République **A**lgérienne **D**émocratique et **P**opulaire

Ministère de l'**E**nseignement **S**upérieur et de la **R**echerche **S**cientifique

UNIVERSITE **M**ouloud **M**AMMERI DE **T**IZI- **O**UZOU

FACULTE DE **G**ENIE **E**LECTRIQUE ET D'**I**NFORMATIQUE

DEPARTEMENT D'ELECTRONIQUE

Mémoire de Fin d'Etudes

De MASTER ACADEMIQUE

Filière : Télécommunications

Spécialité : Réseaux et Télécommunications

Présenté par :

M^{r} ABIZAR Belaid

M^{r} NAIT ABDESSELAM Ahcene

Thème

Sécurisation du serveur de fichiers et du serveur Backup au niveau de l'entreprise 2INT Partners

M^{r} M. LAZRI, Maitre de conférences A, UMMTO, Président

M^{r} F. OUALLOUCHE, Maitre de conférences B, UMMTO, Encadreur

M^{r} W. KHADIR, Directeur d'études, 2INT Partners, Co-encadreur

M^{r} D. ALOUACHE, Maitre de conférences B, UMMTO, Examinateur

Soutenu le : 04/07/2018

Remerciements

On remercie Allah qui nous a aidés et nous a donné la patience, le courage et la force d'achever ce travail.

Nous tenons à remercier en cette occasion tout le corps professoral et administratif de la faculté de génie électrique et d'informatique de l'université Mouloud Mammeri Tizi-Ouzou pour la richesse et la qualité de leurs enseignements et qui déploient de grands efforts actualisée.

Nous tenons à remercier sincèrement notre encadreur ***Mr OUALLOUCHE*** *pour nous avoir encadré et dirigé ce travail et qui a été disponible tout au long de la réalisation de ce mémoire.*

Un grand merci à ***Mr KHADIR*** *notre co-encadreur au sein de l'école 2INT Partnres, pour son aide, son soutien, ses encouragements, et le temps qu'il a bien voulu nous consacrer.*

Nous tenons à exprimer notre reconnaissance et notre gratitude à tous nos enseignant(e)s qui nous ont accompagnés(e)s durant notre formation et nos familles et nos ami(e)s pour leurs aides considérables.

A tous ceux qui ont contribué à la réalisation de ce mémoire.

Belaid

Ahcene

Dédicaces

Je dédie ce modeste travail à :

Mes chers Parents, aucun hommage ne pourrait être à la hauteur d'amour dont ils ne cessent de me combler. Que dieu leur procure bonne santé et langue vie,

Ma chère grand-mère que dieu l'accueil dans son vaste paradis, pour tout son sacrifice, son amour, son soutien et ses prières tout au long de ma vie,

A mes chers frères et sœurs : Mourad, Kamel, Samira, Amar et ma petite Lina pour leurs encouragements, permanents, et leur soutien moral,

A tous Mes Ami (e)s : Sid Ali, Nassim, Karim, Massi, Salim, Sarah, Mariem et à mon binôme Ahcene ainsi que mes cousin(e)s,

Pour toute ma famille et mes proches pour leurs soutiens tout au long de mon parcours universitaire,

Que ce travail soit l'accomplissement de vos vœux tant allégués, et le fruit de votre soutien infaillible,

Merci d'être toujours là pour moi.

Belaid

Dédicaces

Je dédie ce modeste travail à :

Mes chers grands Parents aucun hommage ne pourrait être à la hauteur d'amour dont ils ne cessent de me combler. Que dieu leur procure bonne santé et longue vie.

Mes chers parents, pour tous leurs sacrifices, leur amour, leur tendresse, leur soutien et leurs prières tout au long de mes études,

A mon cher frère Amokrane et ma chère sœur Sonia pour leurs encouragements, permanents, et leur soutien moral,

A mon oncle Ferhat pour son appui et son encouragement,

A tous Mes Ami (es) : Idir, Amokrane, Abdenour, Brahim, Chafik, Sonia, Samira, Sarah, Meriem et à mon binôme Belaid ainsi que mes cousin(es),

A toute ma famille pour leur soutien tout au long de mon parcours universitaire

Que ce travail soit l'accomplissement de vos vœux tant allégués, et le fuit de votre soutien infaillible,

Merci d'être toujours là pour moi.

Ahcene

Table des figures

Table des figures

Liste des tableaux

Liste des tableaux

Glossaire

Glossaire

- **2INT** : **I**nternational **I**nstitute of **N**ew **T**echnologies

[A]

- **ARP : A**ddress **R**esolution **P**rotocol

[B]

- **BIOS : B**asic **I**nput **O**utput **S**ystem
- **Boot :** Démarrage d'un système informatique

[C]

- **CISCO : C**omité **I**nterministériel de **S**uivi de **C**oordination et d'**O**rientation

[D]

- **DOS : D**isk **O**perating **S**ystem
- **DMZ : D**e**M**ilitarised **Z**one (Zone démilitarisée)

[G]

- **GRUB : : GR**and **U**nified **B**oot **L**oader
- **GO : G**iga **O**ctet

[H]

- **HTTP : H**yper **T**ext **T**ransfe**r P**rotocol
- **HTTPS : H**yper **T**ext **T**ransfe**r P**rotocol **S**ecure

[I]

- **IT : I**nformation **T**echnologie
- **IP : I**nternet **P**rotocol
- **IETF : I**nternet **E**ngineering **T**ask **F**orce

[L]

- **LAN : L**ocal **A**rea **N**etwork

[M]

- **MAC : M**edia **A**ccess **C**ontrol
- **MS-DOS : M**icro**S**oft **D**isk **O**perating **S**ystem

- **MITM : M**en **I**n **T**he **M**iddle

[R]

- **ROM : R**ead-**O**nly **M**emory

[S]

- **SSh : S**ecure **Sh**ell
- **SSL : S**ecure **S**ocket **L**ayer

[V]

- **VPN : V**irtual **P**rivat **N**etwork (Réseau privé virtuel)
- **VLAN : V**irtual **L**ocal **A**rea **N**etwork

[W]

- **WAN : W**ide **A**rea **N**etwork

Sommaire

Sommaire

Sommaire

Cahier des charges

Cahier des charges

Le système informatique en général prend de plus en plus une place stratégique au sein des entreprises, ils sont toujours liés à des menaces ainsi qu'aux types de ressources. Par conséquent, ce système a besoin d'une sécurité pour protéger les données, en particulier le serveur de fichier et le backup existant dans l'architecture de l'entreprise 2INT Partners.

Le projet abordé consiste à intégrer une sécurité aux deux serveurs. Ce projet sera réalisé au sein l'entreprise 2INT Partners.

Le but de ce travail est de sécuriser le serveur de fichiers et le serveur Backup existant qui font face à certaines vulnérabilités qu'il faut identifier au préalable. La solution proposée permettra d'empêcher à tout intrus d'apporter une modification, suppression ou bien voler de données contenues dans ces serveurs.

Une étude approfondie de l'architecture existante est nécessaire afin de relever les failles de sécurité. La solution à ces failles permettra d'avoir un bon fonctionnement et une amélioration dans la gestion même de cette entreprise. Par conséquent les objectifs à atteindre sont :

- Assurer la sécurité au niveau de serveurs de gestion de fichiers ainsi que tous les serveurs existant dans l'entreprise.
- Ajouter d'autres équipements réseaux permettant d'avoir une meilleure sécurité.
- Mettre les équipements dans un endroit sécurisé.
- Mettre en place une protection physique c'est-à-dire la sécurité au niveau des infrastructures matérielles.
- Mettre en place une sécurité logique, c'est-à-dire la sécurité au niveau des données de l'entreprise, les applications ou encore les systèmes d'exploitation.

Introduction

Introduction

Le développement de l'utilisation d'Internet a permis à beaucoup d'entreprises d'ouvrir leurs systèmes d'information à leurs partenaires, employés, fournisseurs, stagiaires,…etc [1]. Par conséquent, il est essentiel d'avoir une architecture réseau adaptée aux besoins de l'entreprise et de connaître les ressources à protéger et maîtriser le contrôle d'accès au système d'information.

L'évolution de l'infrastructure utilisée dans les réseaux a conduit des personnes malintentionnées à exploiter les failles du réseau afin d'accéder à des informations confidentielles. Ce qui peut conduire à des conséquences nuisibles à l'entreprise. Les différentes données de l'entreprise se trouvent généralement sur des serveurs. A cet effet, sécuriser les serveurs devient une préoccupation de plus en plus importante et la mise en place d'une politique de sécurité est donc nécessaire [2]. La sécurité des systèmes informatique a pour objective de garantir les droits d'accès aux données et ressources d'un serveur ainsi que tout le réseau. Ceci est obtenu en mettant en place des mécanismes d'authentification et de contrôle permettant d'assurer que seuls les utilisateurs possédant les droits d'accès y sont autorisés.

Croyant que le fait d'utiliser le système d'exploitation Linux réduit la problématique de sécurité aux seules failles de l'infrastructure réseau, la plupart des solutions de sécurité proposées aux entreprises ne tiennent pas compte des failles de Linux [3]. Par conséquent, un utilisateur confirmé de Linux pourra détourner les outils de sécurité déployés dans l'infrastructure en exploitant les failles de Linux pour accéder aux différents serveurs.

Dans le cadre de notre projet de fin d'études, nous avons effectué un stage au sein de l'entreprise 2INT Partners. Nous nous sommes intéressé à sécuriser deux serveurs installés sous Linux : le serveur de fichiers et le serveur backup.

Nous avons structuré le présent mémoire en trois chapitres :

- Dans le premier chapitre, des généralités sur la sécurité informatique sont présentées ainsi que les attaques qui peuvent avoir lieu.
- Dans le second chapitre nous présenterons l'étude du réseau existant afin de trouver les failles des deux serveurs.

- Dans le troisième chapitre, nous exposerons la solution mise en place pour sécuriser les deux serveurs étudiés et les tests afin de s'assurer de la fiabilité de cette solution.

Enfin, nous terminons ce mémoire par une conclusion et une bibliographie.

Chapitre 1 : Généralités sur la sécurité informatique

1.1. Préambule

La sécurité d'un réseau est un niveau de garantie pour que l'ensemble des machines de ce dernier fonctionnent d'une façon optimale. En conséquence, la mise en œuvre de la sécurité est indispensable au sein d'un réseau afin de le protéger de tout sort d'intrusion malveillante.

Dans ce chapitre nous allons présenter les différents aspects liés à la sécurité. Les types d'attaques et leurs mécanismes de détection et la protection des réseaux informatiques.

1.2. Définition de la sécurité informatique

La sécurité informatique est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour conserver, rétablir, et garantir la sécurité des systèmes informatiques. Elle est intrinsèquement liée à la sécurité de l'information et des systèmes d'information [4].

1.3. Les objectifs de la sécurité informatique

La sécurité informatique vise généralement cinq principaux objectifs :

La disponibilité : Le système doit fonctionner sans faille durant les plages d'utilisation prévues et garantir l'accès aux services et ressources installées avec le temps de réponse attendu.

L'intégrité : Les données doivent être celles que l'on attend, et ne doivent pas être altérées de façon fortuite, illicite ou malveillante. En clair, les éléments considérés doivent être exacts et complets.

Les confidentialités : Seules les personnes autorisées peuvent avoir accès aux informations qui leur sont destinées. Tout accès indésirable doit être empêché.

L'authentification : L'identification des utilisateurs est fondamentale pour gérer les accès aux espaces de travail pertinents et maintenir la confiance dans les relations d'échange.

La non-répudiation : Aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées et aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur.

1.4. Politique de sécurité

La politique de sécurité exprime la stratégie de l'entreprise en matière de sécurité de l'information. Toutefois, Il n'existe pas de règles déclinables à tous, chaque entreprise présente des particularités et utilise une politique de sécurité selon l'architecture de son réseau [2]. La sécurité de sécurité définit les règles à suivre pour l'accès au réseau informatique et pour gérer les flux de données entrants et sortants. La mise en place d'une politique de sécurité adéquate est essentielle à la bonne sécurisation des réseaux et des systèmes d'information.

Une politique de sécurité doit comprendre au moins les éléments suivants :

- Les fondements de la sécurité de l'information propre à l'organisme intégrant les obligations légale et les missions propres à l'organisme précisera notamment les principes régissant la protection des données à caractère personnel.
- Les exigences de sécurité à respecter en termes de confidentialité, intégrité, disponible, imputabilité, authenticité, fiabilité et non répudiation des informations.
- Les différents éléments de sensibilisation aux arguments et au contenu même de cette politique définie par l'organisme.
- La description des différents rôles, responsabilités et règles organisationnelles cadrant la mise en application de la politique.
- La démarche de gestion des risques adoptée par l'organisme afin de détecter les risque, de les apprécier selon des critères définis et de déterminer les modalités pour les traiter en les réduisant à un niveau acceptable.
- La description du cadre organisationnel des processus de gestion des incidents de sécurité.
- Les modalités générales de gestion de la sécurité de l'information, notamment en matière de protection et de prévision.
- Les modalités retenues par l'organisme afin d'intégré la politique de sécurité dans les processus de développement, de maintenance et de changement.

1.5. Objectif d'une politique de sécurité

La définition d'une politique de sécurité est une démarche de toute l'entreprise visant à protéger son personnel et ses biens d'éventuels incidents de sécurité dommageable pour son activité. La définition d'une politique sécurité réseau fait intégralement partie de la démarche sécuritaire de l'entreprise [2]. Elle s'étend à de nombreux domaines dont les suivants :

- Audit des éléments physiques et logiques constituant le système d'information de l'entreprise.
- Formation du personnel utilisant les moyens informatiques du système d'information.
- Identifier les besoins en termes de sécurité, les risques informatiques pesant sur l'entreprise et leurs éventuelles conséquences.
- Elaborer des règles et des procédures à mettre en œuvre dans les différents services de l'organisation pour les risques identifiés
- Surveiller et détecter les vulnérabilités du système d'information et se tenir informé des failles sur les applications et matériels utilisés
- Définir les actions à entreprendre et les personnes à contacter en cas de détection d'une menace

1.6. Classification des attaques

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque. Celle-ci est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel,…etc.) ou bien même de l'utilisateur à des fins non autorisées par l'exploitant des systèmes [4].

Sur le réseau Internet, des attaques ont lieu en permanence, à raison de plusieurs attaques par minute sur chaque machine connectée. Ces attaques sont pour la plupart lancées automatiquement à partir de machines infectées (par des virus, chevaux de Troie, vers, etc.), à l'insu de leur propriétaire [5].

1.6.1. Types d'attaques

1.6.1.1. Les attaques directes :

C'est la plus simple des attaques à réaliser :

Le hacker attaque directement sa victime à partir de son ordinateur par des scripts d'attaques faiblement paramétrable.

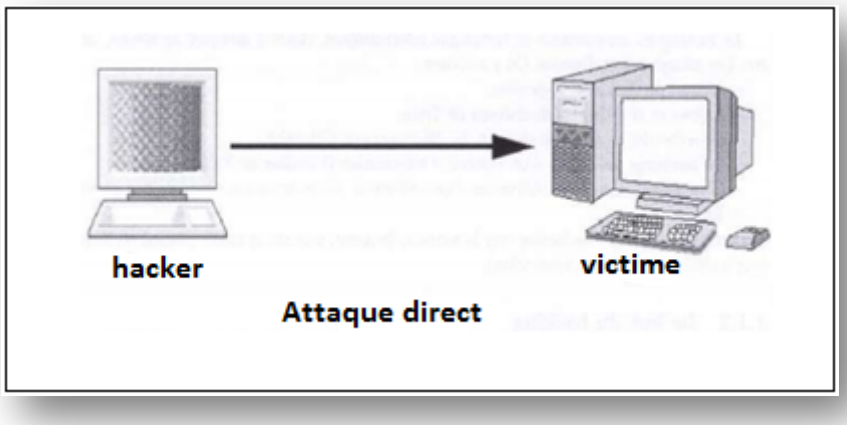

Fig.1.1 : Attaque directe.

1.6.1.2. Les attaques indirectes par rebond :

Dans ce cas, une machine cible est attaquée par l'intermédiaire d'une autre machine.

Fig.1.2 : Attaque par rebond.

1.6.1.3. Les attaques indirectes par réponse :

Cette attaque est une dérivée de la précédente.

La réponse à la première attaque représente une attaque plus virulente pour la machine cible.

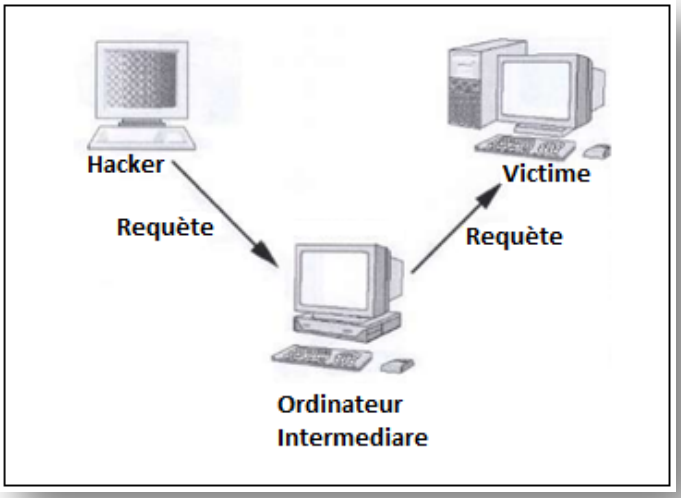

Fig.1.3 : Attaque indirecte par réponse

1.6.2. Attaques sur les réseaux

1.6.2.1. Attaque par usurpation d'adresse IP (IP spoofing)

Cette attaque consiste à remplacer l'adresse IP du l'expéditeur d'un paquet IP par l'adresse IP d'une autre machine.

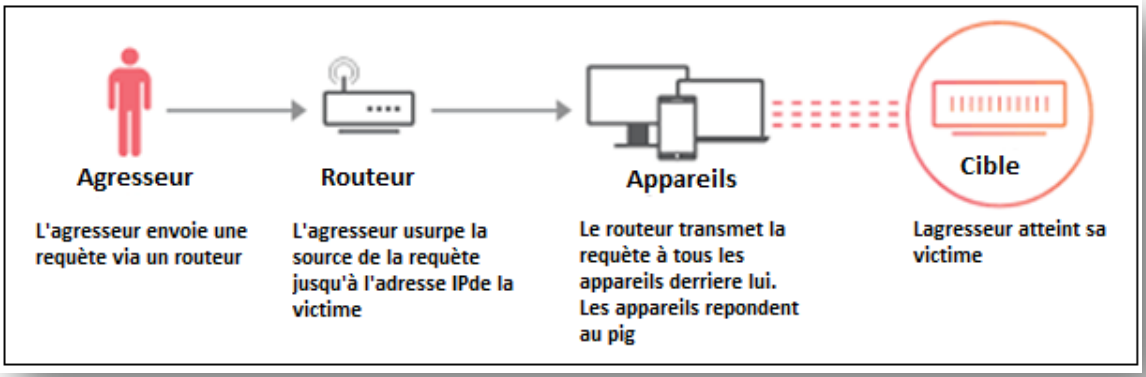

Fig.1.4 : Attaque par adresse IP

1.6.2.2. Attaque par usurpation d'adresse MAC (MAC spoofing) :

Elle consiste à se faire passer pour une machine autorisée. Il suffit à l'intrus d'utiliser l'identité (adresse MAC) d'une machine autorisée à utiliser un service donnée.

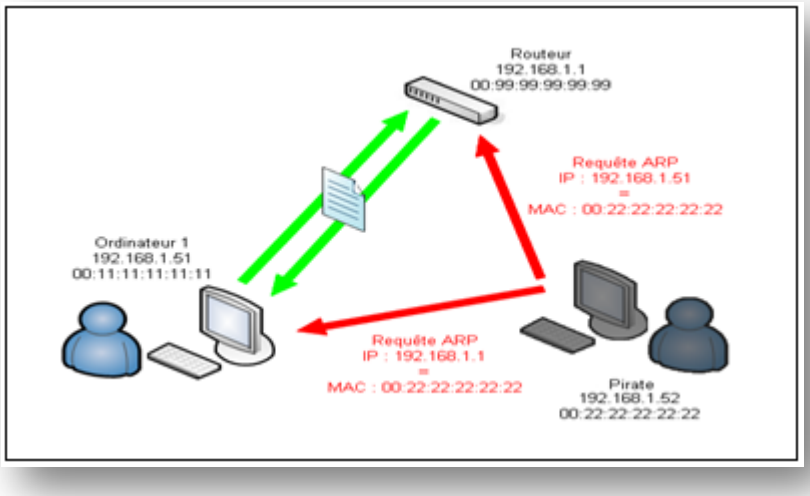

Fig.1.5 : Attaque par adresse MAC

1.6.2.3. ARP spoofing :

Cette attaque permet de rediriger le trafic d'une machine vers une autre. Grâce à cette redirection une personne mal intentionnée peut se faire passer pour une autre.

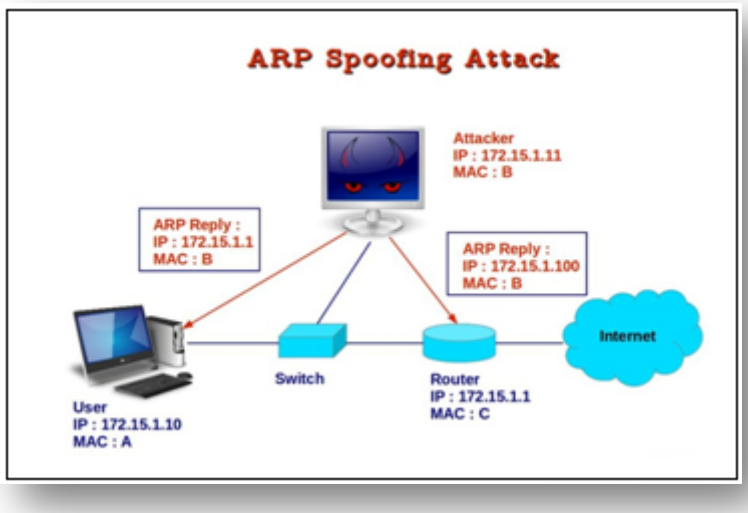

Fig.1.6 : ARP Spoofing

1.6.2.4. Attaque de mot de passe :

Il est très simple d'obtenir un programme permettant de retrouver le mot de passe utilisé pour l'accès à un service en utilisant des logiciels spéciaux comme les Keyloggers. Il permet de fait l'enregistrement de frappes qui espionne électroniquement l'utilisateur d'un ordinateur.

