République Algérienne Démocratique et Populaire
Ministère de l'Enseignement supérieur et de laRecherche Scientifique
Université ABDERRAHMANE MIRA - BEJAIA -

Faculté science exacte
Département Informatique

Mémoire pour l'obtention du diplôme de master en informatique
Option : Administration et Sécurité des réseaux

AUDIT DE SÉCURITÉ D'UN SYSTÈME D'INFORMATION

ET référentiel de sécurité informatique

Élaboré par :
- SAIDANE Amirali
- OUAZENE Bilal

Encadré par :
- MOKTFI Mohend
- KHOULALENE Nadjette

Devant le jury :
- BOUKERRAM Samira
- HOUHA Amel

2021-2022

Remerciment

Je remercie ALLAH qui m'a donné la santé et la force pour réaliser ce memoire ainsi que mon promoteur M*r* Moktefi Mohand et ma promotrice MM*e* Khoulalene Nadjette
pour avoir accepté de m'encadrer, et me suivi durant toute l'année en assurant le suivi scientifique et technique du présent mémoire. Je le remercie pour sa grande contribution à l'aboutissement de ce travail, et pour s'être montré disponible.
Mes remerciements vont aussi aux membre du jury pour l'honneur qu'ils me fait en acceptant de juger ce modeste travail.
je remercie tous qui ont participé de près ou de loin à l'élaboration de ce travail.

Dédicace

Je dédie ce mémoire
À Yemma qui m'a soutenu et encouragé durant ces années d'études.
Qu'elle trouve ici le témoignage de ma profonde reconnaissance.
À mes frères, mes grands parents et Ceux qui ont partagé avec moi tous les moments d'émotion lors de la réalisation de ce travail. Ils m'ont chaleureusement supporté et encouragé tout au long de mon parcours.
À ma famille, mon père, mes proches et à ceux qui me donnent de l'amour et de la vivacité.
À tous mes amis qui m'ont toujours encouragé.

Table des matières

Chapitre II Audit de sécurité d'un système d'information

Chapitre III Méthodes et normes d'audit (référentiels)

Table des figures

Liste des tableaux

Acronymes

AESC : American Engineering Standards Committee

AFNOR : Association Française de Normalisation

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information

APT : Advanced Persistent Threat

ARP : Address Resolution Protocol

ASA : American Standards Association

BGP : Border Gateway Protocol

BSI : British Standards Institute

CEI : Commission Electronique Internationale

CEN : Comité Européen de Normalisation

CFISE : Catalogue des Fonctions des Informations de Sécurité d'Etat

CLUSIF : Club de la Sécurité de l'Information Français

CSD : Conseil Supérieur de Défense

CVSS : Common Vulnerability Scoring System

EBIOS : Etude des Besoins et Identification des Objectifs de Sécurité

ENISA : European Network and Information Security Agency

FTP : File Transfer Protocol

HTML : Hypertext Markup Language

HTTP : Hypertext Transfer Protocol

ICMP : Internet Control Message Protocol

IEEE802.1 : Standard IEEE qui définit le support des VLAN sur un réseau Ethernet

IP : Internet Protocol

ISL : Intrusion Specification Language

ISO : Organisation Internationale de Normalisation

JTC : Joint Technical Committee

LCEN : Limerick Community Education Network

MAC : Media Access Control

MARION : Méthode d'Analyse de Risques Informatiques Optimisée par Niveau

MEHARI : Méthode Harmonisée d'Analyse des Risques

MELISA : Méthode d'Evaluation de la Vulnérabilité Résiduelle des Systèmes d'Armement

NIST : National Institute of Standards and Technology

OCTAVE : Operationally Critical Threat, Asset, and Vulnerability Evaluation

OSPF : Open Shortest Path First

DICP : Disponibilité, Intégrité, Confidentialité, Preuve

PDCA : Plan, Do, Check, Act

PME : Petites et Moyennes Entreprises

POE : Plans Opérationnels Entreprise

POS : Plans Opérationnels de Sécurité

PSS : Plans Stratégique de Sécurité

SAS : Statistical Analysis System

SoA : Statement of Applicability

SMI : Système de Management de l'Information

SMSI : Système de Management de la Sécurité de l'Information

SMTP : Simple Mail Transfer Protocol

RTT : Round Trip Time

TCP : Transmission Control Protocol

TI : Technologies de l'Information

TIC : Technologies de l'Information et de la Communication

TTL : Time To Live

VLAN : Virtual Local Area Network

WAN : Wide Area Network

Introduction générale

À l'heure du « tout est disponible partout tout de suite », le transport de données en dehors du domicile d'un particulier ou d'une entreprise est une réalité qui mérite que l'on s'intègre sur la sécurité des transmissions pour ne pas compromettre un système d'information.

Que ce soit à l'échelle d'une entreprise, d'une multinationale ou à plus petite échelle, la sécurité d'un système d'information prends plus au moins d'importance selon la valeur que l'on confère à ces données.

Avec le développement de l'internet, chacun a accès au réseau où de plus en plus d'information circulant. De plus en plus, les entreprises communiquent et diffusent via ce media, que se soit dans leurs liens avec leurs fournisseur ou leurs partenaires ou en interne, dans les relation entre les employés eux-même.

Problèmatique

Nous somme face non seulement à une augmentation de la qualité, mais aussi et surtout de l'importance des données. L'ensemble formé par tout le réseau d'utilisateurs de ce systèmes d'information se doit d'être connu pour être sûr. Les ressources qui y circulent doivent absolument être protégés et pour cela, la maîtrise du système d'information est indispensable. Chaque acteur du système a un rôle à respecter qui doit être définit scrupuleusement.

Objectifs

Ce mémoire couvre toutes les étapes nécessaires à la sécurisation d'un système d'information de l'entreprise. Ces étapes décrivent une démarche générique permettant d'appréhender et de construire une politique de sécurité du système d'information mais aussi de choisir des solutions techniques adaptées à ses besoins de sécurité. Elles permettent également de mettre en place des contrôles de sécurité à la fois pour vérifier que la politique de sécurité est appliquée.

Organisation du mémoire

Ce mémoire est organisé en 6 chapitre :

① **Chapitre I :**
Il présente quelque définitions ainsi que les principes de base de la sécurité de l'information, définit la politique de sécurité, ces objectifs et les outils associés.

② **Chapitre II :**
Il parle sur l'audit de sécurisé, son rôle, son objectif et détail la démarche de réalisation d'un audit de sécurité du système d'information.

③ **Chapitre III :**
Puisque un audit de sécurité informatique se référe à des référentiels et normes spécifiques, ce chapitre touche un peu à leurs histoires et décrit brièvement la série d'*ISO 27k [27000-27007]* qui sont des standards d'un Système de management de la sécurité de l'informarion dit *SMSI*. Il détaille la norme ISO 27001 et la méthode MEHARI afin de pouvoir élaborer une politique de sécurité plus claire.

④ **Chapitre IV :**
Il évoque nos ennemis et la manière dont ils procédaient. Nous présentons également dans ce chapitre quelques attaques les plus fréquemment utilisées qui peuvent affecter un réseau informatique.

④ **Chapitre V :**
Il s'agit de la partie pratique dont un test d'intrusion est appliqué à une infrastructure réseau d'une entreprise quelconque.
Et pour avoir une vision complète d'un test d'intrusion orienté Infrastructure, on a utilisé un *Framework pentest* qui permet de renseigner les vulnérabilités identifiées et exploitées durant le test d'intrusion et d'en sortir un score d'impact technique et métier.

Le volet théorique

ChapitreI

La sécurité informatique

I.1 Introduction

Ce chapitre présente quelques définitions et principes de base de la sécurité de l'information. Il définit également la politique de sécurité et ses objectifs, ainsi que les outils liés à la bonne exécution de cette politique.

I.2 Définition d'un système

Un système est un ensemble d'éléments en relation les uns les autres en formant un tout. Il représente une unité parfaitement identifiable et évoluant dans un environnement. Il existe donc une limite qui partage le système de son environnement.

I.3 Définition d'un système d'information

Un système d'information noté (SI) définit l'ensemble des données et des ressources matérielles et logicielles de l'entreprise. Ce système permet de stocker et de faire circuler les ressources qu'il contient. Il représente également le réseau d'acteurs qui interviennent dans celui-ci, qui échange les données, y accèdent et les utilisent.

Ce système représente la valeur de l'entreprise, il est essentiel de le protéger. Le compromettre revient à compromettre l'entreprise. Il convient donc d'assurer sa sécurité en permanence, et surtout dans des conditions d'attaque, d'espionnage ou de défaillance.

Le SI se construit tout autour des processus des « métiers » et ces interactions, pas seulement autour des bases de données ou de logiciels informatiques qui le constitue. Le SI doit être en accord avec la stratégie de l'entreprise.

I.4 L'intérêt de la sécurité

Parce que on estime si la perte des informations, va à l'encontre :

- ✦ une perte financière (exemple : destruction du fichier client, récupération d'un contrat avec un concurrent).
- ✦ Une perte de l'image de marque (exemple : piratage d'une banque, divulgation d'un numéro de téléphone sur liste rouge).
- ✦ Une perte d'efficacité ou de production (exemple : rendre indispensable un serveur de fichier sur le quel travaillent les collaborateurs).

I.5 Nécessité de sécuriser un système d'information

Certains facteurs peuvent apparaître de l'ordre de l'évidence comme la nécessité de protéger le patrimoine opérationnel de l'entreprise. Toutefois, l'ensemble des menaces n'est pourtant pas toujours identifié. Par contre, d'autres sont souvent méconnues comme les obligations et responsabilités légales des dirigeants d'entreprise dans l'exploitation et la

maîtrise de leur système d'information. Ces exigences impliquent la mise en place d'une protection des systèmes sous la forme d'une politique de sécurité avec :[1]

- ✦ L'élaboration de règles et procédure.
- ✦ La définition des actions à entreprendre et des personnes responsables.
- ✦ La détermination du périmètre concerné.

Ce périmètre comprend à la fois les données aussi bien sous forme électronique que papier (fichier, message...), les transactions, les applications logiciels et base de données. Il ne faut pas oublier l'aspect continuité des services de traitement de l'information et les plans reprisent d'activités après sinistre.

I.6 Les principes de base, objectifs principaux et la mise en œuvre

La sécurité des données couvre quatre objectifs principaux, et est représentés sous la forme d'acronymes DICP (Disponibilité, Intégrité, Confidentialité et Preuve) : [1]

① **La disponibilité :** est l'assurance que les personnes autorisées ont accès à l'information quand elles le demandent ou dans les temps requis pour son traitement.

② **L'intégrité :** est la certitude de la présence non modifiée ou non altérée d'une information et de la complétude des processus de traitement. Pour les messages échangés, il concerne la protection contre l'altération accidentelle ou volontaire d'un message transmis.

③ **La confidentialité :** est l'assurance que l'information n'est accessible qu'aux personnes autorisées, qu'elle ne sera pas divulguée en dehors d'un environnement spécifié, elle traite de la protection contre la consultation de données stockées ou échangées. Ceci est réalisable par un mécanisme de chiffrement pour le transfert ou le stockage des données.

④ **La preuve :** consiste à garantir que l'émetteur d'une information soit bien identifié et qu'il a les droits d'accès logiques, que le récepteur identifié est bien autorisé à accéder à l'information.

D'autre principe de sécurité peuvent être établis, il s'agit de :

- ✦ La non-répudiation : considérée comme le cinquième principe, il a été introduit dans la norme ISO 7498-2 comme un service de sécurité pouvant être rendu par un mécanisme comme le signature numérique, l'intégrité des données ou la notarisation. L'élément de la preuve de non-dénonciation doit permettre l'identification de celui qu'il représente, il doit être positionné dans le temps (horodatage) et il doit présenter l'état du contexte dont lequel il a été élaboré (certificats).

- ✦ L'authentification : est le moyen qui permet d'établir et valider la requête émise pour accéder à un système. L'authenticité est la combinaison d'une authentification et de l'intégrité.
- ✦ Le mécanisme de chiffrement : procède du principe que l'émetteur et le récepteur convient d'un mot de passe connu d'eux seuls. L'émetteur utilise ce mot de passe comme clé de chiffrement pour le message à transmettre, seul le récepteur connais ce mot de passe pour l'utiliser comme clé pour déchiffrer le message et y accéder.

Les objectifs de base peuvent être traités sous la forme de solution de sécurité à l'aide de matériels, de logiciels, de procédures, de support opérationnel pour :

- ✦ L'intégrité de données et la confidentialité : gestion des accès physiques et logiques, sécurisé le réseau.
- ✦ La disponibilité : redondance des systèmes, associées aux bonnes pratiques à mettre, de l'alimentation électrique, sauvegarde et archivage des données.

I.7 La politique de sécurité

La politique de sécurité a pour objectif de définir la protection des systèmes d'information de l'entreprise. Elle comprend un ensemble de bases définissant une stratégie des directives, des procédure, des codes de conduite, des règles organisationnelles et techniques. Elle implique une mise en œuvre d'une sécurité adaptée aux usages, économiquement viable et conforme à la législation.

Cette politique doit être formalisée dans l'entreprise sous forme d'un document. Il peut représenter le sommaire des pratiques qui régissent la manière de gérer, de protéger et de transmettre des informations critiques ou sensibles appartenant à l'organisation. La documentation sur la norme ISO 27001 aide à la réalisation de ce référentiel.

Il est recommandé d'inclure les thème sur :

- ✦ L'organisation et les structure de l'entreprise impliquées dans la gestion de sécurité.
- ✦ Les éléments fondateurs d'une culture de sécurité.
- ✦ Le maintien de la cohérence dans les solution techniques mise en œuvre.
- ✦ Les moyens prévus pour la mise en œuvre et les méthodes de pilotage.

Représentation du positionnement respectif de chaque document, comme illustrer à la Figure I.1[3]

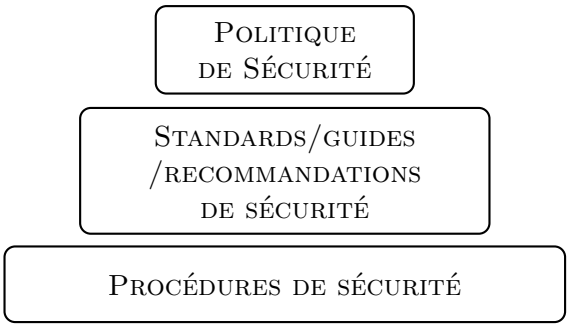


Figure I.1 – Pyramidale des politiques de sécurité

La politique est l'expression des besoins. La procédure, ou recommandation technique, est l'implémentation du besoin. À titre d'exemple, lorsque certains produits pare-feu présentent les règles de filtrage comme une politique de sécurité, c'est le concepts même de politique de sécurité qui est employé.[2]

L'objectif de la sécurité informatique est de protéger ou de sauvegarder la pérennité du patrimoine informationnel de l'entreprise. C'est pour cela que la politique de sécurité mise en œuvre doit s'inspirer des besoins réels qui ont été définis à partir des évaluation des actifs, des menaces et des vulnérabilités. Elle impose une complémentarité entre les procédures, les outils mis en œuvre et les personnes impliquées.

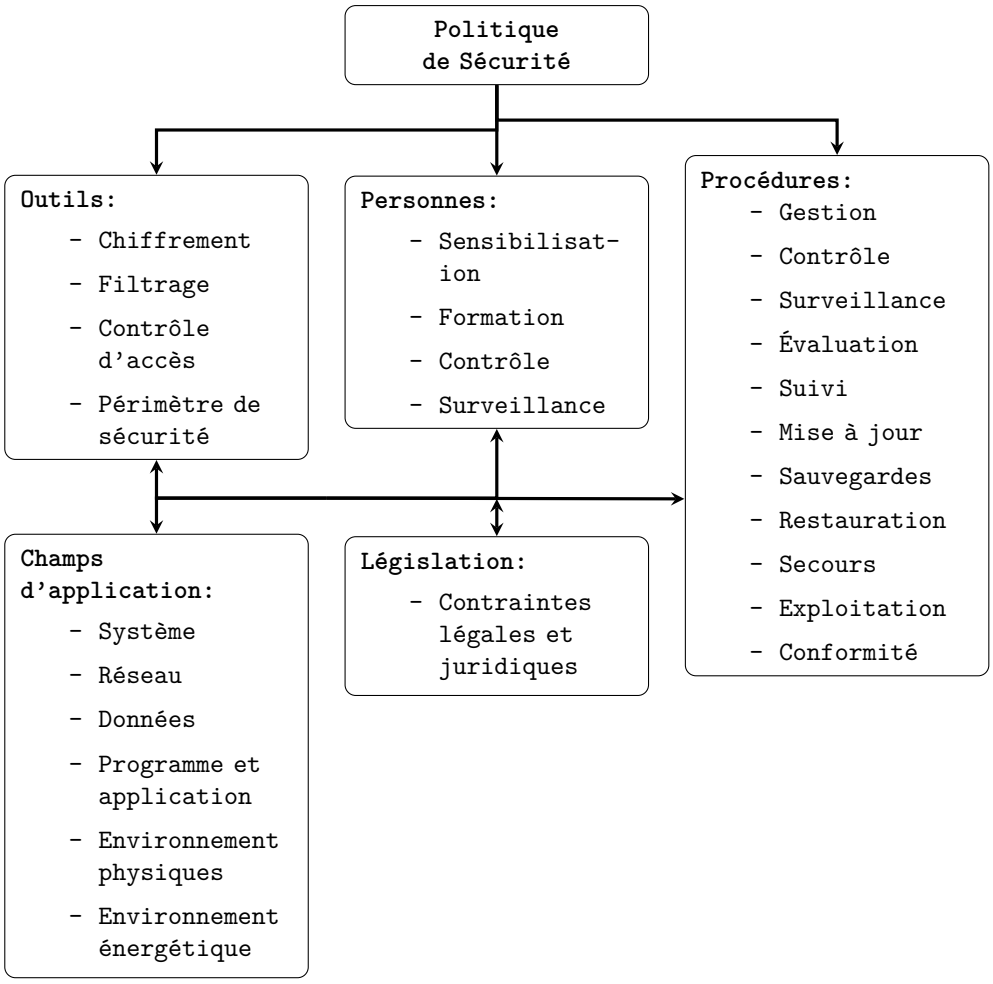


FIGURE I.2 – Stratégie et politique de sécurité

I.7.1 Les principes de la sécurité informatique

Le rôle principale de la sécurité informatique est scindé en trois démarches principales : [1]

- ✦ Définir le périmètre de la vulnérabilité lié à l'usage des technologies de l'information et de communication.
- ✦ Offrir un niveau de protection adapté aux risques encourues par l'entreprise.
- ✦ Mettre en œuvre et valider l'organisation, les mesures, les outils et les procédures de sécurité.

La première étape consiste à connaître le périmètre lié à la sécurité, c'est-à-dire la zone qui correspond aux services (authentification, contrôle d'accès physique et logique, disponibilité, intégrité et confidentialité) utilisés sur le réseau d'entreprise (post client, réseaux LAN et WAN), sur les serveurs, avec les points d'accès externes (serveurs distant, accès VPN...). Le réseau d'entreprise s'étend maintenant aux terminaux mobiles et au cloud computing.

À chaque sous ensemble de périmètre correspond un niveau de sécurité différent selon les menaces possibles et en fonction de la valeur des informations à protéger.

Les principes de base de cette sécurité impose de :

- ✦ Définir et implémenter une stratégie de sécurité adaptée au contexte ou au métier de l'entreprise.
- ✦ Appliquer les dernières mises à jour et corrections pour les systèmes d'exploitation (serveurs, postes de travail, terminaux mobiles), les logiciels applicatifs, principalement pour ceux qui sont établis en protection (antivirus...).
- ✦ Utiliser les recommandations des éditeurs en ce qui concerne la gestion des mots de passe des comptes privilégiés.

Pour bâtir une politique de sécurité adaptée au métier de l'entreprise, il est nécessaire de préparer les étapes suivantes :

- ✦ Identifier les actifs à protéger :
  - — Matériel, logiciels...
  - — Les données sensible de l'entreprise.
  - — Les service et les applications : application métier internes et externes pouvant communiquer avec le monde extérieur (fournisseurs, clients, site de commerce électronique) ou en interne.

- ✦ Découvrir les réseaux de communication. Cela consiste à découvrir les interactions entre les différents matériels et logiciels, identifier les applications et services communiquant avec l'extérieur.

I.7.2 L'élaboration du document (Politique de sécurité)

Après avoir évalué les besoins globaux en sécurité, le document présentant la politique peut être conçu selon le bon sens pratique. Une façon simple est d'utiliser une approche hiérarchique pour définir le périmètre globale, en suite de le décomposer en différents composants.[1]

La politique de sécurité doit être rigoureuse, mais doit rester flexible. Elle peut tenter de répondre au première questions suivantes :

- ✦ Quel est le niveau de criticité ou d'importance des données de l'entreprise ?
- ✦ Quels sont les objectifs principaux et le périmètre ?
- ✦ Quels systèmes d'information sont à protéger ?
- ✦ Quels sont les mesures minimales à définir pour leurs protections ?
- ✦ Quels sont les personnes responsable de la sécurité des données (accès logique, privilèges d'administration...) et les ressources matérielles et logicielles mises à disposition ?

- ✦ Quels sont les droit et devoir des utilisateurs ou des administrateurs ?

Cette politique peut se matérialiser sous la forme d'un document officiel. Il représente les règles qui peuvent être rédigées sous forme d'instruction à adopter pour une meilleur prise en compte de la sécurité de l'information dans l'organisation.

Ces règles ont pour objectif :

① De protéger le système d'information et ces données.

② D'être conforme avec la réglementation au regard du traitement de l'information.

I.7.3 Les outils associés à la politique de sécurité

Tout projet de mise en place de la politique de sécurité dans l'entreprise requiert une documentation adaptée sous forme de guides de bonne pratique et de procédure.Les documents présentant les normes peuvent être acquis, les guides et procédure doivent être rédigées par les personnes en charge de la sécurité des systèmes et de l'exploitation des systèmes de l'information.

Les procédures consistent à décrire les étapes détaillées qui doivent être suivies par les utilisateurs, les responsables systèmes et toutes les personnes qui doivent accomplir une tâche particulière liée à la protection du patrimoine informationnel.

Chaque document doit être rédigé en terme claire et adapté selon le personnel concerné et sa fonction dans l'entreprise.

L'objectif final des documents est d'assister les utilisateurs, les responsables systèmes et toutes les personnes impliquées dans la gestion des systèmes d'information dans l'optique de la politique de sécurité définie.

I.8 Conclusion

La sécurité informatique est de faire tout pour protéger et assurer la pérennité du patrimoine informationnel de l'entreprise. C'est-à-dire de préserver la disponibilité, l'intégrité, la confidentialité et la traçabilité.

ChapitreII

Audit de sécurité d'un système d'information

II.1 Introduction

Ce chapitre traite de la compréhension théorique du concept d'audit et se familiarise avec son approche méthodologique. À cet effet, il revient sur le concept de test. Il visualise tous les contours sémantiques possibles des concepts liés au fonctionnement du SI, à sa finalité, à ses méthodes et outils, et définit tous les autres aspects qu'il met en avant lors de l'évaluation des systèmes d'informationS et de communication.

II.2 Définition d'un audit

En informatique, le terme « Audit (Une écoute) » est apparu dans les années 70 et a été utilisé de manière relativement aléatoire. Nous considérons par la suit un audit de sécurité du système d'information comme une mission d'évaluation de conformité par rapport à une politique de sécurité ou à défaut par rapport à un ensemble de règles de sécurité.[4]

Une mission d'audit ne peut être réalisée que si l'on définit auparavant un référentiel, c'est-à-dire en l'occurrence, un ensemble de règles organisationnelles ; procédurales ou/et techniques de référence. Ce référentiel permet au cours de l'audit d'évaluer le niveau de sécurité réel du « terrain » par rapport à une cible.

Pour évaluer le niveau de conformité, ce référenciel doit être :

- **Complet (mesurer l'ensemble des caractéristiques) :** il ne doit pas s'arrêter au niveau système, réseau, télécoms ou applicatif, de manière exclusive, de même, il doit couvrir les points techniques et organisationnels.
- **Homogène :** chaque caractéristique mesurée doit présenter un poids cohérent avec le tout.
- **Pragmatique :** c'est-à-dire aisé à quantifier (qualifier) et à contrôler. Ce dernier point est souvent négligé.

La mission d'audit consiste à mesurer le niveau d'application de ces règles sur le système d'information par rapport aux règles qui devraient être effectivement appliquées selon les processus édictés. L'audit est avant tout un constat.

II.3 Rôle et objectif de l'audit

Une mission d'audit vise différents objectifs. En effet nous pouvons énumérer à ce titre :[4]

- La détermination des déviations par rapport aux bonnes pratiques de sécurité.
- La proposition d'action visant l'amélioration du niveau de sécurité du système d'information.

Également, une mission d'audit de sécurité d'un système d'information se présente comme un moyen d'évaluation de la conformité par rapport à une politique de sécurité ou par rapport à un ensemble de règles de sécurité.

II.4 Cycle de vie d'un audit de sécurité des systèmes d'information

Le processus d'audit de sécurité est un processus répétitif et perpétuel. Il décrit un cycle de vie qui est schématisé à l'aide de la figure suivante :[5]

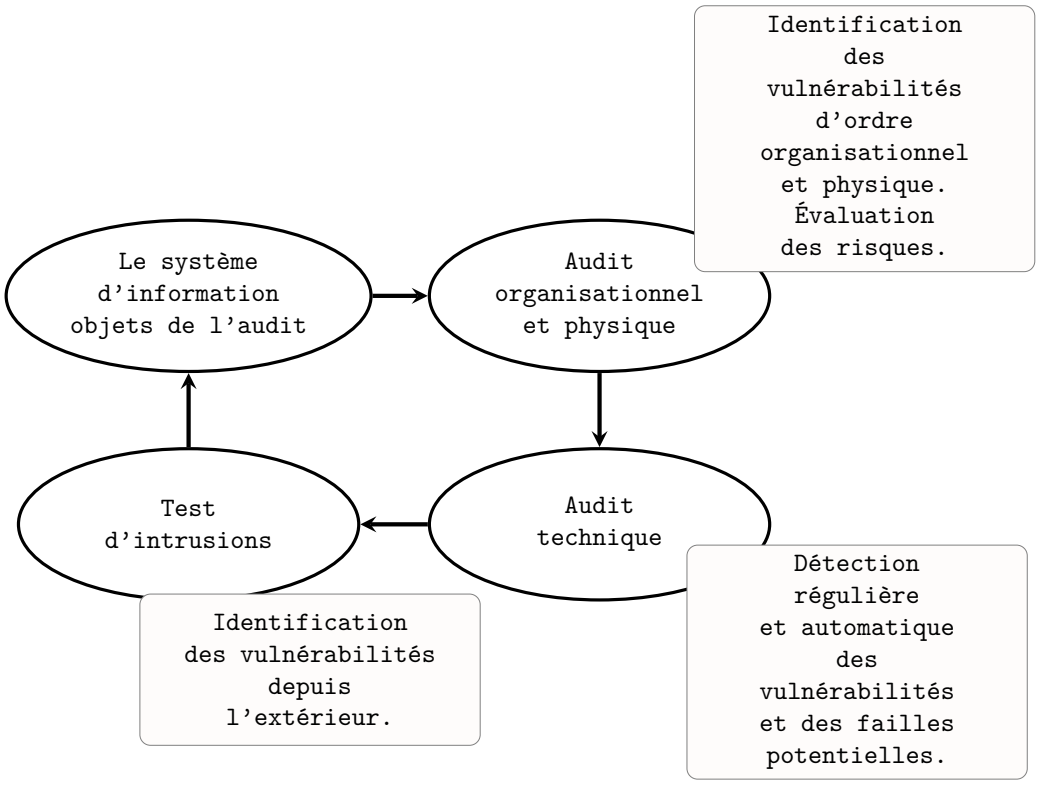


FIGURE II.1 – Le cycle de vie d'audit de sécurité

L'audit de sécurité informatique se présente essentiellement suivant deux parties comme le présente le précédent schéma :

- ✦ L'audit organisationnel et physique.
- ✦ L'audit technique.

Une troisième partie optionnelle peut-être également considérée. Il s'agit de l'audit intrusif (test d'intrusion). Enfin un rapport d'audit est établie à l'issue de ces étapes.

Ce rapport présente une synthèse de l'audit. Il présente également les recommandations à mettre en place pour corriger les défaillances organisationnelles ou techniques constatées.

II.5 Démarche de réalisation de l'audit de sécurité de système d'information

Dans la section précédente Nous avons évoqué les principale étapes de l'audit de sécurité des systèmes d'information. Cependant il existe une phase aussi importante qui est une phase de préparation.

