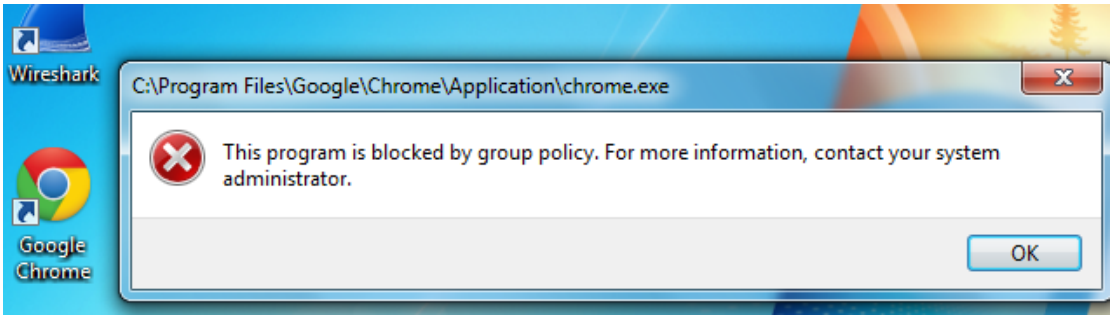
Test numero 8 : Quels sont les ports du serveur visible, avec Firewall, pour un ordinateur hors domaine ? (Firewall ON)



1. **Test numéro 9 :** Est-il possible de lire un CD ?



Test numéro 10 : L'élévation de privilèges est-elle possible ?



En exécutant un programme en tant que : run as administrator, le lancement de l'application n'est pas possible.

IV/ Problèmes rencontrés

Il n'y aurait malheureusement pas assez de temps pour expliquer tous les problèmes rencontrés, mais j'en listerais quelques un.

4.1) VMWARE

Lorsque je suis arrivé à la fin de la période d'évaluation d'ESXi, il m'a fallu le réinstaller et relier le HDD virtuel à une nouvelle configuration virtuelle de serveur 2012. Malgré la prise de snapshots, il m'a été impossible de continuer le projet dû à une corruption de la base AD lors de l'opération et il m a fallu tout recommencer.

4.2) Application des GPOs

Il a fallu de nombreux redémarrages ou de logoff pour appliquer correctement les politiques de sécurités. En effet, celles-ci n'étaient pas toujours prises en compte directement, surtout lorsque la configuration s'appliquait aux machines, et il ne faut pas oublier de spécifier sur quels utilisateurs ou machines, la GPO doit s'appliquer.
Ne jamais configurer une GPO pour toutes les fonctionnalités, mais toujours une par domaine d'application.

4.3) Audit

Les logs ne fonctionnaient pas toujours au début du à une mauvaise configuration de ma part (oubli d'avoir affecter la GPO au serveur). Un mauvais login n'était pas enregistré.

4.4) Firewall et IPSec

Il m'a été impossible d'activer le log du firewall. La configuration s'effaçait à chaque fois.

Il m'est arrivé d'appliquer la configuration du firewall ou de l'IPSec en premier au serveur, ce qui empêchait le client de récupérer la configuration et donc il fallait désactiver la politique et d'abord la déployer au client.

Il m'est arrivé d'appliquer le « require security » au client, et cette fonctionnalité ne fonctionnant pas correctement, il m'est arrivé de l'appliquer en premier au client ce qui le bloquait définitivement. Il m'était impossible d'effacer la configuration du client et la machine n'était plus utilisable. Les communications étaient bloquées, car elles nécessitaient un chiffrement et une authentification.
Il m'a fallu beaucoup de temps afin de diagnostiquer les problèmes liés au « require security ». En effet, une fois activé, les machines ne semblaient pas pouvoir communiquer pour l'échange des données concernant l'authentification et le chiffrement et les machines ne pouvaient plus communiquer. Mais parfois, cela fonctionnait tout de même. Je n'ai trouvé aucune explication à ce sujet qui m'a valu de perdre plusieurs jours de travail pour les diagnostiques et les tests. Cette solution a été abandonnée et remplacée par le « request security ».

