République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A. MIRA-BEJAIA

جامعة بجاية

Tasdawit n Bgayet

Université de Béjaïa

Faculté des Sciences Exactes

Département d'Informatique

MEMOIRE

EN VUE DE L'OBTENTION DU DIPLÔME DE MASTER PROFESSIONNEL

Domaine : Mathématiques et Informatique **Filière :** Informatique

Spécialité : Administration et sécurité des réseaux

Présenté par

Mme Bensahnoune Zahra Mme Benzouaoua Selma

Thème

Etude et proposition d'un référentiel de sécurité réseau informatique au profit de la Spa Général Emballage

Soutenu le 27 sept 2020 **Devant le jury composé de :**

Nom et Prénom		**Grade**	
M.	MOUHAND MOKTEFI	MAA	Univ. de Béjaia	Encadrant
M.	YAZID Mohand	MCA	Univ. de Béjaia	Encadrant
M.	KACIMI FARID	MAB	Univ. de Béjaia	Examinateur
M.	HOUHA AMEL	MAA	Univ. de bejaia	Examinateur

Année Universitaire : 2019/2020.

Remerciements

Nous remercions Dieu, le tout-puissant, de nous avoir donné le courage et la volonté pour mener à terme ce modeste travail et de nous avoir aidés tout au long de nos années d'études.

Nous adressons nos remerciements à Monsieur M.MOKTEFI de nous avoir encadrés et guidés.

Nous exprimons nos plus vives reconnaissances envers tout le personnel de l'entreprise SPA GENERAL EMBALLGE , plus particulièrement le personnel du service informatique pour le temps qu'ils nous ont consacré, leurs directives précieuses, et pour la qualité de leur suivi durant toute la période de notre stage.

Que les membres de jury trouvent ici nos sincères remerciements pour avoir accepté d'honorer par jugement notre tâche.

Dédicaces

Je dédie notre travail à ma très chère mère "Mekrez Nadia" et mon père "Bensahnoune Abderrahmane" pour tous leurs sacrifices et leurs amours, leurs soutiens et leurs prières, à mes très chers frères "Mouhou", "Samir", "Yacine" qui ont su être là au moindre besoin.

À mes chers grands pères et grandes mères défunts et ceux qui sont en vie.

À ma familles, pour leurs appuis et leur pertinence à nous donner l'envie de nous surpasser.

À tous ceux qui ont contribué de loin ou de près à l'aboutissement de ma modeste travail, Pour leur soutien tout au long de mon parcours universitaire.

Que ceci soit l'accomplissement de vos vœux tant allégés, et le fruit de votre soutien infaillible.

Merci d'être toujours là pour moi.

BENSAHNOUNE Zahra.

Dédicaces

Je dédie notre travail à ma très chère mère "Djelouah koko" et mon père "Benzouaoua L'hacene " pour tous leurs sacrifices et leurs amours, leurs soutiens et leurs prières, à mon très cher grand frère "Fouad" et ma trés chère soeur "Rima", qui ont su être là au moindre besoin, et à mon neveu "Yanis" et ma nièce "Léa", ainsi que mon beau-frère Hamza et ma belle-soeur Tasaadite.

À mes chers grands pères et grandes mères défunts et ceux qui sont en vie.

À ma familles, pour leurs appuis et leur pertinence à nous donner l'envie de nous surpasser.

À tous ceux qui ont contribué de loin ou de près à l'aboutissement de mon modeste travail, Pour leur soutien tout au long de mon parcours universitaire.

Que ceci soit l'accomplissement de vos vœux tant allégés, et le fruit de votre soutien infaillible.

Merci d'être toujours là pour moi.

BENZOUAOUA Selma

TABLE DES MATIÈRES

TABLE DES FIGURES

LISTE DES TABLEAUX

LISTE DES ABRÉVIATIONS

AUP	Politique d'Utilisation Acceptable
ARP	Address Resolution Protocol
CIA	Confidentialité Integrité Availabilité
COBIT	Control Objectives for Information and Related Technology
CPU	Central Processing Unit
DSI	Directeur des Systèmes d'Information
DDOS	Distributed Denial of Service
DOS	Denial of Service
DELL	Digital Electronic Link Library
DMZ	zones démilitarisées
DNS	Domain Name System
EISA	Entreprise Information Security
EC-COUNCIL	International Council of Electronique Commerce Consultants
GNS3	Graphical Network Simulator 3
HP	Hewlett-Packard
HTTP	Hypertext Transfer Protocol
ISO	organisation international de normalisation
IP	Internet Protocol
ITIL	Information Technology Infrastructure Library
IDS	Intrusion detection System
IPS	Intrusion Prevention System
ICMP	Internet Control Message Protocol

LAN	Local Aria Network
LAND	local area network denial
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
MTD	Maximum Tolerable Downtime
NIST	National Institute of Standards and Technology
OOB	L'attaque Out Of Band
OS	Operating System
RSSI	Responsable de Sécurité des Systèmes d'Informations
RFC	Requests For Comments
RJ 45	Registered Jack
RTO	objectif temps de récupération
RPO	objectif de rétablissement
SSL	Secure Socket Layer
SSID	Service Set Identifier
SPA	Société Par Actions
SD WAN	Software Defined Wide Area Network
TLS	Transpot Layer Security
TCP	Transmission Control Protocol
UDP	protocole de datagramme utilisateur
VPN	Virtual Private Network
VPN MPLS	MultiProtocol Label Switching
WIFI	Wireless Fidelity
WSUS	Windows Server Update Services
WWW	World Wide Web

INTRODUCTION GÉNÉRALE

L'homme dans sa nature essaie toujours de se développer et de s'adapter au fil du temps avec les changements. Pour cela, il n'a jamais cessé d'innover dans tous les domaines et de créer une assurance et une protection pour ces derniers ainsi que pour soi-même. La création de l'ordinateur a permis à un tas de secteurs de s'améliorer. Celui-ci est passé d'une version à une autre et d'un système basique à un système complexe. Cela n'exclus pas l'amplification du vol et de la malveillance ou ce qu'on appelle « le piratage ». Pour cela, les informaticiens n'ont jamais cessé de se creuser le cerveau afin de mettre au point des barrières, des antivirus, des systèmes de protection réseau....etc. De ce fait, nous allons nous intéresser à la sécurité des réseaux informatiques ou les risques sont divers. L'automatisation de l'information est devenue de plus en plus une nécessité dans chaque entreprise. Le partage des informations soit à travers un réseau local ou externe offre une opportunité d'invasion qui peut être facilement exploité par un pirate. Dans un autre contexte, la performance du réseau et la haute disponibilité des différents services applicatifs sont l'objet de chaque entreprise. C'est pourquoi l'intégration et la mise en place et l'implémentation de diverses politiques de sécurité protégeant le réseau d'entreprise contre les attaques internes et/ou externes est le souci de l'administrateur ; Ce qui conduit à notre travail qui s'intitule : « Etude et proposition d'un référentiel de sécurité réseau informatique » qui se réalisera au sein de la SPA General emballage – Akbou-. Ainsi, a fin d'apporter une réponse à notre problématique qui est la suivante :

Quelle sont les méthodes et les dispositifs les mieux adaptés afin d'avoir une sécurité optimale d'un réseau informatique ? Pour ce faire, nous avons deux hy-

pothèses :

- Dans le but de mieux sécuriser un réseau, il est important de sensibiliser le personnel ainsi qu'auditer régulièrement le système de sécurité déjà mis en place.
- Dans le but d'avoir une sécurité maximale, il est indispensable de mettre à jour tous les équipements, logiciels, et systèmes de sécurité régulièrement.

La réponse à notre problématique et la validation de ces hypothèses dépendra naturellement de l'analyse et de l'application du manuel de sécurité proposé, fait auprès de l'entreprise General emballage. Pour pouvoir affirmer ou rejeter l'une des hypothèses précédentes, porter une considération à notre problématique et mener à bien cette étude, nous avons choisi d'organiser le travail comme suit : Tout d'abord, dans le premier chapitre, nous allons commencer par traiter les grands traits sur la sécurité informatique, les attaques et les fondements des politiques de sécurité. Au second chapitre nous allons intéresser à la sécurité des réseaux, leurs architectures et nous allons par la suite proposer un référentiel contenant les bonnes pratiques afin de bâtir une sécurité réseau robuste. Puis nous avant consacré le troisième chapitre tout entier pour la future présentation de l'organisme d'accueil et de sa structure. En outre nous allons tester leurs taux de sécurité en appliquant notre référentiel de sécurité proposé et nous allons ainsi analyser leur architecture de sécurité. On va enchainer par un quatrième chapitre qui porte où on va proposer une future solution qui comprendra une nouvelle architecture de réseau se basant sur le futur référentiel dans le but d'avoir une sécurité maximale. Enfin nous avons terminerons par une conclusion générale.

CHAPITRE 1

SÉCURITÉ INFORMATIQUE

1.1 Introduction

Dans ce premier chapitre, nous allons présenter la sécurité informatique, ses objectifs, principes fondamentaux, ainsi que les multiples vulnérabilités et menaces auxquelles cette dernière pourra faire face. En outre, nous allons parler des attaques et hackers qui peuvent nuire au système. On va par la suite introduire les multiples bases, politiques, services et défis de la sécurité.

1.2 Définition de la sécurité

Le terme sécurité, regroupe l'ensemble des moyens, outils et mesures mises en œuvre dans le but de protéger un système d'information contre toute agression. Le NIST(National Institute of Standards and Technology), présente la sécurité telle que la protection offerte par un système d'information automatisé afin d'atteindre des objectifs applicables, qui sont au cœur de la sécurité informatique[16] :

- Confidentialité :
  - Confidentialité des données : Qui garantit que les informations confidentielles ou privées ne sont pas mises à la disposition ou divulguées à des personnes non autorisées.
  - Confidentialité : Qui garantit que des individus contrôlent les informations qui leur sont liées et par qui est à qui ces dernières peuvent être divulguées.

— Intégrité :
  — Intégrité des données : Qui garantit que les informations (stockées et transmises), ainsi que les programmes ne sont modifiés que d'une manière autorisée.
  — Intégrité du système : Qui garantit que ce dernier remplit sa fonction prévue, sans manipulation non autorisée du système.

— Disponibilité : Qui garantit que les systèmes fonctionnent rapidement, et que le service n'est pas refusé pour les utilisateurs autorisés. Ces trois concepts forment la triade CIA. Toutefois, certains dans le domaine de la sécurité estiment qu'il y a des concepts supplémentaires qui sont nécessaires pour une image complète. La figure suivante illustre les multiples piliers de la sécurité informatique.

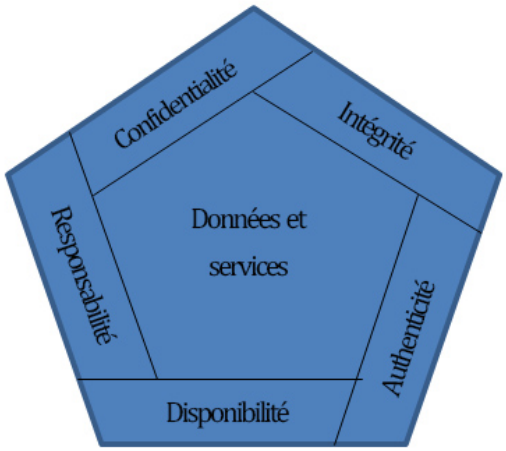

FIGURE 1.1 – Les pilliérs de sécurité informatique et réseau[16].

— Authenticité : c'est le fait de vérifier que les utilisateurs sont bien ceux qu'ils prétendent être et que chaque entrée arrivant sur le système provenait d'une source fiable.

— Responsabilité : qui prend en charge la non-répudiation, isolation des fautes, détection et prévention d'intrusion. les systèmes doivent conserver des enregistrements de leurs activités pour pouvoir les analyser, à fin de détecter les failles de sécurité ou pour faciliter les litiges liés aux transactions [16].

1.3 Vulnérabilités

Une vulnérabilité est simplement une faiblesse qui peut être exploitée par un attaquant pour effectuer des actions non autorisées au sein d'un ordinateur ou d'un système réseau. Il existe de différentes catégories pour placer les vulnérabilités, on trouve notamment [6] :

- Vulnérabilités liées aux domaines physiques :
  - Manque de redondance et de ressource au niveau équipement.
  - Accès aux salles informatiques non sécurisées.
  - Absence ou mauvaise stratégie de sauvegarde des données.
- Vulnérabilités liées aux domaines organisationnels :
  - Manque de Ressources humaines, de personnels qualifiés et de communications.
  - Absence de Contrôles périodiques, Documents de procédures adaptées à l'entreprise.
- Vulnérabilités liées aux domaines technologiques :
  - Pas de mises à jour des systèmes d'exploitation et des correctifs.
  - Pas de contrôle suffisant sur les logiciels malveillants.
  - Récurrence des failles et absence de supervision des évènements.
  - Réseaux complexes, non protégés.

1.4 Menaces

Une menace est l'exploitation d'une vulnérabilité pour obtenir, modifier ou empêcher l'accès à un actif ou encore le compromettre. Les menaces peuvent être classées par[6] :

- Origine ou source.
- Type.
- Motivation.

Elles peuvent être :

- Délibérées (vol, fraude, virus, hacking, incendie, attentat, sabotage, interception, divulgation ou altération de données. . . ,etc.).
- Naturelles ou environnementales (tremblement de terre, éruption volcanique, inondation, coupure de courant, incendie...,etc.).
- Accidentelles (erreurs d'utilisation, omissions. . . ,etc.).

— Dues à des pannes techniques : mauvais fonctionnement d'un équipement, d'un logiciel.

1.5 Attaque

1.5.1 Définition d'une attaque

Attaque, C'est l'acte de cibler et d'engager activement une cible[15].

1.5.2 Surfaces d'attaque

Une surface d'attaque se compose des vulnérabilités accessibles et exploitables dans un système comme :

— Surface d'attaque réseau : Cette catégorie fait référence aux vulnérabilités d'une entreprise : Réseau étendu ou Internet. Cette catégorie comprend le réseau les vulnérabilités du protocole réseau,comme pour une attaque par déni de service, perturbation des liaisons de communication et diverses formes d'attaques par intrusion.

— Surface d'attaque logicielle : Il s'agit des vulnérabilités dans les applications, les utilitaires, ou le code du système d'exploitation. Un serveur particulier dans cette catégorie est le serveur Web Logiciel.

— Surface d'attaque humaine : Cette catégorie fait référence aux vulnérabilités crées par le personnel ou des étrangers, tels que l'ingénieurie sociale, l'erreur humaine.

1.5.3 Types d'attaques

Les nombreuses attaques peuvent être définies dans les catégories suivantes[8] :

1. Les attaques contre les systèmes d'exploitation OS (Operating System) : Elles ciblent toute sorte d'erreurs commises lors des installations de systèmes notamment accepter tout et laisser tout par default, les comptes sans mot de passe, les ports ouverts. . . ,etc. Toute faille laissée pourra être exploitée par un hacker.
2. Les attaques au niveau des applications : Qui ciblent les codes de programmation et des logiciels.

3. Les attaques Shrink-warp code : Qui exploitent les codes et les scripts intégrés et fournies dans la plupart des applications. Les codes et scriptes qui sont destinés ont facilité l'installation et l'administration peuvent rapidement générer des vulnérabilités dans le cas où ce n'est pas gérée de façon appropriée.
4. Les attaques de mauvaises configurations : Qui profitent de la non-configuration intentionnelle ou involontaire des systèmes afin de causer des dommages.

1.5.4 Phases d'attaques

Le EC-conseil(International Council of Electronique Commerce Consultants) les définit comme étant la meilleure façon de concevoir une structure d'attaque. Malgré qu'elles ont de multiples appellations et que certaines d'entre elles se déroulent au même temps, le conseil de EC a défini cinq phases qui capturent tout l'étendue d'une attaque et qui seront présenté dans la figure suivante [13].

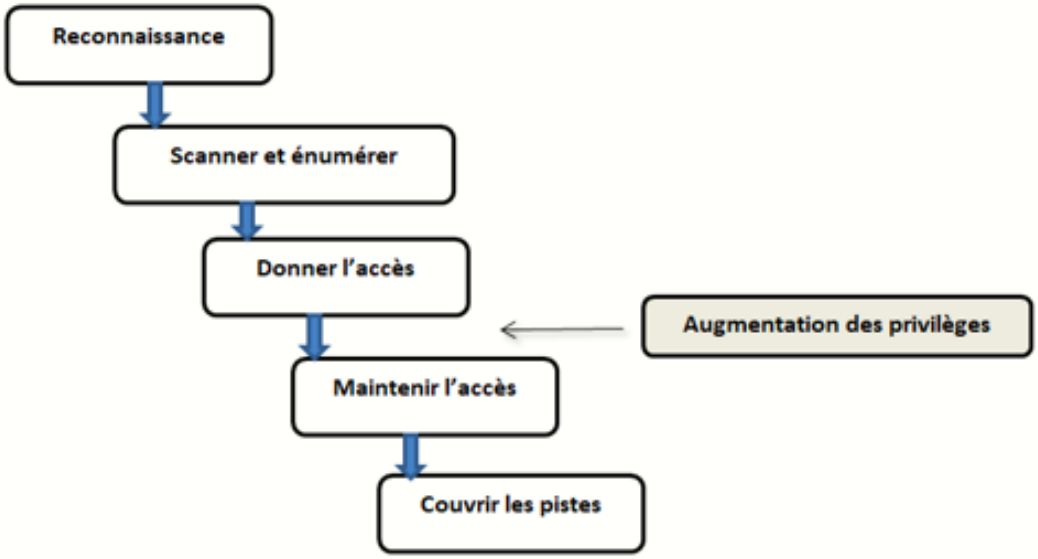

FIGURE 1.2 – Les phases d'une attaque[13].

1.6 Piratage

Le piratage a son propre vocabulaire de termes, les hackers eux-mêmes ont de différents termes et classifications qui sont les suivantes :

1.6.1 Classification des hackers (les chapeaux)

La classification des pirates informatiques est faite de multiples façons. Or le système du chapeau semble avoir résister au temps, désignant les bons, mauvais ou les indécis. En informatique, cette désignation est donnée tel un chapeau de couleur[9].

— Chapeaux blancs (white hats) : considérer comme états les bons, les hackers éthiques sont embauchés afin de tester et améliorer la sécurité, ils n'utilisent pas leurs compétences sans consentement, connus comme étant les analystes de sécurité.

— Chapeaux noirs (black hats) : C'est les méchants, des crackers, utilisant illégalement leurs compétences pour des fins malveillantes comme détruire des données et refuser l'accès aux ressources et aux systèmes.

— Chapeaux gris (gray hats) : Un groupe difficile a catégorisé, ils sont ni mauvais ni bons, cependant on peut les catégoriser en ceux qui sont simplement curieux sur les outils techniques de piratage, ainsi que ceux qui croient que c'est leurs devoirs, avec ou sans l'autorisation du client pour démontrer les failles du système. Dans les deux cas, ceci est considéré comme étant un crime.

On trouve aussi d'autres appellations telles que :

— Les script kiddies : Ce sont de jeunes pirates, généralement adolescents profitant et usant des exploits laissés publics par les white hats dans le but de provoquer des pannes volontaires, des mass-root.

— Les hackers universitaires : C'est des hackers libres, qui sont généralement associés au mouvement de l' Open Source et du logiciel libre, ils sont considérés comme étant des hackers qui partagent leurs connaissances, telles que des programmes, compétences. . . ,etc. ceci est sous raisonnement que l'information est libre et n'appartient à personne. Ces derniers ont tendance à travailler ensemble pour donner naissance à de grandes œuvres telles qu' Internet, Usenet et encore Unix.

— Les hackers suicidaires : C'est des hackers qui ne sont pas discrets et qui visent à faire tomber une cible dans le but de prouver un objectif, ils n'ont pas peur de se faire prendre.

1.6.2 Logiciels malveillants

la figure suivante représente les multiples logiciels malveillants et leurs influence sur les objectifs de la sécurité informatique.

