UNIVERSITE KASDI MERBAH OUARGLA
Faculté des Nouvelles Technologies de l'Information et de la Communication
Département d'informatique et technologie de l'information

Mémoire

MASTER ACADEMIQUE
Domaine : Mathématiques et Informatique
Filière : Informatique
Spécialité : Informatique Fondamentale

Présenté par :
MANKOUR Sihem
NAMOUNE Khadidja

Thème

Sécurité des serveurs sous Linux

Cas Université Kasdi Merbah Ouargla

Soutenu publiquement
Le :

Devant le jury

M. HERROUZ Abdelhakim	Maitre A	UKM Ouargla	Président
M. MAHDJOUBE Mohamed Bachir	Maitre A	UKM Ouargla	Rapporteur

Année universitaire : 2016 /2017

« La sécurité est une chaine.

Un seul maillon faible

fragilise l'ensemble »

Sommaire

Chapitre 2 : La sécurité des serveurs sous Linux

Liste des figures

Liste des tableaux

Résumé

Avec le développement de la technologie et des moyens de stockage et d'échange d'informations de différentes façons dans les entreprises, ces derniers sont devenu plus en plus ouverte vers le monde, ce qui constitue un grand risque de menaces ; la sécurité c'est devenue une préoccupation et un sujet vital très important.

Ce phénomène se rencontre aussi au niveau de l'Université Kasdi Merbah Ouargla où nous effectuions notre travaille afin d'apporter une solution à ce problème par l'analyse des vulnérabilités et des menaces où nous allons proposer une approche globale pour la maîtrise des risques sur les serveurs et des méthodes de gestion de ces derniers ainsi que du management de la sécurité et des solutions à mettre en œuvre.

Mots clés : échange d'informations, risques de menaces, sécurité, serveurs, vulnérabilités.

ملخـــــــص

مع تطور التكنولوجيا ووسائل التخزين وتبادل المعلومات بطرق مختلفة في المؤسسات، أصبحت الشركات مفتوحة على نحو متزايد للعالم، مما يشكل خطرا كبيرا من التهديدات؛ حيث أصبح موضوع الأمن أمرا شاغلا و بالغ الأهمية.

وتحدث هذه الظاهرة أيضا على مستوى جامعة قاصدي مرباح بور قلة حيث قمنا بعملنا هدا من أجل حل هذه المشكلة من خلال تحليل مواطن الضعف والتهديدات حيث نقترح نهجا عالميا لمراقبة المخاطر على مستوى النظام وطرق إدارة هذا الأخير، فضلا عن إدارة الأمن والحلول التي سيتم تنفيذها.

الكلمات الرئيسية: تبادل المعلومات، مخاطر التهديد، الأمن، الخوادم، نقاط الضعف.

Summary

With the development of technology and means of storage and exchange of information in different ways in enterprises, companies have become increasingly open to the world, which poses a great risk of threats; security has become a very important concern and subject.

This phenomenon also occurs at the level of the Kasdi Merbah Ouargla University where we carried out our work in order to solve this problem by analyzing the vulnerabilities and threats where we propose a global approach to the control of risks on the servers and the management methods of the latter as well as the management of the security and the solutions to be implemented.

Keywords: information exchange, threat risks, security, servers, vulnerabilities.

Introduction Générale

Avant l'utilisation des serveurs, l'espionnage industriel était principalement basé sur des techniques physiques, comme fouiller les poubelles à la recherche d'informations sur des feuilles de brouillon ; mais avec l'arrivée de l'informatique, des réseaux, puis d'Internet, les vols d'informations physiques se sont peu à peu transformés en intrusions informatiques. Il devient donc essentiel que les données stockées sur des serveurs soient suffisamment protégées et sécurisées. Pour cela, de nombreuses techniques de sécurisation sont mises en place, afin d'assurer le respect de bonnes pratiques de sécurité.

La sécurité informatique peut être définie comme la science qui assure la protection de l'information contre les risques qui les menacent ; c'est aussi la barrière qui empêche l'agression en fournissant les outils et les moyens nécessaires pour protéger les informations contre les menaces internes ou externes ; elle consiste en les critères et procédures adoptées pour empêcher l'arrivée de l'information entre les mains de personnes non autorisées.

Dans ce cadre, nous avons conçu notre travail, objet de présent mémoire, et qui consiste à assurer la sécurité de system informatique et donc d'améliorer la gestion de la sécurité de l'université.

Dans le premier chapitre nous donnons un aperçu général sur les termes de la sécurité en informatique. En suite, nous détaillerons les termes et les principes de la sécurité des serveurs.

Puis, nous avons fait une analyse de la situation initiale pour déterminer une problématique et les besoins de sécurisation associés. A partir de ces besoins on a fini notre travail par chercher à établir des solutions adéquates. Ces solutions seront présentées sous forme de fiches de recommandations dans le dernier chapitre.

Chapitre 1 :

La sécurité informatique

1. Introduction

A l'heure actuelle, les besoins en matière de sécurité sont grandissants, et la tendance n'est certainement pas à la baisse, parce que le matériel informatique est omniprésent. D'une part le matériel est accessibles à un prix très abordable, et d'autre part, les logiciels tendent à se simplifier et permettent une prise en main rapide. D'un autre coté, les entreprises, elles aussi informatisées, nécessitent un réseau sécurisé pour le transfert des données, que ce soit entre les machines de cette entreprise, ou avec des machines externes, distantes de plusieurs milliers de kilomètres. Si on observe la sécurité d'une manière plus générale, elle est d'ailleurs présente à plusieurs niveaux, qu'il s'agisse des différentes portées de l'information. Dans ce chapitre nous allons essayer de déterminer et détailler quelque terme de la sécurité.

2. Système d'information et système informatique

Il est courant de confondre système d'information et système informatique, et par extension, leur sécurité. Il ne faut pas oublier que l'un est l'outil de l'autre. Le système d'information est généralement défini comme un groupement d'éléments et de ressources structurés qui permettent la transmission, l'interprétation et le stockage de données. Il faut donc comprendre par là que cela permet à des informations d'être acheminées d'un point A à un point B, que l'expéditeur et le destinataire se comprennent et que l'information soit ensuite conservée.

Le système informatique est en réalité celui qui remplit encore le mieux ces missions par le biais d'éléments électroniques et de la télécommunication qui en sont ses composants. Alors qu'autrefois on utilisait des éléments naturels, des matériaux (comme du papier, de la pierre) pour transmettre et conserver l'information et des animaux pour les transmettre (pigeons voyageurs, messagers sur des chevaux), nous utilisons aujourd'hui l'informatique et les systèmes informatiques pour réaliser ces missions. Le fait que ce soit l'outil le plus performant pour réaliser cette tâche fait qu'aujourd'hui, on parle souvent du systèmes d'information pour parler de système informatique et inversement.

3. Pourquoi sécuriser l'information ?

L'information est aujourd'hui la sève de l'entreprise. C'est ce qui fait à la fois sa force et son existence. Fichiers, bases de données, méthodes de travail et de fabrication, fiches des salariés et informations industrielles sont autant d'informations qui composent la structure et

la base d'une entreprise. Il s'agit là son capital intellectuel, ou plutôt capital informationnel. Toute perte d'information peut porter un coup fatal à une entreprise ou même à une nation.

Si ces informations venaient à être perdues, volées ou à tomber dans les mains d'une autre entreprise, la donnée n'aurait plus de raison d'exister car elle ne serait plus exclusive. L'information a aujourd'hui de la valeur de par son côté unique et exclusif pour une entreprise. Il est donc dans l'intérêt de l'entreprise de protéger son patrimoine informationnel.**[5]**

4. Définition de la sécurité informatique

La sécurité d'un système informatique est un ensemble de moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour réduire la vulnérabilité d'un système contre les menaces accidentels ou intentionnels afin d'assurer les services de sécurité. **[1]**

5. Démarche générale de la sécurité

Pour sécuriser les systèmes, la démarche consiste à :

- **Evaluer les risques et leur criticité** : quels risques et quelles menaces, sur quelles données et quelles activités, avec quelles conséquences ?

- **Rechercher et sélectionner les parades** : que va-t-on sécuriser, quand et comment ? C'est une étape difficile : dans un contexte de ressources limitées (en temps, en compétences et en argent), seules certaines solutions pourront être mises en œuvre.

- **Mettre en œuvre les protections et vérifier leur efficacité :** une faiblesse fréquente de cette phase est d'omettre de vérifier que les protections sont bien efficaces.

6. Autres définitions

6.1 La sécurité en parallèle : On parle de sécurité en parallèle lorsque plusieurs mécanismes de sécurité protégeant un système possèdent le même rôle. Dans ce cas, le niveau de protection du système est équivalent à celui du mécanisme le moins sûr. En tant qu'exemple, citons un ordinateur portable que l'on peut déverrouiller par mot de passe ou empreinte digitale.

6.2 La sécurité en série : Plusieurs mécanismes de sécurité protègent un système et ont des rôles différents. On parlera de « défense en profondeur ». Citons par exemple le réseau d'une entreprise où :

- Le réseau est sécurisé par un pare-feu matériel.
- Les liaisons entre machines sont protégées.
- Les machines individuelles sont munies d'un pare-feu logiciel.
- Les accès aux machines se font par empreinte biométrique.
- Le logiciel à utiliser est accessible par mot de passe.

6.3 Vulnérabilité : faiblesse / faille : faute accidentelle ou intentionnelle introduite dans spécification, conception ou configuration du système.

6.4 Attaque : Action malveillante qui tente d'exploiter une faiblesse dans le système et de violer un ou plusieurs besoins de sécurité.

6.5 Intrusion : Prise de contrôle partielle ou totale d'un système distant.

6.6 Menace : Violation potentielle d'une propriété de sécurité.

6.7 Risque : La probabilité qu'une menace exploitera une vulnérabilité du système. Couple (menace, vulnérabilité).

6.8 Mécanismes de Sécurité : un mécanisme qui est conçu pour détecter, prévenir et lutter contre une attaque de sécurité (Chiffrement, Signature, Contrôle d'accès…..).

6.9 Service de Sécurité : un service qui augmente la sécurité des traitements et des échanges de données d'un système. Un service de sécurité utilise un ou plusieurs mécanismes de sécurité. **[1]**

7. Les objectifs principaux

La sécurité des données couvre quatre objectifs principaux, et est représentée sous forme d'acronymes (C.I.D.A) :

7.1 La disponibilité : est l'assurance que les personnes autorisées ont accès à l'information quand elles le demandent ou dans les temps requis pour son traitement.

