N° d'ordre : 08 / RS / TCO Année Universitaire : 2017/ 2018

**UNIVERSITE D'ANTANANARIVO**

**----------**

**ECOLE SUPERIEURE POLYTECHNIQUE**

**----------**

**MENTION TELECOMMUNICATION**


MEMOIRE

en vue de l'obtention

du DIPLOME de Licence

*Domaine :* Sciences de l'Ingénieur

*Mention* : Télécommunication

*Parcours* : RS

*par* : **RANDRIANARISOA Antsaniaina Christian**

# *SÉCURISATION D'UN DMZ : TEST DE PÉNÉTRATION ET MISE EN PLACE D'UN SYSTÈME DE MONITORING*

Soutenu le **Lundi 06 mai 2019** devant la Commission d'Examen composée de :

Président :

M. RAVONIMANANTSOA Ndaohialy Manda-Vy

Examinateurs :

M. RATSIMBAZAFY Andriamanga

M. ANDRIAMANALINA Ando

Mme RAMAFIARISONA Hajasoa Malalatiana

Directeur de mémoire : M. RANDRIARIJAONA Lucien Elino

## REMERCIEMENTS

Tout d'abord je tiens à rendre grâce à Dieu de m'avoir donné le courage, l'enthousiasme, la volonté ainsi que la force nécessaire pour la réalisation de ce mémoire. Je tiens aussi à exprimer ma profonde gratitude aux quelques personnes suivantes sans qui le présent travail n'aurait pas pu être réalisé :

Monsieur RAVELOMANANA Mamy, Professeur Titulaire, Président de l'Université d'Antananarivo.

Monsieur RAKOTOSAONA Rijalalaina, Professeur Titulaire, Responsable du Domaine Sciences de l'Ingénieur de l'Ecole Supérieure Polytechnique d'Antananarivo.

Monsieur RAKOTONDRAINA Tahina Ezéchiel, Maître de Conférences, Responsable de la Mention Télécommunication.

Monsieur RANDRIARIJAONA Lucien Elino, Assistant d'Enseignement et de Recherche, en tant que Directeur de mémoire et Encadreur pédagogique.

Monsieur, RAVONIMANANTSOA Ndaohialy Manda-Vy, Maitre de Conférence, Docteur HDR.

Madame RAKOTO Harimino, Directeur général de l'Institut INSCAE.

Monsieur ANDRIAVELONERA Anselme Alexandre, responsable du centre informatique de l'Institut INSCAE et Encadreur professionnel, Ingénieur Informaticien.

Les membres du jury, d'avoir accepté d'examiner ce travail malgré leurs occupations :

− Monsieur RATSIMBAZAFY Andriamanga, Maitre de Conférence.

− Monsieur ANDRIAMANALINA Ando, Maitre de Conférence, Docteur HDR.

− Madame RAMAFIARISONA Hajasoa Malalatiana, Maître de Conférence, Docteur HDR.

Les enseignants et tout le personnel de l'ESPA.

Mes parents, les membres de ma famille, mes collègues, mes amis et tous ceux qui de près ou de loin ont contribué à l'aboutissement de ce travail.

## TABLE DES MATIÈRES

## NOTATIONS

Abréviations

| | |
|---|---|
| ACK | Acknowledgement |
| ARP | Address Resolution Protocol |
| CIA | Central Intelligence Agency |
| DDoS | Distributed Denial of Services |
| DMZ | Demilitarized Zone |
| DNS | Domain Name Service |
| DoS | Denial of Service |
| DPI | Deep Packet Inspection |
| ICMP | Internet Control Message Protocol |
| INSCAE | Institut National des Sciences Comptable et d'administration d'Entreprise |
| IP | Internet protocol |
| ITU | International Telecommunication Union |
| LAN | Local Area Network |
| MAC | Medium Access Control |
| MITM | Man In The Middle |
| OS | Operating System |
| PC | Personal Computer |
| RAM | Random Access Memory |
| SMS | Short Message Service |
| SQL | Structured Language Query |

| | |
|---|---|
| SQLi | Structured Language Query injection |
| SSH | Secure SHell |
| SSL | Secure Sockets Layer |
| SYN | Synchronization |
| SYN-ACK | Synchronization- acknowledgement |
| TCP | Transport Control Protocol |
| UDP | User Datagram Protocol |
| UCS | Unified Computing System |
| URL | Uniform Ressource Location |

# INTRODUCTION GÉNÉRALE

Actuellement, l'utilisation d'Internet est une activité journalière pour une entreprise. Or l'exposition d'une entreprise à Internet engendre des risques. La sécurité informatique n'est plus un luxe, en fait aucune entreprise ne peut s'en passer. Elle devient un besoin fondamental pour tout organisme ayant un système d'information.

Le domaine de la sécurité informatique est en perpétuelle évolution dans le monde actuel où l'on vit. De nombreuses attaques émergent tous les jours et menacent les entreprises qui ont une présence sur Internet.

En matière de sécurité informatique, la question à se poser n'est pas de savoir "si" les attaques vont se produire, mais "quand" les attaques vont se produire. Les menaces sont réelles et les attaques peuvent frapper à tout moment sans prévenir. Ignorer la sécurité informatique pour économiser de l'argent au niveau d'une entreprise est une erreur courante.

En plus, la mise en place de mesure défensive en matière de sécurité informatique au sein d'une entreprise n'est plus suffisante. En fait, il est nécessaire de savoir comment les attaquants procèdent lors des attaques et surtout il est nécessaire de trouver les failles des systèmes avant ces personnes malveillantes. D'où la nécessité de mettre en œuvre de mesure offensive pour l'anticipation des actions des attaquants et pour augmenter la sécurité des systèmes d'information.

C'est dans ce cadre que ce mémoire a été dirigé : « Sécurisation d'un DMZ : Test de pénétration et mise en place de système de monitoring ».

Cet ouvrage est divisé en quatre chapitres. Le premier chapitre se concentrera sur ce qu'on appelle la sécurité informatique et introduira les concepts clés de cette dernière.

Le deuxième chapitre consistera à explorer les différents types d'attaques informatiques ainsi que les différentes méthodes pour la mise en œuvre de ces attaques.

Le troisième chapitre parlera de différents outils et techniques qu'on peut utiliser pour sécuriser un système informatique.

Le dernier chapitre concerne la démarche qu'on a suivie pour la sécurisation du DMZ de l'INSCAE, l'organisme d'accueil, ainsi que la réalisation d'une simulation d'attaque et une série de tests pour évaluer l'efficacité des mesures mise en place.

# CHAPITRE 1 SÉCURITÉ INFORMATIQUE

## 1.1 Introduction

Dans ce chapitre, on va développer le concept de sécurité informatique et les différents types de cette dernière. On verra tout d'abord quelques notions de base en sécurité informatique, ensuite on va voir les buts visés par cette dernière ainsi que ses différents aspects.

## 1.2 Définitions

### *1.2.1 Système d'information*

C'est un système d'organisation des activités consistant à acquérir, stocker, exploiter, transformer, gérer les informations et produire des services. [1]

Pour le bon fonctionnement des systèmes d'information, on utilise un moyen technique moderne : les systèmes informatiques.

Le système d'information est, de nos jours, au cœur des stratégies commerciales, marketing et même de sécurité, de l'ensemble de l'entreprise.

### *1.2.2 Système informatique*

Un système informatique est un ensemble d'équipements (matériels et logiciels) destiné au traitement automatique de l'information. Il constitue la base sur laquelle repose un système d'information. En général, il est constitué de serveurs, routeurs, pare-feu, commutateurs, imprimantes, médias (câbles, air, etc.), points d'accès, stations de travail, systèmes d'exploitation, applications, bases de données, etc. En d'autres termes, il s'agit de tout le matériel et logiciel, qui est voué à traiter l'information.

### *1.2.3 Sécurité informatique*

La sécurité, au sens général, consiste à se « protéger ». La sécurité informatique est la protection des systèmes et des ressources (en particulier les données) informatiques. La sécurité informatique est donc la protection des systèmes informatiques et des services contre les menaces accidentelles ou intentionnelles touchant la confidentialité, l'intégrité de l'information et la disponibilité des systèmes informatique et de différents services. [2]

C’est l’ensemble des moyens mis en œuvre pour réduire la vulnérabilité d’un système informatique contre les menaces auxquelles il peut être confronté. En d’autres mots, c’est l’ensemble des techniques qui assure que les ressources du système informatique d’une organisation sont utilisées uniquement dans le cadre où il est prévu qu’elles le soient.

### *1.2.4 Principe du maillon le plus faible*

Une personne cherchant à pénétrer un système utilisera tous les moyens possibles de pénétration, mais pas nécessairement le plus évident ou celui bénéficiant de la défense la plus solide. Le niveau de sécurité d’un système est mesuré à partir du maillon le plus faible.[3]

### *1.2.5 Responsabilité des usagers*

Thucydite dit : « Ce ne sont pas les murs qui protègent la citadelle, mais l’esprit de ses habitants ». Ceci s’applique également aux systèmes d’information où les statistiques indiquent que 40% des attaques sont causées par les usagers du système d’information eux-mêmes. On peut dire que l’être humain est le maillon le plus faible dans la chaîne de la sécurité informatique.

En effet, les utilisateurs sont aussi responsables de la sécurité du système d’informations. S’ils ne prennent pas garde, même si les mesures prises par les responsables de sécurité de système d’information de l’entreprise prennent beaucoup d’initiative pour la sécurité, ce serait vain, car les utilisateurs constitueraient une porte d’entrée pour les hackers.[4]

### *1.2.6 Cybersécurité*

La cybersécurité est un sous-ensemble de la sécurité informatique et des réseaux appliqués aux cyberespaces et à tout environnement informatique connecté à l’Internet. Elle peut être mise en défaut par des cyberattaques informatiques. Du fait de l’usage extensif de l’Internet, de nouvelles menaces sont apparues générant des risques additionnels dont les impacts, de niveaux d’importance variables, peuvent affecter les individus, les organisations ou les États.

Selon l’Union internationale des télécommunications (ITU : International Télécommunication Union), la cybersécurité est « l’ensemble des outils, politiques, concepts de sécurité, mécanismes de sécurité, lignes directrices, méthodes de gestion des risques, actions, formations, bonnes pratiques, garanties et technologies qui peuvent être utilisés pour protéger le cyber environnement et les actifs des organisations et des utilisateurs ».[4]

### *1.2.7 Vulnérabilité*

C'est une faiblesse d'un système qui se manifeste par l'incapacité de ce dernier à contrer les différentes menaces qui pèsent sur lui. Elle peut provenir d'une configuration mal faite ou d'insouciance ou encore d'ignorance de la part des utilisateurs, développeurs d'applications.

### *1.2.8 Risque*

Les menaces engendrent des risques et des coûts matériels, financiers et humains : perte de confidentialité des données sensibles, indisponibilité des infrastructures et des données, dommages pour le patrimoine intellectuel et de la notoriété [1][2][4]

### *1.2.9 Attaque informatique*

C'est l'exploitation d'une faiblesse ou d'une faille d'un système informatique : par exemple faiblesse au niveau du système d'exploitation, application, configuration et beaucoup d'autres.

### *1.2.10 Monitoring ou supervision d'un réseau*

Le monitoring ou monitorage est une activité de surveillance et de mesure d'une activité informatique. On parle aussi de supervision. La supervision se définit comme une technique utilisant au mieux les ressources informatiques pour obtenir des informations sur l'état des réseaux et de leurs composants. Ces informations seront ensuite traitées et affichées afin de mettre en lumière d'éventuels problèmes.

Superviser un réseau, en tant que pratiquant d'une discipline professionnelle, signifie assurer qu'un réseau, des serveurs, des applications, des services soient stables, en bon état, et fonctionnant à un niveau maximum d'efficacité à tout moment. Ce qui consiste non seulement à être alerté quand un système a cessé de fonctionner, mais surtout, être capable de prédire une panne et ainsi intervenir pour que celle-ci soit évitée.

## 1.3 Objectifs et fondements de la sécurité informatique

Le principal but de la sécurité informatique est de réduire le plus possible la surface d'attaque des machines hôtes et du réseau tout entier.

La sécurité informatique vise généralement cinq principaux objectifs. Ce sont les bases de ladite sécurité informatique :

- Confidentialité
- Intégrité
- Disponibilité
- Authenticité
- Non-répudiation

L'ensemble de la confidentialité, l'intégrité et l'authenticité est aussi appelé triade de la CIA (Central Intelligence Agency).

### *1.3.1 Confidentialité*

La confidentialité est, par définition, le maintien du secret des informations. Dans le domaine de l'informatique et de la télécommunication, elle peut être aussi définie comme étant la protection des données contre une divulgation non autorisée. La confidentialité est la propriété qui garantit que l'information est rendue inintelligible aux personnes, individus, groupes ou entités et processus qui n'ont pas l'autorisation de la voir. Elle permet donc de s'assurer que seuls les utilisateurs habilités ou autorisés ont accès à l'information et de protéger toutes les données transmises entre deux utilisateurs pendant une période donnée.

Il y a deux différents types d'actions complémentaires permettant d'assurer la confidentialité des données :

- Limitation et contrôle des accès afin que seules les personnes autorisées à les lire ou à les modifier peuvent le faire
- Rendre inintelligibles en utilisant le chiffrement ainsi les personnes non autorisées soient incapables de voir les contenus

Le chiffrement des données (ou cryptographie) contribue à assurer la confidentialité des données et à augmenter la sécurité des données lors de leur transmission ou de leur stockage. Bien qu'utilisées essentiellement lors de transactions financières et commerciales, les techniques de chiffrement soient relativement peu mises en œuvre par les internautes de manière courante.

### *1.3.2 Intégrité*

L'intégrité est la propriété permettant la vérification qu'une information ou donnée n'a pas été intentionnellement ou accidentellement modifiée par une entité tierce. L'intégrité veut dire :

exactitude, précision, modifications autorisées seulement, cohérence. Ainsi, une information n'est modifiée que dans des conditions prédéfinies.

Une fonction de hachage est parfois utilisée pour vérifier l'intégrité des données. Dans la suite, on va voir quelques notions de fonction de hachage et de cryptographie.

1.3.2.1 Fonction de hachage cryptographique

Une fonction de hachage fait correspondre une chaîne binaire de longueur variable à une chaîne de longueur fixe.

1.3.2.2 Propriété d'une fonction hachage

- Étant donné un message m, il est facile de calculer *h(m)* qui est la version hachée de *m*.
- Étant donné *h* tel que *h(m) = h*, il est difficile de calculer m.
- Étant donné m, il est difficile de trouver un autre message, *m'*, tel que *h(m) = h (m')*

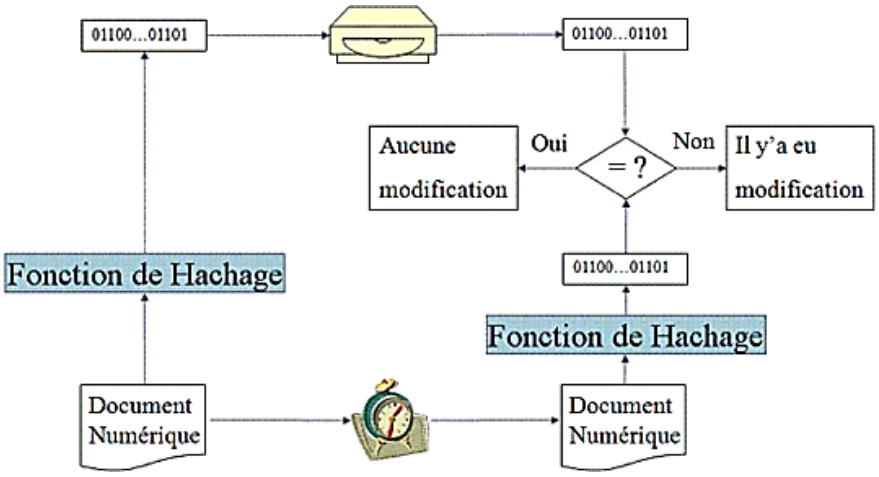


***Figure 1.01*** *:* Vérification de l'intégrité de donnée

Le critère d'intégrité des ressources physiques et logiques (équipements, données, traitements, transactions, services) est relatif au fait qu'elles n'ont pas été détruites ou modifiées à l'insu de leurs propriétaires tant de manières intentionnelles qu'accidentelle.

Les critères de disponibilité et d'intégrité sont à satisfaire par des mesures appropriées afin de pouvoir atteindre un certain niveau de confiance dans les contenus et le fonctionnement des infrastructures informatiques et télécoms.

Si en télécommunication, l'intégrité des données relève essentiellement de problématiques liées au transfert de données, elle dépend également des aspects purement informatiques de traitement de l'information (logiciel d'application, systèmes d'exploitation, environnements d'exécution, procédures de sauvegarde, de reprise et de restauration des données). En principe, lors de leur transfert, les données ne sont pas altérées par les protocoles de communication qui les véhiculent en les encapsulant.

### *1.3.3 Disponibilité*

Le terme disponibilité, dans le monde de l'informatique, fait référence au bon fonctionnement d'un système informatique. Un système informatique doit être disponible pour ses utilisateurs autorisés. En fait, c'est la raison pour laquelle il existe. La disponibilité peut être aussi traduite comme la présence du système sous forme utilisable satisfaisant des contraintes de temps, de performances et de qualité. C'est-à-dire, lorsqu'un utilisateur demande d'accéder à une certaine ressource du système, s'il est authentifié, il doit pouvoir y accéder avec une vitesse assez élevée, une qualité de service et de performance bonne.

La disponibilité d'une ressource est relative à la période pendant laquelle cette dernière fonctionne normalement c'est-à-dire période pendant laquelle le service offert est opérationnel.

Mais il faut noter qu'il ne suffit pas qu'une ressource soit disponible, en effet cette dernière doit pouvoir être utilisable avec des temps de réponse acceptables. Ainsi la disponibilité va toujours de pair avec la capacité à être accessible par l'ensemble des ayants droit. La disponibilité des services, systèmes et données est obtenue par un dimensionnement approprié et une certaine redondance des infrastructures ainsi que par une gestion opérationnelle et une maintenance efficace des infrastructures, ressources et services.

La notion de continuité de service va aussi avec la disponibilité. Donc un service nominal doit être assuré avec le minimum d'interruption possible.

### *1.3.4 Authentification*

Pour assurer l'intégrité et la confidentialité des données, le système informatique doit procéder à l'authentification des personnes ou groupes de personnes voulant y accéder. Donc le mécanisme d'authentification permet de garantir la confidentialité des données d'un système informatique.

L'authentification doit permettre de vérifier l'identité d'une entité afin de s'assurer entre autres, de l'authenticité de celle-ci. Pour cela, l'entité devra prouver son identité, le plus souvent en donnant une information spécifique qu'elle est censée être seule à détenir telle que, par exemple, un mot de passe ou une empreinte biométrique. [4]

L'authentification permet aussi la protection contre l'usurpation d'identité (la signature est un signe d'authentification). Les entités à authentifier sont les suivantes : une personne, un processus (un programme en exécution), une machine dans un réseau. On peut dire alors que l'authentification est le moyen clé de sécurité pour assurer la fiabilité, la confidentialité et l'intégrité des données d'un système informatique.

### *1.3.5 Non-répudiation*

La non-répudiation assure que l'auteur de l'acte ne puisse ensuite nier l'avoir effectuée. C'est-à-dire la non-répudiation permet de rendre vraiment responsable la personne ou l'entité qui a fait tel ou tel acte. Elle empêche donc un responsable d'une action de nier sa responsabilité.

La non-répudiation est une règle de sécurité exigée dans des domaines de traitement de données sensibles (à l'instar d'une transaction commerciale impliquant un transfert monétaire).

Une analogie peut être faite entre la non-répudiation et la signature. En effet, d'un côté la signature est un engagement contractuel, juridique, ainsi le signataire ne peut revenir en arrière. Et d'une autre coté, la non-répudiation donne la preuve d'origine pour qu'un message ne puisse être dénié par son émetteur et la preuve de réception pour le récepteur pour qu'il ne puisse non plus nier avoir reçu le message.

L'identification et l'authentification des ressources et des utilisateurs permettent d'imputer la responsabilité de la réalisation d'une action à une entité. Celle-ci pourra être tenue responsable de certains faits et éventuellement rendre des comptes, s'ils ont été enregistrés, sauvegardés et analysés.

Ainsi la traçabilité des événements est une fonction indispensable qui permet de garder la mémoire des actions survenues à des fins d'analyse pour reconstituer et comprendre ce qui s'est passé.

## 1.4 Différents aspects de la sécurité informatique.

On va voir qu'il y a plusieurs aspects par lesquels on peut classer les différents types de sécurité informatique.

### *1.4.1 Différents aspects selon la manière de sécurisation*

Nous allons ici voir les différents types de manières de sécuriser un système informatique.

1.4.1.1 Sécurité offensive : Red Team

La sécurité offensive, comme son nom l'indique, consiste à attaquer pour mieux se défendre. Même si de nombreuses personnes apprennent les attaques informatiques (généralement de manière autodidacte) dans un but peu louable, ces techniques sont également enseignées soit dans le cadre de ce qu'on appelle « Ethical hacking » ou le piratage éthique, permettant de déterminer les failles d'un système de manière légale, soit dans le cadre d'un audit préalable indispensable à la sécurité défensive ("connaître ses ennemis pour mieux se défendre").