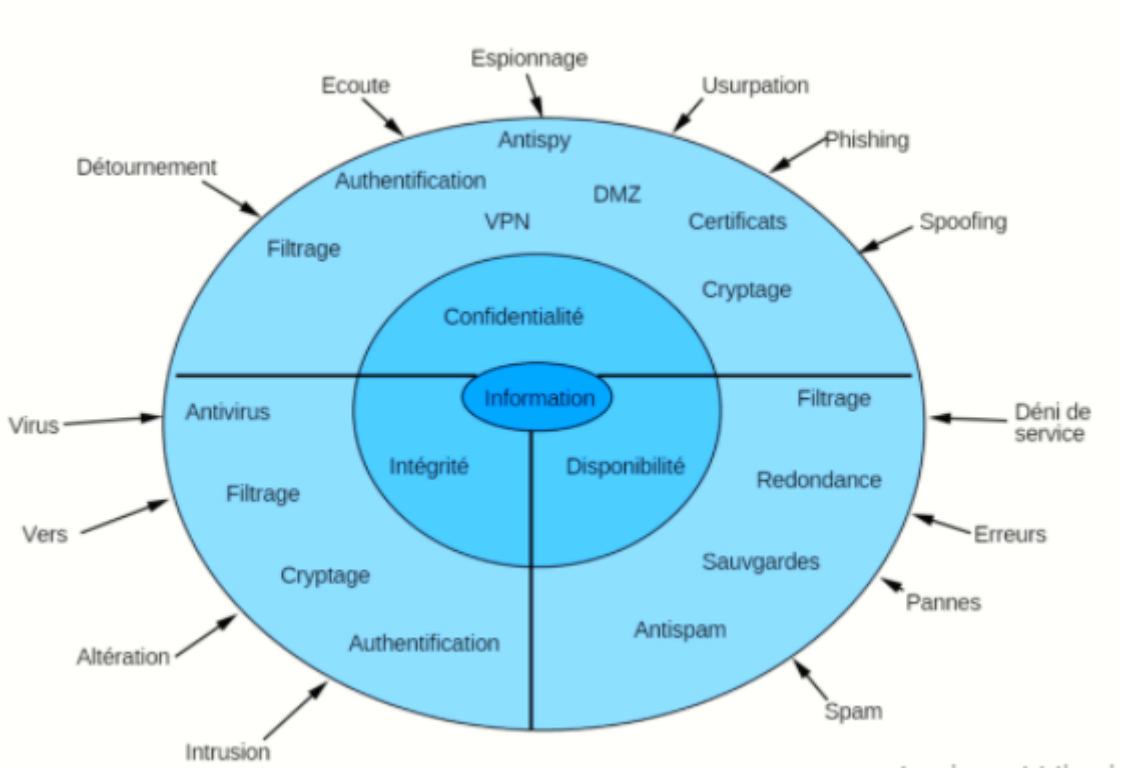

FIGURE 1.3 – Objectif, moyens et attaques[13].

Les logiciels malveillants sont tous ceux qui volent des ressources, du temps où autres. . . ,etc. Les principaux types sont les suivants :

1. Les virus, sont la forme de logiciels malveillants les plus répondus et sont conçus afin de se rupliqués ainsi que s'attacher à d'autres fichiers sur le système. Ils nécessitent une action de l'utilisateur pour lancer leurs activités infectieuses.
2. Les vers sont les succèsseurs des virus, ils ont la capacité de se reproduire par eux-mêmes très rapidement. Les vers étaient l'origine d'attaques par déni de service DoS les plus dévastatrices connues lors de la dernière décennie.
3. Les chevaux de Troie sont un type particulier de logiciels malveillants qui se reposent sur les techniques de l'ingénierie sociale afin d'infecter un système et causer des dommages en prenant l'apparence de programme légitime. Comme les virus, les torjans se lancent quand l'utilisateur lance un programme infecté ou wrapper .

4. Les Rootkits, sont des malwares modernes qui se cachent dans un composant principal d'un système et qui sont non détecté par les scanners modernes et sont plus difficile à retirer.
5. Les logiciels espions, sont conçus afin de recueillir des informations sur un système de manière furtive comme les enregistreurs de frappe.
6. Les logiciels publicitaires peuvent remplacer des pages d'accueil des navigateurs, plaçant des publicités contextuelles, ou installer des éléments conçus pour faire de la pub à des produits ou des services.

1.7 Classification des contre-mesures

Les contre-mesures sont mises par une entreprise ayant identifié les risques et les menaces du système, afin de réduire les risques d'attaques réussies. les méthodes de contrôles comportent généralement les éléments suivants[14] :

— Administratif : Ce sont les politiques, procédures et les lignes directrices, ainsi que des normes écrites, prenant l'exemple d'une politique d'utilisation acceptable (PUA) rédigée et acceptée par chaque usager du réseau.

— Physique : Les contrôles physiques, comprennent la sécurité pour les serveurs, les équipements et les infrastructures du réseau, comme la mise en place de système de verrouillage entre l'armoire électrique et les usagers ou bien l'utilisation de système redondant (un système ininterruptible d'alimentation électrique).

— Logique : ça compte les mots de passe, pare-feu, les systèmes de prévention des intrusions, listes d'accès, les tunnels VPN,. . . ,etc. ces contrôles sont souvent qualifiés de techniques contrôles.

Pas tous les contrôles sont égaux et ils n'ont pas le même objectif. Cependant ensemble ils doivent prévenir, détecter, protéger et récupérer tout en protégeant contre une menace.

1.8 Bases de la sécurité

Elles sont très nombreuses et variées, cependant ce qui les englobe toutes c'est le fait de lutter contre les risques et les éliminer. Comme le EISA (Entreprise Information Security)

qui est un ensemble d'exigences et de processus qui aident à déterminer comment les systèmes d'information d'une organisation sont construits et comment ils fonctionnent. les rapports post-incident suggèrent aux dirigeants qu'ils accordent plus d'attention à la sécurité et les moyens d'identifier les risques présents, ainsi les quantifier sur une échelle de mesure. Cette approche de gestion de risques leur permettrait de proposer des solutions pour atténuer les risques identifiés, la figure suivante illustre l'analyse des risques, par exemple quand le taux de probabilité d'un risque est élevé mais que son impact est faible cela est au cas ou la probabilité d'un risque est faible or que son impact est élevé[16].

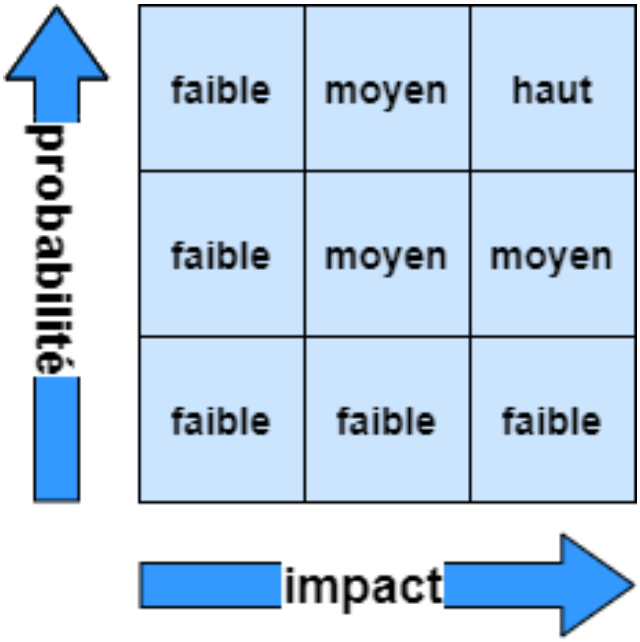

FIGURE 1.4 – Matrice d'analyse de risques..

Les phases de gestion de risques identifiés par EC-Council (International Council of Electronique Commerce Consultants), sont l'identification, l'évaluation, le traitement, le suivi des risques. Identification des actifs organisationnels et des menaces pesantes sur ces actifs et leurs vulnérabilités permettent à l'entreprise d'exploiter les contre-mesures que le personnel de sécurité pourrait mettre en place pour minimiser autant que possible les risques. Ces contrôles de sécurité vont augmenter la posture de sûreté des systèmes. Ils peuvent également être classés comme physiques, techniques et administratifs. les contrôles physiques comprennent les gardes, les lumières et les caméras. Les contrôles techniques englobent les éléments comme le chiffrement, les cartes à puce et les listes de contrôle d'accès. Les contrôles administratifs comprennent la formation, la sensibilisation et les efforts politiques, qui sont bien intentionnés. Certains de ces deniers doivent être

mis en place pour éviter que les erreurs ou les incidents se produisent.

1.9 Politique de sécurité

Elle peut être définie comme étant un document décrivant les contrôles de sécurité mis en place dans une entreprise afin d'atteindre un objectif. Il existe de différents types de politiques de sécurité comme[10] :

- Politique de contrôle d'accès qui identifie les ressources qui ont besoin de protection et les règles pour contrôler l'accès à ces dernières.
- Politique de sécurité de l'information qui identifie aux employés quels systèmes d'entreprise peuvent être adoptés ou pas, et les conséquences de briser les règles. Généralement les employés doivent signer une copie avant d'avoir l'accès aux ressources.
- Politique de protection des informations qui définit les niveaux de sensibilité des informations et qui a l'accès à ces niveaux-là.
- Politique de mot de passe qui définit tous les mots de passe de l'organisation, la longueur, la complexité, l'âge maximum et minimum et la réutilisation.
- Politique de courrier électronique qui définit l'usage de courrier électronique de l'entreprise.
- Politique de l'audit des informations qui définit le cadre d'audit de la sécurité au sein de l'organisation. QUAND, ou COMMENT et QUI conduit les audits de sécurité d'informations.

1.10 Services de sécurité

Vu que la sécurité regroupe toute la protection des informations, l'ISO (organisation internationale de normalisation) s'est tourné à sécuriser les données pendant la transmission, créant ainsi le standard d'architecture international, ISO 7498-2 (OSI Basic Reference Model-Part 2 : Security Architecture) qui est utile pour l'implémentation des éléments de sécurité dans un réseau vu qu'elle détaille les fonctionnalités ainsi que leur emplacement par rapport au modèle de référence. Il définit trois majeurs concepts[7] :

- Les fonctions de sécurité fixées par les actions qui peuvent nuire à la sécurité d'un établissement.

— Les mécanismes de sécurité illustrant les algorithmes à façonner.

— Les services de sécurité décrivant les logiciels, matériels façonnant des mécanismes au but de mettre à disposition les fonctions de sécurité aux utilisateurs.

Cinq types service de sécurité ont été déterminés :

— La confidentialité assurant la protection des données auprès des attaques non autorisées.

— L'authentification permettant d'assurer que l'identité de celui qui se connecte est belle est bien celui qu'il prétend être.

— L'intégrité assurant que les données envoyées correspondent à celles reçues.

— La non-répudiation garantissant que le message a bien été expédié par une source spécifiée et reçu par une destination spécifiée.

— Le contrôle d'accès qui prévient l'accès des utilisateurs spécifiés a des ressources définies. Le tableau suivant montre pour chacun des services les conditions particulières.

	1	**2**	**3**	**4**	**5**	**6**	**7**
Confidentialité :							
Avec connexion	oui	oui	oui	oui		oui	oui
Sans connexion	oui	oui	oui	oui		oui	oui
D'un champ particulier			oui	oui			
Authentification :			oui	oui			oui
Intégrité :							
Avec reprise			oui	oui			oui
Sans reprise				oui			oui
D'un champ particulier							oui
Non-répudiation							oui
Contrôle d'accès			oui	oui			oui

TABLE 1.1 – Sécurité au niveau de l'architecture OSI[11].

En se basant sur les cinq services de sécurité précédents et en analysant les besoins d'émetteur et récepteur, on parvient à atteindre le processus suivant :

1. Seul le destinataire reçoit le message.
2. Le message ne doit arriver qu'au bon destinataire.
3. L'émetteur est obliger d'être connu avec certitude.
4. L'émetteur et le récepteur doivent être connus.
5. Le destinataire ne peut nier la réception d'un message.
6. La source ne peut nier l'émission d'un message.
7. La source ne peut accéder à des ressources sauf si elle en est autorisée.

Le premier besoin équivaut au service de confidentialité ainsi que le 2 et 3 correspondent à l'authentification, quant au besoin 4 à un service d'authentification, 5 et 6 a un service de non-répudiation, enfin le besoin 7 au contrôle d'accès.

1.11 Défis de la sécurité informatique

La sécurité informatique et réseau est fascinante, mais complexe pour plusieurs raisons dont les suivantes [10] :

— les mécanismes utilisés afin de répondre aux exigences de la sécurité peuvent être assez complexes, et les comprendre peut demander un raisonnement assez subtil.

— Il est toujours nécessaire d'envisager des attaques potentielles contre les fonctionnalités de sécurité.

— Il est nécessaire de décider ou utiliser les divers mécanismes de sécurité, en termes de placement physique (à quels moments dans un réseau, certains mécanismes de sécurité sont nécessaires) ainsi que dans un emplacement logique (à quelle couche d'une architecture comme TCP/IP ces mécanismes sont mis en place).

— Les participants sont en possession de certaines informations secrètes (clés de chiffrement), soulève des questions sur la distribution et la protection de ces dernières.

— La sécurité informatique et réseau est principalement une bataille d'esprit entre un attaquant qui essaye de trouver des trous et administrateurs qui essaye de

fermer ces derniers, l'attaquant a besoin seulement d'une seule faiblesse alors que l'administrateur doit toutes les retrouver et les éliminer.

— Les utilisateurs et gestionnaires ont tendance à percevoir peu d'investissement en sécurité jusqu'à ce qu'une défaillance se produise.

— La sécurité requiert une surveillance constante, ce qui est difficile.

— La sécurité est souvent considérer après coup pour être intégrée dans un système après la conception plutôt que de la définir comme une partie intégrante du processus de conception.

1.12 Conclusion

Ce chapitre nous a permis d'avoir une vue générale du phénomène de la sécurité, où nous avons exposé les différentes parties et composants mais aussi les risques, défis et attaques auxquels cette dernière pourra faire face. Dans le prochain chapitre, on y trouvera les principes de la sécurité d'entreprise et les bonnes pratiques à suivre pour mieux sécuriser une entreprise.

CHAPITRE 2

SÉCURITÉ DES RÉSEAUX

2.1 Introduction

Dans ce chapitre, nous allons aborder le sujet de sécurité des réseaux, les différentes étapes requises ainsi que les bonnes pratiques pour avoir une sécurité d'entreprise complète.

2.2 Architecture de la sécurité des réseaux

Structurer une architecture sécurisée afin de protéger le réseau des accès non autorisés.

2.2.1 Gestion des risques

Les risques, la conformité ainsi que les politiques de sécurités sont les majeures composantes des architectures de sécurité. Le but de l'analyse des risques consiste à quantifier l'impact d'une menace potentielle.il existe donc deux types d'analyse de risques[15] :

— Analyse de risque quantitatif : fournissant un chiffre réel des pertes attendues, cette analyse use d'un modèle mathématique utilisant une valeur d'un actif par la probabilité de menace.

— Analyse de risque qualitatif : en usant d'un modèle de scénario, les évaluations

qualitatives sont descriptives et cette analyse peut précéder l'analyse quantitative.

2.2.2 Politiques de sécurité

C'est un ensemble d'objectifs, règles de comportement...pour l'entreprise assurant la sécurité des réseaux et des systèmes informatiques. C'est un « document vivant » continuellement mis à jour en fonction des technologies..., etc. Le public de politique de sécurité doit être composé d'employés, contractants, fournisseurs et de client qui ont accès à votre réseau[15].

— Governing policy (politique de gouvernance) : définissant les concepts de sécurité d'information au niveau élevé en décrivant leurs importances. Ils soutiennent les politiques techniques et celles relatives aux utilisateurs finaux.

— Technical policies(politiques techniques) : Elles décrivent ce que le personnel de sécurité doit faire dont lui dicter le comment.

— End-user policies(politiques d'utilisateurs finaux) : Elles contient les politiques de sécurité importantes pour les utilisateurs finaux. Les politiques techniques sont classées comme suit :

  — Politiques générales : Elles définissent l'usage des équipements, services informatiques et sécurité des lignes strictes. Elles peuvent inclure une politique d'utilisation acceptable AUP, un compte politique d'accès, de mot de passe, d'acquisition, d'audit, de sensibilité à l'information, d'évaluation des risques et du serveur web.

  — Politiques d'accès à distances : Elles définissent les normes de connexion au réseau d'organisation à partir d'un hôte ou d'un réseau externe, c'est généralement un réseau virtuel VPN.

  — Politiques réseau : Qui définit des normes afin de sécuriser tous les réseaux câblés et sans fil, les ports de données, elle peut aussi inclure les politiques générales d'accès au réseau et pour accder aux routeurs, commutateurs, serveurs ainsi qu'extranets.

  — Politiques d'email : Définit les normes afin de protéger l'infrastructure de courrier électronique d'organisation, ainsi que les transferts automatiques de courrier électronique et les politiques des spams.

— Autres politiques : Elles peuvent comprendre les politiques de téléphonie et l'usage des applications ainsi que les politiques de communication sans fil.

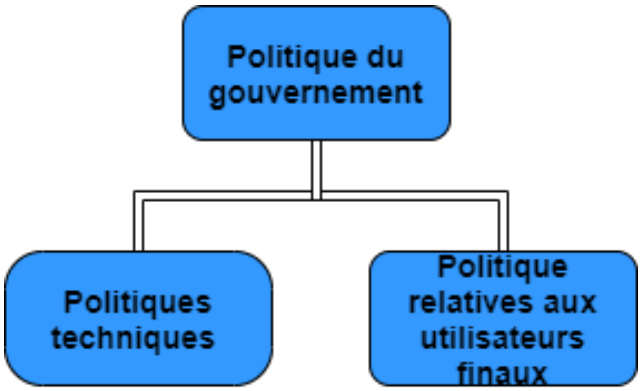

FIGURE 2.1 – Composant de politique de sécurité dans une organisation.

2.2.3 Normes, lignes directrices et procédures

Les politiques bâtissent un cadre de travail, cependant elles sont trop générales pour être d'une grande utilité aux personnes chargées de la mise en œuvre de ces dernières. il existe donc des documents plus détaillés tels que[15] :

— Standards : Aident le personnel informatique à être cohérent en spécifiant l'usage des technologies. Ils sont obligatoires la plupart du temps et contribuent à assurer la cohérence, l'uniformité et l'efficacité.

— Lignes directrices (guide lines) : C'est les meilleures pratiques qui procurent une liste de suggestions sur la bonne pratique des choses, c'est similaire aux normes, mais elles sont plus flexibles et ne sont généralement pas obligatoires.

— Procédures : Englobent les détails de la mise en œuvre, la plupart du temps avec des graphes d'étape par étape et des instructions.

2.2.4 Gestion de sécurité d'un cycle de vie de réseaux sécurisés

Le schéma suivant montre les cinq phases d'approche du cycle de vie, ça illustre le processus de conception, création, maintien des architectures de sécurité[15].

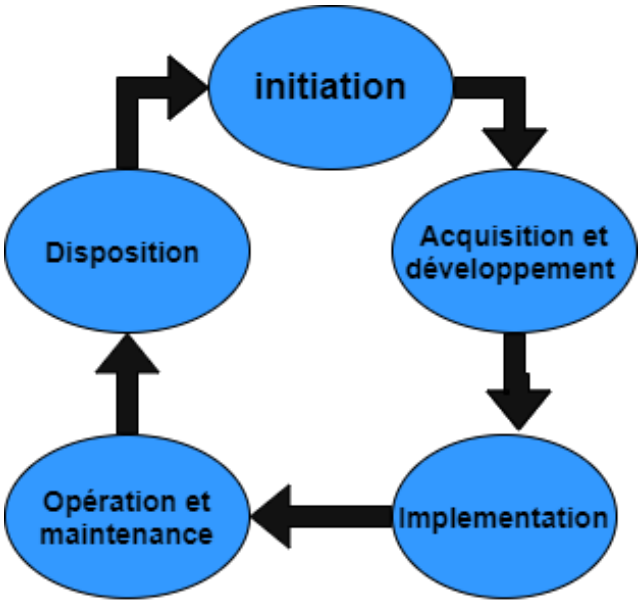

FIGURE 2.2 – Les cinq phases d'approche du cycle de vie de réseaux sécurisés

2.2.5 Modèles et Frameworks

Ces derniers constituent les alternatives à l'approche fondée à base de cycle de vie et des orientations d'architectures de sécurité :

— COBIT (Control Objectives for Information and Related Technology) : Englobe les meilleures pratiques dérivées d'accords d'experts concentraient sur les contrôles et les mesures TI (Information Technology), qui est utiles pour la gouvernance des TI et audits. Permettant d'optimiser les investissements dans les technologies d'informations.

— ISO 27000 : Comprend un ensemble de contrôles ayant les meilleurs pratiques en sécurité d'information et est un organisme certifié et une norme de sécurité reconnue mondialement se concentrant sur l'identification, l'évaluation et la gestion des risques.