7.2 L'intégrité : est la certitude de la présence non modifiée ou non altérée d'une information et de la complétude des processus de traitement. Pour les messages échangés, il concerne la protection contre l'altération accidentelle ou volontaire d'un message transmis.

7.3 La confidentialité : est l'assurance que l'information n'est accessible qu'aux personnes autorisées, qu'elle ne sera pas divulguée en dehors d'un environnement spécifié. Elle traite de la protection contre la consultation de données stockées ou échangées.

7.4 ***L'authentification*** : est le moyen qui permet d'établir la validité de la requête émise pour accéder à un système. L'authenticité est la combinaison d'une authentification et de l'intégrité.

D'autres principes de sécurité peuvent être établis, il s'agit de :

- **La preuve :** consiste à garantir que l'émetteur d'une information soit bien identifié et qu'il a les droits et les accès logiques, que le récepteur identifié est bien autorisé à accéder à l'information.
- ***Le non répudiation :*** considérée comme le cinquième principe, a été introduite dans la norme ISO 74982 comme un service de sécurité pouvant être rendu par un mécanisme comme la signature numérique, l'intégrité des données ou la notarisation. L'élément de la preuve de non répudiation doit permettre l'identification de celui qu'il représente, il doit être positionné dans le temps

(horodatage), il doit présenter l'état du contexte dans lequel il a été élaboré (certificats).

- ***Les mécanismes de chiffrement*** : procèdent du principe que l'émetteur et le récepteur conviennent d'un mot de passe connu d'eux seuls. L'émetteur utilise ce mot de passe comme clé de chiffrement pour le message à transmettre, seul le récepteur qui connaît ce mot de passe peut l'utiliser comme clé pour déchiffrer le message .

8. Les menaces informatiques

En termes de sécurité informatique les menaces peuvent être le résultat de diverses actions en provenance de plusieurs origines :

8.1 Origine opérationnel: Ces menaces sont liées à un état du système à un moment donné. Elles peuvent être le résultat d'un bogue logiciel, d'une erreur de filtrage des entrées utilisateur, d'un dysfonctionnement de la logique de traitement ou d'une erreur de configuration.

8.2 Origine physique: Elles peuvent être d'origine accidentelle, naturelle ou criminelle. On peut citer notamment les désastres naturels, les pannes ou casses matérielles, le feu ou les coupures électriques.

8.3 Origine humaine: Ces menaces sont associées directement aux erreurs humaines, que ce soit au niveau de la conception d'un système ou au niveau de la manière dont on l'utilise. Ainsi elles peuvent être le résultat d'une erreur de conception ou de configuration comme d'un manque de sensibilisation des utilisateurs face au risque lié à l'usage d'un système informatique.

Avec la popularité grandissante des réseaux, des échanges de données, et donc des transmissions entre individus, de nombreuses menaces émergèrent. Parmi celles-ci, on trouve diverses catégories :

- ***Les menaces accidentelles :*** ne supposent aucune préméditation. Dans cette catégorie, sont repris les bugs logiciels, les pannes matérielles, et autres défaillances "incontrôlables".

- ***Les menaces intentionnelles*** : reposent sur l'action d'un tiers désirant s'introduire et relever des informations. Dans le cas d'une attaque passive, l'intrus va tenter de dérober les informations par audit, ce qui rend sa détection relativement difficile. En effet, cet audit ne modifie pas les fichiers, ni n'altère les systèmes. Dans le cas d'une attaque active, la détection est facilitée, mais il peut être déjà trop tard lorsque celle-ci a lieu. Ici, l'intrus aura volontairement modifié les fichiers ou le système en place pour s'en emparer. Les menaces actives appartiennent principalement à quatre catégories :

  - Interruption = problème lié à la disponibilité des données
  - Interception = problème lié à la confidentialité des données
  - Modification = problème lié à l'intégrité des données
  - Fabrication = problème lié à l'authenticité des données. **[6]**

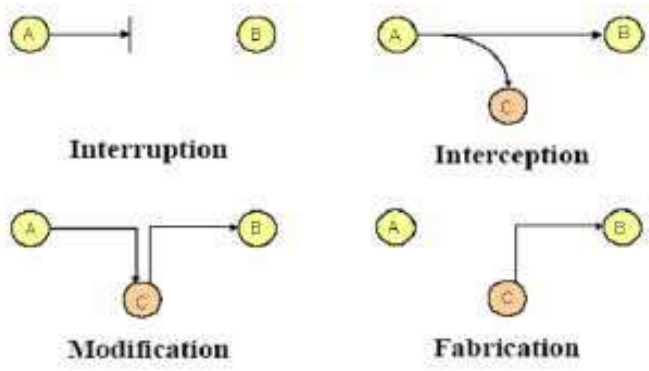

Figure 1 : Les menaces actives

9. Les attaquants

9.1 Pirates : Nous proposons les deux profils de pirate les plus souvent identifiées :

- ***Hacker :*** individu curieux, qui cherche à se faire plaisir. Pirate par jeu ou par défi, il ne nuit pas intentionnellement. Plutôt jeune, avec des compétences non négligeables.

- ***Cracker :*** plus dangereux que le hacker, cherche à nuire et montrer qu'il est le plus fort. Souvent mal dans sa peau et dans son environnement, il peut causer de nombreux dégâts en cherchant à se venger d'une société (ou d'individus) qui l'a rejeté ou qu'il déteste. Il veut prouver sa supériorité et fait partie de clubs où il peut échanger des informations avec ses semblables.

9.2 Fraudeurs : Les fraudeurs se répartissent en deux catégories :

- ***Le fraudeur interne :*** Possédant de bonnes compétences sur le plan technique. Il pense que ses qualités ne sont pas reconnues, qu'il n'est pas apprécié à sa juste valeur. Il veut se venger de son employeur et chercher à lui nuire en lui faisant perdre de l'argent. Pour parvenir à ses fins il possède les moyens mis à sa disposition par son entreprise qu'il connaît parfaitement.
- ***Le fraudeur externe :*** Bénéficiant presque toujours d'une complicité, volontaire ou non, chez ses victimes, il cherche à gagner de l'argent par tous les moyens. Parfois lié au grand banditisme, il peut attaquer une banque, falsifier des cartes de crédit ou se placer sur des réseaux de transfert de fonds, et si c'est un particulier il peut vouloir fausser sa facture d'électricité ou de téléphone.

9.3 Espions : Ils travaillent pour un État ou pour un concurrent. Choisis pour leur sang-froid et leur haut niveau de qualification, il sont difficiles à repérer :

- ***L'espion d'État :*** professionnel, entraîné, rompu à toutes les techniques, il dispose de nombreux moyens d'attaque et d'une importante puissance de calcul. Il peut aller jusqu'à acquérir, légalement ou non, une copie du système qu'il veut attaquer pour l'analyser et l'étudier sous toutes ses coutures. Il est patient et motivé. Il sait garder le secret de sa réussite pour ne pas éveiller les soupçons et continuer son travail dans l'ombre.
- ***L'espion privé :*** souvent ancien espion d'État reconverti, il a moins de moyens mais une aussi bonne formation.

9.4 Terroristes : Moins courant, le terroriste est aidé dans sa tâche par l'interconnexion et l'ouverture des réseaux. Il est très motivé, il veut faire peur et faire parler de lui. Ses actions se veulent spectaculaires.

10. Les techniques d'attaques :

10.1 Attaques physiques : Nous plaçons ici les attaques qui nécessitent un accès physique aux installations ou qui se servent de caractéristiques physiques particulières. Les attaques physiques se divisent par plusieurs catégories comme suite :

- **Interception** : L'attaquant va tenter de récupérer un signal électromagnétique et de l'interpréter pour en déduire des informations compréhensibles. L'interception peut porter sur des signaux hyper- fréquences ou hertziens, émis, rayonnés, ou conduits.
- **Brouillage :**Utilisée en télécommunication, cette technique rend le système inopérant. C'est une attaque de haut niveau, car elle nécessite des moyens importants, qui se détectent facilement. Elle est surtout utilisée par les militaires en temps de crise ou de guerre.
- **Écoute :** L'écoute consiste à se placer sur un réseau informatique ou de télécommunication et à analyser et à sauvegarder les informations qui transitent. De nombreux appareils du commerce facilitent les analyses et permettent notamment d'interpréter en temps réel les trames qui circulent sur un réseau informatique.

10.2 Attaques Logiques :

- **Substitution :** Ce type d'attaque est réalisable sur un réseau ou sur un système comportant des terminaux distants. L'agresseur écoute une ligne et intercepte la demande de déconnexion d'un utilisateur travaillant sur une machine distante. Il peut alors se substituer à ce dernier et continuer une session normale sans que le système note un changement d'utilisateur.

  Un cas bien connu est celui des ordinateurs sur un réseau local qui ne sont déclarés que par leur adresse Internet. Un attaquant peut alors attendre qu'une machine soit arrêtée pour se faire passer pour elle en usurpant l'adresse de la machine éteinte.

- **Saturation (DOS) :** Cette attaque contre la disponibilité consiste à remplir une zone de stockage ou un canal de communication jusqu'à ce que l'on ne puisse plus l'utiliser. Il en résultera un déni de service.

11. Les infections informatiques :

11.1 Virus : Nommé ainsi parce qu'il possède de nombreuses similitudes avec ceux qui attaquent le corps humain, un virus est un programme malicieux capable de se reproduire et qui comporte des fonctions nuisibles pour le SI : on parle d'infection. Le virus dispose de fonctions qui lui permettent de tester s'il a déjà contaminé un programme, de se propager en se recopiant sur un programme et de se déclencher comme une bombe logique quand un événement se produit. Ses actions ont généralement comme conséquence la perte d'intégrité des informations d'un système ou une dégradation ou une interruption du service fourni.

11.2 Cheval de troie : (*trojan horse*) un programme informatique effectuant des opérations malicieuses à l'insu de l'utilisateur. Le nom « Cheval de Troie » provient d'une légende. La légende veut que les Grecs, n'arrivant pas à pénétrer dans de la ville Troie, eurent l'idée de donner en cadeau un énorme cheval de bois en offrande à la ville en abandonnant le siège. Les troyens (peuple de la ville de Troie), apprécièrent cette offrande à priori inoffensive et la ramenèrent dans les murs de la ville. Cependant le cheval était rempli de soldats cachés qui s'empressèrent d'en sortir à la tombée de la nuit, alors que la ville entière était endormie, pour ouvrir les portes de la cité et en donner l'accès au reste de l'armée.