Dans ce type de sécurité, une équipe ou un groupe fait des tests d'intrusions physiques, c'est-à-dire sur le site de l'entreprise client, logique via Internet ou d'autres moyens pour tester la sécurité globale de l'entreprise. Souvent, lorsque l'équipe opère, les personnels de l'entreprise ne connaissent pas l'existence de l'opération pour pouvoir bien assimiler le niveau de sécurité de l'entreprise et pour pouvoir bien voir tous les risques et y remédier rapidement. Ainsi, en procédant de cette manière, on peut voir si les personnels sont bien éveillés et conscients des risques de cyber sécurité d'aujourd'hui.[5][6]

1.4.1.2 Sécurité défensive : Blue team

Cette équipe est destinée à être sur le défensif. C'est-à-dire, il opère pour garde la sécurité informatique de l'entreprise aussi intacte que possible. Ainsi, ils constituent la ligne défensive en termes de sécurité informatique.

Là où il y a des risques, il doit nécessairement y avoir une protection face à ces risques. La sécurité défensive se doit donc d'évaluer et quantifier les risques éventuels, de déterminer les failles à leur

origine, et de déterminer en conséquence une politique de sécurité permettant de garantir la bonne marche (continuité) des affaires courantes.

Le « Blue team » aussi est responsable pour les réponses aux incidents dans le cas échéant. C'est à eux de prendre les actions nécessaires pour limiter les dégâts d'une attaque informatique visant l'entreprise.

Ils sont aussi responsables des investigations si cela est nécessaire.

### *1.4.2 Types de sécurité informatique selon le domaine d'application*

Dans ce paragraphe, nous allons voir les différents aspects de la sécurité informatique selon son domaine d'application c'est-à-dire nous allons voir pour une organisation, quels sont les différents stades qu'on peut sécuriser dans son système informatique.

1.4.2.1 Sécurité physique et environnementale

Si un intrus ou un non autorisé arrive à accéder physiquement aux ressources matérielles d'une entreprise ou organisation, ce sera un peu facile pour lui d'obtenir des informations confidentielles qui pourraient compromettre la sécurité de l'entreprise. C'est pourquoi la sécurité physique des systèmes informatiques est un aspect à ne pas négliger de la sécurité informatique. Il faut bien noter que, quelles que soient les mesures de sécurité prises si les lieux où se trouvent les ressources matérielles ne sont pas bien sécurisés, les attaquants pourraient trouver facilement des failles dans le système. [3][5] La sécurité informatique et environnementale se focalise sur tous les aspects liés à l'environnement où se trouve le système. Il s'agit donc de la maîtrise du système et des alentours.[7] Pour cela on peut citer :

- La mise en place de caméra de surveillance dans l'entrée des datacenters, mais aussi dans ces derniers permet d'enregistrer toutes les activités qui se sont déroulées dans ces derniers. Les caméras servent de surveillance, mais aussi des preuves dans une enquête lorsqu'un incident s'est produit.
- Les serveurs et les équipements d'un datacenter doivent être placés dans un lieu physiquement et hautement sécurisé. D'où la nécessité d'utilisation des portes blindées pour éviter tout dégât inutile.

- Il est aussi nécessaire de noter que l'accès à la salle du datacenter doit être enregistré et répertorié afin de garder la traçabilité des changements effectués par quiconque qui' s'est rendue dans la salle.
- La mise en place d'un système de privilège est aussi un moyen pour la sécurisation physique. En effet, seules les personnes qui ont des accréditations suffisantes peuvent entrer et faire ce qu'ils ont à faire dans la salle des serveurs. Pour cela, le verrouillage des portes des datacenters par des systèmes de cartes est aussi des mesures de sécurité à ne pas négliger.
- La réplication physique des sites d'emplacements, infrastructures et sources énergétiques le marquage des matériels pour notamment contribuer à dissuader le vol de matériel et éventuellement le retrouver

Pour préserver la sécurité des ordinateurs et machines qui stockent des informations confidentielles, il est préférable d'isoler ces derniers dans une salle et bâtiment vraiment sécurisés et sous haute surveillance.

#### 1.4.2.2 Sécurité de l'exploitation

Comme son nom l'indique, ce type de sécurité permet de mener à bien l'exploitation du système. Cela consiste à la mise en place de différentes mesures de sécurité pour les outils d'exploitation : la maintenance, le test, le diagnostic, la gestion des performances, la gestion des changements et des mises à jour.

Les principaux points de la sécurité de l'exploitation sont :

- Gestion des configurations et des mises à jour : toutes les applications utilisées au sein d'une organisation doivent être à jour et patchées.
- Plan de sauvegarde : Les backups des données de l'organisation sont une mesure importante à ne pas négliger
- Analyse des fichiers de journalisation et de comptabilité : Les fichiers logs des serveurs et systèmes sont des informations vraiment essentielles en termes de sécurité informatique. Ainsi, l'analyse de ces derniers ne doivent pas être non plus sous-estimer.
- Séparation des environnements de développement et de production des applicatifs.

1.4.2.3 Sécurité de l'information, sécurité logique et applicative

La sécurité logique concerne la réalisation de mécanismes de sécurité par logiciel contribuant au bon fonctionnement des programmes, des services offerts et à la protection des données.

Elle s'appuie généralement sur :

- La qualité des développements logiciels et des tests de sécurité ;
- Une mise en œuvre adéquate de la cryptographie pour assurer intégrité et confidentialité notamment sur les développements d'applications qui nécessitent des transferts ;
- Des procédures de contrôle d'accès logique, d'authentification

La sécurité logique fait également référence à la sécurité applicative qui doit tenir compte des besoins de sécurité et de robustesse développement des logiciels, des applications et de leur contrôle qualité. Le cycle de vie des logiciels, comme leur intégration dans des environnements de production doit également satisfaire aux exigences de sécurité en termes de disponibilité, de continuité des services, d'intégrité ou de confidentialité. La sécurité applicative comprend le développement pertinent de solutions logicielles (ingénierie du logiciel, qualité du logiciel) ainsi que leur intégration et exécution harmonieuses dans des environnements opérationnels.

Elle repose essentiellement sur l'ensemble des facteurs suivants :

- Une méthodologie de développement (en particulier le respect des normes de développement propre à la technologie employée et aux contraintes d'exploitabilité)
- La robustesse des applications en termes d'authentification et de contrôle d'accès ;
- Des jeux de tests (test de sécurité) ;
- L'intégration de mécanismes de sécurité, d'outils d'administration et de contrôle de qualité dans les applications ;
- La sécurité des progiciels (choix des fournisseurs, interface sécurité, etc.) ;
- La validation et l'audit des programmes ;

1.4.2.4 Sécurité des infrastructures informatique et de télécommunication.

Ces types de sécurité concerne la sécurité des réseaux et sécurités Internet.

La sécurité des télécommunications a pour but d'assurer de la sécurité de toutes les liaisons dans une entreprise ou organisation. Elle consiste à offrir à l'utilisateur final et aux applications

communicantes, une connectivité fiable de « bout en bout ». Ceci se fait par la réalisation d'une infrastructure réseau sécurisé au niveau des accès au réseau et du transport de l'information (sécurité de la gestion des noms et des adresses, sécurité du routage, sécurité des transmissions à proprement parler) et s'appuie sur des mesures architecturales adaptées, l'usage de plateformes matérielles et logicielles sécurisées et une gestion de réseau de qualité.

La sécurité des télécommunications ne peut à elle seule garantir la sécurité des informations. Elle ne constitue qu'un maillon de la chaîne sécuritaire, car il est également impératif de sécuriser l'infrastructure informatique dans laquelle s'exécutent les programmes.

Un environnement informatique et de télécommunication sécurisé implique la sécurisation de tous les éléments qui le compose. La sécurité est toujours celle du maillon le plus faible, comme on l'a déjà mentionné depuis le début.

Implanter des mécanismes de chiffrement pour rendre les données transférées confidentielles est de peu d'utilité si d'aucuns peuvent y accéder lorsqu'elles sont manipulées par des plateformes matérielles et logicielles non correctement sécurisées.

L'implantation de mesures de sécurité doit répondre à des besoins de sécurité clairement identifiés à la suite d'une analyse des risques spécifiquement encourus par une organisation.

De plus, un système sécurisé, mobilisant d'importants moyens sécuritaires, aussi pertinents soient-ils, ne pourra être efficace que s'il s'appuie sur des personnes intègres et sur un code d'utilisation adéquat des ressources informatiques pouvant être formalisé par une charte de sécurité.

Souplesse et confiance réciproque ne peuvent se substituer à la rigueur et au contrôle imposés par le caractère stratégique des enjeux économiques et politiques que doivent satisfaire les systèmes d'information et les réseaux de télécommunications.

Il ne faut jamais oublier que dans le domaine de la sécurité, la confiance n'exclut pas le contrôle. La sécurité, en tant que propriété d'un système, peut être qualifiable (notion d'assurance de sécurité qui fait référence à la quantification de la qualité de la sécurité).

En revanche, la confiance est une relation binaire entre deux entités qui relève du sentiment.

## 1.5 Politique de sécurité

### *1.5.1 Généralités*

Une politique de sécurité peut être définie comme étant un plan d'action pour la préservation de l'intégrité et la pérennité d'un groupe social. Ainsi une politique de sécurité informatique est un plan d'action défini pour le maintien d'un certain niveau de sécurité informatique.

Elle reflète la vision stratégique de la direction de l'organisme en matière de sécurité informatique.

La politique de sécurité d'une entreprise donnée définit les objectifs spécifiques de la sécurité des systèmes informatiques de cette entreprise.

Il y différents types de politique de sécurité informatique : la politique immorale, permissive, prudente, paranoïaque.

### *1.5.2 Principes*

La sécurité informatique doit toutefois être étudiée de telle manière à ne pas empêcher les utilisateurs de développer les usages qui leur sont nécessaires, et de faire en sorte qu'ils puissent utiliser le système d'information en toute confiance. C'est la raison pour laquelle il est nécessaire de définir dans un premier temps une politique de sécurité, c'est-à-dire :

- Élaborer des règles et des procédures, installer des outils techniques dans les différents services de l'organisation (autour de l'informatique) ;
- Définir les actions à entreprendre et les personnes à contacter en cas de détection d'une intrusion ;
- Sensibiliser les utilisateurs aux problèmes liés à la sécurité des systèmes d'informations
- Préciser les rôles et responsabilités.

La politique de sécurité est donc l'ensemble des orientations suivies par une entité en matière de sécurité. À ce titre, elle se doit d'être élaborée au niveau de la direction de l'organisation concernée, car elle concerne tous les utilisateurs du système.

### 1.6 Dispositifs de protection

Pour le maintien d'un certain niveau de sécurité pour un organisme donné, divers outils sont mis à disposition des administrateurs réseaux et des responsables de sécurité des systèmes d'informations. On peut citer :

- Pare-feu
- Serveur Proxy
- « Reverse proxy »
- Système de détection et de prévention d'intrusion
- VPN
- Anti-virus

On détaillera quelques-uns de ces outils dans le chapitre III.

### 1.7 Conclusion

On a vu ce qu'on entend par sécurité informatique, la définition, les types. Lorsqu'on parle de sécurité, on parle toujours d'attaques. Ainsi dans le chapitre suivant, on va voir les différentes manifestations des attaques informatiques.

# CHAPITRE 2 LES DIFFÉRENTS TYPES D'ATTAQUES INFORMATIQUES

## 2.1 Introduction

Comme on a déjà vu, une attaque informatique est l'exploitation d'une faille ou vulnérabilité au sein d'un système. L'attaque est essentiellement basée sur les trois points suivants : la motivation de l'hacker, sa méthodologie et la vulnérabilité du système.

Tout d'abord, la motivation de l'hacker est fondamentale et c'est ce qui le pousse à creuser et à chercher des failles et des moyens pour pénétrer un système. Cette motivation peut être le vol d'informations pour ensuite les vendre, donc un but financier. La vengeance est aussi une motivation vraiment dangereuse. La motivation d'un hacker dépend aussi de la valeur des données ou des informations qui' il a l'intention de voler ou d'altérer, ici on parle de « hack value ».

Ensuite, lorsque l'hacker possède la motivation nécessaire, il va procéder suivant une certaine méthodologie.

Enfin, le dernier point qui pousse les hackers à attaquer un système est la vulnérabilité de ce dernier. En fait, tout est vulnérable lorsqu'il est exposé sur Internet. C'est l'initiative de sécurisation du système qui compte et aussi l'initiative d'être toujours en veille technologiquement.

Dans ce chapitre, on va voir tout d'abord les différents types d'attaques informatiques et ensuite on va voir quelques variétés d'attaques informatiques.

## 2.2 Différents types d'attaques informatiques

Il y a trois différents types d'attaques informatiques. Ce sont :

- Les attaques directes
- Les attaques indirectes par rebond
- Les attaques indirectes par réponse

On va développer un à un ces types d'attaques et voir le type d'attaque qui privilégie le plus un attaquant.

### *2.2.1 Attaques directes*

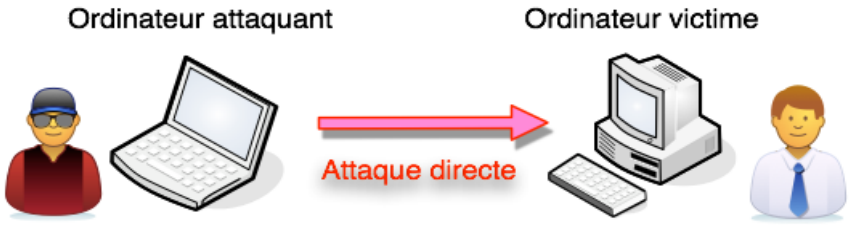


***Figure 2.01:*** Attaque directe

Dans ce type d'attaque, l'attaquant ou le pirate attaque directement l'ordinateur de la victime avec sa machine, c'est à dire il n'y a pas d'intermédiaire. Ainsi, l'hacker envoi directement les paquets de sa propre machine vers celle de la victime. Ces types d'attaques se produisent lorsqu'une machine est connectée directement à un LAN ou à Internet et l'attaquant utilise des différents logiciels pour l'envoi des paquets directement à partir de son ordinateur à la victime.

Dans ce genre d'attaque, si l'hacker ne couvre pas soigneusement toutes ses traces, il peut être retracé, car dans ce cas, il est assez facile de remonter jusqu'à la source vue que l'attaque est directe.

### *2.2.2 Attaques indirectes par rebond*

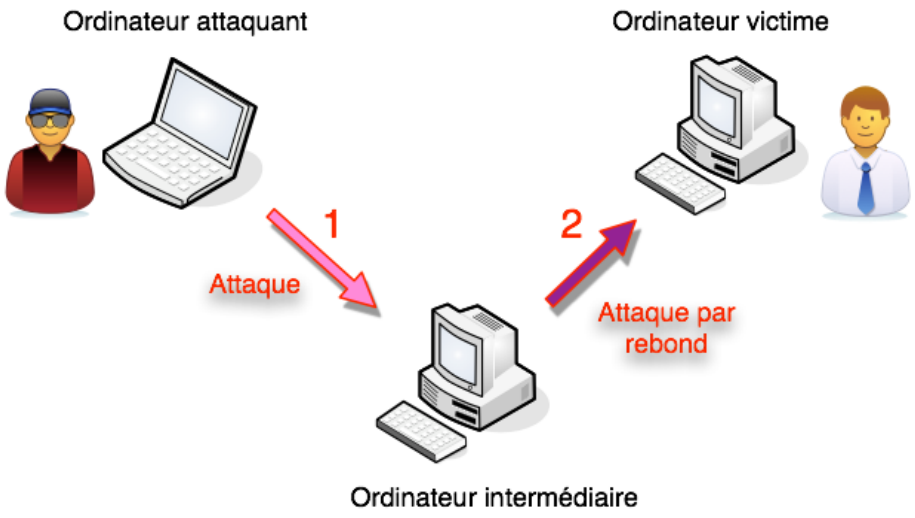


***Figure 2.02 :*** Attaque indirecte par rebond

Dans ce type d'attaque, les attaques par rebond constituent un ensemble d'attaques à envoyer à l'ordinateur intermédiaire qui répercute l'attaque vers la victime. Cette attaque est très prisée des hackers. En effet, le rebond a deux avantages :

- Masquer l'identité (l'adresse IP) de l'hacker.
- Éventuellement, utiliser les ressources de l'ordinateur intermédiaire, car il est plus puissant (CPU, bande passante...etc.) pour la réalisation d'une attaque

### *2.2.3 Attaques indirectes par réponse*

C'est une attaque dérivée de l'attaque par rebond. Les avantages, pour l'hacker, qu'offre ce type d'attaques sont les mêmes que les avantages des attaques par rebond.

Mais au lieu d'attaquer l'ordinateur intermédiaire pour qu'il répercute l'attaque aux victimes, l'attaquant envoie une requête vers la machine intermédiaire. Ensuite, c'est la réponse à la requête qui va être envoyée à l'ordinateur victime. Et c'est comme ça que l'attaque va toucher la victime.

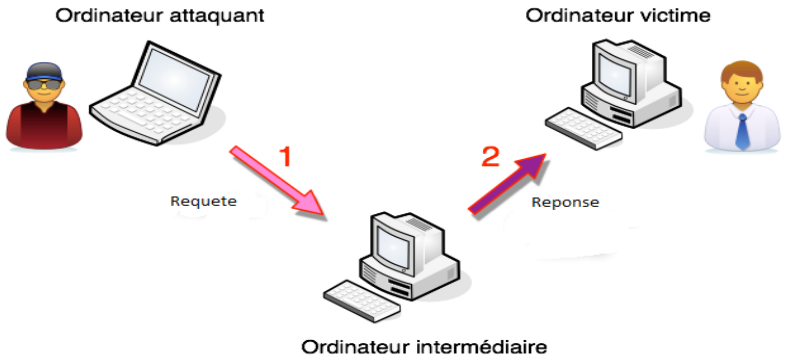


***Figure 2.03 :*** Attaque indirecte par réponse

## 2.3 Différentes techniques pour la réalisation de ces différentes attaques

Maintenant on va voir les différents techniques et moyens pour attaquer un système informatique.

### *2.3.1 Déni de service le déni de service distribué.*

2.3.1.1 Généralités

Les attaques par déni de service ou « Denial of Service » et par déni de service et distribué ou « Distributed Denial of Service » sont des attaques faciles à mettre en place du coup, elles sont aujourd'hui très fréquentes. Les résultats de ces attaques peuvent engendrer des pertes financières non négligeables par l'interruption de service ou encore indirectement, par l'atteinte portée à l'image de la cible.[4][5]

Ce sont des attaques simples à réaliser du coup en raison de l'existence de plusieurs outils prêt à être utilisé. Même des simples gens qui savent télécharger des scripts sur Internet peuvent perpétrer des attaques qui peuvent engendrer un grand dégât si on ne prend pas garde.

2.3.1.2 DoS ou Denial of Service

L'attaque par déni de service ou DoS est l'ensemble de toutes les actions ayant pour résultat la mise hors ligne d'un serveur. Une attaque par déni de service est une attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser. Ainsi, les attaques par déni de service sont opérées en saturant la bande passante d'un serveur défini. Il peut s'agir de :

- L'inondation d'un réseau afin d'empêcher son fonctionnement ;
- La perturbation des connexions entre deux machines, empêchant l'accès à un service particulier ;
- L'obstruction d'accès à un service pour une personne en particulier ;
- Le fait d'envoyer des milliards d'octets à un box Internet.

Tout d'abord, les premières n'étaient perpétrées que par un seul « attaquant », rapidement, des attaques plus évoluées sont apparues, impliquant une multitude de « bots ». On parle alors de DDoS (*Distributed denial of service attack*). Certains pirates informatiques se sont spécialisés dans la « levée » d'armées de « zombies », qu'ils peuvent ensuite louer à d'autres personnes ou groupes malveillants pour attaquer une cible particulière. Avec la forte augmentation du nombre d'échanges commerciaux sur Internet, le nombre de chantages au déni de service a très fortement progressé.

On va voir quelque type d'attaque par déni de service.

*a) Exploitation des failles ou des limites des machines.*

Cette attaque consiste à saturer une machine ou plus précisément le processeur d'une machine par l'envoi (excessivement) successivement plusieurs paquets par seconde.

Toutefois, l'augmentation de la puissance du processeur a permis d'éviter la saturation rapide des machines. Cependant, l'envoie d'une anomalie avec un rythme suffisamment rapide conduira encore la mise hors ligne un serveur ou un système entier.

On va voir plus tard une attaque plus avancée de DoS.

