

# DÉDICACES

Je dédie ce travail à mes chers parents qui m'ont fortement soutenu tout au long de ma vie et dans tous les projets que j'ai entrepris, qui ont partagé avec moi tous les moments d'émotion lors de la réalisation de ce travail..

Tous mes sentiments de reconnaissance, d'amour et de fierté pour eux. Que Dieu, le Tout-Puissant, leur procure santé et bonheur tout au long de leur vie.

Je tiens à exprimer ma gratitude envers mon encadrant pour son expertise, sa disponibilité et sa patience tout au long de ce projet. Grâce à son soutien, j'ai pu acquérir de nouvelles compétences et approfondir mes connaissances dans le domaine de la sécurité informatique.

Je remercie également mon grand frère pour son soutien moral et son aide. Je lui souhaite tout le bonheur et la réussite dans sa vie.

Je remercie particulièrement les responsables et à l'équipement informatique de la société pour leur aide, leur patience et leur disponibilité.

Je dédie également ce travail à mes ami(e)s qui n'ont cessé de me soutenir et de m'encourager à avancer.

# REMERCIEMENTS

Nous remercions en premier lieu **DIEU**, le Tout-Puissant, qui m'a doté d'une santé morale et physique ainsi que du courage et de la force pour pouvoir accomplir ce travail.

Nous tenons à remercier particulièrement notre cher encadrant académique **M. Bayrem Triki**, pour son encadrement, ses précieux conseils, sa patience et sa générosité.

Nous remercions également notre encadrant pour son aide et son soutien durant la période de PFE.

Nous remercions également tous nos enseignants de l'EPI qui nous ont formés en **Cybersécurité**.

Nous n'oublierons jamais tous ceux qui m'ont aidé de près ou de loin à réaliser ce travail.

Mes remerciements vont aussi aux **membres du jury**, qui donneront à mon travail une valeur ajoutée à travers leurs recommandations et leurs remarques si importantes, dont je serai très reconnaissant.

Enfin, un remerciement particulier à tous les membres de **ma famille** ainsi qu'à **nos ami(e)s** et collègues pour leur soutien et leurs encouragements.

# Table des matières

---

<b>Introduction Générale</b>	<b>1</b>
<b>Chapitre 1 : Cadre général du projet</b>	<b>2</b>
Introduction	2
1. Présentation de l'Entreprise	2
2. Contexte du Projet	4
2.1 Problématique	4
2.2 Objectif	4
2.3 Cadre juridique et réglementaire de la mission d'audit	5
3. Lois relatives à la sécurité informatique en Tunisie	6
4. Normes et standards de sécurité informatique	7
5. Les principes de base, objectifs principaux et leur mise en œuvre	8
6. La politique de sécurité	9
5.1 Les principes de la sécurité informatique	11
5.3 Les outils associés à la politique de sécurité	13
7. Conclusion	13
<b>Chapitre 2 : Les fondements de PCI DSS</b>	<b>14</b>
Introduction	14
1. Présentation de PCI DSS	15
2. Niveaux de conformité	17
3. Contrôles de sécurité PCI DSS	18
4. Entités concernées par la conformité à la norme PCI DSS	21
5. Avantages de la norme PCI-DSS	22
6. Quels sont les impacts du non-respect de la norme PCI DSS	23
7. Meilleures pratiques pour la conformité PCI-DSS	24
8. Conclusion	25
<b>Chapitre 3 : L'audit de sécurité informatique</b>	<b>26</b>
Introduction	26
1 . Définition d'un audit	26
2. Rôle et Objectif de l'Audit	27
3. Relation entre l'Audit Informatique et PCI DSS :	28
4. Processus d'audit de sécurité du cycle de vie des systèmes d'information	29
5. Processus de mise en œuvre d'une mission d'audit de sécurité des systèmes d'information	31
5.1 Élaboration de la Charte d'Audit	31
5.2 Préparation de l'audit	32
5.3 Audit Organisationnel et Physique	32
5.4 Audit Technique	33
5.5 Audit Intrusif	34

5.6 Rapport d'Audit	35
6 . La méthode MEHARI	35
6.1 Principe de fonctionnement	36
6.2 Mise en place de la méthode	36
7. Référence CIS Microsoft Windows Server 2016	37
7.1 Méthodologie	38
7.2 Principales Recommandations du Benchmark CIS	38
7.3 Politique de mot de passe	39
7. Conclusion	41
<b>Chapitre 4 : Réalisation</b>	<b>42</b>
Introduction	42
1 .Présentation du périmètre	42
2. Présentation des échelles utilisées	45
3. Outil d'audit utilisés	47
4 . Etat de maturité de la sécurité du système d'information	47
5. Audit organisationnelles et physiques	50
6 . Taxonomies des failles techniques	56
6.1 Scan de Vulnérabilités de PCI DSS	56
6.1 Pentest externe :	58
6.2 Pentest interne :	63
6.2.1 Évaluation de la Sécurité de la Zone DMZ	64
6.2.1 Mécanisme / politique d'accès défaillant	67
6.2.2 Évaluation de la Sécurité de la Zone LAN	70
6.3 audit de configuration	72
6.3.1 Accès privilégié	73
6.3.2 - Analyse de la politique d'usage des mots de passe	74
6.3.3 - Analyse du Firewall	75
7. Recommandations	75
8. Conclusion	80
<b>Conclusion Générale</b>	<b>81</b>
<b>Webographie</b>	<b>82</b>
<b>Annexes</b>	<b>83</b>
Annexe A	83