— ITIL (Information Technology Infrastructure Library) : Inclue un ensemble de huit guides de pratiques enveloppant la majorité des aspects de gestion des services informatiques.

— NIST (National Institute of Standards and Technology) : La série NIST 800 fournit des documents détaillés sur la façon dont sécurisera une infrastructure en réseau.

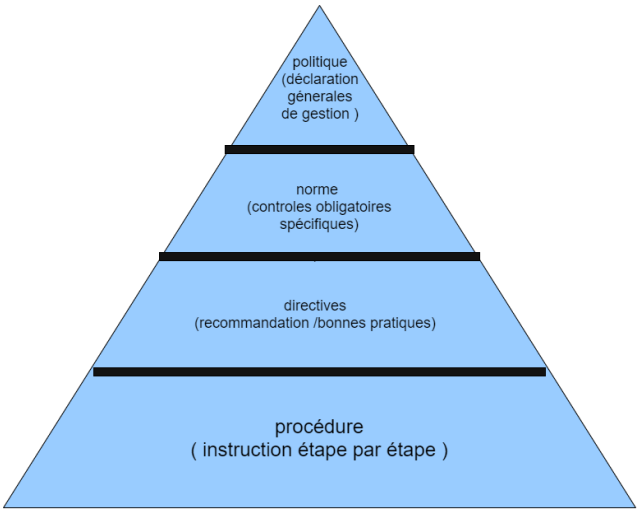

FIGURE 2.3 – Cadre de la politique de sécurité d'information.

2.2.6 Principes fondamentaux de conception de la sécurité

— L'économie de mécanisme signifie que la conception des mesures de sécurité incarnées dans le matériel et le logiciel devrait être aussi simple et petite que possible.

— Les valeurs par défaut de sécurité signifie que les décisions d'accès doivent être basées sur l'autorisation plutôt que l'exclusion.

— Méditation complète signifie que chaque accès doit être vérifié par un mécanisme de contrôle d'accès.

— la conception ouverte signifie que la conception d'un mécanisme de sécurité doit être ouverte plutôt que secrète .

— Séparation des privilèges qui est une pratique dans laquelle des attributs de privilèges sont requis afin d'accéder à une ressource restreinte.

— Le moindre privilège signifie que chaque processus ainsi qu'utilisateur du système fonctionnent en utilisant le minimum de privilèges nécessaires pour effectuer la tâche.

— Le moindre mécanisme signifie que la conception devrait minimiser les fonctions partagées par différents utilisateurs, offrant une sécurité mutuelle.

— L'acceptabilité psychologique implique que les mécanismes de sécurité ne doivent pas interférer indument avec le travail des utilisateurs, tout en répondant aux besoins de ceux qui autorisent l'accès .

— Isolement Est un principe qui s'appuie sur trois contextes. D'abord, les systèmes d'accès public doivent être isolés des ressources critiques(données, processus. . . ,etc.), pour empêcher la divulgation ou l'altération. L'isolement physique est d'assurer qu'il n'existe aucun lien physique entre l'accès public d'une organisation et les ressources d'informations et les informations critiques d'une organisation. Dans l'isolement logique, les mécanismes de sécurité entre les systèmes publics et les systèmes sécurisés sont chargés de protéger les ressources critiques. Ensuite, les processus et les fichiers des utilisateurs individuels doivent être isolés les uns des autres, sauf quand cela est souhaité. Tous les systèmes d'exploitation modernes fournissent des installations pour une telle isolation, de sorte que les utilisateurs individuels aient un espace de processus isolé, espace mémoire et espace fichier, avec des protections afin d'empêcher l'accès non autorisé.

— Encapsulation peut être considérée telle une forme d'isolement spécifique basée sur une fonctionnalité orientée objet. La protection est assurée en encapsulant un ensemble de procédures et des objets de données dans un domaine qui lui est propre, de sorte que la structure interne d'un objet de données n'est accessible qu'aux procédures du sous-système protégé, et les procédures ne peuvent être appelées qu'aux points d'entrée de domaine désignés.

— Modularité Où le contexte de la sécurité renvoie aux fonctions du développement de la sécurité tel que des modules séparés et protégés et à l'utilisation d'une architecture modulaire pour la mise en place des mécanismes et la conception. Avec le respect de l'utilisation des modules de sécurité distincts, l'objectif de conception ici est de fournir des fonctions et des services de sécurité communs, tel que les fonctions cryptographiques comme des modules communs.

— La superposition Fait référence à l'usage de plusieurs approches de protection qui se superposent comme les aspects humains, technologiques et opérationnels des systèmes d'information.

— Le moindre étonnement signifie qu'un programme ou une interface utilisateur doit toujours répondre de la manière la moins susceptible détonné l'utilisateur[15].

FIGURE 2.4 – Principes fondamentaux de conception de la sécurité

2.3 Auditer son système

Il est fort recommander d'auditer son système afin de connaitre son niveau de sécurité réel, et ceci avec la réalisation de testes d'intrusions établit soit par le responsable de sécurité ou par un hacker professionnel en accord avec l'entreprise. Ce dernier va appliquer un test d'intrusions du système, des attaques y compris. Cette opération connue sous le nom d'audit de vulnérabilités, ceci est fait en autorisation par le responsable de sécurité des systèmes d'information (RSSI), seuls lui ou le responsable de sécurité de l'entreprise peuvent faire ce test[13].

2.4 Classification des attaques

Les attaques de sécurité sont classées autant qu'attaques passives et actives en utilisant à la fois dans X .800 et RFC 4949[12].

1. **Attaques passives** Les attaques passives sont de la nature d'écoute ou de surveillance des transmissions dans le but d'obtenir des informations qui sont transmises. Il existe donc deux types d'attaques passives qui sont la libération du contenu des messages et l'analyse du trafic. Les attaques passives sont très difficiles à détecter, car elles n'impliquent aucune Altération des données.
2. **Attaques actives** Les attaques actives impliquent une certaine modification du flux de données, ou une création d'un faux flux et ces attaques peuvent être subdivisées en : intrusion et déni de service.

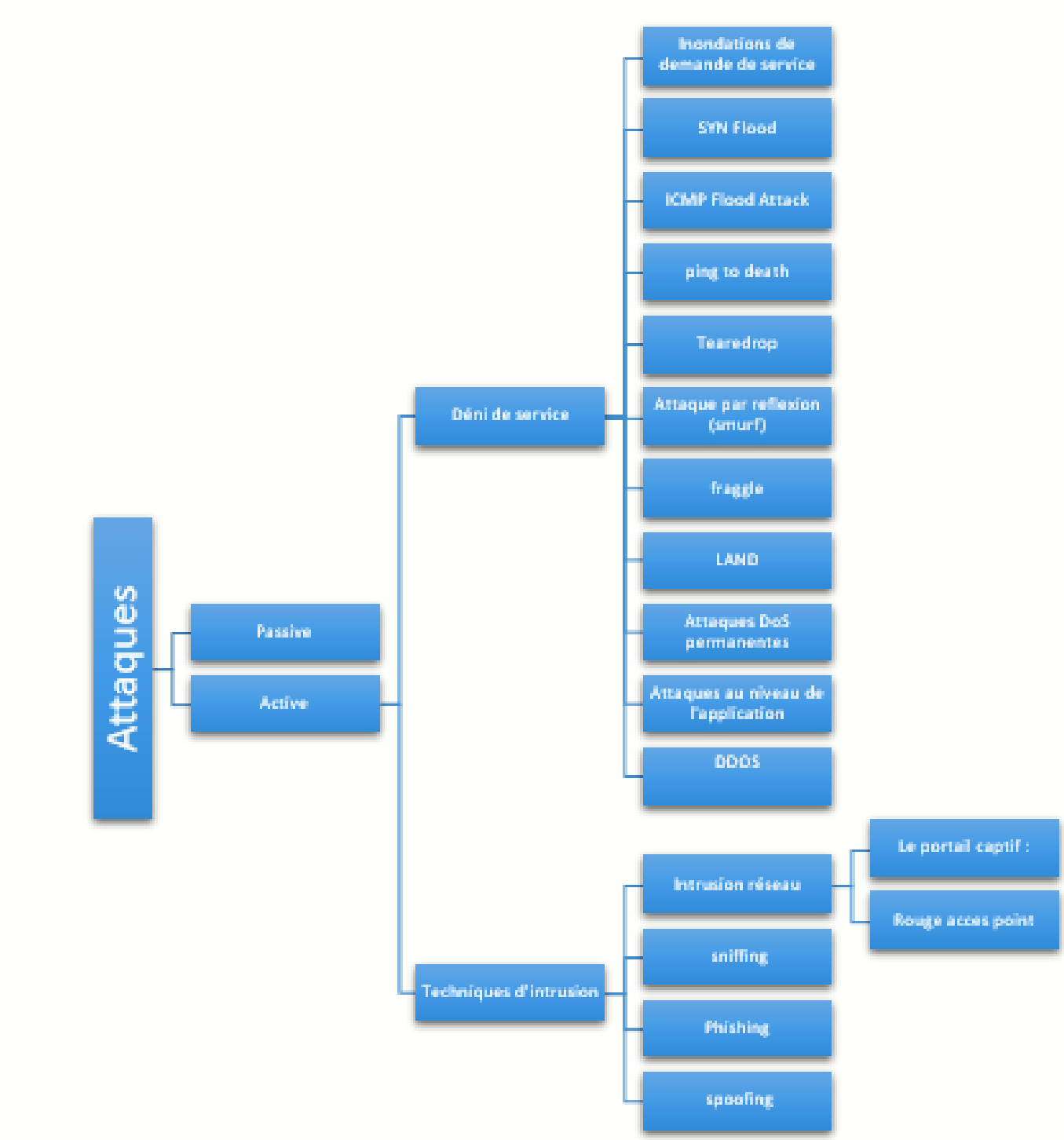

FIGURE 2.5 – La classification d'attaques

Pour voir les attaques en détail, Un état de l'art sur les différentes attaques a était dressé dans [AnnexB].

2.5 Bâtir de bonnes pratiques de sécurité

La sécurité est indispensable dans chaque système, cependant elle ne doit pas constituer de gêne aux utilisateurs et doit permettre tout accès en toute confiance. C'est pour ça qu'il faut devoir aménager une politique de sécurité en identifiant d'abord les besoins et les risques ainsi évaluer l'importance des données pour enfin mettre en place les règles et procédures pour les différents services. Un administrateur doit faire de la surveillance active et passive. Il doit être au courant des vulnérabilités matérielles ou logicielles et des failles pouvant nuire au système .il faut aussi définir une politique à appliquer en cas de menace ou de détection de vulnérabilités[1].

2.6 Conclusion

Les bonnes pratiques et les fondamentaux de la sécurité sont clairs, cependant la réalisation de cette dernière est bien plus difficile et pas toujours évidente. Dans la partie suivante, nous allons prendre un cas d'étude qui est une entreprise sur laquelle on va appliquer ces pratiques réunies afin de réaliser un audit de sécurité de cette dernière.

CHAPITRE 3

ORGANISME D'ACCUEIL

3.1 Introduction

Dans cette partie, nous allons présenter l'entreprise dans laquelle nous avons effectué notre stage. On va exposer et parcourir leurs multiples équipements ainsi que leur architecture réseau dans le but d'appliquer les bonnes pratiques de sécurité énumérer dans le précédant chapitre sur notre cas d'étude.

3.2 Définition de l'entreprise Général Emballage d'AKBOU

Général Emballage, est une entreprise algérienne de papeterie spécialisée dans la fabrication et la transformation de carton ondulé. Fondée par Ramdane Batouche en 2000, l'actuel président du conseil d'administration. Général Emballage est le plus grand producteur dans ce domaine en Afrique.

3.3 Historique de l'entreprise Général Emballage

Général Emballage a été fondé pour percer dans le domaine de l'industrie du carton, considéré comme une SPA (société par actions), dispose d'un capital de

32 millions de DZD, elle est située dans la zone d'activité Taharacht à Akbou, Wilaya, Bejaia.

— En 2002, l'usine a été mise en production, et comptait 83 employés.

— En 2006, le capital a été porté à 150 millions de dinars et comptait 318 employés.

— En 2007, l'unité Setif a été mise en service, le capital a été porté à 1,23 milliard de Dinars et elle comptait 425 employés.

— En 2008, elle a commencé à exporter vers la Tunisie, ainsi que l'exploitation du département d'Oran.

— En 2009, son capital est passé à 2 milliards de DZD, et a rejoint Maghreb Invest avec une participation de 40 pour cent. Le nombre d'employés atteint donc les 597 employés.

— En 2010, avec son chiffre d'affaires elle parvenait à occuper une place parmi les 50 grandes entreprises algériennes.

— En 2011, la capacité totale de production des trois usines d'Akbou, d'Oran et de Sétif était de 130 000 tonnes, soit 80 pour cent de la consommation algérienne.

— En 2012, l'usine d'Oran a été transférée dans la zone industrielle de Hasi Amer. Elle a signé un accord-cadre de coopération avec l'Université de Bejaia.

— En 2013, Général Emballage a obtenu la certification ISO 9001 : 2008, est a commencé à exporter vers la Libye en 2014.

— En 2015, elle remporte le Trophée Export 2014 (World Trade Center).

3.4 Plans du réseau de l'entreprise

La figure suivante représente les plans fournit par l'entreprise et qui détaille les differentes zones définis par l'entreprise. On trouve la zone A qui est une zone démilitarisée comprenant les multiples serveurs. La zone B contenant des réseaux LANs, reliées avec un Switch géré par un pare-feu Fortinet. Ce dernier est connecté à internet via un routeur.

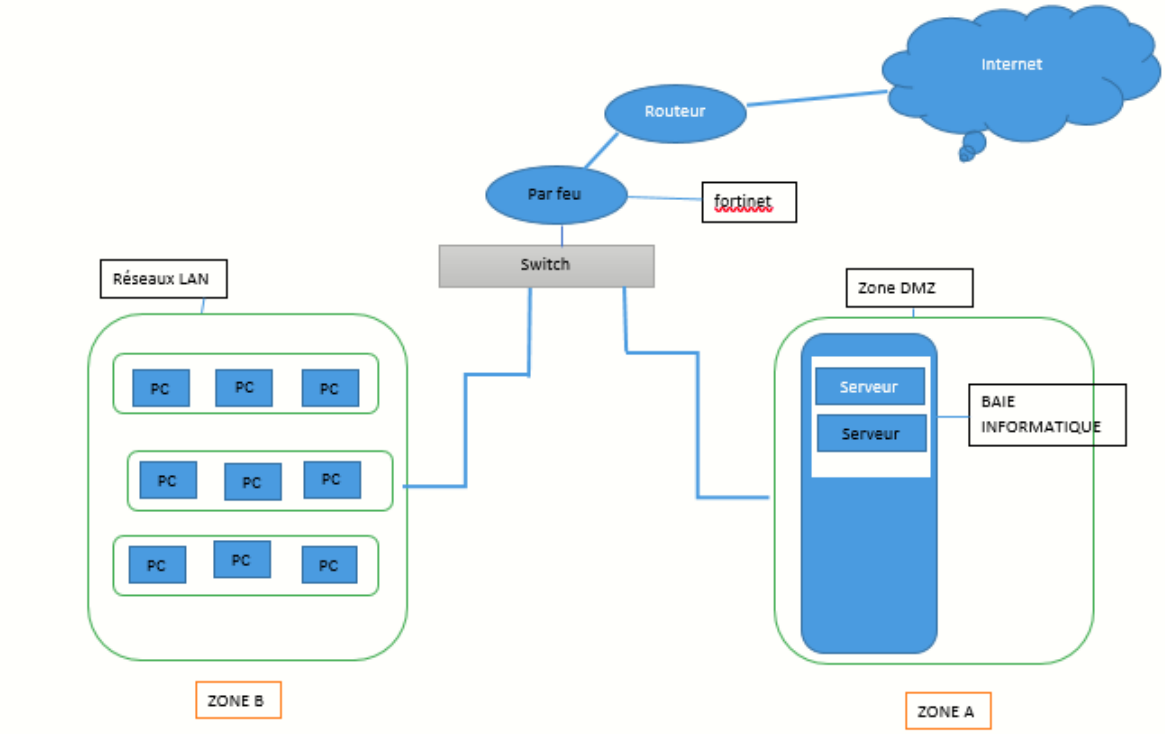

FIGURE 3.1 – Le plan du réseau de l'entreprise.

3.5 Étude du réseau de l'entreprise

3.5.1 Équipements actifs

Équipements d'interconnexion

— Equipements de sécurité :
  — Pare-feu (Fortinet) Les pare-feu nouvelle génération de Fortinet sont équipés de processeurs SPU (Security Processing Units), et des services de sécurité des FortiGuard Labs.Le pare-feu dont dispose l'entreprise : Fortinet (Fortios 6.2.3)
— Points d'accès : Les points d'accès FortiAPs existent en plusieurs modèles et à des tarifs différents. Le réseau sans fil se configure et se gère via la plateforme de sécurité FortiGate.
— Routeur Cisco C'est un périphérique intermédiaire dans un réseau informatique qui a pour rôle d'assurer le routage des paquets entre réseaux indépendants.Il aide à mettre en place un réseau plus intelligent, plus réactif et mieux intégré.les routeurs dont dispose l'entreprise :
  — Routeur CISCO 2801 ;
— Switch Cisco : Le commutateur réseau est un équipement reliant les multiples segments d'un réseau informatique et dispose de multiples services de sécurité. Les commutateurs Cisco, sont évolutifs et économiques et répondent aux besoins de toute taille d'entreprise.les switch dont dispose l'entreprise :
  — Switch Cisco 3750 ;
  — Switch Cisco 2960 ;
— Switch D-Link : Les commutateurs D-Link, étaient parmi les premiers, économiques et ils accomplissent leur fonction par rapport aux besoins de l'entreprise.

Équipements terminaux

— serveur : C'est un équipement informatique qui fournit des services à un ou plusieurs clients. les services les plus courants sont :
  — La sauvegarde de données ;

- L'accès aux informations du World Wide Web ;
- Le courrier électronique ;
- Le partage d'imprimantes ;
- Le commerce électronique ;
- Le stockage en base de données ;
- La gestion de l'authentification et du contrôle
- Le jeu et la mise à disposition de logiciels applicatifs (optique software as a service).

Les serveurs dont dispose l'entreprise sont :

- Serveur HP DL380 G7 ;
- Serveur DELL PowerEdge R520.

— Des ordinateurs : Des ordinateurs bureaux et des portables DELL et HP reliés au réseau soit à partir des switchs soit à partir du serveur.

— Des imprimantes.

— Des appareils téléphoniques.

3.5.2 Équipements passifs

— Les Câbles :

Pour que l'entreprise assure le câblage, elle utilise :

- La fibre optique.
- des connecteurs RJ45.

— Armoire de brassage : BAIE informatique.

— Tiroir optique coulissant 19 pouces.

3.5.3 Équipements logiques

— Systèmes d'Exploitation Windows et Linux.

— Systèmes de BACKUP« sauvegarde automatique ».

— antivirus kaspersky.

— Bureautique Microsoft Office.

— Protection d'accès :active directory.

3.5.4 Équipements service de connexion

— Connexion : ISO/CEI 8802-11 « wifi ».
— Messagerie : Général Emballage.
— Angular LDAP.

Note : Suite à la pandémie mondiale du COVID 19 qui a touché les 4 coins du globe et notre pays y compris, nous n'avons pas eu suffisamment de temps de stage et donc nous n'avons pas pu collecter toutes les informations et les données nécessaires afin de réaliser un audit complet. En outre, pour raisons de sécurité et confidentialité, la communication de quelques informations nous ont étaient interdites par le personnel de l'entreprise.

3.6 Étude de l'existant

On pourra résumer et classifier ces mesures en quatre grands titres : **Sécurité réseau** L'architecture du réseau est protégée par pare-feu (Fortinet) ainsi qu'un proxy filtrant tous les paquets entrant et sortant, il dispose aussi d'un outil de détection contre intrusion (IDS/IPS). Or la sécurité réseau n'est pas parfaite et on peut trouver des lacunes tel que la configuration du pare-feu de telle sorte qu'il ne peut être identifié comme tel ainsi que le manque de vérification périodique des cahiers de configuration du pare-feu. Aussi la disposition des points d'accès de telle sorte à accomplir la minimisation de propagation du signal au-delà du périmètre de l'organisme n'est pas réalisée. En outre, la personnalisation de la valeur par défaut du SSID (Service Set Identifier) ne doit pas comprendre des indicateurs sur l'organisme, son lieu et les fonctions des points d'accès.