1.6.2.5. Les portes dérobées (backdoor):

La porte dérobée est généralement introduite par un développeur de logiciels. Celui-ci crée un chemin non-surveillé pour accéder à l'ordinateur de la victime.

Une fois qu'une porte dérobée est installée avec le logiciel développé, l'attaquant a la possibilité de surveiller ce que fait l'utilisateur et de copier ou détruire les données ou bien la possibilité de prendre le contrôle d'un ordinateur (réseau).

1.6.2.6. Attaque Man In The Middle (MITM):

Cette attaque est une redirection complète du flux échangé entre deux machines. Chacun des interlocuteurs croit dialoguer directement avec l'autre, mais en réalité il s'adresse à une 3ème machine qui joue le rôle d'un intercepteur de ces données.

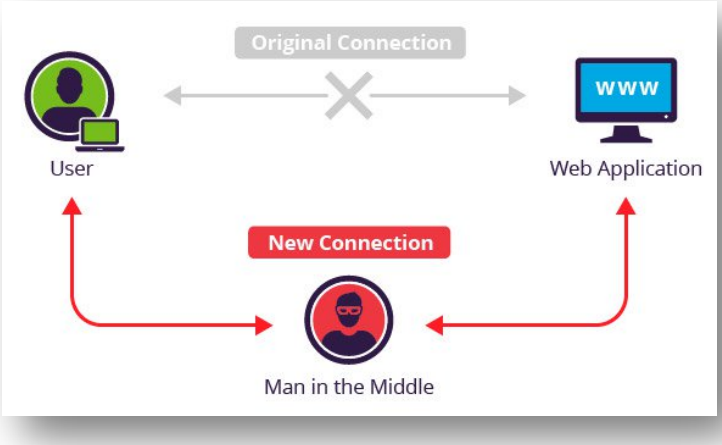

Fig.1.7: Attaque Men In The Middle.

1.7. Attaques logiciel

Le cheval de Troie : C'est un programme informatique malveillant parfois destructeur. Il est souvent porté par un logiciel sous licence et protégé, modifié par des hackers pour en faire cadeau à la communauté numérique, et aussi c'est un logiciel en apparence légitime, mais qui contient une fonctionnalité malveillante. Son rôle est de faire entrer ce parasite sur l'ordinateur et de l'y installer à l'insu de l'utilisateur.

Le virus : C'est un programme malveillant conçu pour se propager à d'autres ordinateurs (équipements) en s'insérant dans des logiciels légitimes.

Les vers informatiques : Un ver, contrairement à un virus informatique, n'a pas besoin d'un programme hôte pour se reproduire. Il exploite les différentes ressources de l'ordinateur qui l'héberge pour assurer sa reproduction.

Un spyware : Logiciel espion qui s'installe sur un ordinateur, dans le but de collecter et transférer des informations sans que l'utilisateur en ait connaissance.

Le déni de service (attaque DOS) : Le principe de cette attaque consiste à envoyer des paquets IP ou de données de taille ou de constitution inhabituelle afin de provoquer une saturation ou un état instable des machines victimes et de les empêcher d'assurer les services voulus.

1.8. Les types de menaces :

Les menaces sont classées en deux catégories :

1.8.1. Les menaces passives :

Elles consistent essentiellement à copier ou à écouter l'information contenue dans un système. Ces attaques nuisent à la confidentialité des données. Dans ce cas, celui qui prélève une copie ne cherche pas à altérer cette information ou le système. Ce type de menace est difficile à détecter.

1.8.2. Les menaces actives :

Elles nuisent à l'intégrité des données. Dans ce cas, l'intégrité ou l'existence même du système est menacé.

Les menaces dues aux accidents représentent 26% des menaces .Elles sont le fait d'incendies, de panes d'équipements ou du réseau, défaut de qualité. 17% des menaces sont dues aux erreurs d'utilisation. 57% sont dues à la malveillance dont 80% sont d'origines interne. Elles concernent les actes tels que : Vol d'équipement, intrusions, écoute du réseau, attaque logique (virus, modification, …).

1.9. Piratage (Hacking) :

Le piratage informatique est une pratique visant à un échange discret d'informations illégales ou personnelles. Cette pratique, établie par les hackers, le hacking peut se définir également comme un ensemble de techniques permettant d'exploiter les failles et vulnérabilités d'un élément ou d'un groupe d'éléments matériels ou humains [6].

1.10. Les différents types de pirates informatiques

Les pirates informatiques (hackers) sont des informaticiens qui utilisent leurs connaissances de la sécurité informatique pour en rechercher et en exploiter les faiblesses, chacun a un but différent des autres, pour certains, le piratage est juste un loisir, pour d'autres c'est pour acquérir un savoir ou faire des choses illégales comme voler des données confidentielles.

Il existe de nombreux types de pirates informatiques catégorisés selon leurs motivations, on peut citer :

1.10.1. Le hacker au chapeau blanc (White Hat Hacker) :

Il s'agit souvent d'une personne qui a atteint une maturité d'esprit ainsi que des qualifications suffisantes et approuvées par les autres.

Il aide les victimes, il aide à sécuriser les systèmes et combat contre la cybercriminalité, ce hacker au chapeau blanc est également le hacker éthique dont on reparlera souvent, son slogan est « apprendre l'attaque pour mieux se défendre » et non pas pour causer des dommages.

1.10.2. Le hacker au chapeau noir (Black Hat Hacker) :

Le hacker au chapeau noir peut être aussi expérimenté que celui au chapeau blanc, voire plus. Mais il agit par contre à des fins qui lui sont propres**,** et qui sont illégales**.** Il vole des données, s'introduit illégalement dans les systèmes ou encore pirate des comptes.

1.10.3. Le hacker au chapeau gris (Grey Hat Hacker) :

C'est un mélange de White Hat et de Black Hat, ce hacker agit des fois pour la bonne cause, comme un White Hat le fait mais peut commettre de temps à autre des délits.

Il s'introduit illégalement dans un système afin d'en prévenir ensuite les responsables des failles qu'il aura trouvées. Son action est louable, mais tout de même illégale.

1.10.4. Les hacktivistes :

Ils agissent pour une cause souvent politique. Ils attaquent généralement des entreprises et non pas des utilisateurs particuliers.

1.10.5. Les script-kiddies :

Sont tous ces jeunes hommes qui loin d'avoir compris les grands principes du hacking et l'éthique du hacker, se servent des programmes tout faits pour causer des dommages qui peuvent êtres très gênants.

1.11. Le but du hacking

Le but du hacking est divers. Selon les individus (les "hackers"), on y retrouve :

- Vérification de la sécurisation d'un système.
- Vol d'informations (fiches de paye...).
- Terrorisme.
- Espionnage "classique" ou industriel.
- Chantage.
- Manifestation politique.
- Par simple "jeu", par défi.
- Pour apprendre.

1.12. Les phases du piratage :

Ce processus peut être décomposé en cinq phases, qui sont similaires peu importe les intentions du pirate informatique. La figure suivante illustre ces cinq phases :

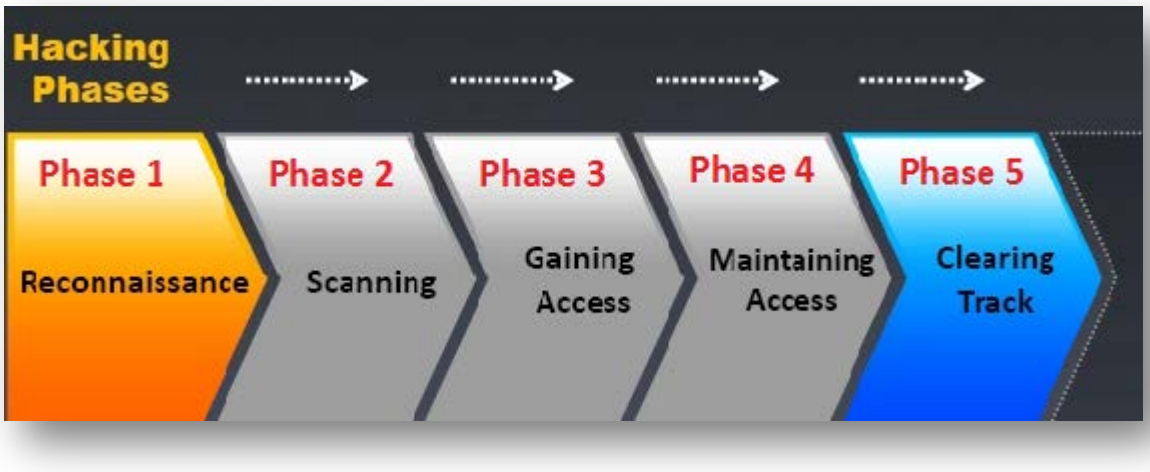

Fig.1.8 : Les phases du piratage

Reconnaissance : C'est de collecter les informations de la cible. On distingue deux types de reconnaissance :

- Reconnaissance passive : Via internet
- Reconnaissance active : Après avoir connecté avec la personne.

Scanning : Il s'agit de prendre l'information découverte lors de la reconnaissance et de l'utilisé pour examiner le réseau, les outils qu'un hacker peut utiliser pendant la phase d'analyse peuvent inclure des numéroteurs, des scanners de porte, des balayeurs, et les scanners de vulnérabilité.

Gaining Access (acquisition de l'accès) : Après la numérisation le hacker reçoit le plan du réseau de la cible à laide des données collecté pendant la phase 1 et la phase 2. C'est la phase ou le véritable piratage a lieu.

Maintaining Access : (maintien de l'accès) Une fois qu'un pirate a obtenu l'accès, après avoir obtenu l'accès, l'intrus peut maintenir cet accès pour une exploitation et des attaques futures.

Clearing hacker: (Effacer les traces) C'est la dernière phase, une fois que les pirates ont réussi a obtenir et maintenir l'accès, ils couvrent leurs trace pour évité d'être repéré par le personnelle de sécurité, de continuer à utilisé le système, d'éliminer les preuves de piratage.

1.13. Triangle de sécurité :

Tout système peut être défini par la force de trois composants qui sont :

La sécurité, la fonctionnalité et la convivialité. L'idéal est d'avoir « la balle » au milieu afin d'optimiser ces trois composants au même temps.

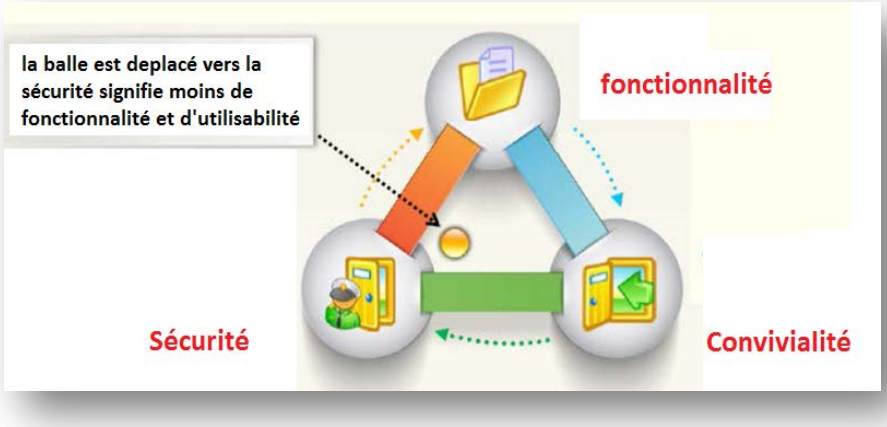

Fig.1.9 : Triangle de sécurité.

1.14. Les outils utilisés pour sécuriser un réseau :

1.14.1. Le pare-feu (firewall) :

Dispositif qui protège un système informatique connecté à Internet des tentatives d'intrusion qui pourraient en provenir.

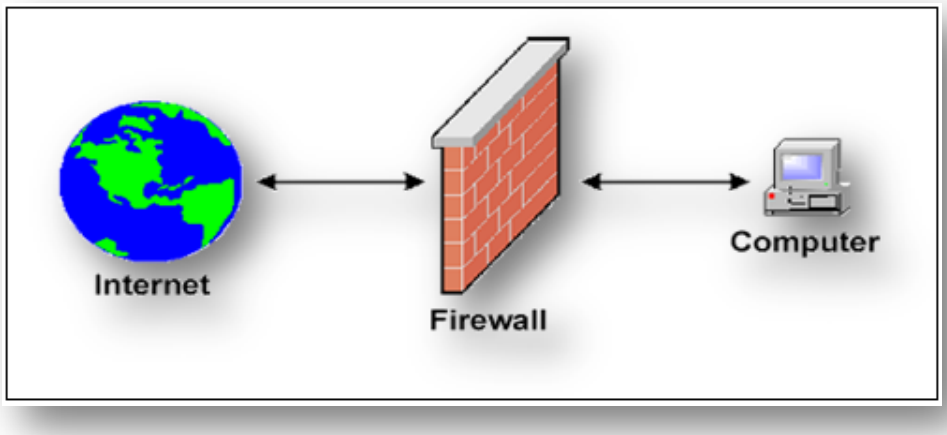

Fig.1.10 : Utilité d'un pare-feu

1.14.2. Le VPN (Virtual Private Network):

C'est un système permettant de créer un lien direct entre ordinateurs distants. C'est un tunnel Sécurisé à l'intérieur d'un réseau (Internet).

Cependant, l'information VPN, dispose des informations permettant d'identifier l'utilisateur.

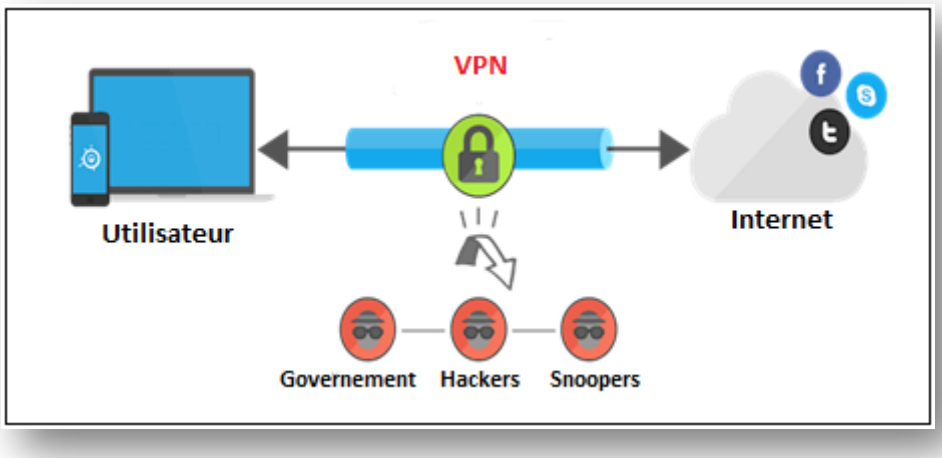

Fig.1.11 : Système VPN

1.14.3. VLAN :

Un réseau local virtuel, qui est un réseau logique indépendant sert à segmenter le réseau en sous réseaux logiques.

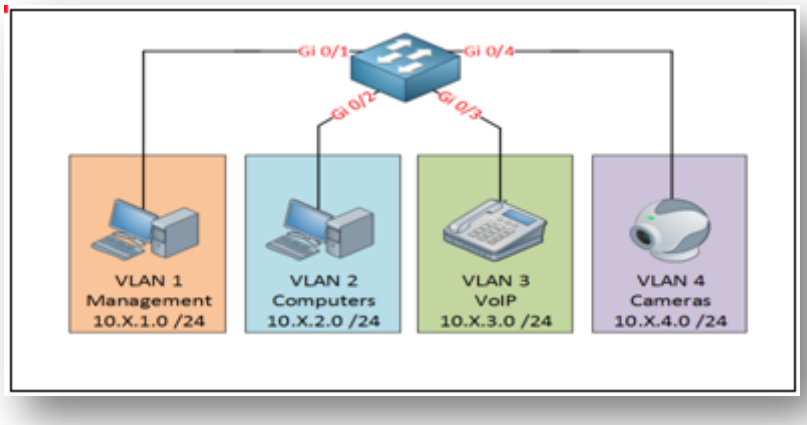

Fig.1.12 : Exemple d'un réseau VLAN

1.14.4. Zone démilitarisée (DMZ) :

Zone démilitarisée C'est un sous-réseau séparé du réseau local et isolé de celui-ci et d'Internet (ou d'un autre réseau) par un pare-feu. Ce sous-réseau contient les machines étant susceptibles d'être accédées depuis Internet.

Le pare-feu bloquera donc les accès au réseau local pour garantir sa sécurité. Et les services susceptibles d'être accédés depuis Internet seront situés en DMZ.

En cas de compromission d'un des services dans la DMZ, le pirate n'aura accès qu'aux machines de la DMZ et non au réseau local [5].

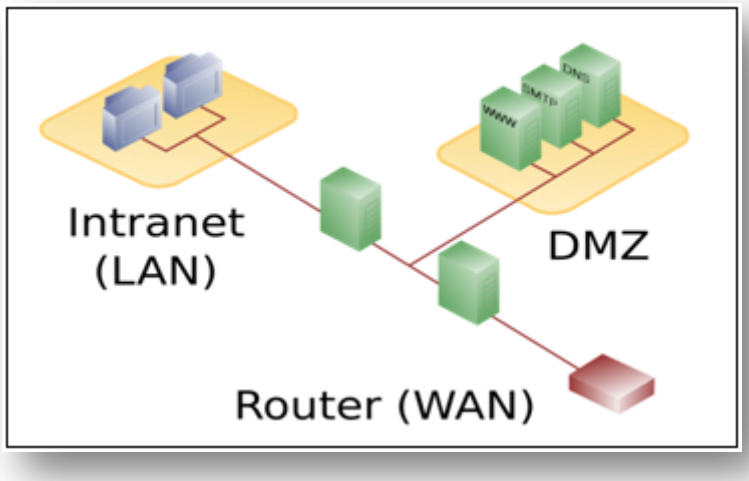

Fig.1.13 : Zone DMZ.

1.14.5. Le proxy :

C'est un composant logiciel qui joue le rôle d'intermédiaire en se plaçant entre hôtes. Dans le cas des réseaux un proxy sert à une machine intermédiaire pour accéder à un autre réseau généralement internet.

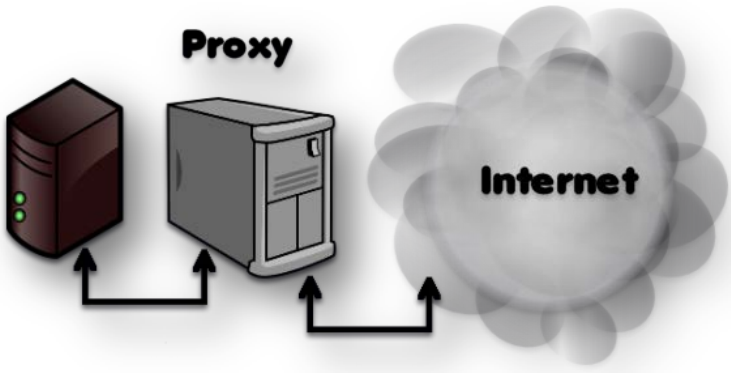

Fig.1.14 : Proxy.

1.14.6. Les anti-virus :

Les anti-virus sont des logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants (dont les virus informatique1 ne sont qu'une catégorie).

Ces derniers peuvent se baser sur l'exploitation de failles de sécurité, mais il peut également s'agir de logiciels modifiant ou supprimant des fichiers, que ce soit des documents de l'utilisateur stockés sur l'ordinateur infecté, ou des fichiers nécessaires au bon fonctionnement de l'ordinateur (le plus souvent ceux du système d'exploitation).

1.15. Test d'intrusion :

Les tests d'intrusion consistent à éprouver les moyens de protection d'un système d'information en essayant de s'introduire dans le système en situation réelle.

Et parmi ses objectifs d'un test d'évaluation sont :

- Evaluation des systèmes.
- Indication des failles.
- Faire un rapport général.
- Evaluer la sécurité et pour dire qu'elle est normalisée.

1.16. Types de test d'intrusion :

On distingue généralement trois méthodes distinctes :

- **Black box (boite noir)** : consistant à essayer d'infiltrer le réseau sans aucune connaissance du système.
- **white box (boite blanche)** : consistant à tenter de s'introduire dans le système en ayant connaissance de l'ensemble du système, afin d'éprouver au maximum la sécurité du réseau.
- **Grey box (boite grise) :** est une combinaison en boite blanche et boite noir, son but est de recherché les défauts. Le cas d'échéant en raison d'une mauvaise utilisation des applications [4].

1.17. Phase de test d'intrusion

La figure ci-dessous nous montre les différentes phases existantes dans un test d'intrusion :

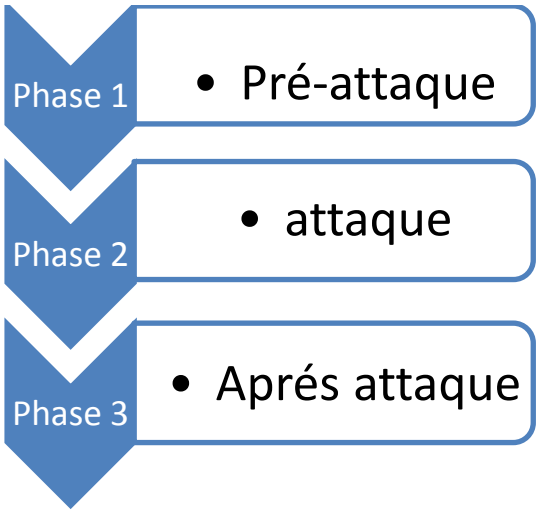

Fig.1.15 : Différente phase d'intrusion.

- ✓ **Phase 1** : Pré-attaque : c'est avoir les outils pour faire un test d'intrusion.
- ✓ **Phase 2** : Attaque : voler les informations
- ✓ **Phase 3** : Après l'attaque : Généré un rapport.

1.18. Les protocoles de sécurité

1.18.1. Protocole SSL

Le SSL est le protocole de sécurité le plus répandu qui crée un canal sécurisé entre un client et un serveur communiquant sur internet ou un réseau interne. Dans notre société centrée sur un internet vulnérable. Le SSL est généralement utilisé lorsqu'un navigateur doit se connecter de manière sécurisée à un serveur web [2].

En pratique, le SSL devrait être utilisé dans les cas suivants :

- Pour sécuriser les transactions bancaires en ligne.
- Pour sécuriser les connexions et tout échange d'information confidentielle.
- Pour sécurisé les applications et les messageries web.

- Pour sécurisé les flux de production et les applications de virtualisation tels que les plates-formes sur le Cloud.