# Liste des figures

---

Figure 1.1 : Services de IT CyberSec Expert	3
Figure 1.2 : Logo IT-CyberSec	4
Figure 1.3 : Pyramidale des politiques de sécurité	10
Figure 1.4 : Stratégie et politique de sécurité	11
Figure 2.1 : Les six domaines de la conformité de PCI DSS	14
Figure 2.2 : Types de Données sur une Carte de Paiement	17
Figure 3.1 : Le cycle de vie d'audit de sécurité	30
Figure 3.2 : Schéma du processus d'audit	31
Figure 3.3 : Enjeux critique + Vulnérabilités fortes = Risques inacceptables	36
Figure 3.4 : CIS Microsoft Windows Server 2016 Benchmark	37
Figure 4.1 : Infrastructure de l'entreprise lors de l'audit	43
Figure 4.2 : Résultats de scan des vulnérabilités PCI DSS	51
Figure 4.2 : générateur à l'extérieur de la société	50
Figure 4.3: Exemples d'observations de chers visiteurs	51
Figure 4.4: plan physique de la société	52
Figure 4.5: Engagement de confidentialité visiteur	53
Figure 4.6: avant entre du SAS	54
Figure 4.7: Sortie du SAS	54
Figure 4.8: la salle mailer	55
Figure 4.9 : Résultats de scan des vulnérabilités PCI DSS	57
Figure 4.10 : Scan tous les ports TCP	58
Figure 4.11 : Scan tous les ports UDP	59
Figure 4.12 : détecté la présence d'un pare-feu	59
Figure 4.13 : Scan port pare-feu	60
Figure 4.14 : Version de Firewall	61
Figure 4.15 : Scan des port ouvert avec Nessus	64
Figure 4.16 : Scan de vulnérabilités de zone DMZ	64
Figure 4.17 : Scan des port ouvert avec NMAP	65
Figure 4.18 : service info de version et os de serveur FTP	66

Figure 4.19 : Brute Force de FTP	66
Figure 4.20 : Interface login d'Imprimante	69
Figure 4.21 : Preuve de réussite de l'exploitation imprimant	69
Figure 4.22 : Résultat de scan de zone LAN	70
Figure 4.23 : Interface login de Switch	71
Figure 4.24 : Preuve de réussite de l'exploitation Switch	72

## Liste des tableaux

---

Table 2.1 : Exigences du Standard PCI DSS	15
Table 2.2 : Données de Compte	16
Table 3.1 : Tableau de Politique de mot de passe	41
Table 4.1 : L'échelle de risque	45
Table 4.2 : Le niveau de risque d'une vulnérabilité	46
Table 4.3 : Échelle de gravité métier	46
Table 4.3 : Outil d'audit utilisés	47
Table 4.4 : Terminaux finaux des utilisateurs	48
Table 4.5 : Droits d'accès privilégiés	49
Table 4.6 : Restriction d'accès aux informations	49
Table 4.7 : Masquage des données	50
Table 4.8 : Évasion de pare-feu et Usurpation	60
Table 4.9 : Remote Code Execution	62
Table 4.10 : Métriques d'Exploitabilité de Remote Code Execution	63
Table 4.11 : Métriques d'Impact de Remote Code Execution	63
Table 4.12 : Mécanisme de gestion d'accès	67
Table 4.13 : Métriques d'Exploitabilité de mécanisme de gestion d'accès	68
Table 4.14 : Métriques d'Impact de mécanisme de gestion d'accès	68
Table 4.15 : Mauvaise configuration de sécurité	71
Table 4.16 : Métriques d'Impact de mauvaise configuration de sécurité	71

# Acronymes

---

**AD** : Active Directory

**BGP** : Border Gateway Protocol

**CVSS** : Common Vulnerability Scoring System

**DSI** : Directeur des Systèmes d'Information

**EBIOS** : Étude des Besoins et Identification des Objectifs de Sécurité

**FTP** : File Transfer Protocol

**ICMP** : Internet Control Message Protocol

**IP** : Internet Protocol

**ISO** : Organisation Internationale de Normalisation

**MAC** : Media Access Control

**MEHARI** : Méthode Harmonisée d'Analyse des Risques

**NIST** : National Institute of Standards and Technology

**OCTAVE** : Operationally Critical Threat, Asset, and Vulnerability Evaluation

**DICP** : Disponibilité, Intégrité, Confidentialité, Preuve

**PME** : Petites et Moyennes Entreprises

**POS** : Plans Opérationnels de Sécurité

**PSS** : Plans Stratégiques de Sécurité

**SAS** : Statistical Analysis System

**SMI** : Système de Management de l'Information

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

**SMTP** : Simple Mail Transfer Protocol

**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



## **POLITIQUE DE CONFIDENTIALITÉ**

- DANS LE SOUCI D'ASSURER LA CONFIDENTIALITÉ DES DONNÉES AU SEIN DU CABINET IT CYBERSEC EXPERT, LE NOM DU CLIENT DE LA MISSION D'AUDIT IT À LAQUELLE J'AI ÉTÉ AFFECTÉ EST CONFIDENTIEL.

# Introduction Générale

---

La sécurité des systèmes d'information est devenue un enjeu crucial. Elle pose des questions nouvelles en termes de respect des droits et des libertés individuels, elle est un facteur de différenciation pour les entreprises et contribue directement au développement de nouveaux services. Elle est également au centre des relations entre l'Etat, l'entreprise, les partenaires sociaux et le citoyen. Longtemps reléguée au second plan et limitée à un seul volet technologique, la sécurité de l'information est aujourd'hui au cœur de la création de valeur et s'adresse à tous les acteurs de la société.

Le rapport est structuré de manière à fournir une vue d'ensemble complète de mon expérience de stage, en mettant particulièrement l'accent sur l'audit technique réalisé conformément aux normes PCI DSS (Payment Card Industry Data Security Standard). Cette norme revêt une importance cruciale dans le domaine de la cybersécurité, garantissant la sécurité des données des titulaires de cartes de paiement.

Notre projet se compose du contenu du rapport suivant :

La première partie présente des généralités sur la sécurité informatique et sur une mission d'audit ainsi qu'un aperçu sur les normes de sécurité de l'information

Le deuxième chapitre abordera les fondements de PCI DSS et Niveaux de conformité

Le troisième chapitre décrit la L'audit de sécurité informatique est les processus en présentant notamment leur méthode

Enfin, le quatrième chapitre portera sur la réalisation de la mission d'audit et les outils utilisés est présentée partie technique .