Sécurité physique La sécurité physique est basée sur les faits suivants :
— Des agents d'accueil contrôlant l'accès au périmètre du site et enregistrant les informations associés aux visiteurs.
— Les numéros de série des appareils mobiles des employés de l'organisation ne sont pas enregistrés.

— Les utilisateurs sont sensibilisés au risque informatique (phishing, malware, vol de données, etc.) sans pour autant avoir des rappels réguliers aux apparitions des nouvelles menaces.
— Des salles d'équipements fermées à clef et avec accès réservé aux personnes autorisées.
— Climatisation assurée dans les salles de serveurs.
— Toute personne ayant accès aux emplacements des matériels peut utiliser les ports car ils sont ouverts et non sécurisés.
— Les données chiffrées ne sont pas conservées dans des sites distants.
— Manque de mesures de sécurités tel que de distancement du matériel de secours en cas d'incident touchant le site principal.
— Absence de la désactivation des ports physiques non utilisés.
— Pas de mise en place de câbles blindés et de boites de verrouillage aux extrémités.
— Pas de documentation de traçabilités du matériel sensible circulant en dehors des locaux de l'organisme.

Sécurité logique La sécurité logique est basée sur les faits suivants :
— L'architecture réseau est segmentée.
— La gestion des postes de travail des utilisateurs par l'existence d'un contrôleur de domaine.
— Le filtrage des accès réseau vers internet assuré à l'aide d'un proxy.
— L'existence d'un firewall afin de configurer les accès.
— L'opération d'audit périodique des systèmes et applications est absente ainsi que les procédures d'audit des systèmes de traitement de données.
— Absence de la synchronisation des horloges des systèmes dans le but d'assurer la précession des données et des journaux d'audit.
— Absence de l'analyse régulière des journaux d'évènements.

Sécurité machine
— Gestion des équipements :
  — Le switch D-LINK employé n'a pas d'interface web, il n'est pas mangeable, et donc pas sécurisé.

  - L'absence d'un switch CORE, et de redondance de matériels.
  - les matériels sont vieux, pas mis à jour et ne sont remplacés que dans le cas où ils sont défectueux.
- Gestion et mises à jour de la distribution des correctifs :
  - Pas de mises à jour des logiciels et systèmes ni de plan de restauration en cas de mises à jour critiques, pas d'enregistrement des opérations de mises à jour.
  - l'entreprise ne dispose pas de stratégie de minimisation de risques contre les vulnérabilités comprises dans les logiciels non mis à jour.
  - Les sauvegardes ne sont pas externalisées.
  - Absence des tests périodiques des mesures d'authentification des équipements connectés au réseau.
  - Absence des tests périodiques des mesures d'authentification des équipements connectées au réseau.
- Le système antiviral :
  - La solution antivirale employée est la solution Kaspersky afin de détecter et d'éliminer les menaces ainsi que les codes malicieux, cependant l'opération de scan présente une défaillance à cause du choix laissé au client.
- Gestion des mots de passe :
  - Pas d'utilisation des techniques d'authentification fortes et des mots de passe respectant la politique mise par l'organisme ainsi que l'absence de la double authentification.

Le tableau suivant represente les résultats déduits après l'application du référentiel de sécurité sur le cas d'étude qui est la Spa Général Emballage.

Les bonnes pratiques de la sécurité d'une entreprise	**l'entreprise de Général Emballage**	**Discription**
Conception et Gestion des réseaux	oui	
Configuration des équipements réseaux	moyenne	car ces deux conditions ne sont pas réalisées :La synchronisation des horloges de tous les systèmes pour assurer la précision des données et des journaux d'audit ansi que la désactivation des ports physiques non utilisés.
Segmentation du réseau	oui	
Authentification des équipements réseaux	non	car cette condition n'est pas réalisée : Le test périodique des mesures d'authentification des équipements connectés aux réseaux n'est pas rempli .
Routage et configuration des pare-feu et VPN	moyenne	car ces deux conditions ne sont pas réalisées : Configuration des pare-feu de sorte qu'on ne peut pas l'identifier en tant que tel et la vérification des fichiers de configuration des pare-feu périodiquement.
Utilisation des systèmes de détection et de prévention d'intrusion IDS/IPS	oui	

Transmission des données	moyenne	car cette condition n'est pas réalisée : utilisation des techniques d'authentification forte.
Courriel et Communication sur Internet	moyenne	car cette condition n'est pas réalisée : Eviter le piratage et les accès non autorisés en utilisant des mots de passe divers respectant la politique mise par l'organisme pour chaque réseau et se servir de la double authentification.
Sécurisation des réseaux sans fil	moyenne	car ces deux conditions ne sont pas réalisées : accès physique : En disposant les points d'accès de telle sorte à accomplir, la minimisation depropagation du signal au-delà du périmètre de l'organisme. Accès réseau : La personnalisation de la valeur par défaut du SSID et SSID ne doit comprendre des indicateurs sur l'organisme, son lieu, les fonctions de point d'accès.
Sécurité des systèmes	moyenne	car ces deux conditions ne sont pas réalisées : Les Mises à jour des logiciels et systèmes sont imposées et doivent être adaptées dés publication et un plan de restauration doit être mis en position en cas des mises à jour critiques. Les mises à jour doivent être testées dans un cadre de test similaire a un déploiement.et les opérations de mises à jour doivent être enregistrées et ne doivent être faites que par le personnel qualifier.

Opérations réalisées sur les systèmes et logiciels	moyens	car ces deux conditions ne sont pas réalisées : La nécessité d'auditer périodiquement les systèmes et applications. Opération des utilisateurs : L'analyse régulière des journaux d'événements.
Teste	oui	
Développement et la maintenance des sites web	oui	
Usage des appareils mobiles et supports de stockage	non	car cette condition n'est pas réalisée : La sauvegarde n'est pas externalisée.
Usage des appareils mobiles	moyens	car cette condition n'est pas réalisée : Enregistrement des numéros de série des appareils mobiles des employés par l'organisation.
Usage des supports de stockage	oui	
Gestion de données	oui	
Sauvegarde et la restauration et l'archivage	moyenne	car cette condition n'est pas réalisée :la conservation des données chiffrées dans un site distant.
Partenaires	oui	
Sécurité physique :		
Zones sécurisées	oui	car cette condition n'est pas réalisée : Distancement du matériel de secours pour éviter les dommages engendrés par un accident touchant le site principal.

Matériel	non	car cette condition n'est pas réalisée : la Mise en place de conduit de câbles blindés, des boites verrouillées aux extrémités en guise d'inspection et sécurité du matériel hors site : Documenter la traçabilité du matériel quand il circule en dehors des locaux de l'organisme.
Gestion des incidents reliés a la sécurité de l'information :	oui	
Contrôle des systèmes	moyenne	car cette condition n'est pas réalisée : mise en place des procédures d'audit périodique des systèmes de traitement de données.
Protection des informations journalisées	oui	
Signalement et gestion des incidents de sécurité informatique	moyenne	car cette condition n'est pas réalisée : mise au courant de tous les utilisateurs sur les procédures de signalement des divers événements, et les failles pouvant avoir un impact avec la sécurité
Gestion des risques après accident	oui	
Solutions aux incidents	oui	
Relance après catastrophe et la pour suite des activités	oui	

TABLE 3.1: résultats d'application du référentiel sur la SPA Général Emballage.

3.7 Niveau de sécurité dans l'entreprise

Niveau de sécurité	Description
Plus que 75%	Niveau de sécurité optimal
50% – 75 %	Niveau de sécurité moyen
Moins de 50%	Niveau de sécurité faible

TABLE 3.2 – Les niveaux de sécurité.

À l'issue de notre questionnaire [AnnexeC], l'organisme enregistre une conformité globale de71.42%, par rapport à notre Référentiel de sécurité [AnnexeA]et suivant l'échelle de la norme ISO/IEC 17799 :2005 prouve qu'il y a des efforts à faire concernant la sécurité.On a classifié les mesures en quatre catégories :

— logique et réseau :32.14%
— physique :14.29%
— machine :3.57%
— Gestion des incidents reliés à la sécurité de l'information :21.43%

3.8 Conclusion

Tout au long de ce chapitre, nous avons présenté la société Général Emballage, son réseau ainsi que les équipements dont cette dernière dispose. Par la suite nous avons mis en évidence les multiples vulnérabilités et problèmes de sécurité dont cette dernière dispose. On a aussi appliqué notre référentiel de sécurité sur leur système de sécurité du réseau dans le but de proposer dans le chapitre qui suivra des solutions, une nouvelle architecture du réseau bien plus sécurisé est plus robuste.

CHAPITRE 4

RÉALISATION

4.1 Introduction

Après avoir étudié et parcouru l'architecture existante ainsi que les mesures de sécurité dont dispose l'entreprise Général Emballage, et après avoir énuméré les multiples failles qui peuvent nuire à la sécurité du réseau de l'entreprise en général. Nous allons dans ce qui suit énumérer les différentes solutions et proposer une nouvelle architecture du réseau dans le but d'avoir une sécurité robuste.

4.2 Présentation de l'environnement du travail

4.2.1 GNS3 (Graphical Network Simulator 3)

GNS3 est un simulateur de réseau graphique qui permet l'émulation de réseaux complexes. Son avantage par rapport aux autres simulateurs (tel que Packet Tracer) est qu'il est proche de la réalité. La flexibilité et la richesse de GNS3 permettent l'utilisation d'une variété de matériels,de ce fait, nous pouvons installer l'image ISO appropriée (comme un routeur)et même d'utiliser des machines virtuelles pour simuler avec.La simulation à l'aide de machines virtuelles peut être intégrée à l'environnement physique [2].

FIGURE 4.1 – Le logo de gns3.

4.2.2 VMware

Un hyperviseur, également appelé moniteur de machine virtuelle, est un processus qui crée et exécute des machines virtuelles (VM). Il permet à un ordinateur hôte de prendre en charge plusieurs VM clientes en partageant virtuellement ses ressources, telles que la mémoire et la capacité de traitement[3].

FIGURE 4.2 – Le logo de la vmware.

4.3 Solutions recommandées afin d'avoir une sécurité robuste de la spa général emballage

Afin d'avoir une meilleure sécurité et après avoir constaté que les divers problèmes même les plus minuscules et les moins attendus peuvent être exploités par un individu malveillant dans le but de pénétrer le réseau et d' y attaquer ce dernier. En se basant sur notre référentiel de sécurité, on propose d'ajouter et de changer quelques équipements ou configuration tel que :

— Tester périodiquement les mesures d'authentification pour les différents équipements connectés au réseau, et employer des mots de passe variés.

— Configuration du pare-feu de telle sorte qu'il ne soit pas identifié en tant que tel ainsi que la vérification périodique des fichiers de configuration du

pare-feu.

— L'emploi des techniques d'authentification fortes.

— La minimisation de propagation du signal en dehors du périmètre de l'organisme.

— L'application des diverses mises à jour.

— Auditer périodiquement les systèmes et les applications.

— Externalisation de la sauvegarde, et la conservation des données chiffrées dans un site distant.

— Protéger les câbles par la mise en place des conduits de câbles blindés.

— La proposition d'un VPN MPLS.

— Utilisation d'un SDWAN (Software Defined wide Area network).

— Utilisation d'un switch fédérateur.

— L'utilisation d'une technique sans fil tel que la WiMax pour s'en service en cas de coupure de fil.

— Disposer d'une redondance d'équipements dans le cas où l'un d'eux est défectueux.

— Sécurisation des ports des switches et routeurs et désactivation des ports non utilisés.

— Emploi des onduleurs de type UPS.SNMP.

— Utiliser des prises PDU 0.

— Utiliser les RAID 50, pour les stockages.

4.4 Présentation de l'architecture proposée

La nouvelle architecture du réseau de l'entreprise comporte les solutions qu'on estime imporatntes pour pouvoir sécuriser le réseau de cette dérnière.

La figure suivante présente la nouvelle architecture du réseau de l'entreprise après application des différentes modifications et améliorations,et qui consistent à installer un VPN MPLS (MultiProtocol Label Switching), mettre en place un système de redondance de routeurs en cas d'altération du routeur initialement mis en place, configuration et sécurisation des ports. Vu que les ports ne sont pas sécurisés donc il est très facile de s'introduire dans le réseau ainsi le com-

promettre par différentes attaques tel que des attaques par déni de service (que nous avons simulé et que nous verrons par la suite) qui peuvent être facilement établies une fois connect au réseau, donc nous avons configur et sécurisé les nombreux ports. Or en raison de la contrainte de temporelle,nous n'avons pas pu mettre en œuvre la SD WAN (Software Defined Wide Area Network) qui est une nouvelle technologie, mais que nous envisageons de réaliser au futur.

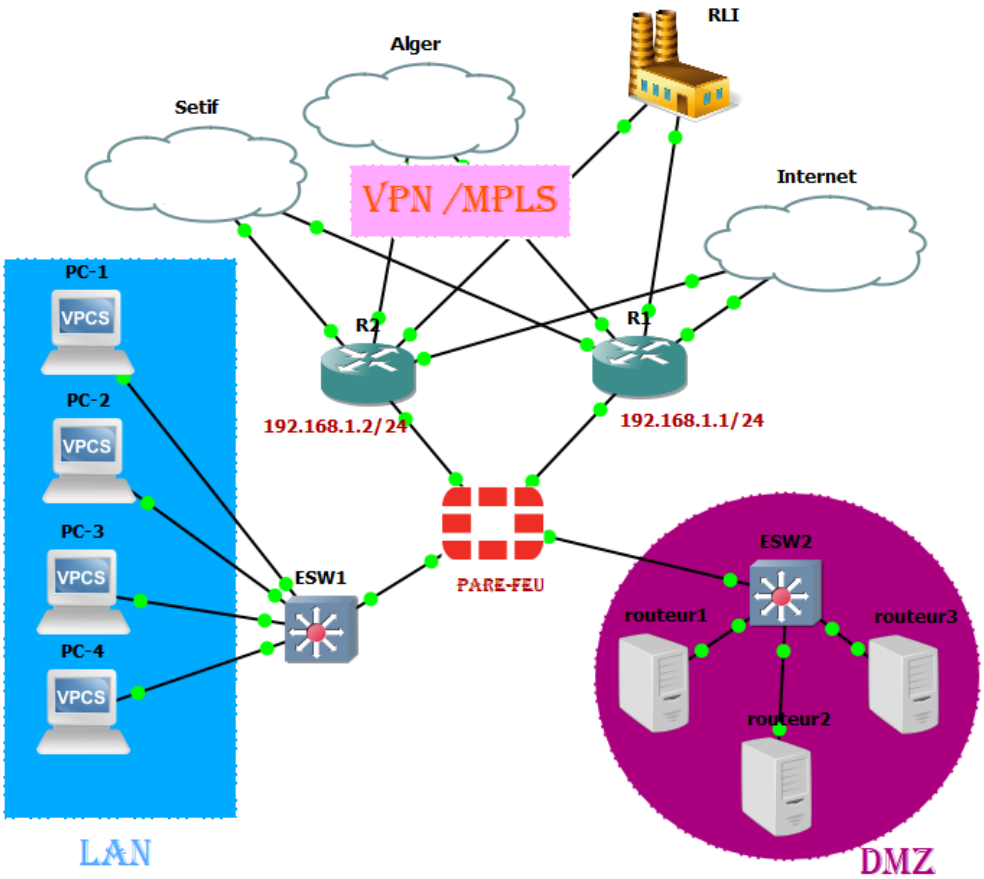

FIGURE 4.3 – Présentation de l'architecture proposée.

VPN MPLS : C'est la solution la plus répondue avant l'apparition des SD WAN. Elle est la plus adapté aux grandes entreprises, or elle a des inconvenants tel que l'agilité dans l'ajout des liens privés,. . . , etc. Malgré cela elle dispose de nombreux avantages comme[**?**] :

— La fiabilité.

— Canal privé pour le trafic

— Evolutivité

SD WAN : Cette solution est neuve et offre de nombreux avantages pour les entreprises cherchant plus d'agilité ainsi que la préparation des différents évolutions avec l'émergence du cloud, elle présente beaucoup d'avantages dont [**?**] :

— Préparation à l'intégration du Cloud.

— Simplification de l'évolution de l'infrastructure réseau.

— Omission des limitations de bande passante.

La différence entre les deux : La solution VPN MPLS est extrêmement fiable en offrant aux clients le service de lignes privées ou alloues, contrairement à la SD WAN qui emploie l'infrastructure Internet public tel que réseau de transport[**?**].

— La SD WAN est conçu pour surpasser les performances de MPLS, cependant elle peut aussi fonctionner avec MPLS.

— SD WAN offre de multiples types de connections réseau, dont les lignes MPLS.

— La SD WAN a virtualiser les infrastructures alors que le MPLS est toujours basé sur le hardware.

— La SD WAN vise à réduire les couts.

4.5 Attaque DNS Spoofing :

Cette attaque consiste à configurer le DNS en modifiant le fichier etter.dns qui appartient à l'outil ettaercap. Une explication théorique détaillée de l'attaque se trouve dans l'annexe B. Tout d'abord, La commande employée pour accéder

au fichier **etter.dns** est : **nano /etc/ettercap/etter.dns** . Après avoir accédé au fichier etter.dns, nous avons ajouté la ligne : ***A 192.168.81.130.** Cette dernière signifie qu'on va rediriger tout le trafic vers l'adresse IP **192.168.81.130** qui est celle de notre machine kali linux. La figure suivante illustre l'ajout de la commande de redirection du trafic dans le fichier **etter.dns**.

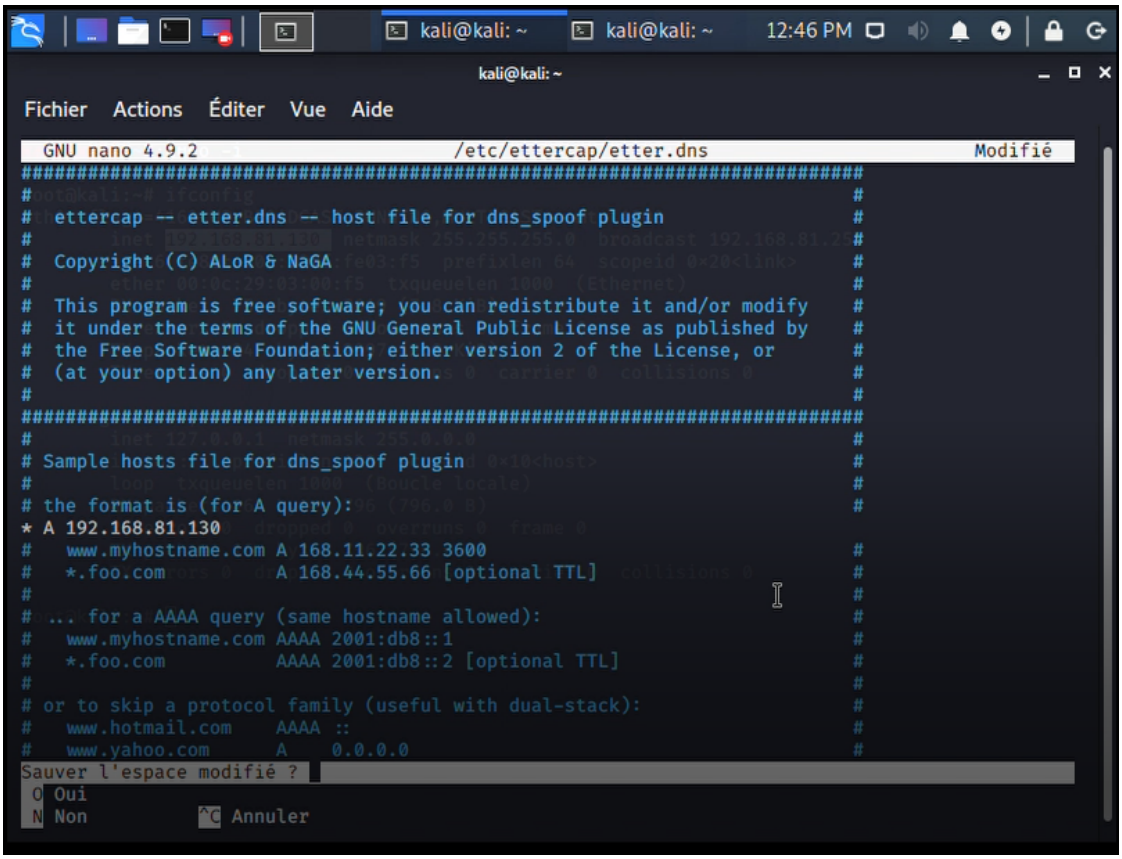

FIGURE 4.4 – L'ajout de commande de redirection de trafic dans le fichier etter.dns.