*b) Attaque par déni de service SYN Flood.*

C'est une attaque visant à provoquer un déni de service en émettant un nombre important de demandes de synchronisation TCP incomplète avec un serveur. Pour établir une connexion TCP entre client et serveur, ces derniers s'échangent des messages. Tout d'abord, le client envoie un message SYN au serveur. Ensuite, lorsque le serveur a reçu le message, il envoie un message d'accusé de réception ou SYN-ACK. Et enfin pour terminer, le client envoie un ACK et finit d'établir la connexion. La possibilité d'attaque se situe au moment où le client doit répondre le serveur par le dernier ACK pour finaliser l'établissement de la connexion.

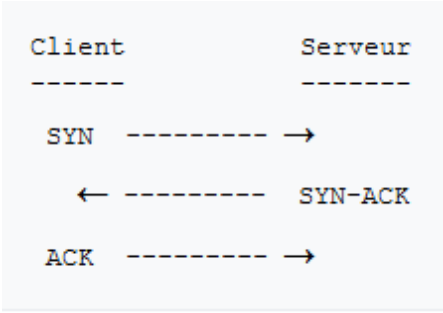


***Figure 2.04 :*** Échange de message entre client et serveur lors de l'établissement de la connexion

En effet, le problème se pose lorsque le serveur envoie le message SYN-ACK, mais ne reçoit pas de L'ACK. Le serveur construit dans sa mémoire système une structure de données décrivant toutes les connexions. Cette structure de données est de taille finie et elle peut être débordée s'il y a trop de connexion partiellement ouverte. Normalement, il y a un délai d'attente et après le serveur victime ferme la connexion, mais si plusieurs connexions sont semi-ouvertes simultanément et très rapidement, la victime aura du mal à accepter les nouvelles connexions entrantes d'où le déni de service.

*c) UDP Flooding*

Ce type d'attaque exploite le mode de transmission du protocole UDP. Il consiste à créer une UDP Packet Storm (génération d'une grande quantité de paquets UDP) à destination soit d'une machine soit entre deux machines. Cette attaque entraîne la congestion du réseau et aussi la saturation des ressources des hôtes victimes. Cette congestion est plus importante, car le trafic UDP est prioritaire sur le trafic TCP. En effet le protocole TCP à une gestion de congestion. Dans le cas où l'acquittement d'un paquet arriverait après une longue durée, le mécanisme adapte la fréquence

d'émission des paquets TCP et le débit diminue. Le protocole UDP ne possède pas ce mécanisme. Au bout d'un certain temps, le trafic UDP occupe donc toute la bande passante, ne laissant qu'une infime partie au trafic TCP.

2.3.1.3 Déni de service distribué ou effet de levier.

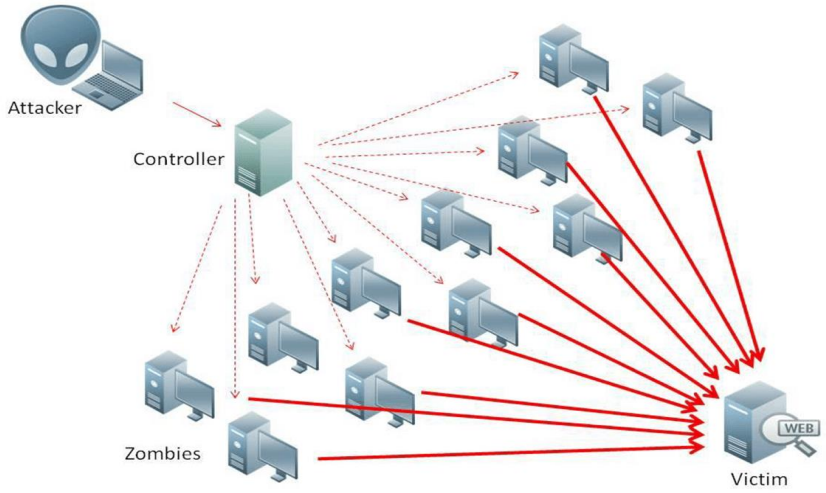


***Figure 2.05 :*** Réseau DDoS

Avec l'évolution de la technologie des serveurs actuels, et l'utilisation de technique de répartition de charge : il est quasiment impossible de provoquer un déni de service simple comme on l'a vu précédemment. Il est donc souvent nécessaire de trouver un moyen d'appliquer un effet multiplicateur à l'attaque initiale.

Principe **:**

Utilisation de plusieurs sources (daemons) pour l'attaque et des maîtres (masters) qui les contrôlent. Les sources sont contrôlées facilement par l'attaquant en utilisant les maîtres. Pour configurer et préparer l'attaque, l'attaquant doit se connecter en TCP aux maîtres. Ensuite les maîtres envoient en UDP les commandes aux sources qui facilitent le travail de l'attaquant (pas besoin de se connecter manuellement aux sources). Chaque daemon et master discutent en échangeant des messages spécifiques selon l'outil utilisé. Ces communications peuvent même être chiffrées et/ou authentifiées. Pour installer les daemons et les masters, l'attaquant peut utiliser des failles connues (buffer overflow sur des services RPC, FTP ou autres). Le résultat d'un déni de service est donc de rendre un réseau inaccessible.

### *2.3.2 Attaque MITM (Man In The Middle )*

L'attaque MITM ou « Man In The Middle » consiste à s'interposer entre deux hôtes et recevoir toutes les informations que les deux hôtes s'échangent. Les deux hôtes victimes de l'attaque ne se doutent pas que le canal de communication entre eux est compromis. Le but de cette attaque est que l'attaquant récupère l'information qui transite entre les deux hôtes victimes. [8][9][10]

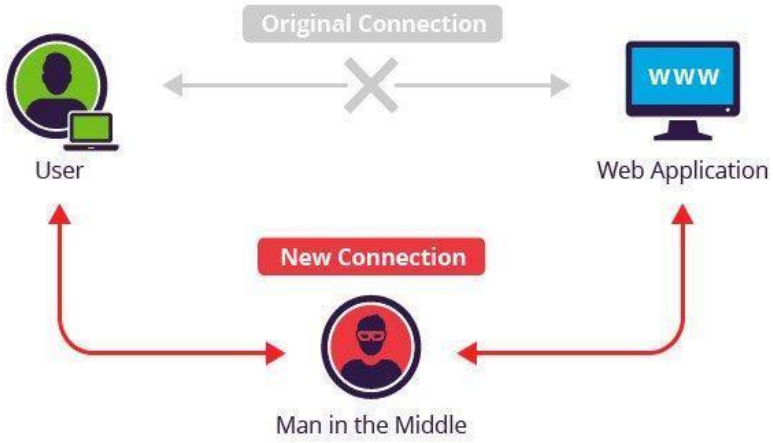


***Figure 2.06 :*** Man In The Middle Attack

La méthode utilisée est appelée ARP (Address Resolution Protocol) poisonning qui consiste à empoisonner la table ARP des machines victimes afin de se faire passer pour telle ou telle machine et récupérer les données. Mais cette méthode est très agressive et très voyante et peut entraîner la coupure du réseau la plupart du temps. [9].

L'attaque MITM est très courante dans les entreprises et les différentes organisations. Ils sont faciles à mettre en place, mais difficiles à contrer [10].

2.3.2.1 Protocole ARP

Le protocole ARP a pour but premier de faire la transition entre adresses MAC et adresses IP. C'est un protocole assez simple.

Les échanges pour connaître une adresse IP sur un réseau ressemblent à ceci :

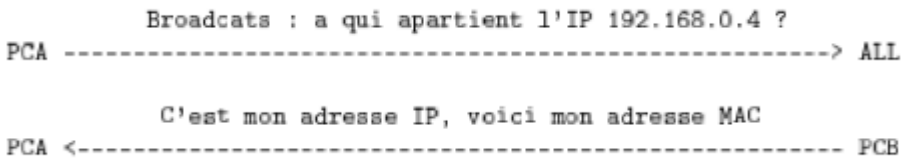


***Figure 2.07 :*** Processus de détermination de la correspondance entre adresse IP et MAC

Ici, le PCA fait une émission en broadcast (requête ARP) pour connaître à qui appartient l'adresse IP 192.0168.0.4. Ainsi, on peut découvrir l'adresse MAC d'un autre PC afin de communiquer avec lui.

Pour ne pas envoyer un broadcast à chaque fois qu'un PC veut savoir l'adresse IP correspondant à un adresse MAC (ce qui saturerait le réseau), le PC stocke une correspondance entre les adresses MAC et adresses IP des machines qui ont déjà été en communication avec lui, l'ensemble de ces correspondances constitue ce qu'on appelle table ARP. [10].

2.3.2.2 But de l'attaque

Le but de l'attaque MITM est de se place entre deux PC et de modifier la cache ARP (ou table ARP) des deux PC entre lesquels on veut se placer. C'est l'ARP « cache poisonning ». Ainsi en modifiant la table ARP des machines victimes, l'attaquant reçoit tous les paquets qui transitent entre les deux PC. (L'attaquant et les deux interlocuteurs se trouvent sur le même réseau local)

L'attaque MITM peut être passive ou active. Elle est passive lorsque l'attaquant ne fait qu'observer les différentes informations qu'il intercepte, mais elle est active lorsque l'attaquant modifie le contenu de l'information avant de l'envoyer au vrai destinataire.

2.3.2.3 DNS Poisonning

Cette attaque consiste à la manipulation du serveur DNS pour rediriger les utilisateurs vers le serveur de l'attaquant.

Différentes façons de réaliser un DNS poisonning.

- L'attaquant a compromis l'organisation des serveurs web de la victime et change la correspondance entre « hostname » et adresse IP. Quand l'utilisateur fait une requête vers le nom de l'hôte, ce dernier est redirigé vers le serveur de l'hacker.

- L'usurpation d'adresse IP peut être aussi un moyen d'effectuer le DNS poisonning

### *2.3.3 Injection SQL.*

La faille SQLi ou « SQL injection » est une exploitation des failles d'une application interagissant avec une base de données SQL. Une injection SQL, est une attaque qui consiste à injecter du code SQL dans une donnée pour détourner la requête. Les injections SQL sont, comme beaucoup d'autres failles, dues à un manque de vérification de la part du développeur. Cette attaque permet la manipulation des bases de données pour accéder à des données sensibles (nom d'utilisateur et mot de passe par exemple) et pour effectuer des opérations dont on n'a pas le droit de faire (suppression d'une ou des entrées d'une base de données, ajout d'entrée dans une base de données, création ou lecture de fichiers).

Une attaque SQLi peut affecter n'importe site web utilisant une base de données SQL et ayant des failles. Aujourd'hui les injections SQL augmentent en raison de l'existence des programmes d'injections SQL automatisés.

Ainsi, l'injection SLQ est une attaque due à l'insouciance des développeurs.

Pour éviter ces attaques, il ne faut jamais faire confiance aux utilisateurs lorsqu' on les demandes pour faire entrer des données dans l'application.

### *2.3.4 Hameçonnage ou le phishing*

2.3.4.1 Généralité

Grâce à l'Internet, nombreux services sont maintenant à la disposition des utilisateurs. L'existence du divers service en ligne comme la transaction en ligne donne des opportunités aux pirates pour l'exploitation, de diverses failles.

Tout d'abord, le mot phishing vient du mot anglais « fishing » (pêche) écrit avec un « ph ». Le terme « phishing » s'inspire du terme phreaking, qui est un diminutif de phone et freak. Originellement, le phreaking était un type d'arnaque utilisé afin de profiter de services téléphoniques gratuits surtout présents à l'époque des appareils analogiques (années 70). Ce terme est utilisé parce qu'il s'agit d'une pêche des utilisateurs d'Internet. Phishing est une attaque qui consiste à voler les informations d'un utilisateur comme le nom d'utilisateur, mots de passe, numéro de carte de crédit. [11]


***Figure 2.08:*** Le Phishing

Un des scénarios de cette attaque peut consister à envoyer des courriels contrefaits appelés courriels hameçons utilisant l'identité d'une institution financière ou d'une organisation connue pour tromper l'utilisateur. Ainsi, en guise d'hameçon ce courriel est lancé sur l'Internet jusqu'au moment où un internaute, moins soupçonneux qu'un autre, s'y accroche.

Dans les courriels hameçons, les pirates demandent aux destinataires, par exemple, de mettre à jour leurs identités bancaires ou personnelles en cliquant sur un lien qui redirige l'utilisateur vers un site de l'attaquant qui est une copie de site originale de l'institution ou de l'entreprise. Ainsi, le pirate pourra utiliser ces informations bancaires ou professionnelles à son avantage.

Il y a aussi ce qu'on appelle le « Vishing » ou « Voice fishing » qui consiste à piéger l'utilisateur à l'aide d'un appel téléphonique.

2.3.4.2 Fonctionnement du Phishing

Les messages envoyés par les pirates semblent émaner des sociétés dignes de confiance et sont formulés de manière à ne pas alarmer le destinataire afin qu'il effectue une action en conséquence. Une approche souvent utilisée est d'indiquer à la victime que son compte a été désactivé dû à un problème et que la réactivation ne sera possible que lorsque l'usager suivra certaines instructions. Le message fournit alors un lien qui dirige l'utilisateur vers une page Web qui est une copie conforme du vrai site de la société de confiance. Arrivé sur cette page trompeuse, l'utilisateur est invité à entrer des informations confidentielles qui sont alors capturées et enregistrées par le criminel. L'hameçonnage est donc une forme de vol d'identité électronique. [12].

2.3.4.3 Quelques techniques utilisées par les pirates pour le Phishing

- Utilisation d'une adresse IP au lieu d'un nom de domaine dans les hyperliens qui dirigent les utilisateurs vers le site illégitime. La plupart des utilisateurs ne vérifieront pas qu'une adresse IP est enregistrée et assignée à la compagnie visée et dont le site illégitime dit représente
- Enregistrement des noms de domaines DNS similaires ou très proches de celui du nom utilisé par la compagnie visée en espérant que les utilisateurs se méprendront entre le vrai nom de domaine de la compagnie de celle vers laquelle ils se font malicieusement diriger.
- En encodant ou en rendant la fausse adresse URL obscure. Dépendamment de la méthode utilisée, plusieurs utilisateurs ne se rendront pas compte ou ne comprendront tout simplement pas que les hyperliens ont été altérés et assumeront alors qu'ils sont légitimes.
- Configuration du site Web illégitime pour capturer et enregistrer les données entrées par l'utilisateur puis en redirigeant celui-ci vers le vrai site Web. Cette action occasionnera sûrement un message d'erreur (mot de passe non valide, essayer de nouveau) ou être totalement transparent. Dans ces deux cas, le pirate aura obtenu ce qu'il voulait,
- Configuration du site Web illégitime pour qu'il puisse agir en tant que proxy (ou d'aiguilleur) pour le vrai site Web, qui pourra donc capturer et enregistrer les données sensibles des utilisateurs piégés qui ne sont pas chiffrés (utilisant SSL), ou parfois même en les décryptant en utilisant un certificat SSL valide pour le domaine illégitime,

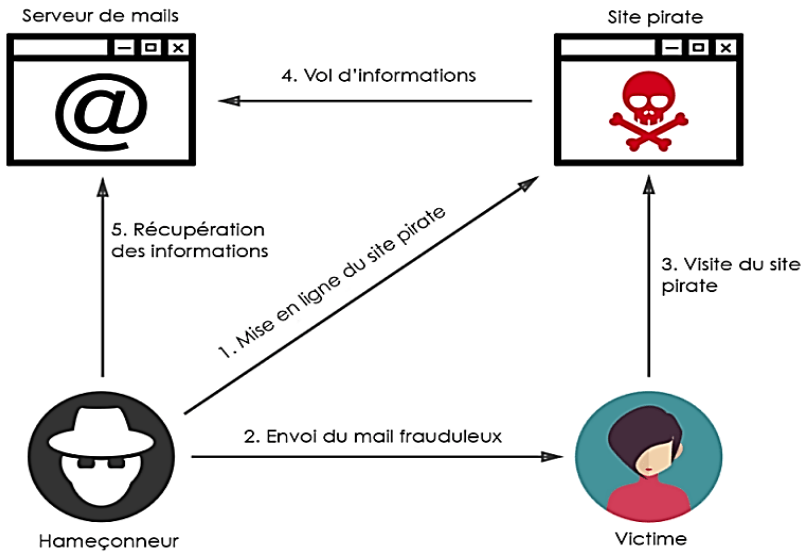


***Figure 2.09 :*** Technique d'hameçonnage

2.3.4.4 Raisons pour lesquelles l'hameçonnage fonctionne

*a) Utilisateurs non familiers aux nombreux pièges de l'Internet*

En effet, la plupart des utilisateurs des services en ligne ne sont pas au courant de l'existence du phishing et ne savent pas différencier les vrais sites web de société et les sites web contrefaits. Ceci est dû à l'ignorance de l'utilisateur.

*b) Adresses courrielles des banques facilement accessibles*

Un autre facteur est la facilité avec laquelle les pirates peuvent avoir accès aux adresses de courriel. Les pirates d'aujourd'hui possèdent d'immenses bases de données contenant plusieurs millions d'adresses de courriel. Ceci leur permet d'être en mesure de contacter le plus de proies possibles. Ces adresses de courriel peuvent aussi bien appartenir à des utilisateurs quelconques qu'à des utilisateurs de banques et autres firmes de crédits en ligne.

### *2.3.5 Usurpation d'identité ou Spoofing*

C'est le fait de se prétendre être quelqu'un qu'on n'est pas réellement. On va voir ce qu'est l'IP spoofing.

C'est l'un des facteurs qui permet la réalisation d'une attaque par déni de service distribué.

L'IP spoofing est un moyen sophistiqué d'authentifier une machine à une autre en utilisant des paquets falsifiés. Cette technique consiste à tromper le destinataire et à faire en sorte que ce dernier agit comme si le paquet provenait vraiment de la source modifiée.

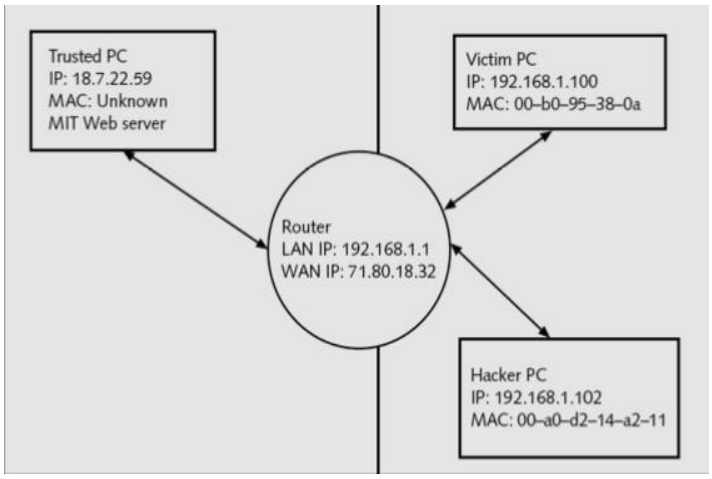


***Figure 2.10 :*** IP Spoofing dans un réseau TCP/IP

A priori, L'IP spoofing est possible, car le routage global d'Internet est basé sur l'adresse IP destination et non l'adresse IP source. Précisément, un routeur d'Internet avec sa configuration par défaut transmet les paquets d'une interface vers un autre en tenant seulement compte de l'adresse destination.

2.3.5.1 Types de Spoofing

| | |
|---|---|
| Blind spoofing | Usurpation d'identité qui ne connaît qu'une façade de la relation ou de la liaison qu'on veut attaquer. |
| Active spoofing | L'attaquant voit les deux parties, c'est-à-dire les deux victimes de l'usurpation d'identité. Il peut alors voir les données qui transitent entre les victimes, les modifier, les altérer. |
| IP Spoofing | L'attaquant se place comme un tiers de confiance entre les victimes. Cette attaque peut être mise en place soit par blind spoofing soit par active spoofing. |
| ARP Spoofing | L'attaquant modifie la table ARP des machines cibles pour des buts malveillants. |
| Web Spoofing | L'attaquant vole une adresse IP par l'intermédiaire d'un site web. En effet il fait en sorte que les données qui transitent entre les utilisateurs du site et le site lui-même passent d'abord par l'hacker avant d'arriver à destination. |
| DNS Spoofing | L'hacker change l'adresse IP d'un site en sa propre adresse IP pour pouvoir tromper les utilisateurs qui se connectent au site. Lorsque l'utilisateur se connecte au site, il a l'impression d'être vraiment sur le site qu'il croit. |

***Tableau 2.01:*** Types de « Spoofing »

### *2.3.6 Social engineering ou ingénierie sociale*

C'est l'art de manipuler les gens à faire une certaine action ou à divulguer des informations confidentielles. C'est l'exploitation de la confiance aveugle des utilisateurs inconscients de l'Internet et de ses différents dangers. C'est une attaque qui ne nécessite pas beaucoup de compétence technique.

L'ingénierie sociale n'est pas un concept nouveau. En effet, ce genre d'attaque est possible, car l'être humain a une tendance naturelle à faire confiance et à croire. Ainsi l'attaquant manipule le facteur humain et exploite la confiance pour voler d'informations importantes. Certaines des méthodes ci-dessous ont été déjà abordées, ainsi, on ne les détaillera pas.