En conclusion, nous synthétisons l'ensemble de notre travail.

# Chapitre 1 : Cadre général du projet

---

## Introduction

Dans ce chapitre nous allons présenter l'organisme d'accueil, contexte général notre projet de fin étude ainsi qu'à la problématique est cadre juridique et réglementaire de la mission d'audit .

### 1. Présentation de l'Entreprise

IT CyberSec Expert est une entreprise reconnue pour son expertise spécialisée dans le domaine de la cybersécurité. Son engagement inébranlable envers la protection des actifs numériques de ses clients en fait un acteur majeur dans le secteur. Fondée sur les principes d'intégrité, d'innovation et d'engagement envers l'excellence, en fournissant des services de pointe en matière de tests de pénétration, de sécurité des applications web, audit , et de consultation en sécurité informatique [1].

L'entreprise offre une gamme complète de services de cybersécurité pour répondre aux besoins variés de ses clients.

#### Domaines d'Expertise :

- **Tests de Pénétration** : IT CyberSec Expert excelle dans la réalisation de tests de pénétration approfondis, identifiant les vulnérabilités potentielles et renforçant la résilience des systèmes.
- **Sécurité des Applications Web** : L'entreprise se spécialise dans la sécurisation des applications web, un domaine critique où les attaques sont fréquentes.

- **Audit de Sécurité Informatique** : Les experts d'IT CyberSec apportent leur savoir-faire en matière de cybersécurité, offrant des conseils stratégiques pour renforcer la posture de sécurité des entreprises.



**Services Certifiés**  
Nous sommes qualifiés par l'Agence Nationale de la Sécurité Informatique (ANSI), afin de vous fournir des audits, expertises et tests d'intrusion qualitatifs.

**Équipe talentueuse et qualifiés**  
Notre équipe est composée d'experts consultants en cyber sécurité hautement qualifiée, et d'une équipe technique compétente et ultra passionnés.

**Nous Offrons une assistance rapide 24/7**  
Intervenir en cas d'incident ,pour assurer une continuité d'activité avec délégation des responsabilités en toutes transparences.

**Figure 1-1 : Services de IT CyberSec Expert**

**Points Forts :**

- **Intégrité** : IT CyberSec Expert opère avec une intégrité inébranlable, assurant la confidentialité et la protection des données de ses clients.
- **Innovation** : L'entreprise reste à la pointe de l'innovation, anticipant les nouvelles menaces et développant des solutions adaptées.
- **Engagement** : Engagée envers l'excellence, IT CyberSec Expert collabore étroitement avec ses clients pour atteindre les plus hauts standards de sécurité.

Ce contexte souligne l'importance cruciale de l'audit technique dans le cadre des activités de sécurité informatique d'IT CyberSec Expert et met en évidence l'engagement de

l'organisation envers la conformité aux normes de sécurité les plus élevées pour assurer la protection des données de ses clients.



**Figure 1-2 : Logo IT-CyberSec**

## **2. Contexte du Projet**

### **2.1 Problématique**

Nous sommes confrontés non seulement à une augmentation de la quantité, mais aussi et surtout à l'importance croissante des transactions financières au cœur des activités frauduleuses. L'ensemble formé par tout le réseau d'utilisateurs de ce système d'information doit être connu pour être sûr. Les ressources qui y circulent doivent absolument être protégées, et pour cela, la maîtrise du système d'information est indispensable. Chaque acteur du système a un rôle à respecter qui doit être défini scrupuleusement.

### **2.2 Objectif**

La mission d'audit réglementaire de sécurité, en application du **décret-loi 2023-17 du 11 mars 2023**, menée pour la société, visait à atteindre plusieurs objectifs essentiels :

- Identifier les écarts par rapport aux meilleures pratiques de sécurité.
- Proposer des mesures d'amélioration pour renforcer le niveau de sécurité du système d'information.

L'audit avait pour but spécifique d'évaluer la conformité de l'entreprise aux normes ISO 27001 et PCI DSS dans ses processus de création et de fourniture de services de sécurité informatique.

En outre, cette évaluation de sécurité informatique permet d'évaluer la conformité de l'organisation à une politique de sécurité définie ou à un ensemble de règles de sécurité.

## **2.3 Cadre juridique et réglementaire de la mission d'audit**

L'audit de la sécurité des systèmes d'information en Tunisie est régi par le **Décret-loi 2023-17 du 11 mars 2023** et organisé par l'arrêté conjoint du ministre des technologies de la communication et de l'économie numérique et du ministre du développement, de l'investissement et de la coopération internationale du 1er octobre 2019. Cet arrêté fixe le cahier des charges relatif à l'exercice de l'activité d'audit dans le domaine de la sécurité informatique. Les critères techniques d'audit et les modalités de suivi de la mise en œuvre des recommandations contenues dans le rapport d'audit sont également définis par arrêté du ministre des technologies de la communication [2].

### **L'obligation de l'audit concerne :**

- Les systèmes informatiques et les réseaux des organismes publics,
- Les opérateurs de réseaux publics de télécommunications et les fournisseurs de services de télécommunications et d'internet,
- Les entreprises dont les réseaux informatiques sont interconnectés via des réseaux de télécommunications,
- Les fournisseurs de services d'hébergement et d'informatique en nuage,
- Les entreprises qui traitent automatiquement les données personnelles de leurs usagers dans le cadre de la fourniture de leurs services à travers les réseaux de télécommunications,
- Les infrastructures numériques d'importance vitale.

Les seules personnes habilitées à effectuer ces missions d'audit sont les **auditeurs certifiés par l'Agence nationale de la Cybersécurité**, conformément à l'arrêté du 1er octobre 2019 fixant le cahier des charges relatif à l'exercice de l'activité d'audit dans le domaine de la sécurité informatique.

**La circulaire n°24 du 5 novembre 2020**, relative au renforcement des mesures de sécurité des systèmes d'information dans les établissements publics, stipule entre autres la création d'un Comité de pilotage et d'une Cellule opérationnelle de sécurité ainsi que la nomination d'un Responsable de la Sécurité des Systèmes d'Information (RSSI). Elle présente également l'ensemble des mesures que ces établissements doivent respecter pour garantir la sécurité des sites web et des services en ligne.