Puis on a lancé le service **Apache2** là où la cible va atterrir (ce dernier est modifiable et personnalisable) avec la commande : service apache2 start . Il s'active en tapant la commande : **/var/www/html/index.html**. Voici dans la figure suivante le code source de la page **index.html** là où la cible va atterrir dès qu'elle essaiera de se connecter à internet.

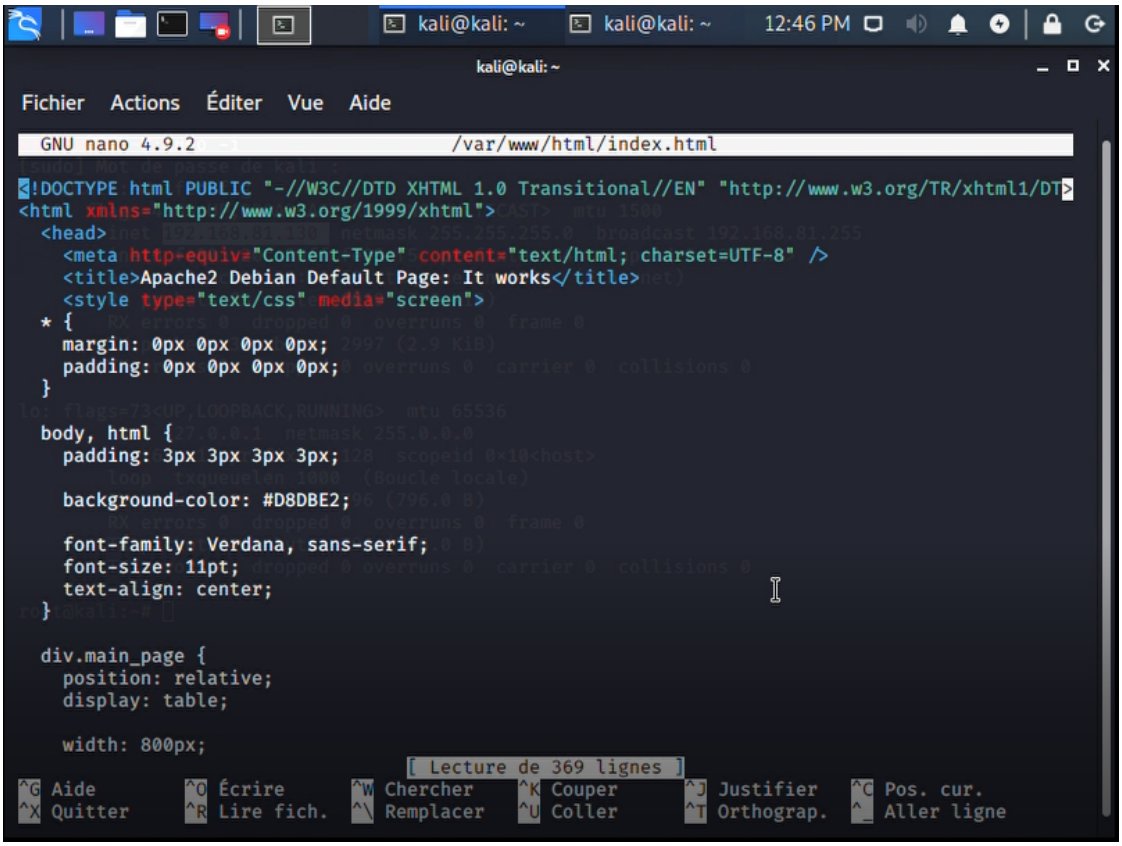

FIGURE 4.5 – La page html qui s'affichera en cas de tentative d'accès à Internet.

Enfin, dans la dernière étape qui consiste à exploiter le protocole ARP avec la commande suivante :**ettercap Tqi eth0 P dns-spoof -M arp** .En employant l'extension **dns-spoof** et l'attaque ARP avec **-M arp** . Dans ce cas l'attaque s'est exécutée directement et l'extension **dns-spoofing** s'est activé, puis le lancement de l'attaque s'est suivi. Et donc tous les utilisateurs du réseau ont été redirigés vers le serveur de notre machine kali linux. La figure suivante illustre la manière dont le trafic est spoofer vers la machine kali.

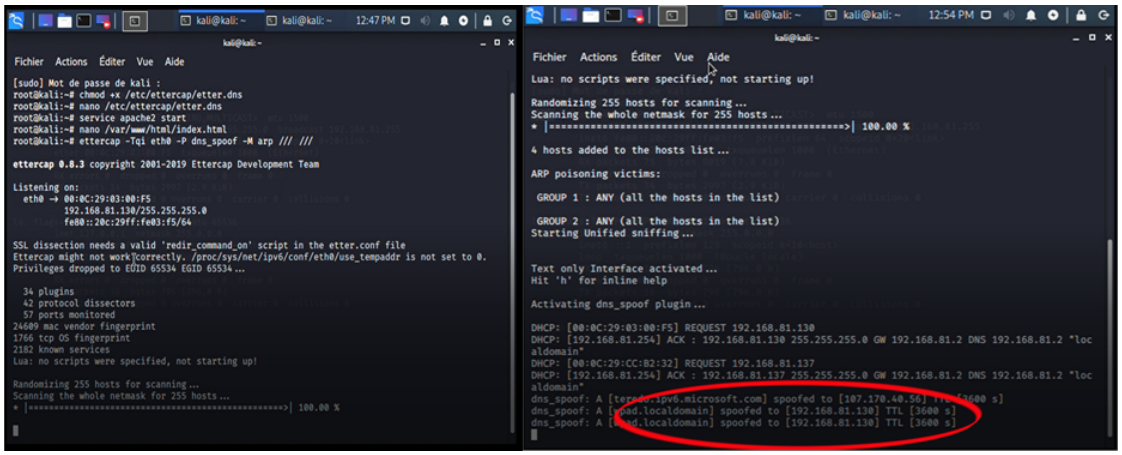

FIGURE 4.6 – Le lancement de l'attaque ARP et la redirection du trafic.

Des pages de login peuvent également être employées dans le but de récupérer des informations.

4.6 Attaque DoS TCP SYN flood :

C'est une attaque par protocole qui consiste à envoyer des requêtes de type SYN à la machine cible dans le but d'envahir cette dernière, elle reserve le port 80 dans notre cas et le service mis en arrêt. Une explication théorique détaillée de l'attaque se trouve dans l'annexe B. Tout d'abord nous avons commencé par lancer l'outil Metasploit avec la commande : **msfconsole**, puis avec la commande **use auxiliary/dos/synflood** nous avons pu avoir accès à l'outil. Ensuite nous avons modifié les paramètres afin de cibler le port et la machine qu'on voulait attaquer et qui est dans notre cas le port 80 correspondant au service HTTP (Hypertext Transfer Protocol), puis nous avons défini l'adresse IP de la cible avec la commande : **set RHOST 192.168.81.138** , et nous avons défini l'adresse IP qui s'affichera chez la cible comme étant l'adresse IP source dans le but de camoufler notre adresse. Dans notre cas on avait choisi de définir deux adresses source qui sont **192.168.81.26 et 192.168.81.04** avec la commande : **set SHOST 192.168.81.26**, pareil pour l'adresse **192.168.81.04** . La figure suivante montre les étapes de configuration des options de l'outil Metasploit.

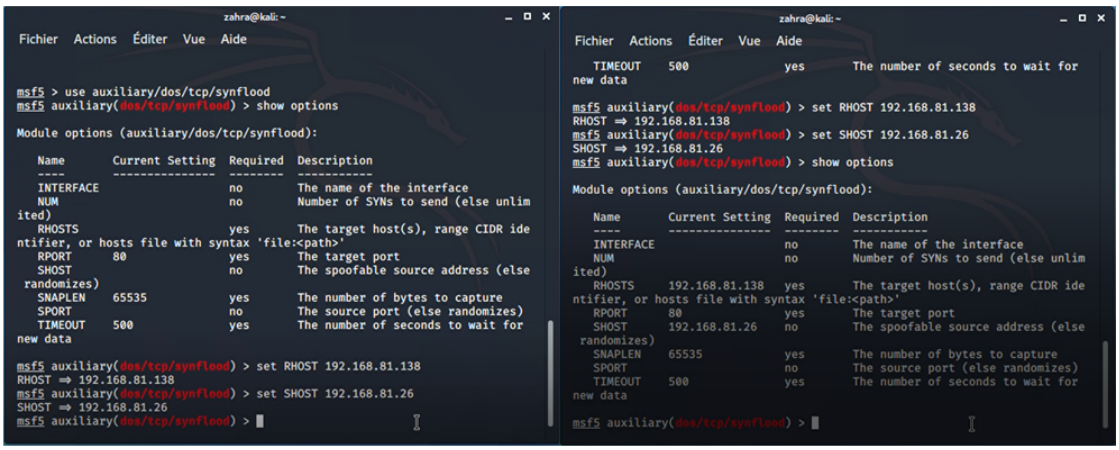

FIGURE 4.7 – La configuration de l'outil Metasploit afin de réaliser une attaque TCP SYN flood.

En outre, à l'aide de la commande **exlpoit** on a pu mener l'attaque. Afin de voir le comportement de la machine cible, on a appliqué un filtre dans le but de voir le comportement des paquets TCP, et comme prévu nous avons constaté qui il n'existait que des requêtes SYN de la part des deux adresses que nous avions précédemment configuré sans réponse preuve de succès de l'attaque. La figure suivante nous montre les différents paquets reçus par la machine cible après l'application de l'attaque DoS TCP SYN flood.

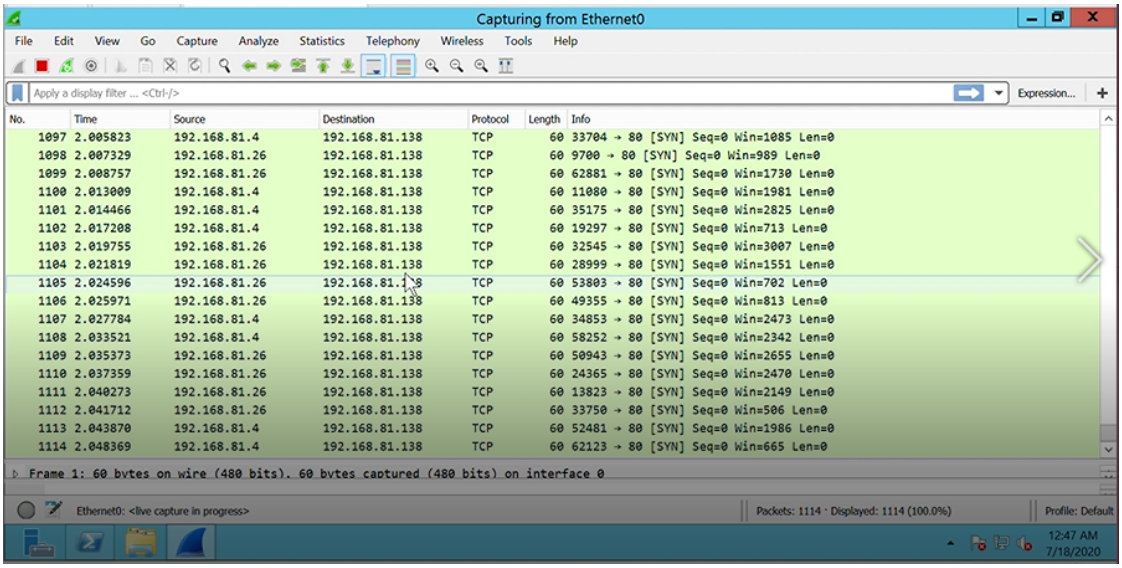

FIGURE 4.8 – Les paquets reçus par la machine cible.

4.7 Conclusion

La sécurité des réseaux informatiques est difficile à réaliser, un attaquant n'aura besoin que d'une seule faille pour pouvoir accéder et nuire à un réseau alors qu'un administrateur doit identifier toutes les failles possibles et les sécuriser afin d'éviter les multiples attaques. C'est pour cela que nous avons parcouru et chercher à corriger les failles et les ouvertures qu'on a pu en tirer après application de notre référentiel de sécurité pour en arriver à l'architecture proposer dans ce chapitre. On a voulu employer la technologie de la SD WAN, cependant par manque de temps et de stage vu les conditions sanitaires actuelles, on estime qu'il est meilleur d'adopter cette technologie dans le futur.

CONCLUSION GÉNÉRALE

Dans le contexte de sécurité, les entreprises mènent des efforts et réflexions pour assurer la sécurité du réseau, cependant cette dernière est particulièrement en évolution constante ce qui s'accroit à cause de l'ouverture des systèmes informatiques sur internet, et donc l'augmentation de niveau de risque interne et /ou externe, par conséquent les entreprises doivent protéger leurs réseaux en suivant une architecture de sécurité bien définie. Tout au long de notre travail, qui consiste à bâtir un référentiel de sécurité comportant les différentes faces de sécurité réseau, nous nous sommes basés sur le fait que la sécurité peut être très sensible et qu'elle peut être défectueuse par l'influence d'un minimum de menaces présentes. Dans le but de cerner la sécurité réseau dans une entreprise, nous nous sommes tournées vers la récolte d'un maximum d'information sur le concept de sécurité, puis nous nous sommes trouvés à faire une recherche sur les diverses attaques qui peuvent nuire à un système informatique en général et à la sécurité des réseaux en particulier ainsi que simuler quelques-unes d'entre elles. En outre, nous avons bâti un référentiel de sécurité des réseaux en nous basant sur nos recherches, et qui a pour but de sécuriser un réseau d'entreprise contre tout incident ou attaque malveillants. Nous avons par la suite appliqué ce dernier sur un cas d'étude qui est la SPA General Emballage afin de tester la robustesse de son réseau, puis proposé des solutions et une nouvelle architecture réseau sur GNS3 pour mieux assurer la sécurité.

En réponse à notre problématique de départ qui consistait à recueillir toutes les méthodes pour avoir une sécurité optimale d'un réseau informatique. En

effet, il existe de nombreuses méthodes à suivre afin de réalisé la sécurité d'un réseau informatique, cependant il ne faut pas prendre en considération que les configurations de base, mais plein d'autres facteurs peuvent jouer sur le taux d'exposition du réseau aux multiples risques, et donc un attaquant pourra s' y introduire et infecter le réseau. C'est pourquoi notre référentiel recueillant les divers dispositifs et visant la sécurité optimale traite tous les angles et passe au peigne fin les endroits ou une menace pourra naitre et ainsi endommager notre sécurité. Tout au long du processus d'application de notre référentiel sur notre cas de recherche, nous avons constaté des anomalies de sécurité, c'est pourquoi nous avons présenté plusieurs solutions qui mettent fin à plusieurs problèmes et qui ont pour but de rendre la sécurité réseau de Général Emballage plus robuste et optimale. Or c'est toujours insuffisant, car il existera toujours une attaque qui pourra surgir et nuire à la sécurité. En guise de perspective, nous envisageons de :

— Appliquer une connexion SDWAN entre les différents sites de l'entreprise, dans le but d'optimiser un réseau Internet.
— Installation d'un VPN MPLS.

BIBLIOGRAPHIE

[1] http :// referentiel-de-normalisation-de-la-securité-informatique.com.

[2] http ://Graphical Network Simulator.com.

[3] https ://www.vmware.com.

[4] www.sdxcentral.com.

[5] http :// Kali Linux Wireless Pentesting and Security for Beginners-rootsh3ll.com, (Consulté le 1 septembre 2020).

[6] J.-F. CARPENTIER. *sécurité informatique dans la petite entreprise*. 13 janvier 2016.

[7] S. Lohier. *le réseau intrenet*.

[8] R. Messier. *CEH v10 Certified Ethical Hacker Study Guide*. Sybex, 2019.

[9] S.-P. Oriyano. *CEH v9-Certified Ethical Hacker version 9 study guide*. Sybex, 2016.

[10] G. Pujolle. *les réseaux*. 2008.

[11] V. REMAZEILLES. *La sécurité des réseaux avec CISCO et le guide sécurité Cisco*. Eni, 09/02/2009.

[12] V. REMAZEILLES. *Le grand livre de securite*. https ://www.securiteinfo.com/, 19 février 2004.

[13] Sean-philip. *Ethical Hacking priyano –ceh v9.* 2016.

[14] W. Stallings. *Cryptography and Network Security Principles and Practice.* Global Edition-Pearson, 2017.

[15] B. Vachon. *CCNA Security (210-260) Portable Command Guide.* Global Edition-Pearson, 2016.

[16] M. Walker. *CEH Certified Ethical Hacker All-in-One Exam Guide.* 2019.

ANNEXE A

RÉFÉRENTIEL DE SÉCURITÉ

A.1 Bonnes pratiques pour mieux sécurisé un réseau

En se basant sur le référentiel de normalisation de la sécurité informatique et sur de nombreux ouvrages et recherches, nous avons pu mettre à pied le référentiel suivant :

A.1.1 Sécurité logique et réseau

Conception et Gestion des réseaux

Les mécanismes de gestion de l'infrastructure réseau :

- La distribution des tâches, rôles, responsabilités des acteurs qui sont responsables de la gestion de la configuration des réseaux ;
- Un document réseau qui contient :
  - La topologie du réseau, les équipements réseaux et les connexion autorisées ;
  - Un diagramme logique des services et les serveurs critiques ;
  - La configuration de tous les équipements ;
- Le document doit être actualiser à chaque changement.

— Installation des équipements réseaux actifs (routeurs, pare-feu, Switch) pour interdire les accès physique non autorisé et assuré l'intégrité.
— Administré les périphériques en assurant l'authentification, la traçabilité et l'autorisation.
— La surveillance du trafic et l'enregistrement des logs.
— Des accès aux ressources réseaux à fin d'exécuter leurs tâches.

Configuration des équipements réseaux

— Les premières protections du périmètre réseau tel que les routeurs et les pare-feu et tous les équipements de connectivité doivent être personnalisé et reconfiguré lors de l'installation :
  — La désactivation des comptes par défaut ou changer leur identité avant l'utilisation de ces derniers.
  — Application de la gestion des configurations et des correctifs de tous les équipements.
  — Autorisation formelle des modifications.
  — La synchronisation des horloges de tous les systèmes pour assurer la précision des données et des journaux d'audit.
  — Assurer que les équipements sont reliés à une source d'alimentation sans coupure.
  — La désactivation des ports physique non utilisés.

Segmentation du réseau

— Pour la protection des serveurs on doit séparer le réseau interne de l'organisme en definissant des zones demilitarisées DMZ.
— L'évaluation des risques de la sécurité à fin de déterminé les nombres de zones à éliminer. La documentation des zones : Ses composantes, les risque,...,etc.
— Si l'organisme utilise un réseau sans fil destiné aux visiteurs alors ce dernier doit l'isoler du réseau interne.
— Si l'organisme utilise un réseau sans fil dans son réseau interne il doit appliquer des méthodes de sécurité très strictes.

— Séparation des serveurs d'applications et les serveurs de base de données par des mécanismes et des dispositifs.

— Les organismes ne disposant pas des moyens permettant la mise en œuvre de la segmentation du réseau et autres exigences de sécurité doivent identifier les zones réseaux et documenter les raisons ayant empêché leur mise en œuvre. Ces zones doivent être mise en œuvre dès la levée des raisons ayant empêché leur concrétisation.

— La sécurisation des environnements virtuels (entre les machines virtuelles), et on doit les séparer du réseau (équivalent à L'environnement physique).

Router(config)# privilege mode level level command — reset command	Attribuer des commandes à un niveau de privilège personnalisé Entre le niveau 2 et 14. Il existe 16 niveaux de privilèges. Le niveau 0 est l'entrée niveau, le niveau 1 est pour l'accès EXEC de l'utilisateur, et le niveau 15 est un mode EXEC privilégié. Les niveaux 2 à 14 sont Personnalisable.
Router(config)# enable algorithm-type md5 — sha256 — scrypt secret password	Attribuer un mot de passe au niveau de privilège personnalisé.
Router #¿ enable level	Entrez un niveau de privilège personnalisé.

TABLE A.1 – Les lignes virtuelles.

Authentification des équipements réseaux

— Le teste périodiques des mesures d'authentification des équipements connectés aux réseaux.
— Les équipements réseau de l'organisme ne doivent autoriser que la connexion des équipements préalablement identifiés à partir de chemins spécifiques.