2.3.6.1 Phishing :

Le phishing est l'un des scénarios ou l'attaquant fait recourt à l'ingénierie sociale. En fait, le phishing peut être défini comme l'utilisation de l'ingénierie sociale pour pouvoir obtenir les données (souvent bancaire : carte de crédit, etc.) en se faisant passer pour une entité de confiance.

En général, le social engineering vise les organisations. En effet, il peut sembler que la cible est l'utilisateur en personne, mais la vraie finalité que les pirates cherchent en effectuant du social engineering est une organisation (une banque par exemple).

Beaucoup d'utilisateurs se font duper et ouvrent des emails qu'ils ne doivent pas ouvrir ou faire des actions qu'ils ne sont pas censés faire.

Une des méthodes du social engineering : le Voice phishing. Il consiste à voler des données confidentielles des utilisateurs par SMS ou par appel téléphonique. Les attaquants se font passer pour des services clientèle ou des personnels des grandes institutions pour duper les utilisateurs.

Donc, cette attaque essaie d'exploiter la vulnérabilité de l'être humain. Cette technique se base sur l'établissement d'une confiance aveugle pour duper la cible.

2.3.6.2 Accès physique

Il existe aussi un autre type de social engineering qui consiste à aller sur terrain pour la recueille d'information. En fait, les hackers peuvent se faire passer pour des responsables techniques, électriques ou autres. Ils demandent souvent l'accès au data center de l'entreprise par l'utilisation du social engineering pour tromper les employés. Une fois à l'intérieur, ils peuvent déployer leur système pour y laisser un backdoor par exemple.

Donc, on peut dire que l'être humain est le maillon le plus dans la chaîne de sécurité informatique d'une entreprise. [11][12]

### *2.3.7 Malwares*

Un malware ou « Malicious Software » est un programme qui s'exécute sans le consentement de l'utilisateur. Cette attaque consiste à prendre le contrôle à distance d'une machine sans que l'utilisateur ne le sache, vol des informations confidentielles, espionnage.

2.3.7.1 Catégories des malwares

Il y a trois catégories de malwares :

a) Virus et vers

Ce genre de programme a la capacité de se propager par eux-mêmes et d'infecter le plus de cibles possibles : des fichiers exécutables par exemple.

b) Chevaux de Troies, backdoors, Rat [13]

Contrairement au virus, ces types de malwares ne peuvent pas se propager d'eux-mêmes. Ces programmes sont déployés dans les machines cibles généralement pour des vols de données, l'espionnage, et la prise de contrôle à distance de la machine de la victime.

c) D'autres programmes

Dans cette catégorie, ce sont les programmes malveillants autres que les chevaux de Troie et les virus. Ils agissent de manière différente de ce qu'on a vu. On citer par exemple les adwares ou logiciels de publicités et les ransomwares qui est un logiciel qui crypte toutes les données et le propriétaire de ce dernier demande une somme d'argent avant de débloquer ledit ransomware.

2.3.7.2 Moyens de diffusion des malwares

En général, c'est l'action de l'utilisateur qui invite, aveuglements, les malwares à s'installer sur sa propre machine sans s'en rendre compte. En faisant confiance, les programmes trouvés sur Internet, l'utilisateur se trouvent infectés sans même le savoir.

Voici les principaux vecteurs d'infection des malwares :

*a) Exploits*

C'est un logiciel ou programme qui utilise les vulnérabilités ou bugs des autres programmes. Les malwares utilisent ces failles pour se propager et infecter le plus de cibles possibles.

*b) Social engineering*

C'est l'art de duper et de tromper l'utilisateur et l'inciter à partager des informations confidentielles par exploitation des vulnérabilités humaines.

*c) Périphériques USB*

Moins utilisé aujourd'hui depuis que l'exécution automatique des périphériques USB a été désactivée par défaut. Néanmoins, ce vecteur d'attaque est encore utilisé.

*d) Cracks et les keygen*

Pour utiliser un logiciel payant sans payer un centime, les cracks peuvent être utilisés pour enlever les protections de ces logiciels. Les keygen servent pour générer des numéros de série qui permettent aussi d'enlever la protection des logiciels payants. Les cracks et les keygen sont généralement infectés par les attaquants. Mais il faut bien noter que ce ne sont pas tous les cracks et les keygen qui sont contaminés.

2.3.7.3 Trojans et backdoors. [13]

*a) Trojans ou cheval de Troie*

Le cheval de Troie vient de l'histoire de Grec ancien. Lors de la guerre entre les troyens et les grecs, Les grecs voulaient écrases ses adversaires. Ainsi ils ont piégé les troyens en construisant un grand cheval en bois dans lequel les soldats grecs se sont cachés. Ils ont ensuite déposé le cheval devant le portail des troyens. Ces derniers croient que c'est un cadeau que les grecs les ont offerts donc ils l'ont laissé entrer dans leur cité. Ainsi, une fois la nuit tombée et les soldats troyens endormis, les grecs sont sortis du cheval et ont éliminé les troyens.

C'est cette image des soldats grecs que prend ce type d'attaque informatique : le cheval de Troie. Ainsi un jeu gratuit, des logiciels inconnus peuvent être un cheval de Troie qui peut nuire aux données de la victime ou même créer un backdoor sur la machine de la victime.

*b) Backdoor ou porte dérobée*

C'est une façon d'accéder à un système de manière inhabituel. En effet, l'accès à une machine doit normalement se faire avec un login et un mot de passe. Mais un attaquant peut utiliser un backdoor pour accéder à un système sans savoir le login et le mot de passe. Le backdoor permet à un attaquant d'avoir toujours accès à un système tant qu'il veut. Le moyen le plus populaire pour installer un backdoor est le cheval de Troie ou trojans. Un autre moyen pour installer un backdoor sur une machine victime est aussi l'utilisation de site web malveillant qui incite l'utilisateur à installer un plugin par exemple.

L’attaquant cache toujours ses traces et il rend aussi indétectable son accès au système. Souvent il utilise la cryptographie pour crypter l’échange de données entre la victime et lui-même. SSH ou VPN sont des méthodes que les pirates utilisent pour crypter les trafics. L’échange des paquets utilisant la technologie de VPN ou SSH est indétectable par le firewall.

### 2.4 Conclusion

En somme, il y a plusieurs types d’attaques informatiques et il y aura encore plus dans les années à venir. Ainsi la sécurité d’une organisation dépend de son initiative à prendre les mesures nécessaires pour lutter contre ces attaques. Dans le chapitre suivant, on va voir ces différentes mesures qu’on peut prendre pour lutter contre les attaques informatiques.

# CHAPITRE 3 OUTILS ET TECHNIQUES DE SÉCURISATION INFORMATIQUE

## 3.1 Introduction

Dans ce chapitre, on va voir quelles sont les différentes manières et techniques qu'on peut appliquer pour pouvoir se protéger des dangers des attaques informatiques. On va voir tout d'abord quelques outils qu'on peut utiliser pour la sécurisation de l'entreprise et ensuite les techniques qu'on peut appliquer.

## 3.2 Outils pour la sécurisation

Dans cette partie, on va voir quelques outils pour la sécurisation informatique d'une entreprise ou d'une organisation.

### *3.2.1 Firewall ou pare-feu*

3.2.1.1 Généralités

Un firewall ou pare-feu est un système de sécurité qui permet de surveiller et de contrôler les trafics entrants et sortants d'un réseau. Le contrôle et la surveillance se font suivant un système de règle ou « Rules ». Un firewall peut être un dispositif matériel, mais peut aussi être logiciel.

On peut dire qu'un firewall met en place un système de barrière pour séparer deux réseaux différents ou tout simplement, séparer deux zones différentes (par exemple un ordinateur et les environnements extérieurs à l'ordinateur). Par exemple, le firewall permet de séparer le réseau interne d'une entreprise et un réseau externe. [14][15]

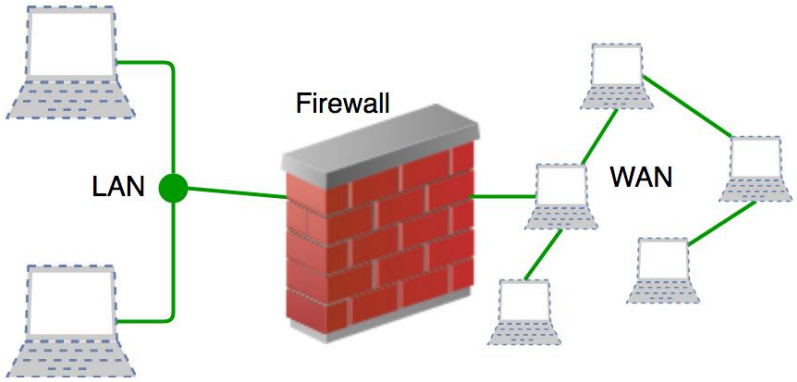


***Figure 3.01:*** Pare-feu séparant Internet à un réseau local

La première génération est aussi appelée « Packet filter » ou filtreur de paquet. Ce dernier avait pour rôle de filtrer les paquets transférés entre deux machines en tenant compte d'un jeu de règle qui se base sur l'adresse source et l'adresse destination, port source et destination, les protocoles. Les paquets qui ne satisfont pas les règles sont rejetées silencieusement (l'expéditeur ne connaît pas que son paquet a été rejeté) ou le firewall envoie un paquet ICMP à l'expéditeur.

Aujourd'hui on a les firewalls de la génération suivante ou « Next Generation Firewall » ou NGFW. Ce genre de firewall intègre les fonctionnalités des firewalls traditionnels, mais en intègre aussi d'autres comme le firewall applicatif( filtre et contrôle au niveau des données applicatives) en utilisant le DPI ou « Deep Packet Inspection » ou encore inspection en profondeur des paquets .L'intégration d'un système de prévention d'intrusion est aussi l'une des fonctionnalités en plus de ce genre de firewall .D'autres fonctionnalités comme le filtre de site web , le QoS , antivirus , Active directory et autres .

3.2.1.2 Types de firewalls

Selon les positions où sont basées les firewalls, il y a deux types de firewalls : les firewalls sur les hôtes ou « host-based » firewall et les firewalls de réseau ou « network-based firewall ».

*a) Firewalls basés sur les hôtes*

C'est un logiciel utilisé pour la sécurisation de l'hôte où il se trouve. Il est presque disponible sur tous les systèmes d'exploitation en tant que modules surtout pour les systèmes d'exploitation Linux. On voit souvent ce type de firewall sur un serveur.

Le principal rôle de ce dernier est le filtrage et la restriction des flux de paquet selon les règles configurées et la politique de sécurité adoptée par l'administrateur de l'hôte.

*b) Firewalls réseaux*

Ce type de firewall sert pour la sécurisation d'un réseau. En effet, c'est un système entier qui sert de « Gateway » au réseau. C'est à dire c'est le portail qui sépare un réseau avec d'autres réseaux de niveau de confiance bas comme les réseaux publics. Ce genre de firewall est une machine sur laquelle tourne un système d'exploitation avec une version très sécurisée. Les services qui sont vraiment importants sont les seules qui sont installées sur ce dernier pour éviter toutes vulnérabilités

inutiles : exemple HTTP, DNS, FTP. Ce firewall sert donc de proxy, c'est à dire d'intermédiaire où les connexions et les paquets passent avant de sortir.

*c) Firewalls personnels*

Ce sont des firewalls directement connectés sur le nœud qu'on veut protéger. Ils permettent le filtre de paquet et analysent les applications pour savoir si c'est une menace ou non. Ce pare-feu contrôle le trafic entre le PC d'un utilisateur et un réseau externe, exemple : Internet. Ce type de pare-feu est moins complexe que les autres types de firewalls. Le principal rôle de ce dernier est de refuser l'accès à distance non autorisé sur le PC. Il surveille aussi les activités de l'utilisateur pour détecter et bloquer les malwares. C'est un firewall de type « host-based »

### *3.2.2 Reverse proxy*

3.2.2.1 Proxy

*a) Généralité*

Le proxy est un composant logiciel ou matériel qui agit au niveau de la couche applicative dans le modèle OSI ou le modèle TCP/IP.

Un serveur proxy peut être un proxy HTTP ou un proxy FTP selon les services qui y transitent. Mais généralement, on utilise souvent les serveurs proxy HTTP, c'est-à-dire pour le web.

Le proxy sert de contrôle, de surveillances. Le proxy permet aussi de mettre en cache des données applicatives.[16]

*b) Principe de fonctionnement d'un proxy serveur*

Le principe de fonctionnement basique d'un serveur proxy est assez simple : il s'agit d'un serveur "mandaté" par une application pour effectuer une requête sur Internet à sa place. Ainsi, lorsqu'un utilisateur se connecte à Internet à l'aide d'une application cliente configurée pour utiliser un serveur proxy, celle-ci va se connecter en premier lieu au serveur proxy et lui donner sa requête.

*c) Différentes fonctionnalités d'un proxy en matière de sécurité*

Les serveurs proxy ont beaucoup de fonctionnalité qui ne se limite pas seulement à la sécurité informatique. Mais ici, on se focalisera sur les aspects sécurité de ces derniers

- Filtrage

Grâce à l'utilisation d'un proxy, il est possible d'assurer un suivi des connexions (en anglais le tracking) via la constitution de journaux d'activité (logs) en enregistrant systématiquement les requêtes des utilisateurs lors de leurs demandes de connexion à Internet.

Il est ainsi possible de filtrer les connexions à Internet en analysant d'une part les requêtes des clients, d'autre part les réponses des serveurs. Lorsque le filtrage est réalisé en comparant la requête du client à une liste de requêtes autorisées, on parle de liste blanche, lorsqu'il s'agit d'une liste de sites interdits on parle de liste noire. Enfin l'analyse des réponses des serveurs conformément à une liste de critères (mots-clés ...) est appelée filtrage de contenu.

Ainsi, le proxy joue aussi un rôle dans la sécurisation d'une infrastructure informatique par le moyen du filtrage. En effet, en mettant dans la liste blanche toutes les requêtes permises, les sites malveillants peuvent être évités. Cela permet d'éviter les utilisateurs à naviguer sur des sites risqués.

- Authentification

Dans la mesure où le proxy est l'intermédiaire indispensable des utilisateurs du réseau interne pour accéder à des ressources externes, il est parfois possible de l'utiliser pour authentifier les utilisateurs, c'est-à-dire de leur demander de s'identifier à l'aide d'un nom d'utilisateur et d'un mot de passe par exemple. Il est ainsi aisé de donner l'accès aux ressources externes aux seules personnes autorisées à le faire et de pouvoir enregistrer dans les fichiers journaux des accès identifiés. Donc cette fonctionnalité est aussi dans le cadre de la sécurité informatique.

3.2.2.2 « Reverse Proxy » ou mandataire inverse [17][18]

Aujourd'hui l'utilisation de plusieurs applications web n'est plus un concept nouveau. L'existence de plusieurs menaces pour ces différentes applications n'est plus aussi nouvelle. En effet, toute application exposée à Internet est vulnérable et susceptible de subir une attaque c'est pourquoi, on a recours au mandataire inverse ou « reverse proxy ».

Le proxy inverse reçoit les requêtes HTTP ou HTTPS provenant de l'extérieur, c'est-à-dire des clients le serveur mandataire inverse transmet les requêtes des clients à un autre serveur et renvoie la réponse au client après.[19]

Donc, la mise en place d'un « reverse proxy » donne les fonctionnalités suivantes :

La surveillance et l'audit des trafics après déchiffrement du trafic HTTPS, prévention contre les attaques DDoS et les DoS, détection des requêtes malicieuses et le blocage de ces derniers, répartition des charges entre plusieurs systèmes.

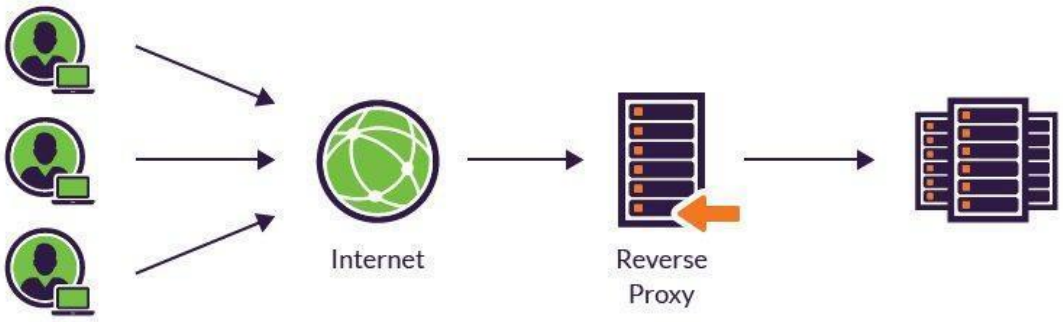


***Figure 3.02:*** Fonctionnement d'un « reverse proxy »

### *3.2.3 VPN ou « Virtual Private Network »*

3.2.3.1 Généralité [20]

Le VPN est une technique de sécurisation de communication. C'est-à-dire, c'est une technique utilisée pour obtenir une communication sûre et sécurisée entre deux sites d'une organisation par exemple.

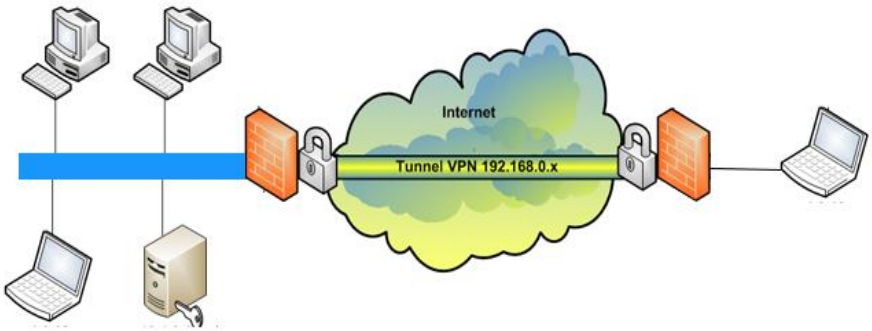


***Figure 3.03 :*** Tunnel Virtual Private Network

Le VPN est un moyen pour avoir un canal sécurisé tout en utilisant un réseau non sécurisé pour support. Un VPN est un réseau privé qui utilise un réseau public comme backbone.

Un VPN est une technique qui permet à un ou plusieurs postes distants de communiquer de manière sécurisée. Il permet l'utilisation d'infrastructures publiques (par exemple Internet). Ce type de lien est apparu à la suite d'un besoin croissant des entreprises de relier les différents sites de manière simple et économique. Jusqu'à l'avènement des VPN, les entreprises devaient utiliser lignes louées (LS). Les VPN ont permis de démocratiser ce type de lien.

3.2.3.2 Avantages d'un VPN

- La communication est sécurisée et chiffrée
- Simple : utilisation des circuits de télécommunication classiques
- Économique : L'utilisation d'Internet comme étant un média principal de transport évite les locations des lignes dédiées

### *3.2.4 DMZ ( Demilitarized Zone )*

Une DMZ (Demilitarized Zone) est une zone tampon d'un réseau d'entreprise, située entre le LAN et un réseau WAN (Internet par exemple), derrière le pare-feu. En fait, c'est un réseau intermédiaire qui regroupe des serveurs publics (HTTP, DHCP, mails, DNS, etc.).

En d'autres termes, une zone démilitarisée 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, et qui n'ont pas besoin d'accéder au réseau local.

Les services susceptibles d'être accédés depuis Internet sont situés dans le DMZ, et tous les flux en provenance d'Internet sont redirigés par défaut vers ce dernier par le firewall. Le pare-feu bloquera donc les accès au réseau local à partir de la zone démilitarisée pour garantir la sécurité du LAN. En cas de compromission d'un des services dans la DMZ, le pirate n'aura pas d'accès au réseau local. Donc l'utilisation d'un DMZ si on veut exposer à Internet des serveurs de l'entreprise est vraiment une mesure de sécurité à ne pas négliger.

La figure ci-dessous représente une architecture DMZ avec un pare-feu à trois interfaces. L'inconvénient est que si cet unique pare-feu est compromis, plus rien n'est contrôlé. Il est cependant possible d'utiliser deux pares-feux en cascade afin d'éliminer ce risque.

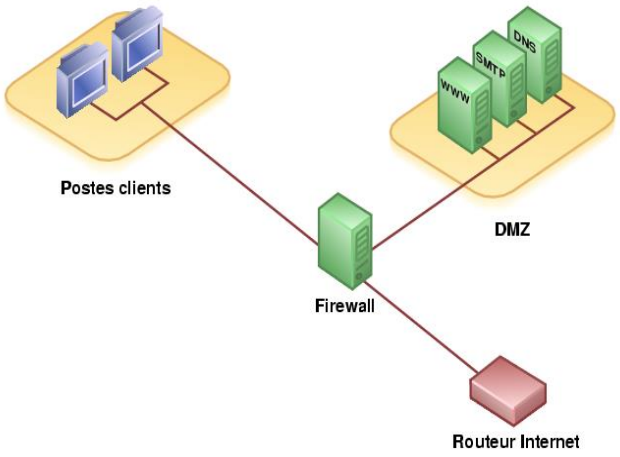


***Figure 3.04 :*** Architecture réseau possédant un DMZ

### *3.2.5 IDS (Intrusion Detection System) et IPS (Intrusion Prevention System)*

Actuellement, l'utilisation des systèmes de détection et de prévention est l'une des solutions de sécurité réseau très utilisées par les entreprises.