Toujours appliquer la configuration au client d'abord puis au serveur. En effet, une politique appliquée en premier à un serveur peut empêcher plus tard le client de récupérer la configuration et le bloque.

4.5) Radius

La version de 802.1x est buggé sur Windows 7 et peut ne pas fonctionner dans certains cas. Plusieurs jours de travail ont été nécessaire pour le diagnostique et les tests. Il est obligatoire d'effectuer les mises à jour du système et cela n'a pas été fait. J'ai testé toutes les combinaisons d'algorithmes d'authentifications, mais il n'a pas été possible de faire fonctionner 802.1x avec Windows 7 du laboratoire de HEPIA. J'ai donc utilisé un MAC OSX, pour tester RADIUS, et cela fonctionne parfaitement.
Les codes d'erreurs trouvés sur Wireshark ne donnaient aucune informations utilisables pour le diagnostique.

V/ Conclusion

Ce projet a été très intéressant à mettre en œuvre dans le cadre où il m'a permis de mettre en pratique différentes notions de sécurités étudiées à HEPIA, d'observer l'effet des mauvaises configurations et des comportements inattendus. Vu les menaces grandissantes, en ce qui concerne les réseaux et les utilisateurs, il est difficile de mettre en œuvre un système de sécurité fiable prenant en compte tous les paramètres. Le risque 0 n'existe pas et la solution parfaite non plus. Afin d'assurer une sécurité maximale, il a été important d'avoir plusieurs niveaux et normes de sécurités. Il aura fallu passer du simple contrôle des comptes utilisateurs et machines, à l'authentification de ces derniers (par la mise en place d'une PKI et d'un système 802.1x), à mettre en place un système d'audit ainsi qu'un chiffrement et un contrôle d'intégrité des connections et des données échangées (IPSec). Mais avec un plus haut niveau de sécurité ne nuisons nous pas aux fonctionnalités et aux interopérabilités ?

VI/ Annexe

6.1) Prérequis

Voici une liste de prérequis (non exhaustive) pour ESXi, selon le fabricant. Nous nous intéresserons aux aspects les plus importants : le processeur, la mémoire, le réseau et le stockage.

Processeur :

- 64-bit x86 CPUs
- 2 cœurs au minimum
- Pour supporter des machines virtuelles 64-bit il faut activer la virtualisation matériel sur le processeur (Intel VT-x ou AMD RVI)

RAM :

- 4 GB au minimum
- Recommandé 8 GB pour bénéficier de performances optimales

Réseau :

- Il faut vérifier avec la base de donnée de VMware la compatibilité des cartes réseaux. En effet, Avec une infrastructure virtualisée de type 1, les drivers disponibles sont moins nombreux qu'avec une de type 2.

Stockage :

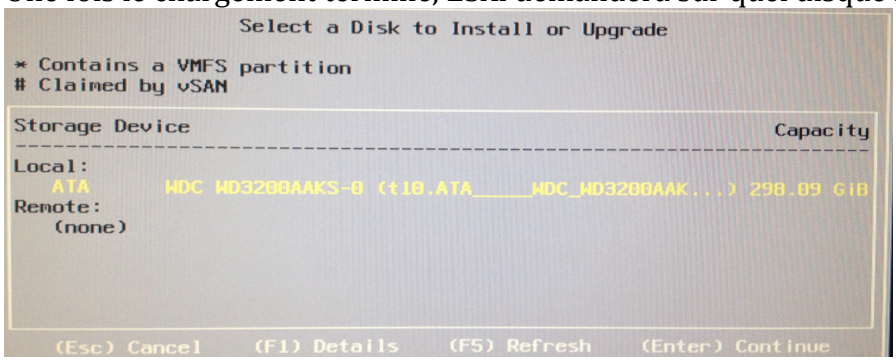
- Disques SCSI
- Disques SATA connectés avec un contrôleur SAS compatible ou un contrôleur SATA intégré