Le principe des chevaux de Troie étant généralement d'ouvrir un port de votre machine pour permettre à un pirate d'en prendre le contrôle (par exemple voler des données personnelles stockées sur le disque), le but du pirate est dans un premier temps d'infecter votre machine en vous faisant ouvrir un fichier infecté contenant le troyen et dans un second temps d'accéder à votre machine par le port qu'il a ouvert.

11.3 Ver : Un ver informatique (*worm*) est un programme qui peut s'auto reproduire et se déplacer à travers un réseau en utilisant les mécanismes réseau, sans avoir réellement besoin d'un support physique ou logique (disque dur, programme hôte, fichier, etc.) pour se propager; un ver est donc un virus réseau.

11.4 Bombe : Les bombes sont des dispositifs programmés dont le déclenchement s'effectue à un moment déterminé en exploitant la date du système, le lancement d'une commande, ou n'importe quel appel au système. Les bombes logiques sont généralement utilisées dans le but de créer un déni de service en saturant les connexions réseau d'un site, d'un service en ligne ou d'une entreprise.

11.5 Spam : Le spamming consiste à envoyer massivement des e-mails de type généralement publicitaire, à un grand nombre de personnes n'ayant pas sollicité ce type d'envoi publicitaire. Les e-mails "spammés" constituent actuellement la quasi-moitié des e-mails "circulant" à l'échelle planétaire.

11.6 Spyware : Un espiogiciel est un programme chargé de recueillir des informations sur l'utilisateur de l'ordinateur sur lequel il est installé. Les spywares s'installent généralement en même temps que d'autres logiciels la plupart du temps des freewares.

11.7 keylogger : (*enregistreur de touches*) est un dispositif chargé d'enregistrer les frappes de touches du clavier et de les enregistrer, à l'insu de l'utilisateur. Il s'agit donc d'un dispositif d'espionnage. **[7]**

12. Différents modèles de sécurité

12.1 CIA (1987) : Le triangle CIA est le pilier immuable présentant les grands axes de la sécurité. La plupart des autres modèles utilisent cette représentation en tant que base. On peut définir les différents termes employés comme suit :

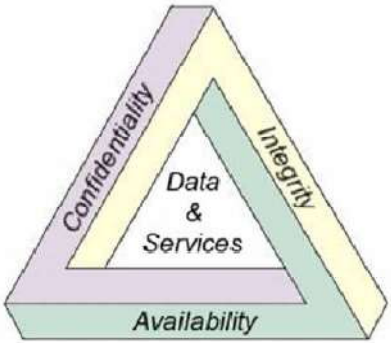

Figure 2 : Le triangle CIA

- Confidentialité.
- Intégrité.
- Disponibilité.

12.2 McCumber Cube (1991) : On y retrouve les trois piliers de la sécurité (CIA), mais deux autres dimensions apparaissent :

- ***L'état des données :*** le stockage, la transmission, l'exécution.
- ***Les méthodes :*** les principes et règles à adopter pour atteindre le niveau de sécurité souhaité.

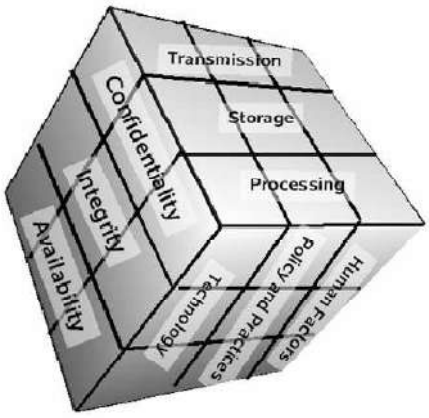

Figure 3 : McCumber Cube

12.3 Le contrôle d'accès (Le protocole AAA) : Le contrôle d'accès se fait en 4 étapes :

- Identification : Qui êtes-vous ?
- Authentification : Prouvez-le !
- Autorisation : Avez-vous les droits requis ?
- Accounting /Audit : Qu'avez-vous fait ?

On parlera d'Accounting lorsque le fait de comptabiliser des faits sera demandé, et d'Audit lorsque des résultats plus globaux devront être étudiés.

12.4 Parkerian Hexad (2002) : Ce modèle, initié par Donn Parker, ajoute la nuance d'utilité (une information chiffrée pour laquelle on a perdu la clé de déchiffrement n'est plus d'aucune utilité, bien que l'utilisateur y ait accès, que cette information soit confidentielle, disponible et intègre). **[6]**

Figure 4 : Parkerian Hexad

13. Conclusion

Les moyens modernes de communication ont grandement facilité la transmission de l'information ; les distances ne constituent plus un handicap et le temps aussi est maitrisé ; on dit bien maintenant que le monde est un village. Cet avantage appréciable exige, cependant, un tribut à payer : les systèmes informatiques sont exposés à des menaces de piratage. Nous sommes donc obligés de fournir des efforts supplémentaires pour sécuriser nos moyens de communications.

Chapitre 2 :

Sécurité des serveurs sous Linux

1. Introduction

Aujourd'hui les réseaux informatiques mondiaux, tels qu'Internet par exemple, du commerce électronique, chaque machine est une cible potentielle. Il ne se passe pas une semaine, une journée même, sans qu'un système informatique ne soit compromis par une attaque distante ou locale. Devant l'importance de ce phénomène, les responsables informatiques doivent prendre les devants, et les administrateurs systèmes et réseaux doivent se défendre et prévoir chaque faille potentielle de leurs machines. Ce chapitre a pour but d'expliquer quelles méthodes et techniques peuvent être utilisées pour sécuriser des systèmes Linux en réseau.

2. Politique de sécurité

Pour pouvoir sécuriser un système, il convient d'en analyser les points importants, d'identifier les failles, et de mesurer le risque induit par ces failles, et donc d'en tirer un police définissant comment les procédures doivent se dérouler.

L'identification des points importants peut se faire en dressant une liste, en les divisant en deux classes, d'un côté les éléments tangibles (ordinateurs, données, données sauvegardées, données personnelles) et d'un autres, les éléments intangibles (vie privée des employés, mots de passes, disponibilité du système, informations de configuration, réputation de la société et image publique). La détermination des dangers potentiels se fait en examinant chaque point important de la liste précédemment établie, et en déterminant les risques induits. Il ne faut pas avoir peur d'être trop large, et vraiment trouver tout ce qui peut représenter un risque (maladie d'employés clés, éclair tombant sur le bâtiment, défaillance d'un disque dur, introduction d'un virus, vol physique d'un support de sauvegarde, entrée d'un pirate dans le système,…). On définit ce qu'on appelle un périmètre de sécurité, incluant tous les éléments devant rentrer dans la police de sécurité de ce système.

La mesure du risque induit peut se faire, entre autres manières, en évaluant le coût de chaque défaillance (financièrement, durée de l'indisponibilité), et sa probabilité. Cette dernière est très dure à déterminer.

Enfin, un dernier élément à calculer est le coût de prévention de chaque risque déterminé à la deuxième étape (coupure de courant => coût financier d'un onduleur,...).

Il est alors possible d'établir une liste de politique de sécurité, chaque règle devant spécifier ce qui est protégé, pourquoi ça l'est, qui est responsable de cet élément. On peut partir d'un principe simple, comme les deux philosophies bien connues : « Tout ce qui n'est pas autorisé est interdit » et « Tout ce qui n est pas interdit est autorisé », bien que ne jamais choisir la première.

2.1 Utilisateurs, mots de passes, et authentification

Une bonne politique est primordiale, et constitue un élément de base d'un système.

a. **Login avec utilisateurs et mots de passe :** Toute personne utilisant une machine Linux devrait avoir son propre compte utilisateur sur le système, et être ainsi identifié sur celle ci par un numéro d'authentification unique (UID, user identification). De cette manière, toute action sur la machine peut être tracée, et on a un moyen de savoir qui a fait quoi. Ce login est appelé identifiant utilisateur et sert à savoir qui vous êtes, tandis que le mot de passe associé est appelé « authentificator », et sert à prouver que ce compte est bien le votre. L'identifiant doit bien sûr être unique, et peut se baser sur beaucoup d'éléments, tels le nom ou le prénom de la personne, son métier, sa localisation, ou une combinaison de ces éléments et d'autres. Une machine sous Linux possède un certain nombre de compte particuliers, qui ne doivent par conséquent pas être utilisés par des utilisateurs.

   Le mot de passe est un élément secret partagé entre un utilisateur et une machine. Les mots de passes ne devraient jamais être vides, et devraient systématiquement respecter une politique de complexité. Les systèmes Linux respectent la casse, et à ce titre les bon mots de passes doivent en tirer partie, en mélangeant minuscules, majuscules, caractères alphanumériques, et caractères spéciaux. Un mauvais mot de passe est comme une porte qui serait fermée mais dont on n'aurait pas tourné la clé. Un élément à ne pas négliger est la manière dont les personnes stockent leurs mots de passe, il faut éviter de le noter, et essayer de l'apprendre.

b. **Utilisateurs et groupes :** Chaque utilisateur d'un système Linux a donc un identifiant utilisateur unique, mais il fait aussi parti d'au moins un groupe. Ces groupes peuvent améliorer grandement la sécurité, car c'est en jouant avec ceux-ci que l'on va

permettre le partage de ressources et de fichiers, chaque élément du système Linux étant vu comme un fichier, dans la mesure où les droits sur ceux ci sont définis en fonction de trois éléments : l'utilisateur, le groupe de l'utilisateur, les autres groupes.

c. **Pam :** « Pluggable Authentication Modules », c'est une interface de d'authentification système permettant d'interagir avec différents systèmes d'authentification, tels passwd, LDAP, Kerberos, ou d'autres encore. Cela permet d'offrir une couche d'abstraction et donc de s'identifier de manière unique.