Nous pouvons schématiser l'ensemble du processus d'audit comme suite :[2]

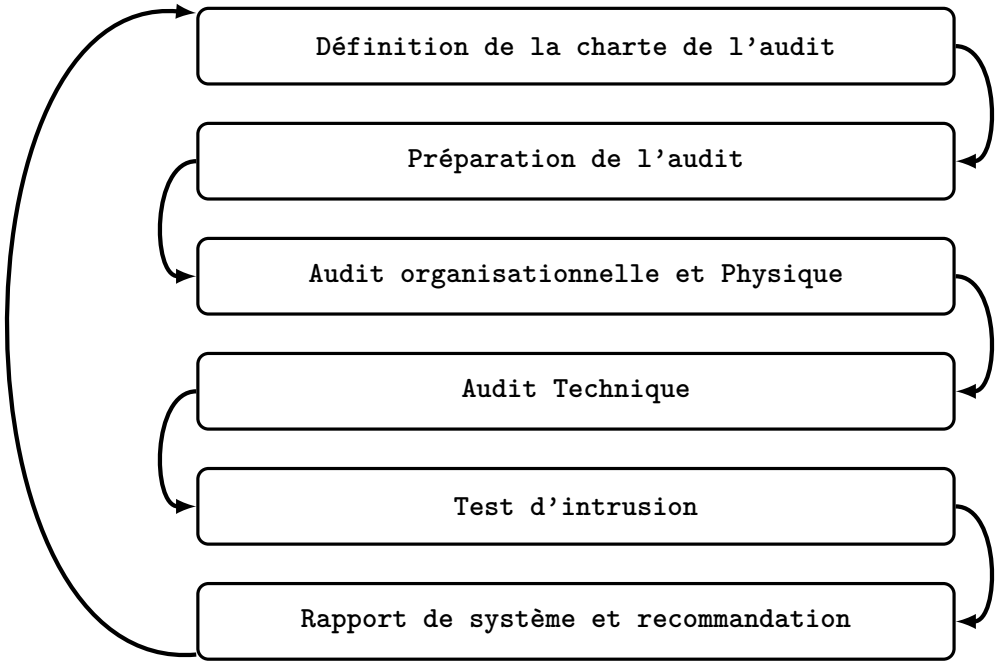


FIGURE II.2 – Schéma du processus d'audit

II.5.1 Définition de la charte d'audit

Avant de procéder à une mission audit, une charte d'audit doit être réalisée, elle a pour objet de définir la fonction de l'audit, les limites et modalités de son intervention, ses responsabilités ainsi que les principes régissant les relations entre les auditeurs et les audités. Elle fixe également les qualités professionnelles et morales requises des auditeurs.

II.5.2 Préparation de l'audit

Cette phase est aussi appelée phase de pré-audit. Elle constitue une phase importante pour la réalisation de l'audit sur terrain. En effet, c'est au cours de cette phase que se dessinent les grands axes qui devront être suivis lors de l'audit sur terrain. Elle se manifeste par des rencontres entre auditeurs et responsables de l'organisme à auditer. Au cours de ces entretiens, les espérances des responsables vis-à-vis de l'audit devront être exprimées. Aussi, le planning de réalisation de la mission de l'audit doit être fixé.

Les personnes qui seront amenées à répondre au questionnaire concernant l'audit organisationnel doivent être également identifiées. L'auditeur (ou les auditeurs) pourrait également solliciter les résultats des précédents audits. Cette phase sera suivie par l'audit organisationnel et physique.

II.5.3 Audit organisationnel et physique

① Objectifs :

Dans cette étape, il s'agit de s'intéresser à l'aspect physique et organisationnel de l'organisme cible, à auditer. Nous nous intéressons donc aux aspects de gestion et d'organisation de la sécurité, sur les plans organisationnels, humains et physiques.

L'objectif visé par cette étape est donc d'avoir une vue globale de l´état de sécurité du système d´information et d´identifier les risques potentiels sur le plan organisationnel.

② Déroulement :

Afin de réaliser cette étape de l'audit, ce volet doit suivre une approche méthodologique qui s'appuie sur « une batterie de questions ». Ce questionnaire préétabli devra tenir compte et s'adapter aux réalités de l'organisme à auditer. A l'issue de ce questionnaire, et suivant une métrique, l'auditeur est en mesure d'évaluer les failles et d'apprécier le niveau de maturité en termes de sécurité de l'organisme,ainsi que la conformité de cet organisme par rapport à la norme référentielle de l'audit.

II.5.4 Audit technique

① Objectifs :

Cette étape de l'audit sur terrain vient en seconde position après celle de l'audit organisationnel. L'audit technique est réalisé suivant une approche méthodique allant de la découverte et la reconnaissance du réseau audité jusqu'au sondage des services réseaux actifs et vulnérables.

Cette analyse devra faire apparaître les failles et les risques, les conséquences d'intrusions ou de manipulations illicites de données. Au cours de cette phase, l'auditeur pourra également apprécier l'écart avec les réponses obtenues lors des entretiens. Il testera aussi la robustesse de la sécurité du système d'information et sa capacité à préserver les aspects de confidentialité, d'intégrité, de disponibilité et d'autorisation.

Cependant, l'auditeur doit veiller à ce que les tests réalisés ne remettent pas en cause la continuité de service du système audité.

② **Déroulement :**

Vu les objectifs escomptés lors de cette étape, leurs aboutissements ne sont possibles que par l'utilisation de différents outils. Chaque outil commercial qui devra être utilisé, doit bénéficier d'une licence d'utilisation en bonne et du forme.

Également les outils disponibles dans le monde du logiciel libre sont admis. L'ensemble des outils utilisés doit couvrir entièrement ou partiellement la liste non exhaustive des catégories ci-après :

- ✦ Outils de sondage et de reconnaissance du réseau.
- ✦ Outils de test automatique de vulnérabilités du réseau.
- ✦ Outils spécialisés dans l'audit des équipements réseau (routeurs, switchs).
- ✦ Outils spécialisés dans l'audit des systèmes d'exploitation.
- ✦ Outils d'analyse et d'interception de flux réseaux.
- ✦ Outils de test de la solidité des objets d'authentification (fichiers de mots clés).
- ✦ Outils de test de la solidité des outils de sécurité réseau (Firewalls, IDS, outils d'authentification).
- ✦ Outils de scanne d'existence de connexions dial-up dangereuses (wardialing).
- ✦ Outils spécialisés dans l'audit des SGBD existants.

Chacun des outils à utiliser devra faire l'objet d'une présentation de leurs caractéristiques et fonctionnalités aux responsables de l'organisme audité pour les assurer de l'utilisation de ces outils.

II.5.5 Test d'intrusions (Audit intrusif)

① **Objectifs :**

Cet audit permet d'apprécier le comportement du réseau face à des attaques. Également, il permet de sensibiliser les acteurs (management, équipe informatique sur site, les utilisateurs) par des rapports illustrant les failles décelées, les tests qui ont été effectués (scénarios et outils) ainsi que les recommandations pour pallier aux insuffisances identifiées.[2]

② **Déroulement :**

La phase de déroulement de cet audit doit être réalisée par une équipe de personnes ignorante du système audité avec une définition précise des limites et horaires des tests. Étant donné l'aspect risqué (pour la continuité de services du système d'information) que porte ce type d'audit, l'auditeur doit :

- ✦ Bénéficier de grande compétences.
- ✦ Adhérer une charte déontologique.

- ✦ S'engager (la charte d'audit) à un non-débordement : implication à ne pas provoquer de perturbation du fonctionnement du système, ni de provocation de dommages.

II.5.6 Rapport d'audit

A la fin des précédentes phases d'audit sur terrain, l'auditeur est invité à rédiger un rapport de synthèse sur sa mission d'audit.[2]

Cette synthèse doit être révélatrice des défaillances enregistrées. Autant il est important de déceler un mal, autant il est également important d'y proposer des solutions. Ainsi, l'auditeur est également invité à donner ses recommandations, pour pallier aux défauts qu'il aura constaté.

Ces recommandations doivent tenir compte de l'audit organisationnel et physique, ainsi que de l'audit technique et intrusif.

II.6 Conclusion

Toute approche de test de la sécurité des systèmes d'information devrait être le résultat d'une réflexion préalable pour envisager les meilleures solutions possibles. Il prend en compte les besoins spécifiques de l'organisation, tant sur le plan organisationnel que technique.

ChapitreIII

Méthodes et normes d'audit (référentiels)

III.1 Introduction

Les audits de sécurité informatique sont liés aux référentiels et norme. Cependant, ce chapitre fournit un peu d'histoires et une brève description de l'ensemble de normes système ISO 27k. Le système de gestion de la sécurité de l'information appelé ISMS. Il explique la norme ISO 27001 et la méthode MEHARI pour aider à développer des politiques de sécurité plus claires.

III.2 Définitions

Les concepts de méthode de sécurité et de norme de sécurité portent souvent à confusion. Nous allons tenter de définir chacun de ces concepts.

III.2.1 Les méthodes

Une méthode est une démarche, un processus ou un ensemble de principes qui permettent d'appliquer une norme au système d'information de l'entreprise. La méthode sert aussi à faire un audit qui permet de faire, par exemple, un état de la sécurité du système d'information. Une méthode est souvent accompagnée d'outils afin d'appuyer son utilisation. Ils peuvent être disponibles gratuitement auprès des organismes qui les ont produits. Par exemple la méthode *MEHARI*, que nous verrons plus loin, propose un outil (fichier *Microsoft Excel*). Le fichier contient un ensemble de questions et de scénarios. Cette base de connaissance permet de ressortir toutes les vulnérabilités du système d'information et émet des recommandations pour y remédier. La plupart des méthodes sont appliquées par des experts en gestion des risques (*EBIOS, MEHARI, OCTAVE*).[4]

III.2.2 L'ISO (Organisation Internationale de Normalisation)

L'ISO est le fruit d'une collaboration entre différents organismes de normalisation nationaux. Au début du 20ème siècle, l'American Institute of Electrical Engineer (Aujourd'hui appelé Institute of Electrical and Electronics Engineers ou IEEE) invite quatre autres instituts professionnels pour constituer une première organisation nationale, l'AESC (American Engineering Standards Committee) qui aura pour objectif de publier des standards industriels communs avant de prendre le nom d'ASA (American Standards Association) et d'établir des procédures standardisées pour la production militaire pendant la seconde guerre mondiale. En 1947, l'ASA, le BSI (British Standards Institute), l'AFNOR (Association Française de Normalisation) et les organisations de normalisation de 22 autres pays fondent l'Organisation Internationale de Normalisation (ISO).

A ce jour, l'ISO regroupe 157 pays membres et coopère avec les autres organismes de normalisation comme le CEN (Comité européen de normalisation) ou la Commission Electronique Internationale (CEI). En 1987, l'ISO et le CEI créent le Joint Technical Committee (JTC1) pour la normalisation des Technologies de l'Information (TI). Le JTC1 allie les compétences de l'ISO en matière de langage de programmation et codage de l'information avec celles du CEI qui traitent du matériel tel que les microprocesseurs.

Le JTC1 est composé de plusieurs comités techniques (SC) qui traitent de sujets tels

que la biométrie, la téléinformatique, les interfaces utilisateurs ou encore les techniques de sécurité de l'information relatives aux normes de la série ISO/CEI 27k

III.2.3 Les normes

Une norme est, selon le guide ISO/CEI, *« un document de référence approuvé par un organisme reconnu, et qui fourni pour des usages communs et répétés, des règles, des lignes directrices ou des caractéristiques, pour des activités, ou leurs résultats, garantissant un niveau d'ordre optimal dans un contexte donné »*[3].

Les entreprises se font certifier pour prouver qu'elles suivent les recommandations de la norme. Pour être certifié, il faut, dans un premier temps acheter la norme. Les normes appliquées à la sécurité des systèmes d'information sont généralement éditées par l'organisme ISO. Ensuite l'entreprise doit mettre en pratique les recommandations décrites dans la norme.

Généralement, une entreprise peut se faire certifier pour trois raisons :

① Pour une *raison commerciale* : pour certaines entreprises, être certifiées par des normes de qualité, par exemple, est un gage de qualité pour les clients et est donc un atout commercial.

② *Par obligation* : En industrie aéronautique, par exemple, les constructeurs exigent de leurs sous-traitants qu'ils soient certifiés par certaines normes.

③ Il y a aussi des entreprises qui se *certifient pour elles-mêmes*, pour optimiser leur processus en interne.

III.2.4 Historique des normes en matière de sécurité de l'information

Au cours des vingt dernières années les normes liées à la sécurité de l'information ont évolué ou ont été remplacées. Ces changements rendent difficile une bonne compréhension du sujet. Un rappel historique de l'évolution de ces normes permet de clarifier la situation normative en matière de sécurité de l'information.

Au début des années 90, de grandes entreprises britanniques se concertent pour établir des mesures visant à sécuriser leurs échanges commerciaux en ligne. Le résultat de cette collaboration servit de référence en la matière pour d'autres entreprises qui souhaitaient mettre en œuvre ces mesures. Cette initiative privée fut appuyée par le Département des Transports et de l'Industrie britannique qui supervisa la rédaction au format du BSI, d'une première version de projet de norme de gestion de la sécurité de l'information.

✦ **En 1991,** un projet de «best practices» code de bonnes pratiques, préconise la formalisation d'une politique de sécurité de l'information. Cette politique de sécurité doit intégrer au minimum huit points «stratégique et opérationnel» ainsi qu'une mise à jour régulière de la politique.

- **En 1995,** le BSI publie la norme BS7799 qui intègre dix chapitres réunissant plus de 100 mesures détaillées de sécurité de l'information, potentiellement applicables selon l'organisme concerné.

- **En 1998,** la norme BS7799 change de numérotation et devient la norme BS7799-1. Elle est complétée par la norme BS7799-2 qui précise les exigences auxquelles doit répondre un organisme pour mettre en place une politique de sécurité de l'information. Cette nouvelle norme est fondée sur une approche de la maîtrise des risques et sur le principe du management de la sécurité de l'information.

- **En 2000,** la norme BS7799-1, devient la norme de référence internationale pour les organismes souhaitant renforcer leur sécurité de l'information. Après avoir suivi un processus de concertation au niveau international et quelques ajouts, l'ISO lui attribue un nouveau nom, ISO/IEC 17799 : 2000.

- **En 2002,** le BSI fait évoluer la norme BS7799-2 en s'inspirant des normes ISO 9001 :2000 et ISO 14001 : 1996. La norme adopte définitivement une approche de management de la sécurité de l'information.

- **En 2005,** l'ISO/CEI adopte la norme BS7799-2 sous la référence ISO/CEI 27001 : 2005 en y apportant quelques modifications pour se rapprocher le plus possible du principe de «système de management » développé par les normes ISO 9001 et ISO14001. L'ISO/IEC 27001 : 2005 spécifie les exigences pour la mise en place d'un SMSI (Système de Management de la Sécurité de l'Information).

- **En 2007,** dans un souci de clarification, l'ISO renomme la norme ISO/IEC 17799 :2005 en changeant sa numérotation pour ISO/IEC 27002. La norme se greffe à la famille des normes ISO/IEC 27k toujours en développement.

Le tableau ci-après reprend cet historique.

TABLE III.1 – Historique des normes en matière de sécurité de l'information

ANNÉE	NORME	TRAITE DES SMSI	REMPLACE LA NORME
1995	BS 7799 :1995	NON	
1998	BS 7799-2 :1998	OUI	
2000	ISO 17799 :2000	NON	BS 7799 :1995
2002	BS 7799-2 :2002	OUI	BS 7799-2 :1998
2005	ISO 17799 :2005	NON	ISO 17799 :2000
2005	ISO 27001 :2005	OUI	BS 7799-2 :2002
2007	BS ISO 27002	NON	ISO 17799 :2005

III.3 La série des normes de la famille ISO 27k

Cette série aussi connue sous le nom de famille des standard SMSI ou ISO27k, comprend les normes de sécurité de l'information publiées conjointement par l'organisation interna-

tionale de normalisation (ISO) et la commission électrotechnique internationale (CEI).

La suite contient des recommandations des meilleures pratiques en management de la sécurité de l'information, pour l'initialisation, l'implémentation ou le maintien de systèmes de management de la sécurité de l'information, ainsi qu'un nombre croissant de normes liées au SMSI.[3]

Les normes publiées sont :

ISO/CEI 27000 : (PUBLIÉE EN 2018).
Systèmes de management de la sécurité de l'information–Vue d'ensemble et vocabulaire.

ISO/CEI 27001 : (PUBLIÉE EN 2013 - ACTUELLEMENT EN COURS DE DÉVELOPPEMENT SERA REMPLACÉ PAR ISO/CEI FDIS 27001).
Norme principale de définition des besoins pour le SMSI. Elle correspond au principe de certification des organisations.

ISO/CEI 27002 : (PUBLIÉE EN 2022)
Il s'agit de la description des bonnes pratiques décrivant un ensemble compréhensible d'objectifs de contrôle de sécurité et un ensemble de bonne pratiques de contrôle de sécurité généralement acceptés.

ISO/CEI 27003 : (PUBLIÉE EN 2017)
Comprends le guide implémentation détaillée relatif à l'adoption de la série complète de ISO 27001.

ISO/CEI 27004 : (PUBLIÉE EN 2016).
Contient la norme qui définit les principes d'évaluation et de mesure de ce qui a été implémenté dans le cadre du système de management de la sécurité de l'information pour mesurer l'efficacité du système de gestion de la sécurité mise en place.

ISO/CEI 27005 : (PUBLIÉE EN 2018 - ACTUELLEMENT EN COURS DE DÉVELOPPEMENT SERA REMPLACÉ PAR ISO/CEI FDIS 27005).
Contient la norme de gestion de risque de sécurité de l'information comprenant des conseils sur la sélection des analyses de risque appropriées, les méthodes et outils de gestion.

ISO/CEI 27006 : (RETIRÉE EN 2011 - PUBLIÉE ISO/CEI 27006/AMD-1 EN 2015 - ACTUELLEMENT EN COURS DE DÉVELOPPEMENT SERA REMPLACÉ PAR ISO/CEI DIS 27006-1)
Guide décrivant les exigences pour les organismes procédant à l'audit et la certification qui ont réussi la certification de ISO/IEC 27001.

ISO/CEI 27007 : (PUBLIÉE EN 2020)
Cette norme repose sur des instruction pour les audit accrédités en cas d'audit ISO 27001 d'un SMSI.

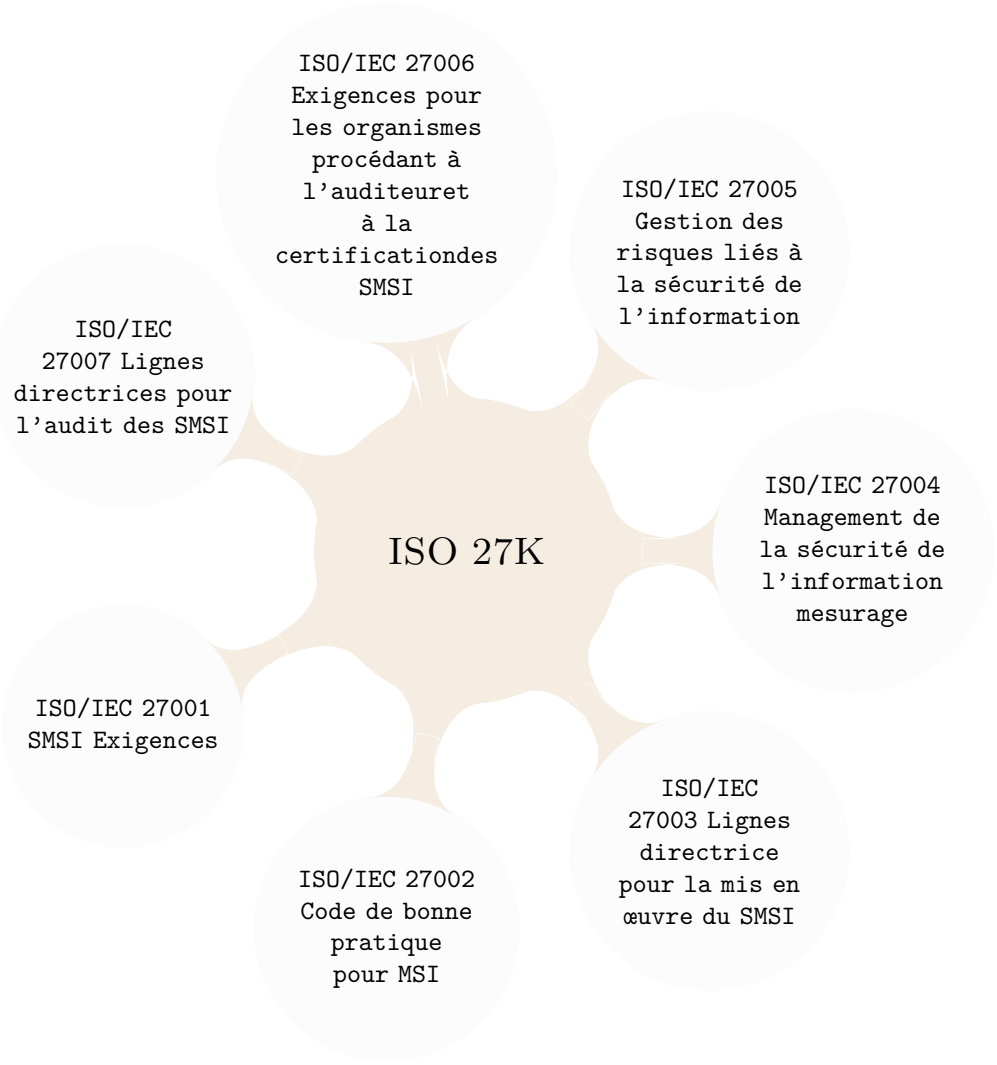


FIGURE III.1 – Les standards d'un SMSI

III.3.1 ISO/CEI 27000

Systèmes de management de la sécurité de l'information – vue d'ensemble et vocabulaire

L'ISO/CEI 27000 est une norme de sécurité de l'information publiée conjointement en mai 2009 et révisée en 2012, 2016 et 2018 par l'Organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (CEI), faisant partie de la suite ISO/CEI 27k.

III.3.2 ISO/CEI 27001

Systèmes de management de la sécurité de l'information – Exigence :

L'ISO/CEI 27001 est la norme centrale de la famille ISO 27k, c'est la norme d'exigences qui définit les conditions pour mettre en œuvre et documenter un SMSI.

Les Objectifs de la norme ISO 27001 publiée en octobre 2005 succède à la norme BS 7799-2 de BSI(British Standards Institution), révisée en 2013 et aujourd'hui en cours de développement sera remplacée par ISO/CEI FDIS 27001. Elle s'adresse à tous les types d'organismes(entreprises commerciales, administrations, etc...). La norme ISO/CEI 27001 décrit les exigences pour la mise en place d'un Système de Management de la Sécurité de l'Information. Le SMSI est destiné à choisir les mesures de sécurité afin d'assurer la protection des biens sensibles d'une entreprise sur un périmètre défini. C'est le modèle de qualité PDCA (Plan-Do-Check-Act) qui est recommandé pour établir un SMSI afin d'assurer une amélioration continue de la sécurité du système d'information.

La norme dicte également les exigences en matières de mesures de sécurité propres à chaque organisme, c'est-à-dire que la mesure n'est pas la même d'un organisme à l'autre. Les mesures doivent être adéquates et proportionnées à l'organisme pour ne pas être ni trop laxistes ni trop sévères. La norme ISO 27001 intègre aussi le fait que la mise en place d'un SMSI et d'outils de mesures de sécurité aient pour but de garantir la protection des actifs informationnels. L'objectif est de protéger les informations de toute perte ou intrusion. Cela apportera la confiance des parties prenantes.

L'ISO/CEI 27001 définit l'ensemble des contrôles à effectuer pour s'assurer de la pertinence du SMSI, à l'exploiter et à le faire évoluer. Plus précisément, l'annexe A de la norme est composée des 133 mesures de sécurité de la norme ISO/CEI 27002 (anciennement ISO/CEI 17799), classées dans 11 sections. Comme pour les normes ISO 9001 et ISO 14001, il est possible de se faire certifier ISO 27001.

III.3.3 ISO/CEI 27002

Code de bonne pratique pour le management de la sécurité de l'information :

L'ISO/CEI 27002 est un ensemble de 114 mesures dites « best practices » (bonnes pratiques en français), destinées à être utilisées par tous ceux qui sont responsables de la mise en place ou du maintien d'un Système de Management de la Sécurité de l'Information.

La sécurité de l'information est définie au sein de la norme comme la *« préservation de la confidentialité, de l'intégrité et de la disponibilité de l'information ».*

Cette norme n'a pas de caractère obligatoire pour les entreprises. Son respect peut toutefois être mentionné dans un contrat : un prestataire de services pourrait ainsi s'engager à respecter les pratiques normalisées dans ses relations avec un client.

Objectifs ISO/IEC 27002 est plus un code de pratique, qu'une véritable norme ou qu'une spécification formelle telle que l'ISO/IEC 27001. Elle présente une série de contrôles (39 objectifs de contrôle) qui suggèrent de tenir compte des risques de sécurité des informations relatives à la confidentialité, l'intégrité et les aspects de disponibilité. Les entreprises qui adoptent l'ISO/CEI 27002 doivent évaluer leurs propres risques de sécurité de l'information et appliquer les contrôles appropriés, en utilisant la norme pour orienter l'entreprise.

La norme ISO 27002 n'est pas une norme de nature technique, technologique ou orientée

produit, ou une méthodologie d'évaluation d'équipement telle que les critères communs CC/ISO 15408. Elle n'a pas de caractère d'obligation, elle n'amène pas de certification, ce domaine étant couvert par la norme ISO/IEC 27001.

III.3.4 ISO/CEI 27003

Lignes directrices pour la mise en œuvre du système de management de la sécurité de l'information :

La norme ISO/CEI 27003 fournit une approche orientée processus pour la réussite de la mise en œuvre d'un SMSI conformément à l'ISO 27001.

Objectifs ISO / IEC 27003 guide la conception d'une norme ISO / IEC 27001-SGSI conforme, conduisant à l'ouverture d'un SMSI [la mise en œuvre du projet]. Il décrit le processus du SMSI et la spécification de conception, du début jusqu'à la production des plans d'exécution des projets, couvrant la préparation et la planification des activités préalables à la mise en œuvre effective, et en prenant des éléments clés tels que :

- ✦ Approbation de la direction et l'autorisation définitive de procéder à l'exécution des projets.
- ✦ Détermination de la portée et la définition des limites en termes de TIC et les lieux physiques.
- ✦ L'évaluation des risques sécurité de l'information et de la planification des traitements de risque appropriés, le cas échéant en définissant des exigences de contrôle de sécurité de l'information.
- ✦ Conception du SMSI.
- ✦ La planification du projet mise en œuvre.

III.3.5 ISO/CEI 27004

Management de la sécurité de l'information – Mesurage :

ISO/CEI 27004 couvre les mesures de management de sécurité de l'information, généralement connu comme les mesures de sécurité. Elle est élaborée par l'ISO et la Commission électrotechnique internationale (CEI). Son nom complet est la technologie de l'information - Techniques de sécurité - Management de la sécurité de l'information – Mesurage.

Objectifs Le but de la norme ISO / IEC 27004 est d'aider les organisations à mesurer, rapporter et donc d'améliorer systématiquement l'efficacité de leurs systèmes de gestion de sécurité de l'information (SGSI).

La norme est destinée à aider les organisations à mesurer, rendre compte et donc d'améliorer systématiquement l'efficacité de leurs systèmes de gestion de l'information de sécurité.

III.3.6 ISO/CEI 27005

Gestion des risques liés à la sécurité de l'information :

La première norme de gestion des risques de la Sécurité des Systèmes d'Informations est l'ISO/CEI 27005. Cette norme est un standard international qui décrit le Système de Management des risques liés à la Sécurité de l'information.

Certains expliquent que cette norme est en fait une méthode quasi-applicable en se servant des annexes et en les adaptant à leur contexte. D'ailleurs dans l'enquête 2010 du CLUSIF, 35% des entreprises qui font analyses de risques déclarent le faire en utilisant la norme ISO 27005.

Objectifs La norme ISO 27005 explique en détail comment conduire l'appréciation des risques et le traitement des risques, dans le cadre de la sécurité de l'information. La norme ISO 27005 propose une méthodologie de gestion des risques en matière d'information dans l'entreprise conforme à la norme ISO/CEI 27001.

La nouvelle norme a donc pour but d'aider à mettre en œuvre l'ISO/CEI 27001, la norme relative aux systèmes de management de la sécurité de l'information (SMSI), qui est fondée sur une approche de gestion du risque. Néanmoins, la norme ISO 27005 peut être utilisée de manière autonome dans différentes situations. La norme ISO 27005 applique à la gestion de risques le cycle d'amélioration continue PDCA (Plan, Do,Check, Act) utilisé dans toutes les normes de systèmes de management.

III.3.7 ISO/CEI 27006

Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information :

ISO/CEI 27006 est un standard de sécurité de l'information publié conjointement par l'ISO et la CEI, afin de fixer les exigences pour les organismes réalisant l'audit et la certification de SMSI.

Objectifs Son objet est de fournir les prérequis pour les organismes d'audit et de certification à la norme ISO 27001 pour les Systèmes de Management de la Sécurité de l'Information. Cette norme a été remise à jour en 2011 et porte la référence ISO/IEC 27006.

III.3.8 ISO/CEI 27007

Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information :

Cette norme fournit les lignes directrices pour les audits des systèmes de management de la sécurité de l'information, ainsi que des conseils sur la compétence des auditeurs des SMSI. Elle inclue aussi les lignes directrices contenues dans la norme ISO 19011.