3.2.5.1 Système de détection d'intrusion

*a) Définition*

Un IDS, ou « Intrusion Detection System » est un dispositif qui permet la surveillance de l'activité d'un réseau ou d'un hôte donné. Composé généralement de logiciel et éventuellement de matériel, ce système informatique a pour rôle la détection de toute tentative d'intrusion. Par définition, une IDS n'a pas de signal réactif dans la mesure où il n'empêche pas une intrusion de se produire. En effet, il se contente juste d'analyser certaines informations pour détecter des activités malveillantes qui seront notifiées aux responsables de la sécurité du système dans le plus bref délai possible et ce sont eux qui prennent les dispositions nécessaires pour régler l'incident qui vient d'être détecté.

*b) Types d'IDS*

On peut classer les IDS en trois selon les places où on les déploie dans l'architecture d'un réseau :

- Systèmes de détection d'intrusion réseau (NIDS)

Les IDS réseaux analysent en temps réel le trafic qu'ils aspirent à l'aide d'une sonde (carte réseau en mode « promiscious » : c'est-à-dire une configuration de la carte réseau qui permet de faire en sorte que cette dernière accepte tous les paquets qu'elle reçoit, même si ceux-ci ne lui sont pas

adressés). Ensuite, les paquets sont décortiqués puis analysés. Il est fréquent de trouver plusieurs IDS sur les différentes parties du réseau. On trouve souvent une architecture composée d'une sonde placée à l'extérieure du réseau afin d'étudier les tentatives d'attaques et d'une sonde en interne pour analyser les requêtes ayant traversé le pare-feu.

- Systèmes de détection d'intrusion de type hôte (HIDS)

Ces types d'IDS analysent le fonctionnement de l'état des machines sur lesquelles ils sont installés afin de détecter les attaques en se basant sur des « daemons » (tels que syslogd par exemple). L'intégrité des systèmes est alors vérifiée périodiquement et des alertes peuvent être levées.

*c) Méthodes utilisées pour la détection d'intrusion*

Généralement, dans les systèmes informatiques, il existe deux types d'approches pour la détection d'intrusion : l'approche par scénario ou bien détection basée sur les signatures (« Signature-based ») sur un modèle constitué des actions interdites contrairement à l'approche comportementale (« Anomaly-based ») qui est basé sur un modèle constitué des actions autorisées.

- Détection basée sur les signatures ou « signature-based detection » :

Cette méthode consiste à identifier une suite d'événements ou des marques d'une attaque connue dans les paquets analysés. Ceci peut se faire en faisant des « Pattern Matching » ou en utilisant des expressions régulières. En fait, le trafic réseau peut être vu comme une chaîne de caractères principale et les scénarios d'attaque comme des sous-suites qu'on veut identifier.

- Approche comportementale « Anomaly detection » :

Les détecteurs d'intrusion comportementaux reposent sur la création d'un modèle de référence qui représente le comportement de l'entité surveillé en situation de fonctionnement normal. Ce modèle est ensuite utilisé durant la phase de détection afin de pouvoir mettre en évidence d'éventuelles déviations comportementales. Pour cela, le comportement de l'entité surveillée est comparé à son modèle de référence. Le principe de cette approche est de considérer tout comportement n'appartenant pas au modèle de comportement normal comme une anomalie symptomatique d'une intrusion ou d'une tentative d'intrusion.

Ces systèmes basés sur l'approche comportementale utilisent généralement des techniques d'apprentissage automatique pour identifier les intrusions et les anomalies dans les données.

*d) Architecture d'un IDS*

En général, le mode de fonctionnement d'un système de détection d'intrusion peut être décrit de la manière suivante :

- Tout d'abord, il y a la partie qui fait la capture des paquets qui circulent dans le réseau.
- Ensuite, il y a le moteur de détection qui sert à analyser les paquets et en déduire s'il y a des attaques ou non. C'est ce moteur qui s'occupe de la prise de décision concernant certains paquets donnés.
- Après cela, il y a une base de données pour le stockage des logs et des alertes du système.

3.2.5.2 Système de prévention d'intrusion

*a. Définition*

IPS est un autre concept qui a fait son apparition au début des années 2000 sous l'idée qu'un système de détection d'intrusion peut certes détecter des attaques contre un réseau, mais ne peut empêcher l'intrusion. Un système de prévention d'intrusion est un ensemble de composants logiciels et/ou matériels dont la fonction principale est d'empêcher toute activité suspecte détectée au sein d'un système.

*b. Différence entre IDS et IPS*

L'IDS réalise le monitoring du système et alerte les responsables de sécurité informatique de l'entreprise lorsqu'une activité suspecte se présente.

L'IPS en plus de détecter les activités suspectes, il peut aussi les bloquer et les empêcher de nuire. Ainsi, les IPS peuvent dropper des paquets, interrompre une session en cours.

### *3.2.6 Système de monitoring et gestion de logs*

Les menaces peuvent venir de partout. Il est donc important d'avoir une vision globale de ce qui se passe dans tout le système en temps réel. C'est pourquoi il est utile et important d'utiliser le monitoring pour la supervision du système en temps réel.

En plus de cela, le suivi des logs peut aussi être un aide majeur dans la détection et la suivie des attaques, car les logs renferment beaucoup d'information.

Donc combiner la gestion de logs avec le monitoring est un des moyens efficaces pour se protéger et pour surveiller le système.

Il faut noter que les logs sont vraiment très nombreux et il faut avoir un système capable de bien indexer les logs afin de ne pas se perdre lors de l'analyse de ces derniers. Une solution à cela est l'utilisation de la suite elastic ou elastic stack qui est système de gestion logs ou (log management) permettant de récolter, trier indexer et visualiser les logs en temps réels.

Elastic est conçu pour être rapide. Les données sont indexées au fur à mesure de leur ingestion. L'accès à l'information ne prend plus que quelques secondes, ce qui facilite l'exécution de requêtes ad hoc et la visualisation en temps réel.

## 3.3 Technique offensive pour la sécurisation informatique

### *3.3.1 Test de pénétration*

3.3.1.1 Généralité

Le test de pénétration ou « Penetration Testing » est une technique qui permet de simuler des attaques informatiques externes et/ou internes autorisées qui a pour but de voir toutes les brèches et failles dans la sécurité informatique d'une organisation et d'évaluer l'exploitabilité de ces failles. Cette technique consiste à l'analyse de l'infrastructure d'un réseau informatique pour pouvoir simuler les attaques possibles.

En utilisant différents outils et techniques, ce procédé permet d'exploiter différentes vulnérabilités pour accéder à des données critiques ou sensibles de l'organisation et ensuite d'y remédier à ces dernières.

En fait, lors d'un test d'intrusion, le « pentester » adopte la position et l'état d'esprit de l'hacker. C'est une technique de sécurisation offensive. En tentant de contourner les contrôles de sécurité et d'esquiver les mécanismes de sécurité, un pentester sera capable d'identifier les voies par lesquelles un pirate pourrait compromettre la sécurité d'une entreprise et l'endommager dans son ensemble.

Il y a trois manières de réaliser un test de pénétration : le mode boîte noire ou « Black box », boîte blanche ou « White box » et la boîte grise ou « Grey box ».

- Dans le mode « Black box », les personnes qui réalisent le test de pénétration n'obtiennent aucune information de la part de l'organisation où l'activité aura lieu. Contrairement aux tests boîte blanche, les tests de pénétration de type boîte noire permettent de simuler les actions d'un attaquant et sont effectués à l'insu de l'organisation. Les tests boîte noire sont réalisés afin de tester la capacité de l'équipe de sécurité interne à détecter une attaque et à y répondre. Par conséquent, on ne tentera généralement pas de trouver un grand nombre de vulnérabilités, mais simplement le moyen le plus facile d'accéder à un système sans être détecté.
- Dans le mode « White box », l'organisation donne toutes les informations nécessaires dont le « pentester » a besoin pour mener à bien son travail. Lors d'un test de pénétration de type boîte blanche, on travaille avec l'organisation pour identifier les menaces potentielles. L'avantage principal de ce type de test est qu'on a accès aux connaissances de quelqu'un de l'intérieur et qu'on peut lancer des attaques sans craindre d'être bloqué. L'inconvénient est qu'on pourrait ne pas avoir de résultats exacts en ce qui concerne le programme de sécurité et sa capacité à détecter certaines attaques. Quand le temps est compté et que certaines étapes du test de pénétration telle que la collecte de renseignements sont hors de portée, un test de type boîte blanche la meilleure option.
- Le mode « Grey box » est un mode entre le « black box » et le « white box ». Ainsi, le « pentester » possède des informations limitées.

#### 3.3.1.2 Type de test de pénétration

*a) Test de pénétration d'un réseau informatique*

Le test de pénétration de réseau est généralement la méthode de test de pénétration la plus courante. En effet, une fois qu'un pirate informatique obtient l'accès au réseau, 90% des obstacles sont éliminés pour un acteur menaçant.

Un pentester peut effectuer une exploitation interne et externe du réseau. Ceci permet d'émuler un pirate informatique qui a réussi à pénétrer les défenses du réseau externe. Ainsi, cela donne l'occasion d'explorer de nombreuses facettes de la posture de sécurité d'une organisation.

Un test d'intrusion d'un réseau est inévitable pour un organisme ayant un réseau informatique si ce dernier veut être préparé à l'inévitable qui est une tentative d'attaque ou même une attaque.

*b) Test de pénétration physique*

Certaines organisation ou entreprise peuvent ne pas considérer l'accès physique non autorisé comme une vulnérabilité informatique, mais ceci constitue une véritable porte d'entrée pour les hackers.

Au cours de ce test de pénétration physique, le pentester tentera d'accéder à l'installation par les moyens suivants :

- RFID (Radio Frequency Identification) et systèmes d'entrée de porte (clonage de carte)
- Crochetage ou Lock-picking
- Usurpation d'identité des personnels ou d'autres partenaires de l'entreprise

Souvent, le test de pénétration physique utilise le social engineering pour la manipulation des employés.

*c) Test de pénétration d'application web, mobile*

Pendant ce test, on essaie d'exploiter les failles et les vulnérabilités que les développeurs n'ont pas corrigées.

On essayera les injections SQL, failles XSS, exploitation des configurations mal faites et des utilisations de version obsolètes de librairies par le développeur et tant d'autres.

*d) Test d'ingénierie sociale*

Comme on a toujours dit, la sécurité informatique d'une organisation est aussi forte que le maillon le plus faible de la chaîne de cette dernière. Les gens font des erreurs et peuvent être facilement manipulés. Le maillon le plus faible est souvent les employés. L'ingénierie sociale est l'un des moyens les plus répandus par lequel les individus mal intentionnés peuvent s'infiltrer dans votre environnement.

Les types les plus courants de techniques d'ingénierie sociale utilisées par les pentesters sont :

- Phishing
- Tailgating : gain d'accès non autorisé d'un lieu en suivant un utilisateur qui a suffisamment de droits d'accès
- Dumpster Diving : fouille des poubelles
- Eavesdropping : Ecoute clandestine (conversation).

#### 3.3.1.3 Standards et méthodologies de test de pénétration

Le principal avantage de l'utilisation d'une méthodologie est qu'elle permet aux évaluateurs d'évaluer un environnement de manière globale et cohérente. Être cohérent avec une évaluation signifie qu'il est moins probable qu'un évaluateur manque de grandes vulnérabilités, le client recevra à chaque fois un produit de haute qualité avec peu de chances qu'un évaluateur manque de détails. On va voir le standard PTES (Penetration Testing Execution Standard).

#### 3.3.1.4 Étapes de test de pénétration

PTES définit les tests de pénétration en 7 phases :

a) *Interactions avant l'engagement (Pre-engagement Interactions)*

La première phase de PTES concerne tous les travaux préalables à l'engagement. Il s'agit sans aucun doute de la phase la plus importante pour un engagement harmonieux et fructueux. Cette phase commence généralement par une demande de test de pénétration de l'organisation cliente. Cette dernière détaille le type d'environnement et les résultats attendus. Un accord est signé par l'organisation et le pentester en vue de conclure tous les préparatifs du test de pénétration. Il faut aussi spécifier, pendant cette phase, le point de contact entre les pentesters et l'organisation client.

b) *Collecte d'informations et de renseignements (Information Gathering)*

Il s'agit de la deuxième phase du programme PTES et revêt une importance particulière si l'organisation souhaite que l'équipe de pentester détermine son exposition externe. Ceci est très courant avec les tests de type boîte noire ou grise. Au cours de cette phase, un évaluateur utilisera des bases de données publiques, des outils de recherche de référentiels d'informations tels que WhoIs, Shodan, des sites de médias sociaux et des outils tels que Recon-ng et la base de données de piratage Google (Google Hacking DataBase). Outre les évaluations externes, les données collectées au cours de cette phase sont idéales pour créer des profils d'ingénierie sociale et d'engagement physique. Les composants découverts sur une organisation et ses employés fourniraient à un évaluateur les moyens d'interagir avec les employés. Ceci est fait dans l'espoir que les employés divulguent des informations ou les prétextent afin que des données critiques puissent être extraites. Ainsi cette phase permet de mieux cibler le travail effectué sur le site et de mieux connaître l'environnement autour de l'organisation cible. D'ailleurs, c'est aussi la manière de procédé des hackers.

*c) Modélisation de la menace (Threat Modeling)*

La troisième phase de PTES est la modélisation de la menace. La modélisation des menaces fait souvent partie d'un engagement distinct consistant à répertorier les menaces potentielles auxquelles une organisation peut être confrontée en fonction d'un certain nombre de facteurs.

Les types de menaces les plus courants auxquels les organisations sont confrontées sont les suivants : États ou nations, Crime organisé, Pirates informatiques (Black Hat), Script kiddies, Hacktivistes

*d) Analyse des vulnérabilités (Vulnerability analysis)*

Jusqu'ici, la plupart des actions effectuées, sinon toutes, n'ont pas touché de ressources organisationnelles. Au lieu de cela, les informations ont été extraites depuis d'autres référentiels. Au cours de la quatrième phase du test de pénétration, le pentester est sur le point d'identifier des cibles viables pour des recherches plus poussées. Cela concerne directement les analyses de ports, les récupérations de bannières, les services exposés, les réponses du système et du service, ainsi que l'identification de la version. Bien qu'apparemment minimes, ces éléments sont le pivot pour accéder à une organisation.

Les pentesters recherchent ce qui est exposé, quelles vulnérabilités sont viables et quelles méthodes peuvent être utilisées pour exploiter ces systèmes.

*e) Exploitation*

C'est à ce stade que tous les travaux antérieurs aboutiront à l'accès effectif à un système. L'exploitation ne signifie pas seulement l'accès à un système via un morceau de code, un exploit distant, la création d'un exploit ou le contournement d'un antivirus. Cela peut être aussi simple que de se connecter directement à un système avec des informations d'identification par défaut ou faibles. En effet, l'accès natif est moins susceptible d'être détecté et il est plus proche de l'activité réelle qu'un acteur malveillant est en train d'effectuer.

Une fois qu'on peut accéder au système, on doit profiter de cet accès. Lorsqu'on examine la différence entre les professionnels expérimentés et les nouveaux pentesters sur le terrain, le but n'est pas une exploitation, mais une post-exploitation. En effet, l'accès initial lui seul ne permet pas d'obtenir des données sensibles, mais que le suivi et la post-exploitation le font généralement.

Ainsi le post-exploitation est une suite logique et nécessaire de l'exploitation.

*f) Post-exploitation*

La phase six consiste à l'escalade des privilèges, la recherche de références, l'extraction de données. C'est à ici que le pentester a la possibilité de prouver le risque pour une organisation en prouvant le niveau d'accès atteint, la quantité et le type de données critiques consultées et les contrôles de sécurité contournés. Tout cela est typique de la phase post-exploitation.

*g) Rapport du test de pénétration*

La phase la plus importante liée aux tests de pénétration concerne les rapports. En fin de compte, l'entreprise cliente demande et paie pour un rapport. Le rapport est la seule chose qu'elle peut tenir dans ses mains à la fin du contrat. Le rapport traduit les risques identifiés par le pentester dans l'environnement. Il doit également contenir un scénario expliquant ce qui a été fait pendant la mission, les constatations ou faiblesses réelles en matière de sécurité et les contrôles positifs établis par l'organisation. Chaque constatation de sécurité notée doit inclure une preuve de concept lorsque cela est possible.

Une preuve de concept est une preuve qui permet l'existence d'une exception à un état sécurisé par l'exploitation. Ainsi, chaque constatation identifiée doit inclure une capture d'écran liée à l'activité réalisée, telle que des mots de passe faibles, des systèmes exploités et des données critiques auxquelles on a accès. Tout comme les constatations de sécurité identifiées dans l'organisation, toute constatation positive doit être notée et décrite. [21]

### *3.3.2 Langage de Scripting : Python pour les pentesters*

Python est un puissant langage de scripts qui permet de créer facilement des exploits, d'évaluer des services, d'automatiser et de relier des solutions. Comme on a déjà vu, les tests d'intrusion consistent à tester un système informatique, un réseau ou une application Web afin de détecter les faiblesses de la sécurité pouvant être exploitées par un attaquant. En raison de la puissance et de la flexibilité qu'il offre, Python est devenu l'un des langages les plus utilisés pour les tests de pénétration.

Les principaux avantages de python sont la simplicité de sa syntaxe et aussi sa modularité. En effet, il a un riche ensemble de bibliothèques et de programmes utiles prêt à être utilisé pour accélérer le test de pénétration. Pour notre cas, on a utilisé Python pour l'écriture de script utilisée pour le test de pénétration qu'on a réalisé.

### 3.4 Conclusion

En guise de conclusion, on a vu dans ce chapitre les différents moyens qu'on peut mettre en œuvre pour la sécurisation d'un système informatique. Dans le chapitre suivant, on va voir les procédés suivis pour la sécurisation du DMZ de l'INSCAE.

# CHAPITRE 4 SÉCURISATION DU DMZ DE L'INSCAE

## 4.1 Introduction

Dans ce chapitre, on va voir les différentes étapes qu'on a suivies pour la sécurisation du DMZ de l'INSCAE. On va passer par une brève présentation de l'Entreprise, ensuite on va faire une étude des existants et une analyse des besoins, après on va voir l'architecture de la solution. Enfin, on va passer à la simulation de monitoring en utilisant Snort et la suite elastic.

## 4.2 Présentation de l'INSCAE

L'INSCAE ou Institut National de Science Comptable et d'Administration d'Entreprise est un institut de formation universitaire qui a pour but principal de former les étudiants dans la gestion, finance et l'administration d'entreprise. INSCAE est un institut vraiment réputé et est l'une des grandes universités prestigieuses de Madagascar.

Maintenant on va voir les organisations au sein de l'entreprise.

Il y a principalement trois directions : la Direction Administrative et Financière, la Direction des Études, la Direction des Perfectionnements des Affaires.

Ensuite, il y a la direction générale qui se trouve au-dessus de ces trois directions. Le centre informatique est directement relié à la direction générale donc c'est cette dernière qui supervise toutes les activités au sein du service.

## 4.3 Architecture du système informatique existant

L'informatisation du système d'information de l'INSCAE a commencé en 2015 avec la subvention de Banque mondiale et de la BADEA. Cette subvention en matérielle informatique (serveurs) a permis à l'entreprise de posséder ses propres serveurs. Donc, le site web de l'entreprise est hébergé localement.

Dans cette partie, on va voir l'existant au sein de l'entreprise ainsi que l'architecture globale du système informatique.

### *4.3.1 Architecture globale*

Le processus d'informatisation de l'INSCAE a déjà commencé il y a longtemps. En fait, de nos jours il est impératif et vraiment indispensable d'informatiser le système d'information des

entreprises. Cela permet une exploitation rapide, mais aussi des automatisations de certaines tâches répétitives.

Ici on va voir l'architecture globale de la solution implémentée au sein de l'entreprise.