Les système Linux propose par défaut une authentification par le fichier /etc/passwd, auquel il convient si on décide d'en garder l'utilisation d'ajouter le mécanisme « Shadow », qui stocke les mots de passes et des données temporelles relatives aux comptes dans un fichier séparé, lisible uniquement par le super-utilisateur (root). L'intérêt de PAM est aussi de proposer une gestion fine des mécanismes de sessions utilisateurs, grâce aux quatre phases de son processus d'accès :

- Vérification que le compte utilisé existe, et est autorisé à se connecter au moment désiré, depuis l'endroit désiré.
- Authentification de l'utilisateur (grâce au mot de passe, ou à d'autres moyens, tels qu'une clé publique, mais nous y reviendrons lorsque nous parlerons de SSH.
- Mise à jour des mots de passes si besoin.
- Mise en place et fermeture de la session utilisateur, ce qui peut inclure des mécanismes d'audit, et une limitation de l'accès aux ressources

Le fichier PAM est composé de 4 colonnes :

- **Type de module :**
  - **auth** : authentification de l'utilisateur (LDAP...)
  - **account** : gestion des utilisateurs (restrictions horaires)
  - **session** : tâches à effectuer en début et fin de chaque session
    ex : montage de répertoires, contrôle des ressources
  - **password** : mise à jour du jeton d'authentification de l'utilisateur

- **Contrôle de réussite :**
    - **required** : la réussite d'au moins un des modules required est nécessaire
    - **requisite** : la réussite de tous les modules requisite est nécessaire
    - **sufficient** : la réussite d'un seul module sufficient est suffisant
    - **optional** : la réussite d'au moins un des modules required est nécessaire si aucun autre n'a réussi

- chemin du module, en général dans **/usr/lib/security** .
- arguments optionnels.

Le fichier **/etc/pam.d/other** fournit les configurations par défaut pour tout type de module non spécifié dans le fichier de configuration de l'application.

Voici quelques modules intéressants :

- **pam_cracklib** : ce module utilise la bibliothèque cracklib pour vérifier la solidité d'un nouveau mot de passe. Il peut également vérifier que le nouveau mot de passe n'est pas construit à partir de l'ancien.
- **pam_limits** : ce module permet de limiter les ressources accessibles à un utilisateur et/ou à un groupe comme le nombre de processus simultanés et leurs temps CPU, le nombre de fichiers ouverts simultanés et leurs tailles, le nombre de connexions simultanées, etc.
  La configuration se fait via le fichier **/etc/security/limits.conf**
- **pam_rootok** : permet à root l'accès à un service sans avoir à rentrer de mot de passe.
- **pam_time** : permet de limiter les horaires d'accès.
  La configuration se fait via le fichier **/etc/security/time.conf. [3]**

d. Le Super utilisateur : Un utilisateur particulier des systèmes Linux possède un UID égal à zéro. Son nom est généralement root (racine). Cet utilisateur a un contrôle proche du maximum sur la machine, c'est le compte le plus critique, qui a tous les droits, aux limitations physiques ou imposées par le noyau par exemple.

Le problème avec cet utilisateur est qu'il représente la principale faiblesse des systèmes Linux. Parce qu'il peut tout faire, si une personne arrive à récupérer les privilèges du super-utilisateur, elle peut virtuellement faire ce que bon lui semble. Dans ce cas, tous les systèmes de sécurités deviennent inutiles.

On peut limiter les pseudo-terminaux sur lesquels l'utilisateur peut se connecter, grâce au fichier /etc/securetty. Une configuration idéale pour la sécurité serait d'empêcher la connexion du super utilisateur par le réseau, et d'obliger le login en utilisant un autre compte, et en devenant root par la suite avec la commande « su », qui permet de changer d'identité.

e. **Les listes de contrôle d'accès (ACL) :** liste de permissions sur un fichier, un répertoire ou une arborescence, ajoutée aux permissions de ce fichier. Ces permissions concernent des utilisateurs et/ou des groupes définis.

Avec les ACL, on peut ajouter à un fichier d'autres utilisateurs et groupes et définir leurs droits séparément.

La mise en place des ACL permet une gestion fine des accès des utilisateurs, des groupes, aux répertoires et aux fichiers d'une partition qui dispose d'un système de fichier qui accepte les ACL (Ext3).

2.2 Systèmes de fichiers

1. **Arborescence et hiérarchie du système de fichier :** Le système de fichiers est la manière dont l'OS organise, maintient la hiérarchie des fichiers au sein des périphériques de stockage. Les utilisateurs du système voient une arborescence de fichiers uniques. Mais celle ci est en fait l'unification de plusieurs arbres, chacun de ceux-ci pouvant être stockés sur un disque local, ou être un arbre distant, par le réseau. Différentes arborescences contenant une catégorie de fichiers particulière peuvent être décrites ainsi :

Emplacement	Définition
/	Partition racine, base du système linux.
/root	Partition contenant les fichiers du super-utilisateur.
/boot	Partition contenant les fichiers de démarrage, tels les noyaux linux
/bin	Répertoire contenant des fichiers binaires exécutables système, donc primordiaux.
/dev	Les fichiers contenus dans /dev sont connus comme pilotes de périphériques; ils sont utilisés pour accéder aux périphériques et ressources du système, comme les disques durs, modems, mémoire, souris, etc.
/etc	Contient beaucoup de fichiers de configuration système, programmes et utilitaires, la plupart du temps appartenant au super-utilisateur.
/home	Contient traditionnellement les répertoires utilisateurs.
/lib	Contient les bibliothèques partagées. Ces librairies partagées contiennent le code que beaucoup de programmes partagent ensemble.
/mnt	Répertoire de montages généralement temporaires.
/proc	Signifie processus, c'est un système de fichiers "virtuel", les fichiers sont simulés en mémoire. Ils correspondent aux différents processus présents sur le système. On va y trouver des fichiers spéciaux permettant une interaction avec le noyau linux.
/sbin	Répertoire contenant aussi des binaires systèmes, appartenant à l'utilisateur.
/tmp	Répertoire de fichiers temporaires, en général liés au fonctionnement des programmes, ceux-ci doivent être effacés à la terminaison de ces programmes (doit être vide au démarrage initial d'un système).

/usr	Il contient un certain nombre de sous-répertoires qui à leur tour, contiennent les programmes ou les fichiers de configuration les plus utiles du système. Il contient donc l'essentiel des éléments de la distribution en cours d'utilisation.
/var	Contient des répertoires dont la taille est appelée à varier grandement et de manière potentiellement imprévisible.
/usr/local	Contient les fichiers locaux à la machine particulière sur laquelle elle se trouve. Sa structure est semblable à /usr.
/usr/src	Contient des fichiers sources des logiciels installés, /usr/src/linux contient ainsi les sources du noyau linux du système.
/usr/man	Contient les manuels du système.
/var/log	Contient les fichiers journaux du système.

Tableau 1 : Arborescences du système linux

La sécurité du fonctionnement d'un système est fortement influée par la manière dont celui-ci est organisé, grâce à différents systèmes de fichiers. Si un système de fichiers est endommagé, les dégâts seront ainsi limités à l'arborescence qu'il contenait. Une bonne division du système de fichier va permettre à l'administrateur de cloisonner l'espace pour certains utilisateurs ou programmes. Dans la mesure où les droits de création de certains utilisateurs sont limités à certains répertoires, l'administrateur est certain qu'ils n'auront pas plus d'espaces que celui disponible sur la partition de ce système de fichier.

b. Choix du système de fichiers : Le noyau Linux supporte différents systèmes de fichiers, ce qui permet à l'utilisateur d'avoir le choix entre ces différents systèmes. Le système de fichiers standard sous Linux est à l'heure actuelle *ext*. Ext fut créé par Wayne Davidson en collaboration avec Stephen Tweedie et Theodore Ts'o.

c. Sécurisation : Le système Linux est vu sous forme de fichiers, il est donc primordial de gérer correctement les droits sur ces fichiers et répertoires. Il ne faut pas que les droits sur les fichiers sensibles soient trop laxistes. L'accès à une ressource ou à une commande sensible peut compromettre l'ensemble du système en cas d'attaque. Les protections positionnées sur les fichiers (et donc les répertoires, qui sont eux aussi des fichiers, en fait) sont constitués de trois triplets qui correspondent aux permissions données au propriétaire (user, utilisateur) du fichier, au groupe du propriétaire (group, groupe), et au reste du monde (others, autres). Chaque triplet est composé du droit de lecture (r pour read, lecture), d'écriture (w pour write, écriture), et d'exécution (x pour execute, exécution). Les droits sont à toujours placer au plus restrictif

2.3 Réseaux

a. Pare-feu : (firewall) est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment internet). Le pare-feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau suivante :

- une interface pour le réseau à protéger (réseau interne) ;
- une interface pour le réseau externe.

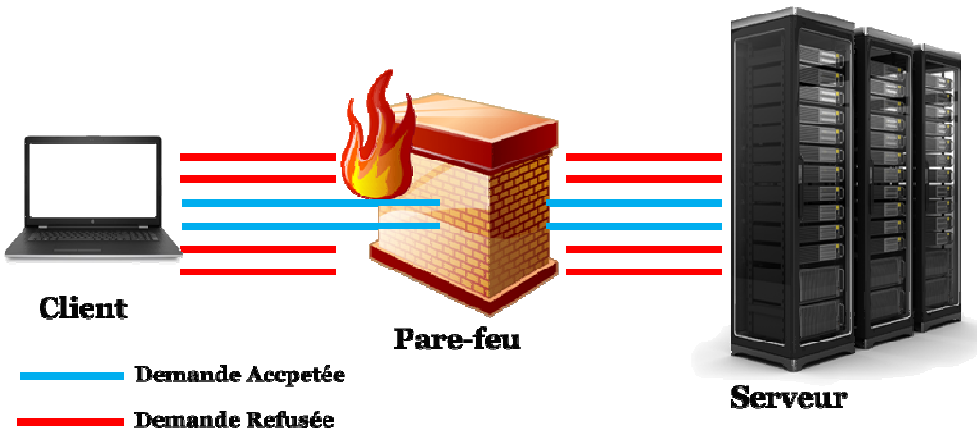

Figure 5 : Pare-feu

Le système firewall reposant parfois sur un matériel réseau dédié, constituant un intermédiaire entre le réseau local (ou la machine locale) et un ou plusieurs réseaux externes. Il est possible de mettre un système pare-feu sur n'importe quelle machine et avec n'importe quel système pourvu que :

- La machine soit suffisamment puissante pour traiter le traffic ;
- Le système soit sécurisé ;
- Aucun autre service que le service de filtrage de paquets ne fonctionne sur le serveur.