1.18.2. Protocole SSH

Le protocole SSH a été mis au point en 1995, il s'agit d'un protocole permettant à un client (un utilisateur ou même une machine) d'ouvrir une session interactive sur une machine distante (serveur) afin d'envoyer des commandes ou des fichiers de manière sécurisé [5,7].

- Les données circulant entre le client et le serveur sont chiffrées, ce qui garantit leur confidentialité. Il est donc pas possible d'écouter le réseau à laide d'un analyseur de trames.
- Le client et le serveur s'authentifient mutuellement afin d'assurer que les deux machines qui communiquent sont bien celles que chacune des partie croit être. Il n'est donc plus possible pour un pirate d'usurper l'identité du client ou du serveur.

SSH est un protocole, c'est-à-dire une méthode standard permettant à des machines d'établir une communication sécurisée. A ce titre, il existe de nombreuses implémentations de clients et de serveurs SSH. Certains sont payants, d'autres sont gratuits ou open source. Son fonctionnement est décrit comme suit :

- Dans un premier temps le serveur et le client s'identifient mutuellement afin de mettre en place un canal sécurisé (couche de transport sécurisée).
- Dans un second temps le client s'authentifie au prés du serveur pour obtenir une session.

1.18.3. Protocole HTTP

Le protocole HTTP est un protocole de transfert, il définie la communication entre un client et un serveur sur le (WWW).

Ce protocole fonctionne sur le principe « requête-réponse ». En prenant un exemple commun, de communication entre un navigateur web et un serveur web [2], la communication se déroule de la manière décrite sur le schéma suivant :

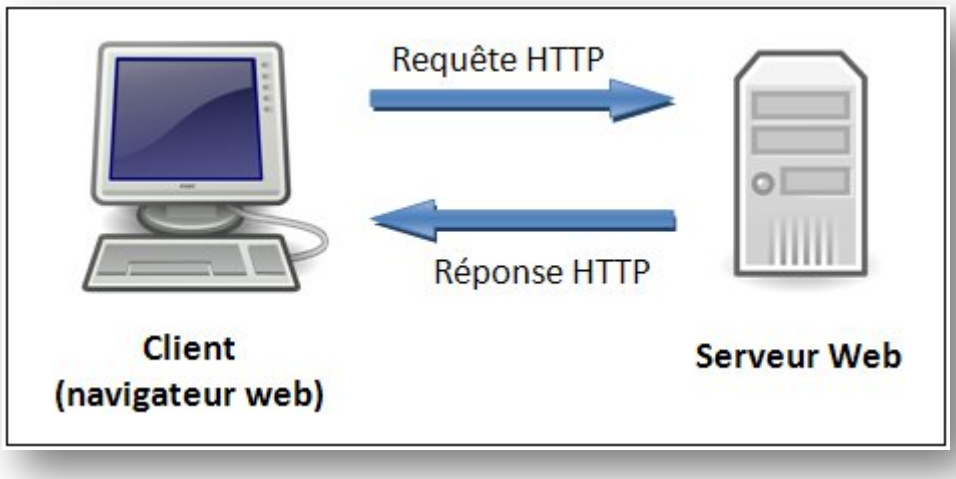

Fig.1.16 : Schéma d'une requête http.

1.18.4. Protocole HTTPS

HTTPS est un procédé de sécurisation des transactions http reposant sur une amélioration du protocole http mise au point en 1994 par l'EIT. Il permet de fournir une sécurisation des échanges lors de la transaction de commerce électronique en cryptant les messages afin de garantir aux clients la confidentialité de leur numéro de carte bancaire ou de toute autre information personnelle [2].

1.19. La cryptographie

La cryptographie est une science permettant de convertir des informations "en clair" en Informations codées, c'est à dire non compréhensible, puis, à partir de ces informations codées, de restituer les informations originales [5].

1.19.1. La cryptographie symétrique

On parle de cryptographie à algorithme symétrique lorsque plusieurs personnes utilisent une même clé pour crypter et décrypter des messages. Cette clé est le plus souvent appelée "secrète" (en opposition à "privée") car toute la sécurité de l'ensemble est directement liée au fait que cette clé n'est connue que par l'expéditeur et le destinataire.

Le principal inconvénient de ce système est le partage de cette clé unique entre les différentes personnes.

1.19.2. La cryptographie asymétrique

La cryptographie asymétrique est un domaine de la cryptographie où il existe une distinction entre des données publiques et privées, en opposition à la cryptographie symétrique où la fonctionnalité est atteinte par la possession d'une donnée secrète commune entre les différents participants. Son but est de garantir la confidentialité d'une donnée.

Dans ce type de cryptographie, chaque utilisateur comporte deux clés :

- Une clé privée qui doit être gardée secrète.
- Une clé publique qui est disponible pour tous les autres utilisateurs.

Ce système permet de :

Chiffrer le message à envoyer : l'expéditeur utilise la clef publique du destinataire pour coder son message. Le destinataire utilise sa clef privée pour décoder le message de l'expéditeur, garantissant la confidentialité du contenu.

S'assurer de l'authenticité de l'expéditeur : L'expéditeur utilise sa clef privée pour coder un message que le destinataire peut décoder avec la clef publique de l'expéditeur ; c'est le mécanisme utilisé par la signature numérique pour authentifier l'auteur d'un message.

C'est-à-dire, ces deux clés sont mathématiquement liées. Dans la pratique, la clé publique sert à crypter les messages, et la clé privée sert à les décrypter. Une fois le message crypté, seul le destinataire est en mesure.

1.20. Discussion

La sécurité informatique est un vaste domaine de l'informatique. Dans ce chapitre, nous avons abordé une vue globale des différentes notions permettant de comprendre l'importance de la sécurité informatique à l'heure actuelle. En effet, la sécurité informatique représente une problématique très importante à prendre en compte par toute entreprise qui désire disposer d'un ensemble d'outils et de méthodes qui lui permettent et assurent la gouvernance efficace de son système d'information. Ainsi plusieurs méthodes d'analyse des systèmes informatiques proposent des démarches afin de garantir une image pérenne aux entreprises intégrant les processus de sécurité dans la liste de leur préoccupation managériale.

Chapitre 2 : Etude du réseau existant dans l’entreprise 2int partners

2.1. Préambule

Une bonne compréhension de l'environnement informatique aide à déterminer la portée du projet,Il est essentiel de disposer d'informations précises sur l'infrastructure réseau physique et les problèmes qui ont une incidence sur nos serveurs.

En effet, ces informations affectent une grande partie des décisions que nous allons prendre dans le déploiement de la solution.

2.2. Présentation de l'entreprise 2INTPartners

2INT Partners est une société de prestation de service informatique et de formation. Elle est spécialisée dans le déploiement et l'installation de solutions réseau et la recherche d'une solution économique et robuste pour satisfaire la clientèle et répondre aux mieux aux besoins et aux exigences de ses clients.

2.3. Historique de l'entreprise

Créée en 2012, 2INT Partners débute comme une entreprise d'installation de solutions réseaux et serveurs. Avec le progrès technologique, l'entreprise tente de suivre l'évolution des besoins des utilisateurs afin d'innover en matière de solutions IT.

Parmi les objectifs recherchés par cette entreprise, nous pouvons citer :

- ✓ Innover afin de suivre l'évolution des besoins.
- ✓ Satisfaire la clientèle en privilégiant les besoins des clients.
- ✓ Fournir une assistance aux clients après qu'ils aient acquit un produit ou un service.

L'entreprise compte actuellement 24 salariés, dont 10 responsables des différents services.

2.4. Architecture du réseau existant

Nous ne pourrons pas proposer une solution de sécurité sans avoir étudié au préalable le réseau existant. A cet effet, nous avons étudiésle matériel physique et logique existant dans l'architecture du réseau 2INTPartners.

Lors de la première visite dans cette entreprise, nous avons relevé le réseau existant puis nous l'avons schématisé en utilisant le logiciel en ligne « creatly.com ».

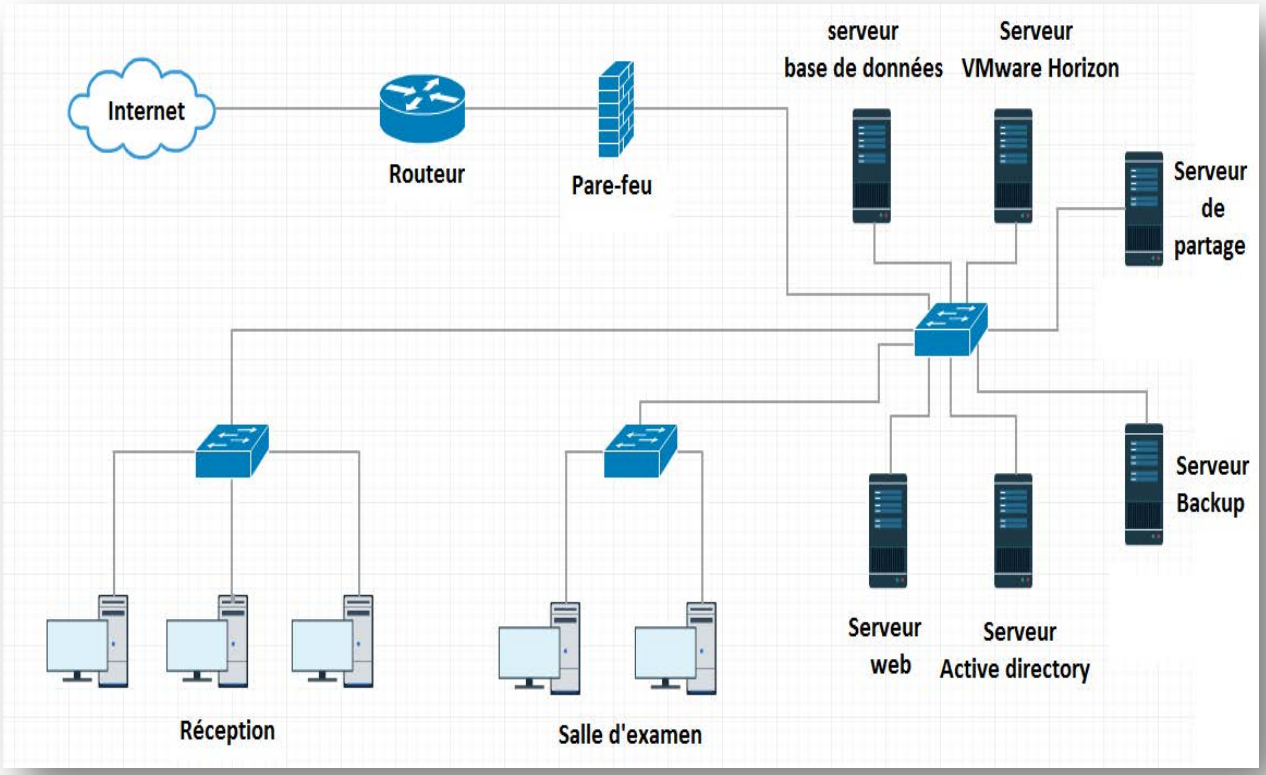

Fig.2.1. Architecture existante au sein de 2INT Partners.

Nous avons constatés quel'entreprise 2INT Partnerspossède :

- Trois salles contenant différents équipements :
  - Une salle de réception composée de trois ordinateurs qui contiennent les informations sur les étudiants (leurs coordonnés), les plannings, les notes des étudiants… etc.
  - Une salle d'examen composée de deux ordinateurs pour faire les tests d'évaluations.
  - Une salle contenant six serveurs.
- Trois Switch qui relient les différents ordinateurs.
- Un pare-feu qui permet de filtrer les paquets entrant et sortant vers le réseau Internet.
- Un routeur qui assure l'acheminement des paquets entre le réseau local et le réseau Internet.

D'après le cahier des charges du départ, nous nous sommes intéressés à la protection des deux serveurs ; celui de partage et le Backup.

Dans ce réseau, l'implémentation d'un serveur de fichier permet de simplifier la gestion des fichiers et l'échange de données entre les différents utilisateurs.De plus, un serveur de sauvegarde de données (Backup) est utilisé pour l'enregistrement automatique et régulier des données importantes partagées. Cela nous permet de récupérer ces données en cas d'une perte.

Cependant, ces deux serveurs font face à certaines vulnérabilités en termes de sécurité qui sont :

- Accès aux données de ces serveurs est possible même aux personnes non autorisées.
- Système d'exploitation Linuxutilisés comme serveurs objet d'intrusions.
- Données partagées non cryptées.

2.5. Equipements existant

L'architecteur du réseau de l'entreprise 2INTPartners se compose des équipements suivant :

- **Routeur :**est un équipement d'interconnexion de réseaux informatiques permettant d'assurer le routage des paquets entre deux réseaux ou plus afin de déterminer le chemin qu'un paquet de données va emprunter.

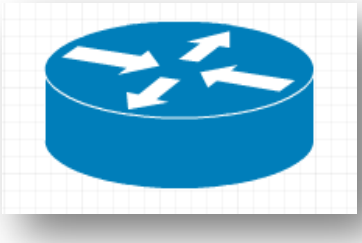

Fig.2.2. Représentation d'un routeur

- **Serveurs :** est un dispositif informatique matériel ou logiciel qui offre des services, à un ou plusieurs clients.

  Dans l'architecteur, il existe six serveurs différents dans un laboratoire et présentent comme suit :

  - **Serveur Web :** est un programme qui utilise le protocole HTTP pour fournir les fichiers qui constituent les pages Web que les utilisateurs ont demandés, via des requêtes transmises par les clients HTTP de leurs

ordinateurs. Des ordinateurs et des Appliance dédiés peuvent également jouer le rôle de serveurs Web.

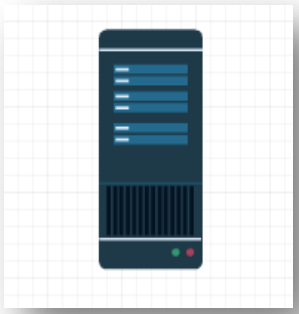

Fig.2.3.Représentation d'un serveur

- **Active Directory :**est un service d'annuaire créé par Microsoft en 1996, destiné à être installé sur les Windows Server. En stockant dans une base de données les renseignements relatifs aux ressources réseau d'un domaine, il a pour objectif premier de centraliser l'identification et l'authentification d'un réseau de postes Windows. Ses fonctions additionnelles permettent aux administrateurs de gérer efficacement une stratégie de groupe, ainsi que l'installation des logiciels et des mises à jour sur les stations du réseau.

- **Serveur VMware horizon** : est un ensemble de produits et de technologies conçus pour aider les administrateurs IT à fournir des postes de travail, des applications et des données, de manière sûre, sur différents types de terminaux.

- **Serveur base de données** : est un serveur qui permet de stocker ses propres bases de données, c'est-à-dire, les bases de données utilisées par ses composants ainsi que les bases de données créées par l'hébergement des sites Web, des clients et des applications Web.

- **Serveur Back up** : est un serveur de stockage pour une protection des données en continu, il permet une sauvegarde les données et assure une copie intégrale du serveur initial, tout en réduisant le risque de pertes de

données à quelques secondes ou quelques minutes au maximum. Tous les fichiers sont copiés même ceux qui restent ouverts lors de la sauvegarde.

- **Serveur de partage** : permet de partager des données à travers un réseau. Le terme désigne souvent l'ordinateur (serveur) hébergeant le service applicatif. Il possède généralement une grande quantité d'espace disque où sont déposés des fichiers.
- **Poste client :** les postes de travail sont orientés Windows et connectés au réseau avec un accès à internet.

Nombre	Rôle du poste	Composants
05	Poste de travail	CPU : Core i3 2.40GHZ Capacité du disque dur : 500 GO

Tableau 1 : Caractéristique des postes de travail

- **Switch** : désigne un commutateur réseau, équipement ou appareil qui permet l'interconnexion d'appareils communicants, terminaux, ordinateurs, serveurs, périphériques reliés à un même réseau physique.

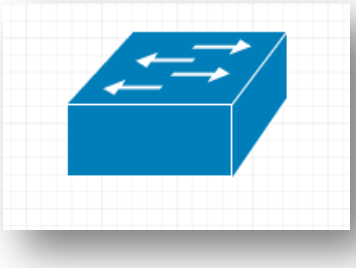

Fig.2.4. Représentation d'un switch.

- **Firewall :**est un outilconçu pour protéger les données d'un réseau et d'assurer la sécurité des informations internes au réseau local en filtrant les entrées et en contrôlant les sorties selon une procédure automatique bien établie.

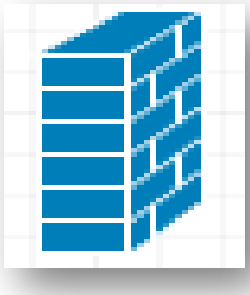

Fig.2.5. Représentation du firewall

Le réseau de l’entreprise 2INT Partners, est un réseau « fastethernet » commuté à 10/100Mbps.

Le tableau suivant désigne les équipements d’interconnexion utilisés dans l’architecture de l’entreprise 2INT Partners

Nombre	Types de Terminaux	Modèles
1	Modem et routeur	Huawei HG532e
1	Switch	CISCO catalyst 2950
2	Switch	D-Link DES-1008A

Tableau 2 : Liste des équipements d’interconnexion.

2.6. Applications installées

Les postes de travail sont équipés d'un système d'exploitation Windows 7 avec une suite bureautique Microsoft office 2007 professionnel. Par contre, les serveurs sont équipés du système d'exploitation Linux Debian 9.

Les applications installées sur les serveurs étudiés sont présentées dans le tableau suivant :

Applications	Descriptions
Owncloud	un logiciel libre offrant une plateforme de services de stockages et de partage de fichiers.
Duplicati	un logiciel de sauvegarde qui planifie et stocke une copie complète ou incrémentielle des fichiers à conserver.

Tableau 3 : Liste des applications.

2.7. Aspects de la sécurité existante

2.7.1. Sécurité physique :

La sécurité physique est un aspect fondamental de tout type de sécurité pour garantir l'intégrité, la confidentialité et la disponibilité des informations, protéger les données personnelles et professionnelles contre les attaques internes ou externes. Si quelqu'un réussit à accéder au système informatique de l'entreprise, il peut l'endommager ou même le détruire. Elle vise aussi à favoriser l'exploitation des équipements informatiques dans des conditions fonctionnelles optimales, de manière à bénéficier d'un maximum de performances durant un maximum de temps. [4]

Des mesures de sécurité ont été prises pour assurer la sécurité de l'infrastructure.

D'après les visites et les entretiens, nous avons constaté les faits suivants :

- Les ports USB sur les postes des utilisateurs ont été désactivés afin d'empêcher le vol d'informations et les infections liées aux virus.
- Le routeur et les Switch ont été placés dans une armoire fermée.

2.8.2. Sécurité logique :

Pour une sécurité logique, les moyens mis en place sont :

- Anti-virus Kaspersky est mis e en place sur chaque client connecté au réseau, un scan complet automatique est activé ainsi que les mises à jours sont programmées afin de détecter de nouveaux virus pour mieux protégé ses machines.
- Un pare-feu (firewall) est un logiciel ou un équipement permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communications autorisés sur ce réseau informatique. Il surveille et contrôle les applications et les flux de données (paquets).

Malgré que la sécurité mise en place afin d'éviter les intrusions, il existe toujours des vulnérabilités qui peuvent affecter le serveur de fichier et le serveur backup.

2.8. Critique de l'existant :

D'après nos analyses précédentes faites sur l'infrastructure, nous avons constaté quelques points faibles qui existent au sein du réseau :

- Absence de la sécurité physique au niveau de la salle contenant les différents serveurs.En effet, l'accès vers la salle est libre à toute personne (employés, étudiants, visiteurs,…etc.)
- Du fait que le système Linux est open source, des utilisateurs initiés peuvent modifier les paramètres de démarrage et le bios. En conséquence, ces utilisateurs pourront par la suite modifier les règles de sécurité des serveurs.

- Risque d'accès (localement et à distance) aux deux serveursétudiés par des personnes non autorisées.
- Malgré que les applications (Owncloud et duplicati) sont protégés par un mot de passe mais les données qui sont a l'intérieur sont lisible (ne sont pas chiffrées).
- Toute les machines cliente qui sont liées au réseau peuvent y'accéder aux deux serveurs.

2.9. Solutions proposées

Afin de remédier aux différentes failles de sécurité du réseau existant, nous proposons les solutions suivantes :

- Fermer la salle des serveurs avec une clef et ne distribuer cette clef qu'aux seules personnes autorisées.
- Sécuriser le mode mono-utilisateur de Linux.
- Sécuriser le boot loader en introduisant un mot de passe au démarrage de la machine.
- Sécuriser le BIOS pour bloquer l'accès, prévenant de toute modification. Cela fait par un mot de passe au démarrage de système d'exploitation.
- Sécuriser le serveur de fichier en attribuant les différentes règles de permission.
- Sécuriser l'accès à distance au serveur de fichiers.
- Crypter les données afin de rendre les informations indéchiffrables.
- Sécuriser les comptes utilisateurs par la sécurité des mots de passes ainsi que la sécurité des réseaux (sécurité SSH, configuration d'un TCP wrappers).

Pour une meilleure sécurité, nous allons appliquer toutes ces solutions citéespourproduire une sécurité optimalesur cette architecture.On ne peut pas choisir quelques solutions au détriment des autres.

2.10. Discussion

Nous avons effectué dans ce chapitre l'étude du réseau existant au sein de l’entreprise 2INT Partners. Cette étude s’est focalisée sur les différents équipements existant dans l’infrastructure de l’entreprise et les applications installées sur les serveurs backup et les serveurs de fichier. Ceci nous a permis de recenser les différentes failles sécuritaires de ce réseau afin de proposer une solution qui répond au cahier des charges initial.

Chapitre 3 : Implémentation de la solution

3.1. Préambule

Un système d'exploitation est un ensemble de programmes permettant l'utilisation des ressources matérielles d'un ou plusieurs ordinateurs. Il assure le démarrage de l'ordinateur et l'exécution des logiciels applicatifs. Il existe plusieurs systèmes d'exploitations : MS-DOS, Windows, GNU/Linux,…etc.

GNU/Linux est un système Unix open source complètement libre et performant, hautement configurable. Il est supporté par une grande communauté d'utilisateurs souvent prêts à aiderd'autres utilisateurs. Linux est réputé entre autres pour sa sécurité et pour ses mises à jour moins fréquentes que Windows[8].

La sécurisation de Linux est paradoxale : d'un côté, c'est un système qui peut être extrêmement hermétique et d'un autre côté, il est souvent vulnérable compte tenu des nombreuses possibilités de configuration offertes.