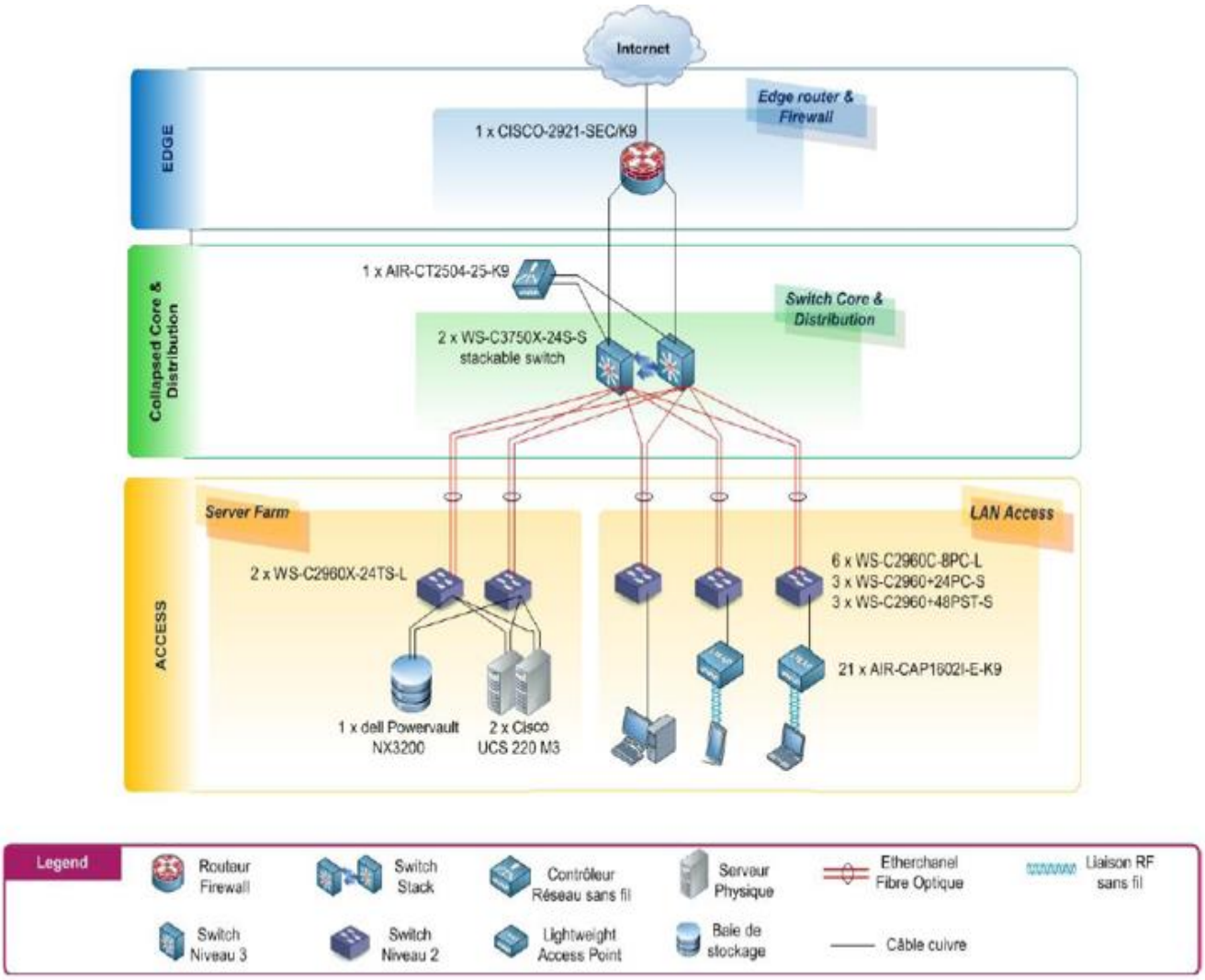


***Figure 4.01:*** Architecture globale de l'INSCAE

### *4.3.2 DMZ de l'INSCAE*

Les serveurs web et les autres serveurs accessibles depuis Internet de l'entreprise se trouvent tous dans le DMZ de l'entreprise.

Comme on a déjà vu, le but de la mise en place d'un DMZ est de pouvoir isoler le réseau où se trouvent les serveurs accessibles depuis Internet du réseau local. Ainsi la compromission des serveurs du DMZ n'affecte pas le réseau local (LAN : Local Area Network).

Principalement, il y a deux UCS (Unified Computing System) Cisco dans le DMZ de l'INSCAE. Un Cisco UCS est un serveur composé de la partie hardware et un support de virtualisation, la gestion des logiciels.

Sur l'un d'eux tourne l'intranet et sur l'autre est hébergé le site web de l'INSCAE. L'intranet de l'INSCAE tourne sur un système Debian et le serveur d'hébergement est un serveur CentOS.

### 4.4 Analyse des besoins de l'entreprise

On sait que tout système exposé à Internet est vulnérable et susceptible d'être attaqué tôt ou tard. Ainsi, en prenant conscience de ce fait indéniable, on a choisi de renforcer la sécurité du DMZ de l'INSCAE. Comme on a vu, penser comme un hacker est un moyen de détecter les failles qui existent au sein d'un système. Ainsi on a opté pour la réalisation d'un test de pénétration des serveurs de l'entreprise. Ensuite, la mise en place d'un IDS est une solution vraiment intéressante et assez aisée à mettre en place.

En effet, en prenant en compte la situation actuelle de l'entreprise, utiliser des solutions de sécurisations qui sont propriétaires peut être vraiment coûteux. Or on ne peut pas nier que la présence de l'entreprise sur Internet augmente la probabilité de se faire attaquer. Ainsi l'entreprise a besoin de solution de sécurité efficace, mais aussi open source.

De ce fait, on a adopté les solutions suivantes pour répondre aux différents besoins de l'entreprise :

- Mesure préventive : mise en place d'un système de défense (détection d'intrusion, monitoring)
- Réalisation d'un test de pénétration pour assimiler la capacité du DMZ de l'entreprise à faire face aux différentes attaques et menaces.

### 4.5 Méthodologie pour la sécurisation du DMZ de l'INSCAE

Dans cette section, on va voir les différentes étapes qu'on a suivies pour la sécurisation du DMZ de l'INSCAE.

D'une manière générale, les mesures qu'on a prises peuvent être classées en deux catégories :

- Sécurisation offensive
- Sécurisation défensive

### *4.5.1 Sécurisation offensive : test de pénétration au niveau du DMZ*

Comme on a déjà vu, ce test permet de savoir les vulnérabilités existant sur le site web, de les exploiter et de les corriger pour réduire les vecteurs d'attaques des hackers et voir les attaques existant sur le serveur avant eux.

On a réalisé un test de pénétration du site web de l'entreprise en procédant de la manière suivante :

*a) Information Gathering*

On a utilisé Shodan et Google hacking database pour regrouper les informations disponibles publiquement. En effet, on a réalisé le test de pénétration en boîte grise, c'est à dire, certaines informations ont été acquises et certaines sont les fruits de recherches sur des bases de données publiques et avec les interactions directes avec le serveur (le scan des ports, scan d'OS).

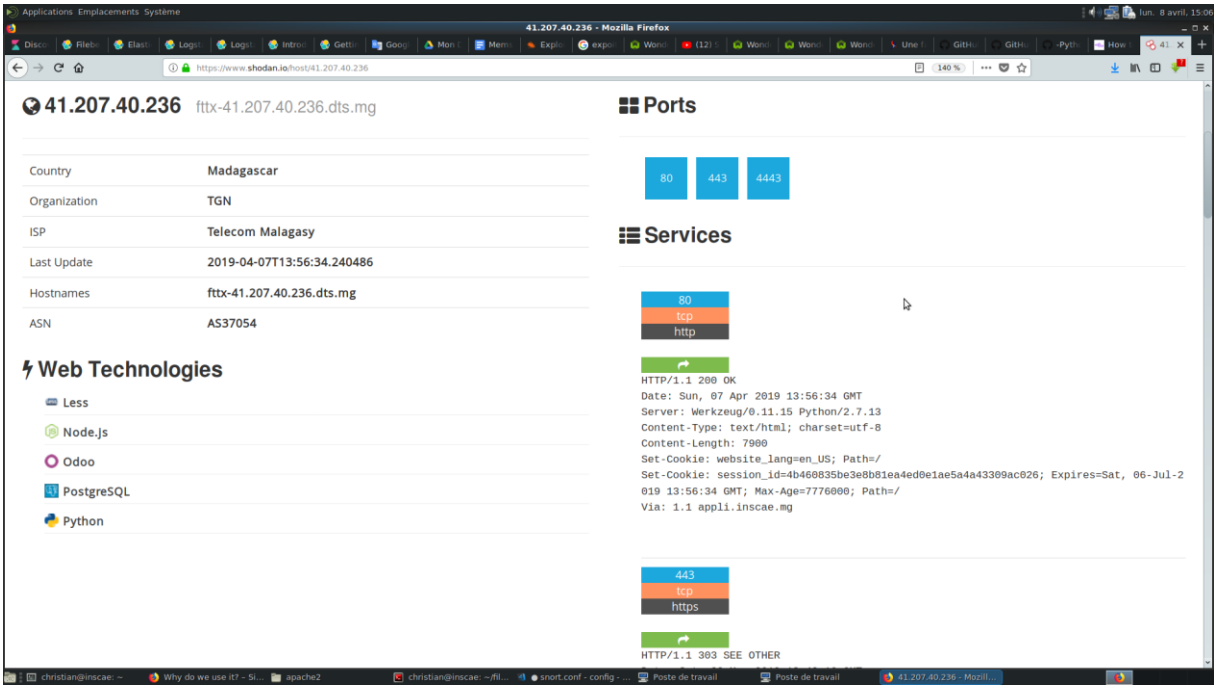


***Figure 4.02 :*** recherche d'information avec des bases de données publiques

On a aussi utilisé Nmap pour le scan actif sur le serveur. Après ce scan, on peut déjà lister les services disponibles sur le serveur de l'entreprise en se basant sur la liste des ports. Il faut tout de même noter que connaître les ports ouverts et disponibles sur un serveur n'entraîne forcément pas la connaissance des services qui tourne au-dessus du serveur. Nmap peut aller au-delà d'un simple scan général.

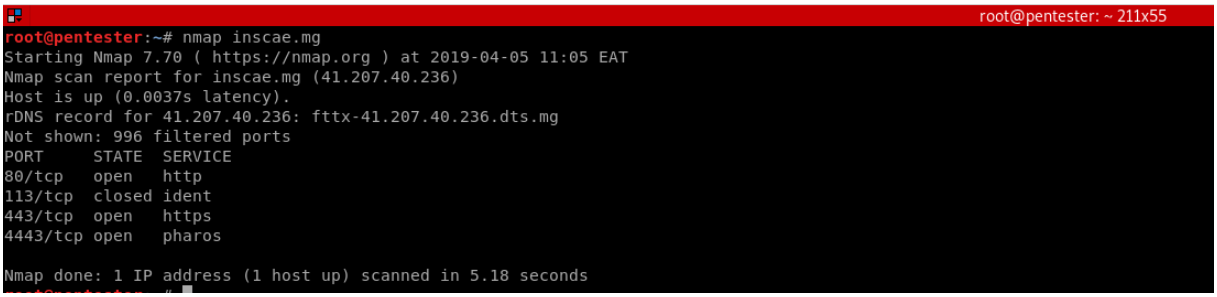


***Figure 4.03 :*** scan général avec Nmap

En plus des scans réalisés avec Nmap, on a utilisé une base de données publique à l'aide de Shodan. Ce dernier est un site web spécialisé dans la recherche d'objets connectés à Internet, et ayant donc une adresse IP visible sur le réseau. Il permet ainsi de trouver une variété de serveurs web, de routeurs ainsi que de nombreux périphériques tels que des imprimantes ou des caméras. Une telle requête est traitée avec une simple analyse de l'en-tête HTTP renvoyée par l'appareil ou le serveur. Il est alors possible de récupérer des listes d'éléments spécifiques. Pour chaque résultat, on trouve l'adresse IP du serveur ainsi que d'autres types d'informations sensibles, mais accessibles.

*b) Threat modeling*

Les menaces qui peuvent nuire à la sécurité informatique de l'entreprise sont :

- Les scripts kiddies ou les personnes qui téléchargent des scripts, déjà prêts sur Internet, et essaient ces scripts sur des sites d'entreprise ou sur des systèmes publics. En fait, la disponibilité de plusieurs outils d'hacking open source donne la possibilité à des personnes, qui n'a pas vraiment de compétence technique, à nuire à système si des mesures de sécurité nécessaires ne sont pas prises.
- D'autres hackers qui peuvent être engagés par des concurrents pour nuire à la réputation de l'entreprise et salir son image publique.

*c) Analyse de risque*

Il convient pour chaque entreprise d'évaluer les risques, c'est-à-dire les mesurer en fonction de la probabilité de leurs apparitions et de leurs effets possibles. Les entreprises ont tout intérêt à évaluer, quoique grossièrement ces risques et les moyens à mettre en œuvre, en fonction de leurs coûts.

Dans notre situation, les risques se pèsent surtout sur les serveurs du DMZ. En effet, les serveurs du Datacenter sont des cibles potentielles pour les hackers, car ce sont ces serveurs qui sont exposés à Internet. Ces derniers constituent les fondations du système d'information de l'INSCAE donc si ces derniers s'effondrent suite à une quelconque attaque, les dégâts seraient vraiment gigantesques pour l'activité quotidienne de l'entreprise.

Ainsi on peut dire que les principaux risques sont la vulnérabilité des serveurs dans lesquels tournent l'Intranet et l'hébergement web de l'INSCAE. Donc notre but principal est d'apporter le maximum en matière de sécurité pour ces serveurs.

*d) Analyse des vulnérabilités (Vulnerability Analysis)*

Dans cette phase, on a réalisé un scan de vulnérabilités sur le site web de l'INSCAE.

Pour cela on utiliser un outil de scan de vulnérabilité appelé Nikto.

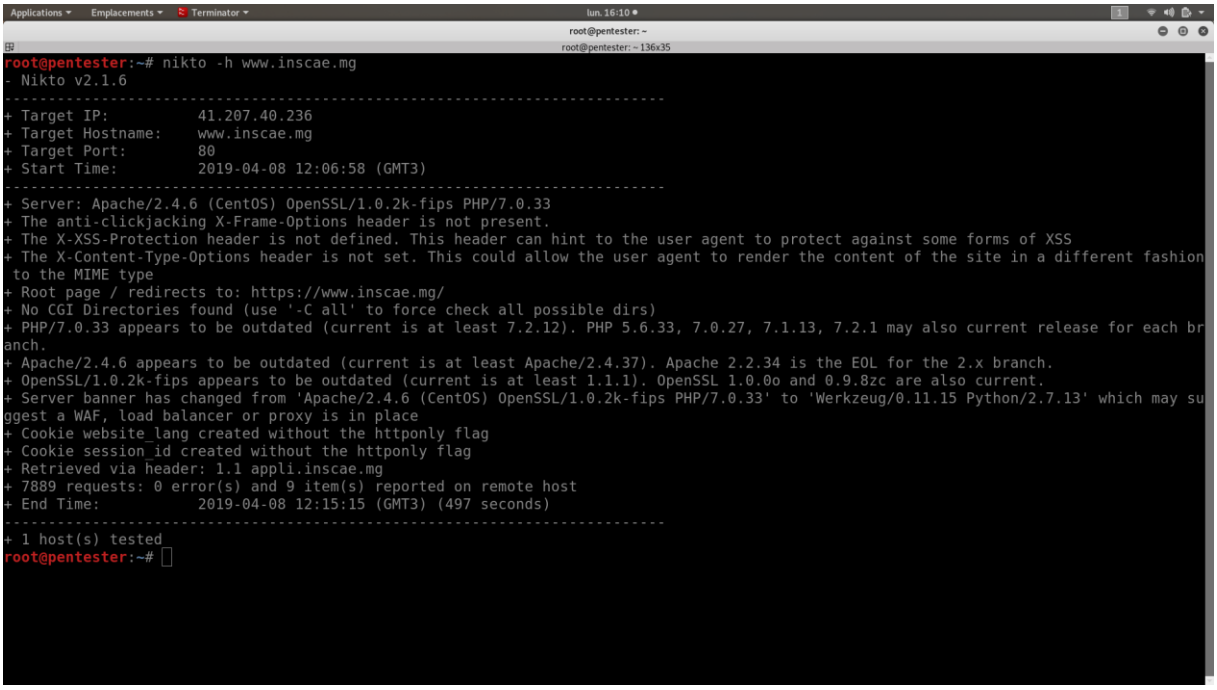


***Figure 4.04 :*** Scan de vulnérabilité de site de l'entreprise utilisant Nikto

Le scan de vulnérabilité permet de voir des informations sur la configuration du serveur, sur les headers. Les informations obtenues permettent de bien calibrer l'attaque et permettent aussi de ne pas perdre trop de temps pendant le test de pénétration.

Pendant un scan de vulnérabilité, on peut par exemple avoir accès à certains dossiers qui ne sont pas censés être exposés, ce qui facilite beaucoup les taches d'un Ethical hacker.

*e) Exploitation et post exploitation*

Pour notre cas, on a essayé d'exploiter les failles possibles existant sur les serveurs, et/ou sur l'application qui tourne sur le serveur.

Principalement, on s'est focalisé sur les attaques type injection SQL et failles XSS et les attaques par déni de service.

En raison de l'exposition de certains documents et dossiers confidentiels, aucune capture d'écran lors de l'exploitation et de la post-exploitation ne sera présente dans cet ouvrage.

*f) Rapport de test de pénétration*

La figure ci-dessous montre quelques parties du rapport :

Missing HTTP security headers

| HTTP Security Header | Header Role | Status |
|---|---|---|
| X-Frame-Options | Protects against Clickjacking attacks | Not set |
| X-XSS-Protection | Mitigates Cross-Site Scripting (XSS) attacks | Not set |
| Strict-Transport-Security | Protects against man-in-the-middle attacks | Not set |
| X-Content-Type-Options | Prevents possible phishing or XSS attacks | Not set |

***Figure 4.05 :*** Rapport sur quelques problèmes au niveau de http

### *4.5.2 Sécurisation défensive : mise en place de système de détection d'intrusion Snort*

4.5.2.1 Architecture de la solution

Snort est un système de détection et prévention d'intrusion « open source ». Il permet de détecter les attaques en utilisant un système de règle qui contient les signatures d'une attaque. Snort génère des logs lorsqu'il détecte une activité malveillante.

On sait aussi que les serveurs web génèrent beaucoup de logs lorsqu'ils sont en production. Ainsi, pour renforcer la sécurité du DMZ de l'entreprise, on a choisi de mettre en place aussi un système de monitoring et on a choisi la suite elastic (elastic stack) pour cela.

Elastic Stack, anciennement ELK (Elasticsearch, Logstash, Kibana), est une suite d'outils, qui ensemble permet de superviser des serveurs. Différents logs provenant de différentes sources : Snort, serveurs Apache.

Pour mettre en place Elastic stack :

- Il faut que Beats et ses sous-modules soient à installer sur les serveurs clients à superviser. Le rôle de beat est de récupérer les logs (à l'aide de Filebeat) et informations machine (CPU, RAM, Disk) avec Metricbeat.
- Logstash collecte ces données (provenant de beat), les transforme (filtrer, enrichir) si besoin et les insère dans Elasticsearch
- Elasticsearch stocke et index toutes les données, c'est-à-dire les logs provenant de différentes sources.
- Kibana est responsable de l'interface, permettant de créer des tableaux de bord personnalisés, et de chercher des informations dans Elasticsearch.

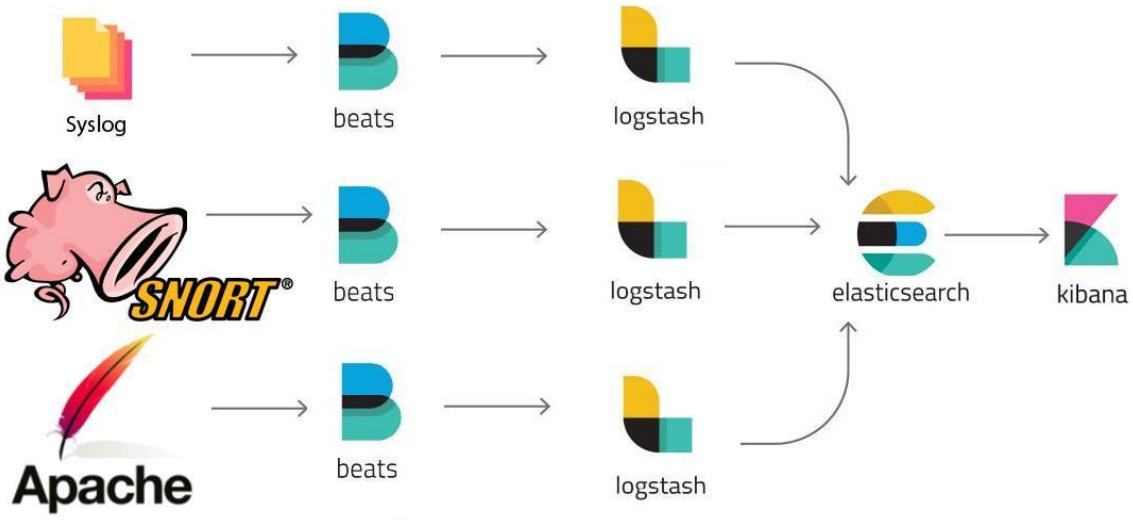


***Figure 4.06 :*** Architecture globale de la solution

La figure ci-dessus représente le flux de données dans la solution qu'on a proposée. Tous les logs provenant de Snort et des serveurs apache sont ingérés par beat. Ensuite, beat passe les données à logstash qui les traite et les donne à Elasticsearch. C'est ce dernier qui sera responsable de l'indexation et du stockage.

4.5.2.2 Snort

C'est l'IDS qu'on a choisi de déployer pour s'occuper de la détection d'intrusion dans notre serveur et pour la détection des attaques.

4.5.2.3 Architecture de Snort

Snort a une architecture organisée en module. La figure suivante représente l'architecture de base de Snort.