Dans le cas où le système pare-feu est fourni dans une boîte noire (clé en main), on se parle sur Appliance.

Pour le fonctionnement d'un système pare-feu, il contient un ensemble de règles prédéfinies permettant :

- D'autoriser la connexion (allow) ;
- De bloquer la connexion (deny) ;
- De rejeter la demande de connexion sans avertir l'émetteur (drop).

Un pare-feu fonctionne sur le principe du filtrage simple de paquets. Il analyse les en-têtes de chaque paquet de données (datagramme) échangé entre une machine du réseau interne et une machine extérieure. Les paquets de données échangées entre une machine du réseau extérieur et une machine du réseau interne transitent par le pare-feu et possèdent les en-têtes suivants, analysés par le firewall :

- adresse IP de la machine émettrice ;
- adresse IP de la machine réceptrice ;
- type de paquet (TCP, UDP, etc.) ;
- numéro de port. **[4]**

b. TCP/IP : La forge de paquet (IP spoofing), consiste à forger son identité pour cacher quelle est sa propre adresse IP. Cette technique peut permettre de pénétrer des réseaux, en faisant croire à un routeur qu'un paquet en fait issu d'Internet vient du réseau, et ainsi pénétrer le réseau.

Le noyau Linux permet également de se protéger des attaques de type Syn Flood, qui consiste à ouvrir un très grand nombre de connexion TCP, sans donner de suite à ces demande d'établissement de connexion, dans le but de saturer la table des connexions TCP de la couche réseau, jusqu'à paralysie du système.

c. Topologie : Il est primordial du point de vue de la sécurité d'avoir une architecture réseau cohérente. On va segmenter le réseau en différentes zones, une zone démilitarisée (DMZ) contenant les machines proposant des services vers Internet, et une zone contenant le reste du réseau, qui ne propose pas de service vers Internet. Si une machine ouverte vers Internet est ainsi compromise, les machines internes resteront en sécurité. Il convient donc de posséder au moins deux pare-feu, un en contact direct avec Internet, et un deuxième pour protéger le réseau interne. Le matériel d'interconnexion ne devrait compter que des routeurs et des commutateurs, si possible implémentant des réseaux virtuels, encore appelés VLAN, pour permettre une segmentation sans avoir à segmenter physiquement les machines.

d. Chiffrement des communications : Le chiffrement doit remplir les quatre fonctions importantes que sont l'authentification, l'intégrité, la confidentialité, la signature des communications. Différents types de chiffrement existent, on peut les diviser en deux catégories, les chiffrements symétriques, et les chiffrements asymétriques.

- **Le chiffrement symétrique :** aussi connu sous le nom de chiffrement à clé secrète utilise un mot de passe qui doit être connu de l'expéditeur comme du destinataire, ce mot de passe servant autant au chiffrement qu'au déchiffrement de ce qui a été chiffré. L'intérêt de cette méthode est sa rapidité d'exécution, ce qui fait qu'il est largement utilisé pour les communications réseau d'égal à égal. Son point faible est de devoir utiliser une clé secrète commune.

- **Le chiffrement asymétrique :** plus connu sous le nom de chiffrement à clé publique exige que chaque personne prenant part à une communication chiffrée possède sa propre paire de clés, celles ci allant par deux, une clé publique et une clé privée. Comme son nom l'indique, la clé publique est destinée à être diffusée largement, elle sert à chiffrer les données expédiées à son propriétaire, qui les déchiffre à sa guise avec sa clé privée.

e. **SSL :** (secure socket layer, couche de connexion sécurisée) est un protocole introduit par la société NetScape initialement, et est aujourd'hui très reconnu et très utilisé à but d'authentification et de chiffrement de connexions client-serveur. Un standard basé sur SSL a été normalisé par l'IETF (Internet Engineering Task Force). Il offre aux protocoles applicatifs qui l'utilisent des possibilités de chiffrement pour établir des connexions sécurisées.

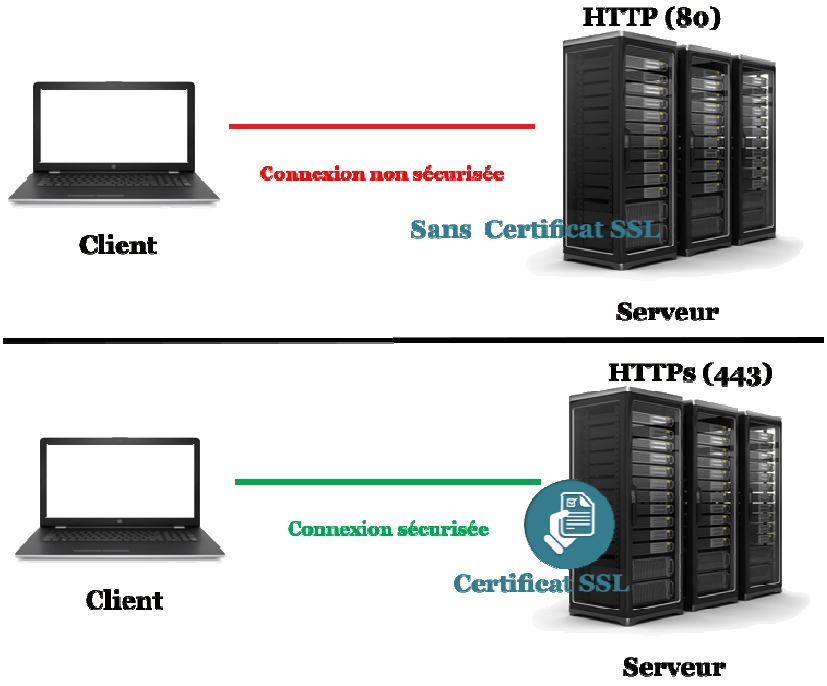

Figure 7 : Certificat SSL

f. **SSH :** (Secure Shell) est un protocole réseau sécurisé permettant l'ouverture de sessions interactives, l'exécution de commandes distantes, le transfert de fichiers, l'encapsulation de connexions TCP. SSH vient avec des mécanismes de chiffrement, mais aussi des mécanismes d'authentification forte.

SSH permettent de transférer des fichiers en toute sécurité, de travailler sur en hôte distant tout en ayant l'esprit tranquille.

2.4 Services

a. Configuration globale : Il convient de se limiter au strict nécessaire, de manière à limiter les failles. Donc tous les services inutiles au fonctionnement prévu de la machine doivent être désactivés, ou même désinstallés. Cela améliore la sécurité du système d'une part, et fait en sorte de libérer des ressources systèmes. **[2]**

b. TCPWrapper : est installé par défaut et fournit un contrôle d'accès basé sur l'hôte aux services réseau. Lorsqu'une tentative de connexion est effectuée sur un service TCP-wrapper, le service fait d'abord référence aux fichiers d'accès de l'hôte (***/etc/hosts.allow et /etc/hosts.deny***) pour déterminer si le client est ou non autorisé à se connecter. Si un client est autorisé à se connecter, TCP Wrappers libère le contrôle de la connexion au service demandé et ne participe plus à la communication entre le client et le serveur. Les règles dans ***hosts.allow*** ont priorité sur les règles dans ***hosts.deny*** .Vous ne pouvez avoir qu'une seule règle par service dans les fichiers ***hosts.allow*** et ***hosts.deny***. S'il n'y a pas de règles correspondantes dans l'un des fichiers ou si les fichiers n'existent pas, alors il est autorisé à accéder au service. Toute modification apportée aux fichiers ***hosts.allow*** et ***hosts.deny*** prend un effet immédiat. La syntaxe des fichiers ***host.allow*** et ***hosts.deny*** prend la forme suivante:

daemon : client [:option1:option2:...]

- **daemon** peut être une combinaison de ssh daemon, ftp daemon, portmap daemon, etc.
- **client** est une liste séparée par des virgules de noms d'hôtes, d'adresses IP d'hôte, de motifs spéciaux ou de caractères génériques spéciaux qui identifient les hôtes effectués par cette règle.
- **options** est une action facultative, comme par exemple envoyer un courrier à l'administrateur lorsque cette règle est associée, se connecter à un fichier particulier et ainsi de suite. Il peut également s'agir d'une liste séparée par deux points.

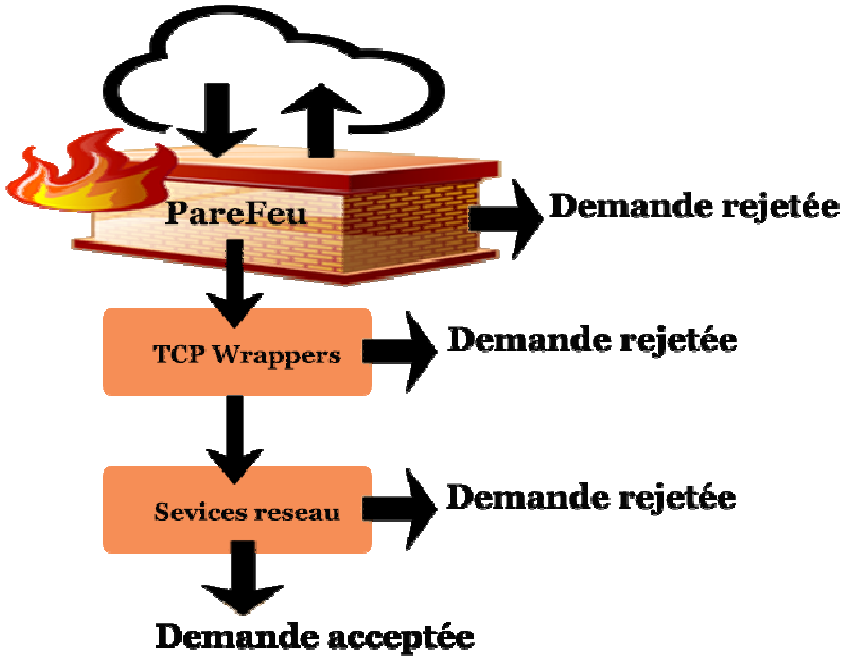

Figure 7 : TCPWrappers

TCP Wrappers offre les avantages suivants par rapport aux autres techniques de contrôle de service réseau:

- ***Transparence tant pour le client que pour le service réseau enroulé* :** Le client de connexion et le service réseau enroulé ignorent que TCP Wrappers est utilisé. Les utilisateurs légitimes sont enregistrés et connectés au service demandé alors que les connexions des clients interdits échouent.