La solution que nous avons adoptée est basée d'une part sur le verrouillage de quelques configurations du système d'exploitation Linux et d'autre part sur la sécurité d'accès au serveur de fichier. A cet effet, nous avons effectués les tâches suivantes :

- Sécuriser le mode mono-utilisateur de Linux
- Sécuriserle boot loader de Linux.
- Verrouiller l'accès au bios,
- Crypter les données
- Sécuriser l'accès à distance

Dans ce chapitre, nous présenterons la solution mise en œuvre permettant de remédier à chaque faille trouvée lors de l'étude de l'existant

3.2. Sécuriser le mode mono-utilisateur de Linux

Le mode mono-utilisateur (Single user mode) est un mode de fonctionnement du système Linux qui fournit le moins de services possibles et une fonctionnalité minimale. Il est utile pour démarrer un ordinateur dont le système d'exploitation a été endommagé et il est utilisé afin d'effectuer certaines tâches de diagnostic et de réparation.Par conséquent, à l'aide de ce mode, un intrus pourra accéder à la racine de ce système d'exploitation (root).

Le serveur de fichier installé à l'école 2INT Partners utilise Linux comme système d'exploitation. Avant d'implémenter la solution de sécurité adaptée, nous allons verrouiller l'accès en mode mono-utilisateur. Pour cela, on va suivre les étapes présentées suivantes :

- Nous démarrons le système Linux puis nous allons appuyer sur lettre « e » dès l'affichage de la (figure 3.1)

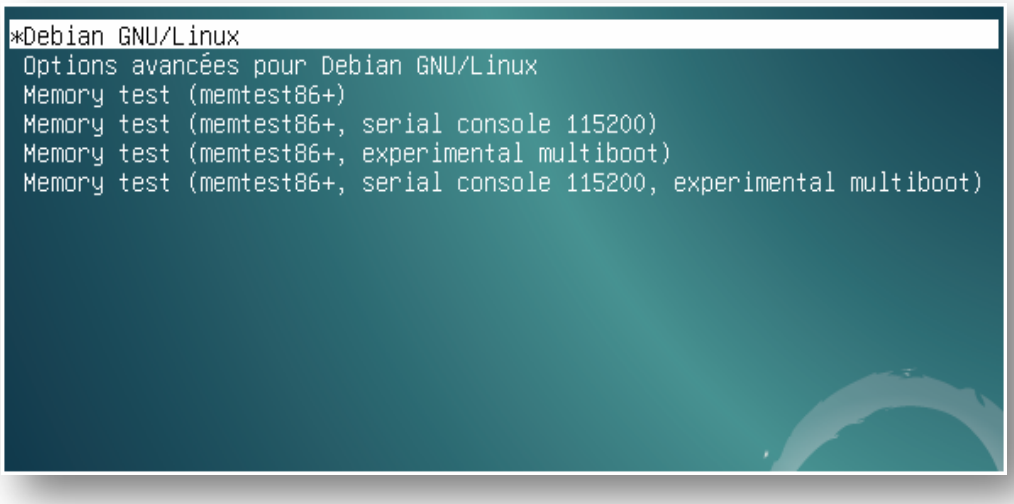

Fig.3.1 : Menu de boot.

- Ajout de la lettre « s » à la fin de la ligne "linux /boot/vmlinuz", puis Ctrl-x pour démarrer le système d'exploitation.

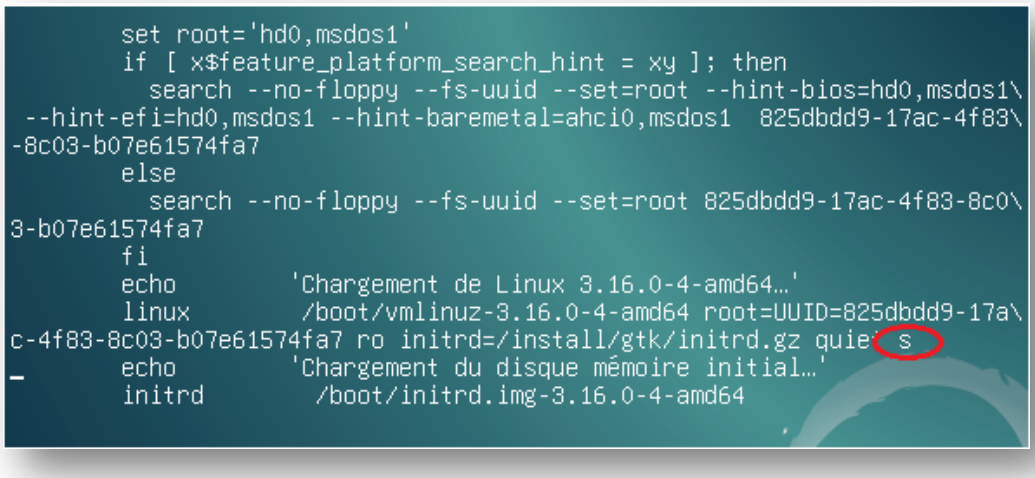

Fig.3.2 : Ajout de la lettre « s » à la ligne.

- Un mot de passe nous ademandé comme le montre la figure ci-dessous.

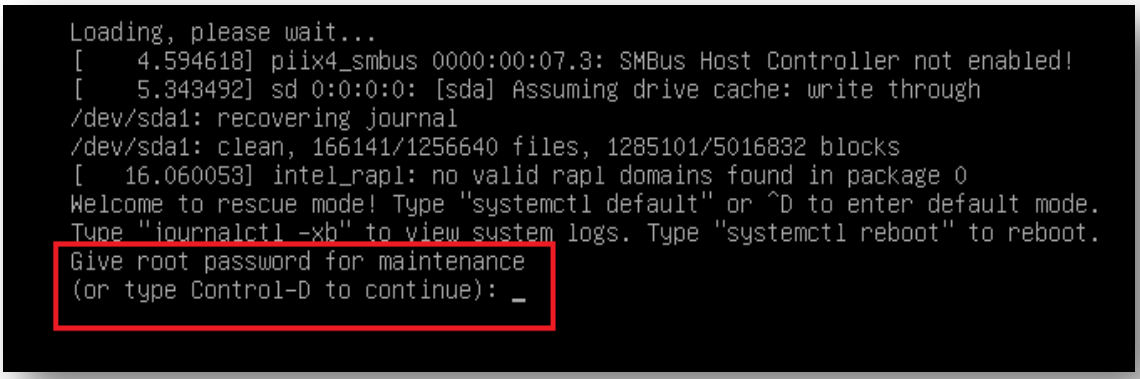

Fig.3.3 : demande de saisir un mot de passe.

Dans cette partie, on constate que dés qu'on essaie d'accéder à la machine en single user mode,un mot de passe nous ait demandé, donc ce mode est déjàverrouillé par l'administrateur du réseau.

3.3. Sécuriser le boot loader

Le « Boot loader »(gestionnaire de démarrage) est un programme qui charge et démarre leprocessus de démarrage d'un système d'exploitation ou du système informatique. Il permet de charger le système d'exploitation dans la mémoire de l'ordinateur lors de démarrage ou de l'amorçage d'un ordinateur.

Nous nousintéressonsà une autre failleque l'on trouve au niveau du logiciel d'amorçage GRUB. Cette faille repose sur la possibilité de contourner le fonctionnement normal du gestionnaire d'amorçage.

3.3.1. Présentation de la faille

Cette faille ressemble à la faille précédente.Toutefois, nous allons rajouter à la ligne qu'on a déjà identifiés la commande init=/bin/bash a l'apparition du menu de démarrage comme le monte la fig.3.4, cela on passant par trois étapes :

Etape 1 :nous allons appuyer sur « e » à l'affichage de la fenêtre présentéepar la fig.3.4

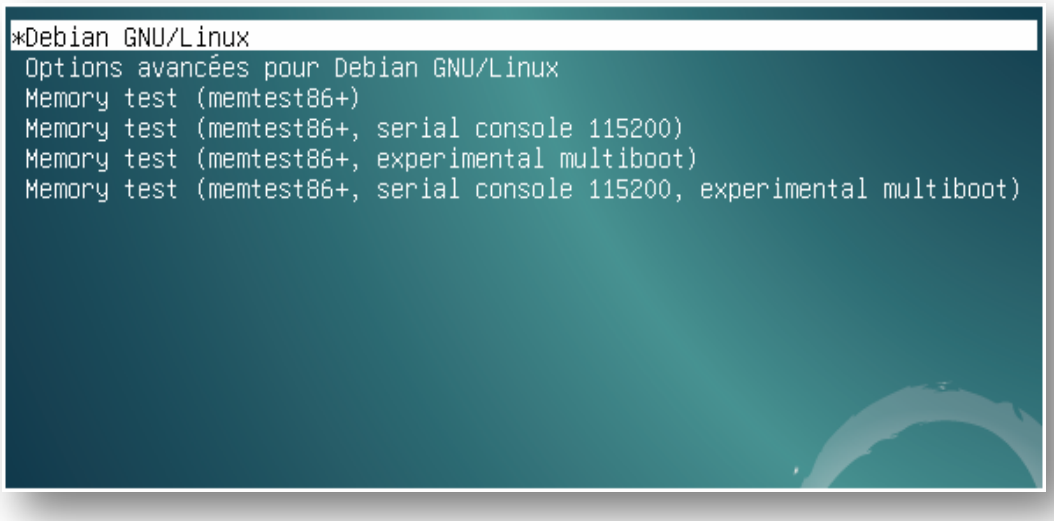

Fig.3.4 : Menu BOOT

Etape 2 : identification de la ligne "linux /boot/vmlinuz", et nous saisissons à la fin de cette dernière la commande « init=/bin/bash ».

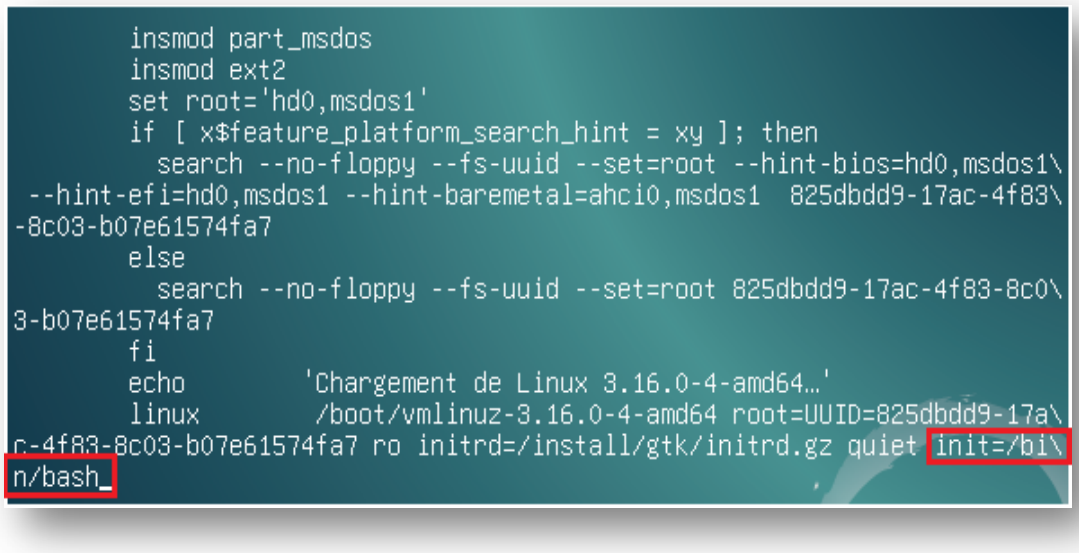

Fig.3.5 : Edition du GRUB et ajout de la commande

Etape 3 : On tape sur les touchesCtrl+x pour démarrer le système d'exploitation, la machine accède au root comme le montre la fig.3.6

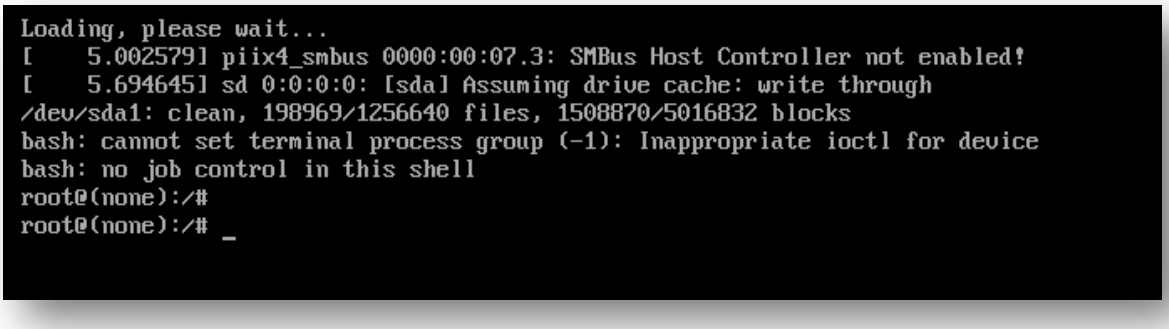

Fig.3.6 : Accès au root.

Cette figure indique que le boot loader n'est pas sécurisé et qu'il est accessible à toute personne possédant des notions sur Linux. L'accès au root par une personne malintentionnée pourra conduire à modifier la configuration initiale du serveur de fichier.

3.3.2. Solution proposée

Il est possible de remédier à cette faille en définissant un mot de passe pour l'accès au menu «GRUB »,selon les étapes ci-dessous :

Etape 1 : accéder au GRUB et afficher son contenu.

Nous choisissons le fichier « 40_custom » parce quece fichier a la caractéristique de ne pas changer aprèsles mises àjour.

Fig.3.7 : accéder au GRUB.

Etape 2 : Nous éditons le fichier « 40_custom » et nous ajoutonsla ligne login et mot de passe.

```
#!/bin/sh
exec tail -n +3 $0
# This file provides an easy way to add custom menu entries.  Simply type the
# menu entries you want to add after this comment.  Be careful not to change
# the 'exec tail' line above.
set superusers="2int"
password 2int root
```

Fig.3.8 : Ajout de nom d'utilisateur et mot de passe au fichier « 40_custom »

Etape 3:Nous mettons à jour le GRUB

```
root@debian:/etc/grub.d# update-grub
Création du fichier de configuration GRUB…
Found background image: /usr/share/images/desktop-base/desktop-grub.png
Image Linux trouvée : /boot/vmlinuz-3.16.0-4-amd64
Image mémoire initiale trouvée : /boot/initrd.img-3.16.0-4-amd64
Found memtest86+ image: /boot/memtest86+.bin
Found memtest86+ multiboot image: /boot/memtest86+_multiboot.bin
fait
```

Fig.3.9 : Mise à jour du GRUB

Dès le nouveau démarrage de la machine, le GRUB demande de saisirun nom utilisateur et un mot de passe.

```
Entrez le nom d'utilisateur :
2int
Entrez le mot de passe :
```

Fig.3.10 : Demande de nom d'utilisateur et mot de passe

3.3.3. Cryptage du mot de passe

Afin de sécuriser le nom d'utilisateur et le mot de passe définis précédemment, nous allons les crypter. En effet, même en cas d'interception, ces informations sont illisibles. Pour cela, à l'aidede la commande « grub-mkpasswd-pbkdf2 », nous allons saisir le mot de passe qu'on veut crypter deux fois de suite.

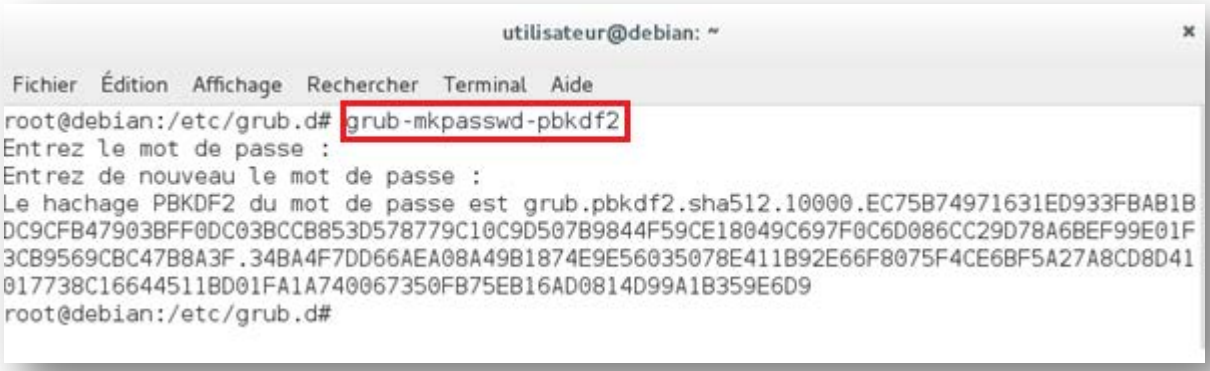

Fig.3.11 : Affichage du mot de passe crypté

Nous rééditons le fichier « 40_custom » pour y coller le mot de passe crypté.

Fig.3.12 : Ajout du mot de passe crypté au fichier « 40_custom »

La figure 3.12 nous montre que le mot de passe est crypté par l'algorithme de hackagesha512.

Au démarrage de notre ordinateur, pour des questions de sécurité, Linux nous demande toujours un mot de passe utilisateur pour pouvoir s'ouvrir.

On a constaté une autre faille qui est due à la possibilité d'accéder à notre machine physiquement et de désactiver le mot de passe du GRUB à travers un « CD-ROM » de Linux.

3.4. Désactiverle mot de passe à partir du Bios

Le Bios est un ensemble de fonctions, contenu dans la mémoire morte (ROM) de la carte mère d'un ordinateur, lui permettant d'effectuer des opérations de base lors de sa mise sous tension.

3.4.1. Présentation de la faille

Les figures ci-dessous montrent les étapes à suivre pour désactiver le mot de passe du GRUB à travers un « CD-ROM ». Cette faille permet d'accédé à la racine de linux a partir de Bios, pour le faire, des étapes à suivre sont présentées sous l'ordre suivant :

- Accéder au BIOS
- Sélectionner le menu boot et choisir « CD-ROM » comme première source du système d'exploitation puis sauvegarder avec « F10 »

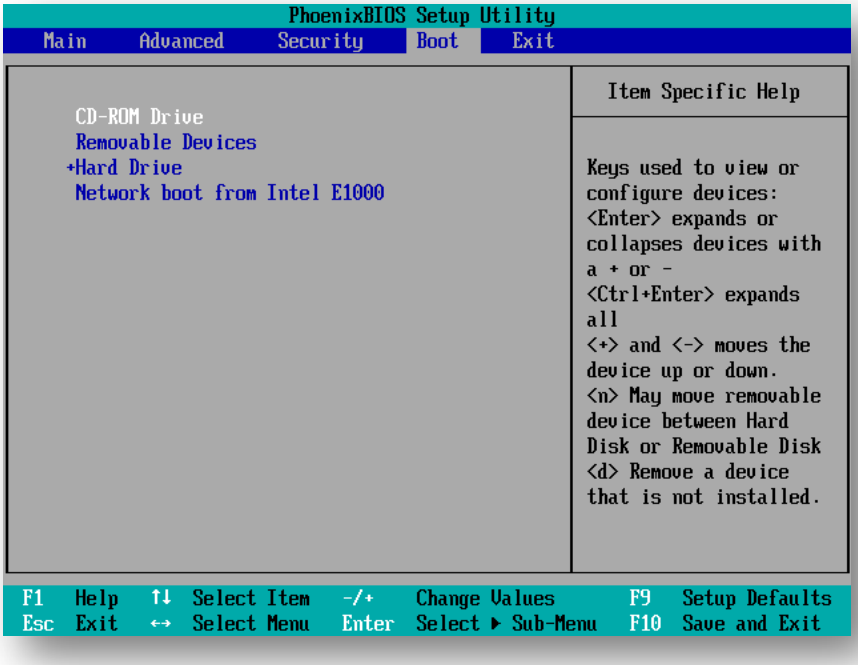

Fig.3.13 : Choisir « boot » et « CD-ROM ».

- Live : Au démarrage du boot menu, un menu apparait comme le montre la Fig.3.14

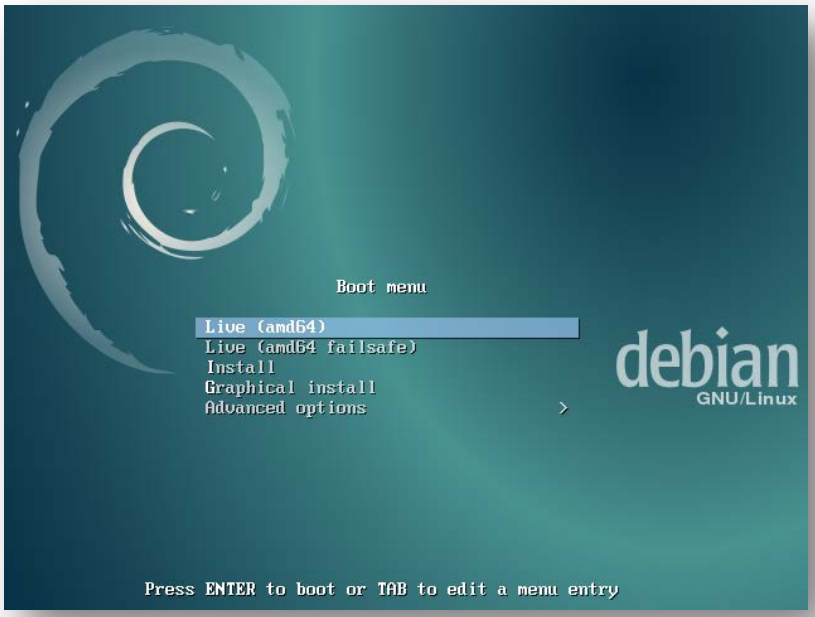

Fig.3.14 : Menu de Boot

Ensuite, Nous allons exécuter les commandes suivantes sur le terminal

- accéder au terminal en cliquant « activité »

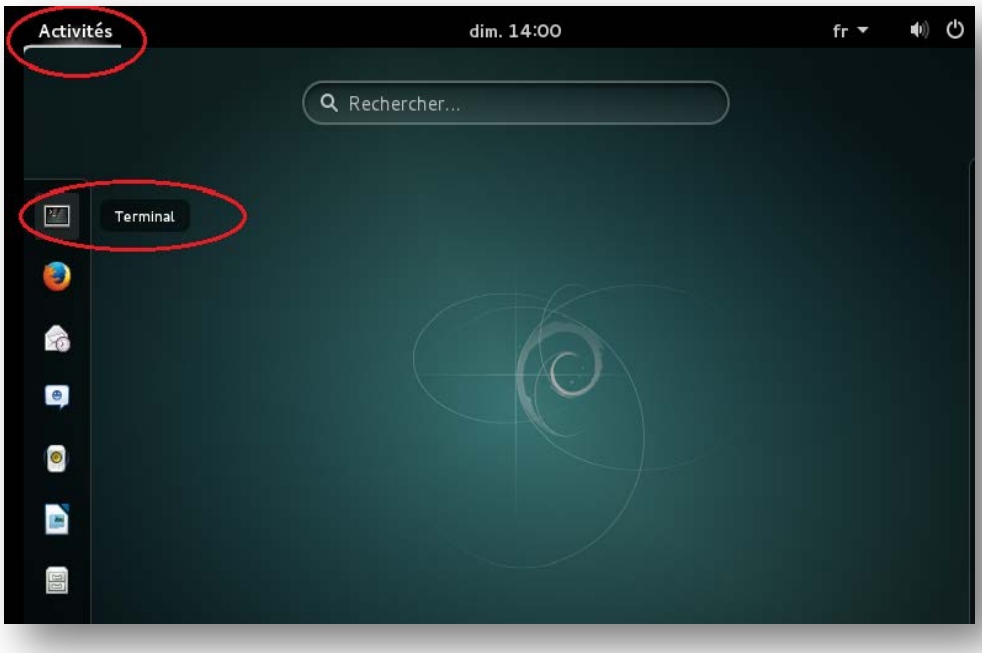

Fig.3.15 : Les étapes pour accéder au Terminal

Sur la fenêtre du terminal, nous allons saisir les commandes suivantes :

- Sudo –i : Cette commande permet d'accéder au root

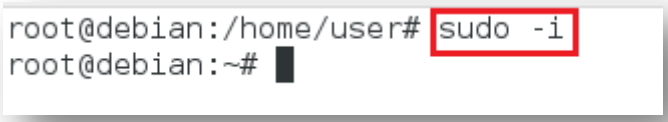

Fig.3.16 : Accès au root Debian

- Montage de la partition : Nous allons monter les partitions del'installation de Linux existantes avec la commande suivante

Fig.3.17 : Montage de la partition linux existante.