III.4 Les Système de Management

Le principe de système de management n'est pas nouveau. Il concerne historiquement le monde de la qualité, surtout dans le domaine des services et de l'industrie. La norme ISO 9001 précise les exigences auxquelles il faut répondre pour mettre en place un système de management de la qualité (SMQ).[2]

Un système de management est un système permettant :

① d'établir une politique ;

② d'établir des objectifs ;

③ d'atteindre ces objectifs ;

Nous pouvons ainsi dire qu'un système de management est un ensemble de mesures organisationnelles et techniques visant à atteindre un objectif et, une fois celui-ci atteint, à s'y tenir, voire à le dépasser.

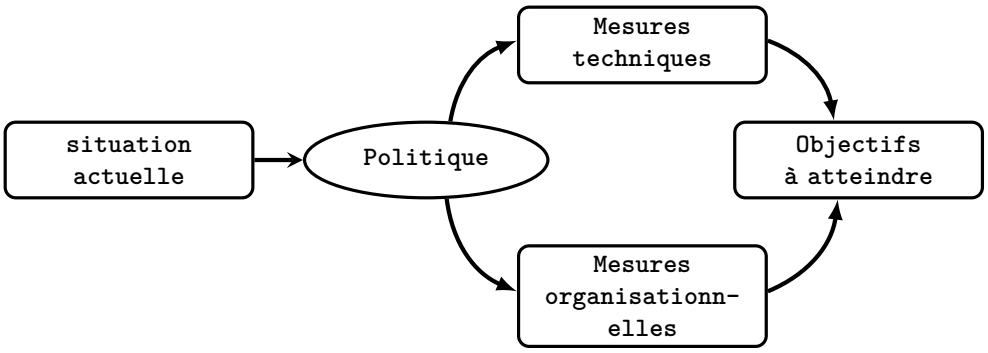


FIGURE III.2 – Le processus du systèmes de management

III.4.1 Les principaux systèmes de management

Les systèmes de management ne se cantonnent pas uniquement à la qualité. Ils concernent des domaines très variés comme l'environnement, les services informatiques, la sécurité de l'information, la sécurité alimentaire ou encore la santé.[5]

Le tableau ci-après donne un aperçu non exhaustif des principaux référentiels de systèmes de management.

Table III.2 – Historique des normes en matière de sécurité de l'information

Référentiel	Domaine
ISO 9001	Qualité
ISO 14001	Environnement
ISO 27001	Sécurité de l'information
ISO 20000	Services informatiques
ISO 22000	Sécurité alimentaire
OHSAS 18001	Santé/Sécurité du personne

Nous constatons que la majorité de ces référentiels sont normalisés par l'ISO (Organisation internationale de normalisation). Cependant, d'autres organismes privés ou nationaux peuvent proposer leurs propres référentiels. La dernière ligne de cette liste montre, en effet, que l'ISO n'a pas le monopole des systèmes de management, puisque la norme relative à la sécurité du personnel au travail (OHSAS 18001) n'est pas spécifiée par l'ISO.

III.4.2 L'apport des systèmes de management

Les propriétés que nous venons de décrire donnent de bonnes raisons de penser que la mise en place et l'exploitation d'un système de management n'est pas un projet facile à mener. Il faut commencer par fixer des politiques, formaliser les procédures par écrit et mener à bien des audits réguliers. Ces opérations sont loin d'être transparentes. Souvent lourdes à implémenter, leur coût humain et financier n'est pas négligeable. Dans ces conditions, il est légitime de se demander ce qui justifie un tel investissement. Quels bénéfices concrets pouvons-nous en espérer ?[5]

① **Premier apport : l'adoption de bonnes pratiques**

Les systèmes de management se basent sur des guides de bonnes pratiques dans le domaine qui les concerne (qualité, sécurité, environnement, etc.). Ainsi, celui qui se lance dans la mise en place d'un système de management est quasiment obligé d'adopter ces bonnes pratiques.

② **Deuxième apport : l'augmentation de la fiabilité**

L'adoption de bonnes pratiques a pour conséquence directe, à court ou moyen terme, l'augmentation de la fiabilité. Ceci est principalement dû au fait que les systèmes de management imposent la mise en place de mécanismes d'amélioration continue favorisant la capitalisation sur les retours d'expérience.

③ **Troisième apport : la confiance**

Nous touchons enfin à la raison d'avoir un système de management ; il fournit la confiance envers les parties prenantes. Une partie prenante est toute personne, groupe ou instance envers laquelle l'entreprise doit rendre des comptes *(Par exemple : Les actionnaires, Les autorités de tutelle, Les clients, Les fournisseurs, Les partenaires, etc...).*

En fait, nous oublions trop souvent que la confiance est le vecteur qui permet toute

relation entre un client et un fournisseur. Autant dire qu'il n'y aurait aucune activité économique sans la confiance.

III.4.3 Les systèmes de management de la sécurité de l'information (SMSI)

Le principal objectif d'un SMSI est de faire en sorte de préserver la confidentialité, l'intégrité et la disponibilité pour les informations les plus sensibles de l'entreprise. La norme ISO 27001 insiste sur ces notions. Ces derniers sont formellement définis dans la norme ISO 13335-1.

Le SMSI est cohérent avec les autres systèmes de management de l'entité, notamment avec les systèmes de management de la qualité, de la sécurité des conditions de travail, et de l'environnement.

Le SMSI inclut donc au minimum :

- ✦ Des éléments documentaires (politique, description des objectifs, cartographie des processus impactés, des activités de sécurité, et des mesures).
- ✦ La description de la méthode d'analyse des risques utilisée.
- ✦ Les processus impliqués dans la mise en œuvre de la sécurité de l'information.
- ✦ Les responsabilités relatives à la sécurité de l'information.
- ✦ Les ressources nécessaires à sa mise en œuvre.
- ✦ Les activités relatives à la sécurité de l'information.
- ✦ Les enregistrements issus des activités relatives à la sécurité de l'information.
- ✦ Les mesures prises sur les processus.
- ✦ Les actions relatives à l'amélioration de la sécurité de l'information.

L'existence d'un SMSI dans l'organisme permet de renforcer la confiance dans le mode de gestion de la sécurité de l'information.

III.5 La norme ISO/CEI 27001 (Le modèle PDCA)

III.5.1 Définition

La méthode PDCA(Plan, Do, Check, Act) issue de l'ISO 9000 est appelée roue de l'amélioration de la qualité ou « Roue de Deming », du nom de W.Edward Deming, statisticien et philosophe américain, inventeur des principes de la qualité, et Walter Andrew Shewhart, statisticien américain inventeur de la roue de Deming.

Le principe propose de maîtriser et d'améliorer un processus par l'utilisation d'un cycle continue en quatre étapes visant à réduire le besoins de corrections. Et les systèmes de management fonctionnent selon cette méthode qui comporte les étape suivantes :[4]

① **Phase Plan (Prévoir) :** Définit l'objectif principale qui consiste à identifier et à préciser les besoins du maître d'ouvrage. Elle effectue l'inventaire des moyens nécessaires à sa réalisation, son coût et son planning.

② **Phase Do (Faire) :** C'est la partie opérationnelle de la méthode. Elle comporte :

- ✦ L'allocation des ressources en personne, temps et budget.
- ✦ La rédaction de la documentation.
- ✦ La formation du personnel concerné.
- ✦ La gestion du risque.
- ✦ L'exécution des tâches.

③ **Phase Check (Vérifier) :** C'est ici que les opérations réalisées précédemment sont vérifiées pour qu'elles correspondent aux besoins exprimé, dans les délais et les coûts précisés à la première étape. Elle comprend :

- ✦ Une évaluation à partir de ce qu'est déjà été implémenté dans d'autre environnement.
- ✦ Un contrôle globale des résultats produits.
- ✦ Un audit de l'environnement du système de gestion de la sécurité du système d'information, soit un audit annuel, sur la base du documents et de trace d'évènements produit par les outils de supervision.

④ **Phase Act (Réagir) :** Cette étape recherche les amélioration à apporter au projet globale de changement. Des mesures sont évaluées à partir des bilans ou des constatations relevées lors de la phase de vérification. Des actions possibles sont élaborées selon les cas :

- ✦ Passage à phase de planification : si de nouveau risque ou modification ont été identifiés.
- ✦ Passage à la phase exécution : si la phase de vérification en montre le besoin.
- ✦ Après la constatation de non-conformité, des actions correctives ou préventives sont déployés.

Ce modèle présente deux propriétés principales : il est cyclique et fractal.

✦ **Caractère cyclique :** c'est ce cycle Plan, Do, Check, Act qui permet d'atteindre les objectifs (de sécurité, de qualité, d'environnement ou autre) fixés par le management. En revanche, une fois que l'objectif a été atteint, un nouveau cycle doit être entrepris.

✦ **Caractère fractal :** quelle que soit l'échelle à laquelle on observe les systèmes de management, on doit retrouver le modèle Plan, Do, Check, Act.

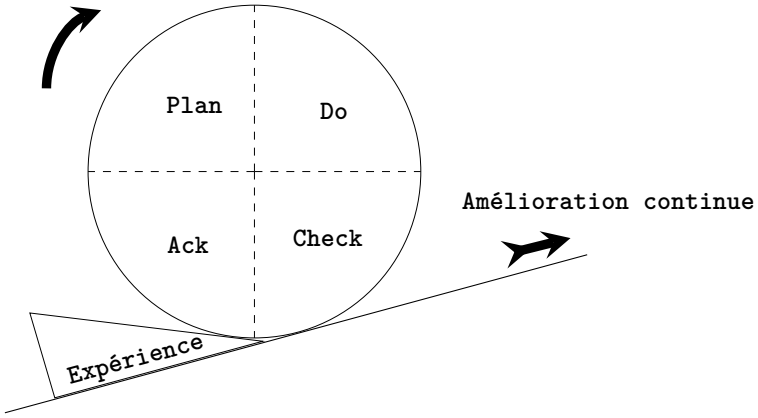


FIGURE III.3 – Le modèle PDCA

III.5.2 Phase Plan

La phase « Plan » du PDCA consiste à fixer les objectifs du SMSI en suivant quatre grandes étapes, la politique et le périmètre du SMSI, l'appréciation des risques, le traitement des risques décidé en tenant en compte des risques résiduels et la sélection des mesures de sécurité présentées dans le SoA (Statement of Applicability) qu'est un document sous forme de tableau qui énumère les mesures de sécurité du SMSI ainsi que celles non appliquées.

Dans la figure ci-dessous, une vue du déroulement de la phase Plan.

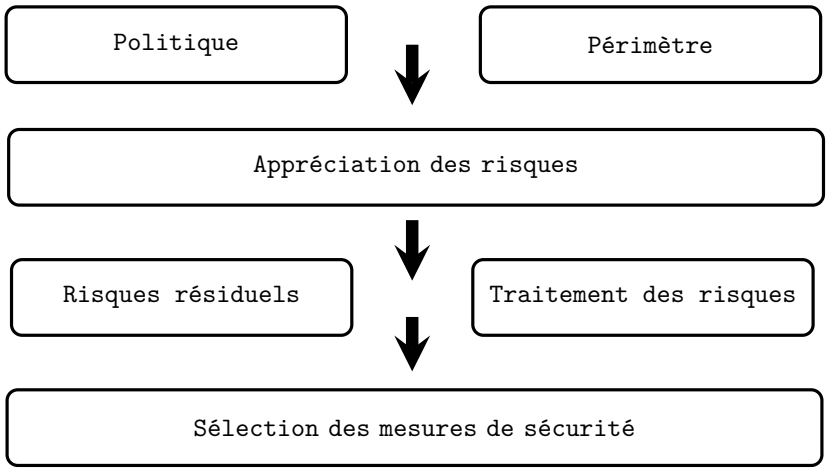


FIGURE III.4 – Processus de déroulement de la phase Plan

III.5.2.1 Politique et périmètre du SMSI

La première étape consiste à définir la politique et le périmètre du SMSI. La politique est là pour préciser le niveau de sécurité qui sera appliqué au sein du périmètre du SMSI. La norme ne fixe pas d'exigences sur le périmètre, il peut être restreint ou couvrir l'ensemble

des activités de l'organisme. L'objectif est d'y inclure les activités pour lesquelles les parties prenantes exigent un certain niveau de confiance.

III.5.2.2 Appréciation des risques

La deuxième étape concerne un des points les plus importants de l'ISO/CEI 27001, l'appréciation des risques. Le problème de l'appréciation des risques n'est pas nouveau et est traité par de nombreuses méthodes développées dans différents secteurs privés, académiques et agences gouvernementales. Certaines méthodes sont très répandues dans les organismes. En France, les plus connues sont EBIOS et MEHARI, aux Etats- Unis, OCTAVE. L'ISO/CEI propose aussi une méthode, la norme ISO/CEI 27005. Cette norme ne fait que fixer un cahier des charges spécifiant chacune des étapes clefs de l'appréciation des risques.

III.5.2.2.1 Processus de l'appréciation des risques : le processus d'appréciation des risques se déroule en sept étapes, illustrées dans figure ci-dessous.

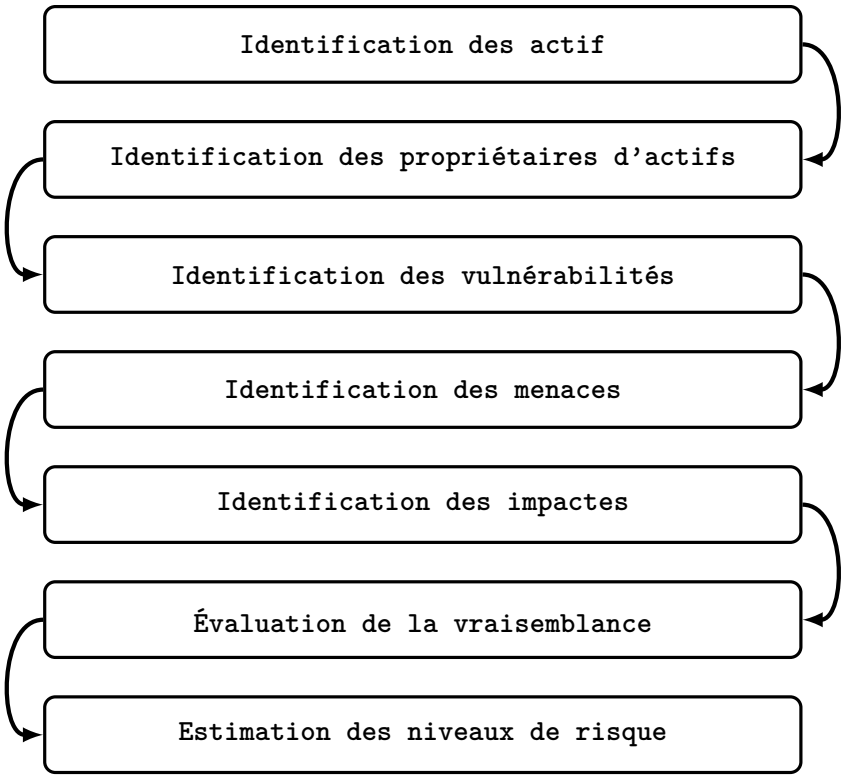


FIGURE III.5 – Schéma du processus d'audit

❶ **Identification des actifs :** consiste à dresser une liste de tous les actifs qui ont une importance en matière d'information au sein du SMSI. On distingue généralement six catégories d'actifs :

① Matériel, pour tous les équipements réseau et système.

② Physique, pour les bureaux, lieux de production, de livraisons.

③ Logiciel, pour les bases de données, fichiers, les systèmes d'exploitation.

④ Humain, pour tous les collaborateurs de l'organisme.

⑤ Documents, pour les documents papier, manuels d'utilisation.

⑥ Immatériel, pour le savoir-faire de l'organisme.

❷ **Identification des propriétaires d'actif :** vise à attribuer pour chaque actif d'information un « propriétaire ». La norme définit le propriétaire comme étant la personne qui connaît le mieux la valeur et les conséquences d'une compromission en termes de disponibilité, d'intégrité et de confidentialité de l'actif.

❸ **Identification des vulnérabilités :** est l'identification des vulnérabilités des actifs recensés. La vulnérabilité est la propriété intrinsèque du bien qui l'expose aux menaces. A titre d'exemple, un ordinateur portable est vulnérable au vol mais sa vulnérabilité n'est pas le vol mais sa portabilité. Dans ce cas, l'identification de la vulnérabilité est la portabilité.

❹ **Identification des menaces :** est l'identification des menaces qui pèsent sur les actifs d'information précédemment recensés. Si l'on reprend l'exemple de l'ordinateur portable, la menace est dans ce cas le vol.

❺ **Identification des impactes :** vise à évaluer l'impact d'une perte de la confidentialité, de la disponibilité ou de l'intégrité sur les actifs. Pour mesurer cet impact on peut par exemple utiliser une matrice des risques, la norme n'impose aucun critère de mesure.

❻ **Évaluation de la vraisemblance :** demande d'évaluer la vraisemblance des précédentes étapes du processus en plaçant dans leur contexte les actifs. Il s'agit par exemple de considérer les mesures de sécurité déjà en vigueur dans l'organisme. Si l'ordinateur portable possède une clef d'authentification, un cryptage de ses données ou un accès VPN pour travailler, alors la vraisemblance d'observer un impact sur la confidentialité, la disponibilité ou l'intégrité de ses données est limitée.

❻ **Estimation des niveaux de risque :** consiste à attribuer une note finale reflétant les risques pour chacun des actifs d'information. La norme n'impose aucune formule, on peut par exemple utiliser un code couleur (rouge pour un niveau de risque très élevé, orange pour moyen et vert pour faible.

Dans le point suivant, nous présentons deux méthodes connues et largement employées par les organismes pour l'appréciation des risques de leur SMSI.

III.5.2.2.2 Méthodes d'appréciation des risques :

en 2004, une étude du CLUSIF (Club de la Sécurité de l'Information Français) dénombrait plus de deux cents méthodes d'appréciation des risques. Nous allons parler des méthodes, *EBIOS et MEHARI.*

III.5.3 La méthode EBIOS

Développée dans les années 90 sous l'autorité de l'agence française ANSSI (Agence nationale de la sécurité des systèmes d'information), cette méthode est l'«Expression des Besoins et Identification des Objectifs de Sécurité». Elle permet d'apprécier, de traiter et communiquer sur les risques au sein d'un SMSI.[4]

L'ANSSI et le Club EBIOS proposent en libre accès sur leur site web toute la documentation ainsi qu'un logiciel libre facilitant l'utilisation de la méthode.

L'approche de la méthode est itérative, chaque module peut être révisé, amélioré et tenu à jour de manière continue.

EBIOS se compose de cinq modules représentés dans la figure ci-dessous :

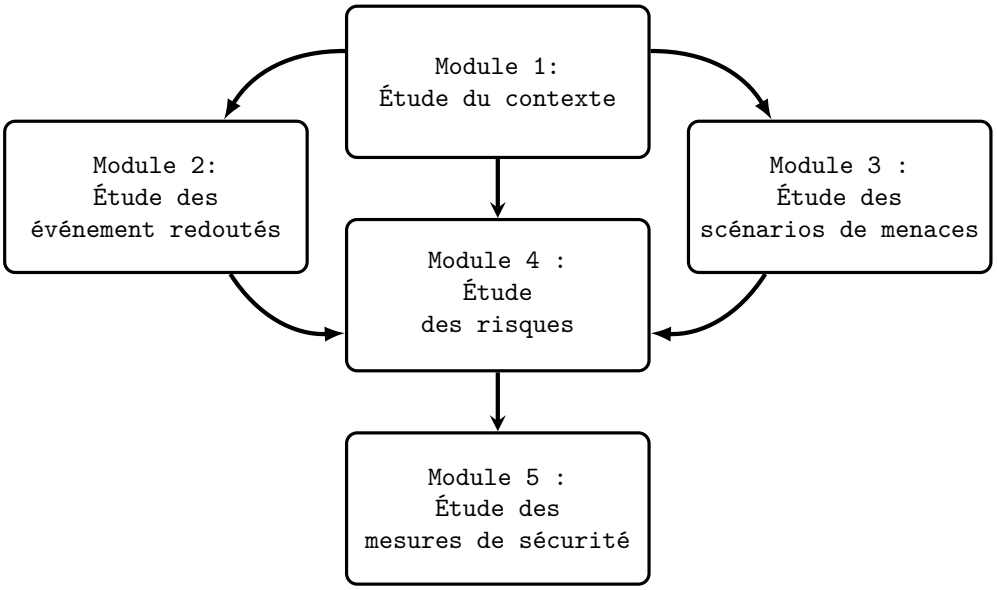


FIGURE III.6 – Les cinq modules de la méthode de EBIOS

❶ **Étude du contexte :** concerne l'étude du contexte. Il s'agit de détailler l'organisation, les missions, les contraintes et les métiers pour rendre applicable et cohérent le choix des objectifs de sécurité. Le point suivant consiste à identifier les fonctions estimées sensibles, la perte, le dysfonctionnement ou la divulgation d'informations qui peuvent avoir des répercussions sur le bon fonctionnement de l'organisme.
Enfin, on répertorie sous forme de matrice les entités techniques propres au SMSI (matériel, logiciels, réseaux) ainsi que les entités organisationnelles (groupes de collaborateurs) pour établir les liens entre les éléments essentiels et les entités.

❷ **Étude des événement redoutés :** Cette étape permet de définir les besoins de sécurité des éléments essentiels précédemment identifiés. On quantifie les besoins sur une échelle de 0 à 4 à l'aide d'un questionnaire que l'on adresse aux collaborateurs de l'organisme. Les besoins sont sélectionnés sur des critères de sécurité tels que la disponibilité, l'intégrité, la confidentialité et la non-répudiation ainsi que sur des

critères d'impacts (interruption de services, dommages matériels).

❷ **Étude des scénarios de menaces :** elle consiste à estimer, évaluer les menaces (incendie, perte d'alimentation électrique, divulgation d'information etc.) et identifier les objectifs de sécurité qu'il faut atteindre pour les traiter. EBIOS fournit une liste de menaces que l'on associe aux éléments essentiels définis dans le module 1. Puis on attribue à chaque élément un niveau de vulnérabilité sur une échelle de 0 à 4.

❸ **Étude des risques :** cette étape permet de dresser une cartographie des risques. Elle explique aussi comment traiter le risque. Estimer, évaluer les risques puis identifier les objectifs de sécurité à atteindre pour les traiter.

❹ **Étude des mesures de sécurité :** cette dernière étape explique comment appliquer les mesures de sécurité à mettre en œuvre, comment planifier la mise en œuvre de ces mesures et comment valider le traitement des risques résiduels.

En conclusion, la méthode EBIOS par son caractère exhaustif, permet de formaliser tout le SMSI et son environnement. Cette méthode contribue à formuler une politique de sécurité du système d'information. C'est une des méthodes pour mettre en œuvre le cadre défini par l'ISO/CEI 27005. Elle répond aux exigences de l'ISO/CEI 27001 et peut exploiter les mesures de sécurité de l'ISO/CEI 27002.

III.5.4 La méthode MEHARI

La méthode *MEHARI* (Méthode Harmonisée d'Analyse de Risques) a été développée dans les années 1990 par le *CLUSIF* (Club de la Sécurité de l'Information Français). A l'origine, cette méthode ne traitait que de l'analyse des risques. Elle a évolué pour permettre une gestion de la sécurité de l'organisme dans un environnement ouvert et géographiquement réparti.[4]

MEHARI a été adoptée par des milliers d'organismes à travers le monde et reste la méthode la plus utilisée en France, en particulier dans l'industrie. L'utilisation et la distribution de son logiciel sont libres. En outre, certaines bases de connaissances sont disponibles et une étude illustre la méthode pour faciliter son utilisation.

Contrairement à la méthode EBIOS, MEHARI repose sur des scénarios de risques qui permettent d'identifier les risques potentiels au sein de l'organisme. Elle est définie comme une boîte à outils conçue pour la gestion de la sécurité. En fonction des besoins, des choix d'orientation, de politique de l'organisation ou simplement des circonstances, la méthode veille à ce qu'une solution d'appréciation des risques appropriée puisse être élaborée. La méthode est présentée sous la forme d'un ensemble que l'on appelle modules, centrés sur l'évaluation des risques et leur gestion.

III.5.4.1 Principe de fonctionnement

La méthode méhari prend avant tout en compte les informations de l'entreprise afin de développer un plan afin de mieux définir les points à protéger dans l'entreprise. MEHARI

permettra à l'entreprise de définir :

- ✦ Un plan stratégique de sécurité.
- ✦ Un plan opérationnel de sécurité par site ou entité.
- ✦ Le traitement d'une famille de scénarios ou d'un scénario particulier.
- ✦ Le traitement d'un risque spécifique (Accident, Erreur, Malveillance).
- ✦ Le traitement d'un critère de sécurité (Disponibilité, Intégrité, Confidentialité).

MEHARI, conjugue la rigueur d'une analyse des risques liés formellement au niveau de vulnérabilité du système d'information, à l'adaptabilité de la gravité des risques étudiés. En effet, la présence ou l'absence de mesures de sécurité va réduire ou non, soit la potentialité de survenance d'un sinistre, soit son impact. L'interaction de ces types de mesures concoure à réduire la gravité du risque jusqu'au niveau choisi.

FIGURE III.7 – Enjeux critique + Vulnérabilités fortes = Risques inacceptables

Cette expression très simple signifie que le management de la sécurité a pour objectif fondamental d'éviter de se trouver dans une situation telle que des vulnérabilités fortes pourraient être exploitées et conduire à des sinistres très critiques pour l'entreprise ou l'organisation qui en est victime.

Les phases de MEHARI sont les suivantes :[4]

① **Phase 1 (PSS) :** établissement d'un plan stratégique de sécurité (global) qui fournit notamment :

- ✦ la définition des métriques des risques et la fixation des objectifs de sécurité.
- ✦ l'établissement d'une politique de sécurité entreprise, l'établissement d'une charte de management et classification des ressources.

② **Phase 2 (POS) :** établissement de plans opérationnels de sécurité réalisés par les différentes unités de l'entreprise qui fournit aussi :

- ✦ Audit de l'existant.
- ✦ Evaluation de la gravite des scénarios.

- ✦ Expression des besoins de sécurité et construction du plan opérationnel de sécurité.

③ **Phase 3 (POE) :** consolidation des plans opérationnels (Plan global) qui fournit :

- ✦ Choix d'indicateurs représentatifs.
- ✦ Elaboration d'un tableau de bord de la sécurité de l'entreprise.
- ✦ Rééquilibrage et arbitrages entre unités.

III.5.4.2 Mise en place de la méthode

MEHARI se présente comme un ensemble cohérent d'outils et de méthodes de management de la sécurité, fondés sur l'analyse des risques. Les deux aspects fondamentaux de MEHARI sont le modèle de risque (qualitatif et quantitatif) et les modèles de management de la sécurité basés sur l'analyse de risque. MEHARI vise à donner des outils et des méthodes pour sélectionner les mesures de sécurité les plus pertinentes pour une entreprise donnée.

Les différentes phases ont pour objectif d'établir le contexte d'entreprise, d'identifier les actifs et les menaces, d'analyser les risques et enfin de définir les mesures de sécurité (traitement du risque).

A) Plan stratégique :

C'est le plan qui examinera l'entreprise sur un aspect général. Les aspects qui seront pris en compte lors de cette analyse sont : la classification des ressources de l'entreprise, l'ensemble des risques existants et ses objectifs en terme de sécurité.

① **Mettre en avant les risques possibles :** lors de l'audit nous allons donc répertorier les risques pouvant pénaliser l'activité de l'entreprise. Ensuite pour chacun des risques détectés on définit :

- ✦ **Son potentiel :** c'est-à-dire la capacité de destruction. C'est pour cela que l'on mettra en place des tests ou plus précisément des scénarios qui permettent de se mettre en situation et dévaluer ce potentiel.
- ✦ **Son impact :** en clair, une fois la catastrophe arrivée concrètement quel seront les dégâts réels.
- ✦ **Sa gravité :** déterminer si vraiment les dégâts son handicapants pour l'entreprise et son fonctionnement.

② **Limite d'acceptabilité :** de part ces caractéristiques il faut mettre en place une échelle pour le degré d'acceptabilité non seulement sur le plan de la gravité mais aussi du temps. Combien de temps l'entreprise pourra être dans cette handicape sans que cela devienne dangereux pour sa survie.

③ **Les ressources de l'entreprise :** lors de cette étape il faut définir les valeurs de l'entreprise, quels services génèrent le plus de chiffre d'affaire, ou sont vital pour le fonctionnement de la société.

④ **Solution et indicateurs :** C'est l'étape finale, c'est lors de celle-ci qu'il faut mettrre en place dans un premier temps les indicateurs afin de prévenir au maximum l'arrivée d'une catastrophe. Que l'on regroupera toutes les informations récupérées et qui seront analysées de façon globale afin de pouvoir mettre en œuvre des solutions : règles de sécurité et de responsabilité. Les solutions s'appliquent sur plusieurs niveaux.

Ce découpage permet un regroupement des mesures en six grandes familles :

❶ **Les mesures structurelles :** qui jouent sur la structure même du système d'information, pour éviter certaines agressions ou en limiter la gravité.

❷ **Les mesures dissuasives :** qui permettent, dans le cas d'agresseurs humains, d'éviter qu'ils mettent à exécution la menace potentielle en déclenchant l'agression.

❸ **Les mesures préventives :** celles qui permettent d'empêcher les détériorations ou d'éviter qu'une agression n'atteigne des ressources du système d'information.

❹ **Les mesures de protection :** qui, sans empêcher les détériorations, permettent tout au moins d'en limiter l'ampleur.