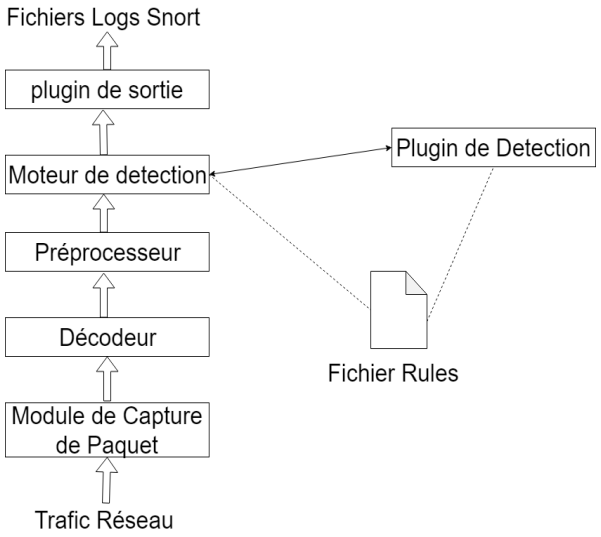


***Figure 4.07:*** Architecture de Base de Snort

| Modules | Description |
|---|---|
| Module de Capture de paquet | Ce module a été construit à partir de libcap (librairie de programmation qui permet l'accès à la capture de paquet qui est une fonctionnalité fournie par un OS). Il permet de faciliter la capture de Paquet |
| Décodeur | Ce module dissecte les paquets capturés en différentes structures de données et identifie les liens à vérifier dans le module suivant, comme les tentatives de connexion suspectes à Ports TCP / UDP ou trop de paquets envoyés sur une courte période. |
| Préprocesseurs | • Ils peuvent être utilisés soit pour examiner les paquets pour une activité suspecte ou modifier les paquets pour que le prochain module puisse interpréter correctement ces paquets.<br>• Les autres préprocesseurs sont responsables de la catégorisation du trafic afin que le prochain module puisse correspondre exactement signatures. Ces |

| | |
|---|---|
| | préprocesseurs déjouent les attaques qui tentent d'échapper au moteur de détection de SNORT en manipulant le trafic. |
| Moteur de détection | Ce module utilise des plugins de détection et fait correspondre les paquets à des règles ou « Rules » chargé en mémoire durant l'initialisation de Snort. |
| Plugins de détection | La définition du plug-in de détection se trouve dans les fichiers de règles. Ils sont utilisés pour identifier des modèles. |
| Fichiers de règles | Ce sont des fichiers texte contenant une liste de règles. La syntaxe comprend les protocoles, les adresses et certaines autres données importantes. |
| Plugins de sortie. | Ce module formate les notifications (alertes, les logs) pour l'utilisateur. |

***Tableau 4.01:*** Les modules composant Snort

4.5.2.4 Configuration de Snort en tant que NIDS dans le DMZ

*a) Environnement utilisé*

La plupart des serveurs de l'INSCAE utilisent la distribution Debian Linux avec la version 9, nom de code stretch. Ainsi, on effectuera la configuration et l'installation en utilisant comme système d'exploitation Debian 9.

*b) Mise en place de Snort en tant que NIDS dans le DMZ*

On a configuré Snort en tant que NIDS dans le DMZ de l'entreprise.

On a choisi d'utiliser un NIDS pour pouvoir avoir une vue globale du DMZ de l'INSCAE. En effet, on a besoin d'avoir une vue globale du DMZ pour pouvoir mettre en place un système de monitoring efficace.

Ainsi, lorsqu'une attaque est initiée au niveau du DMZ, si Snort est bien configuré, il les détectera.

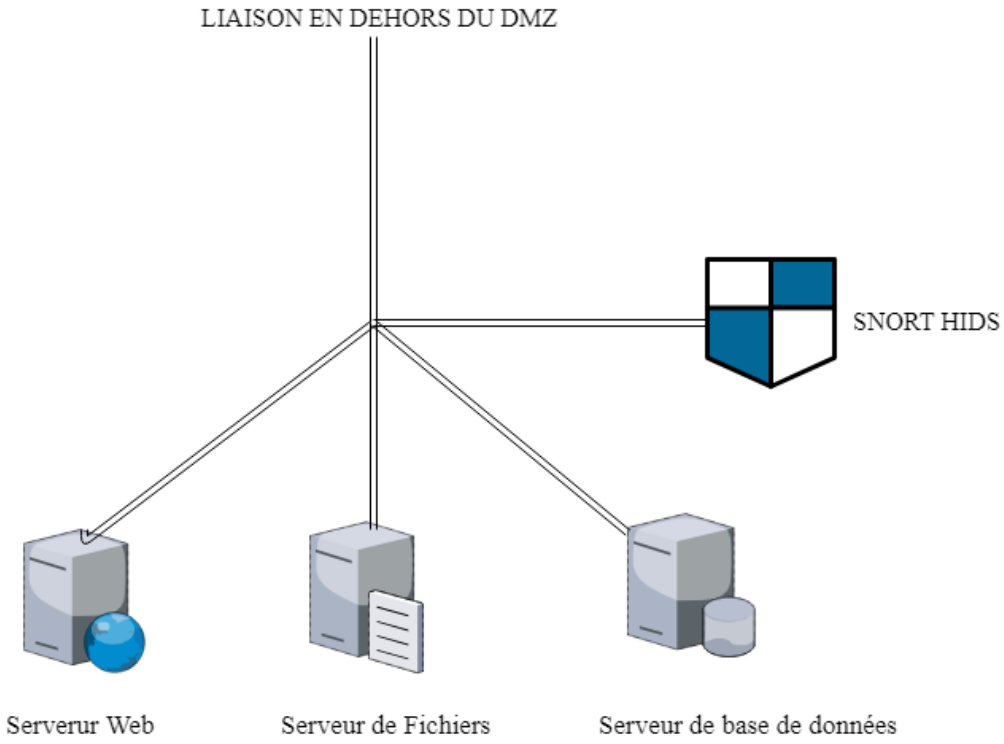


***Figure 4.08 :*** architecture de la solution NIDS mise en place

### *4.5.3 Mise en place du stack Elastic pour la visualisation, traitement et enrichissement des logs*

4.5.4.4 Généralité

On a choisi d'utiliser la suite elastic (ELK stack : Elasticsearch, Kibana, Logstash) pour la visualisation des logs de Snort et des logs des serveurs (apache). Mais le rôle d'elastic stack ne se limite pas seulement aux visualisations des logs de Snort, on peut aussi analyser d'autres logs pour détecter d'autres attaques (logs des serveurs apache par exemple). Elastic stack permet aussi de faire une investigation sur des incidents (en termes de sécurité informatique) qui se sont produits au sein de l'entreprise. Elle permet aussi de réaliser ce qu'on appelle Threat Hunting ou chasse des menaces. Cela consiste à chercher tous les indices nécessaires pour savoir comment un attaquant a compromis un système et pour y remédier à différents damages.

La force de l'Elastic stack réside dans sa capacité à analyser, stocker et indexer efficacement un très grand volume de données (logs) et permet la visualisation avec une facilité assez considérable.

#### 4.5.4.5 Beats

Beats sont des expéditeurs de données open source qu'on installe en tant qu'agents sur les serveurs pour envoyer des données opérationnelles à Elasticsearch.

Il y a plusieurs types de Beats, mais on va utiliser Filebeat.

Filebeat est un chargeur de logs léger permettant de transférer et de centraliser les données de logs. Installé en tant qu'agent sur des serveurs, Filebeat surveille les fichiers logs, collecte les événements de log et les transmet à Elasticsearch ou à Logstash pour l'indexation.

L'installation de Filebeat se fait de la manière suivante :

```
# curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-6.7.1-amd64.deb
# sudo dpkg -i filebeat-6.7.1-amd64.deb
```

#### 4.5.4.6 Logstash

*a) Généralité*

Logstash est un moteur de collecte de données open source doté de fonctionnalités de traitement en pipeline en temps réel. Logstash peut unifier de manière dynamique les données provenant de sources différentes et les normaliser dans les destinations souhaitées.

Logstash permet d'enrichir les logs et les données en utilisant différentes techniques comme les filtres.

*b) Installation*

Logstash nécessite Java 8 ou Java 11 installé.

Pour installer logstash, il faut tout d'abord enregistrer le dépôt où se trouve le paquet de logstash dans */etc/apt/sources.list.d/elastic-6.x.list* :

```
# echo "deb https://artifacts.elastic.co/packages/6.x/apt stable main" | tee -a /etc/apt/sources.list.d/elastic-6.x.list
```

Ensuite, on installe le paquet logstash :

```
# sudo apt-get update && apt-get install logstash
```

La figure suivante montre les résultats après avoir parsé les logs provenant de Filebeat . En effet, logstash permet d'enrichir les logs et de les traiter pour obtenir les maximums d'informations et pour faciliter la tâche de monitoring. Ce sont ces résultats qui seront envoyés dans elasticsearch pour l'indexation et le stockage.

Après indexation, ce sont ces résultats qui seront accessibles via Kibana avec une interface utilisateur intuitive et facile à interpréter par rapport à la lecture sur la console.

4.5.4.7 Elasticsearch

Elasticsearch est un moteur d'analyse, de recherche et de stockage distribué en temps réel. Elasticsearch excelle dans l'indexation de flux de données semi-structurées, telles que des logs.

Installation

Elasticsearch nécessite au moins Java 8 installé sur la machine.

On installera Elasticsearch à partir du tar disponible sur le site officiel :

Téléchargement d'Elasticsearch :

```
# curl -L -O https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-6.7.1.tar.gz
```

Ensuite on va l'extraire :

```
# tar -xvf elasticsearch-6.7.1.tar.gz
```

Enfin, pour le lancer, on va dans le dossier bin et on l'exécute :

```
# cd elasticsearch-6.7.1/bin
```

```
# ./elasticsearch
```

4.5.4.8 Kibana

*a) Généralité*

Kibana est une plateforme d'analyse et de visualisation open source conçu pour fonctionner avec Elasticsearch. Kibana permet de rechercher, d'afficher et d'interagir avec les données stockées dans les index Elasticsearch. On peut facilement effectuer une analyse de données avancée et visualiser des données dans une variété de graphiques, de tableaux et de cartes.

Kibana facilite la compréhension de gros volumes de données. Son interface simple, basée sur un navigateur, permet de créer et de partager rapidement des tableaux de bord dynamiques affichant les modifications apportées aux requêtes Elasticsearch en temps réel.

*b) Installation*

Kibana tourne sur nodejs donc il faut que nodejs soit installé.

L'archive Linux pour Kibana v6.7.1 peut être téléchargée et installée comme suit :

```
# wget https://artifacts.elastic.co/downloads/kibana/kibana-6.7.1-linux-x86_64.tar.gzshasum -a 512 kibana-6.7.1-linux-x86_64.tar.gz
# tar -xzf kibana-6.7.1-linux-x86_64.tar.gz
```

*c) Description de l'interface de Kibana*

Dans cette partie on va voir les différentes parties constitutives de l'interface de Kibana.

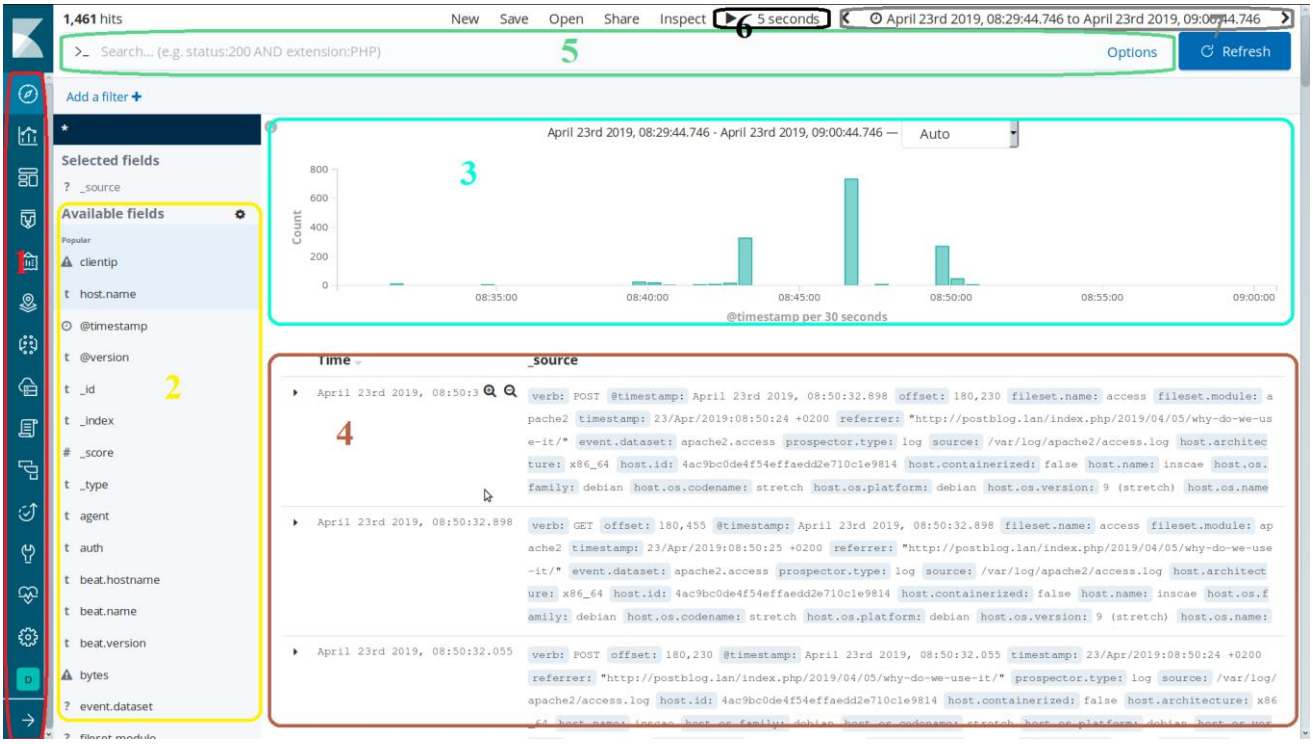


***Figure 4.09:*** Interface de visualisation des logs de Kibana

La figure ci-dessus montre l'interface de visualisation de Kibana.

L'interface de Kibana est divisée principalement en deux grandes parties :

- L'interface de visualisation
- Le Dashboard ou le tableau de bord

On va voir un à un les zones de cette interface. Il y a sept (7) principales sections dans l' interface de visualisation des logs .

(1) Cette partie montre les menus disponibles
(2) Cette section montre les champs des logs
(3) Histogramme qui représente les nombres de requêtes dans une durée définie dans (7)
(4) Liste des logs
(5) Champs de recherche qui permet d'effectuer
(6) Temps de rafraîchissement pour l'actualisation des données affichées
(7) Intervalle de temps, choisi, pendant lequel les logs ont été capturés.

### *4.5.4 Simulation d'attaque et de monitoring*

4.5.4.1 Outils utilisés pour la simulation

Dans cette partie on va procéder à une simulation d'attaque d'un serveur. Ce dernier aura Snort comme IDS et on va superviser le serveur avec la suite elastic.

- VMWare Workstation

C'est un outil de virtualisation de poste de travail créé par la société VMware, il peut être utilisé pour mettre en place un environnement de test pour développer de nouveaux logiciels, ou pour tester l'architecture complexe d'un système d'exploitation avant de l'installer réellement sur une machine physique. Ici, on a utilisé VMWare pour faire tourner un serveur web.

- Serveur utilisé pour la simulation : Debian 9

La version 9.8 de Debian (connue sous le nom de Stretch) a été publiée le 16 février 2019. La version 9.0 a été initialement publiée le 17 juin 2017. On a choisi le système d'exploitation Debian pour la simulation, car c'est celle que l'entreprise utilise et ainsi, on peut aussi simuler l'environnement de l'entreprise.

- Parrot Linux :

C'est une distribution GNU / Linux libre et open source basée sur les tests Debian, conçue pour les experts en sécurité, les développeurs et les personnes sensibilisées à la vie privée.

Il comprend un arsenal entièrement portable pour la sécurité informatique et les opérations d'investigation numérique, mais il contient également tout ce dont vous avez besoin pour développer vos propres programmes ou protéger votre vie privée tout en surfant sur Internet.

Le système d'exploitation est livré avec l'environnement de bureau MATE préinstallé et est disponible en plusieurs versions pour répondre aux besoins des utilisateurs.

4.5.4.2 Déroulement de la simulation

On a mis en place Snort sur le serveur Debian pour pouvoir détecter toute tentative d'intrusion dans le serveur. On a aussi déployé la suite elastic sur ce dernier pour pouvoir le superviser.

On a mis en place en place un serveur web apache qui héberge un site WordPress pour la réalisation de la simulation.

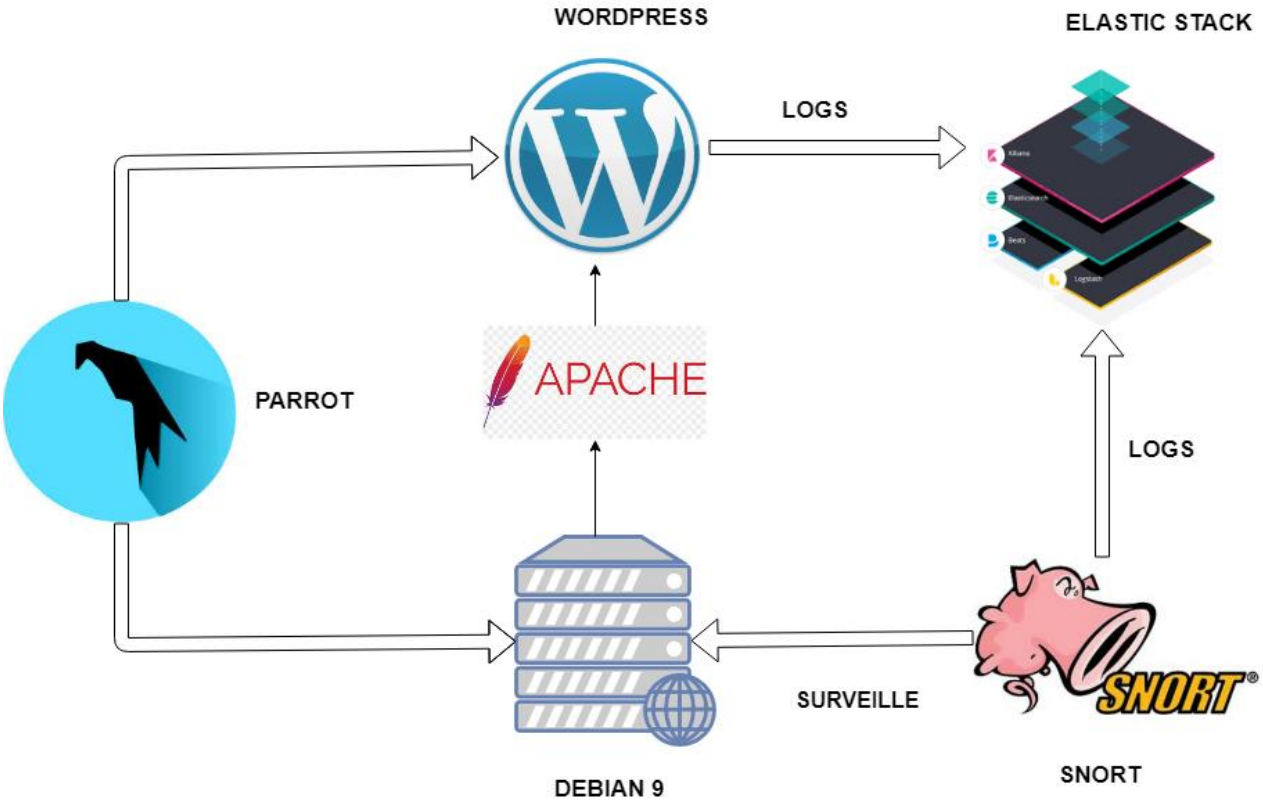


***Figure 4.10:*** Architecture de la simulation

La machine sous Parrot Linux servira d'attaquant dans la présente simulation.

Pendant la simulation, on va réaliser une série d'attaques contre le serveur web et le site WordPress qu'on a mis en place et on va voir si on arrive à détecter ces attaques grâce à l'architecture qu'on a mise en place. On se basera sur les logs fournis par Snort et les « Access logs » et « Error logs » du serveur apache pour la détection des attaques.

On considérera les scénarios suivants :

*a) Reconnaissance et scan du serveur avec Nmap*

Dans ce scénario, on va utiliser l'outil de scan Nmap ou Network Mapper pour réaliser une reconnaissance au niveau du serveur. Le but est de savoir les services qui tournent sur le serveur. Donc ce premier scénario, on a effectué une reconnaissance avant le lancement de quelques attaques.


***Figure 4.11:*** logs montrant la détection d'un scan avec Nmap

*b) Attaque DoS : déni de service avec hping3*

Dans ce deuxième scénario, on a lancé une attaque par déni de service pour altère le bon fonctionnement du serveur. Pour cela on a utilisé l'outil hping3.