- Accéder a la partition monté « mnt »

Fig.3.18 : Lire le la partition monté

- Accéder aux fichiers du GRUB

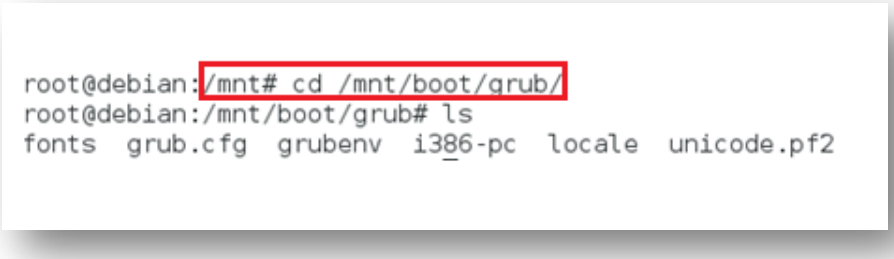

Fig.3.19: Accéder au GRUB de la partition montée

- Editer le fichier « grub.cfg »

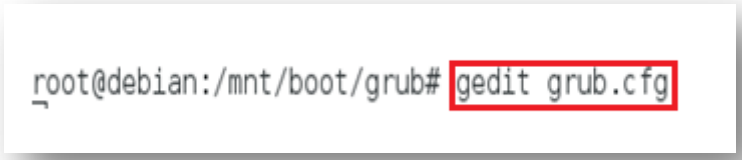

Fig.3.20: Edition de fichier « grub.cfg ».

- Ajouter « # » au nom d'utilisateur et mot de passe pour les remettre comme commentaires, du coup désactiver le mon d'utilisateur et le mot de passe

Fig.3.21: Modification de contenu du fichier

- Démontage de la partition

Fig.3.22 : Démontage de la partition

- Redémarrage la machine

Une fois la machine redémarrée, l'accès se fait sans mot de passe. Ce qui constitue une faille qu'on doit éliminer.La seul solution possible est de sécurisé le Bios d'une manière à définir un accès unique pour l'administrateur.

3.4.2. Sécuriser le BIOS

Pour définir ce mot de passe, il faut redémarrer la machine et accéder à l'espace de configuration du BIOS.

- Sélectionné le menu « Security » et entrer un mot de passe.

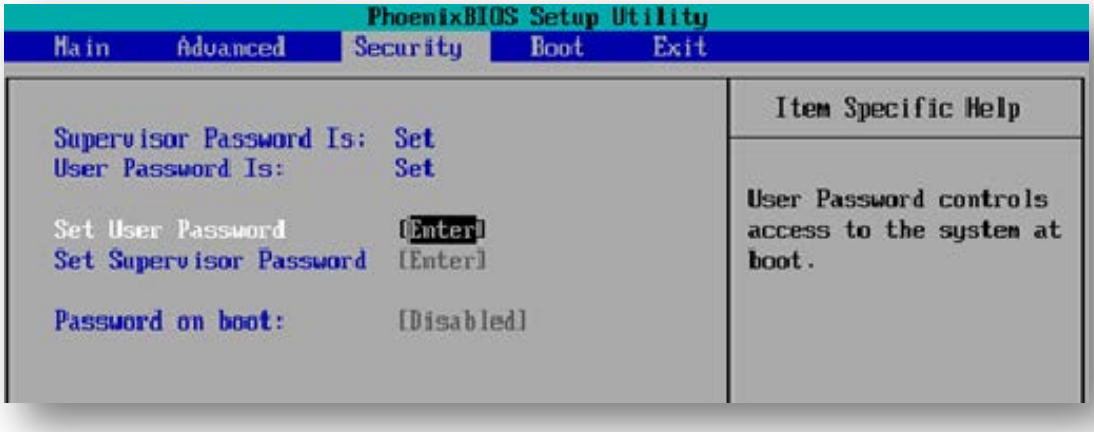

Fig.2.23 : Création du mot de passe

- Ce mot de passe est demandé pour accéder au BIOS.

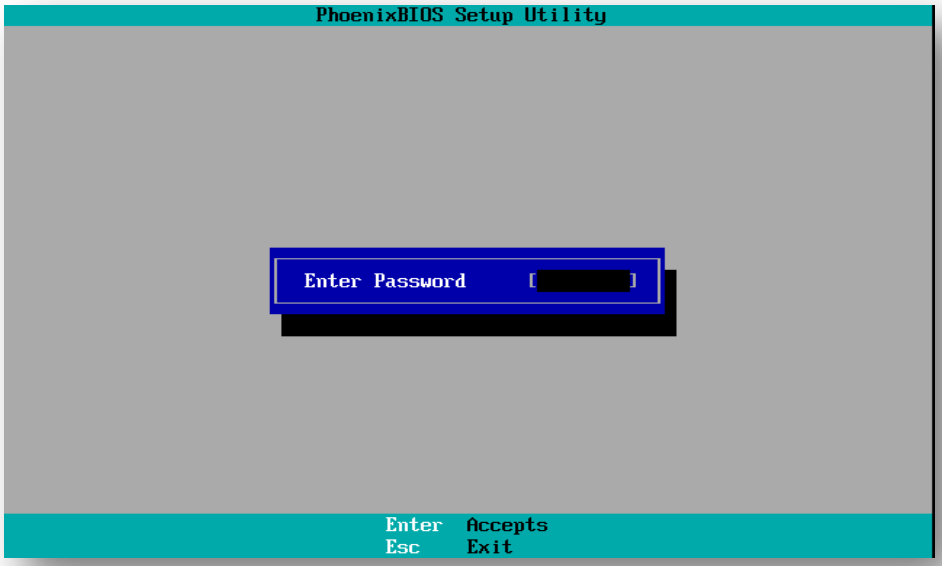

Fig.3.24: Saisie du mot de passe BIOS

Les mots de passes BIOS et Boot loader permettent une sécurité appréciable afin d'empêcher toute personne non autorisée a y'accéder au root.

3.5. Cryptage de données

Le cryptage de données est un processus informatique qui rend les informations indéchiffrables. Cela permet de protéger les données d'un utilisateur contre les lectures et les utilisations non autorisées.

Afin de protéger au mieux nos données personnelles, il peut être nécessaire de chiffrer nos partitions utilisateurs, En effet, si via le système il est impossible d'accéder aux fichiers qui ne nous appartiennent pas, nous allons tenter de rendre le disque dur illisible pour toute personne non autorisée en créant un espace dans le disque qu'on va monter comme un disque virtuel dans le but de crypté juste l'espace crée au lieu de crypté tout le disque, cette partition sert aux utilisateurs.

L'objectif principale visé par cette démarche est de crypté toutes les données envoyer par les utilisateurs sur le site et les traiter et stocker en toute sécurité en préservant leur confidentialité et intégrité.

Le schéma présenté dans la fig.3.25nous montre les étapes de cette démarche.

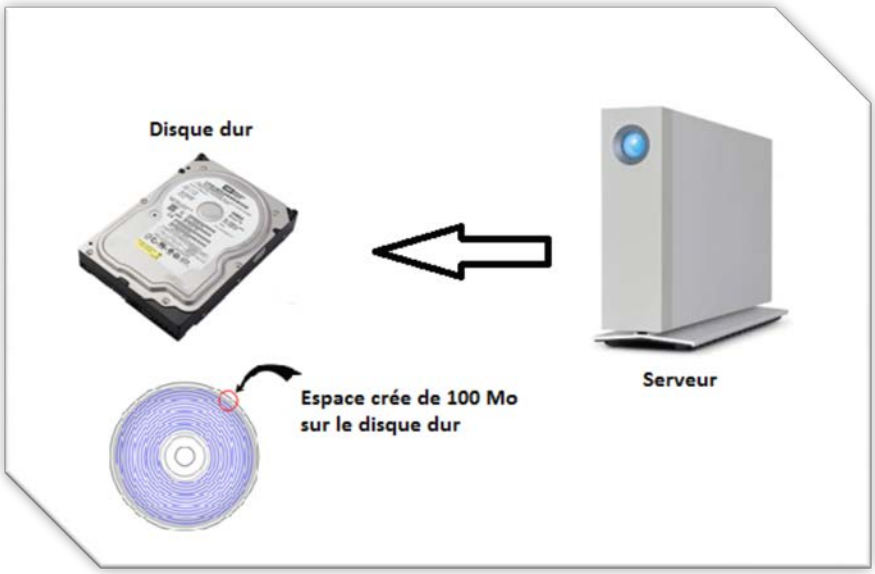

Fig.3.25 : Schéma de création d'un espace sur le disque.

Pour procéder à cette démarche, nous allons suivre certaines étapes :

Etape 1 : Installation de CryptSetup

Cryptsetupest un logiciel qui permet de chiffrer les partitions utilisateurs

```
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
belaid@debian:~$ su
Mot de passe :
root@debian:/home/belaid# apt-get install cryptsetup
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
```

Fig.3.26 : Installation de Cryptsetup.

« LUKS » permet de chiffrer l'intégralité d'un disque de telle sorte que celui-ci soit utilisable sur d'autres plates-formes et distributions de Linux. Il supporte des mots de passe multiples, afin que plusieurs utilisateurs soient en mesure de déchiffrer le même volume sans partager leur mot de passe.

Etape 2 : Création d'un espace sur le disque

Nous allons crée un espace « data.img » de 100 Mo sur le disque avec la commande suivante :

```
root@debian:/home/belaid# sudo fallocate -l 100M data.img
```

Fig.3.27 : Création d'un espace sur le disque

Etape 3 : Crée 100 cases vide de 1Mo sur l'espace crée :

```
root@debian:/home/belaid# sudo dd if=/dev/urandom of=/data/data.img bs=1M count=100
```

Fig.3.28 : Répartition de l'espace crée

Etape 4 : Remplir tout l'espace avec des caractères aléatoire

La commande « strings » est une commande UNIX qui permet de sortir sur la console les caractères affichables d'un fichier ou d'un flux.

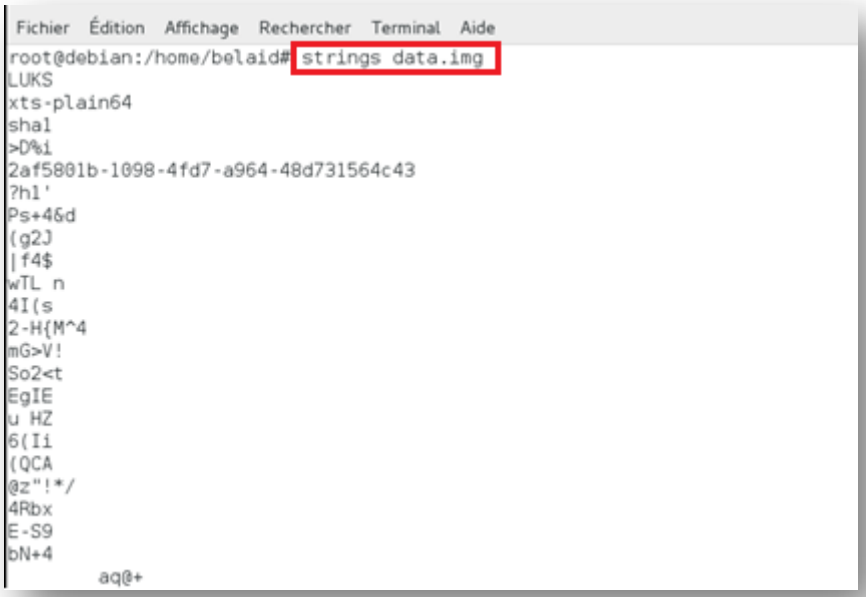

Fig.3.29 : Remplissage de l'espace par des caractères

Etape 5 : Nous allons formater le disque.

Cela se fait avec la commande « cryptsetupluksFormat ». Cette commande est pour objectif de formater la partition au type « LUKS ». Une confirmation est demandée. Inscrire « YES », l'outil demande une clé de chiffrement.

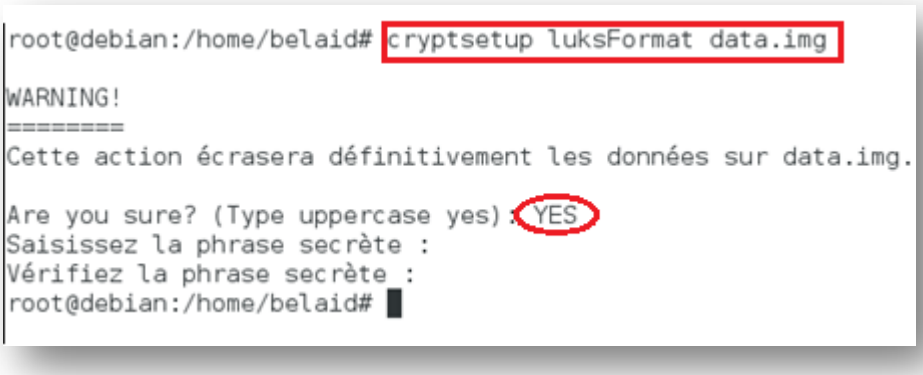

Fig.3.30 : Chiffrement de l'espace crée sur le disque

A l'exécution de cette commande, Nous allons introduire un mot de passe (clé de chiffrement) pour crypter le disque.

Etape 6 : ouvrir le disque (décrypter le disque), saisir le mot de passe qui est la clé de décryptage

La commande « cryptsetupluksOpen » permet l'ouverture de la partition chiffrée.

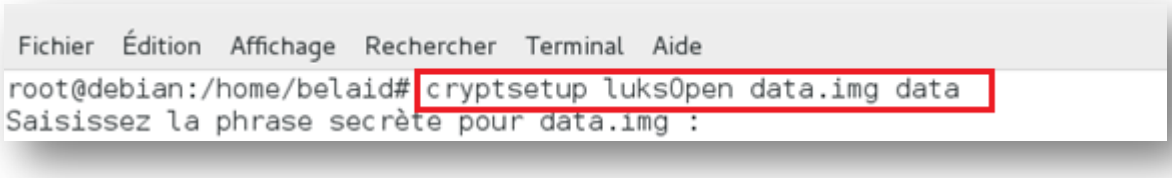

Fig.3.31: ouverture de la partition chiffrée

Etape 7 : création d'un système fichier pour lire toutes les données contenants dans le dossier « data »

La commande « mkfs » permet de créer un système de fichiers EXT4.

EXT4 est un système de fichiers destiné aux systèmes basés sur Linux, il peut gérer les volumes de grandes tailles. Sa fonctionnalité majeure est l'allocation par « extent » qui permet la pré-allocation d'une zone contiguë pour un fichier.

Ce système modifié les structures de données importantes de système de fichiers telles que celles destinées à stocker les données du fichier. Le résultat est un système de fichiers avec une conception améliorée, de meilleures performances, une fiabilité et des fonctionnalités.

La commande présente dans la fig.3.32 montre la création de système de fichiers EXT4

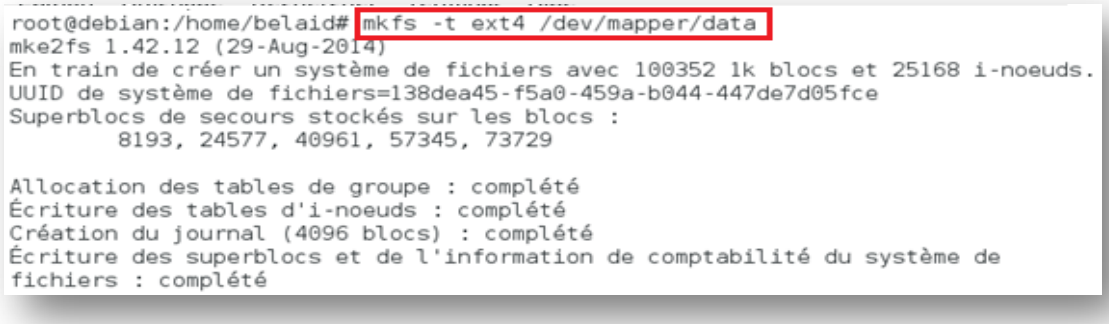

Fig.3.32 : Création d'un système fichier EXT4

Etape 8 : Montage du disquechiffré

La commande « mount » permet de monter un système de fichier (partition, lecteur de disquettes ou second disque dur).

```
root@debian:/home/belaid# mount /dev/mapper/data /data
root@debian:/home/belaid#
```

Fig.3.33 : Montage du disque chiffré

Après avoir crypté l'espace crée, nous allons l'ouvrir avec « gedit data.img »

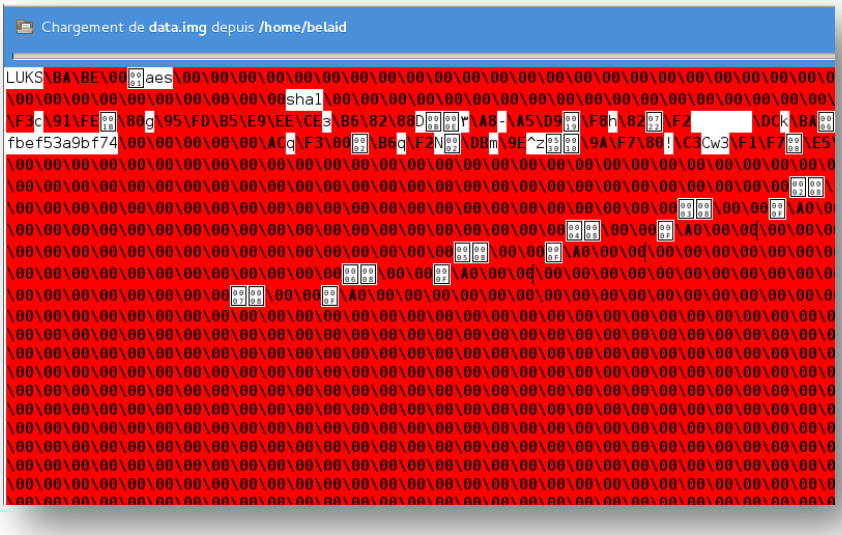

Fig3.35 : L'espace crypté.

D'après la **fig 3.35**, on constate que les données contenants dans le fichier « data.img » sont chiffrés.

3.6. La sécurité de l'accès à distance

L'accès à distance c'est une méthode qui permet, depuis un ordinateur éloigné et sans limite théorique de distance, de prendre le contrôle d'un autre ordinateur en affichant l'écran de celui-ci et en manipulant les fonctions correspondant au clavier et à la souris. Cet accès peut être effectué vers des postes de travail ou des serveurs informatiques en fonction des possibilités du logiciel utilisé.

Dans cette partie, nous allons étudier l'accès à distance au serveur en cas de panne de ce dernier en installant le service « SSH ».

3.6.1. Installation de service SSH :

SSH (Secure Socket Shell), est un protocole réseau qui permet aux administrateurs d'accéder à distance à un ordinateur, en toute sécurité. Il désigne également l'ensemble des utilitaires qui mettent en œuvre le protocole. Ce dernier assure une authentification forte et des communications de données chiffrées sécurisées entre deux ordinateurs connectés sur un réseau [7].

Nous allons utiliser le programme « OpenSSH », qui est la version libre du client et du serveur SSH.

Installer un serveur SSH permet aux utilisateurs d'accéder au système à distance.

- **Mode de fonctionnement de SSH**

L'établissement du dialogue entre le client et le serveur suit un protocole particulier :

- établissement d'une couche transport sécurisée
- chiffrement des données à l'aide de clefs symétriques pendant la transaction

Le client peut s'authentifier en toute sécurité, et accéder aux applications conformes aux spécifications du protocole.

Pour installer ce service, on utilise la commande suivante :

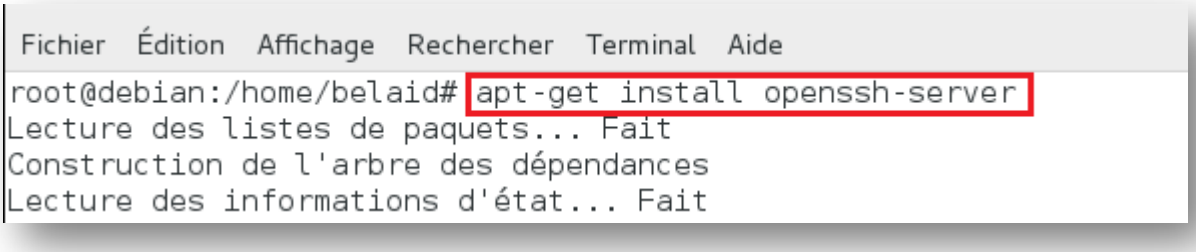

Fig.3.35 : Installation de service SSH

A cet effet, nous allons télécharger un logiciel qui permet la connexion à distance.