- ***Gestion centralisée des protocoles multiples* :** TCPWrappers fonctionne séparément des services réseau qu'ils protègent, permettant à de nombreuses applications serveur. de partager un ensemble commun de fichiers de configuration de contrôle d'accès, ce qui permet une gestion plus simple.

c. **Cron :** est un utilitaire permettant l'exécution de tâches planifiées à intervalles réguliers. On peut spécifier qui a le droit de créer des tâches planifiées avec les fichiers /etc/cron.allow et /etc/cron.deny, on n'autorisera que les utilisateurs potentiellement appelés à en créer, et en l'interdisant par défaut.

d. Autres services : Les services réseaux sont particulièrement exposés, car ils ne sont pas utilisables par les seuls utilisateurs d'une machine mais par toute machine du réseau et/ou d'Internet. S'il est facile de filtrer les accès non prévus avec le pare-feu externe, ou des règles d'accès sur un routeur, certains services ont pour vocation d'être publics. On surveillera alors très attentivement les alertes de sécurité sur les logiciels ou bibliothèques sur lesquelles reposent les services utilisés.

2.5 Le noyau Linux

La configuration de son noyau Linux est primordiale, dans la mesure où celui ci constitue le cœur du système d'exploitation Linux, et défini le comportement, entre autres, de la couche réseau du système. On recompilera donc le noyau pour qu'il colle aux besoins sur la machine sur laquelle il se trouvera.

2.6 Sauvegarde

Avoir des systèmes sécurisés signifie avoir un accès sûr aux données. Les différents incidents qui pourraient compromettre celles-ci ne sont pas prédictibles, et malheureusement malgré une politique très bien pensée et appliquée, ils ne peuvent parfois pas être évités. Et si les assurances couvrent les dégâts matériels, les pertes de données peuvent être définitives, et donc non récupérables à moins de tout régénérer, ce qui n'est pas toujours possible.

L'établissement d'un plan de sauvegarde doit se faire au cas par cas, il est dur d'établir une politique qui serait considérable comme absolue à ce vaste problème. On peut toutefois citer les questions à se poser pour établir le plan de sauvegarde.

- Que faut-il sauvegarder?
- A quelle fréquence?
- Combien de temps conservera-t-on les sauvegardes, à quel endroit, en combien d'exemplaires?
- A quel endroit sera stocké l'historique de ces sauvegardes?
- Quel support de sauvegarde utilisera-t-on?

- Quels sont les besoin en matière de capacité?
- Combien de temps la sauvegarde peut-elle durer?
- Combien de temps mettra-t-on à restaurer un fichier? Une machine complète?
- Le mécanisme de sauvegarde sera-t-il automatique ou manuel?

2.7 Sécurité physique du serveur

Toutes les sécurités systèmes imaginables sont inutiles si la sécurité physique n'est pas prise en compte. La sécurité physique vise à conserver l'intégrité matérielle des équipements informatiques. Les risques physiques sont davantage liés aux évènements imprévisibles comme les pannes, les accidents ou encore les atteintes intentionnelles aux matériels. On peut énumérer quelques dangers physiques :

- Feu, Fumée, Poussière.
- Catastrophes naturelles (forte chaleur, grand froid, tremblement de terre,...)
- Explosion.
- Bruit électromagnétique.
- Vibration.
- Humidité, Liquides.
- Terminaux laissé ouverts sans verrouillage de la console.

Tous sont à prendre en compte lors de la conception du lieu d'exploitation (Datacenter) qui sera appelé à contenir tout ou partie du système final.

2.8 Journalisation, audit, et surveillance

a. Syslog : est un logiciel de base des systèmes Linux, c'est un système de journalisation des messages produits par le système et les logiciels. Il offre la possibilité de les archiver localement, dans des fichiers, ou bien de les envoyer vers une machine du réseau, qui sera par exemple destinée à recevoir tous les logs des autres machines du réseau. Tous les problèmes peuvent donc être détectés grâce à une analyse de ces fichiers journaux.

b. **RootKits :** est un logiciel qui permet de rechercher si un rootkit est installé sur sa machine. Un RootKit est un ensemble de programmes permettant d'infecter une machine tout en cachant ces traces. Il remplace un certain nombre d'outils système (ls, ps, netstat ...) pour que les utilisateurs de la machine ne puissent pas voir ces traces, des personnes malveillantes arrivent à l'installer suite à l'exploitation d'une faille dans un système. Un passage de ce logiciel chaque nuit, avec un envoi des résultats et une analyse de ceux ci chaque jour est un bon moyen de détecter au plus vite la compromission d'une machine. L'exécution de ce logiciel devrait faire partie de tout audit sécuritaire d'une machine Linux.

c. **Audit réseau :** Les audits réseaux permettent de détecter d'éventuelles failles réseaux. on pourra distinguer deux types d'outils parmi d'autres, on verra un scanner, et un logiciel de vérification de failles. Un scanner extrêmement connu est Nmap, ce type de logiciel tente d'établir des connexions sur des ports d'une machine, permettant de vérifier quels ports sont en écoute sur cette machine. On peut aussi analyser toute une étendue de machines. Il convient de surveiller si tous les services en écoute le sont bien de par la volonté du mainteneur de la machine. **[2]**

Conclusion

La sécurité informatique est constituée par des applications et services reliés entre eux et dépendant les uns des autres ; il suffit qu'un seul maillon soit vulnérable pour que toute la chaine perde son efficacité. Nous devons donc veiller à ce que cette suite des opérations soit toujours hermétique et inviolable.

Chapitre 3 :

Etude de l'existant

1. Introduction

L'université de Ouargla est l'un des plus importants universités du pays ; elle dispose d'un système informatique performant pour gérer les multiples fonctions des diverses facultés et administrations. Ce système névralgique est d'une importance capitale pour le bon fonctionnement de l'université ; il utilise une technologie de pointe et son fonctionnement est assuré par un personnel spécialisé qui bénéficie d'une formation continue.

Dans ce chapitre, nous avons étudié la composition de l'existant et relevé les problèmes rencontrés dans son exploitation. Nous verrons donc la liste des équipements utilisés et nous passerons ensuite en revue les problèmes rencontrés.

2. Présentation de l'Université

L'université Kasdi Merbah Ouargla tire ses origines de l'Ecole Normale Supérieure (E.N.S.) érigée par le Décret n° 65-88 du 22 mars 1988. En 1997, par le Décret n°159-97 du 10 mars 1997 est créé le Centre Universitaire de Ouargla qui regroupe désormais sous son autorité l'Institut national de Formation Supérieure en Agronomie Saharienne (INAFSAS – Décret n°337-97 du 10 septembre 1997) au côté des 05 instituts fondateurs :

- Institut d'Agronomie saharienne
- Institut des sciences exactes
- Institut de Droit et sciences politiques
- Institut des Lettres et Langues
- Institut des Sciences Economiques et Sciences Sociales

L'Université kasdi Merbah-Ouargla se compose actuellement de 10 facultés ; chacune d'elles compte plusieurs départements conformément aux textes en vigueur, notamment le Décret exécutif n° 13-100 du 2 Joumada El Oula 1434 correspondant au 14 mars 2013 modifiant et complétant le Décret exécutif n° 01-210 du 2 Joumada El Oula 1422 correspondant au 23 juillet 2001 portant création de l'université de Ouargla.. Le nombre et la vocation des facultés composant l'Université Kasdi Merbah Ouargla sont fixés comme suit :

- Faculté des Mathématiques et des Sciences de la Matière (FMSM)

- Faculté des Nouvelles Technologies de l'Information et de la Communication (FNTIC)
- Faculté des Sciences Appliquées (FSA)
- Faculté des Hydrocarbures, des Energies Renouvelables, des Sciences de la Terre et de l'Univers (FHERSTU)
- Faculté des Sciences de la Nature et de la Vie (FSNV)
- Faculté des Sciences Economiques, Commerciales et des Sciences de Gestion (FSECSG)
- Faculté de Droit et des Sciences Politiques (FDSP)
- Faculté des Lettres et des Langues (FLL)
- Faculté des Sciences Humaines et Sociales (FSHS)
- Faculté de Médecine (FM)

et deux instituts à savoir:

- Institut des Sciences et Techniques des Activités Physiques et Sportives (ISTAPS)
- Institut de Technologie (IT)

Le rectorat de l'Université Kasdi Merbah Ouargla se situe sur la route de Ghardaïa. Trois grands campus composent l'architecture principale de l'Université. Depuis le 05 septembre 2005, l'Université porte désormais le nom de "Université Kasdi Merbah Ouargla".

3. Présentation de l'architecture de système informatique de l'université :

La source du système informatique de l'université est le Centre des Systèmes et Réseaux d'Information et de la Communication, Télé-enseignement et la visioconférence, Ce centre a 3 services :

- Service des Systèmes ;
- Service des Réseaux d'Information et de la Communication ;
- Service du Télé-enseignement et la visioconférence.