Routage et configuration des pare-feu et VPN

— La configuration du système afin de contrôler les communication interne et externe du réseau.
— Dans les contrôles de protection on doit avoir ces éléments :
  — La vérification des adresses source et destinations ;
  — L'authentification des administrateurs des équipements ;
  — Masquer les adresses du réseau interne.
— Installer et configurer le pare-feu comme suivant :
  — La configuration par défaut consiste à interdire les trafics sauf les services autorisés.
  — Le pare-feu peut avoir un ou plusieurs administrateurs.
  — Les ouverture exceptionnelle d'un port doit être limité et autorisée dans le temps, l'administrateur doit fermer le port juste après le délai.
  — Configuration des pare-feu de sorte qu'on peut pas l'identifier en tant que tel.
  — Les pare-feu doit être installer dans des lieux physiques sécurisé et il ne faut pas les déplaces sans l'autorisation de l'organisme.
— Les pare-feu doit avoir les règles suivantes :
  — Interdire le trafic réseau entrant d'une source inconnue.
  — Interdire le trafic réseau entrant d'un réseau externe avec une adresse locale.
  — Interdire le trafic entrant d'une source non autorise avec des paquets ICMP.
  — Interdire le trafic réseau avec des informations de source de routage
  — Interdire le trafic avec une adresse IP 0.0.0.0.
  — Interdire le trafic réseau entrant ou sortant avec des adresses de dif-

fusion.

— La configuration du pare-feu à fin d'enregistre tous les paquets rejetés.

— La vérification des fichiers de configuration des pare-feu périodiquement.

— Realisation de VPN afin de sécuriser les échanges distants, ce qui suit est un exemple de configuration d'un VPN :

titre : Exemple de configuration site a site ipsec vpn[15] :

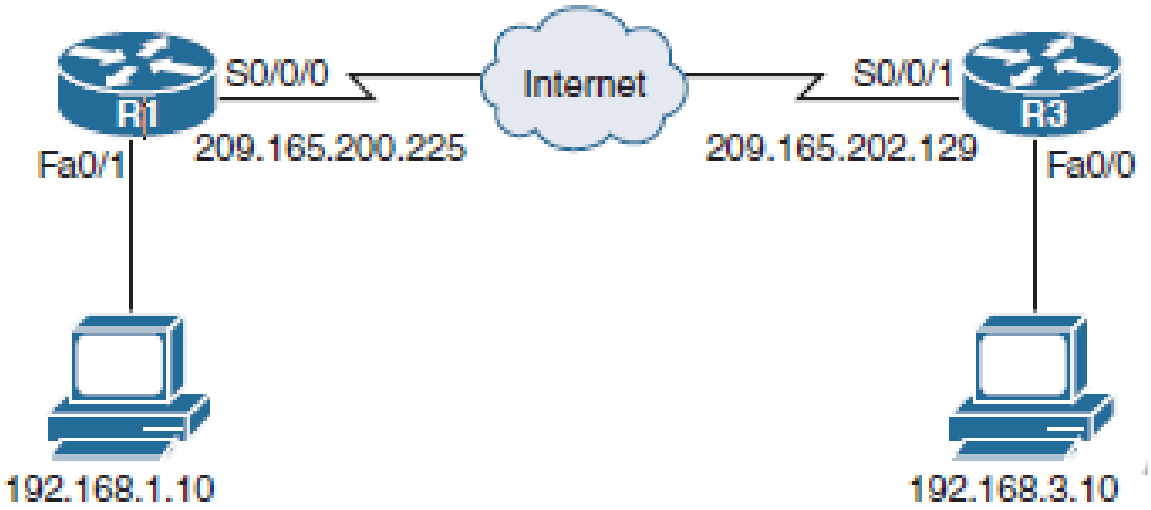

FIGURE A.1 – Exemple de configuration site à site ipsec VPN[15].

Router(config R1(config)# crypto isakmp policy 1	Définir les paramètres de la politique IKE. Des utilisateurs locaux et crypter le mot de passe en utilisant soit le type 8 (sha256), soit Tapez les mots de passe de type 9 (scrypter).
R1(config-isakmp)# hash sha256	Définir l'algorithme de hachage pour l'IKE politique.
R1(config-isakmp)# authentication pre-share	definir la methode d'authentification pour la politique IKE .
R1(config-isakmp)# group 24	Définir le groupe DH à utiliser pour la politique IKE politique.
Router(config-line) line aux 0	Entrez en mode auxiliaire de ligne.
Router(config-line)#no exec	Désactivez le port auxiliaire.

TABLE A.2 – Créer la politique IKE(Internet Key Exchange) 1 et configurer les parametres requis pour la phase 1.

R1(config)# crypto isakmp key cisco123 address 209.165.202.129	Réglez le PSK pour la paire R3.

TABLE A.3 – la precision du PSK et identifier l'addresse.

R1(config)# crypto ipsec transform-set R1-to-R3-SET esp-aes esp-sha-hmac	Définir le jeu de transformation et les paramètres IPsec.
R1(cfg-crypto-trans)# exit	Retour au mode de configuration globale.

TABLE A.4 – La creation de la politique IPsec.

R1(config)# crypto map R1-to-R3-MAP 1 IPsec-isakmp	Définir la carte cryptographique des paramètres du VPN IPsec site à site.
R1(config-crypto-map)# description Create a site-to-site VPN when going from R1 LAN to R3 LAN	documenter la carte cryptographique.
R1(config-crypto-map) # set transform-set R1-to-R3-SET	Identifier la manière de transformer à utiliser avec ce Carte cryptographique.
R1(config-crypto-map)# set peer 209.165.202.129	Identifier la paire utiliser avec cette carte cryptographique
R1(config-crypto-map) # match address VPN-ACL	Identifiez l'ACL (Access Control List) crypto à utiliser avec cette carte cryptographique.
R1(config-crypto-map)# set pfs group24L	Identifier le groupe DH(Diffie Hellman).
R1(config-crypto-map)# set securityassociation lifetime seconds 900	Identifier le temps de vie d'une carte cryptographique.
R1(config-crypto-map)# exit	Retour au mode de configuration globale.

TABLE A.5 – La création de la carte crypto..

R1(config)# ip access-list extended VPN-ACL	Créer un ACL étendu.
R1(config-ext-nacl)# remark IPSec Rule	Fournir la documentation de l'ACL.
R1(config-ext-nacl)# permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255	Identifiez le trafic intéressant.
R1(config-ext-nacl)# exit	Retour au mode de configuration globale.

Table A.6 – La creation du ACL cryptographique

R1(config)# interface s0 R1(config-if) #crypto map R1-toR3-MAP	Précisez le type et le numéro de l'interface .

Table A.7 – L'application de la carte cryptographique à une interface.

Utilisation des systèmes de détection et de prévention d'intrusion IDS /IPS ainsi que d'un vpn multi sites.

— Mettre en œuvre une stratégie de détection d'intrusion, qui comprend :
  — L'installation des identifiants des systèmes de détection des intrusions sur le réseau.
  — Les procédures et les ressources utilisées pour la gestion des bases de connaissance et des mécanismes lors de la détection.
  — L'utilisation des ressources et procédures afin d'analyser les journaux d'évènements et des alertes en temps réel.

Transmission des données

Contrôle de la distribution et transmission des données

— Les organismes gèrent l'échange et le transfert de données électronique pour assurer les exigences de sécurité.
— Les organismes doivent avoir des contrôles et des procédures techniques

afin de garantir que les données ne soient pas échangées qu'avec autorisation.

— L'utilisation de protocole sécurisés doit être privilégiée.

Contrôle des Transactions en ligne

(a) Quand l'organisme autorise les transactions en ligne il doit mettre des contrôles tel que :
   — La validation des identités de la transaction.
   — Obtenir l'approbation appropriée pour la transaction.
   — Protection des données confidentielles.
   — Assurer l'intégrité.
   — Avoir la preuve que la transaction est achevée correctement.
   — Interdire la relecture non autorisée d'une transaction.

(b) Les méthodes pour mettre en œuvre les contrôles ci-dessus dépendent de la nature de la transaction et du niveau du risque identifié. Elles peuvent inclure sans s'y limiter :
   — L'utilisation des signatures électroniques ;
   — L'utilisation des techniques d'authentification fortes ;
   — l'Enregistrement des transactions dans un lieu sécurisé.

Courriel et Communication sur Internet

Envoi et réception de courrier électronique (e-mail)

— Chaque organisation doit installer une messagerie électronique, hébergée sur le territoire national pour les utilisations professionnelles.
— Mettre des règles pour l'utilisation de la messagerie :
   — règle liées au transfert automatique des emails.
   — La Protection des données confidentielles transmises.
— La messagerie professionnelle doit être utilise que pour le travail.
— Interdire l'usage des adresse mails personnelles et l'ouverture des pièces jointes avec des adresses mails inconnues.
— Le personnel doit être professionnelle leur de l'utilisation des courriers électroniques :
   — L'adresse du destinataire est bien formulée ;

  - Le destinataire est habilité à accéder au contenu transmis ;
  - Les bonnes pièces jointes ont été rattachée au document ;
- Interdire l'ouverture des boites mail professionnelle dans des espaces communautaires d'accès a internet et sensibiliser les utilisateurs aux risques liée à l'usage de la messagerie.

Usage d'internet pour des buts de travail les usagers d'Internet doivent se tenir aux :

- Le respect des droits d'auteurs de logiciels et licences et ne pas accéder là où on n'est pas autorisé.
- Ne pas s'en servir pour des fins malveillantes, ne pas encombrer le réseau et faire attention lors des téléchargements en employant des antivirus.

Usage des medias sociaux

- Quand ils sont employés dans des buts professionnel, l'organisme se doit de :
  - Mettre en place des guides de travail pour les employés destinés à utiliser ces sites dans le cadre professionnel ;
  - Eviter le piratage et les accès non autorisés en utilisant des mots de passes divers respectant la politique mise par l'organisme pour chaque réseau et se servir de la double authentification.
- Dans le cas d'usage privé, l'organisme se doit d'interdire l'emploi d'adresse professionnelle pour l'ouverture des comptes de medias sociaux ainsi que de fournir des informations liées au grade, ou aux fonctions de ces derniers dans les réseaux sociaux. Il leur est interdit de divulguer toute information liée à la vie professionnelle et les sensibiliser aux risques de divulgations d'informations sur les réseaux sociaux.

Filtrage du contenu non appropriés sur Internet

- Mise en place de dispositifs afin de filtrer le contenu et l'accès à internet, et en informer le personnel de sa présence.
- le dispositif va stocker l'historique des visites et des téléchargements des sites web et documenter.

Sécurisation des communications Afin de sécuriser les communication de type confidentiel :

— Interdiction du transfert des données confidentielles par ligne téléphonique.
— Prise en charge des mesures de sécurité appropriées dans des échanges par voie IP et interdire ceux hébergées en dehors du territoire national.
— Chiffrer les données confidentielles lors de transmission passant par les réseaux sans fil ou publics.

Sécurisation des réseaux sans fil

afin d'éviter l'écoute et l'accès non autorisé, les points d'accès réseau sans fil de l'organisme employer pour usage interne doivent respecter[1] :

(a) Accès physique :

i. La sécurisation des points d'accès au réseau, ainsi que les équipements connexes par des mécanismes de verrouillage, ou les placer dans une zone d'accès limité au personnel autorisé ;

ii. En disposant les points d'accès de tel sorte à accomplir, La minimisation de propagation du signal au-delà du périmètre de l'organisme.

(b) Accès réseau :

i. Quand les points d'accès sont connectés au réseau local (LAN), ils doivent se connecter via un dispositif (passerelle) ;

ii. La personnalisation de la valeur par défaut du SSID(Service Set Identifier) et le nom SSID ne doit comprendre des indicateurs sur l'organisme, son lieu, les fonction de point d'accès.

(c) Système d'accès :

i. Les points d'accès sont obligées d'imposer un mot de passe afin d'accéder à ses fonctions administratives, il doit être stocké, transmis en format crypté et ne doit être communiquer qu'aux personnes autorisées.

ii. configurer les niveaux des Privilèges[15] :

Router(config)# privilege mode level level command — reset command	Attribuer des commandes à un niveau de privilège personnalisé Entre le niveau 2 et 14. Il existe 16 niveaux de privilèges. Le niveau 0 est l'entrée niveau, le niveau 1 est pour l'accès EXEC de l'utilisateur, et le niveau 15 est un mode EXEC privilégié. Les niveaux 2 à 14 sont Personnalisable.
Router(config)# enable algorithm-type md5 — sha256 — scrypt secret password Définir l'algorithme de hachage pour l'IKE politique.	Attribuer un mot de passe au niveau de privilège personnalisé.
Router # ¿ enable level	Entrez un niveau de privilège personnalisé.

TABLE A.8 – la configuration des privilèges.

(d) Authentification de tout accès au réseau via un réseau sans fil.

Sécurité des systèmes

acquisition et installation des logiciels

— acquisition :
  — Les logiciels et les systèmes utilisés doivent avoir une licence officielle, nulle ne doit être piraté ;
  — Ne passer que par des sites officiels d'éditeur lors des téléchargements de logiciels sur internet, et ne pas obtenir de logiciels/applications dont l'éditeur a annoncé la fin du support ;
  — Il est conseillé d'obtenir les plus récentes versions des systèmes et logiciels ;
— Installation :
  — L'installation et l'usage de logiciel/application sans licence valide doit être interdit ;
  — Un accord des structures concernées est requis pour l'installation des

logiciels/applications par l'utilisateur final sur son poste de travail ;

— Ne doivent pas être installés les postes et les serveurs, ou se trouve les logiciels requis à l'accomplissement des missions de l'organisme ;

— Les mots de passes par défaut doivent être changés en fonction de la politique ajustée à cet effet.

Inspection et le contrôle du code source des différents logiciels afin de lutter contre le détournement et l'usage illicite :

— Les code sources des applications importantes acquises ou développées doivent être examinés ;

— L'accès aux codes sources doit être réservé au personnel autorisé et ils doivent être stockés dans un emplacement préservant leur intégrité et confidentialité.

Maintenance et la mise à jour des logiciels afin de conserver les systèmes d'informations des vulnérabilités découvertes.

Mise à jour des logiciels

(a) Les Mises à jour des logiciels et systèmes sont imposées et doivent être adaptée dès publication et un plan de réstauration doit être mis en position en cas des mises a jours critiques ;

(b) Les mises à jour doivent être testées dans un cadre de test similaire à un déploiement de masse ;

(c) Les opérations de mises à jour doivent être enregistrées et ne doivent être faites que par le personnel qualifié.

Maintenance des logiciels

(a) Dès leurs apparences, les erreurs et les bugs doivent être notifiés au service concerné ;

(b) Les recommandations mises par les organismes officiels autorisés par rapport aux vulnérabilités qui n'ont pas de correctifs, doivent être appliquées après avoir été testées dans un environnement restreint.

Opérations réalisées sur les systèmes et logiciels

afin de modérer les systèmes d'informations et les protéger d'usage non autorisé. Opérations d'administration

(a) La nécessité d'auditer périodiquement les systèmes et applications.

(b) Les administrateurs doivent employer des outils d'administration centralisée quand le nombre des ressources est important et les procédures

(c) La documentation des configurations, des mises à jour et des ressources à chaque changement.

(d) Mise en place de système de surveillance et audit afin de détecter toute activité non autorisées ou l'activation de cette fonctionnalité au niveau des systèmes employés.

(e) Mise en place de contrôles pour empêcher l'usage de logiciels non autorisés.

(f) Mise en place d'antivirus ainsi que sa tenue à jour, enregistrer les incident de sécurité sur un serveur pour analyse statique et gestion de problèmes.

(g) La synchronisation des systèmes utilisés par une référence de temps telle service NTP(Network Time Protocol).

(h) La suppression des services non utilisés.

(i) La nécessité de signer une charte d'éthique par les administrateurs.

(j) La surveillance de gestion et sécurité des données partagées par le système et les applications.

(k) La désactivation d'exécution automatique des supports mobiles de postes de travail des utilisateurs.

(l) L'accès a distance aux serveurs réservé aux administrateurs autorisés.

(m) Désactivation d'accès au bureau distant des utilisateurs.

(n) Le verrouillage du BIOS des serveurs et postes de travail avec un mot de passe ainsi que la désactivation de démarrage par CD/DVD.

Opérations des utilisateurs

(a) Mise en place des politiques de gestion, analyses des journaux.

(b) La journalisation et l'enregistrement de l'historique des évènements de sécurité et les systèmes employés.

(c) La conservation des journaux d'incidents de sécurité suivant la politique de gestion et analyse de l'organisme et les protéger contre tout risque d'intrusions et altération.

(d) L'analyse régulière des journaux d'évènements.

Gestion des logs (journalisation)

Les logs, sont des fichiers journaux des multiples services opérants sur le système et sont employés dans le but de résoudre les divers problèmes. Quand un service ne se lance pas ainsi que voir les attaques, tel que les nombreuses tentatives échouées pour accéder en tant qu'administrateur. Ces fichiers se trouvent dans les différents systèmes d'exploitations, dans l'observateur d'évènements sous Windows, et dans des fichiers textes dans /var/log sous linux. Les attaquants cherchent tout le temps à supprimer ses traces, donc les fichiers vides vont être douteux[11].

Tests

Dans le but de garantir l'intégrité et la confidentialité des informations.

(a) La séparation entre les environnements de développement et ceux de production.

(b) Le respect des règles de confidentialité mise par le propriétaire de données lors d'usage de ces dernières dans des environnements de teste ;

(c) L'obligation de tester et d'approuver que les nouveaux systèmes développés répondent aux besoins de sécurité.

Développement et la maintenance des sites web

Afin de minimiser les risques croissants liées aux applications web.

(a) Usage et développement des sites web par du personnel qualifié et avec des méthodes éprouvés et sécurisé ;

(b) Le stockage des mots de passe par les modules d'authentifications employer dans sites web doit être sous forme transformée à l'aide de fonction de cryptographie non réversible ;

(c) L'administration de site web doit être faite à partir des ordinateurs fiables et avec des protocoles sécurisés ;

(d) Mise à jour des systèmes et applicatifs employer par les sites web et bloquer les transferts de la zone DNS sauf en cas de besoin ;

(e) Priver toute divulgation d'informations sur la configuration technique du site et ce dernier doit régulièrement être audité.

Usage des appareils mobiles et supports de stockage

Afin d'éviter le vol et les pértes de données.

(a) Protection des données peuvent être stockées des appareils mobiles et supports de stockage avec des mesures appropriés, et chiffrer les données contenus dans ces derniers ;

(b) La conservation des appareils mobiles et support de stockage sur soi lors des déplacements.

Usage des appareils mobiles

(a) Signalement instantané de pertes d'appareils mobiles à la hiérarchie.

(b) Enregistrement des numéros de série des appareils mobiles des employés par l'organisation.

(c) Priver les utilisateurs des droits administratifs a mois d'exception validée par la hiérarchie.

(d) Verrouillage des appareils quand elles ne sont pas utilisées.

(e) La désactivation des services Wi-Fi et Bluetooth en cas de non nécessité.

Usage des supports de stockage

(a) L'application des procédures de gestion des supports de stockage selon les plans de classification adopté.

(b) Priver la transmission des documents par support mobile aux personnes en dehors de l'organisme, sauf en cas de données volumineuses qui exige l'emploi de support mobile qui doivent être analysé et favorisé le transfert par courriel.

Gestion de donnees

Afin d'assurer la confidentialité, et l'intégrité des informations.

(a) La garantie de confidentialité, intégrité des données par des outils technique tel que le chiffrement.

(b) L'assurance d'intégrité des données par des contrôles applicatifs.

(c) L'interdiction de conserver des données sur des plateformes hébergées à l'extérieur du territoire national.

(d) L'extrait des supports de données avant tout opération de maintenance externe.

Sauvegarde et la restauration et l'archivage

Afin de garantir une la sauvegarde des données pour les récupérés en cas de parte.

(a) Mise en œuvre de processus de sauvegarde et recouvrement périodique, et effectuer cette derniere sur un support externe en prennant en compte la duré de vie des supports.

(b) L'interdiction de conservation des données professionnelles sur des sites de stockage hébergeant les données ailleurs que le territoire national.

(c) la conservation des données chiffrées dans un site distant.

(d) la sauvegarde des configurations des systèmes et logiciels.

(e) la sauvegarde doit se faire suivant les règles définies par le plan de continuité de l'activité.

(f) la compatibilité du fonctionnement de sauvegarde avec le niveau de disponibilité des applications.

(g) Identification des divers medias de sauvegarde par un nom de machine et numéro de série unique.

(h) Testes réguliers des sauvegardes pour garantir la possibilité de restauration dans les moment critiques.