3.6.2. Logiciel de connexion à distance

« PUTTY » qui est un programme permettant de se connecter à distance à des serveurs en utilisant le protocole SSH.

Fig.3.36 : Logiciel PUTTY

Pour effectuer cette connexion, nous allons pouvoir suivre certaines étapes présentées comme suites :

- **Etape 1** : Avoir l'adresse IP de la machine virtuel

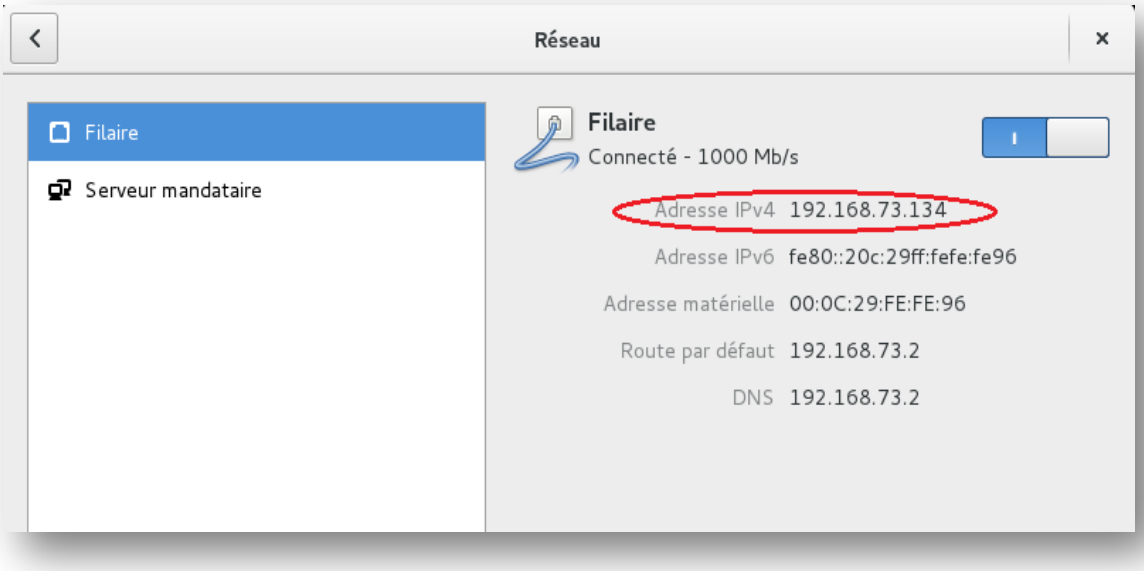

Fig.3.37 : Adresse IP de la machine virtuel

- **Etape 2** : Entrer l'adresse IP de la machine virtuel dans la configurationde logiciel « PUTTY » et choisir de port 22 par défaut

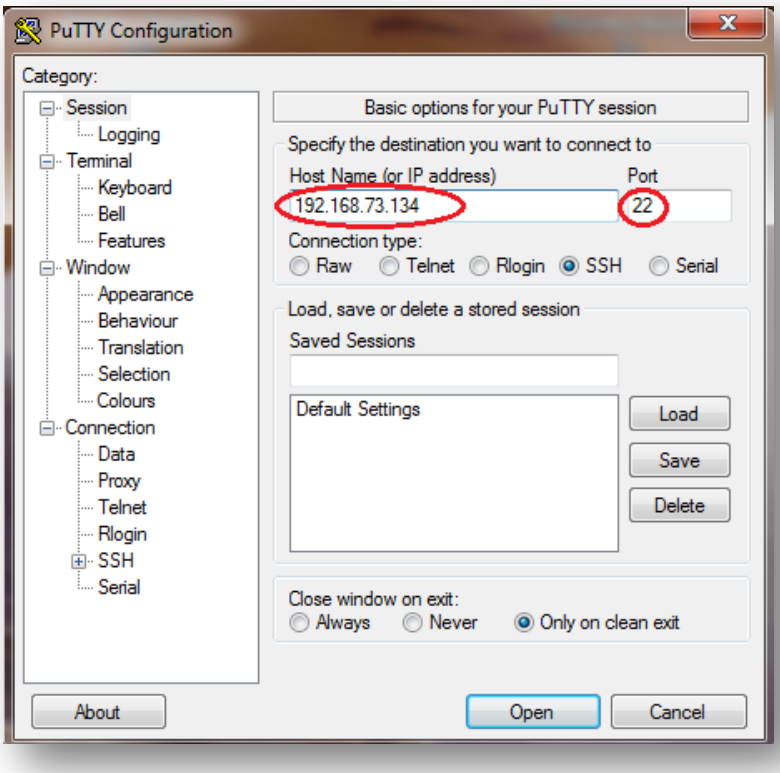

Fig.3.38 : Configuration de « PUTTY »

- **Etape 3** : Après avoir accorder une clé de chiffrement, on doit saisir un login et le mot de passe de serveur

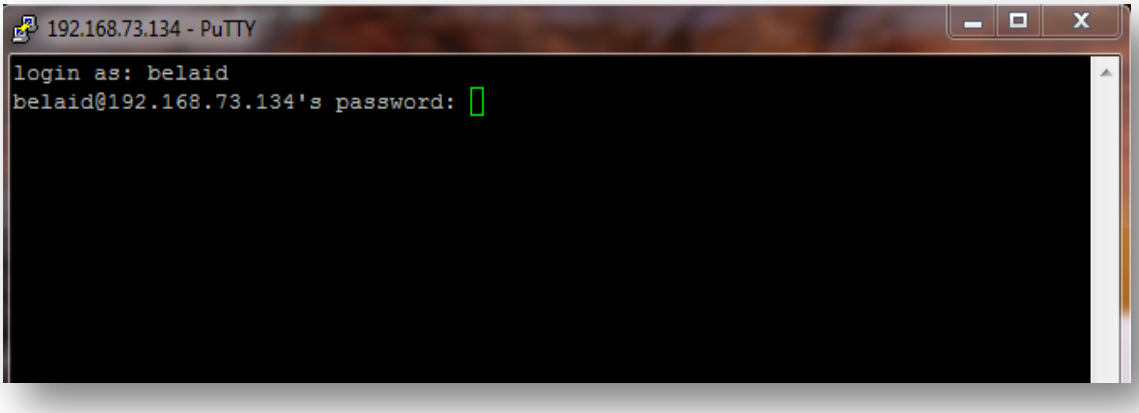

Fig.3.39: Accès au logiciel « PUTTY »

- **Etape 4** : Une fois entrer le login et le mot de passe, nous avons l'accès au rootde serveur à partir de logiciel « PUTTY »

Fig.3.40 : Accès au root à partir de logiciel « PUTTY »

Dans cet accès, on ne peut pas éditer directement un fichier parce que ce n'est pas un accès graphique, par contre c'est un accès console. Pour cela, on doit utiliser la commande « VI » au lieu de « gedit ».

Le problème qui se pose maintenant, c'est que le service SSH utilise le « port 22 » par défaut ce qui le rend facile a détecté. Pour une mesure de sécurité, nous allons changer ce port par un autre plus difficile à détecter

A cet effet, on doit modifier la configuration de fichier sshd comme suit :

- Editer le fichier sshd par la commande suivante

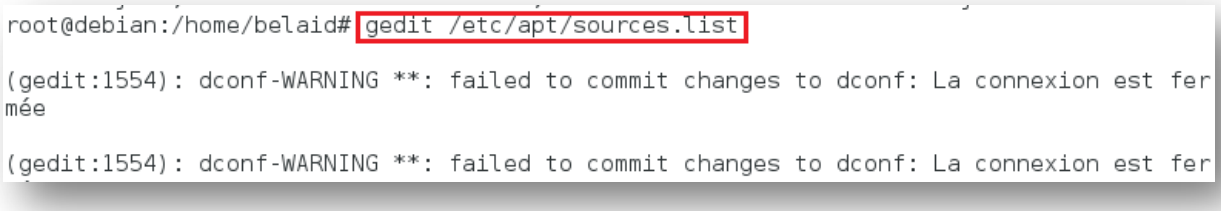

Fig.3.41: Edition du fichier sshd

- Modifier le « port 22 » dans le fichier de configuration de sshd

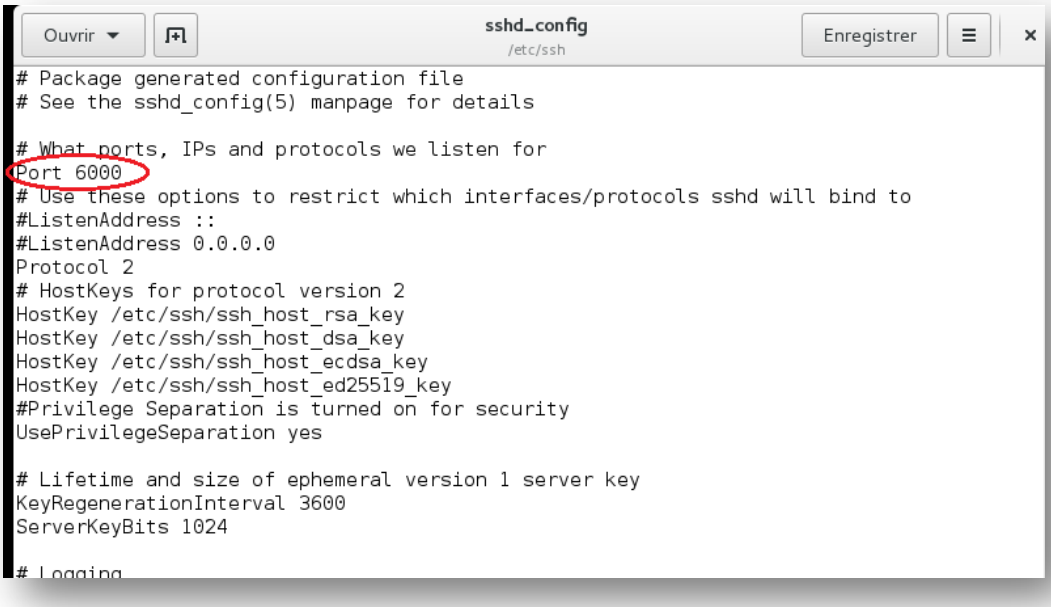

Fig.3.42: Modification du « port 22 » par « port 6000 »

- Redémarrer le service sshdavec la commande suivante

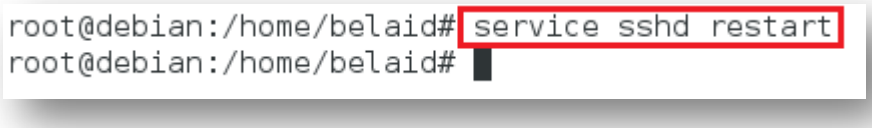

Fig.3.43 : Redémarrage de service sshd

- Après la modification, nous allons accéder au logiciel « PUTTY » avec l'adresse de la machine en gardant le port par défaut.

La **fig.3.44** montre que l'accès est refusé

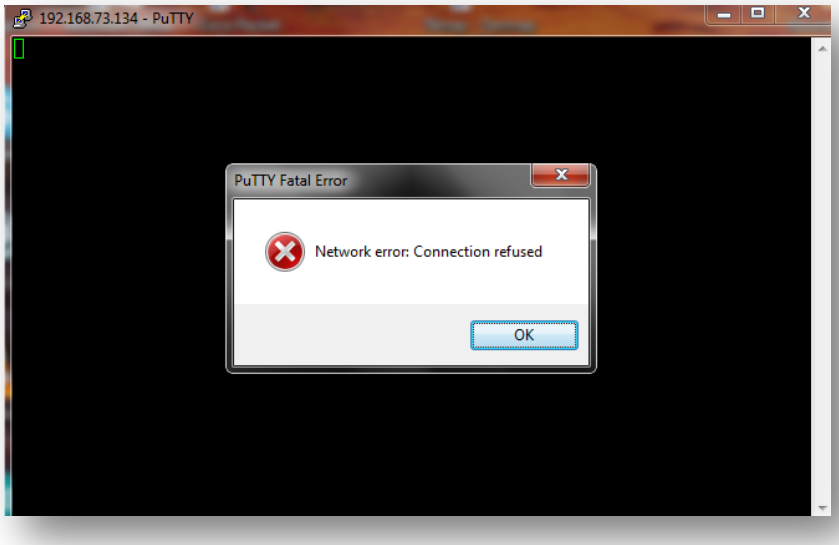

Fig.3.44 : Message d'erreur

- La même chose avec l'étape précédente mais au lieu de « port 22 » on va mettre le « port 6000 » qu'on vient de modifier.

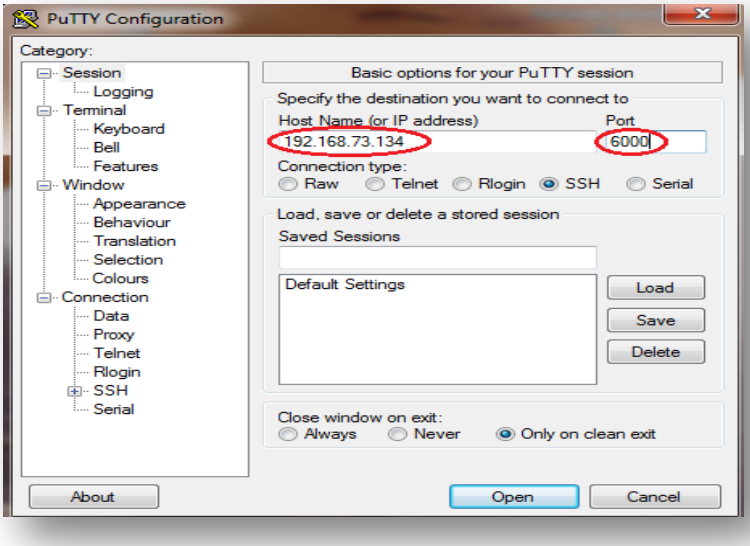

Fig.3.45 : Configuration de logiciel « PUTTY »

En cliquant sur « Open », là on a l'accès à l'utilisateur en saisissant le login et le mot de passe, après avoir accepté la clé de chiffrement

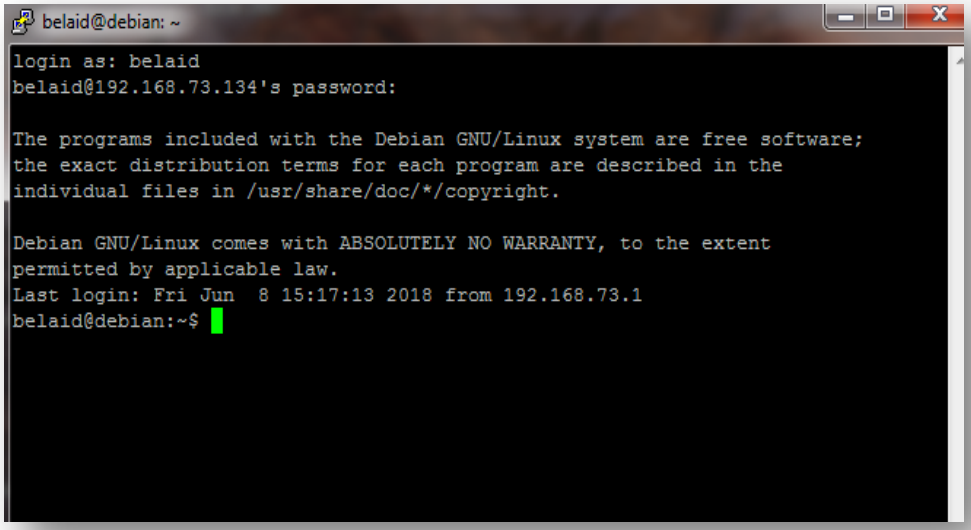

Fig.3.46: Console root en logiciel « PUTTY »

3.7. TCP wrappers

Le TCP wrappers est un outil de sécurité réseau qui permet de contrôler les accès, les tentatives de connexion sur une machine donnée. Il permet à tout instant de savoir qui essaie d'accéder sur un ordinateur mais également de filtrer les accès.

Soit ordinateurs client connecté a un serveur via un Switch et un TCP wrapper qui consulte l'adresse IP de serveur dans les ordinateurs, si il le trouve la connexion sera accordé (allow), si le contraire la connexion sera bloquer (deny).

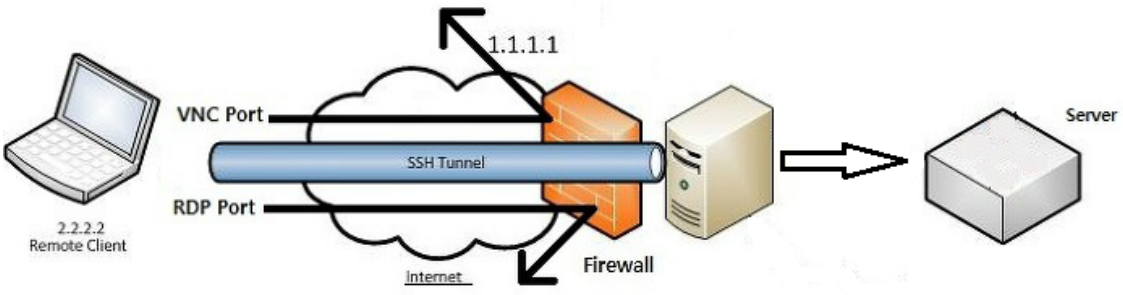

Fig.3.47 : Schéma de fonctionnement de TCPwrapper.

Le TCP est déjà mis en place dans le serveur, il est juste un fichier à remplir dans le serveur.

- Pour une meilleure sécurité, nous allons installer un logiciel « nmap » qui permet de scanner les ports

Dans ce logiciel, nous allons entrer l'adresse IP de serveur et quick scan pour un scan rapide puis on clique sur la touche scan pour commencer le scanner

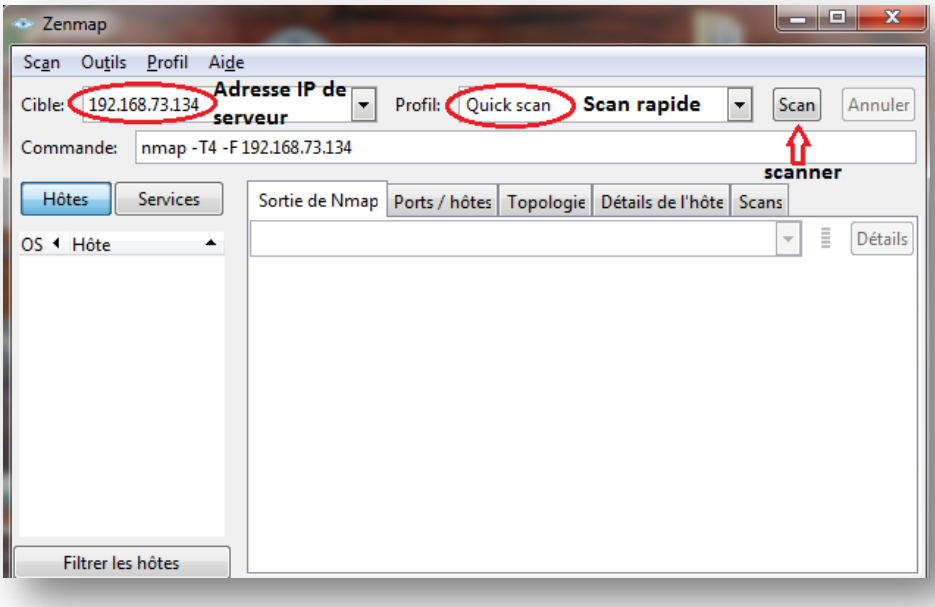

Fig.3.48 :Démarrage du scan

Dans la figure suivante, après le scan il affiche l'adresse Mac de la cible et le port scanné.