Contrôleur SAS et SATA compatibles :

- LSI1068E
- IBM ServerRAID 8K
- Smart Array P400/256
- DELL PERC 5.0.1
- Intel ICH9
- NVIDIA MCP55

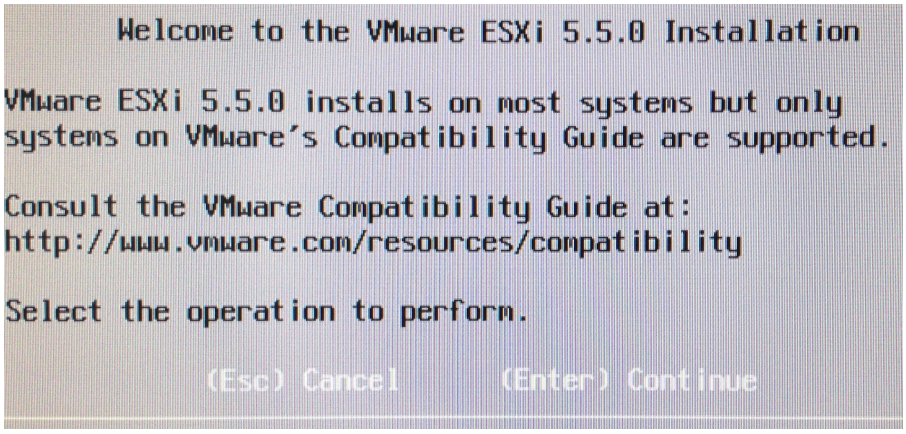
6.2) Installation d'ESXi

- Insérez le disque contenant ESXi
- Booter sur le disque
- Un menu apparaitra. Sélectionnez *ESXi 5.5 standard installer* et patienter durant le chargement
- Une fois le chargement terminé, ESXi demandera sur quel disque installer



(Figure 1)

- VMware nous avertis bien qu'il est possible que le système ne s'installe pas car la compatibilité n'est pas assurée et nous fournit le lien pour vérifier les prérequis cités précédemment. Appuyez sur *Continue*



(Figure 2)

- Acceptez le contrat de License (F11 Accept and Continu)
- Sélectionnez le disque sur lequel l'installer. Confirmez la suppression de données sur le disque
- Insérez un mot de passe fort (HEpia10) et attendez la fin de l'installation

6.3) Configuration

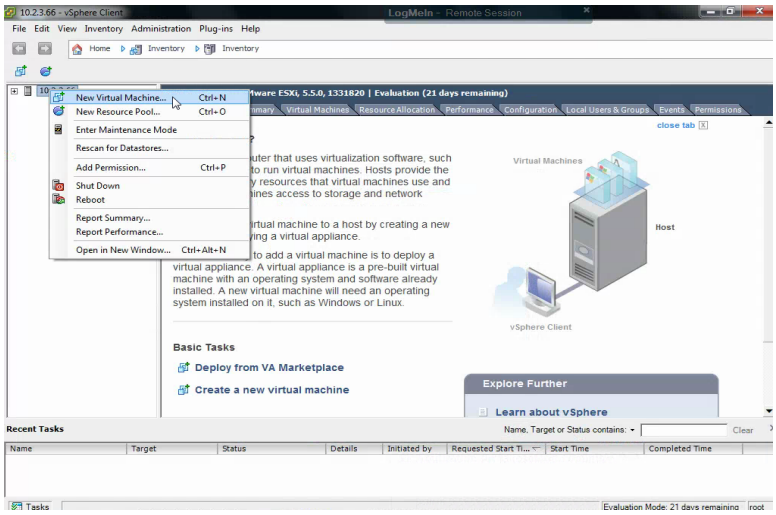
Nous allons maintenant procéder à la configuration IP du serveur