### **3. Lois relatives à la sécurité informatique en Tunisie**

En Tunisie, la sécurité informatique est réglementée par plusieurs lois et réglementations visant à protéger les données, les infrastructures et les systèmes informatiques [2].

Voici quelques-unes des principales lois relatives à la sécurité informatique en Tunisie :

- **Loi n°2004-63 du 27 juillet 2004** relative à la protection des données à caractère personnel : Cette loi établit les principes et les règles régissant la collecte, le traitement et la protection des données personnelles en Tunisie. Elle vise à garantir la confidentialité, l'intégrité et la disponibilité des données personnelles traitées par les organisations.
- **Loi n°2009-04 du 3 février 2009** relative à la sécurité des systèmes et des données informatiques : Cette loi vise à protéger les systèmes informatiques et les données contre les menaces et les attaques informatiques. Elle établit des mesures de sécurité obligatoires pour les entreprises et les organisations opérant en Tunisie, et prévoit des sanctions en cas de violation de ces mesures.
- **Loi n°2016-47 du 14 juin 2016** relative à la protection des données à caractère personnel : Cette loi renforce le cadre juridique relatif à la protection des données

personnelles en Tunisie en alignant la législation nationale sur les normes internationales telles que le Règlement Général sur la Protection des Données (RGPD) de l'Union européenne.

- **Décret n°2016-3662 du 26 décembre 2016** portant création de l'Agence Nationale de la Sécurité Informatique (ANSI) : Ce décret établit l'ANSI en tant qu'organisme gouvernemental chargé de coordonner les efforts de sécurité informatique en Tunisie, de promouvoir la sensibilisation à la sécurité informatique et de fournir une assistance technique aux entreprises et aux organisations.

## 4. Normes et standards de sécurité informatique

Assurer le fonctionnement continu et la protection d'un Système d'Information n'est plus aujourd'hui considéré comme un simple exploit mais plutôt une nécessité. Parmi toutes les tâches qui incombent aux Responsables de la Sécurité des Systèmes d'Information (R.S.S.I) dans les organismes privés ou publics, celle qui consiste à bâtir une politique de sécurité cohérente prenant en compte les aspects humains, organisationnels et juridiques est certainement la plus difficile. Une telle politique doit se baser sur une norme bien spécifique. En effet, il existe de nombreuses normes et méthodes sur lesquelles se basent les missions d'audit de la sécurité des systèmes d'information [4] .

Une norme (qui peut être organisationnelle ou technique) à un objet souvent très vaste et s'appuie généralement sur des concepts ou des notions générales. Le champ d'application de chaque concept doit alors être précisé, pour que la norme puisse être appliquée efficacement.

Voici quelques-unes des normes et standards les plus couramment utilisés dans le domaine de la cybersécurité :

- **La norme ISO/IEC 27001** : définit les exigences en matière de mise en place d'un système de management de la sécurité de l'information. Elle est alignée avec les autres normes de système de management, y compris ISO 9001 (management de la



qualité) et ISO 14001 (management environnemental).et améliorer un système de management de la sécurité de l'information (SMSI).

- **PCI DSS (Payment Card Industry Data Security Standard)** : Il s'agit d'un ensemble de normes de sécurité des données conçu pour garantir la sécurité des transactions par carte de crédit et débit, notamment les exigences de stockage, de transmission et de traitement des données de carte de paiement.
- **La norme ISO/IEC 27005** fixe un cadre pour la gestion des risques de sécurité de l'information. Elle fournit ainsi les conditions à respecter par toute démarche méthodologique. S'y conformer permet de garantir que les principes communément reconnus ont été appliqués. La norme constitue une référence utile pour les faire respecter, sans préjuger des méthodes et outils nécessaires pour les mettre en œuvre.
- **NIST (National Institute of Standards and Technology)** : Ce cadre fournit des lignes directrices sur la façon de gérer et de sécuriser les systèmes d'information en identifiant, protégeant, détectant, répondant et récupérant contre les menaces.
- **GDPR (General Data Protection Regulation)** : Ce règlement de l'Union européenne vise à protéger les données personnelles des individus en réglementant leur collecte, leur stockage, leur traitement et leur transfert.

## 5. Les principes de base, objectifs principaux et leur mise en œuvre

La sécurité des données repose sur quatre objectifs principaux, représentés par l'acronyme **DICP (Disponibilité, Intégrité, Confidentialité et Preuve)** :

- **La disponibilité** : garantit que les personnes autorisées ont accès à l'information lorsque nécessaire ou dans les délais requis pour son traitement.
- **L'intégrité** : assure l'absence de modification ou d'altération d'une information, ainsi que la complétude des processus de traitement. Pour les messages échangés, elle vise à protéger contre toute altération accidentelle ou intentionnelle.
- **La confidentialité** : garantit que l'information n'est accessible qu'aux personnes autorisées et ne sera pas divulguée en dehors d'un environnement spécifié. Elle concerne la protection contre l'accès non autorisé aux données stockées ou échangées,

réalisée par des mécanismes de chiffrement lors du transfert ou du stockage des données.

- **La preuve** : assure que l'émetteur d'une information est correctement identifié et possède les droits d'accès nécessaires, et que le récepteur identifié est autorisé à accéder à l'information.

Les objectifs de base peuvent être atteints grâce à des solutions de sécurité comprenant des matériels, des logiciels, des procédures et un support opérationnel, notamment :

- **Pour l'intégrité des données et la confidentialité** : gestion des accès physiques et logiques, sécurisation du réseau.
- **Pour la disponibilité** : redondance des systèmes, bonnes pratiques en matière d'alimentation électrique, sauvegarde et archivage des données.