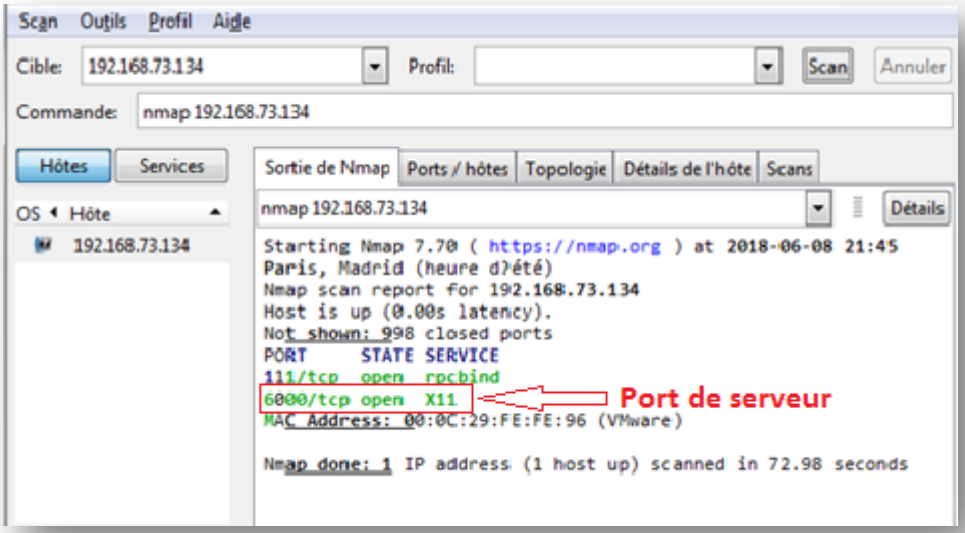

Fig.3.49 : Scan de la cible

- Pour bloquer tout les services pour tout les clients, nous allons configurer le TCP wrapper en éditons le fichier « hosts.deny » avec la commande suivante :

```
root@debian:/home/belaid# gedit /etc/hosts.deny
```

Une fois que le fichier est ouvert, nous allons ajouter au contenu de ce fichier la ligne présentée dans la figure suivante :

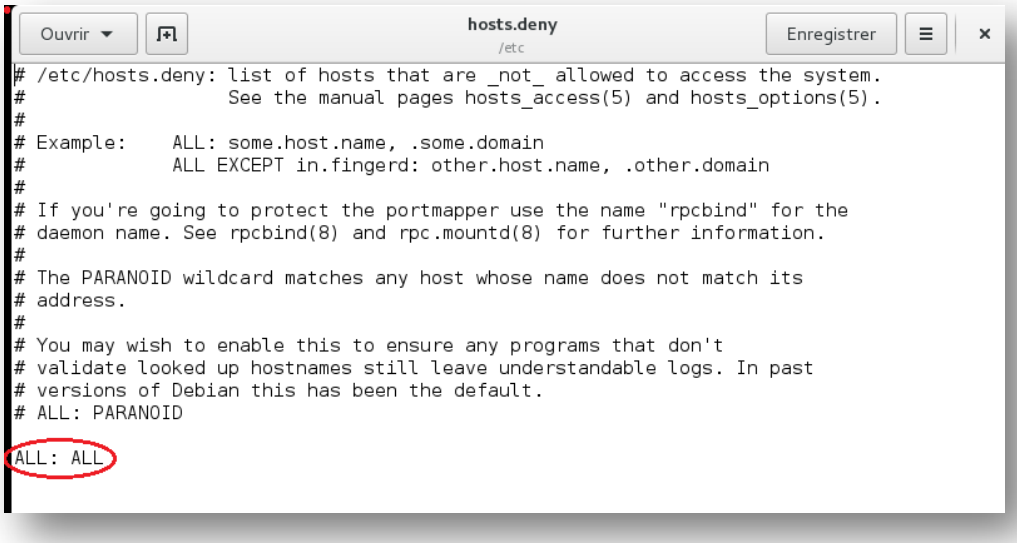

Fig.3.50: fichier « hosts.deny »

Maintenant, nous allons reconnecter au logiciel « PUTTY » avec l'adresse de serveur et le port 6000 pour vérifier l'accès. L'accès est refuser, cela revient à l'étape précédente

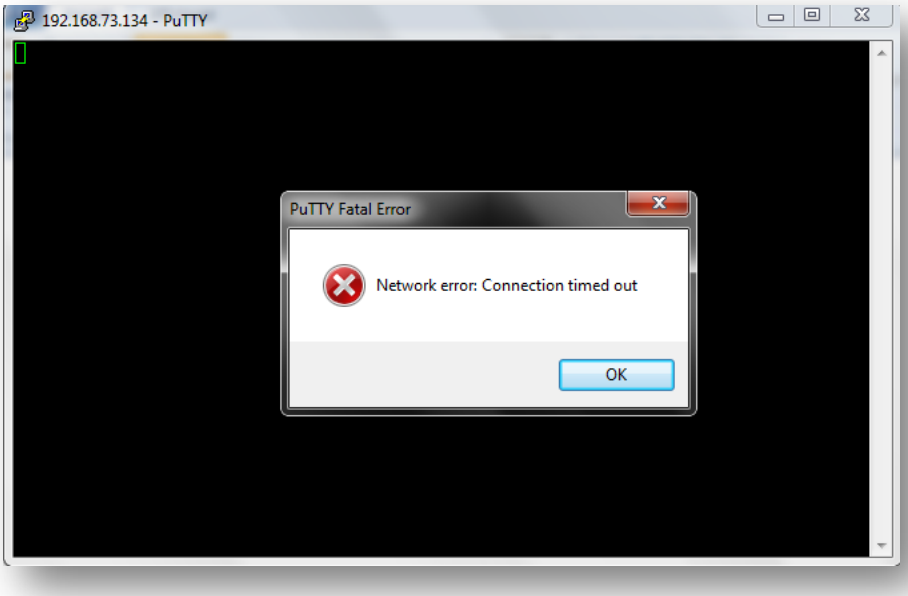

Fig.3.51 : Accès au logiciel « PUTTY » refusé

- Pour autoriser l'accès pour un client, nous allons éditer le fichier « hosts.allow » avec la commande suivante :

```
root@debian:/home/belaid# gedit /etc/hosts.allow
```

Une fois le fichier est ouvert, nous allons ajouter « sshd : l'adresse IP de ce client » puis on doit enregistrer

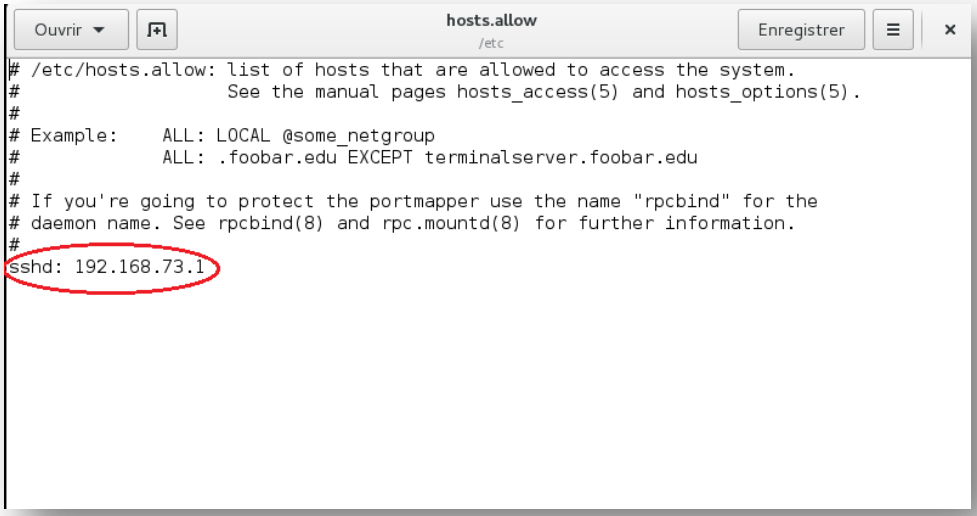

Fig.3.52 : Fichier « hosts.allow »

Pour avoir l'adresse IP de client, on doit accéder au« cmd » dans l'acône de démarrage de pc puis saisir « IPconfig » pour afficher cette adresse

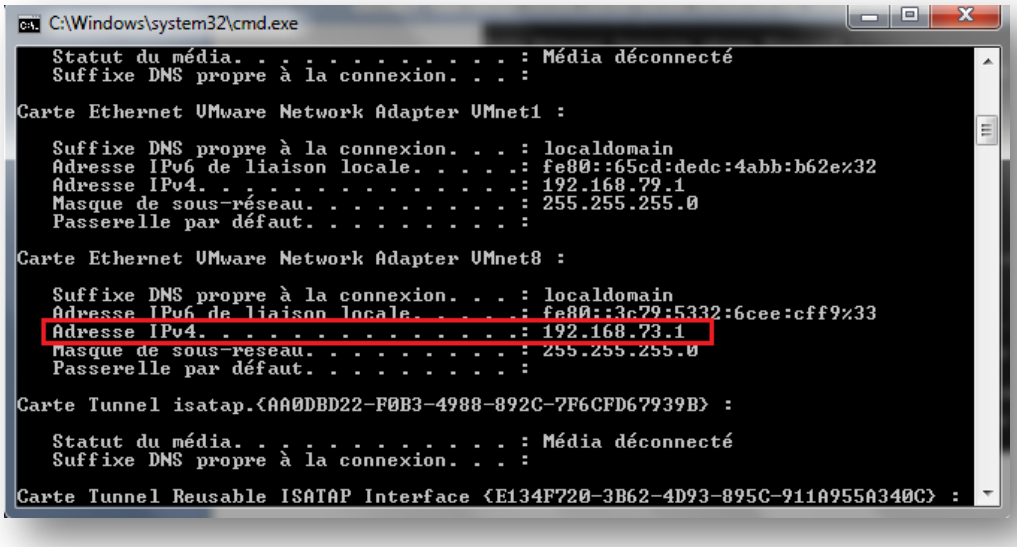

Fig.3.53 : Adresse IP du client

Pour vérifier l'accès de ce client, il faut revenir au logiciel « PUTTY » en ajoutant l'adresse IP de serveur avec le port 6000.

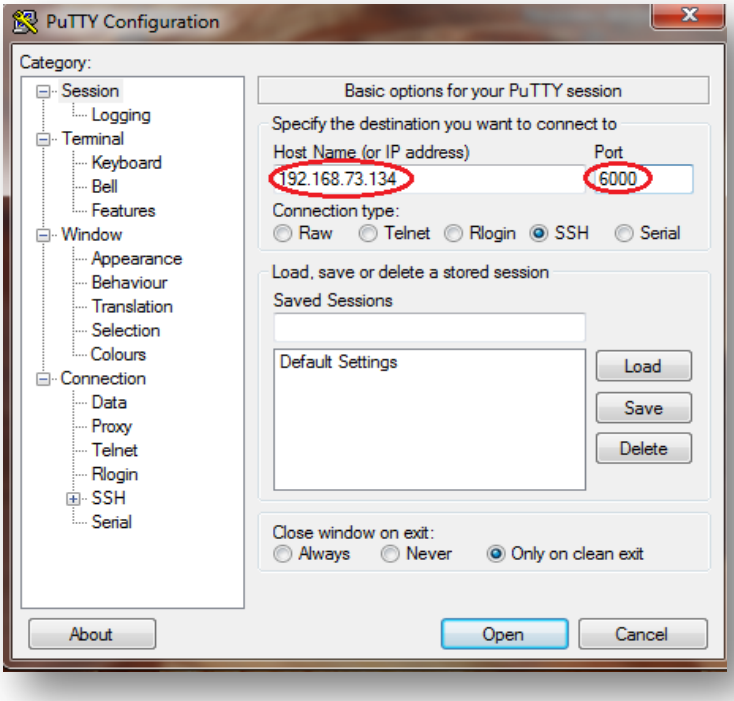

Fig.3.54 : Configuration de logiciel « PUTTY »

En cliquant sur « Open », l'accès est autorisé.

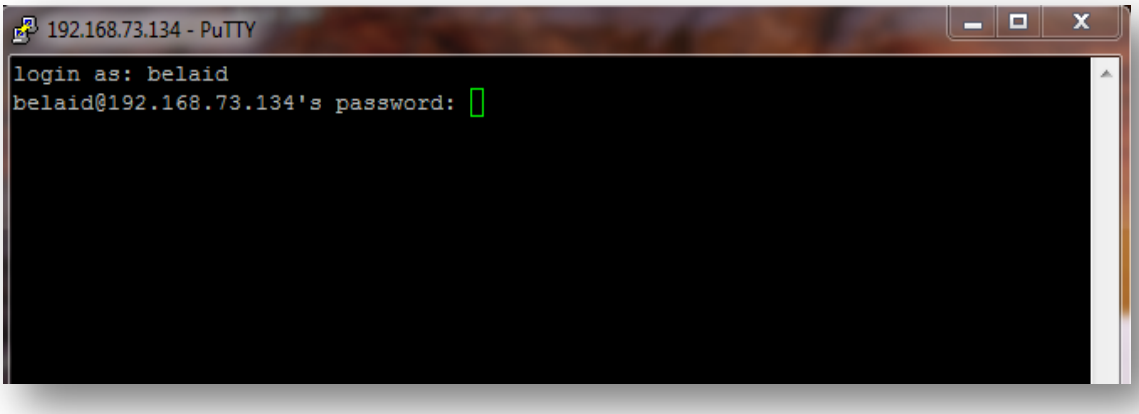

Fig.3.55 : Accès autorisé

- Dans le cas où nous disposonsde tout un réseau (plusieurs machines) et plus,

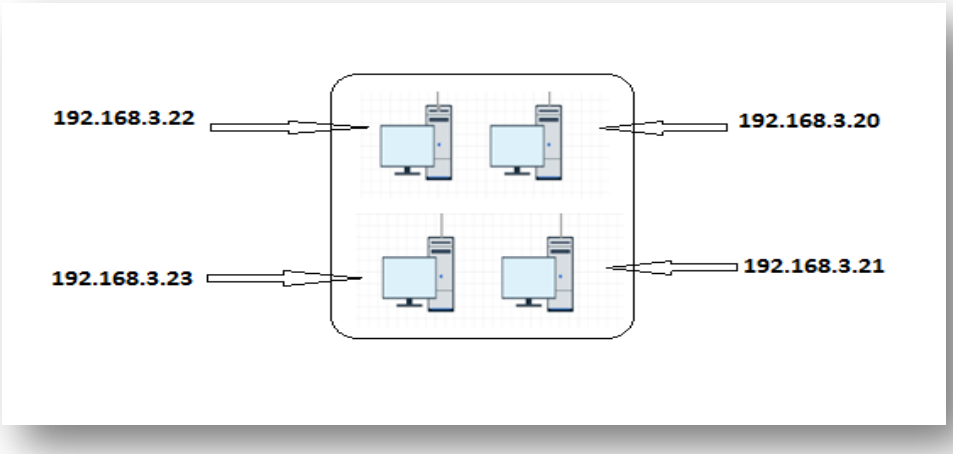

Fig.3.56 : Exemple de schéma d'un réseau

Nous allons mettre tout le réseau comme suit :

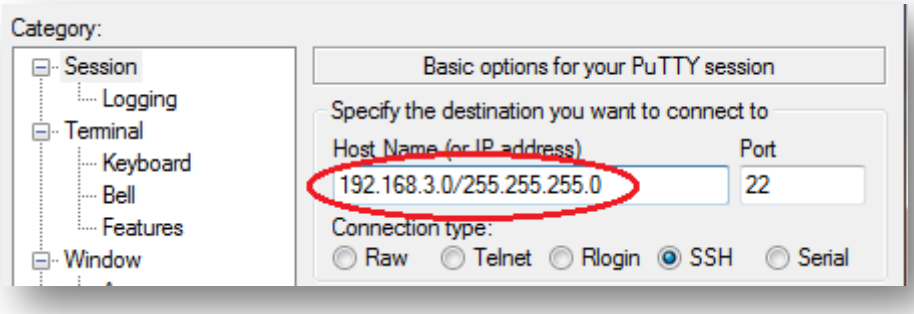

Fig.3.57 : Accèspour tout un réseau

Discussion

Dans ce chapitre, nous avons détaillésla solution nécessaire pour éliminer les failles quideLinux.En effet, la solution proposée permet de sécuriser en premier lieu l'accès vers Linux dernier vu que les deux serveurs sont installés sous Linux.Nous avons commencés par sécuriser son démarrage qui est le boot loader et le mode mono-utilisateur et le BIOS. Ensuite, nous avons utilisés lecryptage des données et sécuriser l'accès à distance. Les tests que nous avons faits montrent que cette solution est très fiable.

Conclusion

Conclusion

Dans ce mémoire, nous avons présenté une méthodologie de sécurité de deux serveurs très importants (serveur de partage et serveur backup) du réseau de l'entreprise 2INT Partners. Cette sécurité tient compte de deux points qui sont l'infrastructure réseau et le système d'exploitation installé sur ces serveurs. A cet effet, nous avons entamé notre démarche par le recensement des failles du réseau existant, puis nous avons proposé pour chaque faille une solution.

Dans la méthodologie suivie nous avons cherché à sécuriser avant tout le système d'exploitation utilisé qui est Linux. En effet, sans cette sécurité, un utilisateur qui a des connaissances sur les différents modes d'accès à Linux, pourra les exploiter pour modifier les droits d'accès aux serveurs. En conséquence, les différents fichiers se trouvant sur le serveur de partage ou sur le backup pourront tomber entre les mains de personnes malintentionnées. La deuxième étape de notre politique de sécurité adoptée permet de sécuriser l'accès à distance à ces serveurs et le cryptage des données échangées.

Les tests que nous avons effectués montrent que la solution proposée permet d'une part de bloquer l'accès non autorisé au système d'exploitation Linux et d'autre part de sécuriser l'accès à distance aux différents fichiers. De plus, ces derniers même en cas d'interception seront illisibles du fait de l'utilisation du cryptage. Ce qui répond au cahier des charges établit par l'entreprise 2INT Partners. La sécurité est très importante pour tous les systèmes informatiques, car toute machine non protégé dans un réseau peut être compromise à n'importe quel moment, de plus on peut perdre toutes les données secrètes et importantes de l'entreprise, ce qui sera une grande perte.

Comme perspectives de ce travail, nous proposons d'appliquer d'autres outils de sécurité de l'infrastructure tel que l'IDS.

Références Bibliographiques

Références bibliographiques

[1] : www.viviani.org/cours/util_int/internet/2intern.pdf, consulté le 15/06/2018.

[2] : Hélie, S. Ghernaouti, 2006. *Sécurité informatique et réseau*, Edition Eyrolles, France.

[3] : B. Boutherin, B. Delaunay, 2004. *Sécuriser un réseau Linux*, Edition Eyrolles, France.

[4] : S.MEDRA, S.MEDJAD, 2014. *Test de pénétration dans un réseau,* Mémoire de master académique réseaux et télécommunication. Département d'électronique, Université de MOULOUD Mammeri de Tizi-Ouzou.

[5] : J-F. Pillou, J-p. Bay, 2009. *Tout sur la sécurité informatique*, Edition Eyrolles, France.

[6] : W. KHADIR, (2017), « *Etude et mise en place d'un pot de miel virtuel basé sur le Respberry Pi 3 »,* mémoire de master spécialité chef de projet informatique, école 2int partners.

[7] : https://www.lemagit.fr/definition/SSH-Secure-Shell, consulté le 05/06/2018.

[8]: J-P. Armspach, P. Colin, F. Ostré-Waerweggers. 2002, *Linux Initiation et utilisation*, Edition Dunod, France.

Annexes

Annexe 1 : Système Linux et installation de debian

Un système Linux :

Linux est un système d'exploitation complet et libre, qui peut être utilisé en lieu et place de systèmes d'exploitation commercialisés, tels que Windows, de Microsoft. Il est accompagné de nombreux logiciels libres complémentaires, offrant un système complet aux utilisateurs.

Il est conçu dans le but de remplacer Windows et Mac OS X. Il est disponible en téléchargement gratuit et peut être installé sur à peu près n'importe quel ordinateur.

À l'origine, le noyau Linux a été développé pour les ordinateurs personnels compatibles PC, et devait être accompagné des logiciels GNU pour constituer un système d'exploitation. Les partisans du projet GNU promeuvent depuis le nom combiné GNU/Linux. Depuis les années 2000, le noyau Linux est utilisé sur du matériel informatique allant des téléphones portables aux superordinateurs.

Le noyau Linux a été créé en 1991 par Linus Thorvalds. C'est un logiciel libre. Les distributions Linux ont été, et restent, un important vecteur de popularisation du mouvement open source.

Installation de Debian :

Après le lancement de l’installation de Debian par une clé USB, Les étapes de l’installation sont les suivantes :

- Etape 1 : Sélectionner le mode d’installation graphique par défaut.

Fig 1 : Installation de debian

Le mode Graphical Install propose une interface plus jolie et utilisable avec une souris.

- Etape 2 :Choix de la langue et de la situation géographique.

Fig 2 : Sélectionner la langue

- Etape 3 : Choix de la situation géographique

Fig 3 : Situation géographique

- Etape 4 : Sélectionner la langue française

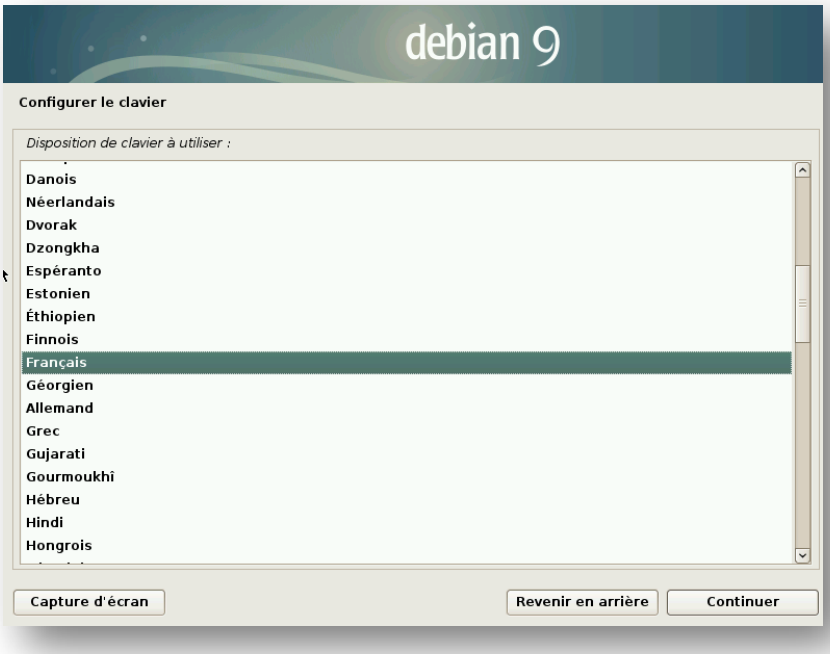

Fig 4 : Sélectionner le français

- Etape 5 : Configurer le nom du système

Fig 5 : Nom de système

- Etape 6 : Définir le mot de passe de super utilisateur « **root**»