- Allez dans la console, appuyer sur F2 deux fois et entrez le login
- Sélectionnez *configure Managment Network* puis *IP Configuration*, puis *set static IP address and network configuration*
- IP : 10.2.3.66 / SM : 255.255.0.0 / GW : 10.2.0.1
- Retourner au menu précèdent et sélectionner DNS configuration
- Entrez comme serveur primaire : 10.2.3.120 et secondaire : 10.2.3.121
- Hostname : ESXi
- Une fois l'installation et la configuration de base terminée, aller sur un poste client et ouvrez une page internet. Insérer l'adresse IP de ESXi, afficher sur la console, pour télécharger le logiciel de control vSphere : https://10.2.3.66 Acceptez l'erreur de certificat.
- Sur la page WEB, cliquez sur *Download vSphere Client* et procédez a l'installation. Un raccourci sera crée sur le bureau.

6.4) Préparation à l'installation de Windows Serveur 2012

Maintenant nous allons procéder à l'installation de Windows Server en passant par l'hyperviseur.

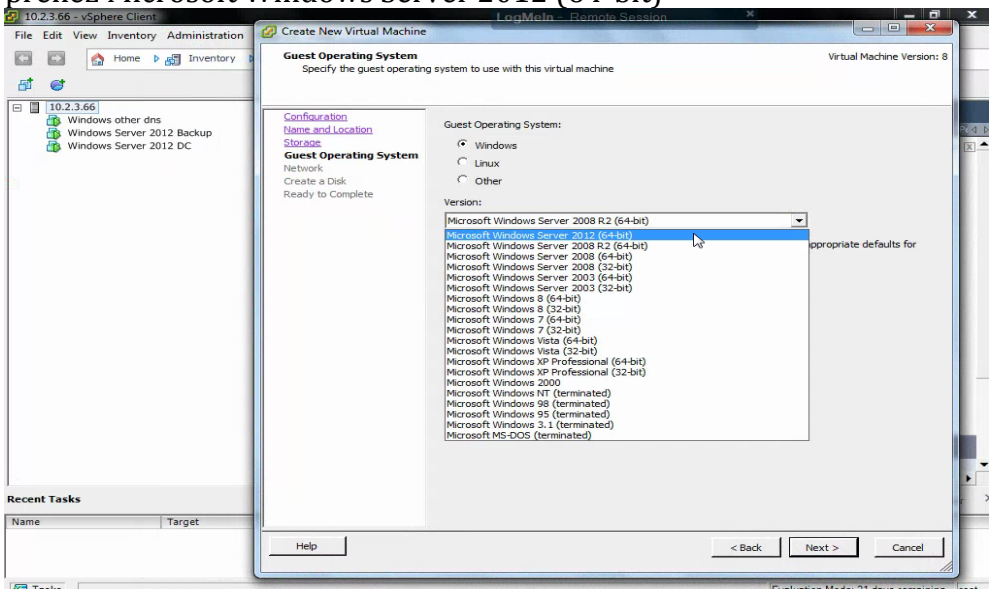
- Ouvrir VMware vSphere Client
- IP Address : 10.2.3.66
- Username : root
- Password : HEpia10
- Faire un clique droit sur l'IP représentant notre ESXi et sélectionnez *New Virtual Machine*



(Figure 3)

- Sélectionnez Typical dans la configuration
- Nom de la machine virtuelle : Windows Server 2012 DC
- Dans la partie Storage, sélectionnez le Datastore. La machine virtuelle y sera stockée.

- Pour le « guest operating system », sélectionnez Windows et dans la liste, prenez Microsoft Windows Server 2012 (64-bit)