(i) Assurer la restauration des données après incident en testant les nouveaux composants avant toute mise en service de nouveau système.

(j) Mise à jour des sauvegardes en cas de création et changement de contexte d'exploitation

Partenaires

Afin que ces derniers ne forment pas de risque.

(a) Etablissement de contrat de confidentialité avec les fournisseurs des équipements liés au centre de traitement de données.

(b) Mise à jour des contrats en cas de changement.

(c) Garantie de respect des politiques, normes et politiques mise par l'organisme.

(d) La conformité des accès au système d'information du personnel d'entreprises extérieurs au politique d'accès aux moyens informatiques.

A.1.2 Sécurité physique

Zones sécurisées

Afin d'omettre tout accès physique non autorisé. Périmètre de sécurité physique

(a) Fixer les périmètres de sécurité, ainsi que déterminer l'emplacement et le niveau de sécurité en fonction des critères de sécurité

(b) La protection des bâtiments contenant les données sensibles contre tout accès non autorisé.

(c) La surveillance et l'équipement des portes coupe-feu d'alarmes de sécurité aux zones sensibles.

(d) La division physique des moyens de traitements de données gérés par l'organisme et ceux gérés par autres.

Contrôles physiques des accès

(a) Imposition du port des moyens visibles d'identification à l'ensemble des employés et autres.

(b) Limite d'accès sauf aux personnes autorisées et la justification d'accès pour les personnes externes et les accompagner en les tenant au courant des exigences de sécurité a respecter.

(c) Application de contrôles supplémentaires en cas d'accès aux zones de traitement ou stockage d'informations sensibles.

(d) Mise à jours permanente des droits d'accès aux zones sécurisées.

Sécurisation des bureaux ,salles et équipements

— Le choix d'emplacements non accessible pour les équipements-clés.

— Les emplacements de traitements de données sensibles ne doivent pas être dévoilés.

Protection contre les menaces extérieures et environnementales

(a) Prise en compte de tout incident pouvant se produire dans les locaux voisins et présentant un risque tel que des incendies,...,etc.

(b) Isolement des matières dangereuses combustibles loin de la zone sécurisée.

(c) Distancement du matériel de secours pour éviter les dommages engendrés par un accident touchant le site principal.

(d) Prévention de lieu approprié pour le matériel de lutte contre incendie.

Travail dans les zones sécurisées

(a) Mise au courant des employés sur l'existence de zones sécurisées et que toute intervention en zone sécurisée doit être encadrée et justifiée.

(b) Verrouillage physique des zones sécurisées non utilisées.

(c) Interdiction de tout appareil enregistrant et filmant sauf avec autorisation.

Zones de livraison et chargement

(a) Empêcher les accès non autorisés en isolant les points d'accès et les moyens de traitements.

(b) La limitation d'accès à la zone de livraison et chargement sauf au personnel autorisé.

A.1.3 Sécurité du Matériel

afin d'omettre les pertes et les problèmes des activités de l'organisme.

Emplacement et protection du matériel

(a) Diminution des accès inutiles aux zones de travail en choisissant soigneusement l'emplacement du matériel.

(b) Protection des moyens de stockage contre tout accès non autorisé.

(c) Isolation des données nécessitant une protection particulière.

(d) Employer des mesures afin de diminuer au maximum les risques d'incidents de toute forme.

(e) Surveillance des conditions comme la température, humidité pouvant nuire au fonctionnement des outils de traitement de données.

(f) Protéger les bâtiments contre la foudre et tonnerre.

Services généraux

(a) Le dimensionnement correcte des services généraux comme l'électricité,...,etc, dans le but de répondre aux besoins de l'organisme.

(b) Garantir le bon fonctionnement des services en les contrôlant régulièrement.

(c) Fourniture d'alimentation électrique appropriée et conforme aux spécifications du fabricant du matériel et prévoir un éclairage de secours.

(d) Usage des onduleurs et générateurs de secours.

(e) Garder en fonctionnement deux voies de communications vers l'extérieur au minimum.

Sécurité du câblage

(a) Enterrement si possible ou prise de toute autre mesure de protection possible pour les lignes électriques et télécommunication liées aux moyens de traitement de données et les départagés afin d'évité toute interférence.

(b) Planification des mesures supplémentaires pour les systèmes sensibles tel que :

   i. Mise en place de conduit de câbles blindés, des boites verrouillées aux extrémités en guise d'inspection ;

   ii. Détection de branchement d'appareils non autorisé en utilisant le balayage technique ainsi que l'inspection physique.

Maintenance du matériel

(a) La conservation du matériel selon les spécifications recommandées par le fournisseur.

(b) La garantie de maintenance du matériel par le personnel autorisés.

(c) Conservation d'une liste de toutes les pannes et de toutes les actions de maintenance préventifs et correctifs.

(d) Mise en place des mesures appropriés lors de maintenance du matériel en prenant en compte la nature de l'information stockée de dans, et la nature des personnes appliquant l'opération de maintenance (personnel sur site ou extérieur à l'organisme).

(e) Vérification du matériel en fin de maintenance avant remise en service.

Sortie des actifs

(a) Les actifs locaux ne doivent pas quitter l'organisme sans autorisation préalable.

(b) Identifications des personnes qui ont l'habilité de retrait d'actifs du site.

(c) Préciser les délais de sortie des matériels et veiller à leur respect, enregistrer leur retour en documentant toute opération de ces derniers

(d) Mise en place des contrôles afin de détecter toute sortie d'actifs non autorisé.

Sécurité du matériel et des actifs hors site

(a) En dehors du site, tout usage des matériels de traitement de données doit être autorisé par l'organisme et des mesures de sécurité doivent etre defini pour leurs emplacements.

(b) Tenir compte des instructions des fabriquant visant à protéger le matériel.

(c) Documenter la traçabilité du matériel quand il circule en dehors des locaux de l'organisme.

Recyclage sécurisés du matériel

Les équipements comportant des informations confidentielles ou protégées par les droits d'auteurs doivent être détruits ou bien les informations contenues doivent l'être en employant des techniques rendant l'information d'origine irrécupérable.

Politique du bureau propre et d'écran vide

(a) Mise sous clé les données sensibles ou critiques associées à l'activité de l'organisme.

(b) Protection des points d'entrée/sortie des courriers postaux et télécopieurs.

(c) Extrait immédiat des documents contenant des informations sensibles des imprimantes.

A.1.4 Gestion des incidents reliés à la sécurité de l'information

Contrôle des systèmes Afin de déterminer les menaces conduisant aux incidents de sécurité d'informations.

(a) Mise en place de système de journalisation afin d'enregistrer les évènements liés à la sécurité d'information.

(b) Sauvegarde des journaux d'évènements durant une période définie pour faciliter les opérations d'audit.

(c) Interdiction de suppression des journaux d'évènement ou la désactivation de journalisation des évènements par les administrateurs sauf en cas d'autorisation.

(d) Mise en place des procédures d'audit périodique des systèmes de traitement de données.

Protection des informations journalisées Afin de garantir l'intégrité et la confidentialité des informations sensibles, l'organisme se doit de :

(a) Protection de confidentialité, intégrité et disponibilité des journaux d'évènements.

(b) Accessibilité et modification aux systèmes de journalisation doit être réserver aux personnes habilité.

(c) Conservation des rapports d'audit selon la politique de sécurité de l'organisme.

Signalement et gestion des incidents de sécurité informatique Afin de déterminer les risques importants et les fixer dans des limites acceptables.

(a) Mise en place des procédures formelles de signalement des actions ayant un impact sur la sécurité, et elles définissent aussi l'interlocuteur, méthodes et délais de signalement.

(b) Mise au courant de tous les utilisateurs sur les procédures de signalement des divers évènements, et les failles pouvant avoir un impact avec la sécurité.

(c) Etablissement des procédures de réponse en cas d'incident lié à la sécurité informatique.

(d) Mise à jour et amélioration des procédures arrêtées.

(e) Avertissement de sa tutelle par l'organisme en cas d'incident de sécurité informatique.

(f) Mise en place de cellule de veille de sécurité informatique.

Gestion des risques après accident Afin de lutter contre les interruptions, des activités de l'organisme et protéger les systèmes d'informations des effets causées par les défaillances et assurer la reprise de fonctionnement dans les meilleurs délais.

(a) Mise en œuvre des plans de poursuite d'activé, afin de garantir la reprise des opérations élémentaires dans les meilleurs délais.

(b) Mise en œuvre de processus de gestion de poursuite d'activité avec des mesures préventifs et correctifs, afin de réduire l'impact des accidents qui peuvent arriver.

(c) Le plan de poursuite d'activité doit comprendre :

i. Identification des actifs impliqués dans les processus de métiers cruciaux ;

ii. Identification des risques et calculer la probabilité d'occurrence et impact ;

iii. Indentification du temps maximum d'arrêt toléré de services critiques ;

iv. Définition de solutions proposées pour le traitement d'incidents identifiés ;

v. Organisationnelles, techniques, financières,. . . ,etc, nécessaires pour reprise d'activités ;

vi. Evaluer et mettre à jour périodiquement les plans et les processus mis en place ;

vii. Identifier, sensibiliser et forger le personnel responsable de la mise en œuvre des plans de continuité.

Solutions aux incidents Un risque ne peut être entièrement éliminé, par conséquent la réponse aux incidents est critique[15].

(a) les phases de réponse aux incidents :

i. Préparation : qui inclue les préparations des installations et coordonnation de l'équipe, définir les outils nécessaires et savoir les utiliser et définir les procédures de prévention.

ii. Détection et analyse : qui définit l'axe de menace, analyse et implémente les outils pour log et corrélations d'erreurs.

iii. Confinement, éradication et récupération : quand un incident est détecté, il doit être contenu avant sa propagation. les stratégies de confinement doivent englober des étapes pour éliminer la menace, récupérer le système, les composants matériels et le temps productif.

iv. Activité post-incident : très importante étape, qui est la documentation de ce qui s'est passé et comment cela a été atténué pour prévenir des incidents futurs.

(b) Enquête de crimes informatiques : les enquêteurs doivent prouver trois choses pour poursuivre avec succès les crimes informatiques :

i. Motif : La raison du crime.

ii. Opportunité : Est-ce qu'ils étaient disponibles afin de commettre de crime.

iii. Significations : Est-ce qu'ils sont capables de commettre un crime.

(c) .Collecte des preuves : le système infecté doit être directement isolé. On va vider la mémoire sur le disque et on va créer de multiples copies principales sur disque dur, elles sont par la suite utilisées par des enquêteurs.

i. L'application de la loi et des responsabilités : La majorité des pays ont trois catégories essentielles de lois Criminel, qui comprend généralement des amandes ou emprisonnement ou les deux :

ii. Civil : Comprend la correction des torts qui ne sont pas des crimes tel qu'une entreprise qui à enfreint un brevet ;

iii. Administratif : Comprend les organismes chargés de faire appliquer les règlements.

(d) Ethique : Qui est une norme plus élevée que la loi et qui représente un ensemble de principes moraux gérant les comportements, ainsi les personnes ayant violé le code d'éthique peuvent perdre leur certification emploi.

Relance après catastrophe et la poursuite des activités C'est le procédé visant à retrouver l'accès aux donnes, matériels ,. . . ,etc, pour reprise d'activités commerciales suite à un incident. Le but d'un plan de reprise après evenement sinistre est de définir les objectifs pour récupération des hôtes de systèmes informatiques. Les conditions associées à la continuité des activités comprend :

(a) MTD (temps d'arrêts maximum tolérable) : Durée totale durant laquelle le propriétaire du système est prêt à accepter une panne ou perturbation.

(b) RTO (objectif temps de récupération) : La durée maximale dans laquelle une ressource peut rester indisponibles avant d'avoir un impact sur d'autres ressources système ;

(c) RPO (objectif de rétablissement) : Le moment avant une perturbation ou pannes du système, dans lequel les données se rapportent aux processus opérationnels peuvent être réstituer après une panne.

ANNEXE B

ÉTAT DE L'ART SUR LES DIFFÉRENTES ATTAQUES

B.1 Classification des attaques

Les attaques Les attaques de sécurité sont classées en tant qu'attaques passives et actives en utilisant à la fois dans X .800 et RFC 4949[12].

(a) **attaques passives** Les attaques passives sont de la nature d'écoute ou de surveillance des transmissions dans le but d'obtenir des informations qui sont transmises. Il existe donc deux types d'attaques passives qui sont la libération du contenu des messages et l'analyse du trafic. Les attaques passives sont très difficiles à détecter, car elles n'impliquent aucune Altération des données.

(b) **Attaques actives** Les attaques actives impliquent une certaine modification du flux de données, ou une création d'un faux flux et ces attaques peuvent être subdivisées en : intrusion et déni de service.

i. **Techniques d'intrusion** Peuvent être classées selon le niveau d'application :

— L'accès physique tel que sniffing.

— L'ingénierie social(physhing).

— L'interception des communications tel que session hijacking et spoofing.

— Les intrusions sur les réseaux.

A. **Le sniffing :** Les hackers utilisent des sniffer ou analyseur du réseau qui scannent tous les messages qui circulent sur le réseau, et recherchent ainsi des identités et des mots de passe comme Wiresharck et la commande tapdump sur Unix qui sont des logiciels de Sniffing[12].

   — Le craquage de mot de passe : Le hacker utilise un dictionnaire de mots de passe constitué à partir d'informations personnelles et privées, ces chaines de caractère sont essayées une à une à partir d'un logiciel. Ce type d'attaque s'appelle une attaque à force brute.

   Contre mesure Mettre des mots de passe assez complexes.

B. **Phishing :** Il s'agit de conduire les internautes à divulguer des informations confidentielles, notamment bancaire en employant un hameçon fait de mensonge et de contrefaçon électronique. Le Phishing utilise également des virus qui installent des programmes espions afin d'intercepter. La frappe des données confidentielles sur le clavier pour les transmettre en suite sur le site ou le phisher pourra les récupérer.

   Contre mesures L'emploi des souris lors de l'introduction des informations personnelles et des codes afin d'éviter cette attaque.

C. **Le spoofing :** Les attaques basiques de ces types est le falsification d'adresse IP (IP spoofing).

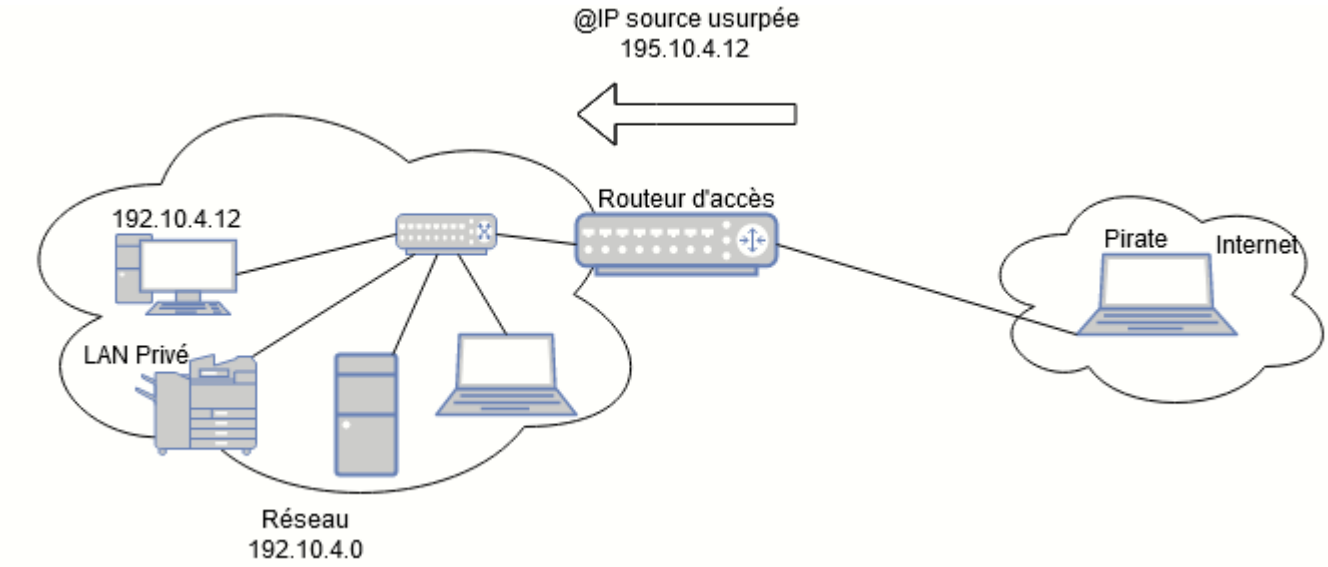

FIGURE B.1 – Exemple de IP spoofing[11].

— Le mail spoofing : Des mails contenant un virus informatique, sont envoyées depuis des adresses e-mail existantes, afin de mieux induire en erreur le destinataire.

contre-mesure Vérification des mails de provenance inconnue, faire attention aux pièces jointes.

— L'Address Resolution Protocol (ARP : Elle consiste à s'accorder l'adresse IP de la machine cible en correspondant son adresse IP à l'adresse MAC de la machine pirate dans les tables ARP de toutes les machines du réseau. En envoyant constamment des paquets du genre ARP replay contenant l'adresse IP cible ainsi que la fausse adresse MAC en diffusion(Broadcast), cette opération provoque le changement des tables dynamiques des machines du réseau. Ces derniers vont donc envoyer des trames Ethernet à la machine pirate et celle-ci va stocker le trafic et renvoyer les trames Ethernet à la véritable machine cible causant la compromission, le DoS (empoisonnement du cache),. . . ,etc.

contre-mesure Mise à jour régulière des logs.
L'emploi des tables ARP statiques seulement.
Le monitoring des paires IP/MAC à l'aide des logiciels spécialisés.

— Le DNS spoofing : Il cherche à rediriger les internautes vers des sites pirates en profitant des faiblesses du protocole DNS (Domain Name System) et/ou son implémentation dans des serveurs de nom de domaine. Les attaques DNS Spoofing peuvent être réparties en deux types : le DNS ID Spoofing et le DNS Cache Poisoning. Le principe de DNS ID Spoofing est que deux machines voudraient communiquer et l'une ne possède que le nom de l'autre machine d'où elle va employer le protocole DNS afin d'obtenir l'adresse IP de la deuxième machine à partir de son nom. La première machine va envoyer une requête DNS au serveur DNS, demandant la résolution du nom de la deuxième machine ainsi que son adresse IP. Un numéro d'identification est attribué à cette requête (un champ de l'entête du protocole DNS) afin d'identifier cette requête. Donc, le serveur DNS va répondre à cette requête avec le même numéro d'identification. Dans ce cas l'attaque se résume à récupérer ce numéro d'identification dans le but d'envoyer une fausse réponse avant le serveur DNS, et donc la première machine emploiera l'adresse IP du pirate et non celle de la deuxième machine. Concernant le DNS Cache Poisoning, les serveurs DNS qui ont un cache qui garde pendant un laps de temps les correspondances entre un nom de machine et son adresse IP des machines du domaine. Pour les autres machines, il contacte le serveur DNS auquel appartiennent les autres machines. Les réponses seront gardées dans le cache, et l'attaque consiste à altérer le cache avec de fausses informations[12].

La contre-mesure Mise à jour des serveurs DNS.
Configuration du serveur DNS de sorte qu'il ne résolve pas directement les noms des machines sauf celles du domaine sur

lequel il est autorisé.

Éviter les systèmes d'authentification par nom de domaine.

— sslstrip : Les messages chiffrés sont problématiques quand il s'agit de capturer le trafic. Le cryptage est destiné à être de bout en bout, ce qui veut dire qu'il n' y a pas de moyen d'intervenir au milieu. Tout mécanisme pour s'introduire au milieu défait les attentes de bout en bout de la plupart des schémas de chiffrement. Cela dit, il existe des moyens d'essayer de briser les protocoles chiffrés. Le programme Ssltrip a été développé afin de récupérer les messages SSL (Secure Socket Layer) et leur retirer le cryptage à l'époque où les SSL étaient toujours répondus, d'où les fortes chances que ça fonctionne. Aujourd'hui y a moins de chances de succès, car idéalement, les administrateurs système ont supprimé l'ancien cryptage des mécanismes tels que SSL et TLS (Transpot Layer Security) 1.0 et 1.1. Si un serveur supporte seulement TLS 1.2 et dessus, la bande SSL ne fonctionne pas, car les vulnérabilités qui lui permettaient de fonctionner ont été résolues. Sslstrip peut être utilisé en tant qu'un programme autonome, il agit essentiellement comme un proxy transparent entre un serveur et un client. Ou il peut charger les liens de https à http dans certains cas. Il utilise également d'autres techniques pour faire apparaitre que la connexion est chiffrée alors que ce n'est pas le cas. Tout comme avec le DNS Spoofing, Sslstrip nécessite la disposition d'un ARP Spoof en place. Le but est d'usurper la passerelle internet, ainsi que renifler les connexions distantes lors de définition de l'attaque Spoofing ARP. Sslstrip, est plug-in de Spoofing DNS a été activé. Ce qui nécessite un changement de configuration dans Ettercap avant d'activer le plug-in, Sslstrip doit savoir quelle commande de pare-feu est utilisée pour qu'il puisse configurer une redirection dans le pare-feu.