❺ **Les mesures palliatives :** qui agissent une fois les détériorations accomplies, et qui permettent, d'une part d'en limiter les conséquences au niveau de l'entreprise, d'autre part de restaurer les ressources détériorées pour retrouver l'état initial.

❻ **Les mesures de récupération :** qui visent à récupérer une partie du préjudice subi par transfert des pertes sur des tiers, par le biais des assurances ou de dommages et intérêts consécutifs à des actions en justice, dans le cas d'agresseurs humains.

Les tableaux qui suivent sont à titre d'exemple de Métrique des risques et objectifs de sécurité lors d'une réunion avec une Direction Générale et les directions opérationnelles d'une entreprise. Les différentes grilles de status sont validés et fourni par la méthode MEHARITM et par le logiciel RISICARE.[9]

Table III.3 – Mesures de récupération

STATUS-RÉCUP	Effet des mesures prises sur l'impact du scénario
1	Effet très faible : ce que l'on peut espérer récupérer des assurances ou d'un recours en justice est négligeable devant l'ampleur des dégâts subis.
2	Effet moyen : ce que l'on peut raisonnablement espérer récupérer n'est pas négligeable, mais les sinistres majeurs restent à la charge de l'entreprise (sinistre non couvert et responsable non solvable).
3	Effet important : l'entreprise est couverte pour les sinistres majeurs, mais ce qui reste à sa charge (franchise) demeure important quoique supportable.
4	Effet très important : l'entreprise est suffisamment couverte pour que l'impact financier résiduel soit négligeable.

Table III.4 – Mesures de protection

STATUS-PROT	Effet des mesures de protection sur l'impact du scénario
1	Effet de protection très faible : le sinistre ne sera détecté qu'au bout d'un délai important. Les mesures qui pourront alors être prises ne pourront limiter la propagation de l'incident initial et se limiteront à la borner dans le temps. L'étendue des conséquences du sinistre est difficilement à cerner.
2	Effet de protection moyen : le début de sinistre ne sera pas identifié très vite et les mesures prises le seront tardivement. Le sinistre aura pris une grande ampleur mais l'étendue de ses conséquences sera encore identifiable.
3	Effet important : le sinistre sera détecté rapidement et des mesures de protection seront prises sans délai. Le sinistre aura néanmoins eu le temps de se propager, mais les dégâts seront circonscrits et facilement identifiables.
4	Effet très important : le début de sinistre sera détecté en temps réel et les mesures déclenchées immédiatement. Le sinistre sera limité aux détériorations directes provoquées par l'accident, l'erreur ou la malveillance.

Table III.5 – Mesures dissuasives

STATUS-DISS	Effet des mesures dissuasives sur la potentialité du scénario
1	Effet très faible : L'auteur n'encourrait aucun risque : il n'a pratiquement aucun risque d'être identifié et de toutes façons cela n'aurait pour lui aucune conséquence.
2	Effet moyen : L'auteur encourrait un risque faible : le risque d'être identifié est faible et les sanctions éventuelles, s'il était découvert, resteraient supportables.
3	Effet important : L'auteur de l'erreur ou de la malveillance encourrait un risque important : il existe une forte probabilité qu'il soit découvert et les sanctions encourues pourraient être graves.
4	Effet très important : Seul un inconscient pourrait courir un tel risque : il sera démasqué à coup sûr, les sanctions seront très lourdes et tout cela est bien connu.

Table III.6 – Mesures palliatives

STATUS-PALL	Effet des mesures palliatives sur l'impact du scénario
1	Effet très faible : les solutions de secours éventuellement nécessaires doivent être improvisées. Il n'est pas assuré que les activités de l'entreprise touchées par le sinistre pourront être poursuivies. L'activité de l'ensemble des acteurs touchés par le sinistre est très fortement perturbée.
2	Effet moyen : les solutions de secours ont été prévues globalement et pour l'essentiel, mais l'organisation de détail reste à faire. Les activités principales touchées pourront se poursuivre après un temps d'adaptation qui peut être long. La reprise des autres activités et le retour à l'état d'origine demandera des efforts importants et occasionnera une forte perturbation des équipes.
3	Effet important : les solutions de secours ont été prévues, organisées dans le détail et validées. Les activités principales pourront se poursuivre après un temps de reconfiguration acceptable et connu. La reprise des autres activités et le retour à l'état d'origine ont également été prévus et se dérouleront avec des efforts importants mais supportables.
4	Effet très important : le fonctionnement des activités de l'entreprise est assuré sans discontinuité notable. La reprise de l'activité en mode normal est planifiée et sera assurée sans perturbation notable.

Table III.7 – Le STATUS-RI, déduit de la grille propre au critère de sécurité considéré (D, I, ou C), est défini selon le tableau standard ci-après :

STATUS-RI	Effet des mesures prises sur la réduction d'impact du scénario
1	Effet très faible
2	Effet moyen : impact maximum jamais supérieur à un impact grave : I<ou = 3
3	Effet important : impact maximum jamais supérieur à un impact moyennement grave : I<ou= 2
4	Effet très important : impact du scénario toujours négligeable quel que soit l'impact intrinsèque

Table III.8 – Exposition naturelle

STATUS-EXPO	Effet des mesures structurelles sur la potentialité du scénario
1	Exposition très faible : Des mesures architecturales ont été prises pour limiter structurellement les risques : cloisonnement des locaux, fragmentation des informations, rendant négligeable la probabilité d'un risque majeur
2	Exposition faible : L'entreprise (le service ou l'unité) est particulièrement peu exposée : le climat social est très favorable, l'environnement ne laisse pas craindre le moindre problème, la position de suiveur de l'entreprise rend peu probable une agressivité notable de concurrents.
3	Exposition moyenne : L'entreprise (le service ou l'unité) n'est pas particulièrement exposée. Le climat social n'est pas mauvais, la concurrence est normalement agressive sans plus, l'environnement ne présente pas de menace particulière.
4	Exposition importante : L'entreprise (le service ou l'unité) est particulièrement exposée au risque envisagé de par un climat social est très défavorable ou un environnement à risque ou une position telle que l'on peut craindre des réactions spécialement agressives de la concurrence.

Table III.9 – Mesures préventives

STATUS-PREV	Effet des mesures préventives sur la potentialité du scénario
1	Effet très faible : Toute personne de l'entreprise ou tout initié la connaissant un minimum est capable de déclencher un tel scénario, avec des moyens qu'il est facile d'acquérir. Des circonstances tout à fait courantes (maladresse, erreur, conditions météo défavorables rares mais n'ayant rien d'exceptionnel) sont à même de déclencher un tel scénario.
2	Effet moyen : Le scénario peut être mis en oeuvre par un professionnel sans autres moyens que ceux dont font usage les personnels de la profession. Des circonstances naturelles rares mais non exceptionnelles peuvent aboutir à ce résultat.
3	Effet important : Seul un spécialiste ou une personne dotée de moyens importants décidée à y consacrer du temps peut aboutir dans la réalisation d'un tel scénario. Des concours de circonstances peuvent rendre le scénario plausible.
4	Effet très important : Seuls quelques experts sont capables, avec des moyens très importants, de mettre en oeuvre un tel scénario. Au niveau des événements naturels, seules des circonstances exceptionnelles peuvent conduire à de tels résultats (catastrophes naturelles).

Table III.10 – Le niveau de la potentialité "P" est apprécié conformément à la grille standard ci-après

STATUS-P	Potentialité
1	Potentialité faible,ne surviendra sans doute jamais
2	Possible, bien que potentialité faible
3	Potentialité certaine, devrait arriver un jour
4	Très forte potentialité, surviendra sûrement à court terme

Table III.11 – La grille suivante, proposée en standard, permet d'évaluer l'impact "I"

STATUS-RI/Classification de la ressource	1	2	3	4
1	1	2	3	4
2	1	2	3	4
3	1	2	3	4
4	1	2	3	4

La figure suivante a pour but de classifier les ressources de l'entreprise [9]

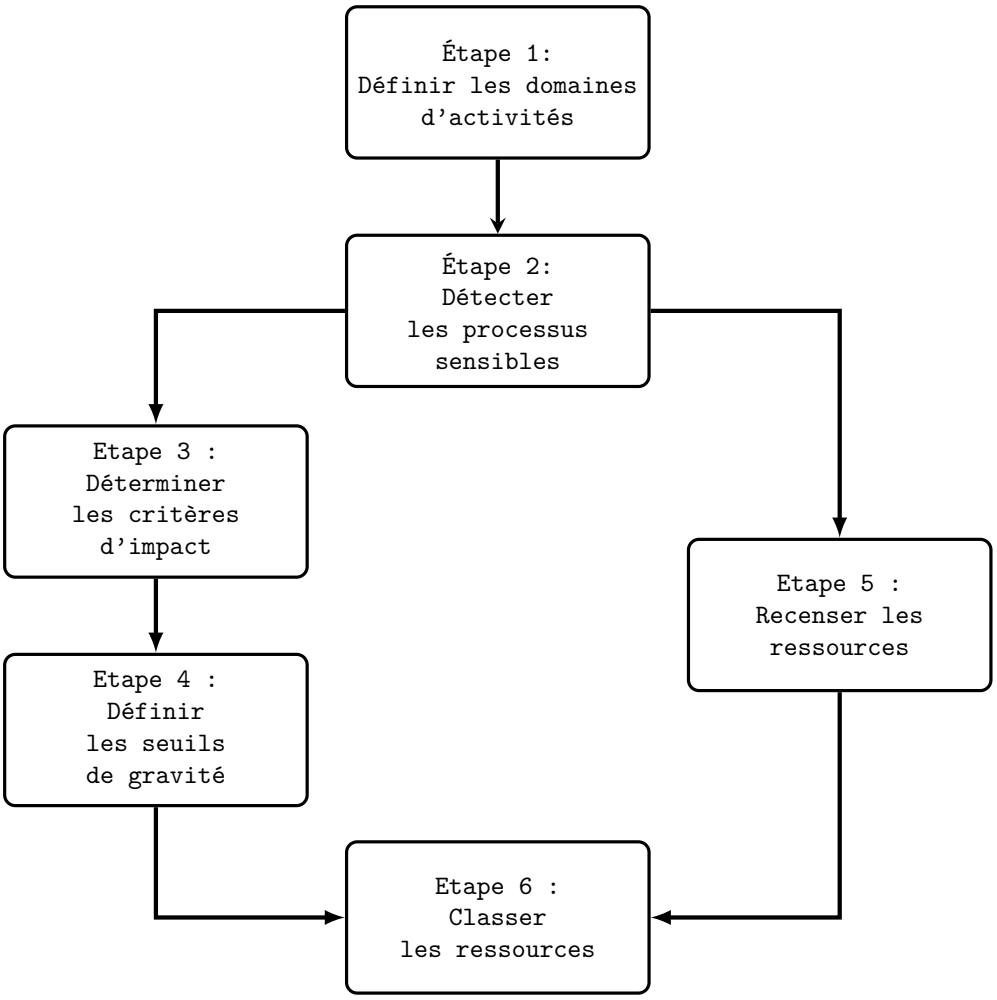


FIGURE III.8 – Classification des ressources de l'entreprise

B) Plan opérationnel de sécurité :

le plan opérationnel est obligatoirement précédé d'un plan stratégique dans la mesure où la définition d'une métrique des risques et une classification des ressources sont indispensables, quelle que soit l'importance de l'entreprise considérée, à l'évaluation des risques et à la détermination objective des besoins en services de sécurité.

L'élaboration d'un plan opérationnel de sécurité résulte soit :[9]

- de la décision d'une unité indépendante ou d'un responsable d'activité (cas des petites entreprises, professions libérales, etc.). Dans ce cas, on peut considérer que, bien que faisant l'objet d'étapes préalables spécifiques (impérativement la définition de la métrique des risques et la classification des ressources), le plan stratégique sera pratiquement intégré dans le plan opérationnel.
- de la décision d'une unité autonome, qui devra se plier aux exigences définies dans le plan stratégique aux fins de coordination et de cohérence.

- ✦ de la mise en oeuvre de la politique de sécurité décidée au niveau central et dont le plan opérationnel est un des composants.

Le plan opérationnel peut être élaboré (voir la figure III.9) :

- ✦ Soit à partir d'une *approche analytique* basée sur un audit des services de sécurité en place assuré principalement, parce que ce sont eux qui en ont la meilleure connaissance par des techniciens.
- ✦ Soit à partir d'une évaluation des facteurs de risque, c'est à dire d'une appréciation de leur incidence sur la gravité du risque. Une telle *approche globale*, fait d'abord appel à l'appréciation et au raisonnement des utilisateurs des systèmes informatiques.

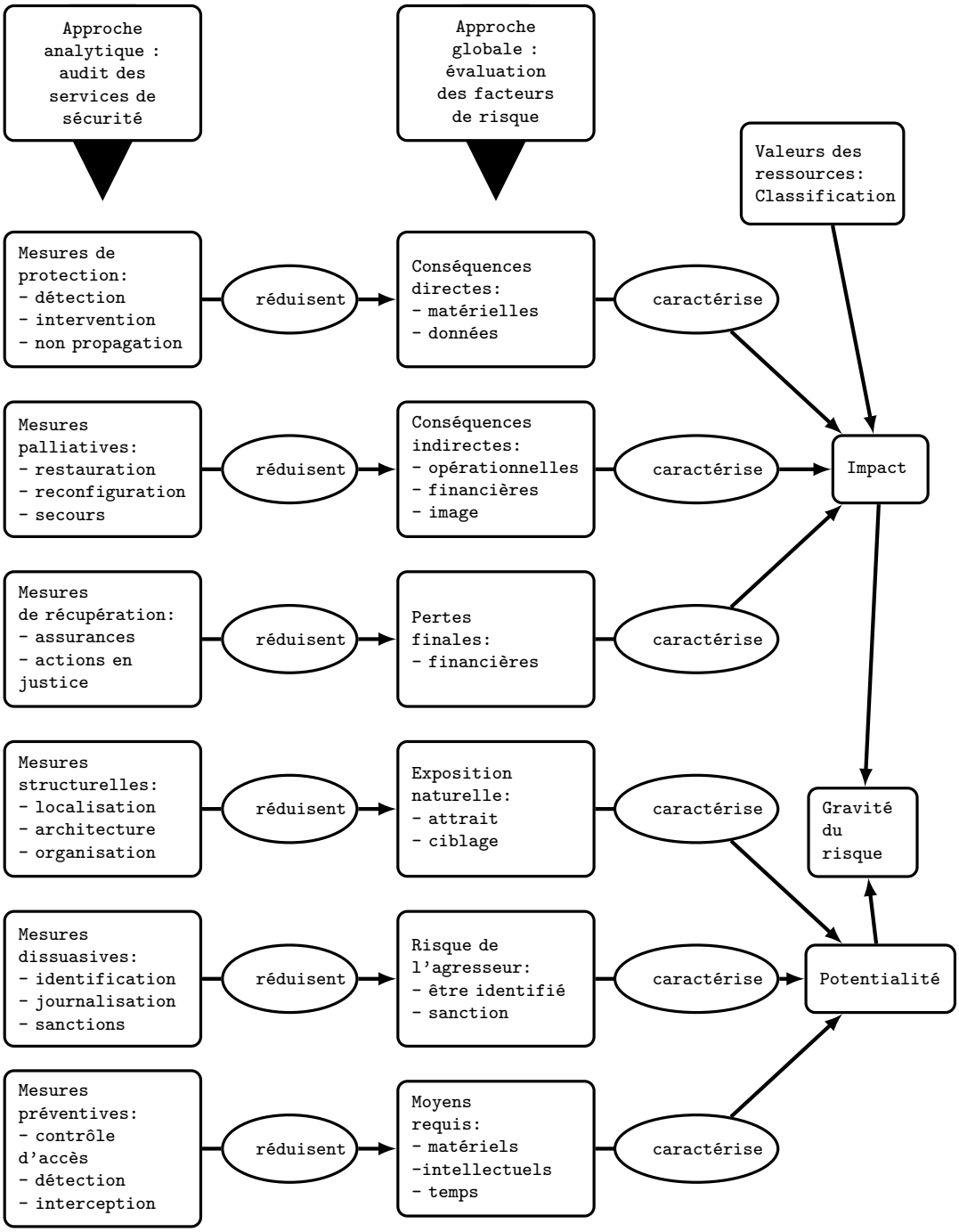


FIGURE III.9 – Exemple d'étude de cas plans Opérationnels de Sécurité

C) Plan opérationnel d'entreprise :

Dans cette étape il s'agit fondamentalement de mettre en place des scénarios sur les impacts et les conséquences que peuvent avoir ces sinistres sur le bon fonctionnement de l'entreprise. Cette partie conclue la boucle de l'application de la méthode Méhari par la mise en place d'un outil permettant le suivi des opérations à effectuer afin d'améliorer la sécurité de la société.

Pour que cette stratégie soit couronnée de succès, il est nécessaire de s'assurer que :

- ✦ Elle est connue et comprise par la Direction et le personnel de l'entreprise.
- ✦ Elle est pilotée et sa mise en œuvre est assurée et mesurée.
- ✦ Elle reste pertinente dans le temps.
- ✦ Elle se décline en objectifs stratégiques reliés à des objectifs tactiques (ensemble des initiatives, projets, processus et organisation) qui forment un tout cohérent et contribuent pleinement à l'atteinte de la couverture des risques.
- ✦ Elle est financée et que les budgets sont affectés avec l'assurance de leur meilleure contribution au succès de cette stratégie.

Bénéfices :

- ✦ Les objectifs poursuivis par la stratégie sécurité sont conformes à ceux de l'entreprise.
- ✦ Impact sur l'image véhiculée par la SSI.
- ✦ Pilotage et mesure dans la durée de la stratégie sécurité sur l'ensemble de ses aspects, en privilégiant le caractère stratège du RSSI (Responsable de la Sécurité de Système d'informations).
- ✦ Intégration des aspects stratégiques et opérationnels.

III.5.4.3 La démarche MEHARI :

La figure ci-dessous montre La démarche MEHARI.

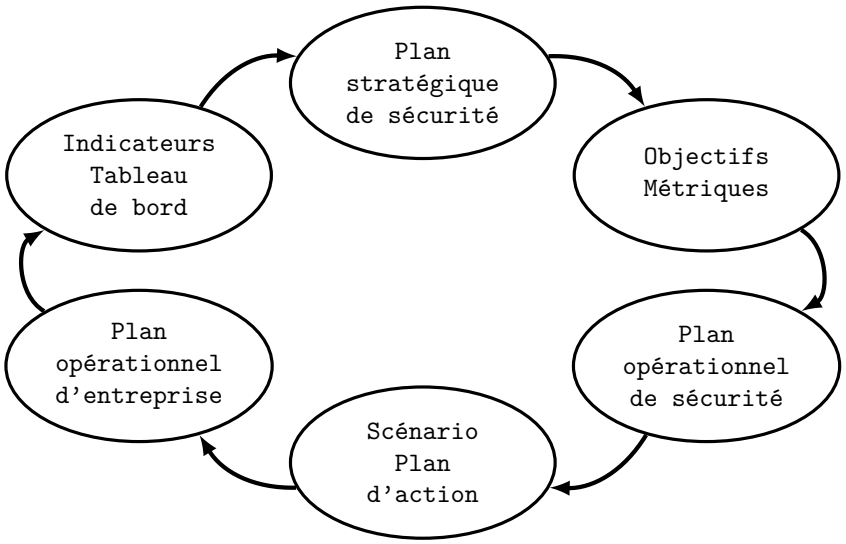


FIGURE III.10 – La démarche MEHARI

III.5.4.4 Traitement des risques :

La troisième étape concerne le choix du traitement des risques. L'ISO/CEI 27001 a identifié quatre traitements possibles du risque, l'acceptation, l'évitement, le transfert et la réduction.

① « **Accepter** » le risque revient à ne déployer aucune mesure de sécurité autre que celles déjà en place. Cette décision peut être justifiée si le vol de données dans un cas précis n'a pas d'impact sur l'organisme.

② « **Eviter** » le risque consiste à supprimer par exemple l'activité ou le matériel offrant un risque.

③ « **Transférer** » un risque par souscription d'une assurance ou par sous-traitance. Ces moyens de transfert du risque sont souvent employés quand l'organisme ne peut ou ne souhaite pas mettre en place les mesures de sécurité qui permettraient de le réduire.

④ « **Réduire** » le risque consiste à prendre des mesures techniques et organisationnelles pour ramener à un niveau acceptable le risque. C'est le traitement le plus courant.

Il existe d'autres traitements du risque possibles mais pour être en conformité avec la norme, il faut en priorité considérer ceux que nous venons de citer.

Après avoir sélectionné le traitement et mis en place les mesures de sécurité, un risque peut persister. Il convient de traiter ce risque comme les autres c'est-à-dire, l'accepter, l'éviter, le transférer ou le réduire.

III.5.4.5 Sélection des mesures de sécurité :

L'étape 4 est la dernière étape de la phase « Plan » du PDCA, elle consiste à sélectionner les mesures de sécurité. La norme ISO/CEI 27001 propose dans son annexe A, 133 mesures de sécurité réparties sur onze chapitres. A ce stade, le travail consiste à dresser un tableau SoA dans lequel figurent les 133 mesures qu'il faut déclarer applicables ou non applicables, pour réduire les risques du SMSI.

Notons que les 133 mesures proposées par l'ISO/CEI 27001 répertorient presque tout ce qui peut être entrepris en matière de sécurité de l'information. Cependant, cette liste ne comporte pas d'exemples ni d'explications sur le déploiement des mesures à entreprendre. L'ISO/CEI 27002 répond en partie à ce besoin en fournissant une série de préconisations et d'exemples techniques et organisationnels qui couvrent la liste de l'ISO/CEI 27001.

Une fois choisie la politique et le périmètre du SMSI, apprécié et traité les risques, et sélectionné les 133 mesures de sécurité dans le tableau SoA, il faut mettre en œuvre les objectifs fixés de la phase « Plan » du PDCA. Il s'agit de la phase « Do » du PDCA.

III.5.5 Phase Do

Cette phase consiste à décrire la mise en œuvre des mesures de sécurité sélectionnées dans le SoA à travers quatre étapes.

III.5.5.1 Plan de traitement

Il faut premièrement gérer l'interdépendance des actions à entreprendre. Certaines mesures sont partiellement ou déjà en place, d'autres doivent être intégralement déployées ou nécessitent la mise en œuvre d'une autre action avant de pouvoir être lancées. Ce travail revient à établir un plan de traitement qui peut être assimilé à de la gestion de projet. Une fois ce travail effectué, il faut déployer les mesures de sécurité en suivant le plan de traitement.

Par la suite, le responsable de projet doit définir des « mesures d'efficacité » pour contrôler le bon fonctionnement du SMSI.

III.5.5.2 Choix des indicateurs

Ce point consiste à mettre en place des indicateurs de performance pour vérifier l'efficacité des mesures de sécurité ainsi que des indicateurs de conformité pour contrôler la conformité du SMSI. Trouver de bons indicateurs n'est pas une tâche facile.

La norme ne préconise pas d'indicateurs précis à utiliser mais l'ISO/CEI 27004 propose une démarche qui peut aider à les sélectionner.

L'étape suivante concerne la sensibilisation des collaborateurs aux principes de la sécurité de l'information.

III.5.5.3 Formation et sensibilisation des collaborateurs

Les mesures de sécurité couvrent de nombreux domaines allant de la sécurité organisationnelle à la sécurité physique, en passant par la sécurité des systèmes réseaux etc. Les collaborateurs doivent maîtriser les outils de sécurité déployés dans les domaines très variés. Une formation du personnel peut s'avérer nécessaire.

La sensibilisation à la sécurité du système d'information concerne tous les collaborateurs. Elle peut débuter par un rappel des engagements de leur entreprise en matière de sécurité et se poursuivre par une liste de conseils tels que le respect de certaines règles de sécurité pour les mots de passe et l'environnement de travail.

III.5.5.4 Maintenance du SMSI

La maintenance consiste à garantir le bon fonctionnement de chacun des processus du SMSI et vérifier que leur documentation est à jour. Cela permet à l'auditeur externe de contrôler la gestion du SMSI. Il est à noter que tous les systèmes de management ISO sont concernés par la maintenance.

A ce stade de l'avancement du SMSI, les mesures identifiées du SoA fonctionnent, les

indicateurs sont implémentés et les collaborateurs de l'organisme formés et sensibilisés à la sécurité du SMSI, nous pouvons poursuivre avec la phase *« Check »* du PDCA.

III.5.6 Phase Check

La phase « Check » du PDCA concerne les moyens de contrôle à mettre en place pour assurer «l'efficacité » du SMSI et sa « conformité » au cahier des charges de la norme ISO/CEI 27001. Pour répondre à ces deux exigences de la norme, les organismes emploient le contrôle et les audits internes ainsi que les revues de direction.

III.5.6.1 Les audits internes

L'audit interne peut s'organiser avec le personnel de l'organisme ou être sous-traité à un cabinet conseil. Si l'audit est confié à un collaborateur, il ne faut pas que ce dernier puisse auditer un processus dans lequel il est impliqué au niveau de sa mise en œuvre ou de son exploitation. L'audit a pour but de contrôler la conformité et l'efficacité du SMSI en recherchant les écarts entre la documentation du système (enregistrement, procédures, etc.) et les activités de l'organisme. La norme exige que la méthode utilisée pour l'audit soit documentée dans une procédure et que les rapports soient enregistrés pour être utilisés lors des revues de direction.

III.5.6.2 Les contrôles internes

L'objectif du contrôle interne est de s'assurer au quotidien que les collaborateurs appliquent correctement leurs procédures. Contrairement à l'audit interne qui est planifié longtemps à l'avance, les contrôles internes sont inopinés.

III.5.6.3 Revues de direction

La revue est une réunion annuelle qui permet aux dirigeants de l'organisme d'analyser les événements qui se sont déroulés sur l'année en cours. Les points passés en revue sont généralement :

- ✦ Les résultats des audits.
- ✦ Le retour des parties prenantes.
- ✦ L'état des lieux sur les actions préventives et correctives.
- ✦ Les menaces mal appréhendées lors de l'appréciation des risques.
- ✦ L'interprétation des indicateurs et les changements survenus dans l'organisme.

À partir de ces informations la direction peut fixer de nouveaux objectifs et allouer de nouvelles ressources (financières, humaines et matérielles).
Les contrôles de la phase « Check » peuvent faire apparaître des dysfonctionnements du SMSI. Cela peut être un écart entre les exigences de la norme et le système de management ou des mesures de sécurité inefficaces.

C'est dans la phase *« Act »* du PDCA que l'on réduit les dysfonctionnements par des actions correctives, préventives ou d'améliorations.

III.5.7 Phase Ack

III.5.7.1 Actions correctives

On intervient de manière « corrective » lorsqu'un dysfonctionnement ou un écart est constaté. On agit premièrement sur les effets pour corriger cet écart ou dysfonctionnement, puis sur les causes pour éviter qu'ils ne se répètent.

III.5.7.2 Actions préventives

On emploie les actions préventives quand une situation à risque est détectée. On agit sur les causes avant que l'écart ou le dysfonctionnement ne se produisent.

III.5.7.3 Actions d'améliorations

Les actions d'améliorations ont pour objectif l'amélioration de la performance du SMSI. Les résultats des différentes actions doivent être enregistrés et communiqués aux parties prenantes. Ces actions contribuent à rendre plus efficace et performant le SMSI.

III.6 Conclusion

Dans Ce troisième chapitre qu'est si riche que l'on peut beaucoup spéculer sur la méthodologie et les références en matière de sécurité informatique, mais il s'avère qu'un système de gestion de la sécurité de l'information ne devrait être figé ,En d'autres termes, c'est un système qui doit persister dans le temps, plutôt que d'être mis en œuvre une seule fois. La norme ISO/IEC 27001 est donc la norme prééminente qui met l'accent sur le modèle PDCA (Contained Improvement) et permet une mise en œuvre efficace. Activez votre ISMS pour suivre le rythme des cyberattaques. Le jour où vous découvrez une nouvelle vulnérabilité.

ChapitreIV

Les Attaques réseau

IV.1 Introduction

Ce chapitre décrit les différentes attaques susceptibles d'affecter un réseau et les systèmes qui le composent. Avec la généralisation d'Internet et des moyens de communication modernes, une nouvelle forme d'insécurité s'est répandue, qui s'appuie sur l'utilisation de codes informatiques pour perturber ou pénétrer les réseaux et les ordinateurs.

Comme l'illustre la figure ci-dessous, les attaques touchent généralement les trois composantes suivantes d'un systèmes : la couche réseau, en charge de connecter le système au réseau, le système d'exploitation , en charge d'offrir un noyau de fonction au système, et la couche applicative, en charge d'offrir des services spécifiques.

Toutes ces composants d'un système constituent autant de moyens de pénétration pour des attaques de toute nature.