## 6. La politique de sécurité

La politique de sécurité vise à définir la protection des systèmes d'information de l'entreprise. Elle englobe un ensemble de principes définissant une stratégie, des directives, des procédures, des codes de conduite et des règles organisationnelles et techniques. Son objectif est de mettre en place une sécurité adaptée aux besoins, économiquement viable et conforme à la législation [6].

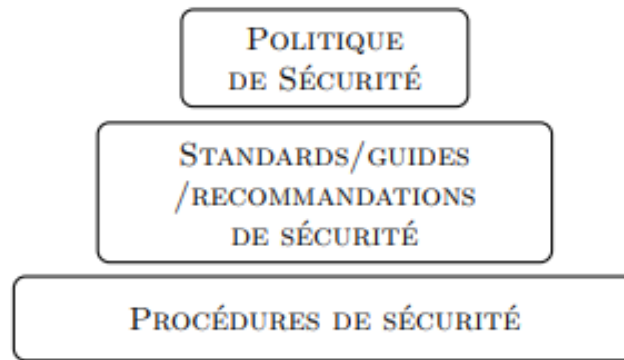
Cette politique doit être formalisée sous forme de document au sein de l'entreprise. Elle résume les pratiques régissant la gestion, la protection et la transmission des informations critiques ou sensibles de l'organisation. La documentation de la norme ISO 27001 peut aider à l'élaboration de ce référentiel.

Il est recommandé d'inclure les thèmes suivants :

- L'organisation et les structures de l'entreprise impliquées dans la gestion de la sécurité.
- Les éléments fondamentaux d'une culture de sécurité.
- Le maintien de la cohérence dans les solutions techniques mises en œuvre.

- Les moyens prévus pour la mise en œuvre et les méthodes de pilotage.

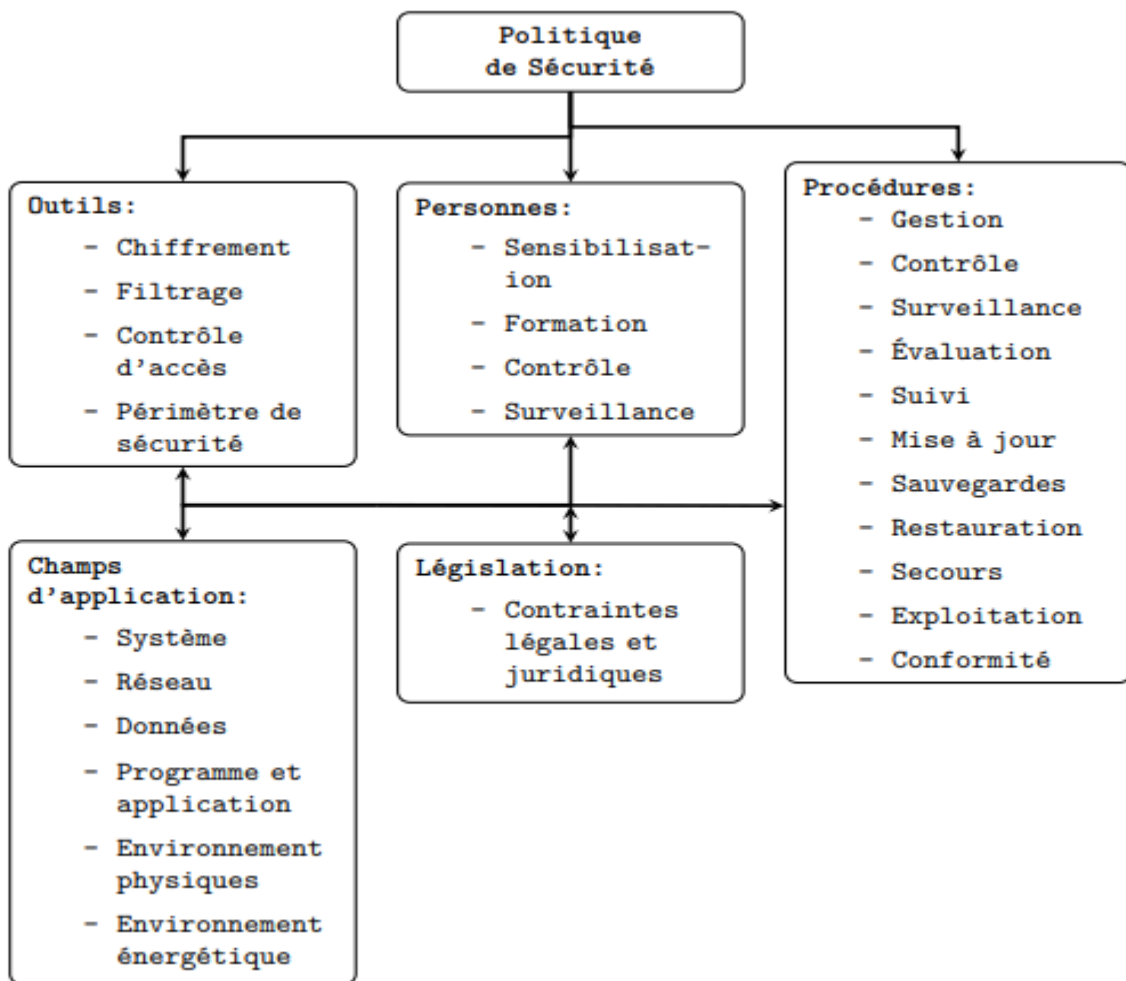
La Figure illustre le positionnement respectif de chaque document.



**Figure 1-3 :** Pyramide des politiques de sécurité

La politique exprime les besoins, tandis que la procédure ou la recommandation technique représente l'implémentation de ces besoins. Par exemple, lorsque certains pare-feu présentent les règles de filtrage comme une politique de sécurité, c'est le concept même de politique de sécurité qui est utilisé.