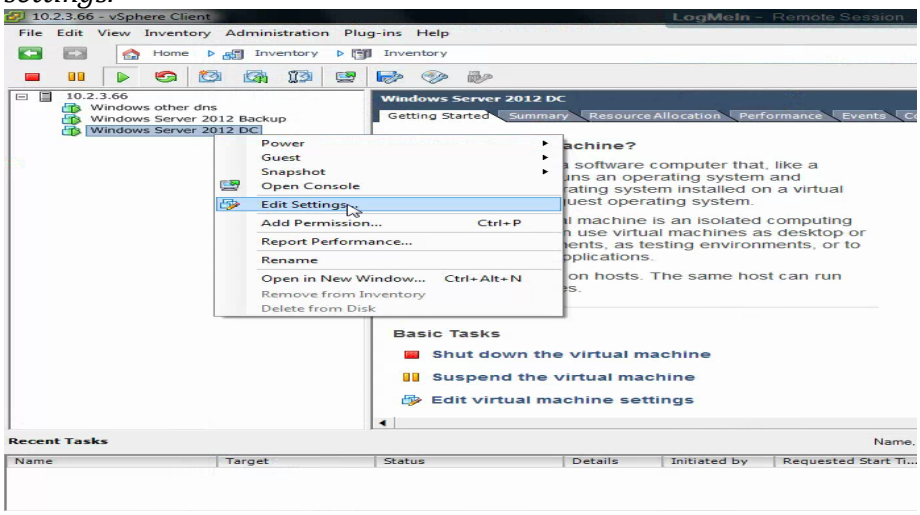


(figure 4)

- Pour le Network, laissez par défaut
- Pour la création du disque virtuelle, entrez la taille de disque souhaiter
- Puis faire *finish*

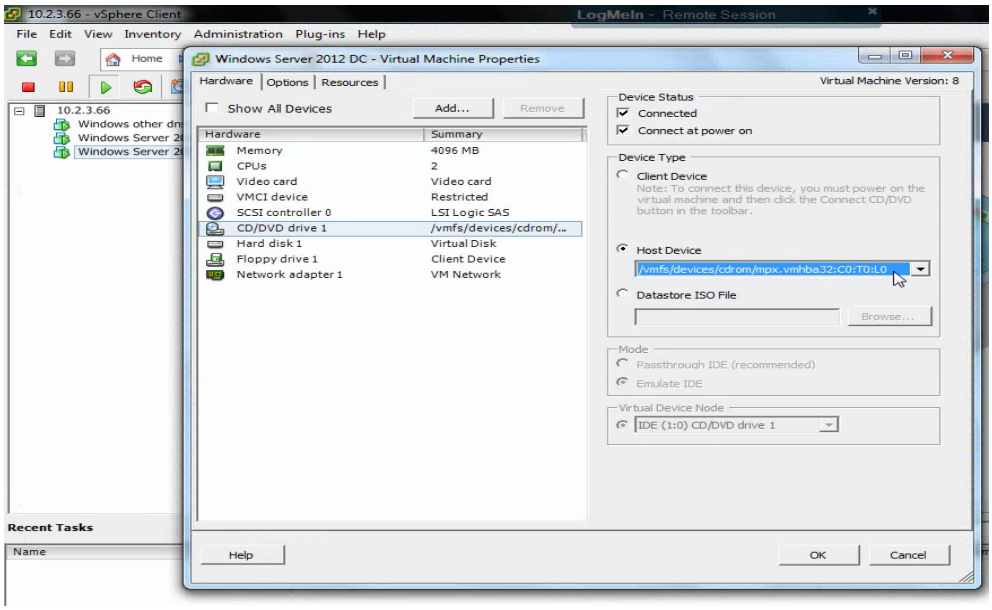
Nous avons donc pu configurer notre machine virtuelle, mais le système d'exploitation n'y est pas encore présent. Nous allons passer à son installation. Nous devons faire en sorte que la machine virtuelle boot sur le lecteur CD.
Pour cela, procédez comme tel :

- Insérez le disque d'installation de Windows dans le serveur
- Dans vSphere Client : clique droit sur notre machine virtuelle puis *edit settings.*



(Figure 5)

- Dans l'onglet *Hardware*, sélectionnez le lecteur CD et configurez telle que l'image. Cela permettra de connecter le lecteur CD à la machine virtuelle et de booter dessus.



(Figure 6)

- Sélectionnez la machine virtuelle puis appuyer sur le bouton en vert *Power on*.