***Figure 4.12:*** logs capturant une attaque DoS contre le serveur web

*c) Attaque par injection SQL*

Pour terminer la série d'attaques, on va s'attaquer au site web. On effectuera une attaque SQLi au niveau du site WordPress et on va voir si Snort arrive à détecter l'attaque qu'on lancé.

4.5.4.3 Visualisation et interprétations des résultats sur Kibana

*a) Interprétations des logs provenant de Snort*

On peut voir d'après l'expérience ci-dessus que Snort arrive bien à détecter les attaques qu'on a réalisées. Ce dernier a réussi à détecter ses attaques grâce aux signatures d'attaque connue qu ' on a pris soin de bien écrire. On peut aussi dire que la stack elastic nous a bien aidés dans la visualisation des logs de Snort. En fait, l'indexation des logs par Elasticsearch a permis de faire une recherche rapide des alertes causées par la détection des attaques.

*b) Logs provenant d'Apache*

Les logs provenant du serveur nous permettent d'obtenir beaucoup d'information sur ce qui se passe sur le serveur. En enrichissant ces logs, on peut avoir les nombres de requêtes pendant un intervalle de temps donné, l'user-agent du visiteur du site web, des informations sur l'hôte utilisé par les visiteurs, des informations sur les requêtes (code de réponse, les méthodes de requête) et tant d'autres. Toutes ces informations aident à voir si quelqu'un effectue des activités malveillantes sur le site web. Et ici, encore, la stack elastic a été de grande utilité, car c'est elle qui a permis d'effectuer des recherches, des tris, des visualisations avec des graphes et des figures, des histogrammes.

Dans cette partie de la simulation, on va voir quelques graphes obtenus avec Kibana, ensuite on va interpréter ces dernières.

- Tout d'abord, on va voir les codes de réponses obtenues par les utilisateurs du site par adresse IP.

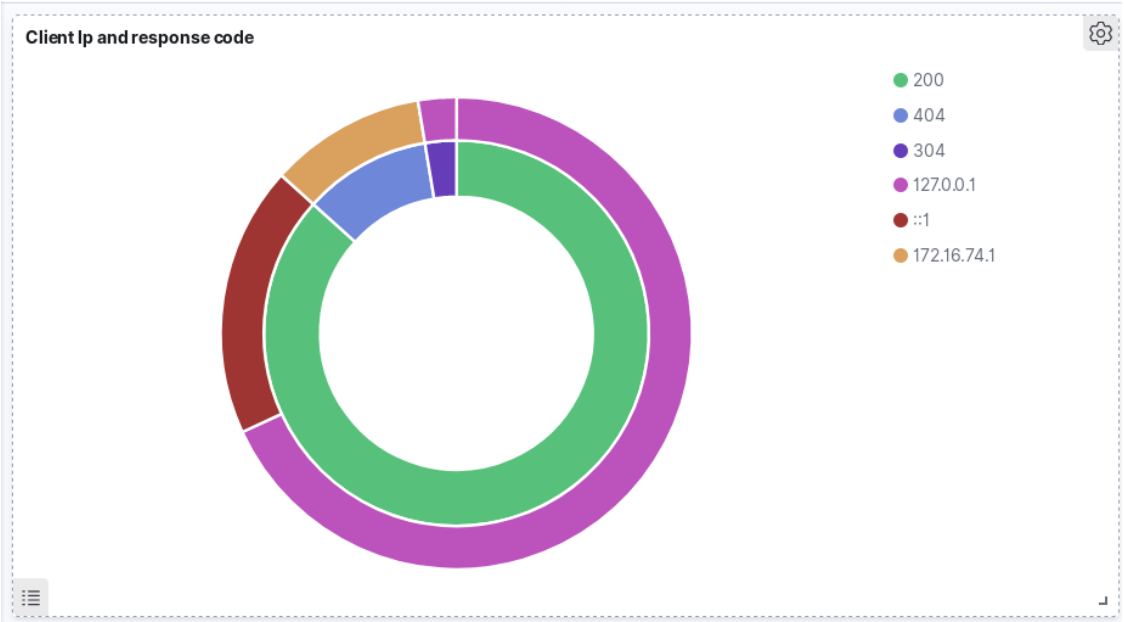


***Figure 4.13*** : code de réponse par adresse IP d'utilisateur

Cette visualisation permet de savoir les activités des utilisateurs du site. En effet, un utilisateur qui obtient toujours une réponse 404 peut être considéré comme un utilisateur malveillant. Mais, il ne faut pas simplement se fier à des simples interprétations, il faut regrouper les données et c'est après qu'on peut prendre des conclusions et des décisions.

- Ensuite, on va voir les méthodes de requêtes utilisées par l'utilisateur. Ceci permet de déterminer les différentes interactions d'un utilisateur avec le site. Tout seul, cette information ne sert pas à grande chose, mais combinée avec d'autres données qu'on a , elle constitue une mine d' informations .

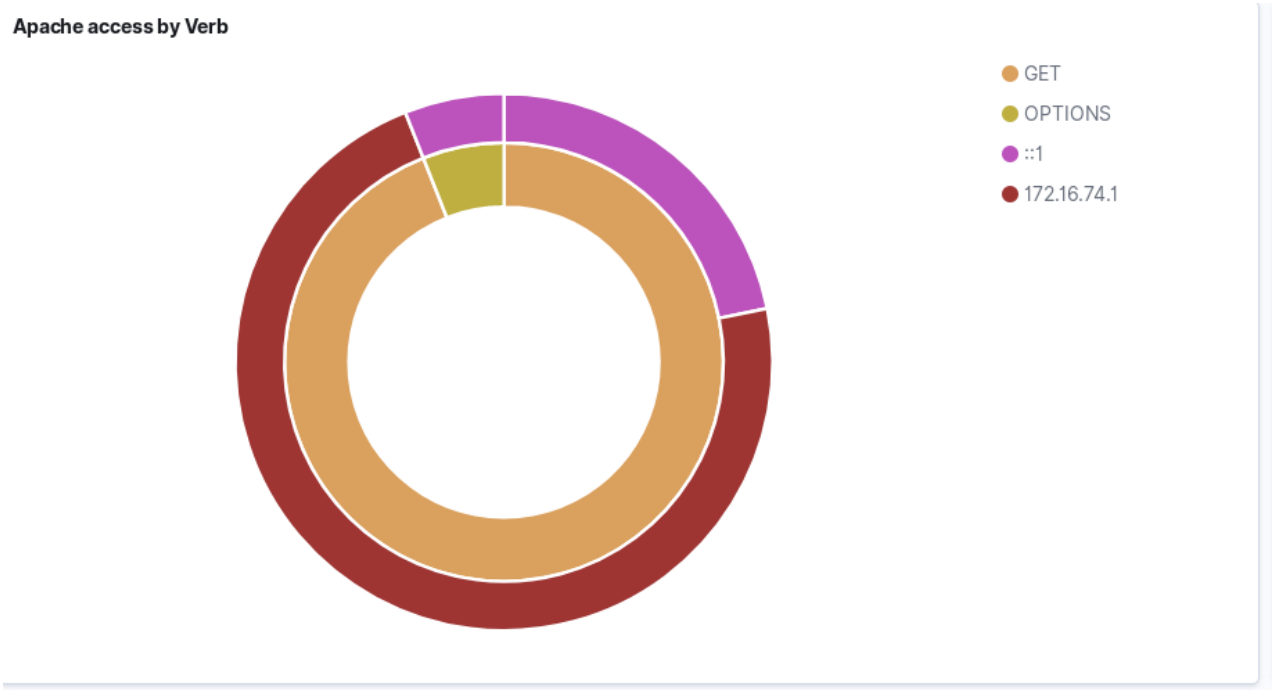


***Figure 4.14:*** Répartition des méthodes de requêtes par adresse IP

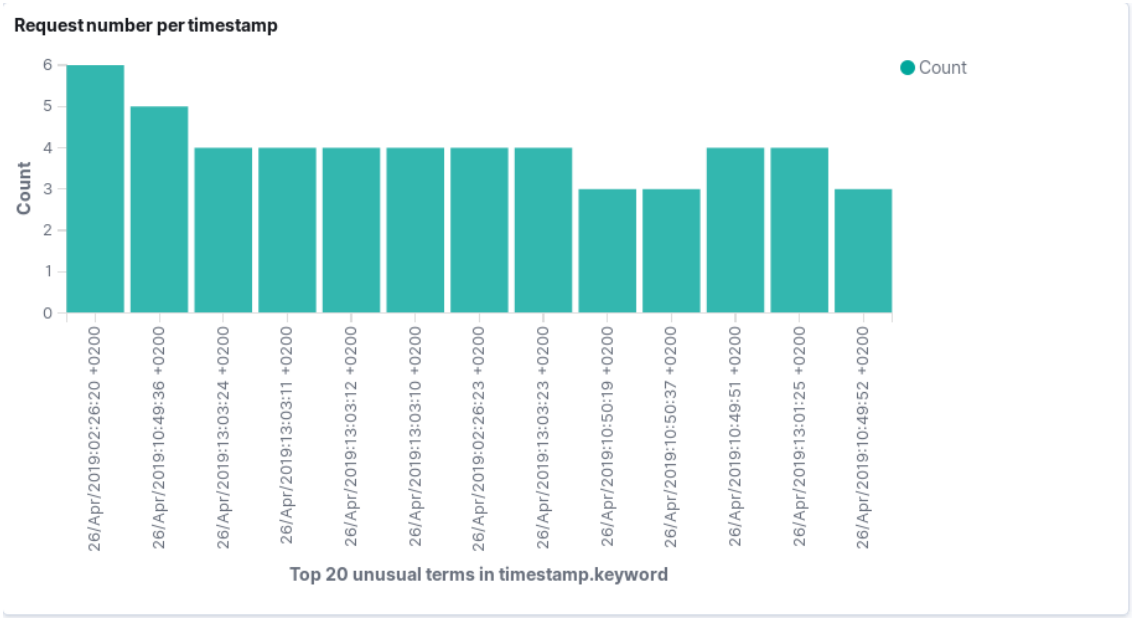


***Figure 4.15:*** Histogramme des nombres de requêtes en fonction du temps

- Enfin, la figure ci-dessus est un histogramme qui permet de voir en temps réels le nombre de Requêtes en direction du serveur. Cet histogramme permet de savoir s'il y a une surcharge de requête au niveau du serveur. Ainsi, des potentielles attaques DoS ou DDoS peuvent être détectés à l'aide de cet histogramme.

### 4.6 Conclusion

En résumé, pour pouvoir se défendre et lutter contre les attaques des hackers de nos jours, on a choisi d'implémenter une sécurité à la fois offensive et défensive. Rien n'est sécurisé à cent pour cent, tout est à mettre en question, ainsi, l'initiative de rester en veille par rapport à l'évolution technologique est importante.

# CONCLUSION GÉNÉRALE

En guise de conclusion, la prise de mesures défensives et offensives pour la sécurisation d'un système informatique va de pair de nos jours. Avec l'avancée des attaques et l'augmentation des outils de piratages open source, il est primordial pour toute entreprise d'être toujours sur ses gardes et surtout de ne jamais croire qu'elle est en sécurité. Rien n'est parfait, il n'y a jamais de sécurité assurée à cent pour cent. Ainsi, rester éveillé en termes de cybersécurité est toujours une bonne manière.

L'objectif principal de ce mémoire a été la mise en œuvre d'un système de monitoring de logs d'IDS et de serveurs web au sein de l'Institut INSCAE ainsi que la réalisation d'un test de pénétration pour mettre en évidence les différentes failles du DMZ de ce dernier.

L'IDS Snort est un système de détection d'intrusion assez efficace pour les attaques dont on possède la signature. Cependant, pour les attaques de type Zero-day ou les nouvelles attaques, Snort rencontre des difficultés pour leurs détections. En effet, c'est la limite de la technique de détection basée sur les signatures. Ainsi, il serait intéressant d'explorer d'autres techniques de détection d'intrusion comme celle basée sur les anomalies qui essaie de définir un comportement normal et se base sur ce dernier pour la classification des trafics.

La suite elastic a un potentiel énorme en termes de traitement, indexation, stockage et visualisation de données. L'analyse des logs a été rendue facile grâce à l'elastic stack. Il faut tout de même noter que le volume des logs généré par les systèmes est gigantesque et tôt ou tard il serait impossible pour un humain d'analyser un tel volume de donnée. Ainsi, l'utilisation de l'apprentissage automatique est une solution envisageable et même incontournable pour la résolution du problème du volume des logs recueillis. Utiliser ce type d'algorithme pour analyser automatiquement les logs est donc une suite logique de ce projet.

Enfin, la réalisation d'un test de pénétration du système informatique a permis de mettre en évidence différentes vulnérabilités et cela a permis la correction de ces dernières. Cependant, certaines tâches sont un peu répétitives et il serait intéressant d'utiliser des techniques d'automatisation pendant le test de pénétration comme l'utilisation du Machine Learning pour la réalisation de certaines attaques et exploitations. Nombreux outils de Machine Learning pour les tests de pénétration existent. Et ils apportent des aides précieux dans la recherche de tous les angles d'attaques disponibles au sein d'un système informatique.

## ANNEXE 1 CONCEPTS DE BASE D'ELASTICSEARCH

- Cluster

Un cluster est un ensemble d'un ou plusieurs nœuds (serveurs) qui, ensemble, contiennent l'ensemble des données et fournissent des fonctionnalités fédérées d'indexation et de recherche sur tous les nœuds.

- Node : Nœud

Un nœud est un serveur unique faisant partie du cluster, stockant les données et participant aux fonctionnalités d'indexation et de recherche du cluster.

- Index

Un index est un ensemble de documents présentant des caractéristiques similaires. Par exemple, on peut avoir un index pour les logs d'un firewall, un autre index pour les logs des IDS.

- Document

Un document est une unité d'information de base pouvant être indexée. Le document est exprimé en JSON (JavaScript Object Notation), format d'échange standard de données dur Internet.

- Shards

Un index peut potentiellement stocker une grande quantité de données pouvant dépasser les limites matérielles d'un seul nœud. Par exemple, un index unique d'un milliard de documents occupant 1 To d'espace disque peut ne pas tenir sur le disque d'un seul nœud ou peut être trop lent pour traiter les demandes de recherche d'un seul nœud.

Pour résoudre ce problème, Elasticsearch offre la possibilité de subdiviser les index en plusieurs fragments appelés « shards ». Lorsqu'on crée un index, on peut simplement définir le nombre de fragments qu'on souhaite. Chaque « shard » est en soi un "index" totalement fonctionnel et indépendant pouvant être hébergé sur n'importe quel nœud du cluster.

## ANNEXE 2 EXTRAITE DU FICHIER DE CONFIGURATION DE LOGSTASH

```
filter {
   if [type] in [ "apache" , "apache_access" , "apache-access" ]  {
      grok {
         match => [
         "message" , "%{COMBINEDAPACHELOG}+%{GREEDYDATA:extra_fields}",
         "message" , "%{COMMONAPACHELOG}+%{GREEDYDATA:extra_fields}"
         ]
         overwrite => [ "message" ]
      }
      mutate {
         convert => ["response", "integer"]
         convert => ["bytes", "integer"]
         convert => ["responsetime", "float"]
      }
      date {
         match => [ "timestamp" , "dd/MMM/YYYY:HH:mm:ss Z" ]
         remove_field => [ "timestamp" ]
      }
      useragent {
         source => "agent"
      }
   }
   if [type] in ["apache_error","apache-error"] {
      grok {
         match => ["message", "\[%{WORD:dayname} %{WORD:month} %{DATA:day}
%{DATA:hour}:%{DATA:minute}:%{DATA:second} %{YEAR:year}\]
\[%{NOTSPACE:loglevel}\] (?:\[client %{IPORHOST:clientip}\]
){0,1}%{GREEDYDATA:message}"]
         overwrite => [ "message" ]
      }
      mutate
      {
         add_field =>
         {
            "time_stamp" =>
"%{day}/%{month}/%{year}:%{hour}:%{minute}:%{second}"
         }
      }
      date {
         match => ["time_stamp", "dd/MMM/YYYY:HH:mm:ss"]
         remove_field => [
"time_stamp","day","dayname","month","hour","minute","second","year"]
      }
   }
}
```

***Figure A2.01 :*** Extrait de configuration de logstash

## BIBLIOGRAPHIE


[1] TATEB Dehia. « *Mise en œuvre d'une solution de sécurité basée sur ids cas d'étude : entreprise Algérie télécom, mémoire de master en informatique* », juin 2014

[2] Laurent Poinsot , Cours *« Sécrypt »* , Chap. I : Introduction à la sécurité informatique, UMR 7030 – Université Paris 13- Institut Galilée

[3] Jennifer Vesperman , « *Introduction to Physical Security and Security of Services* » , 24 Février

[4] Laurent Bloch, Christophe Wolfhugel, «*Sécurité informatique Principes et méthode à l'usage des DSI, RSSI et administrateurs* », 2ème édition, mai 2009

[5] Gary Hall, Erin Watson, « *Hacking : Computer hacking, Security Testing, Penetration Testing And Basic Security* » , Décembre 2016

[6] Pascal Brangetto, Emin Çalişkan, Henry Rõigas, « *Cyber Red Teaming* » , 2015

[7] Jonathan A. Zdziarski jonathan@zdziarski.com , *« DATA CENTER THREATS AND VULNERABILITIES »,* article posté *le* 22 Février 2017

[8] Mattias Eriksson , « *An example of Man-in-the-middle Attack Against Server Autheticated SSL-sessions* » , 1996

[9] Ben Zahler, Isabel Steiner , « *Man in the middle (MITM) attack* »

[10] Ross Anderson and Mike Bond , *« The Man-in-the- Defence »Middle* , 2006

[11] VASCO Data Security , « *Mitigating Human Risk in Banking Transactions* » , 2015

[12] Claude Chaloux, *« Le Phishing » ,* Octobre *2007*

[13] Shahram Monshi Pouri, Nikunj Modi , *« Trojans and Backdoors »* , 24 Octobre 2006

[14] Brian Komar , Ronald Beekelar , Joern Wettern, PhD , *« Firewalls for dummies »* 2nd Edition, 2003

[15] Antonio Lioy, *« Firewall and IDS/IPS »* , Politecnico di Torino Dip. Automatica e Informatica , Decembre 2009

[16] Avi Kak , *« Computer and Network Security »* , Lecture 19: Proxy-Server Based Firewalls , 28 Mars 2019

[17] Pascal Cabaud UFR EILA, Université Paris Diderot , *« Un reverse proxy, pour quoi faire? »* , 2009

[18] Xiao Guo An, « *Differences Between Forward Proxy and Reverse Proxy* » – LinuxBabe , 27 decembre 2018

[19] Dimitri Ségard , « *Fonctionnement et mise en place d'un reverse proxy sécurisé avec Apache* », 8 mai 2011

[20] Sheila Frankel Karen Kent Ryan Lewkowski Angela D. Orebaugh Ronald W. Ritchey Steven R. Sharma , *« Guide to IPsec VPNs Recommendations of the National Institute of Standards and Technology »* , Decembre 2005

[21] https://www.cybrary.it/2015/05/summarizing-the-five-phases-of-penetration-testing , site consulté le 12 /03/2019.

**RENSEIGNEMENTS**

**Nom** : RANDRIANARISOA

**Prénoms** : Antsaniaina Christian

**Adresse** : Lot IAC 14 S Ambohidrapeto Itaosy

christianracrand@gmail.com

(+261) 34 43 095 56

Titre du mémoire :

**SÉCURISATION D'UN DMZ : TEST DE PÉNÉTRATION ET MISE EN PLACE D'UN SYSTÈME DE MONITORING**

Nombres de pages : 76

Nombres de tableaux : 02

Nombre de figures : 30

**Directeur de mémoire** : RANDRIARIJAONA Lucien Elino,

elrandria@yahoo.fr,

(+261) 32 04 747 95

## RÉSUMÉ

La mise en place d'un système de détection d'intrusion au sein d'une entreprise est déjà une mesure de sécurité standard. La principale différence des entreprises dans cette pratique, c'est la capacité des responsables de la sécurité des systèmes d'information (RSSI) à interpréter les alertes et les logs provenant de ces IDS. Concernant les logs, la stack elastic permet de faciliter l'interprétation des logs, mais il faudrait quand même un certain niveau de compréhension pour agir rapidement en cas de détection d'une attaque. Ainsi les RSSI doivent être capables de prendre les mesures nécessaires, en cas d'attaques, sinon la mise en place d'un système de monitoring est inutile.



**Mots clés** : IDS, ELK, Snort, Fichier Log, DMZ, Test de pénétration



## ABSTRACT

Setting up an intrusion detection system within a company is already a standard security measure. The main difference between companies in this practice is the ability of information systems security managers to interpret alerts and logs from these IDS. Regarding the logs, the elastic stack makes it the interpretation of logs easier, but it would still require a certain level of understanding to act quickly in case when an attack occurred. Thus the security managers must be able to take the necessary measures, in case of attacks, otherwise the establishment of a monitoring system is useless.



**Keywords :** IDS, ELK, Snort, DMZ, Log File, Penetration Testing