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



**Figure 1-4 : Stratégie et politique de sécurité**

## 5.1 Les principes de la sécurité informatique

Le rôle principal de la sécurité informatique se décline en trois démarches principales :

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

La première étape consiste à délimiter le périmètre de sécurité, c'est-à-dire la zone correspondant aux services (authentification, contrôle d'accès physique et logique, disponibilité, intégrité et confidentialité) utilisés sur le réseau d'entreprise (postes clients, réseaux LAN et WAN), sur les serveurs, ainsi que les points d'accès externes (serveurs distants, accès VPN, etc.). Le réseau d'entreprise inclut désormais les terminaux mobiles et le cloud computing.

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

Les principes de base de cette sécurité imposent 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) et les logiciels applicatifs, notamment pour ceux qui sont établis en protection (antivirus, etc.).
- Suivre les recommandations des éditeurs concernant la gestion des mots de passe des comptes privilégiés.

Pour élaborer 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, données sensibles de l'entreprise, services et applications (internes et externes).
- Découvrir les réseaux de communication : cela implique de repérer les interactions entre les différents matériels et logiciels, d'identifier les applications et services communiquant avec l'extérieur.

### **5.3 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 bonnes pratiques et de procédures. Si les documents présentant les normes peuvent être acquis, les guides et procédures doivent être rédigés 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 de manière claire et adaptée au personnel concerné et à sa fonction dans l'entreprise.

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

## **7. Conclusion**

L'audit est une démarche collaborative visant à assurer l'exhaustivité de l'analyse. Bien qu'elle soit moins réaliste qu'un test, elle permet en contrepartie de passer méthodiquement en revue l'ensemble du réseau ainsi que chacun de ses composants en détail. Dans le chapitre suivant, nous mettrons l'accent sur l'étude de l'existant et l'identification du système cible.

# Chapitre 2 : Les fondements de PCI DSS

## Introduction

Les pirates informatiques ont pour objectif principal de générer des profits, ce qui place les transactions financières au cœur de leurs activités frauduleuses et cybercriminelles. Par exemple, un rapport de **2022** a révélé une augmentation de **257 %** des attaques contre les applications Web et les API des entreprises de services financiers par rapport à l'année précédente. De plus, les données de la Federal Trade Commission indiquent que les consommateurs subiront des pertes de près de 8,8 milliards de dollars en 2022 en raison de la fraude financière, soit une augmentation de **44 %** par rapport aux chiffres de 2021. Afin de contrer cette vague de fraude financière et de criminalité liée aux données de carte de paiement, le PCI Security Standards Council propose une norme de sécurité de l'information appelée PCI DSS (Payment Card Industry Data Security Standard). Voici un aperçu des exigences de la norme PCI DSS.

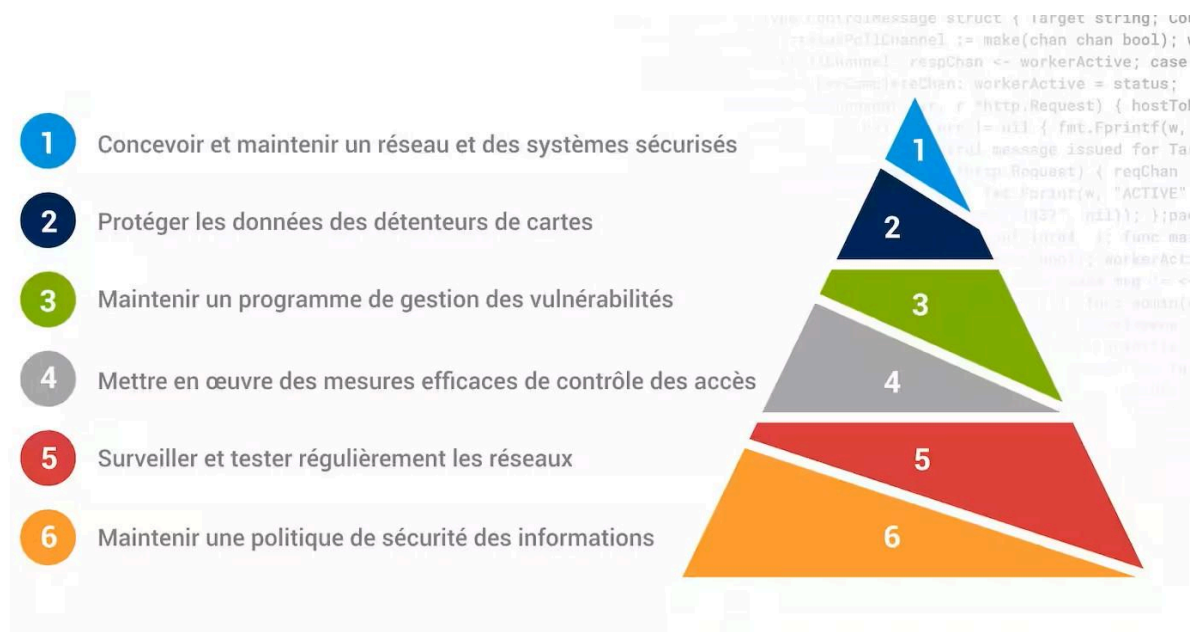


Figure 2-1 : Les six domaines de la conformité de PCI DSS

## 1. Présentation de PCI DSS

Le PCI DSS est un ensemble de normes de sécurité introduit en 2004 ; ces normes s'appliquent à toute organisation qui accepte, traite, stocke ou transmet des données de carte de crédit. Le PCI DSS est administré par le PCI SSC (Payment Card Industry Security Standards Council), un consortium composé des principales sociétés de cartes de crédit : Mastercard, Visa, Discover, American Express et JCB [3].

Le PCI DSS est aujourd'hui une norme mondialement reconnue qui garantit la sécurité des données des cartes de paiement et prévient les failles de sécurité. Cependant, cette norme de cybersécurité est sujette à des changements en raison de l'émergence et de l'évolution des menaces. La dernière version, le PCI DSS v4.0, a été publiée en mars 2022, et la conformité totale est exigée en mars 2025 (12 mois après le retrait du PCI DSS v3.2.1 en mars 2024).