La contre-mesure Disposer d'un pare-feu au niveau du routeur d'accès va éliminer les paquets entrant avec une adresse IP source interne.

D. **Intrusion réseau :**

— Rouge acces point : C'est un faux point d'accès Wi-Fi considéré comme un point d'accès sans fil qui a été installé sur un réseau sécurisé sans autorisation par un attaquant malveillant, que ce soit un administrateur de réseau local, ou bien un employé malintentionné. Un faux point d'accès Wi-Fi est souvent appelé comme :

• Point d'accès non autorisé.

• Point d'accès Evil-Twin.

Contre mesure Implémentation de politique de sécurité en imposant aux employés de la respecter.

— Le portail captif : Le portail captif est une technique consistant à forcer les clients HTTP d'un réseau de consultation à afficher une page web spéciale (le plus souvent dans un but d'authentification) avant d'accéder à Internet normalement.

Contre mesure les administrateurs système doivent utiliser le Radius ou quelque chose de similaire au lieu du portail captif. Dans le cas où son utilisation est obligatoire, un utilisateur doit toujours vérifier s'il s'agit des https (presque aucun site Web https simulé sans certificat), ou il est souhaitable d'insérer un mauvais mot de passe en premier et si le résultat "mauvais mot de passe" est affiché, c'est qu'il peut lui faire confiance (cependant les pirates de proxy peuvent facilement vérifier les informations d'identification).

ii. **Le déni de services :** ou DoS est une attaque puissante qui cause le déni de service en submergeant une machine de trafic inutile, elle cible généralement les serveurs, les sous- réseaux.., etc. cette dernière est encore difficile à éviter.

A. **Inondations de demande de service :** Dans cette forme d'attaque DoS, un service tel qu'un serveur Web ou une application Web est inondé avec les demandes jusqu'à ce que toutes les ressources soient épuisées, ce qu'il est l'équivalent d'appeler quelqu'un plusieurs fois pour qu'il ne puisse répondre à d'autres appels en raison de son occupation. Lorsqu'un seul système attaque un autre, il est difficile de submerger la victime, mais cela peut être fait sur des cibles plus petites ou des environnements non préparés. Les inondations de demande de service sont généralement effectuées en configurant des connexions TCP répétées sur un système. Ces dernières consomment des ressources sur le système de la victime au point d'épuisement[11].

B. **SYN Flood :** Ce genre d'attaques exploite la poignée de main à trois avec l'intention de bloquer un système. Pour que cette attaque ait lieu, l'attaquant forgera des paquets SYN avec une fausse adresse source. Quand le système victime répond avec SYN-ACK, il va à cette fausse adresse et comme l'adresse n'existe pas, l'attaque oblige le système victime à attendre une réponse qui ne viendra pas. Cette période d'attente bloque donc une connexion au système, car le système ne recevra pas d'accusé de réception[12].

   Contre mesure Installer les anti-malwares ou les anti-virus. Il existe plusieurs méthodes pour parer cette attaque :
   - La limitation du nombre de connexions depuis la même source ou la même plage d'adresse IP.
   - La libération des connexions semi-ouvertes selon un choix de client et un délai aléatoire.
   - La réorganisation de la gestion des ressources allouées aux ressources tant que la connexion n'est pas complètement établie.

C. **ICMP Flood Attack :** Une demande ICMP nécessite que le serveur traite la demande et y réponde, consommant ainsi les ressources CPU, les attaques contre ICMP comportent les attaques

par rebond (Smurf attack), les inondations ICMP ainsi que les inondations Ping qui profitent tous de cette situation par inonder le serveur de requêtes ICMP sans attendre la réponse[13].

Contre mesure Tester la taille des paquets.
Tester les adresses sources et destinations.
Tester les nombres de SYN
Contrôler le flux.

D. **ping to death :** C'est un Ping paquet qui était plus grand que la limite autorisée de 64K, alors qu'il ne s'agissait pas de menace importante aujourd'hui à cause du blocage des Ping, des correctifs du système d'exploitation ainsi que la sensibilisation générale, à son apogée, le Ping de la mort était un exploit DoS facile à usage[16].

Contre mesure Mise à jour de l'OS et l'application des tests.

E. **Tearedrop (larme :** Une attaque en forme de larme se produit quand un attaquant envoie des paquets fragmentés personnalisés avec des valeurs offset qui se chevauchent pendant la tentative de reconstruction, ce qui rend la machine cible instable au moment de tentative de reconstruction des paquets fragmentés[16].

Contre mesure Mise à jour de l'OS.
Emploi d'un pare-feu afin de refuser les paquets qui se recouvrent.

F. **Attaque par réflexion (smurf) :** Elle usurpe l'adresse IP de la machine cible et envoie de multiples ICMP écho request packets aux adresses de diffusion des sites intermédiaires. Ces derniers amplifient le trafic ICMP vers l'IP source pour ainsi saturer le réseau segment de machine cible.

G. **fraggle :** C'est une variante d'une attaque smurf qui utilise UDP écho request au lieu de ICMP. Cette attaque utilise toujours un intermédiaire pour l'amplification. Plus généralement, une d'attaque fraggle cible Les requêtes (UDP écho request) vers le port

chargen (générateur de caractères) du système intermédiaire via une demande de diffusion, tel qu'une attaque smurf, l'attaquant usurpant l'adresse IP comme source, tout client qui reçoit l'écho au port chargent va générer un caractère à envoyer à la victime. Une fois reçue, la machine victime va renvoyer l'écho au port chargen de l'intermédiaire, ce qui va ainsi relancer le cycle.

H. **LAND :** Une attaque terrestre va envoyer du trafic vers la machine cible avec la source usurpée, tel que machine cible en elle-même(elles ont le flag SYN positioné, et les adresse source et destination du packet sont la même). la victime va essayer de reconnaitre la demande à plusieurs reprises indéfiniment.

Contre mesure configurer le firewall ou le routeur de sorte à filtrer les packets ayant la même adresse IP source et destination.

I. **Attaques DoS permanentes :** La plupart des attaques DoS, sont temporaires et elles doivent juste être arrêtées. Or, certains types d'attaques DoS détruisent un système et mettent hors ligne un système de façon permanente. le Phlashing, est une forme de DoS permanente qui consiste à pousser des bugs ou d'incorrectes mises à jour au micro logiciel d'un système victime. Quand c'est fait, le matériel devient inutilisable dans de multiples cas et doit être remplacé[13].

J. **Attaques au niveau de l'application :** Elles sont celles qui entrainent une perte ou dégradation d'un service au point qu'il en soit inutilisable, ces dernières peuvent même entrainer la corruption ainsi que la perte de données sur un système. Elles prennent généralement les formes suivantes :
   - Inondation (flood) qui submerge la cible de trafic afin de la rendre difficile ou impossible à répondre aux demandes légitimes.
   - Perturbation (distrup) qui implique d'attaquer un système avec l'intention de verrouiller ou de bloquer un ou plusieurs utilisateurs, comme tenter de se connecter plusieurs fois à un

système pour verrouiller le compte dans le but que l'utilisateur légitime ne puisse l'utiliser.

— Jam ou l'attaquant crée des requêtes SQL afin de verrouiller ou corrompre une base de données.

K. **Débordement de tampon (buffer overflow) :** C'est une technique DoS qui tire parti d'une faille dans le codage d'un programme en entrant plus de données que ce que la mémoire tampon ou l'espace mémoire du programme ne peut contenir. Quand le tampon d'un programme est en état de débordement, toutes autres entrées qui seront écrites dans le tampon peuvent avoir des conséquences négatives, comme des plantages, problèmes de sécurité...,etc[12].

Contre mesure Lors du développement : utilisation des librairies de développement spécialisées contre les buffers overflow (Libsafe d'Avayalabs),...,etc.

Emploi d'un langage n'autorisant pas ce genre d'attaques : Java,...,etc.

L. **DDOS :** Elles ont le même objectif que des méthodes DoS ordinaires ; Toutefois, la majeure différence réside dans la mise en œuvre de l'attaque. Une attaque DoS peut être lancée à partir d'un seul client malveillant, alors qu'une attaque DDoS emploie un groupe d'ordinateurs distribués nommé zombies contrôlés par maitre unique afin d'attaquer une seule cible[13].

Contre mesure

— Désactivation des services inutiles.

— Utilisation de protection antivirus.

— Activation d'étranglement du routeur (enable router throttling).

— L'utilisation d'un proxy inverse.

— Activation de filtrage d'entrée et de sortie.

— La dégradation des services.

— Défenses spécifiques du Botnet.

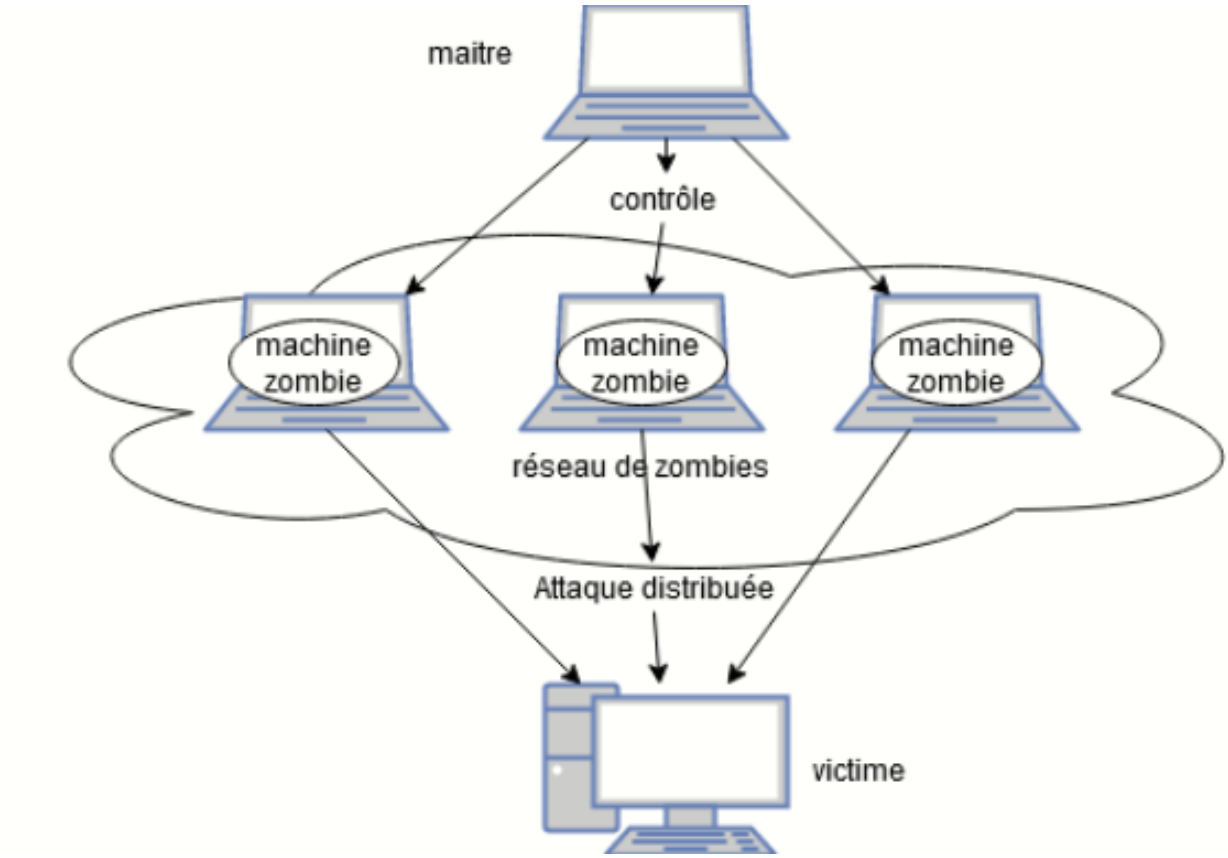

FIGURE B.2 – Le principe de DDOS.

B.2 Autres attaques :

— Vulnérabilité zero-day Une attaque ZETA (Zero Day Exploit Attack), cyberattaque ciblée, basée sur une vulnérabilité zero-day, survient le jour même où une faiblesse est détectée dans un logiciel. Ce point faible est exploité avant la mise à disposition d'un correctif par le créateur du logiciel[12].

— L'attaque +++ATHZero ;

— L'attaque Boink ;

— L'attaque Click – WinNewk ;

— Le Mail Bombing ;

— L'attaque Out Of Band (OOB) ;

— L'attaque NT Inetinfo ;

— L'attaque par requête HTTP incorrecte ;

— L'attaque SMTPd overflow ;

— L'attaque Bonk ;

— L'attaque BrKill ;

— L'attaque Coke ;

— Le FTP Bounce ;

— L'attaque NT Stop ;

— L'attaque Oshare ;

— Ping flooding ;

— L'attaque Pong ;

— Les attaques Smack – Bloop ;

— L'attaque sPing - Jolt – IceNewk ;

— Les trous de sécurité applicatifs ;

— L'attaque UDP 0 ;

— Les attaques WinArp – Poink ;

— L'attaque WINS 53 flood ;

— L'attaque WINS 137 flood ;

— Le Cross Site Scripting ;

— Dictionary Cracking ;

— Brute Force Cracking.

Attaques	Confidentialité	disponibilité	Intégrité
Le snifing	oui		
Le craquage de mot de passe	oui	oui	oui
Phishing	oui	oui	oui
Le spoofing		oui	oui
L'Address Resolution Protocol (ARP)	oui	oui	oui
Le DNS spoofing	oui	oui	oui
sslstrip	oui		oui
Rouge acces point	oui	oui	oui
Le portail captif	oui		
SYN Flood		oui	
ICMP Flood Attack		oui	
ping to death		oui	
Tearedrop		oui	
Attaque par réflexion (smurf)		oui	
fraggle		oui	
LAND		oui	
Attaques DoS		oui	oui
attaques au niveau de l'application		oui	oui
débordement de tampont (buffer overflow)	oui	oui	oui
DDOS	oui	oui	oui

TABLE B.1 – les attaques en fonction des piliers de la sécurité.

ANNEXE C

QUESTIONNAIRE

Périmètre - Internet

— Le réseau informatique dispose-t-il d'un équipement capable de filtrer les URL visitées (proxy ou firewall) ? oui, il dispose d'un proxy et d'un firewall qui filtrent tous les paquets sortant et entrant.

— L'équipement de filtrage est-il capable de faire de la détection applicative ? oui.

— Le réseau dispose-t-il d'un équipement capable de faire de la détection antimalware ? oui.

— Le réseau dispose-t-il d'un équipement capable de faire de la détection contre les intrusions ? oui.

— Est-ce que l'entreprise dispose d'un réseau de caméras de surveillance ? oui.

Périmètre - DMZ

— Une zone cloisonnée appelée DMZ est-elle en place pour isoler les serveurs publiés sur internet du LAN ? oui.

— Les ports ouverts sur internet sont-ils identifiés, limités et nécessaires ? oui.

Réseau LAN

— Votre entreprise dispose-t-elle d'au moins un ordinateur ? oui.

— Votre réseau local couvre-t-il toute l'entreprise ? oui.

— Votre entreprise utilise-t-elle un réseau local d'entreprise de type LAN : réseau filaire connectant les ordinateurs entre eux ? oui.

— Technologie d'interconnexion LAN.

Nom de la technologie	Norme	Type du support	Débit
Ethernet	1000Base-T	Paires torsadées	1000Mbs

— Equipements d'interconnexion

Nom de l'équipement	Modèle
Routeur	CISCO 2801
Switch	Cisco 3750
Switch	Cisco 2960
Switch	D-Link

— Câblage

  — La fibre optique.

  — des connecteur RJ45.

— Equipements terminaux.

Nom de l'équipement	Modèle
Serveur	HP DL380 G7
Serveur	DELL PowerEdge R520.
oridinateurs	HP/DELL
Ordinateurs portables	HP/DELL

— Votre entreprise utilise-t-elle un réseau local d'entreprise de type WLAN/ Wireless LAN : réseau sans fil ? Donnez les technologies sans fil utilisées ? Oui , ISO/CEI 8802-11 « wifi ».

— Les services qui nécessitent l'utilisation de LAN ? Tout les services d'après la disposition des anneaux Réseau .

Authentification

— Les utilisateurs arrivent-ils facilement à retenir leurs mots de passe sans l'écrire et à accéder aux différents services ? oui.

— Les authentifications sont-elles centralisées ? oui.

— Les utilisateurs qui ont la nécessité d'avoir beaucoup d'identifiants différents (services externes non maitrisés par la DSI) ont-ils un gestionnaire de

mot de passe robuste ? ils n'utilisent qu'un seul identifiant qui est leur matricule ou le nom associer à l'initiale de leur prénom.

— Les services critiques et les accès externes disposent-ils d'une authentification forte ? oui.

— Les anciens utilisateurs sont-ils désactivés ? oui.

Mises à jour

— Y a-t-il une stratégie de mise à jour des systèmes d'exploitation (clients et serveurs) ?oui, WSUS(Windows Server Update Services).

— Tous les logiciels d'un système sont-ils maîtrisés ? oui.

— Y a-t-il une stratégie de mise à jour des logiciels ? non.

— Les logiciels ne pouvant pas être mis à jour et comportant des vulnérabilités sont-ils connus et y a-t-il une stratégie de minimisation du risque ? non.

Antivirus et plus

— Les postes de travail et les serveurs sont-ils protégés contre les codes malveillants connus ? oui,kaspersky.

Chiffrement

— Les accès distants sont-ils chiffrés ? oui.

— Les accès métiers de l'entreprise sont-ils chiffrés ? oui.

Sauvegarde

— Les données les plus importantes sont-elles biens incluses dans les jeux de sauvegarde ?oui

— La sauvegarde est-elle supervisée ?oui.

— La sauvegarde fonctionne-t-elle ? Arrive-t-on à restaurer les différents types de données ?oui.

— La sauvegarde est-elle externalisée ? non.

Politique de sécurité informatique

— Disposez-vous d'une politique de sécurité ?oui.

— Couvre-t-elle tous les sujets importants ?oui.

— Est-elle applicable en condition réelle ?oui.

— Les personnes concernées sont-elles informées de son existence ?oui.

Sensibilisation

— Les utilisateurs sont-ils sensibilisés au risque informatique (phishing, malware, vol de données, etc.) ?oui.

— Des actions de sensibilisation et des rappels réguliers sont-ils effectués ?non.

— Les nouveaux arrivants sont-ils informés du risque ? oui.

Abstract

No matter what security measures are implemented. As soon as they are opened up to the Internet, networks become increasingly vulnerable and exposed to multiple attacks, in fact the need to implement security measures to avoid multiple attacks and guarantee the protection and integrity of information. Our work consists in fact on setting up a roadmap taking into account the various weaknesses and vulnerabilities that can be exploited by an attacker and secure and protect the network. Also, this work consists of listing the various attacks that can harm the network as well as the countermeasures in order to protect the system against them. In addition, simulating an attack on the enterprise architecture to test the set up policies and mechanisms put in place.

Key words : SPA Général Emballage, attack , integrety.. . .

Résumé

Peu importe les moyens de sécurité mis en œuvre. Dès l'ouverture vers l'extérieur, les réseaux deviennent de plus en plus vulnérables et exposés aux multiples attaques d'où l'indispensabilité de mise en place des places des mesures de sécurité par l'entreprise afin d'éviter les multiples attaques et garantir la protection et l'intégrité des informations. Notre travail consiste à mettre en place une feuille de route prenant en compte les différentes faiblesses et vulnérabilités qui peuvent être exploité par un attaquant et donc mieux sécuriser et protéger le réseau de l'entreprise SPA Général Emballage. Ce travail consiste aussi à énumérer les diverses attaques qui peuvent nuire au réseau ainsi que les contre-mesures pour se prémunir contre ces dernières. En outre, simuler une attaque sur l'architecture de l'entreprise dans le but de tester l'efficacité des politiques et mécanismes mis en place.

Mots clés : SPA Général Emballage, attaques, intégrité, sécurité, référentiel. . . .