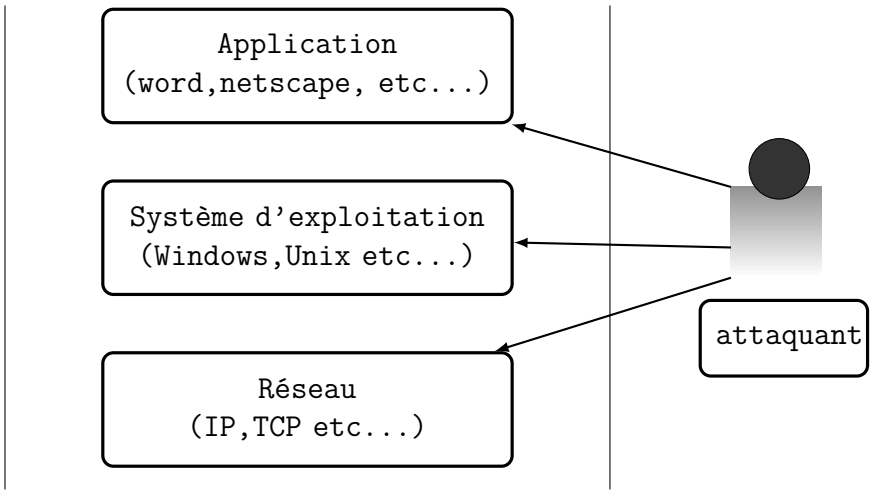


FIGURE IV.1 – Les composantes d'un système susceptible d'être attaquées

IV.2 Connaître son ennemi

IV.2.1 Chaque attaque à son chapeau

IV.2.1.1 Les hackers black hats

Les hackers *black hats*, désignent généralement dans le domaine informatique les hackers révoltés contre le système, qui frôlent les limites de la loi, ou les dépassent carrément.[8]

Ils pénètrent par effraction dans les systèmes, dans un intérêt qui n'est pas celui des propriétaires du réseau ou du système, mais plutôt personnel, voire financier.

Parmi ces hackers, il y a les crackers, qui ont une nette attirance pour ce côté obscur. Ils sont par exemple à l'origine de virus, de chevaux de troie ou de logiciels espions.

Lorsque cela est fait dans le but de nuire à une organisation ou à des individus, on parle aussi de terrorisme ou de *cyberterrorisme*.

Il arrive également que les compétences des hackers black hats intéressent fortement les grandes entreprises, qui finissent par les débaucher pour travailler en collaboration avec eux.

Cependant la communauté des black hats est assez large et posséde des convictions, des opinions et des connaissances bien différentes. Le terme de "black hat" ne veut pas dire sans éthique ni morale. Généralement les techniques sont les mêmes que celle des white hat, seul la fin peu être différente.

IV.2.1.2 Les hackers white hats

Techniquement, l'action menée par les white hats est très proche de celle des black hats. Cependant, elle se différencie par le but ou la finalité.

En effet, les « white hackers » ont plutôt comme ambition d'aider à la sécurisation du système, sans en tirer profit de manière illicite. Les white hats bricolent et testent les systèmes d'information pour découvrir les vulnérabilités pas encore connues ou non publiques, les « 0 day » (zéro day, zéro jour). La technique employée est la même que pour un hacker au chapeau noir.

Leur atttitude est par contre différente lors de la découverte de cette vulnérabilité. La question qui se pose alors est de savoir s'il faut rendre une vulnérabilité publique ou non. Les hackers au chapeau blanc prônent la divulgation totale de la découverte, ce que l'on appelle en anglais la full disclosure, là où les hackers au chapeau noir préfèrent restreindre l'accès à cette information et ne pas la divulguer.

Les white hats rendent alors publiques les vulnérabilités, et parfois même les exploits, qui sont les bouts de code permettant de tester la vulnérabilité d'un système à cette faille. Cela se fait sur des outils en ligne spécialisés comme des listes de diffusion ou des outils de gestion de bug (bugtracking).

Le problème qui en résulte est que ces codes sont également rendus disponibles pour quiconque, dont les script-kiddies.

Cependant, un white hat met également au courant les auteurs des vulnérabilités qui les touchent (lorsqu'ils n'agissent pas dans le cadre d'une mission d'audit qui explique leurs actions), contrairement aux black hats.

Même si les white hats disent agir dans la légalité et pour la bonne cause, en réalité depuis que la loi sur l'économie numérique, la LCEN (Loi pour la Confiance dans l'Economie Numérique), a été votée en France, seule l'intention reste réellement bonne. Ces hackers sont considérés également hors la loi puisque le fait de divulguer des vulnérabilités et des exploits sur Internet est dès lors devenu répréhensible. Cette loi contredit ainsi de plein fouet l'éthique hacker et également le principe du logiciel libre.

IV.2.1.3 Les hackers grey hats

Le hacker au chapeau grey est un peu un hybride du chapeau blanc et du chapeau noir.

Il s'agit d'un hacker compétent, qui agit parfois avec l'esprit d'un white hat mais avec une philosophie de divulgation différente.

Son intention n'est pas forcément mauvaise même s'il commet cependant occasionnellement un délit.

Par curiosité, par exemple il tentera de s'infiltrer dans un système. Une fois la faille trouvée, il n'endommagera pas le système, et préviendra généralement le propriétaire. Cependant ceci reste illégal dans la plupart des pays car il est interdit de pénétrer dans un réseau privé qui n'est pas le sien sans l'approbation de propiétaire.

De plus, il préviendra également au même temps la communauté en divulgant la faille. Beaucoup de hackers qui se disent white hats s'apparentent en réalité plus à des grey hats, dans le sens ou ils divulguent des failles aussitôt qu'elles ont été découvertes, sans prévenir ou laisser le temps nécessaire au responsable pour corriger le problème, ce qui peut nuire gravement au système ciblé indirectement.

IV.2.1.4 Les « script kiddies »

Dans le problème lié à la publication sur Internet des vulnérabilités découvertes, on trouve l'un des éléments clés de la discorde, les *script kiddies*, autrement dit des jeunes pirates néophytes.

Ces individus récupèrent les exploits laissés par les white hats sur les outils publics et les exécutent sur des machines, sans aucune connaissance, dans le but de provoquer des pannes volontaires, des *mass-root.*

Généralement un script kiddie est un jeune adolescent, pénétrant par effraction dans un système, après avoir étudié/lu dans des livres ou sur Internet quelques documentations de base sur le sujet de la sécurité informatique. Le script kiddie n'a aucune notion de l'éthique d'un hacker, il agit par vantardise auprès de ses copains, il n'est pas rare par exemple qu'il demande à "pirater un compte de messagerie instantanée".

Le script kiddie n'a pas de réelles connaissances, il ne fait que réutiliser des codes ou des programmes prêts à l'emploi, il réutilise sans comprendre les enjeux.

Mais les script kiddies sont craints, puisque malgré leur faible niveau, le fait qu'ils utilisent le code des autres représente parfois une menace réelle pour un système, surtout qu'ils sont nombreux et peu soucieux des dégâts qu'ils occasionnent. Cependant ils sont trop souvent confondus avec les réels hackers.

Ils sont également rejetés complètement des communautés underground, où ils sont considérés comme des lamers, c'est-à-dire des personnes dénuées de compétences.

IV.2.1.5 Les hackers universitaires

Ce sont des hackers libres, que l'on associe au mouvement Open Source du logiciel libre. Cette définition du hacker libre est apparue au MIT, le Massachusetts Institute of Technology.

Le hacker est alors défini comme quelqu'un qui partage sa connaissance avec autrui, sur le fonctionnement d'un système, des ordinateurs et des réseaux. Ces hackers prônent la pensée selon laquelle l'information est libre et n'appartient à personne. Ainsi, toute nouvelle connaissance se veut d'être partagée avec tout le monde.

Ces hackers forment une grande communauté qui partage la même culture et qui compte des programmeurs aux compétences aiguisées, des spécialistes des réseaux et des technologies. Les hackers travaillent ensemble et ainsi sont à l'origine de grandes œuvres, comme Internet ou encore Usenet, ou le système d'exploitation Unix.

En 1984 , Steven Levy a défini "l'éthique hacker" selon les principes suivants :

- ✦ Toute information est par nature libre et gratuite.
- ✦ L'accès aux ordinateurs devrait être total, illimité, possible pour tout le monde.
- ✦ La décentralisation des données doit être encouragée.
- ✦ Les hackers devraient être jugés sur le hacking, non pas sur des hiérarchies sociales telles que le diplôme, l'âge ou le grade.
- ✦ On peut créer de l'art et de la beauté avec un ordinateur.
- ✦ Les ordinateurs peuvent améliorer la vie.

IV.2.2 À chaque audit sa boîte à secrets

Lors d'un test d'intrusion où une entreprise fait appel à un spécialiste pour auditer son système, il y a plusieurs façons de faire les choses. Soit l'auditeur n'a accès à aucune information, soit on lui fournit quelques informations, soit il a en sa possession toutes les informations qu'il souhaite. Ces tests sont plus ou moins long, plus ou moins complets et plus ou moins onéreux. Lidéal etant bien sûr de réaliser ces trois type de tests en complémentarité afin de réaliser un test complet.

IV.2.2.1 Les tests en black box

C'est la mèthode la plus réaliste, car c'est elle qui correspond à une situation réelle, est un test en *black box*, un test en boîte noir. Dans ce cas, le hacker qui vient auditer le système n'a aucune information. Il va agir comme le ferait un attaquant, en testant tour à tour les différentes portes à la recherche d'une vulnérabilité à exploiter.

Il peut être dirigé vers quelques vulnérabilités probables à tester de manière plus approfondie mais ne sera pas plus informé qu'un hacker externe.

Ces tests "à l'aveugle" ont pour principaux avantages d'être réalistes, moins onéreux, et plus rapides. Cependant ils sont également moins exhaustifs, et ne testent pas la qualité de la configuration du système (les services sont-ils optimisés ? À jour ? Limités ?). En

effet, un système peut être non optimisé sans être vulnérable à un instant T ; cependant une mauvaise configuration peut conduire à des problèmes postérieurs.

Le test en boîte noir peut être exécuté depuis l'extérieur ou dedpuis l'intérieur, c'est à dire dans les locaux. Généralement, la sécurité n'est dans ce cas pas la même, les droits et autorisations sont moins restreints mais peuvent constituer des portes d'entrée supplémentaire. Le système pourrait donc être étanche à l'extérieur mais vulnérable à l'intérieur : un visiteur malveillant dans vos locaux pourrait s'introduire dans votre système avec quelque ficelles bien conues de *Social Engineering*.

IV.2.2.2 Les tests en grey box

Lors d'un audit en *grey box* le consultant ne posséde qu'une quantité limitée d'information. Cela va ouvrir d'autres portes sans pour autant donner toute les informations. Il permettra d'aller in peu plus loin dans le test, de parcourir d'autres domaines...

Par exemple lors de l'audit d'un site interne ou d'un intranet, le test en black box serait un accès au site sans aucune information, comme lors d'une attaque en situation réelle. L'auditeur devrait d'abord trouver un couple identifiant/mot de passe pour pouvoir s'infiltrer dans le système. En grey box, on peut lui fournir ce couple d'identifaints, voire lui donner l'identifiant de l'administarateur, afin qu'il puisse aller encore plus loin.

IV.2.2.3 Les test en white box

Le test en *white box* (en boîte blanche) sera le plus long, le plus approfondi, mais également le plus onéreux. En effet, ici l'accès au système sera complétement ouvert au spécialiste venu faire l'audit. De ce fait, il est de son devoir de tester chaque service, de vérifier sa configuration, ses vulnérabilités éventuelles, et de faire un tour complet pour assurer l'étanchéité.

Le but ici est donc d'évaluer les risques potentiels en toute connaissance du système, et également de vérifier que le système sera apte à redémarrer sans perte d'informations si une attaque a tout de même lieu, en vérifiant par exemple le système de sauvegarde de données.

Dans le cadre d'un site internet, il aura accès au code source et devra vérifier que celui-ci ne présente pas de risques pour le système.

IV.2.3 Les advanced persistent thread (APT)

IV.2.3.1 Définition

Le National Institute of Standards and Technologie (NIST) définit l'APT comme étant un adversaire qui possède un niveau d'expertise sophistiqué et les ressources importantes, qui lui permettent de créer des opportunités pour atteindre ses objectifs et utilisant de multiples vecteurs d'attaques (par exemple, cyber, physique, diversion).Ces objectifs sont typiquement dans le but d'exfiltrer de l'information, déterrer ou entraver des aspects critiques d'une mission, programme ou organisation ; ou se placer en position de remplir ces objectifs dans le futur.[6]

L'Advanced Persitent Threat poursuit ces objectifs de façon répétée sur une longue période de temps ; s'adapte aux efforts des défenseurs ; et est déterminer à maintenir le niveau d'interaction nécessaire pour atteindre ces objectifss.

IV.2.3.2 La chaîne d'attaque APT

Essayons de visualiser le processus d'une attaque APT dans son intégralité, de la première à la dernière opération.

FIGURE IV.2 – Chaîne d'attaque APT

En fonction du niveau de détail que l'on souhaite représenter, cette chaîne d'attaque APT est plus ou moins longue. Cependant, la plupart des experts de la répense à incident APT sont en symbiose sur les techniques et processus déployés par les attaqants.

- **Étape 1 :** une première phase dite de "reconnaissance" de la cible est lancée. Il s'agit ici de découvrir et collecter toutes les données (relatives à la cible) qui peuvent être utiles lors de l'attaque à venir.

- **Étape 2 :** cette phase consiste en l'attaque initiale du système informatique de la cible afin de compromettre une ou plusieurs machines du parc informatique ciblé.

- **Étape 3 :** le renforcement des accès intervient à l'issue de la compromission initial. Cette étape permet aux attaquant de placer plusieurs outils et malwares à différents endroits du réseau informatique de l'entreprise victime, afin de disposer de plusieurs accès différents, notamment dans l'hypothèse où l'un de ces accès serait découvert et désactivé par la cible.

- **Étape 4 :** les mouvements latéraux permettent aux attaquants de parcourir tout le réseau de la cible et rechercher les informations intéressantes à dérober.

- **Étape 5 :** une fois les données trouvées, il faut les exfiltrer. Cette phase consiste donc en l'envoi des informations dérobées vers l'attaquant.

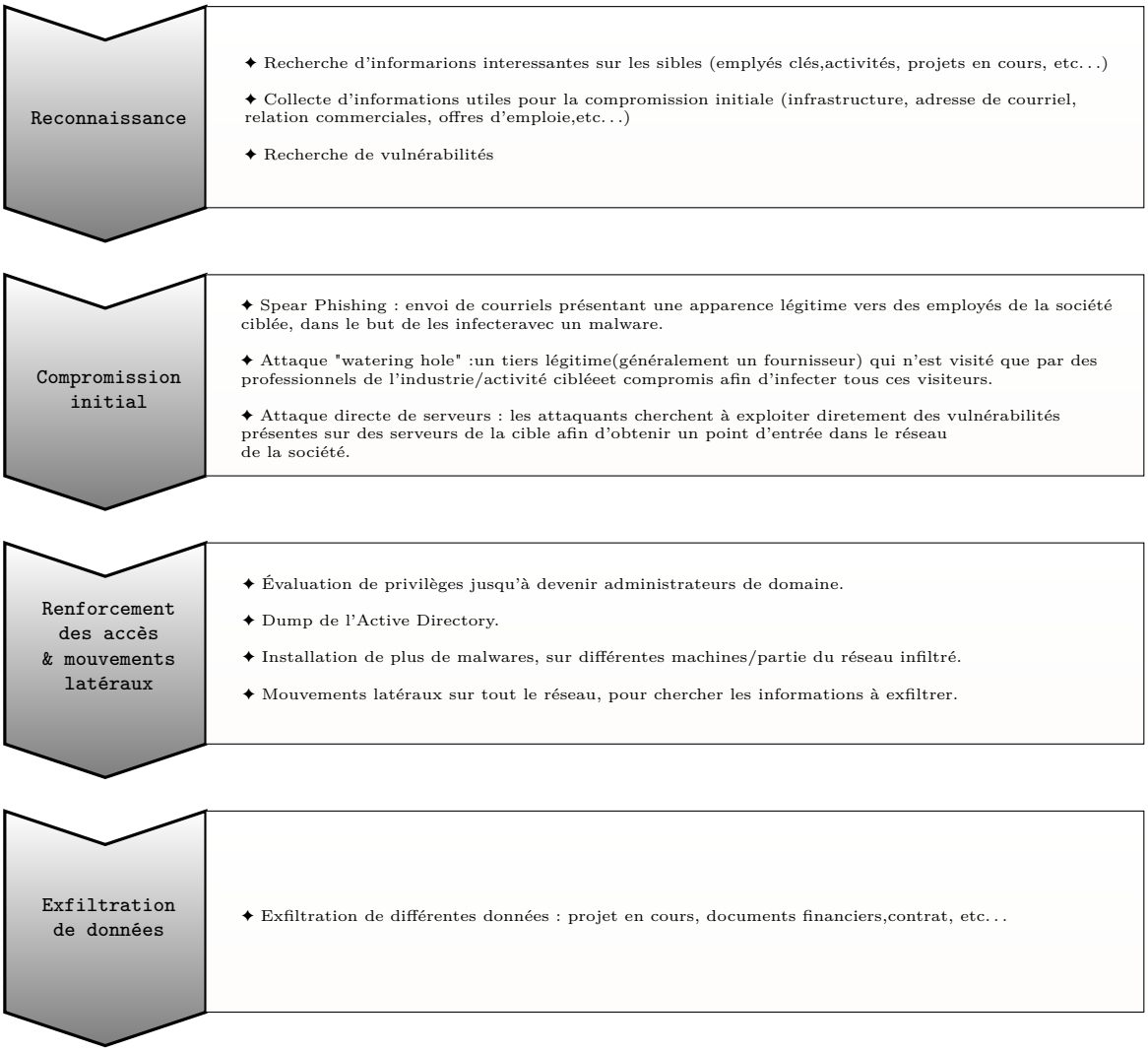


FIGURE IV.3 – Représentation graphique détaillée des phases d'une attaque APT

Une fois ce cycle est achevé, les attaques reviennent à l'étape 3 et boucle ainsi de l'étape 3 à l'étape 5 afin de :

- ✦ maintenir et mettre à jours les accès (porte dérobées, malwares, outils divers) ;
- ✦ surveiller des emplacements susceptibles de contenir régulièrement de nouvelles informations sensibles (généralement des partages réseau) ;
- ✦ si nécessaire, exfiltrer régulièrement les e-mails de certains employé stratègiques.

La Figure IV.3 présente une présentation un peu plus développée.

Comme mentionné précédemment, une fois l'exfiltration réalisée, l'attaque ne s'arrête pas : elle se porsuit par le maintient des accès existants, par éventuellement la création de nouveaux accès, l'exploration du réseau (d'autres movements latéraux) et d'autres exfiltrations.

IV.3 Typologie des attaques réseau

Les attaques réseau sont aujourd'hui si nombreuses qu'il serait illusoire de prétendre les décrire toutes.[7]

Il est cependant possible de dresser une typologie des faiblesses de sécurité afin de mieux appréhender ces attaques, qui ont pour point commun d'exploiter des faiblesses de sécurité.

Comme tout effet a une cause, les attaques réseau s'appuient sur divers types de faiblesses, que l'on peut classifier par catégorie, comme illustré sur la figure suivante :

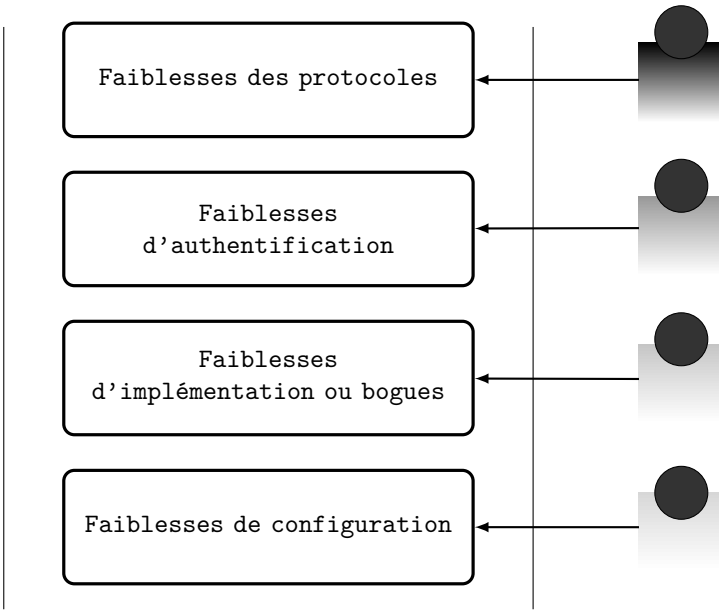


FIGURE IV.4 – Les composantes d'un système susceptible d'être attaquées

En s'appuyant sur ces faiblesses, le pirate peut lancer un ensemble d'attaques permettant d'influencer le comportement du réseau ou de récolter des informations importantes.

IV.3.1 Attaques permettant de dévoiler le réseau

IV.3.1.1 Attaque par cartographie du réseau

Les attaques visant à établir la cartographie d'un réseau ont pour but de dresser les artères de communication des futurs systèmes cibles. Elles ont recours pour cela à des outils de diagnostic tels que Traceroute, qui permet de visualiser le chemin suivi par un paquet IP d'un hôte à un autre.

Traceroute utilise l'option durée de vie, ou TTL (Time To Live) du paquet IP pour émettre un message ICMP time_exceeded (temps dépassé) pour chaque routeur qu'il traverse. Sachant que chaque routeur qui manipule un paquet décrémente le champ TTL, ce champ devient un véritable compteur de tronçon et permet de déterminer l'itinéraire

précis suivi par les paquets IP vers un système cible, comme l'illustre la figure suivante :

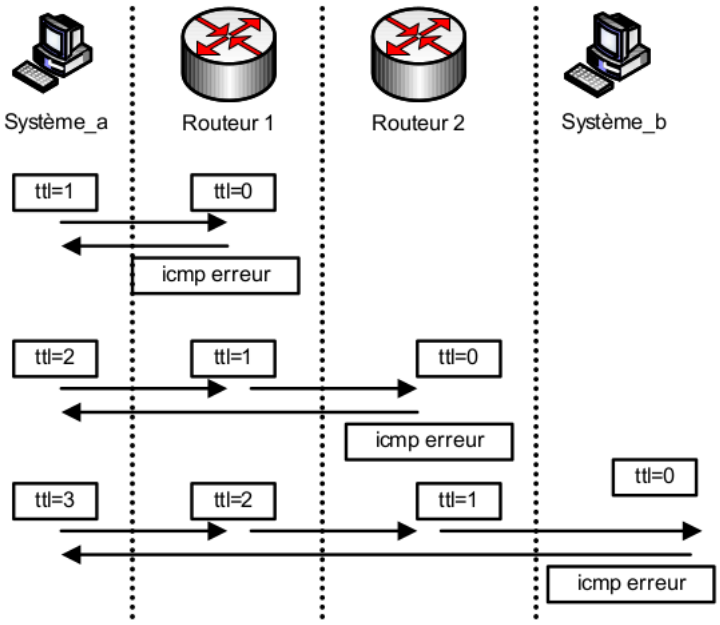


FIGURE IV.5 – Fonctionnement de l'outil Traceroute

Traceroute crée un paquet avec les adresses source et destination et une valeur de durée de vie TTL initiale (nombre de passerelles traversées) égale à 1. Ce paquet s'arrête donc au premier routeur rencontré, et le routeur envoie un message d'erreur ICMP (time_exceeded). Traceroute enregistre cette information et crée un nouveau paquet avec un TTL de 2.

La traversée du premier routeur met le TTL à 1. Le paquet génère une erreur sur le deuxième routeur. Comme précédemment, le deuxième routeur envoie un message d'erreur ICMP avec son adresse, laquelle est mémorisée par Traceroute. Une fois le système cible atteint, une erreur ICMP est générée par ce système cible, et Traceroute affiche la liste des passerelles traversées ainsi que le RTT (Round Trip Time), ou temps aller-retour, pour chacune d'elles.

L'établissement de la topologie réseau n'est pas innocent et représente la première étape d'une future attaque des systèmes réseau. Dans le cas le plus fréquent, le pirate utilise plutôt la technique du balayage (scanning) pour construire l'image du réseau, car elle fournit des informations plus rapidement.

IV.3.1.2 Attaque par identification des systèmes réseau

Certaines attaques visent à identifier tous les systèmes présents dans le but de dresser les futurs moyens de pénétration du réseau ou des systèmes qui le composent. Il existe pour cela différentes techniques de balayage des systèmes, comme l'illustre la figure suisvante :

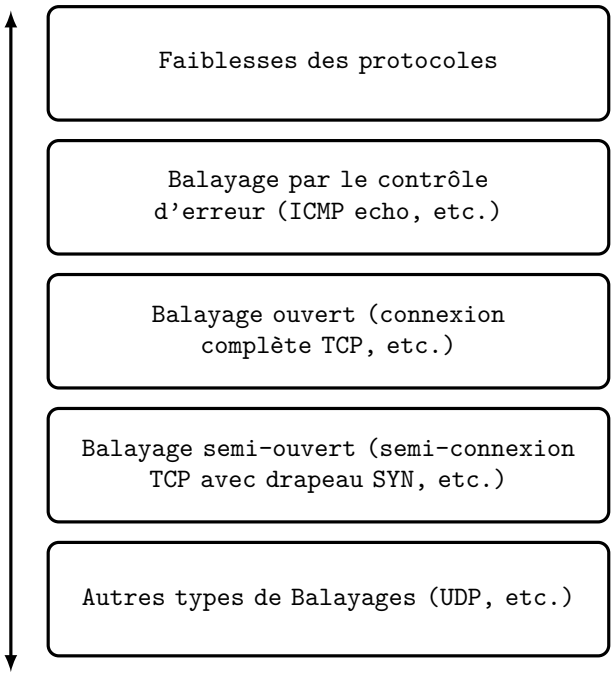


FIGURE IV.6 – Les différents types de balayages

Nous n'abordons que les techniques de base visant à découvrir les éléments du réseau.

IV.3.1.2.1 Attaque par balayage ICMP

La méthode de balayage la plus simple consiste à utiliser le protocole ICMP et sa fonction request, plus connue sous le nom de ping. Elle consiste à ce que le client envoie vers le serveur un paquet ICMP echo-request, le serveur répondant (normalement) par un paquet ICMP echo-reply, comme l'illustre la figure IV.7 Toute machine ayant une adresse IP est un serveur ICMP.

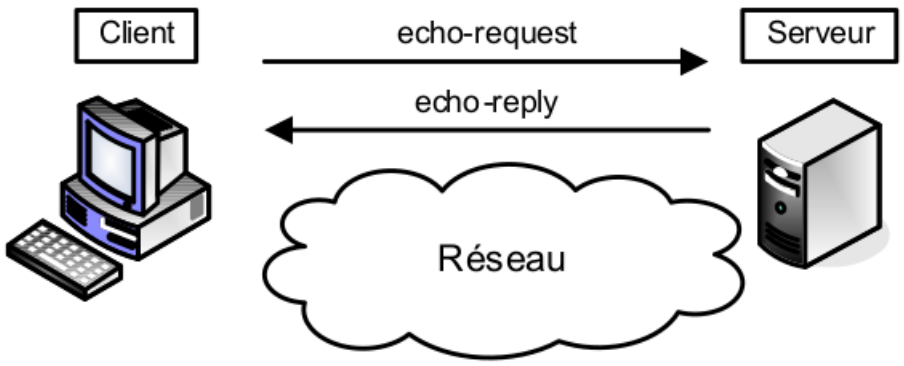


FIGURE IV.7 – Fonctionnement de la commande ping

Il existe deux méthodes pour cartographier le réseau par cette technique :

① En balayant (scanning) le réseau et en interrogeant chaque adresse IP possible, ce qui n'est pas très discret.

② En visant une seule fois l'adresse de broadcast du réseau, ce qui fait répondre toutes les machines présentes. Une seule demande permet ainsi d'engendrer l'envoi de toutes les réponses.

Cependant, du fait de l'accroissement constant de l'insécurité, nombre d'administrateurs de pare-feu ont pris l'initiative de ne pas laisser passer les réponses à de telles demandes.

IV.3.1.2.2 Attaque par balayage TCP

C'est en partant du principe que le flux réseau toujours accessible au pirate est celui qui est destiné à être accessible au public que la technique du balayage TCP a été inventée. Similaire au balayage ICMP, sa spécificité est de s'appuyer sur le protocole TCP. Le client envoie un paquet SYN vers un port réseau particulier de l'adresse IP du serveur. Si le port est en écoute, un paquet SYN/ACK est reçu en retour. Sinon, la réception d'un paquet RST signifie qu'il n'y a pas de service en écoute sur le port. Le client envoie en réponse un paquet RST pour terminer la connexion, comme l'illustre la figure suivante :

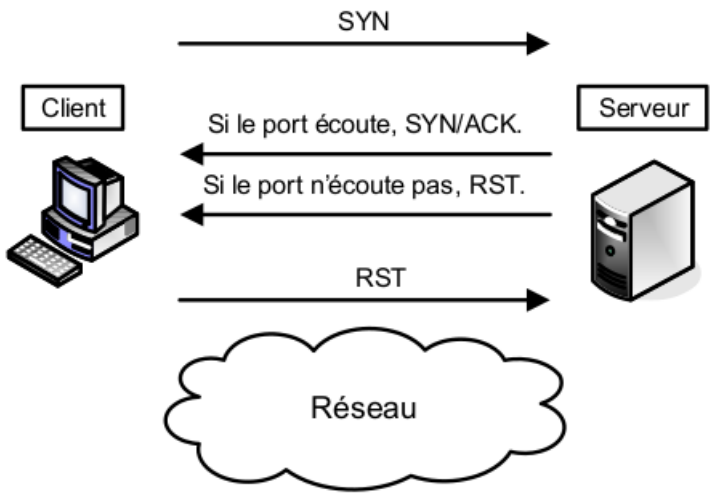


FIGURE IV.8 – Le balayage TCP

Si aucune réponse n'est reçue en retour, c'est qu'il existe un équipement filtrant entre le serveur et le client ou qu'il n'y a aucune machine derrière l'adresse IP visée.