Objectifs	Exigences du Standard PCI DSS
<b>créer et Maintenir un réseau et des Systèmes Sécurisés.</b>	<ol style="list-style-type: none"><li>1. Installer et maintenir des mesures de sécurité du réseau</li><li>2. Applique des configurations sécurisées à tous les composants du système</li></ol>
<b>Protéger les Données de cartes</b>	<ol style="list-style-type: none"><li>3. Protéger les données de cartes pendant leur conservation</li><li>4. Protéger les données des titulaires de carte grâce à une cryptographie robuste lors de la transmission sur des réseaux publics ouverts</li></ol>
<b>Maintenir un Programme de gestion des Vulnérabilités</b>	<ol style="list-style-type: none"><li>5. Protéger tous les systèmes et réseaux contre les logiciels malveillants</li><li>6. Développer et maintenir des systèmes et des logiciels sécurisés</li></ol>
<b>Mettre en oeuvre des Mesures Robustes de contrôle D'accès</b>	<ol style="list-style-type: none"><li>7. Limiter l'accès aux composants système et aux données des titulaires de cartes en fonction des besoins de l'entreprise</li><li>8. Identifier les utilisateur est authentifier l'accès aux composants système</li><li>9. Limiter l'accès physique aux données des titulaire des cartes</li></ol>
<b>Surveiller et tester Régulièrement les Réseaux</b>	<ol style="list-style-type: none"><li>10. Enregistrer et surveiller tous les accès aux composants système et aux données des titulaire de cartes</li><li>11. Tester régulièrement la sécurité des systèmes et des réseaux</li></ol>
<b>Maintenir une Politique de Sécurité des informations</b>	<ol style="list-style-type: none"><li>12. Renforcer la sécurité des informations à l'aide de politique et des programmes organisationnels</li></ol>

**Table 2.1 :** Exigences du Standard PCI DSS



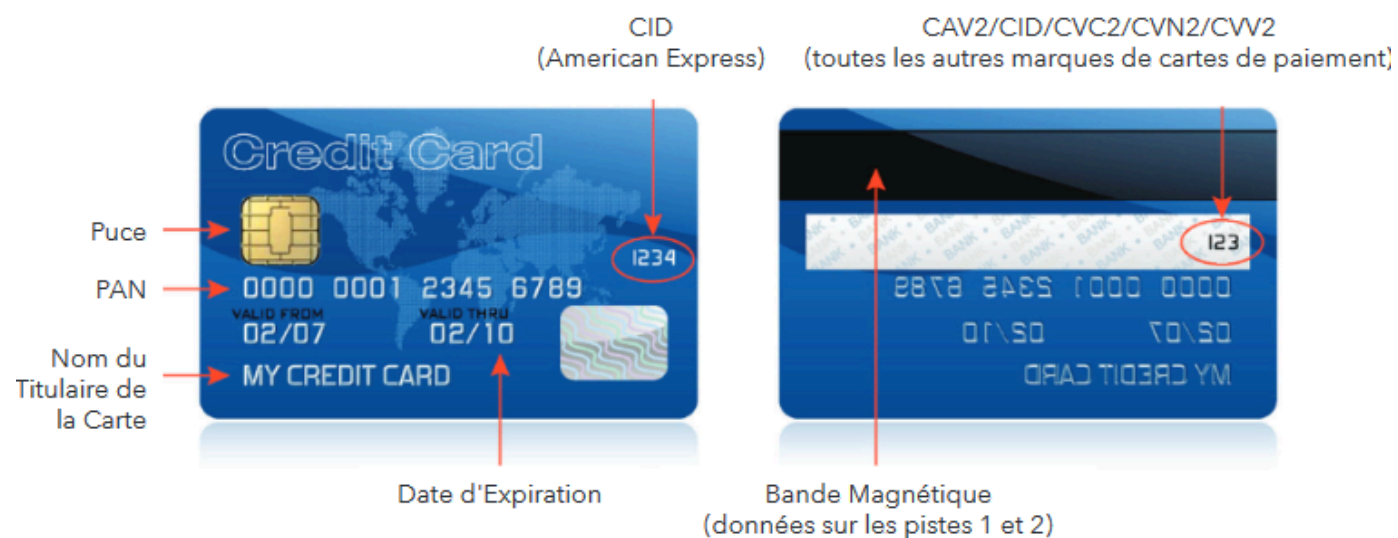
Le standard PCI DSS est destiné à toutes les entités qui stockent, traitent ou transmettent des données de titulaires de cartes (CHD) et/ou des données d'authentification sensibles (SAD) ou qui pourraient avoir une incidence sur la sécurité de l'environnement de données des titulaires de cartes (CDE).

### Données de Compte :

Les Données des Titulaires de Cartes comprennent :	Les Données d'Authentification Sensibles Comprennent :
<ul style="list-style-type: none"> <li>• Le Numéro de compte primaire (PAN)</li> <li>• Le Nom du titulaire de carte</li> <li>• Date d'expiration</li> <li>• Le code de service</li> </ul>	<ul style="list-style-type: none"> <li>• Les données de piste complète (données de la piste magnétique ou équivalent sur une puce)</li> <li>• Le code de vérification de la carte</li> <li>• Les "Pins/Pin blocs"</li> </ul>

**Table 2.2 : Données de Compte**

Le schéma suivant montre où se trouvent les données illustrées dans le tableau ci-dessus sur une carte de paiement. Ces éléments de données de compte sur les cartes de paiement physiques existent également dans les appareils dotés d'une fonctionnalité qui émule une carte de paiement, comme un token de paiement sur un appareil mobile ou une montre intelligente.



**Figure 2-2 : Types de Données sur une Carte de Paiement**

La norme PCI DSS vise de nombreuses menaces, notamment les suivantes :

- Logiciels malveillants
- Hameçonnage (Phishing)
- Contrôle et authentification de l'accès à distance
- Mots de passe faibles
- Logiciels hérités
- Attaques par vol de données de cartes bancaires

## 2. Niveaux de conformité

Tous les commerçants ne traitent pas le même volume de ventes ni ne disposent des mêmes ressources réseau. C'est pourquoi PCI-DSS catégorise les exigences de conformité en fonction des niveaux de commerçants.