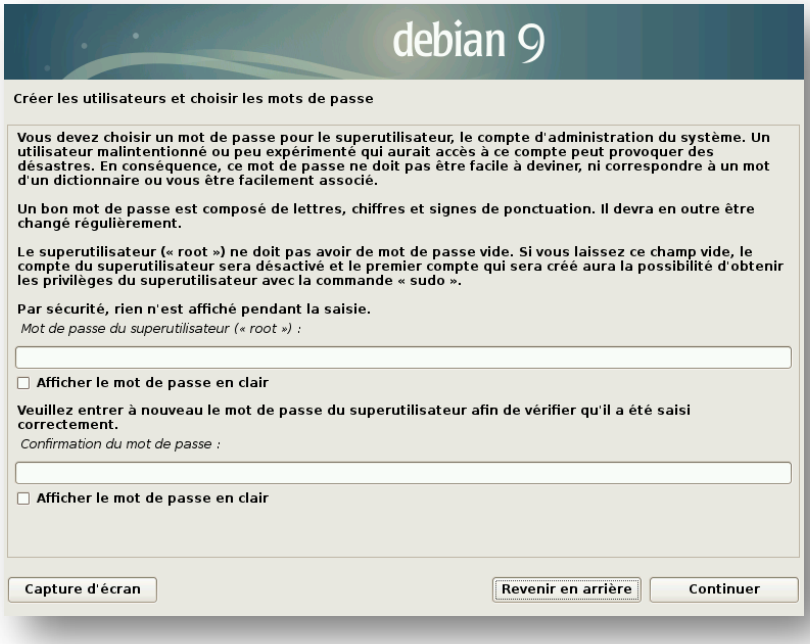

Fig 6 : Création de l’utilisateur et mot de passe

- Etape 7 : Création du premier utilisateur

Fig 7 : Nom de nouvel utilisateur

- Etape 8 : Mot de passe pour le premier utilisateur

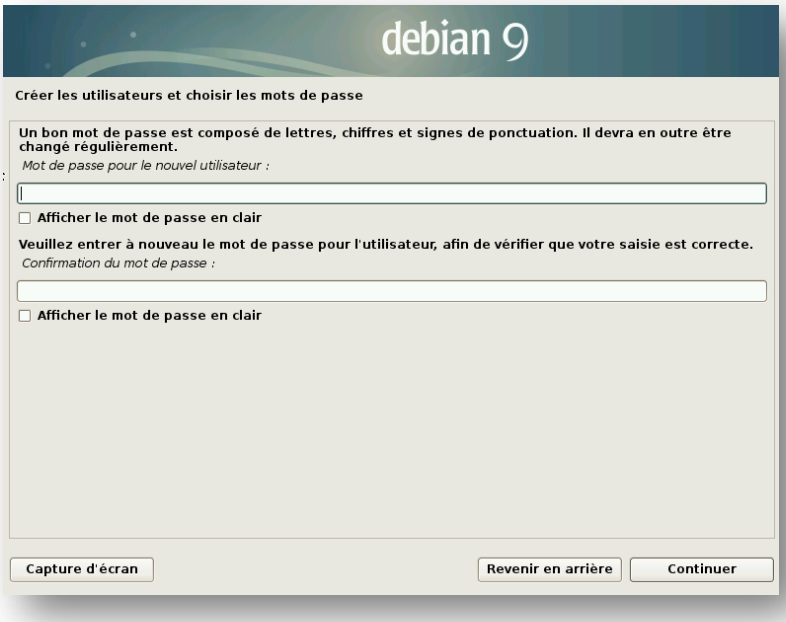

Fig 8 : Mot de passe

- Etape 9 : Choix du mode de partitionnement utiliser un disque dur entier

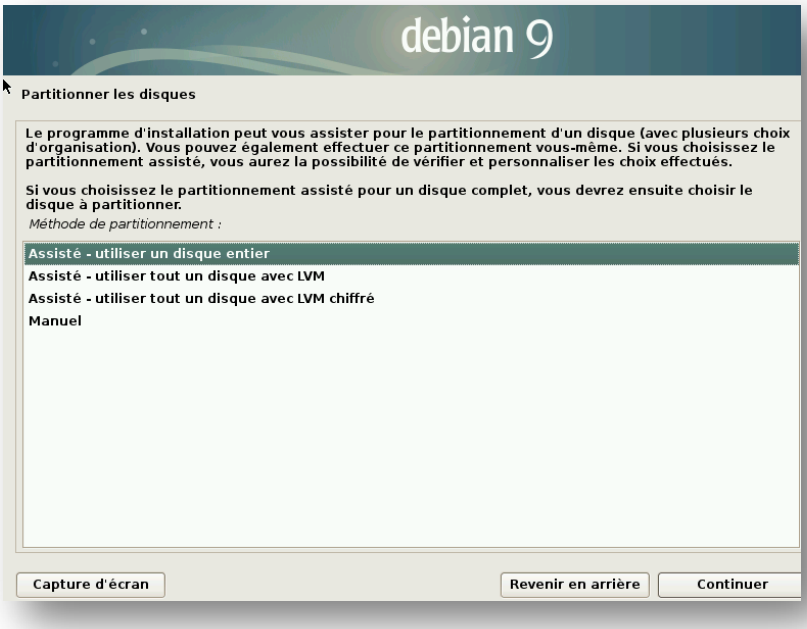

Fig 9 : Partition de disque

- Etape 10 : Choix du disque sur lequel on va créer la partition

Fig 10 : Disque à partitionner

- Etape 11 : Choix du partitionnement

Fig 11: Schéma de partitionnement

- Etape 12 : Continuer ou terminer le partitionnement

Fig 12 : Fin de partitionnement

- Etape 13 : Récapitulatif du partitionnement et lancement du formatage

Fig 13 : Accorder les changements sur le disque

- Etape 14 : Configuration de la gestion des paquets

Analyse du contenu des CD ou DVD supplémentaires si nécessaire

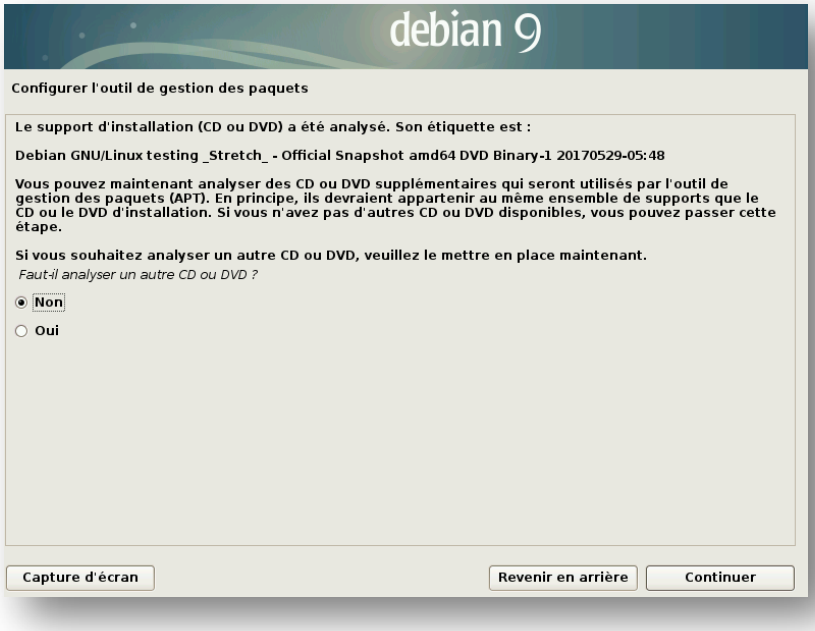

Fig 13 : Refuser l’analyse d’un autre disque

- Etape 15 : Utilisation d'un dépôt miroir

Un dépôt miroir est un serveur informatique accessible qui héberge l'ensemble des paquets Debian.Si vous ne disposez pas de tous les CD, Debian viendra piocher les logiciels ou paquets dont vousavez besoin sur des serveurs miroirs.

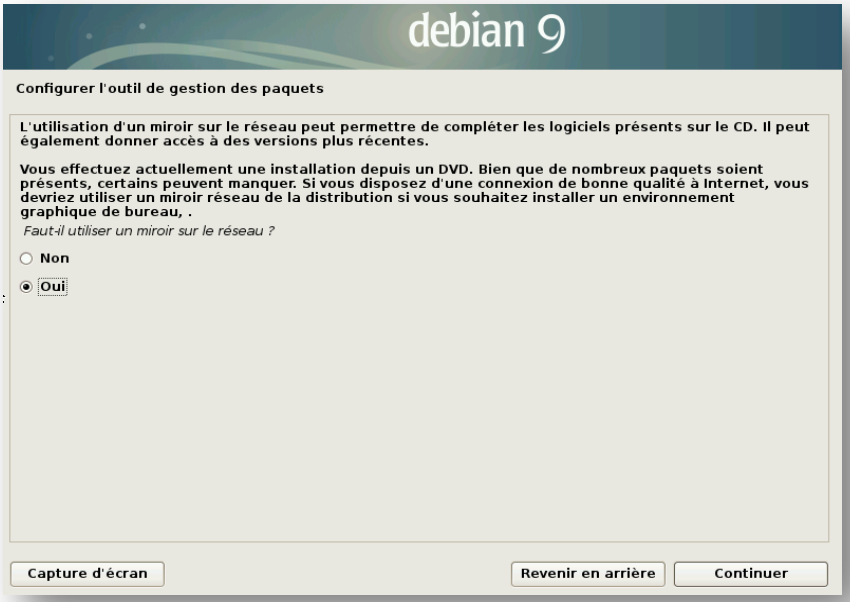

Fig 14 : Utiliser un miroir sur le réseau

- Etape 16 : Choix du pays dans lequel se trouve le miroir

Fig 15 : Pays du mémoire de l'archive debian

- Etape 17 : Choix du serveur hébergeant le miroir

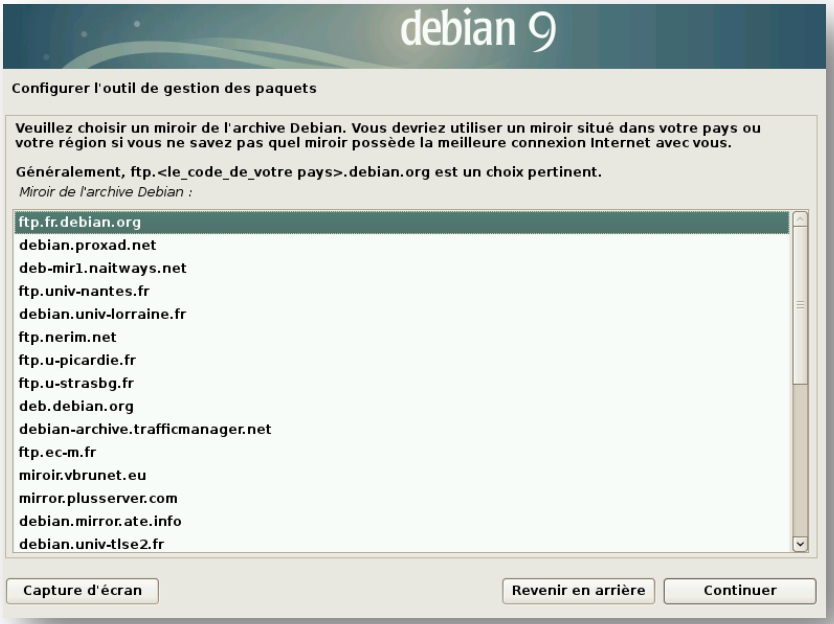

Fig 16 : Miroir de l’archive debian

- Etape 18 : Configuration d'un serveur mandataire "ou proxy" si nécessaire

Fig 17 : Mandataire http

- Etape 19 : Participation ou pas aux statistiques Debian

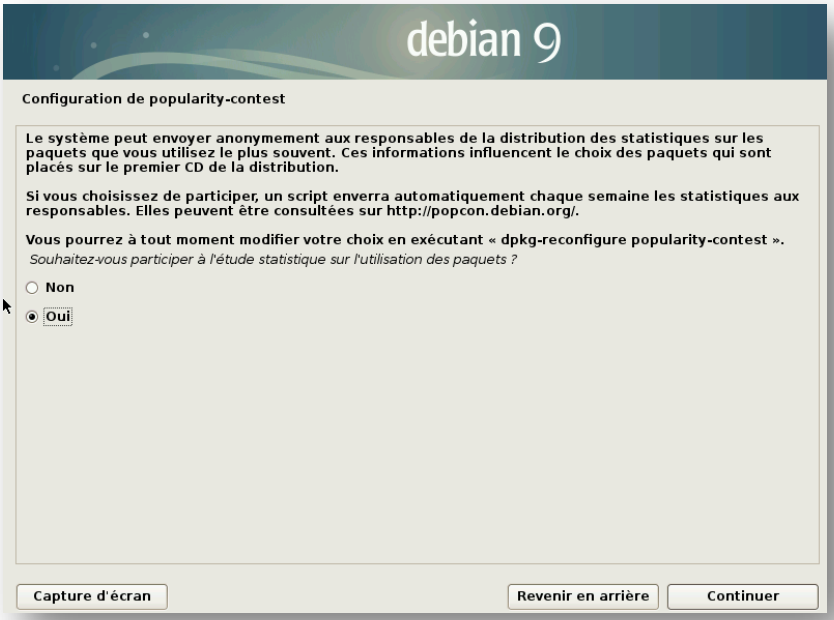

Fig 18 : Etude statistique sur l'utilisation des paquets

- Etape 20 : Sélection des logiciels

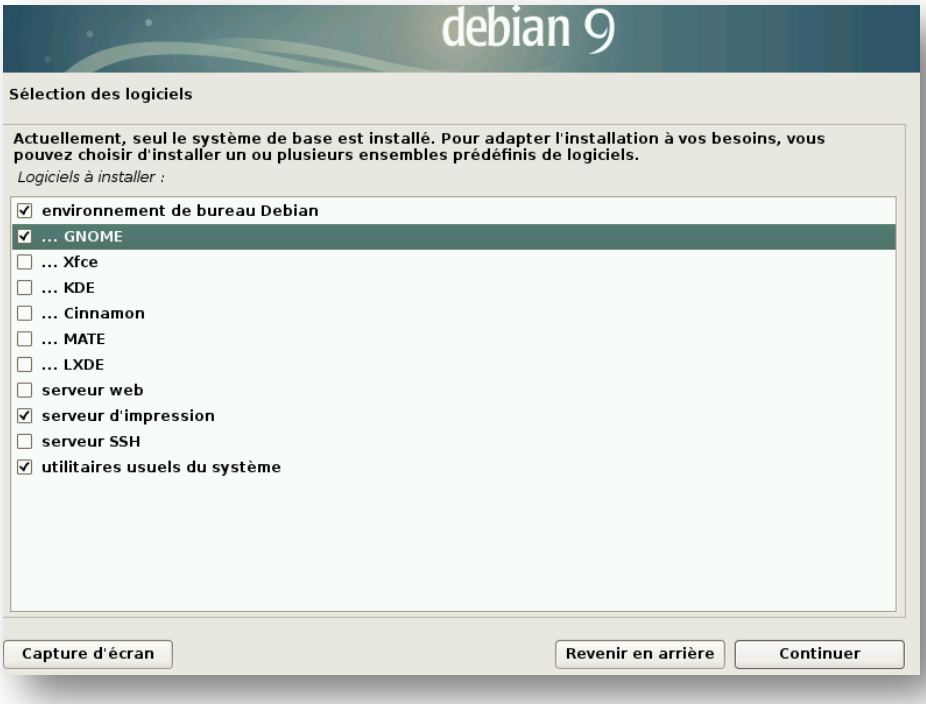

Fig 19 : Logiciel à installer

- Etape 21 : installation des paquets.

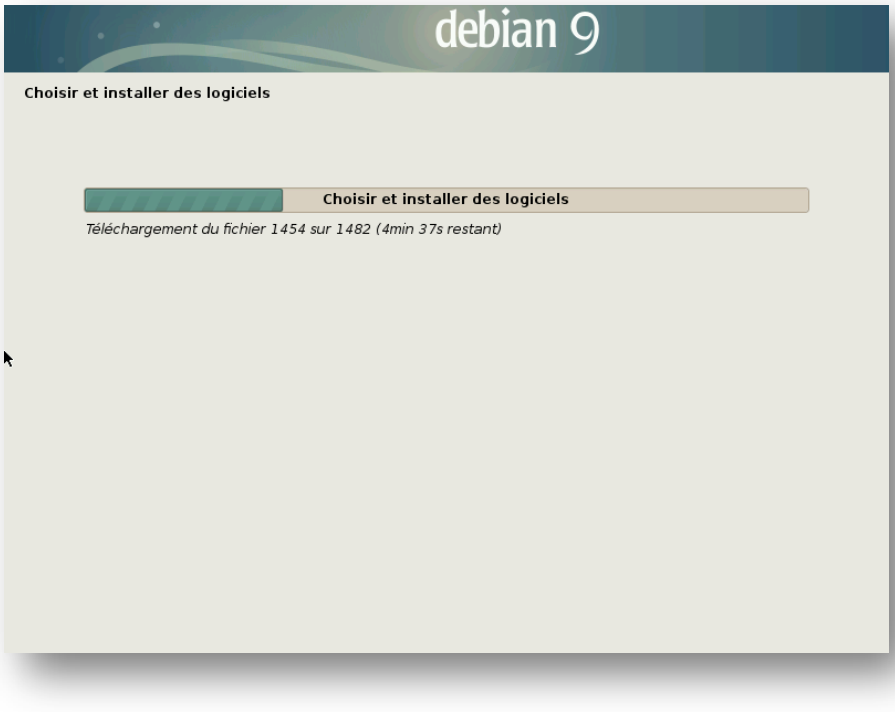

Fig 20 : Choisir et installer des logiciels

- Etape 22 : installation de GRUB.

Fig 21 : Installation de programme GRUB sur le serveur d'amorçage

- Etape 23 : choix de l’emplacement pour le GRUB

Fig 22 : Choix de périphérique

- Etape 24 : Terminer et lancer l’ordinateur.

Fig 23 : Installation terminée

- Etape 25 : Premier démarrage de Debian.

Fig 24 :Démarrage de debian

- Etape 26 : Ouverture de la session.

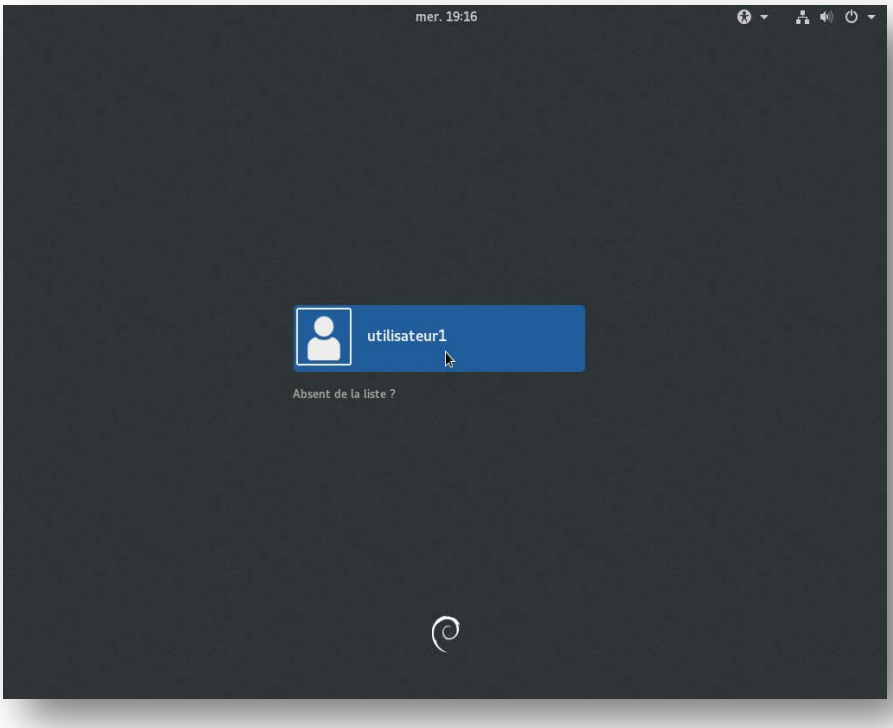

Fig 25 : Ouverture de la session

Annexe 2 : Vmware.

1. Définition d’un Vmware

Une société informatique américaine fondée en 1998, filiale d'EMC Corporation depuis 2004 (racheté par Dell le 7 septembre 20161,2), qui propose plusieurs produits propriétaires liés à la virtualisation d'architectures x86. C'est aussi par extension le nom d'une gamme de logiciels de virtualisation.

2. Fonctionnement d’un Vmware

VMware crée un environnement clos dans lequel sont disponibles un, deux, quatre ou huit (vCPU) processeur(s), des périphériques et un BIOS virtuel.

Selon les concepteurs, le microprocesseur est émulé seulement lorsque c'est nécessaire. Par exemple, les instructions initiées dans la VM (machine virtuelle) en mode user ou en mode virtuel 8086 ne sont pas toujours émulées, elles sont passées directement à l'OS hôte. Par contre, pour les instructions initiées en mode noyau ou en mode réel, VMWare va utiliser la technique dite de translation de code. Tout cela permet à VMware d'être plus rapide que des solutions multiplateformes qui émulent tout.

Lorsqu'une VM s'exécute dans un mode qui nécessite une émulation, VMware traduit dynamiquement le code privilégié en un code équivalent en mode utilisateur, le place dans un endroit libre de la mémoire, le rend invisible et inaccessible au code d'origine et l'exécute à la place. Lorsqu'une machine virtuelle fait appel à un périphérique, VMware intercepte la demande et la traduit pour qu'elle soit gérée par le système hôte. Bien que les machines virtuelles tournent en mode utilisateur, VMware nécessite d'installer plusieurs pilotes de périphériques privilégiés dans le noyau du système hôte, qui notamment interchangent les tables GDT et IDT chaque fois qu'on passe la main à une VM.

VMware assure l'émulation de la carte vidéo, la carte réseau, le lecteur de CD-ROM, le bus USB, des ports série et parallèle et du disque dur de type SCSI ou IDE. Ce dernier étant un fichier extensible d'une taille voisine de la place occupée sur la machine virtuelle ou fixe pour davantage de performance. Ce fichier contenant le contenu du disque peut être copié sur un autre hôte et exécuté par un ordinateur. Pour l'ordinateur virtuel, tous les périphériques sont identiques, même si le système hôte est totalement différent, car c'est VMware qui caractérise les périphériques.

3. Produits

En 2006, les produits suivants étaient disponibles7 :

VMware Workstation : logiciels pour stations de travail.

VMware Fusion : logiciel pour stations de travail Macintosh avec processeurs Intel.

VMware GSX Server, VMware Server et VMware ESX/ESXi Server : logiciels pour serveurs

VMware Virtual Center et VMware Converter : logiciels de gestion et outils.

La combinaison de ces différents produits crée ce que VMware nomme commercialement une infrastructure virtuelle.

Dans notre travail nous sommes intéressés au logiciel de la station de travail :

VMware Workstation :

C'est la version station de travail du logiciel. Elle permet la création d'une ou plusieurs machines virtuelles au sein d'un même système d'exploitation (généralement Windows ou Linux), ceux-ci pouvant être reliés au réseau local avec une adresse IP différente, tout en étant sur la même machine physique (machine existant réellement). Il est possible de faire fonctionner plusieurs machines virtuelles en même temps, la limite correspondant aux performances de l'ordinateur hôte. La version Linux présente l'avantage de pouvoir sauvegarder les fichiers de la machine virtuelle (vmsd) pendant son fonctionnement.

Résumé

L'objectif principal de notre mémoire consiste à étudier et concevoir une solution permettant de sécurisé le serveur back up et le serveur de fichiers de l'entreprise 2INT Partners qui sont installés sous linux.

Cette étude comporte deux grandes parties : partie bibliographique et une partie réservée a la conception et les tests des solution apportées au deux serveurs..

- Dans le premier chapitre sont exposé le cadre et le contexte du projet, présentation de l'organisme d'accueil, architecture du réseau existant, le champ d'étude.

- Le deuxième chapitre traite la sécurité informatique : les risques , les menaces, la politique de sécurité, les mécanismes de sécurité.

- Le troisième chapitre est réservé pour la conception de la solution e les tests

- Enfin, nous terminons notre travail par une conclusion générale et des perspectives sur le travail

Mots clé

Mono-utilisateur, Boot loader, LINUX, GRUB, Sécurité, implémentation