Cette technique est cependant si peu discrète, que des variantes ont été élaborées pour améliorer le balayage en jouant sur le principe de fonctionnement de la pile TCP/IP.

IV.3.1.3 Attaque par identification des routeurs

Certaines techniques permettent de découvrir plus particulièrement les équipements assurant des fonctions de routage. L'écoute d'un réseau, par exemple, peut permettre d'analyser les trames échangées, de capturer les mises à jour des tables de routage et d'identifier les routeurs participant au routage du réseau.

Il est également possible de lancer des requêtes spécifiques afin de forcer ces mêmes routeurs à répondre. Par exemple, des requêtes peuvent s'appuyer sur une demande ICMP de découverte de routeur (ICMP router discovery) ou des requêtes de routage (OSPF, BGP,etc...).

Un pirate peut aussi envoyer des requêtes IRDP (ICMP Router Discovery Protocol), également appelées sollicitations de routeur (router solicitations), vers l'adresse de broadcast afin de connaître la route par défaut du réseau.

IV.3.1.4 Attaque par traversée des équipements filtrants

Lorsqu'un pirate désire établir la cartographie d'un réseau, il rencontre généralement sur son chemin un équipement filtrant. Celui-ci peut être un routeur avec des règles de filtrage ou un pare-feu.

Dans les deux cas, des techniques permettent de traverser les filtres de cet équipement, par l'exploitation d'un bogue, par exemple, ou d'une faiblesse de configuration.

IV.3.1.4.1 Attaque par modification du port source

Lorsqu'un pare-feu n'est qu'un simple routeur utilisant des listes de contrôle d'accès (ACL) ou un pare-feu qui ne peut détecter qu'un flux correspond au trafic retour d'une session sortante déjà initiée (le pare-feu est alors dit « stateful »), il est possible de passer outre les règles de filtrage appliquées en usurpant (spoofing) le port source du paquet émis (source porting).

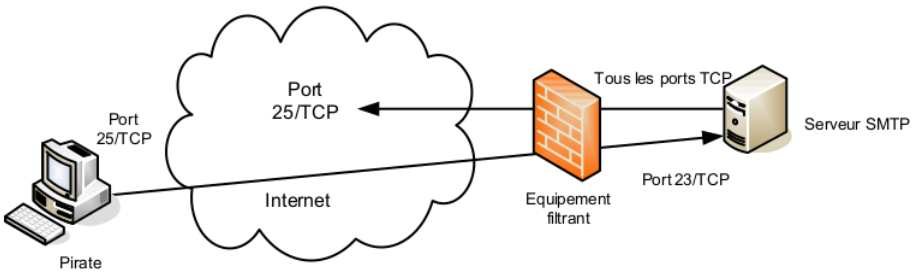


FIGURE IV.9 – Traversée d'un pare-feu en fixant le port source

Comme l'illustre la figure ci-dessus, le pare-feu a pour mission d'autoriser les flux sortants pour n'importe quel port source TCP associé au serveur SMTP situé sur le réseau de l'entreprise, à condition que ces flux visent n'importe quelle machine sur Internet sur le

port destination 25/TCP (le port utilisé par le service SMTP). Il s'agit d'une règle typique pour le trafic SMTP permettant aux serveurs de messagerie d'envoyer des messages électroniques vers l'extérieur. Un pirate peut donc accéder aux ports TCP du serveur SMTP situé dans le réseau de l'entreprise en attaquant avec le port source 25/TCP. Il peut atteindre, par exemple, le port Telnet (23/TCP) du serveur distant.

Ce type d'attaque est rendu possible par l'absence de contrôle par l'équipement filtrant d'un ensemble de caractéristiques associées au paquet IP. Aucune vérification des bits SYN et ACK n'étant effectuée, le fait qu'un paquet SYN sans ACK arrive depuis Internet ne perturbe pas l'équipement filtrant, qui est pourtant configuré pour n'accepter que les retours de sessions sortantes. Il n'y a pas non plus de maintien dynamique des tables de trafic ayant transité par l'équipement filtrant. Celui-ci ne fait donc pas la différence entre une réponse à un trafic sortant et un trafic entrant initié de l'extérieur.

Si l'équipement filtrant appliquait ces contrôles, il ne serait pas vulnérable à ce type d'attaque.

IV.3.1.4.2 Attaque par Fragment de paquet IP (Overlapping)

L'attaque par Fragment Overlapping consiste à fragmenter deux paquets IP au moyen de l'option Overlapping pour faire une demande de connexion TCP ou une autre demande sur une machine cible tout en traversant un filtrage IP.

Le premier paquet IP contient les données de l'en-tête TCP avec les indicateurs à 0. Le second paquet contient les données de l'en-tête TCP avec la demande de connexion TCP (flag SYN à 1 et flag ACK à 0). La figure suivante illustre cette attaque.

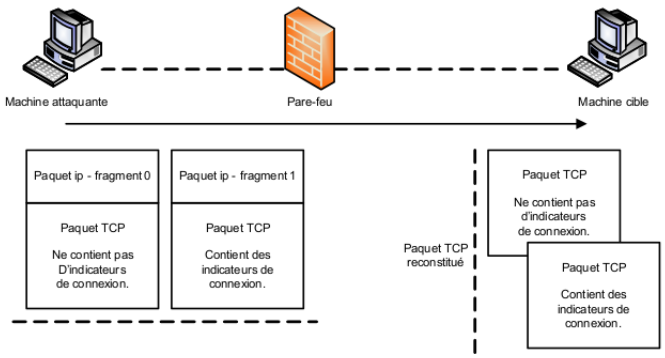


FIGURE IV.10 – Traversée d'un pare-feu en fixant le port source

Sur la figure, la demande de connexion est fragmentée en deux paquets IP contenant les fragments 0 et 1, chacun d'eux passant le système de filtrage et étant à nouveau assemblé par le système cible reconstituant un mauvais paquet TCP dû au chevauchement (overlapping) des fragments 0 et 1.

IV.3.2 Attaques permettant d'écouter le trafic réseau

Cette technique est généralement utilisée par les pirates pour capturer les mots de passe. Lorsqu'on se connecte à un réseau qui utilise le mode broadcast, toutes les données en transit arrivent à toutes les cartes réseau connectées à ce réseau. En temps normal, seules les trames destinées à la machine sont lues, les autres étant ignorées.

IV.3.2.1 Attaque par sniffing

Grâce à une table d'écoute (sniffer), il est possible d'intercepter les trames reçues par la carte réseau d'un système pirate et qui ne lui sont pas destinées, comme l'illustre la figure IV.11

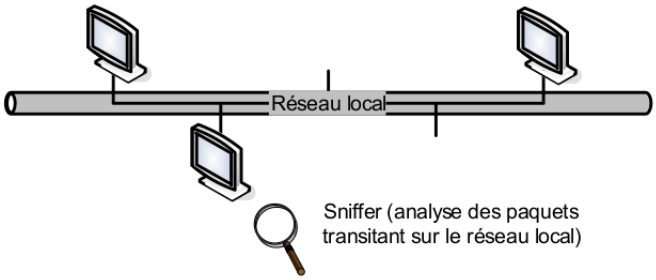


FIGURE IV.11 – Traversée d'un pare-feu en fixant le port source

Le système pirate se situe sur le réseau local et capture tous les paquets réseau transitant sur ce réseau afin d'obtenir des mots de passe, etc. Il n'est pas nécessaire que le sniffer possède une adresse IP sur le réseau qu'il écoute. Une interface réseau active sans adresse IP suffit. L'écoute est alors totalement indécelable au niveau ARP.

Grâce à des outils tels qu'Ethereal ou WinDump/TCPDump, le sniffer peut analyser tous les paquets IP ainsi que les protocoles contenus dans les données du paquet. Par exemple, un sniffer peut analyser un paquet Ethernet susceptible de contenir un paquet IP, qui lui-même pourrait contenir un paquet de type TCP, lequel à son tour pourrait contenir un paquet HTTP renfermant des données HTML.

Si une personne établit une session authentifiée sur un flux réseau non chiffré (Telnet, X11, etc.), son mot de passe transite en clair sur le réseau. De même, il est possible de connaître à tout moment les personnes connectées au réseau, les sessions de routage en cours, etc., par une analyse des paquets qui transitent sur le réseau et qui contiennent toutes les informations nécessaires à cette analyse.

Dans un réseau commuté, il n'est théoriquement pas possible d'écouter le réseau, car le commutateur envoie à chaque machine uniquement les paquets de données qui lui sont destinés. Mais comme tout équipement réseau, les commutateurs ont leurs faiblesses. Ainsi, un client qui enverrait des paquets usurpant l'adresse MAC du serveur qu'il désire écouter pourrait recevoir ces données. Selon les marques et les modèles de commutateur,

le comportement diffère totalement. Cela échoue souvent, mais il arrive que cela marche. Dans certains cas, le commutateur panique et se place en déni de service.

IV.3.2.2 Attaque de commutateur

Le commutateur (switch) a pour fonction de permettre la cohabitation de différents sous-réseaux physiques, qui ne communiquent pas nécessairement entre eux, sur le même équipement.

Pour atteindre cet objectif, le principe du VLAN (Virtual LAN) a été développé. À la base, un port du commutateur est assigné à un VLAN particulier, et seuls les ports du même VLAN peuvent s'échanger de l'information. Dans le but d'améliorer le confort pour l'administrateur et la qualité de service (redondance, etc.), des fonctionnalités supplémentaires ont vu le jour, avec leurs faiblesses. Ainsi, une attaque ARP spoofing peut permettre à une machine de recevoir des données qu'elle n'est pas censée recevoir.

Le protocole IEEE 802.1q a pour fonction principale de permettre à des commutateurs de s'échanger des données entre des VLAN partagés par plusieurs commutateurs. Certaines faiblesses de ce protocole sont cependant exploitables par quiconque est susceptible d'initier et de générer du trafic 802.1q avec le commutateur (ce qui constitue techniquement une faiblesse de configuration).

Par exemple, la technique dite du saut de VLAN (VLAN hopping) consiste pour le pirate à envoyer vers son port des paquets 802.1q ou ISL (Inter Switch Link) afin qu'il devienne un port « trunk », port utilisé par les commutateurs pour partager des VLAN. C'est ce qu'illustre la figure IV.12.

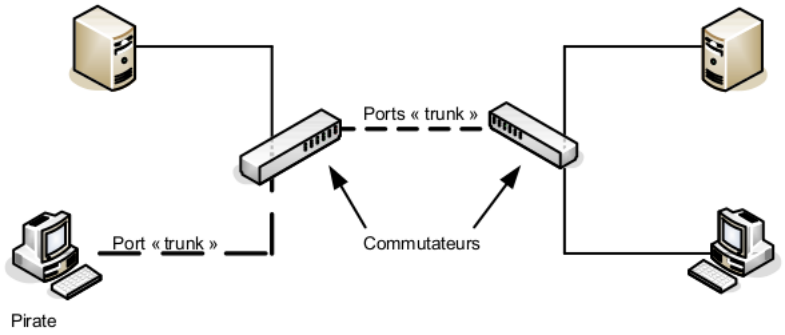


FIGURE IV.12 – L'attaque VLAN Hopping

Si l'attaque réussit, le port par lequel le pirate est attaché au commutateur devient un port « trunk ». À ce titre, il reçoit une copie de tous les paquets en transit sur tous les VLAN du commutateur.

IV.3.3 Attaques permettant d'interférer avec une session réseau

La plupart des protocoles réseau n'ayant prévu aucun mécanisme d'authentification véritable, ils subissent des attaques qui s'appuient sur ces faiblesses d'authentification, au premier rang desquelles les attaques ARP spoofing et man-in-the-middle.

IV.3.3.1 Attaque ARP spoofing

Comme son nom l'indique, l'attaque ARP spoofing s'appuie sur le protocole ARP (Address Resolution Protocol), qui implémente le mécanisme de résolution d'une adresse IP (32 bits) en une adresse MAC (48 bits) pour rediriger le trafic réseau de un ou plusieurs systèmes vers le système pirate.

Lorsqu'un système désire communiquer avec ses voisins sur un même réseau (incluant la passerelle d'accès à d'autres réseaux), des messages ARP sont envoyés afin de connaître l'adresse MAC des systèmes voisins et d'établir ainsi une communication avec un système donné.

Sachant que chaque système possède localement une table de correspondance entre les adresses IP et MAC des systèmes voisins, la faiblesse d'authentification du protocole ARP permet à un système pirate d'envoyer des paquets ARP réponse au système cible indiquant que la nouvelle adresse MAC correspondant à l'adresse IP d'une passerelle est la sienne.

Le système du pirate reçoit donc tout le trafic à destination de la passerelle. Il lui suffit-d'écouter ou de modifier passivement le trafic et de router ensuite les paquets vers leur véritable destination, comme l'illustre la figure IV.13.

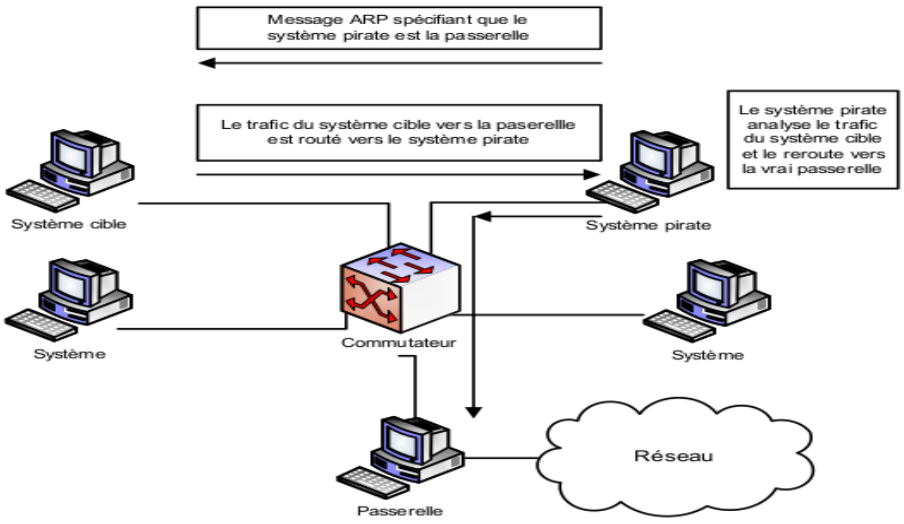


FIGURE IV.13 – L'attaque ARP spoofing

IV.3.3.2 Attaque IP spoofing

Puisqu'un paquet IP n'est qu'une suite d'octets construite par un système d'exploitation s'exécutant sur un système hardware, cette suite d'octets peut être forgée et envoyée sur le réseau sans contrôle préalable de ce dernier.

La plupart des moyens d'authentification s'appuient de nos jours sur les adresses IP, ce moyen faible d'authentification peut entraîner de graves problèmes de sécurité si l'authentification ne recourt qu'à ce mécanisme. Si un système peut donner des privilèges particuliers à un ensemble d'adresses IP sources, un paquet IP forgé avec une telle adresse IP est reçu par ce système avec les privilèges associés.

L'attaque IP spoofing consiste à se faire passer pour un autre système en falsifiant son adresse IP. Le pirate commence par choisir le système qu'il veut attaquer. Après avoir obtenu le maximum de détails sur ce système cible, il détermine les systèmes ou adresses IP autorisés à se connecter au système cible. Le pirate procède ensuite aux étapes illustrées à la figure IV.14 pour mener à bien son attaque sur le serveur cible en utilisant l'adresse IP de la machine A.

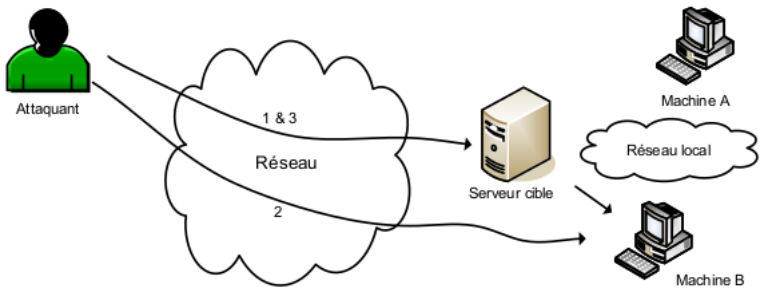


FIGURE IV.14 – L'attaque IP spoofing

L'attaque se déroule de la façon suivante :

① Le pirate essaye de prévoir le numéro de séquence des paquets du serveur cible en envoyant plusieurs paquets et en analysant l'algorithme d'incrémentation de ce numéro.

② Le pirate rend inopérante la machine A autorisée à accéder au serveur cible, de façon à s'assurer qu'elle ne répond pas au serveur cible.

③ Le pirate falsifie son adresse IP en la remplaçant par celle de la machine invalidée et envoie une demande de connexion au serveur cible.

④ Le serveur envoie une trame SYN|ACK à la machine qu'il pense être l'émettrice.

⑤ Celle-ci ne pouvant répondre, le pirate acquitte cette connexion par une trame ACK, avec le numéro de séquence prévu. Il établit de la sorte en toute impunité la connexion avec le serveur cible.

Cette attaque est assez difficile à effectuer, car elle se réalise en aveugle, le pirate ne recevant pas les données transmises par le serveur. Il doit donc maîtriser parfaitement les protocoles pour savoir ce qu'attend le serveur à tout moment. D'autres techniques plus évoluées permettent de contourner ce problème, comme les attaques dites man-in-the-middle (l'homme au milieu) ou les attaques de routage.

IV.3.3.3 Attaque man-in-the-middle

L'attaque man-in-the-middle consiste à faire passer les échanges réseau entre deux systèmes par le biais d'un troisième, sous le contrôle du pirate. Ce dernier peut transformer à sa guise les données à la volée, tout en masquant à chaque acteur de l'échange la réalité de son interlocuteur.

Pour mettre en œuvre l'échange réseau approprié, il faut soit que la machine du pirate se trouve physiquement sur le chemin réseau emprunté par les flux de données, soit que le pirate réussisse à modifier le chemin réseau afin que sa machine devienne un des points de passage (nous détaillons plus loin ce type d'attaque).

Au final, l'échange se présente sous l'une des trois formes suivantes :

- **Relais transparent.** La machine du pirate transforme les données à la volée. Elle veut rester la plus transparente possible et se comporte comme un routeur, conservant toutes les caractéristiques des paquets dont elle assure le transit, à l'exception du contenu. En termes d'adresses IP, A et B sont réellement en relation l'une avec l'autre(voir figure IV.15).

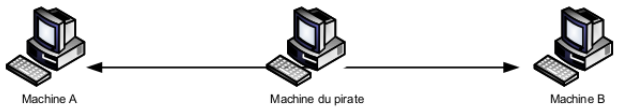


FIGURE IV.15 – Machine du pirate en tant que relais transparent

- **Relais applicatif.** La machine du pirate assure l'échange entre les deux machines A et B. A parle avec la machine du pirate, laquelle parle avec B. A et B n'échangent jamais de données directement. Cette méthode est nécessaire pour les attaques vers SSL, par exemple (voir figure IV.16).

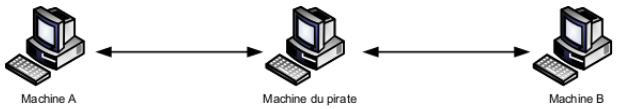


FIGURE IV.16 – Machine du pirate en tant que relais applicatif

✦ **Hijacking.** La machine du pirate utilise la session engagée entre les deux machines A et B afin que ce soit elle (la machine du pirate) qui soit en session avec la machine B. A perd la session avec B, et la machine du pirate continue la session engagée par A sur B (voir figure IV.17).

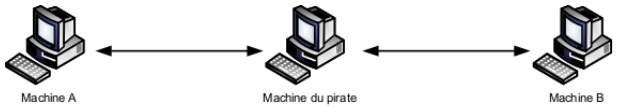


FIGURE IV.17 – Machine du pirate en tant que hijacker

Le détournement (hijacking) des sessions TCP permet de rediriger un flux TCP en outrepassant les authentifications nécessaires à l'établissement des sessions (Telnet, FTP, etc.). Cette attaque porte de manière plus spécifique sur l'analyse des numéros de séquences et des numéros d'acquittements relatifs aux paquets TCP.

IV.3.4 Attaques permettant de mettre le réseau en déni de service

Le déni de service, ou DoS (Denial of Service), est une attaque qui vise à rendre indisponible un service, un système ou un réseau. Ces attaques s'appuient généralement sur une faiblesse d'implémentation, ou bogue, ou sur une faiblesse d'un protocole.
Les premières attaques par déni de service sont apparues entre 1998 et l'an 2000. Elles visaient de grands sites Internet (Yahoo, eBay, eTrade, etc.). Le site Yahoo, a été attaqué en février 2000 et a été inondé (flood) sous 1 Go de données en quelques secondes, les données provenant d'au moins cinquante points réseau différents.

IV.3.4.1 Attaque par inondation

L'inondation est la méthode la plus classique pour empêcher un réseau d'assurer sa mission. Son principe de fonctionnement est le suivant :

- ✦ Une ou plusieurs machines inondent le réseau avec des paquets réseau afin de saturer la bande passante de celui-ci.
- ✦ Une fois que toute la bande est occupée, les autres machines ne peuvent plus travailler, ce qui génère une situation de déni de service.

L'inondation peut recourir à différentes méthodes. La plus classique est l'inondation ping (Ping flooding), une machine envoyant des paquets ping ICMP request et attendant en réponse un paquet ICMP reply. Sans mention d'un délai pour l'obtention de la réponse, la machine envoie ses paquets aussi vite qu'elle le peut, saturant ainsi le réseau.

IV.3.4.2 Attaques smurf et fraggle par amplification de l'inondation

Les attaques smurf et fraggle sont des variantes de la précédente qui s'appuient sur une faiblesse de configuration des routeurs.

Ces techniques consistent à inonder le réseau avec des ping qui n'utilisent que des adresses de broadcast. Pour un paquet envoyé, toutes les machines d'un réseau répondent, ce qui augmente la saturation du réseau, comme l'illustre la figure IV.18.

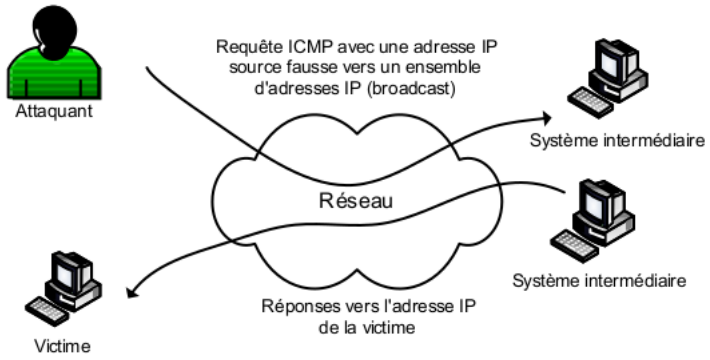


FIGURE IV.18 – Attaques smurf et fraggle

Du fait de l'envoi des paquets ICMP avec une fausse adresse source vers une adresse de broadcast, chaque machine appartenant au réseau couvert par le broadcast répond aux systèmes victimes ou aux systèmes fictifs. Comme le pirate n'attend pas de trafic retour, il peut bombarder un ensemble d'adresses de broadcast et générer un trafic important par phénomène d'amplification.

La différence entre l'attaque smurf et l'attaque fraggle est que cette dernière utilise leprotocole UDP.

IV.3.4.3 Attaque par inondation TCP SYN

La technique d'inondation SYN est identique à celle du balayage SYN, à la différence près qu'elle est utilisée à des fins de déni de service.

Nous avons vu que le principe du balayage semi-ouvert consistait à ce que le client ne termine pas la session TCP par l'envoi d'un paquet RST. Ainsi, le serveur reste dans un état intermédiaire, dans lequel la session n'existe pas réellement puisqu'elle est en cours d'établissement. Dans cet état, le serveur doit réserver des ressources (réseau, mémoire, CPU, etc.) pour le traitement de la session TCP et attendre la fin du handshake.

Tous les serveurs supportent un nombre maximal de sessions TCP en cours. Lorsqu'une session est terminée, les ressources associées à la session sont remises à disposition du système d'exploitation. Lorsque la session n'est pas encore établie, le système prend la peine de faire patienter les paquets manquants, estimant qu'ils sont simplement retardés par le réseau. Ce délai d'attente pour passer les différents états de libération de la session

est paramétrable mais prend généralement une bonne minute.

Ces différentes étapes sont illustrées à la figure IV.19.

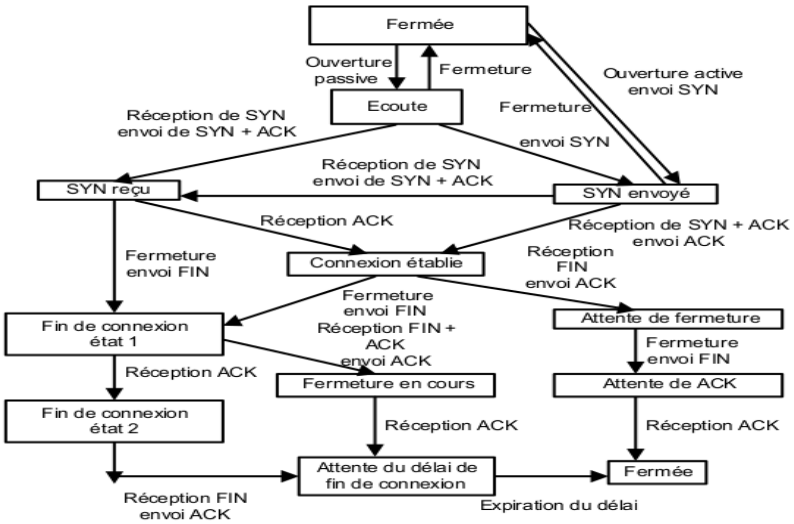


FIGURE IV.19 – États d'une session TCP

L'envoi de paquets SYN par un pirate vers un serveur, une opération très rapide puisque le pirate n'attend pas de réponse de celui-ci, engendre une saturation des ressources réseau de la victime, laquelle ne peut plus dès lors assurer sa mission.

IV.3.4.4 Attaque par épuisement de TCP

La technique par épuisement de TCP consiste à établir un nombre important de connexions (complètes) TCP entre deux acteurs, tout en créant un déséquilibre important d'allocation des ressources.

Ainsi, en exploitant au maximum les possibilités du protocole TCP de garder une connexion active a minima pour l'attaquant (utilisation du paramètre de débit permettant de limiter les requêtes de maintien de connectivité en se plaçant dans un mode congestion), il est possible de créer un nombre important de connexions actives sur le système attaqué de telle manière que le système se sature lui-même.

La raison de la saturation générale est que la plupart des systèmes d'exploitation prennent en charge la gestion réseau et que, par effet de bord, l'attaque par épuisement de TCP impacte l'ensemble des applications jusqu'à obtenir un état de figement du système visé.

IV.3.4.5 Attaques sur les bogues des piles IP/TCP

Les piles IP/TCP développées par différents constructeurs ou fournisseurs de services manifestent des différences de comportement malgré les définitions des RFC et contiennent de multiples faiblesses, qui peuvent être exploitées par des attaques bien ciblées.

Comme il est théoriquement impossible de vérifier l'absence de bogues dans un programme conçu avec les langages de programmation modernes, il existe une forte probabilité que des bogues permettent à des pirates de gagner des privilèges.

Les principales attaques qui s'appuient sur les erreurs de programmation associées aux piles TCP/IP sont le ping de la mort, le baiser de la mort, le win nuke, l'attaque land et l'attaque teardrop.

Le ping de la mort consiste à envoyer une suite de fragments d'une requête de type écho ICMP. Une fois à nouveau assemblés par la pile IP/TCP du système cible, ces fragments forment un paquet d'une taille supérieure à la taille maximale autorisée (65 507 octets) et peuvent faire déborder les variables internes, provoquant un comportement anormal du système (voir figure IV.20).

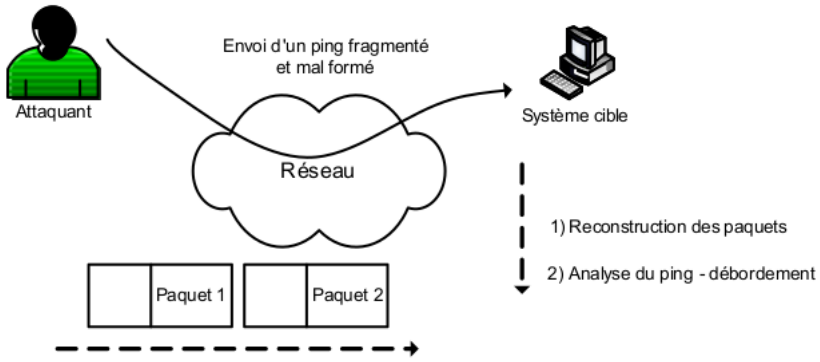


FIGURE IV.20 – L'attaque ping de la mort

Le baiser de la mort consiste à envoyer un paquet IGMP (Internet Group Management Protocol) mal construit, mettant les machines Windows en refus de service.