En termes d'équipement, l'université est parmi les universités qui ont un équipement de haute technologie, ce dernier est utilisé pour héberger les divers sites qui fournissent les services de l'université pour garantir la bonne diffusion de l'information. Les sites de l'université sont :

- Site principale : https://www.univ-ouargla.dz
- Messagerie électronique : https://mail.univ-ouargla.dz
- Bibliothèque électronique : https://bu.univ-ouargla.dz
- Télé-enseignement : https://elearn.univ-ouargla.dz
- Revues : https://revues.univ-ouargla.dz
- Manifestation : https://manifest.univ-ouargla.dz
- Sites des facultés : https://facultes.univ-ouargla.dz
- Dspace : https://dspace.univ-ouargla.dz

Nous avons fait une analyse de la situation existante pour relever les équipements matériels et logiciels du centre S.RCI.TV .qui figurent dans le tableau suivant :

Equipement	Datacentre FUJITSU Serveurs PRIMERGY (Blades)
	Pour chaque Blade : • Ram 64Go • 12 CPUs * 1.999GHz • 4 NICs
	2 Baies de stockage 3T
Technologie	Virtualisation VMware
Hyperviseur	vSphere ESXi
Systèmes exploitation dans les machines virtuelles	Centos 7
Pare-feu	ASA

Tableau 2 : Architecture du système informatique de l'UKMO

4. Schéma de la structure du Datacenter du l'UKMO

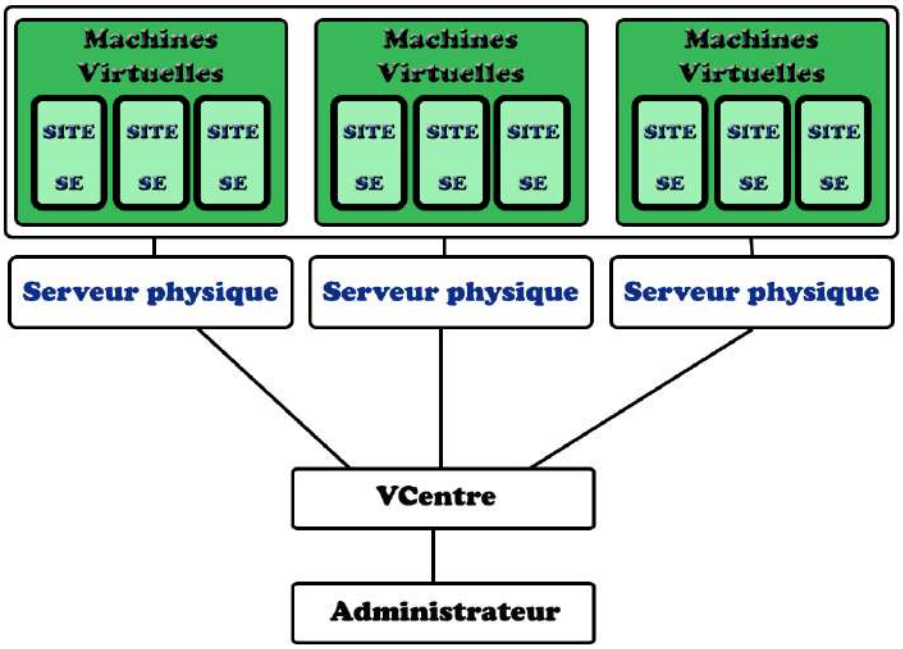

Figure 7 : Schéma de la structure du Datacenter du l'UKMO

5. Problèmes rencontrés dans les divers serveurs de l'université

- Problème du poussier à cause de la nature de la région (problème du vent de sable).
- Problème d'électricité : nombreuses chutes de tension, coupures fréquentes
- Problème de stockage (saturation).
- Problème des ruptures dans le trafic réseau.
- Problème des attaques par SSH.
- Problème des DOS.
- Absence d'équipement de secours.

6. Conclusion

L'université d'Ouargla dispose d'un centre informatique bien équipé. Nous avons passé en revue les équipements composant le système et nous avons recensé quelques problèmes auxquels nous avons proposé des solutions qui figureront au chapitre suivant.

Chapitre 4 :

Les recommandations

1. Introduction

Nous venons de voir, dans le chapitre précédent, que le système informatique rencontre des problèmes qui altèrent son fonctionnement et peuvent donc se répercuter sur les résultats qu'il donne. Après avoir recensé ces anomalies, nous les avons étudiées pour leur trouver des solutions. Nous présentons, ci-contre, les solutions et les préconisations pour pallier à ces défauts.

2. Les recommandations de la sécurité (politique de sécurité proposée) :

2.1 Protection physique :

- Il est fortement recommandé d'utiliser des onduleurs pour assurer une sécurité électrique.
- Il est fortement recommandé de sécuriser l'accès physique au serveur aux seules personnes ayant droit.
- En cas de mise au rebut du serveur, il est fortement recommandé de physiquement détruire les disques durs.
- Utilisez le verrouillage et la vidéosurveillance.

2.2 Baser sur une installation minimale et Supprimer les paquets logiciels inutiles :

- Utiliser l'installation minimale du système dans le cas où la machine est destinée à être utilisée toute sa vie en tant que serveur.
- Installer un logiciel minimal requis pour le serveur.
- Documentez les plus importantes manipulations sur le serveur (sauvegarde, mise en arrêt, démarrage,...).
- Il est fortement recommandé de mettre à jour régulièrement le système d'exploitation ainsi que les applications du serveur, pour combler les vulnérabilités des anciennes versions. L'exploitation de ces vulnérabilités peut provoquer une corruption du fonctionnement du serveur ou un vol respectivement une destruction des fichiers et éventuellement des détournements des flux de données.

- Restreindre la fonctionnalité du serveur à une seule tâche et de n'héberger aucune autre application sur ce même serveur virtuel, respectivement physique.

- Ne jamais installer de programmes ou de services supplémentaires, et installer les packages uniquement à partir de référentiels fiables ou officiels.

Par exemple pour vérifier les packages installés en utilisant la commande suivante:

```
#rpm -qa
```

2.3 Mettre à jour fréquemment le système :

- Mettre à jour régulièrement le système.

- Garder le noyau Linux en synchronisation avec les derniers correctifs de sécurité et tous les logiciels installés à jour avec les dernières versions en émettant la commande ci-dessous:

```
# yum update
```

2.4 Sécuriser la politique des mots de passe : Par l'ajout de cette ligne dans le fichier /etc/login.defs.

```
pass_min_len 14 pass_min_days 1 pass_max_days 60
```

2.5 Définir la dernière connexion / notification d'accès : Ajouter la ligne suivante dans le fichier /etc/pam.d/system-auth après la session requise pam_limits.so:

```
session required pam_lastlog.so showfailed
```

2.6 Tentatives de connexion au mot de passe maximales par session : Définir le nombre de tentatives d'entrer le mot de passe par session, en éditant l'instruction pam_pwquality.so dans /etc/pam.d/system-auth pour retry=3 ou moins.

2.7 Définir le refus pour les tentatives de mot de passe échouées : Bloque les connexions pour l'authentification échouée sur les comptes par l'ajoute des lignes suivantes sous l'instruction pam_unix.so dans la section AUTH de /etc/pam.d/system-auth et /etc/pam.d/password-auth :

```
auth [ default = die] pam_faillock.so authfail deny = 3 unlock_time = 604800 fail_interval = 900
```

2.8 Définir le mot de passe du chargeur de démarrage : Le chargeur de démarrage grub devrait avoir un compte super utilisateur et une protection par mot de passe activée pour protéger les paramètres de démarrage.

2.9 Exiger une authentification pour un mode utilisateur unique : Exiger le mot de passe racine lors de la saisie du mode utilisateur unique, ouvrir /etc/sysconfig/init et ajouter la ligne:

```
SINGLE = /sbin/sulogin
```

2.10 Désactiver l'activation Ctrl-Alt-Del Reboot : Prévert ALT + CTRL + DEL depuis le redémarrage. Ouvrir /etc/init/control-alt-delete.conf et modifier la ligne existante:

```
exec /sbin/shutdown -r now "Control-Alt-Delete pressed"
```

À:

```
exec /usr/bin/logger -p security.info "Control-Alt-Delete pressed"
```

2.11 Activer le verrouillage de l'écran de la console : Installer l'écran Package pour permettre le verrouillage de l'écran de la console. Les utilisateurs peuvent exécuter et verrouiller la console avec ctrl+ax.

```
#yum install screen
```

2.12 Désactiver le support IPv6 dans le chargement automatique: Ouvrir /etc/modprobe.d/disabled.conf et ajouter la ligne:

```
options ipv6 disable = 1
```

2.13 Désactiver l'utilisation de l'interface IPv6 : Ajouter ce qui suit à /etc/sysconfig/network

```
NETWORKING_IPV6 = no IPV6INIT = no
```

2.14 Sécurisation des connexions racines : Autoriser uniquement les connexions root via le terminal local:

```
echo "tty1" > /etc/securetty chmod 700 /root
```

2.15 Sécuriser par TCP Wrappers : exemples d'applications TCP Wrapper sont sshd. Les commandes ci-dessous bloquent tout sauf SSH:

```
echo "ALL:ALL" >> /etc/hosts.deny echo "sshd:ALL" >> /etc/hosts.allow
```

2.16 Règles de base du pare-feu iptables : Règles de base du pare-feu iptables, définies par défaut comme valeur par défaut.

2.17 Vérifier iptables Activé

```
systemctl enable iptables

systemctl start iptables.service
```

2.18 Désinstaller DHCP Server Package : Si vous n'avez pas besoin d'un client DHCP, supprimez-le:

```
#yum erase dhcp
```

2.19 Désactiver le client DHCP : Ouvrir /etc/sysconfig/network-scripts/ifcfg-eth0 (si vous avez plus d'interfaces, faites-en pour chacun) et assurez-vous que l'adresse est affectée de façon statique avec BOOTPROTO = none

```
BOOTPROTO = none NETMASK = 255.255.255.0 IPADDR = 192.168.1.2
GATEWAY = 192.168.1.1
```

2.20 Sécuriser l'Accès SSH : Chaque fois que nous installons, configurons et sécurisons des serveurs Linux dans un environnement de production, il est très important de garder une trace de ce qui se passe avec les serveurs. Ce n'est pas une bonne pratique d'autoriser la connexion racine directe par session SSH et de recommander de créer des comptes non root**.** Chaque fois que l'accès à la racine est nécessaire, connecter en tant qu'utilisateur normal, puis utiliser **su** pour passer à l'utilisateur **root**. Pour désactiver les connexions directes de la racine SSH et pour désactiver l'accès SSH via des mots de passe vides, ouvrir /etc/ssh/sshd_config et assurez-vous que la ligne suivante existe:

```
PermitRootLogin no

PermitEmptyPasswords no
```

Ajouter une entrée au fichier ***.bashrc*** . Ce fichier définit les variables d'environnement locales aux utilisateurs et effectue certaines tâches de connexion. C'est un moyen simple de savoir quand quelqu'un a ouvert ses portes en tant qu'utilisateur root ou normal, il doit envoyer une notification d'alerte par courrier électronique à l'adresse email spécifiée ainsi que l'adresse IP de la dernière connexion. Ainsi, une fois que vous connaissez l'adresse IP de la dernière connexion effectuée par un utilisateur inconnu, vous pouvez bloquer la connexion SSH de l'adresse IP particulière sur Firewall iptables**.**

echo 'ALERT - Raccourcis Shell Access (ServerName) sur:' `date`` who`| mail -s "Alerte: Accès racine de` who | cut -d '(' -f2 | cut -d ')' -f1` "votre_email.com

Une autre méthode est l'authentification par le couple de clés RSA (clé privé et clé public). Le couple de clés RSA stocké dans le répertoire /etc/ssh/ et généré lors de l'installation du serveur. Le fichier ssh_host_rsa_key contient la clé privée et a les permissions 600. Le fichier ssh_host_rsa_key.pub contient la clé publique et a les permissions 644.