Le win nuke envoie un paquet TCP mal construit avec des données OOB (Out Of Band), mettant les machines Windows en refus de service. L'impact de l'attaque peut provoquer des comportements indésirables du système cible.

L'attaque de type land demande une ouverture de session TCP avec l'adresse source du paquet égale à l'adresse destination et le port source égal au port destinataire. Cette attaque utilise principalement le port 139 TCP (NetBIOS Session) afin de viser le système d'exploitation Windows. L'impact de l'attaque peut provoquer des comportements indésirables du système cible.

L'attaque de type teardrop envoie un paquet fragmenté de telle façon que les en-têtes du second paquet écrasent ceux du premier, affolant la pile TCP/IP. Cette attaque a été conçue initialement pour les paquets ICMP fragmentés, mais de nombreuses variantes ont été développées depuis pour fonctionner avec n'importe quel type de protocole IP. L'impact de l'attaque peut provoquer des comportements indésirables du système cible.

IV.3.4.6 Attaques par déni de service distribué (DDoS)

L'attaque DDoS (Distributed Denial of Service) est un dérivé de la précédente sous une forme distribuée, comme l'illustre la figure IV.21.

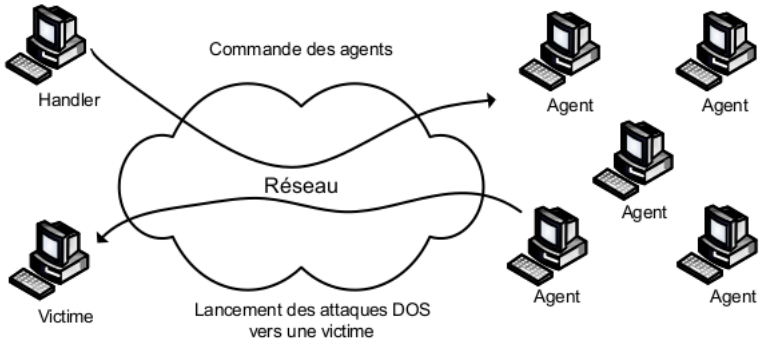


FIGURE IV.21 – Attaque par déni de service distribué

La première étape consiste à pénétrer par diverses méthodes des systèmes dits handlers, ou maîtres (masters), et agents, ou esclaves (slaves). Le pirate contrôle ensuite directement un ensemble de systèmes handlers, qui contrôlent eux-mêmes un ensemble de systèmes agents. La dernière étape consiste pour le pirate à déclencher son attaque vers un ou plusieurs systèmes cibles donnés. Cet ordre d'attaque aura été donné par les systèmes handlers, qui auront eux-mêmes reçu cet ordre du pirate.

IV.4 Conclusion

Le contrôle de la sécurité réseau (interne et externe) fait partie intégrante de la démarche sécuritaire d'une entreprise. Comme nous l'avons détaillé, ce contrôle devient aussi complexe que les techniques mises en place contre les attaques.

L'un des objectifs majeurs des contrôles de sécurité est d'établir des tableaux de bord de sécurité reflétant l'application de la politique de sécurité réseau de l'entreprise. En aucun cas il ne faut assimiler ces courbes à un niveau de sécurité réseau de l'entreprise. Elles ne donnent qu'un état d'application de la politique de sécurité.

Le volet pratique

ChapitreV

Teste d'intrusion avec GNS3

V.1 Introduction

Ce chapitre n'est qu'à titre d'exemple d'une simulation d'une infrastructure réseau d'une entreprise quelconque, ainsi il présente quelques définitions des outils nécessaires afin de pouvoir réaliser cette simulation réseau. Aussi il explique le fonctionnement des fichiers du framework d'un test d'intrusion qui permet de pouvoir mieux nous organiser.

V.2 Simuler des architectures réseaux avec GNS3

GNS3 est un outil simple et intuitif vous permettra de créer vos réseaux, les tester, les installer et paramétrer des switchs, des routeurs, et même des serveurs. Le simulateur GNS3 vous permet en effet de connecter également votre hyperviseur de machines virtuelles depuis Vmware ou virtualbox.

En bref, il est possible d'architecturer les réseaux simples et complexes, et les simuler virtuellement, comme si vous y étiez !

V.2.1 Définition Emuler, simuler, virtualiser

V.2.1.1 Définition de la Simulation

La simulation, en général, est une représentation fictive de la réalité. Il s'agit d'imiter une situation.

La simulation réseau revient à reproduire l'architecture d'un réseau et cela sans utiliser de machine physique.

Pour cela, la simulation passe par un logiciel qui calcule (on emploiera aussi le terme de "modélisation") et donc prédit les événements qui seraient amenés à se produire en prenant en compte leurs caractéristiques. Il existe de nombreux outils pour réaliser ces simulations, comme par exemple :

- ✦ GNS3
- ✦ Cisco Packet Tracer
- ✦ Cisco Virl
- ✦ Marionnet
- ✦ Eve

Certains sont gratuits, d'autres payants.

V.2.1.2 Définition de l'Emulation

Un peu plus ambitieuse que la simulation, l'émulation permet non pas de modéliser, mais bel et bien de *reproduire à l'identique* le comportement d'un logiciel et son architecture matérielle. Ce terme n'apparaît qu'en informatique.

V.2.1.3 Définition Virtualisation

La virtualisation, en général, signifie rendre virtuel c'est-à-dire qui n'existe pas. Cette notion s'oppose au monde physique.

Dans le cadre des systèmes et réseaux, la virtualisation reprend les concepts de l'émulation, à quelques différences notables près. Elle utilise l'architecture du système hôte, alors que l'émulation la reproduisait de manière logicielle.

V.3 Architecture de sécurité

C'est d'organiser le système d'information de manière à pouvoir mieux le contrôler pour ainsi mieux le surveiller et détecter d'éventuelles menaces et évidemment y reprendre.

On va parler de Firewall, DMZ, Proxy, Reverse Rroxy, IDS et IPS. l'objectif de ça et de donner la vision globale de :

- ✦ comment ses 5 différents éléments fonctionnent ensemble,
- ✦ comment ils sont intégrés au sein des systèmes d'informations,
- ✦ et comment ils sont complémentaires entre eux pour assurer la sécurité niveau réseau.

Le réseau permet à des machines de communiquer entre elles pour s'échanger des données. Le réseau permet aussi de faire communiquer des machines internes avec l'extérieur notamment internet, et donc de communiquer avec d'autres machines en dehors du réseau local.

Et à l'inverse avec cette ouverture du réseau interne, les machines deviennent accessibles à des personnes extérieurs du réseau.

Le problème est qu'internet est aussi une porte potentielle pour des actions malveillants comme de l'espionnage ou des attaques informatiques pour compromettre le système informatique, et justement l'architecture de sécurité explique comment mettre en place des éléments structurants pour protéger les machines internes, on parle aussi de la défense périmétrique. La première pierre périmétrique est le *Farewall*.

V.3.1 Le Farewall

Le Farewall a pour fonction de sécuriser un réseau en définissant les communications autorisées ou interdites. Il permet d'interconnecter des réseaux de niveaux de sécurité différents.
Le Farewall a pour but de filtrer les communications entre les zones que ce soit en entrée ou en sortie pour les analyser, et en fin de les autoriser ou de les rejeter selon les règles de sécurité en vigueur.

Les critères les plus courants du filtrage sont les suivants :

- ✦ L'origine ou/et la destination de paquets avec l'adresse IP et les ports.

- ✦ Les options contenues dans les données comme leurs fragmentations ou leurs validités (par exemple les données elle-même et même les utilisateurs pour les Farewall les plus récents)...

Deuxième élément de l'architecture de sécurité qu'est d'ailleurs lié au Farewall, c'est la DMZ.

V.3.2 La DMZ

La DMZ est un sous-réseau isolé qui sépare le réseau local (le LAN), et un autre réseau considéré comme moins sécurisé comme internet.

Le Firewall permet de créer la DMZ, elle héberge des machines de réseau interne mais ce sont des machines qui ont besoin d'être accessibles depuis l'extérieur.

Les serveurs de LAN ne sont jamais exposés directement à internet, et à l'inverse les utilisateurs depuis internet n'ont jamais accès directement aux ressources du LAN. Tout doit d'abord transiter par la DMZ, en terme de sécurité cela aussi veut dire qu'en cas de compromission d'un service dans la DMZ, le pirate n'aura accès qu'aux machines dans la DMZ et non dans le réseau local.

V.3.3 Un serveur proxy

Un serveur proxy est un serveur intermédiaire qui va permettre à une machine d'accéder à internet. Dans ce cas l'utilisateur va d'abord se connecter au serveur proxy et lui envoyer sa requête et c'est le serveur proxy qui va à son tour transmettre le message chez serveurs distants.

V.3.4 Différence entre un farewall et proxy

Les Firewall peuvent bloquer tout ou une partie des communications dans les sens entre les réseaux auxquels il est raccordé, tandi que le serveur proxy masque essentiellement le réseau interne sur internet.

V.3.5 un reverse proxy

un reverse proxy joue le rôle inverse du proxy, il permet à un utilisateur d'internet d'accéder à des serveurs internes.
Le reverse proxy centralise alors le flux entrant depuis internet vers les machines internes.

V.3.6 IDS (Intrusion Détection Système)

IDS s'agit d'un mécanisme qui a pour objectif de repérer tous types de trafic partiellement malveillants (par exemple les tentatives d'intrusion, les attaques virales, les débit trop important) ou tout trafic sortant de l'ordinaire.

IDS surveille et voie tout le trafic et lance des alertes mais il n'arrête pas le trafic, il s'appuie sur une norme pour repérer des activités cible qui peuvent être un réseau ou des machines hôtes et si l'activité s'éloigne de la norme, IDS lancera une alerte.

V.3.7 IPS (Intrusion Prévention Système)

L'IPS va réagir en temps réel en stoppant le trafic suspect qu'il reconnaît notamment en bloquant les ports, et gros l'IPS comme un IDS mais qui bloque le flux.

V.3.8 Différence entre Farewall et IPS

- **IPS**
  Le rôle de IPS est détecter des attaques sur le réseau à partir d'une base données de signature d'attaque (comme antivirus) et les blocs si nécessaire.
- **Farewall**
  Le rôle du FAREWALL est différent puisque son but est de faire du filtrage d'accès en définissant des communications autorisées ou interdites.

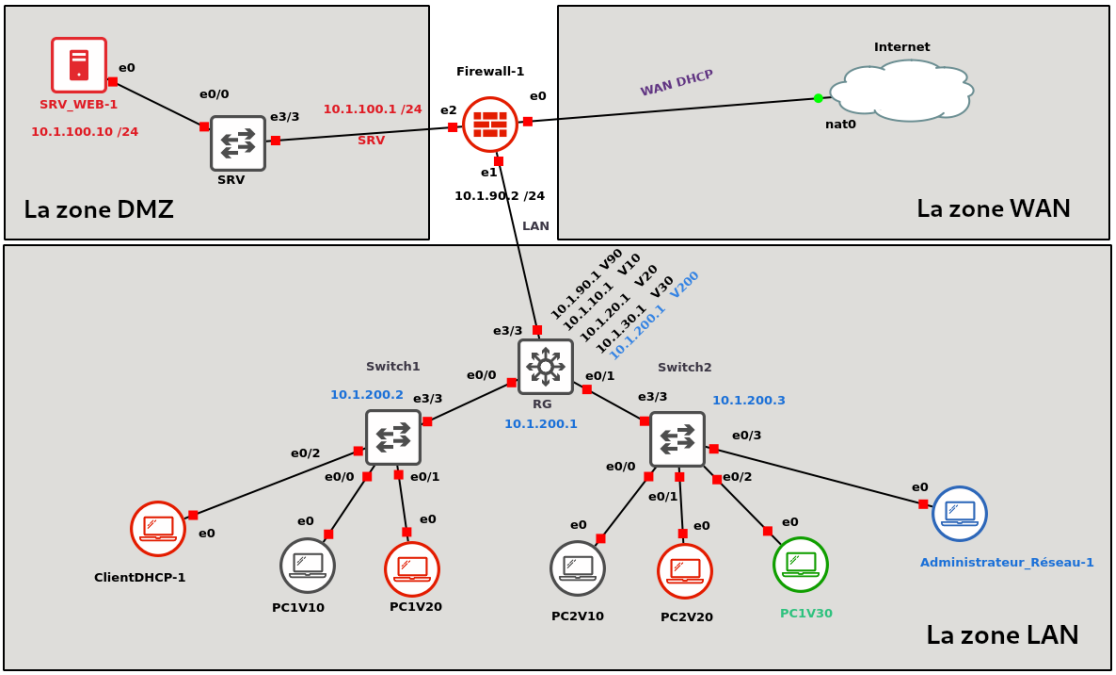


FIGURE V.1 – Exemple d'une infrastructure réseau d'une entreprise

Généralement un réseau d'entreprise est constitué de trois zines (LAN, DMZ et WAW) comme le motre la figure V.1.

Nous allons appliquer un test d'intrusion sur cette infrastructure réseau depuis l'intérieur sur le service DHCP qui se trouve dans RG le répatiteur général *(switch core)* comme étant un White Box.

Avant cela nous allons présenter et définir dans la suite de ce chapitre quelques outils que nous allons utiliser.

V.4 Présentation de Kali Linux

Kali linux est une distribution Linux sortie en 2013, basée sur la disstribution Debian.Kali est le successeur de Linux Backtrack sorti en 2006 basée sur Linux Ubuntu. L'objectif de kali Linux est de fournir une distribution regroupant l'ensemble des outils nécessaire à l'audit de sécurité d'un réseau donné.

V.5 Présentation de Cisco Tools

Cisco tools est une panoplie d'outils permettant de tester les vulnérabilités relatives au équipements Cisco, il se compose de :

① **Cisco-auditing-tool :** un script perl qui teste les vulnérabilités d'un routeur cisco.

② **Cisco-global-exploiter :** ou CGE est un outil d'audit et test avancé des commutateurs et des routeur Cisco.

③ **Cisco-ocs :** un outils scanner des routeurs et des commutateurs Cisco en masse.

④ **Cisco-torch :** un outils scanner des routeurs et des commutateurs Cisco en mode multi thread.

④ **Yersinia :** Un outils d'audit des équipements couche niveau 2 en terme de model OSI.

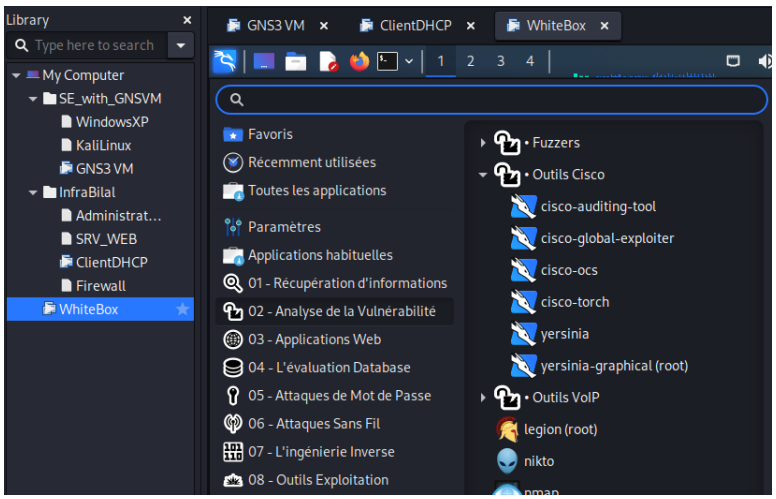


FIGURE V.2 – Une panoplie d'outils

V.6 Framework de pentest

V.6.1 Définition

Le framework de pentest permet d'avoir une vision complète d'un test d'intrusion orienté "Infrastructure". Celui-ci permet de renseigner les vulnérabilités identifiées et exploitées durant le test d'intrusion et d'en sortir un score d'impact technique et métier.[10]

Le framework est composé de deux Documents *(Excel)* et un fichier *Word* qui sont les suivants :

① Document Framework Pentest.

② Suivi Pentest.

③ Et rapport de Pentest.

V.6.2 Document Framework Pentest

Il s'agit du fichier principal du framework. A travers ce fichier il est possible inscrire les vulnérabilités que nous identifierons pendant le test d'intrusion et nous pourrons grace à ce même fichier d'y sortir des scores de gravités et d'exploitabilités.

L'objectif de ce fichier est d'inscrire les vulnérabilités et de leur attribuer un score pour générer des graphiques que nous pouvons intégrer dans un rapport ou dans une présentation.

Ce document est réparti en six onglets qui sont les suivants :

① **Onglet introduction :** Rappel sur le fonctionnement et plan du framework.

② **Onglet références :** Contient les références et liste de donnée composant le framework.

③ **Onglet questionnaires ROE :** Questionnaire permettant de dimmensionner et comprendre les besoins du clients concernant le test à effectuer (Questionnaire d'engagement).

Ce questionnaire nous permet de bien cibler le périmètre (voir les tableaux V.1, V.2, V.3, V.4, V.5, V.6, V.7)

TABLE V.1 – Questions relatives au test d'intrusion

Questions relatives au test d'intrusion		Réponses
1	Pourquoi le client a-t-il besoin d'effectuer un test d'intrusion sur son environnement ?	déceler des faiblesses et vulnérabilités afin de mettre en place de nouvelles mesures de sécurité du système d'information.
2	Quel est le type de test d'intrusion demandé ? (Red-team, blackbox, greybox, whitebox)	Whitebox.
3	Le test d'intrusion est il interne ou externe ?	Interne
4	Quel est le périmètre du test d'intrusion ? (Site physique + Plage d'IP)	Au niveau LAN.
5	Quelles sont les exclusions du test d'intrusion ?	La zone DMZ.
6	Y a-t-il des exclusions d'horraire à prévoir durant l'énumeration ou l'exploitation ?	Oui, le test s'effectuera uniquement durant le week-end.
7	Y a-t-il des obligations de disponibilité sur certains équipements ? (précisez si oui)	Non.
8	Un prêt de materiel interne est il prévue ? (poste utilisateur, carte à puce, ...)	Oui, une machine qui exécute Kali Linux comme système d'exploitation.

TABLE V.2 – Questions relatives au contexte de l'intrusion

Questions relatives au contexte de l'intrusion		Réponses
9	Quel est le contexte prévu dans le test d'intrusion ? (exemple : stagiaire malveillant, ex collaborateur, ..)	Stagiaire malveillant.
10	Quelles seraient les motivations de l'attaquant ?	Voler, altérer ou/et supprimer des données les plus sensibles.
11	Quel est le contexte de compétences de l'attaquant ?	Un mental d'acier et faire preuve de lucidité.

TABLE V.3 – Questions systèmes / réseaux

Questions systèmes / réseaux		Réponses
12	Y a-t-il des équipements sauvegardés ou considérés fragiles ? (Systèmes avec tendances à tomber en panne, systèmes d'exploitation plus anciens ou qui ne sont pas mise à jour)	Non
13	Présence d'équipements appartenant à un tiers ? (Necessitant l'inclusion au contrat de pentest)	Non
14	Y a-t-il des équipements non maitrisé ou non sauvegardé sur le périmètre ? (Incapacité de rollback, pas de sauvegarde, ...)	Non
15	Y a-t-il des équipements avec pertes de données inadmissible ?	Non
16	Des équipements de sécurités risques t-ils de bloquer / remonter l'intrusion ?	Non

TABLE V.4 – Questions sans-fil / GSM

Questions sans-fil / GSM		Réponses
17	Des réseaux WIFI font-il parti du périmètre ?	Non.
18	Des réseau radio, bluetooth, RFID font-ils parti du périmètre ?	Non.

TABLE V.5 – Questions d'attaque physique (RedTeam)

Questions d'attaque physique (RedTeam)		Réponses
19	Combien de sites inclus dans le périmètre ?	Un seul site.
20	Cet emplacement physique est-il une installation partagée ? Si c'est le cas : – Combien d'étages sont dans la portée ? – Quels étages sont dans la portée ?	Non
21	Existe-t-il des gardes de sécurité qui devront être contournés ? Si c'est le cas : – Les agents de sécurité sont-ils employés par une tierce partie ?	Oui
22	L'utilisation de "crochetage" ou hack materiel est-elle autorisée ?	Non.
23	Vol de materiel inclus dans les pratiques autorisés ? (Si oui, tous matériels possibles ? ou seulement une liste autorisé ?)	Non.

TABLE V.6 – Questions d'ingénierie sociale

Questions d'ingénierie sociale		Réponses
24	Pratique de social engineering autorisé dans les tests ?	Sans Objet
25	Y a-t-il une liste d'adresse de courriel autorisé dans le périmètre de la pratique ?	Sans Objet
26	Y a-t-il une liste d'adresse de courriel interdite dans le périmètre de la pratique ?	Sans Objet
27	Le client a-t-il une liste des numéros de téléphone à laquelle il souhaiterait qu'une attaque de l'ingénierie sociale soit effectuée ?	Sans Objet
28	L'ingénierie sociale est-elle destinée à obtenir un accès physique non autorisé ? Si c'est le cas : – Combien de personnes sont ciblées ?	Sans Objet

TABLE V.7 – Questions aux managers

Questions aux managers		Réponses
29	Le ou les managers sont-ils conscients qu'un test est sur le point d'être exécuté ?	Sans Objet
30	Quelle est la donnée principale qui créerait le plus grand risque pour l'organisation si elle était exposée, corrompue ou supprimée ?	Sans Objet
31	Le test d'intrusion est annoncé ou secret ? (Utilisateurs du périmètre)	Sans Objet

④ **Onglet vulnérabilités :**

Inscription des vulnérabilités identifiées et évaluation des impacts.

- ✦ Un tableau égale une vulnérabilité.
- ✦ Un tableau contient deux sous tableaux et une case corrective qui sont les suivants :

  ❶ **Sous tableau de vulnéralité technique :** qui va générer un score d'impacte technique.
  ❷ **Sous tableau business :** de ce qu'est organisationnel qui va générer un score d'impact métier.
  ❸ **Une Case corrective :** c'est une case indispensable, on fait un test pour amener une solution pas pour amener que des problèmes.

⑤ **Onglet synthèse de score :**

Une fois qu'on a scoré tous les vulnérabilités, cet onglet nous donne un score de criticité des vulnérabilités de l'infrastructure et qui sont les suivants :

- ✦ Le niveau de risque.
- ✦ Le score d'impact business.
- ✦ Le score de gravité des vulnérabilité.
- ✦ Facilité d'exploitation des vulnérabilités.
- ✦ Impact financier.
- ✦ Impact légal.
- ✦ Impact image.
- ✦ Impact operationnel.

⑥ **Onglet synthèse des vulnérabilités :**

Synthèse technique simple des vulnérabilités identifiées.
Au fur et à mesure qu'on découvre des vulnérabilités elles s'inscrivent dans le tableau automatiquement. Le but c'est de faire un *copier-coller* du tableau de synthèse qui fera un petit listing rapide dans le bilan du rapport.

V.6.3 Document Suivi Pentest

L'objectif de ce fichier est de pouvoir organiser l'équipe pendant le test d'intrusion. Il contiendra la méthode, la check-list et également un suivi d'intrusion pour inscrire les machines compromises, les mots de passe récupérés etc...

Celui-ci est réparti en quatre onglets qui sont les suivants :

① **Onglet références :**

Il contient les références et liste de données composant le document de suivi. La seule modification à apporter est d'ajouter les noms des pentesters qui seront dans la mission.

TABLE V.8 – L'onglet référence

1_Reconnaissance
2_Énumération
3_Exploitation
4_Post-Exploitation
5_Nettoyage

Les phases d'attaques

OUAZENE BILAL
SAIDANE AMIRALI
Pentester 3
Pentester 4
Pentester 5

Les pentesters

Non applicable
Vulnérable
Non Vulnérable

Les faits

② **Onglet checklist :**

La méthodologie et la checklist à effectuer durant le test. C'est à titre d'exemple bien évidemment, il s'agit d'une mèthodologie à suivre pendant le test. on peut inscrire les tâches à effectuer pendant le test (voir le tableau V.9).

Pour montrer l'utilisation, prenant à titre d'exemple du tuple N°1 :

❶ **Phase :** les phases d'attaques (la reconnaissance, l'énumération, l'exploitation etc...), il est évidemment possible de choisir les autres, (voir la figure V.1).

❷ **Objectif :** c'est de tester si un transfert de zone DNS sur un domaine DNS public. est mal configuré.

TABLE V.9 – L'onglet Checklist

N°	Fait	Phase	Objectif	Vulnérable si	Commandes	Qui
1		1_Reconnaissance	Transfert de zone DNS publique	Transfert de zone possible	dnscan -z $domain	SAIDANE AMIRALI
2		1_Reconnaissance	Récupérer des information et documents via google-dorks	metagoofil	metagoofil -d <Public-Domain> -t pdf,png,jpg,txt, xlxs,docx,xls,doc -l 10 -n 10	
3		2_Énumération	Sous-réseaux bien segmentées ?	netdiscover	netdiscover	
4		2_Énumération	Transfert de zone DNS interne ?	Transfert de zone possible	host -t axfr <DOMAIN.TLD> <DNS-SERVER>	
5		2_Énumération	Services vulnérables ?	Service vulnérables (CVE / exploit)	openvas metasploit	
6		3_Exploitation	Utilisateurs vulnérables au kerbe-roasting	Utilisateurs kerbe-roastable présents	impacket-GetUserSPNs	
7		3_Exploitation	Utilisateurs vulnérables à l'ASREP	Utilisateurs vulnérables présents	impacket-GetNPUsers	
8						
9						
10						
11						
12						

❸ **Vulnérable si :** Vérifie si le transfert de zone est possible, si cela est réussi, c'est que la cible est vulnérable.

❹ **Commandes :** pour faire le test nous avons un exemple de commande donc dnscan -z $domain.

❻ **Qui :** On peut attribuer un respensable sur la tâche. Nous avons inscrit précédement nos 2 pentester (voir la figure V.1), pour l'exemple on dira que SAIDANE AMIRALI effectuera la phase reconnaissance.

❼ **Fait :** donc SAIDANE AMIRALI effectuera le test dnscan -z $domain, est-ce que ça fonction ? Le resultat sera émis à ce niveau (la case fait).

Les réponses aux questions suivantes sont comme suit :

- Est-ce que le transfert de zone est possible ? -> VULNÉRABLE
- Est-ce que le transfert de zone n'est pas possible ? -> NON-VULNÉRABLE
- Ou est-ce que ce n'est pas applicable c'est-à-dire qu'il n'y a pas de zone DNS -> NON-APPLICABLE.

Donc là-dessus (l'onglet checklist), il est possible d'organiser et faire chacune de nos tâches en mettant si c'est vulnérable ou non, ce qui nous permettra par la suite de revenir dessus pour commenter la vulnérabilité.

③ **Onglet cheatsheet :**

Commandes utiles (aide mémoire). Ces informations nous les avons pas en tête tout de suite, voilà l'idée est de faire un CTRL+F pour les retrouver, voilà on prend ce que nous souhaitons. Aussi c'est quelque chose qu'on peut laisser (voir le tableau V.10).

④ **Onglet suivi d'intrusion :**

Suivi d'équipe sur l'avancée de l'intrusion(Loot, Machines compromises, malware déposés, comptes créés, ...).

L'idée ici est de partagé les informations entre les pentesters (voir le tableau V.11).

❶ **Tableau T1 :**
Durant le teste on est arrivé à compromettre le compte de monsieur RACHID qui a un mot de passe (qwerty86) associé au serveur SRV1.

❷ **Tableau T2 :**
Durent le test d'intrusion, nous allons créer des charges malicieuses, des fichiers malicieux et nous allons les déposer sur des serveurs au tant que persistant ou pour obtenir un accès.
on note ces informations car à la fin, on va nettoyer les serveurs affecter plus facilement.

Il ne faut pas oublier de chiffrer le fichier Excel, du moins le protéger après la saisie des données.