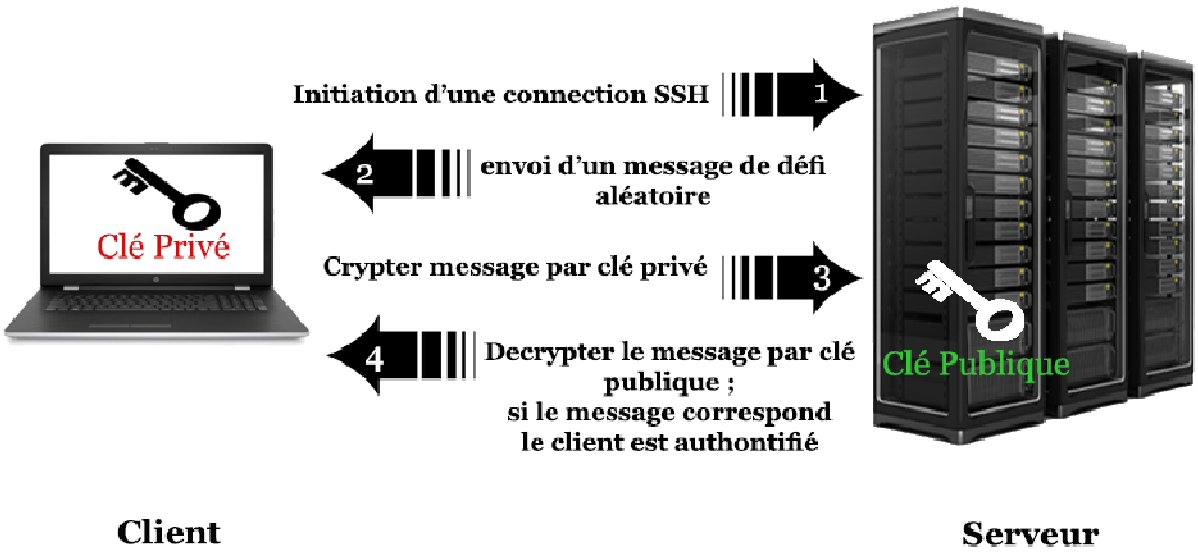

Figure 8 : Authentification par les clés RSA

Pour garantir une sécurité plus efficace dans SSH on va créer un script qui nous envoie un fichier texte qui va contenir les connexions échouées et celles réussies. On recommend de configure l'envoi de courier chaque 30 minutes.

```
#!/bin/bash
touch notification.txt
echo "To: [votre email]" > notification.txt
echo "From: SSH-Login-Alert@[votre serveur].com" >> notification.txt
echo "Subject: SSH Login" >> notification.txt
echo "" >> notification.txt
echo "LOGINS SECURISER" >> notification.txt
cat /var/log/secure | grep -s "Accepted password for" >> notification.txt
echo "" >> notification.txt
cat /var/log/secure | grep -s "Failed password" >> notification.txt
echo "" > notification.txt
echo "LOGINS MESSAGES" >> notification.txt
cat /var/log/messages | grep -s "is now logged in" >> notification.txt
echo "" >> notification.txt
cat /var/log/messages | grep -s "Authentication failed for" >> notification.txt
echo "" >> notification.txt
/usr/sbin/sendmail -t < notification.txt
rm -rf notification.txt
```

2.21 Crypter les données transmises : N'utiliser pas de protocoles non sécurisés pour l'accès à distance ou le transfert de fichiers tels que les **protocoles Telnet** , **FTP** ou d'autres protocoles de texte brut tels que SMTP, http ou NFS, ne chiffrent pas les sessions d'authentification ou les données envoyées. Utiliser uniquement sftp , scp pour les transferts de fichiers et SSH. Afin de tunnelier une console VNC via SSH, utilisez l'exemple ci-dessous qui transmet le port VNC 5901 de la machine distante à votre machine locale:

```
#ssh -L 5902: localhost: 5901 remote_machine
```

2.22 Pare-feu de filtrage de paquets : Utiliser l'utilitaire ***firewalld*** pour protéger les ports système, ouvrir ou fermer des ports de services spécifiques, en particulier des

ports bien connus (<1024). Installer, démarrer, activez et répertorier les règles du pare-feu en émettant les commandes ci-dessous:

```
#yum install firewalld

#systemctl start firewalld.service

#systemctl enable firewalld.service

#firewall-cmd --list-all
```

2.23 Inspecter les paquets de protocole avec tcpdump : Utiliser l'utilitaire **tcpdump** pour renifler des paquets réseau localement et inspecter leur contenu pour un trafic suspect (ports source-destination, protocoles tcp / ip, trafic couche deux, requêtes ARP inhabituelles). Pour une meilleure analyse du fichier capturé par **tcpdump** , utiliser un programme plus avancé tel que **Wireshark** .

```
#tcpdump -i eno16777736 -w tcpdump.pcap
```

2.24 Numérisation du port réseau : Effectuer des contrôles de port externes à l'aide de l'outil nmap à partir d'un système distant sur le réseau local. Ce type de balayage peut être utilisé pour vérifier les vulnérabilités du réseau ou tester les règles du pare-feu.

```
#nmap -sT -O 192.168.1.10
```

2.25 Configuration sécurisé du serveur Apache - SSL: Le module ***mod_ssl*** est un module de sécurité pour le serveur HTTP Apache. Le module ***mod_ssl*** utilise les outils fournis par OpenSSL pour ajouter une fonctionnalité très importante au serveur Apache la possibilité de chiffrer les communications. Les communications HTTP régulières entre un navigateur et un serveur web sont envoyées en texte clair, qui pourraient être interceptées et lues par quelqu'un le long de l'itinéraire entre le navigateur et le serveur.

2.26 Configuration sécurisé du serveur Apache - DOS: Le module Apache ***mod_evasive***, contribue à protéger contre les attaques DoS et la force brute sur le serveur web Apache. Il peut fournir une action évasive pendant les attaques et signaler des abus par courrier électronique et les installations de syslog. Le module fonctionne en créant une table dynamique interne d'adresses IP et d'URI ainsi que de refuser toute adresse IP unique de l'une des options suivantes:

- Demander la même page plusieurs fois par seconde.
- Faire plus de 50 demandes simultanées sur le même enfant par seconde.
- Faire toutes les demandes alors que temporairement.

Conclusion

Les mesures de sécurité sont des mesures comportementales, organisationnelles ou techniques qui cherchent à garantir la confidentialité, l'intégrité et la disponibilité d'un actif. Les mesures de sécurité cherchent à réduire les vulnérabilités exploitées par les menaces pour ainsi réduire les impacts. Les recommandations que nous avons faites peuvent être efficaces mais, malgré ça, il faudra veiller à les actualiser toujours et les améliorer pour prémunir contre les attaques qui abiment la stabilité et bon fonctionnement du système.

Conclusion

Notre travail a consisté à étudier les moyens d'assurer la sécurité informatique du serveur de l'université d'Ouargla. Ce dernier est doté d'une puissance appréciable, il assure le traitement, la transmission et le stockage d'une grande quantité d'informations aussi diversifiées qu'importantes.

La sécurisation des serveurs est primordiale pour une entreprise, à cet effet ceci requiert toute l'attention des responsables. Nous avons conçu un travail pour la sécurisation du serveur qui permettra une bonne maitrise des risques qui menacent le système ; ceci sera un premier pas vers une sécurisation optimale. Nos recommandations devront être correctement mises en pratique et renforcées par une surveillance contenue du serveur.

Comme tout système informatique ce serveur est exposé à des menaces, notre présent travail consiste à appliquer des solutions de protection contre ces menaces ; cependant quelque soit l'efficacité de la sécurisation que nous avons apportée elle reste toujours perfectible, nous souhaitons bon courage aux collègues qui nous suivront pour apporter encore des améliorations. L'actualisation des systèmes et la formation continue maintiennent les performances du serveur.

Bibliographie

[1] . Bernard Cousin, Université de Rennes 1, Sécurité des réseaux Informatiques, http://www.irisa.fr/prive/bcousin/Cours/1-Securite-des-reseaux.2P.pdf

[2] . Charles-Antoine Guillat-Guignard, Sécurité des systèmes GNU/Linux, http://contrib.xarli.net/secure-gnulinux/index.html.

[3] . Denis Ducamp / Hervé Schauer, Cours Sécurité Linux, http://www.hs-c.fr/ressources/cours/linux/SecLinux.htm

[4] . Firewall (pare-feu), http://www.commentcamar-che.net/contents/992-firewall-pare-feu

[5] . Mickael Dorigny, Qu'est ce que la sécurité de l'information ?, https://w-ww.information-security.fr/quest-ce-que-la-securite-de-linformation

[6] . Renaud Dumont, Cryptographie et Sécurité informatique, http://www.montefiore.ulg.ac.be/~dumont/pdf/crypto.pdf

[7] . Sécurité du système d’information (SSI) 3 IAG, http://ayarimanel.y.a.f.unblog.fr/files/2010/11/securiteinformatiquechap2.ppt.

[8] . Solange Ghernaouti-Hélie , Sécurité informatique et réseaux, Edition Dunod.

Acronymes utilisés

ACL : *Access Contrôle Liste*

ASA : *Adaptive Security Appliance*

CIA : *Confidentialité, Intégrité, Disponibilité*

DHCP : *Dynamic Host Configuration Protocol*

DMZ : *Demilitarized Zone*

DOS : *Distributed Denial Of Service*

GID : *Group Identification*

HTTPs : *Hypertext Transfer Protocol Secure*

ICMP : *Internet Control Message Protocol*

IETF : *Internet Engineering Task Force*

IP : *Intenet Protocol*

ISO : *Organisation Internationale De Normalisation*

LDAP : *Lightweight Directory Access Protocol*

PAM : *Pluggable Authentication Modules*

SSH : *Secure Shell*

SSL : *Secure Socket Layer*

TCP : *Transmission Control Protocol*

UDP : *User Datagram Protocol*