TABLE V.10 – L'onglet cheatsheet

N°	Objectif	Outils	Commandes
1	Exposer un service en interne via notre machine en proxy SSH	ssh	ssh –L <our kali port> <service to expose ip> <service to expose port> username@IP
2	Persistence via task sheduler	schtasks	schtasks /create /sc ONLOGON /tn "Name" /tr "path to exe" /ru "SYSTEM"
3	Clé Run	Regedit	Créer une entrée de type "REG_SZ" : HKLM/SOFTWARE/Microsoft/ Windows /CurrentVersion/Run
4	Stealth or Half-Open Scan	Nmap	nmap -sS <ip address or range>
5	Xmas tree Scan	Nmap	nmap -sX -v <target ip address>
6	Fin Scan	Nmap	nmap -sF <target ip address>
7	NULL Scan	Nmap	nmap -sN <target IP address>
8	Idle scanning	Nmap	nmap -Pn -p- -v -sI super12.com luck.org
9	Fragmented Scan	Nmap	nmap -sS -T4 -A -f -v <ip address>
10	Collecte TLD	dmitry	dmitry -iwnse <DOMAIN> > dmitry_<DOMAIN>.txt
11	Enumération TLD	dnscan	dnscan -d <DOMAIN> -r -w /usr/share/dnscan/subdomains-10000.txt
12	Report site + DNS (Ressource => Site report / DNS lookup)	Netcraft	https ://www.netcraft.com/
13	Services vulnérables ?	Censys	https ://censys.io
14	Services vulnérables ?	Shodan	https ://shodan.io
15	Intrusion Wi-Fi	Aircrack	**Enregistrer les captures dans un fichier :** airodump-ng -w <fichier WPA2> –BSSID <MAC> -c <CHANNEL> wlan0 **Ouvrir une nouvelle fenêtre et injecter/générer du trafic (désauthentification) :** aireplay-ng -0 (de-auth) 0 (nb/sec) -a <BSSID> -h <MAC target> wlan0mon **Attendre de récupérer le Handshake WPA2, puis lancer l'attaque par dictionnaire :** aircrack-ng <fichier WPA2>.cap -w rockyou.txt Attaque par dictionnaire personnalisé : crunch <Min-len> <Max-len> <chars> -t <Pattern> | aircrack-ng -w - <WPA.cap> -e <ESSID>
16	Compromission du router / firewall	routersploit	routersploit use exploits/marque/model/... show options ...
17	désactiver historique bash	Bash	HISTSIZE=0
18	Effacement des traces : Powershell	PowerShell	Clear-History
19			

TABLE V.11 – L'onglet suivi d'intrusion

compromis	**Mot de passe / hash**	**Machine associé / Annuaire**
MOKETFI	qwerty86	SRV1

(T1)

Charge déposé	**Machine**	**Emplacement de la charge**
malware.exe	SR1	C :/

(T2)

Test d'intrusion <white box>

V.7 Rapport d'audit

V.7.1 Rappel du périmètre

Le test d'intrusion est porté sur le périmètre suivant :

✦ **Périmètre**

❶ Le réseau LAN en local.
Le test s'est déroulé depuis l'intérieur de l'entreprise en tant que *White Box*.

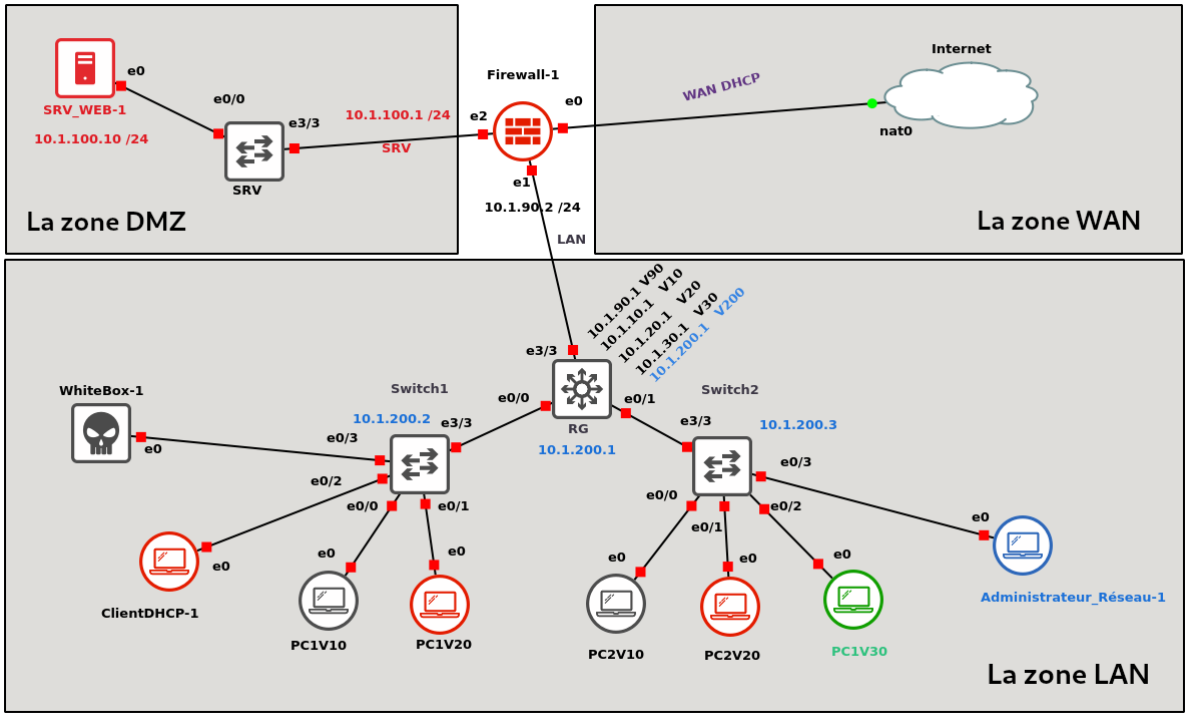


FIGURE V.3 – Infrastructure de l'entreprise lors de l'audit

V.7.2 Présentation des échelles utilisées

L'échelle de risque est classée selon 4 niveaux :

TABLE V.12 – L'échelle de risque

Niveau de risque	Description
Mineur	Faible risque sur le système d'information et pouvant nécessiter une correction
Important	Risque modéré sur le système d'information et nécessitant une correction à moyen terme
Majeur	Risque majeur sur le système d'information nécessitant une correction à court terme
Critique	Risque critique sur le système d'information et nécessitant une correction immédiate ou imposant un arrêt immédiat du service

Le niveau de risque d'une vulnérabilité est calculé en fonction de deux valeurs, sa facilité d'exploitation :

TABLE V.13 – Le niveau de risque d'une vulnérabilité

Difficulté d'exploitation	Description
Difficile	Exploitation de vulnérabilités non publiées nécessitant une expertise en sécurité des Systèmes d'information et le développement d'outils spécifiques et ciblés
Elevée	Exploitation de vulnérabilités publiques nécessitant des compétences en sécurité des Systèmes d'information et le développement d'outils simples
Modérée	Exploitation nécessitant des techniques simples et des outils disponibles Publiquement
Facile	Exploitation triviale, sans outil ni compétences particulières

Ainsi que l'impact technique CVSS de la vulnérabilité :

TABLE V.14 – Niveau d'impact technique CVSS de la vulnérabilité

Gravité	Description
Faible	Faible impact sur le composant
Moyenne	Impact moyen sur le composant
Forte	Impact fort sur le composant
Critique	Impact critique sur le composant

TABLE V.15 – Échelle de gravité métier

Gravité	Description	Valeur
Faible	Faible impact 0 < 2,5	2.5
Moyenne	Impact moyen 2,5 < 5	5
Forte	Impact fort 5 < 7,5	7.5
Critique	Impact critique 7,5 < 10	10

V.8 Synthèse du test d'intrusion

V.8.1 Bilan de l'audit

Le test d'intrusion a permis d'identifier deux vulnérabilités sur le périmètre cible, le diagramme ci-dessous représente la répartition en termes de gravité technique :

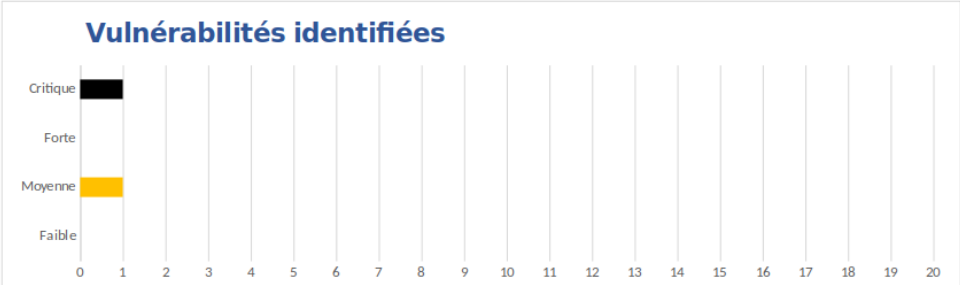


FIGURE V.4 – La répartition en termes de gravité technique

Les vulnérabilités de gravité forte et critique constituent la principale source de menace envers le SI, celles-ci permettent à un attaquant de Compromettre rapidement et facilement l'organisation.

Les vulnérabilités moyennes et faibles sont principalement des vulnérabilités liées à un non-respect des bonnes pratiques de configuration et sécurité pouvant amener (mise bout à bout) une compromission du SI.

La figure ci-dessous représente le score de criticité des vulnérabilités de l'infrastructure.

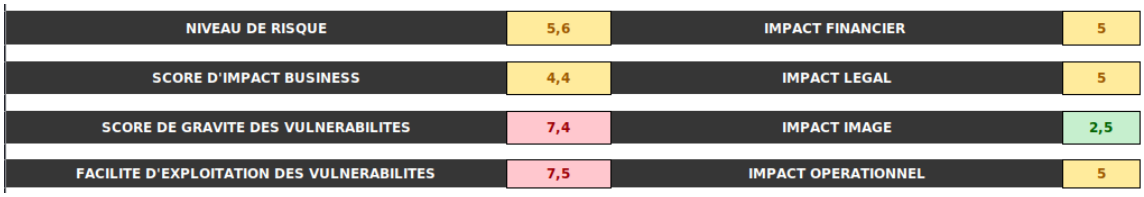


FIGURE V.5 – Criticité des vulnérabilités de l'infrastructure

Enfin, le diagramme ci-dessous présente les impacts "business" sur l'organisation. La moyenne se trouve entre 2.5 et 5 qu'est un score 4.4 et qu'est un impact moyen .

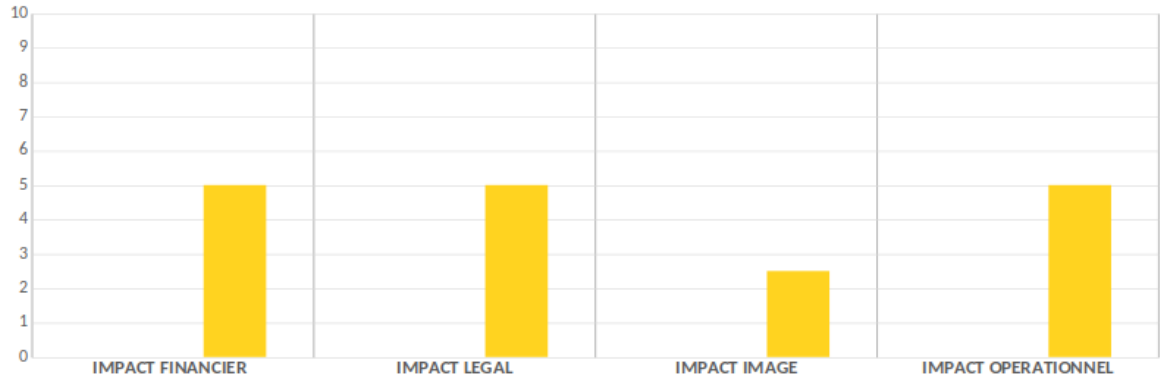


FIGURE V.6 – Impacts "business"

On voit clairement sur la figure V.6 que les switchs qui sont compromis auraient un impact financier, légal et opérationnel.

La figure suivante présente le score du risque globale des vulnérabilités trouver.

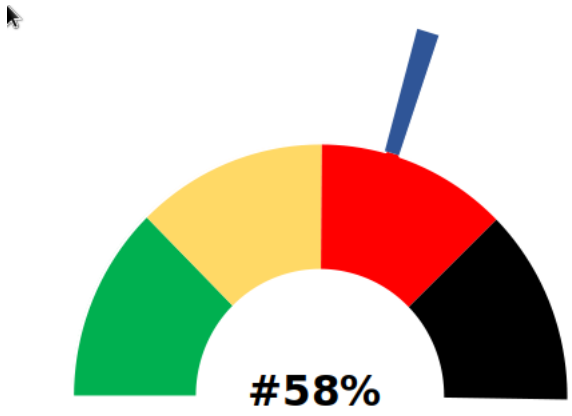


FIGURE V.7 – Score de risque

Le système d'information possède un score de risque de 58 %

V.8.2 Synthèse des vulnérabilités

Au fur et à mesure qu'on découvre des vulnérabilités, le tableau ci-dessus de synthèse technique simple des vulnérabilités identifiées fera un petit listing rapide dans le bilan du rapport, ce qu'est le cas, il présente la liste des vulnérabilités trouver avec leurs degrés de

gravités et d'exploitabilités. .

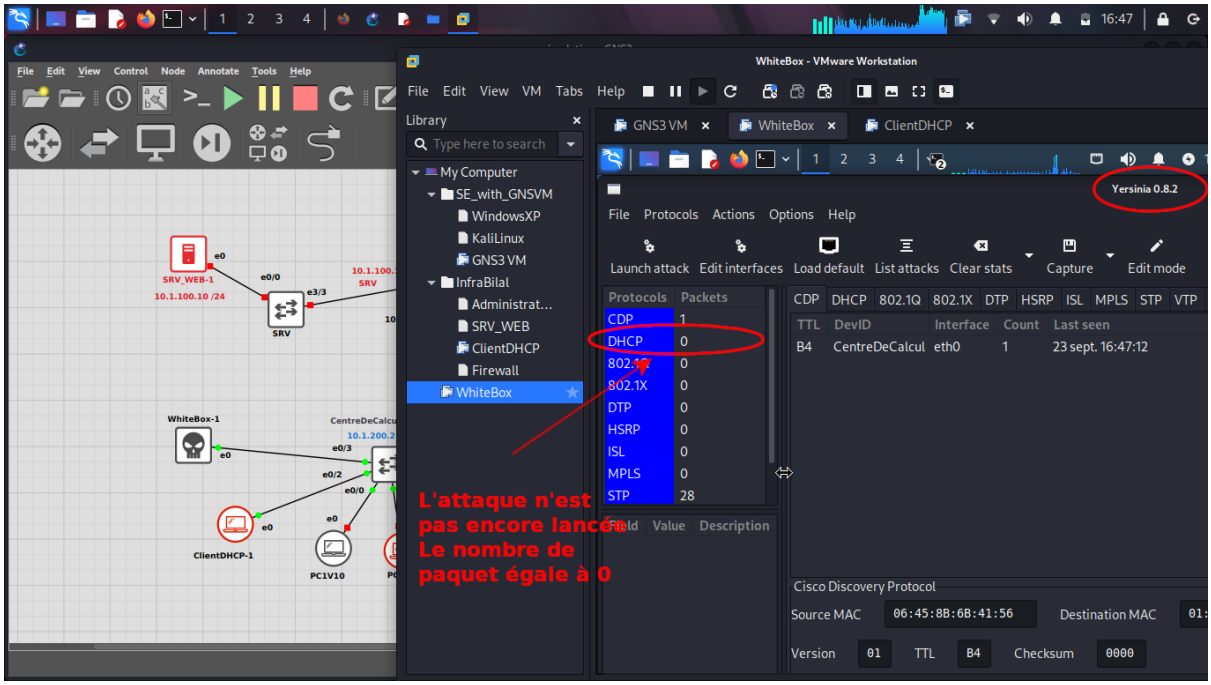
Références	Titre	Composants concernés	Gravité	Exploitabilité
NET 01	Mot de passe d'administration par défaut	Switch1 / Switch2	**Critique**	Modérée
NET 02	Un port ouvert (Vlan 10)	Switch1	Moyenne	Modérée
0	3	0	N/A	N/A
0	4	0	N/A	N/A
0	5	0	N/A	N/A
0	6	0	N/A	N/A
0	7	0	N/A	N/A
0	8	0	N/A	N/A
0	9	0	N/A	N/A

FIGURE V.8 – Synthèse des vulnérabilités

V.8.3 Preuves

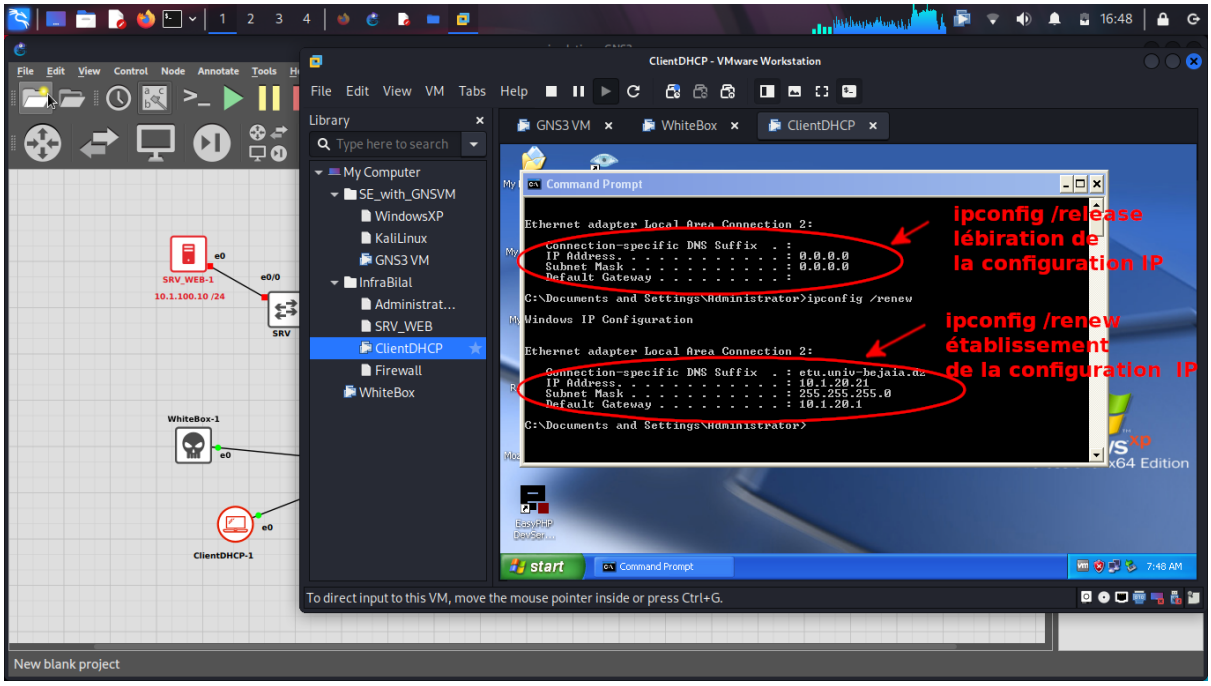
Les images suivantes apportent en guise de preuve l'atteinte des objectifs de l'attaquant.

On a lancé l'outils de teste de vulnérabilité de couche 2 du modèle OSI (yersinia) sur la machine Kali Linux (whitbox), on voit que l'attaque n'est pas encore éffectuer et on remarque que le nombre de paquet envoyer est égale à 0 (voir la figure **A**).



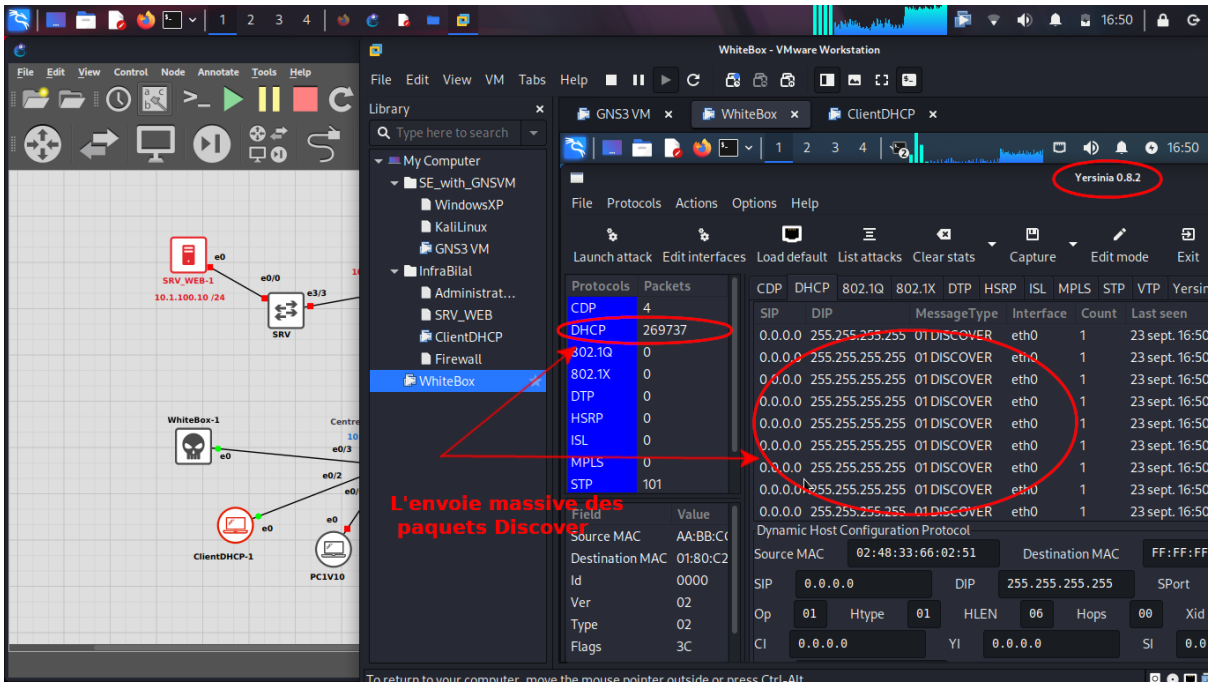
(A)

La figure suivante montre la libération de la configuration IP de la machine Windows XP (ClientDHCP) en tapant `ipconfig /release`, puis on demande à nouveau un établissement de la configuration IP depuis le service DHCP qui se trouve dans le switch core **RG** , en saisissant la commande `ipconfig /renew`.



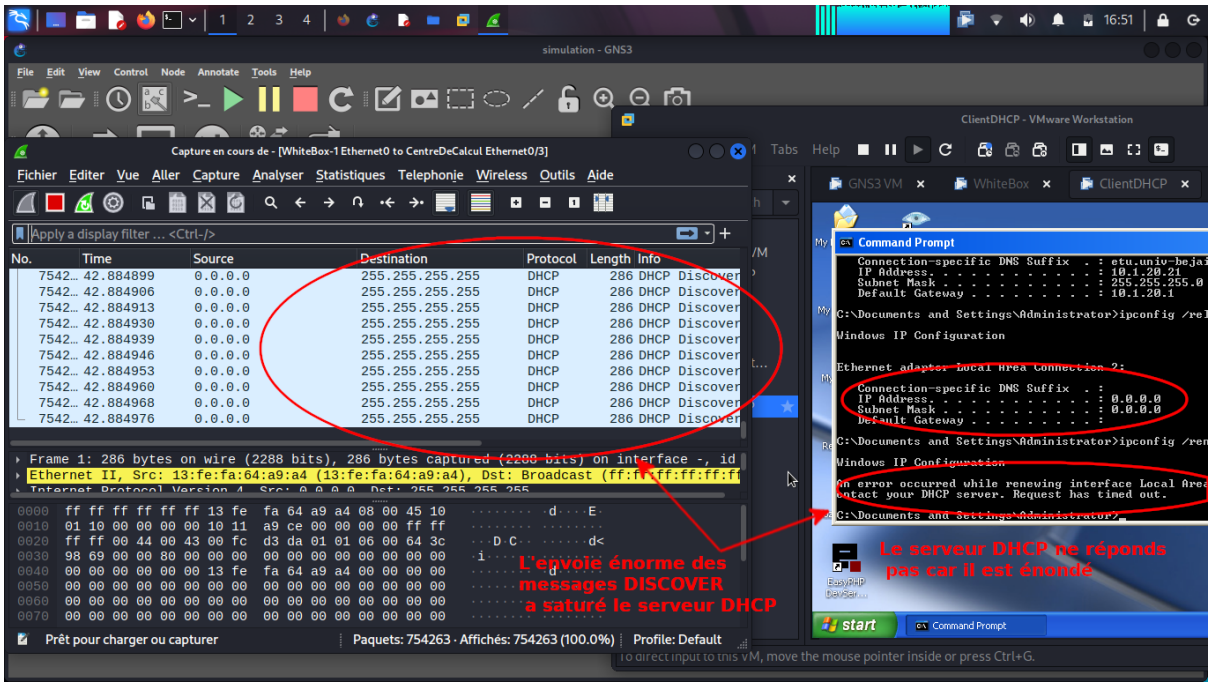
(B)

Maintenant qu'on a lancé l'attaque SYN FLOOD, on voit l'envoit énorme des messages DISCOVER vers le service DHCP (voir la figure **C**).



(C)

D'autre part nous sommes revenus sur notre machine Windows XP (ClientDHCP) pour exécuter la commande `ipconfig /release` et par la suite `ipconfig /renew` et on remarque que c'est impossible d'avoir une configuration IP issue de notre switch core puisqu'il est sous l'attaque de yersinia (voir la figure **D**).



(D)

On remarque que le service DHCP ne répond pas car il est inondé de message DISCOVER.

V.9 Vulnérabilités identifiées

Les tableaux de vulnérabilités identifiées sont le plus important dans le rapport d'audit ou dans chacun de ces tableaux nous fournit des informations importante telque le titre de la vulnérabilité, le composant concercé, le degré d'exploitabilité, le degré de gravité et une description bien détaillée.

① **Mot de passe par défaut :**
Le tableau suivant présente les caractéristiques de la première vulnérabilité.

TABLE V.16 – Vulnérabilité mot de passe par défaut

NET 01	
Titre	**Mot de passe d'administration par défaut**
Composant(s) concerné(s)	Switch1 / Switch2
Exploitabilité	**Modérée**
Gravité	**Critique**
Un attaquant peut obtenir l'accès au menu de des Switchs 1 et 2. Le mots de passe administrateur est celui par défaut,il est pas changé.	

② **Des port ouverts :**
Le tableau suivant présente les caractéristiques de la deuxième vulnérabilité.

TABLE V.17 – Port ouvert

NET 02	
Titre	**Un port ouvert (Vlan 10)**
Composant(s) concerné(s)	Switch1
Exploitabilité	**Modérée**
Gravité	**Moyenne**
Un attaquant peut facilement atteindre le système, le mettre à genoux, Le port e0/3 est up, il faut fermer tout les port non utilisable.	

V.10 Conclusion

Les tests d'intrusion sont un outil essentiel dont les entreprises ont besoin pour découvrir comment leurs systèmes sont vulnérables aux cyber-attaques. Même si les tests d'intrusion internes ne doivent pas être négligés, les menaces à l'internes sont beaucoup moins courantes, ce qui en fait une priorité moins importante.

Conclusion générale

L'objectif initial de cette étude était de présenter l'apport de l'audit de sécurité et de la gestion de la sécurité du système d'information. c'est pourquoi nous avons concentré notre travail sur deux parties.

L'une est la partie théorique et l'autre la partie pratique. La partie théorique consistait à passer en revue les notions d'audit du systéme de managments de la sécurité d'information, normes, référentiels, politiques et méthodes d'audit.

La deuxième partie consiste a la réalisation d'une infrastructure d'une entreprise quelconque afin d'éffectuer un test d'intrusion dessus. En théorie comme en pratique, la notion de sécurité de l'information a pris de l'importance dans le monde des nouvelles technologies d'aujourd'hui.

Étant donné les risques énormes associés à la vulnérabilité des systèmes, à la maladresse ou à la négligence du personnel, des dommages matériels et autres, les entreprises ont maintenant trouvé essentiel de se fournir une variété de moyens pour protéger leurs ressources d'information. Depuis très longtemps, la sécurité des systèmes informatiques et plus généralement des SI est considérée par les sociétés comme un aspect secondaire. Peu à peu, une prise de conscience amène la SSI devant la scène. La raison principale est liée à la multitude d'incidents et plus graves, les pertes qui causent des pertes importantes pour l'entreprise.

La trilogie confidentialité, intégrité, disponibilité, détermine la valeur d'une information. L'SSI vise à assurer la valeur des renseignements que nous utilisons.Si cette garantie n'est plus garantie, on dira qu'il y a eu altération du système d'information.La sécurité de l'information s'applique désormais aux divers secteurs de l'activité économique.

L'exemple du test d'intrusion que nous avons éffectué nous a permis d'apprécier la gestion de la sécurité de l'information.nous savons qu'un systéme quel qu'il soit, n'est à 100% assuré de façon absolue cotre les divers menaces ou risques qui sont de plus en plus multiples par les tecnologies nouvelles de l'information.

Par conséquent, la sécurité de l'information est importante pour toute entreprise qui veut maintenir son activité et son image de marque dans le monde des affaires actuel. Elle doit être la responsabilité de chaque acteur de l'entreprise, peu importe sa position hiérarchique.

Ce qui est considérable à faire est de s'atteler à réduire au maximum les risques qui pourraient survenir et ainsi préserver les différents systèmes d'informations.

Bibliographie

[1] Jean-françois CARPENTIER, La sécurité informatique dans la petite entreprise Etat de l'art et bonne pratique, 2ème édition.

[2] Alexandre Fernandez-Toro, Management de la sécurité de l'information[Mise en place d'un SMSI et audit de certification - Implémentation ISO 27001 et ISO 27002].

[3] ISO, La famille norme ISO 27k, https ://www.iso.org/.

[4] CLUSIF, La mèthode MÉHARI et EBIOS, https ://clusif.fr/.

[5] ANSSI, Méthode de gestion des risques, https ://www.ssi.gouv.fr/.

[6] Cédric Pernet, Sécurité et Espionnage Informatique, 2014.

[7] Cédric Llorens, Laurent Levier, Denis Valois, Benjamin Morin, Tableaux de bord de la sécurité réseau, 3° édition.

[8] ZAC du Moulin Neuf,ENI - Octobre 2009, Sécurité informatique - Ethical Hacking - Apprendre lattaque pour mieux se défendre.

[9] La sécurité informatique, https ://www.ssi.gouv.fr/administration/bonnes-pratiques/.

[10] Outils Pentest infrastructure, https ://github.com/ESD-academy/Outils/tree/master/Pentest%20infra