Les niveaux de commerçants sont déterminés en fonction du volume de transactions par carte de crédit Visa. Bien que la conformité à la norme PCI-DSS concerne les commerçants de toutes tailles, le niveau de conformité requis dépend du niveau du commerçant [3].

Les niveaux de commerçants sont les suivants :

- **Niveau 1** : Comprend les commerçants traitant plus de six millions de transactions Visa par an. Ces entreprises sont généralement de très grandes entreprises mondiales. Visa se réserve le droit de classer un commerçant dans cette catégorie à sa discrétion pour réduire le risque. Un vérificateur Visa évalue la conformité une fois par an, et les commerçants de niveau 1 doivent soumettre une analyse PCI en utilisant un fournisseur d'analyse approuvé.
- **Niveau 2** : Englobe les commerçants traitant entre un million et six millions de transactions Visa par an. Les commerçants de niveau 2 doivent soumettre un questionnaire d'auto-évaluation (SAQ) pour garantir leur conformité au niveau 2 et effectuer des balayages PCI trimestriels.

- **Niveau 3** : Inclut les commerçants traitant entre 20 000 et un million de transactions de commerce électronique Visa par an. Les commerçants de niveau 3 doivent soumettre un questionnaire d'auto-évaluation (SAQ) pour s'assurer de leur conformité au niveau 3 et effectuer des analyses PCI trimestrielles.

- **Niveau 4** : Englobe les commerçants traitant moins de 20 000 transactions de commerce électronique Visa par an, ou les marchands traitant jusqu'à un million de transactions Visa standard par an. Les commerçants de niveau 4 doivent soumettre un questionnaire d'auto-évaluation (SAQ) pour garantir leur conformité au niveau 4 et effectuer des analyses PCI trimestrielles.

### 3. Contrôles de sécurité PCI DSS

Bien que la plupart des réglementations de conformité exigent de nombreux changements d'infrastructure et d'outils de sécurité, la norme PCI-DSS comporte un nombre limité d'exigences, mais elles sont essentielles.

Toute erreur ou omission dans ces exigences peut entraîner de lourdes amendes. Il est donc impératif que les organisations examinent attentivement les directives PCI-DSS et appliquent les contrôles appropriés à leur environnement.

Les sociétés de cartes de crédit imposent **12 exigences** que les organisations doivent respecter pour rester conformes à la norme PCI-DSS. Ces normes visent à protéger les données des titulaires de cartes.

Ces exigences portent sur les nombreuses façons dont les menaces peuvent compromettre les défenses du réseau et permettre aux attaquants de voler des informations essentielles. Toute modification des exigences actuelles est annoncée et publiée par le Conseil de sécurité.

Les organisations doivent donc les revoir chaque année pour s'assurer qu'elles répondent en permanence aux exigences de conformité.

Les 12 exigences PCI-DSS sont les suivantes :

**1. Installer des pare-feu et les configurer pour bloquer le trafic malveillant.** La plupart des organisations ont déjà installé un pare-feu entre l'Internet extérieur et l'environnement interne, mais d'autres sont nécessaires dans les grands environnements où le Wi-Fi public est

proposé et où les départements doivent être segmentés. Par exemple, les organisations utilisent un pare-feu pour séparer les départements financiers et leurs données du département des ventes afin de protéger les données des titulaires de cartes.

**2. Éviter d'utiliser les valeurs par défaut des fournisseurs pour les mots de passe système.** Chaque ressource réseau est livrée avec le mot de passe par défaut du fabricant afin que les administrateurs puissent configurer le matériel pour qu'il fonctionne spécifiquement avec l'infrastructure de l'entreprise. Ces mots de passe sont ouvertement distribués au public, ce qui signifie que les attaquants peuvent accéder aux ressources du réseau sans obtenir d'informations d'identification. Après avoir connecté un composant au réseau, la première étape pour un administrateur est de changer le mot de passe par défaut par le sien. Il est préférable d'utiliser des mots de passe difficiles à deviner, mais faciles à retenir.

**3. Protéger les données financières stockées des consommateurs.** Cette exigence peut sembler évidente, mais toutes les organisations ne stockent pas les données des cartes de crédit et ne font pas le nécessaire pour assurer une sécurité de base. Par exemple, les données de carte stockées dans une base de données doivent être chiffrées et personne au sein de l'organisation ne doit y avoir un accès illimité. Toute demande d'accès doit être contrôlée et une piste d'audit doit être créée pour permettre de réagir en cas d'incident.

**4. Les données financières transférées sur les réseaux publics doivent être chiffrées.** Les données qui transitent par l'internet doivent être chiffrées pour éviter toute écoute clandestine. Les utilisateurs soumettent les informations relatives à leur carte de crédit sur un site de commerce électronique, et ces informations doivent être chiffrées. Les commerçants envoient les données relatives aux cartes de crédit à un processeur, et ces données doivent être chiffrées lorsqu'elles sont transmises aux services commerciaux. Certaines organisations portent la sécurité à un autre niveau et chiffrent le trafic au sein du réseau de l'entreprise.

**5. Installer et maintenir un logiciel antivirus.** Tous les serveurs et postes de travail de l'entreprise doivent être équipés d'un logiciel antivirus. Pour aller plus loin, tout appareil mobile qui stocke ou traite des données de cartes de crédit doit également être équipé d'un logiciel antivirus. La sécurité des points de terminaison est un défi plus récent pour les organisations depuis la popularité croissante des smartphones, mais elle devrait être une priorité pour les organisations prenant des paiements sur des appareils mobiles.

**6. Ajouter des systèmes avec une protection des données en place.** Les systèmes changent constamment et les administrateurs en ajouteront de nouveaux à mesure que l'entreprise se développe. Tout système installé dans l'infrastructure de l'entreprise doit être intégré en tenant compte de la sécurité. Toute nouvelle infrastructure doit être installée en intégrant la sécurité, et toute configuration doit être établie en tenant compte de la sécurité des données des cartes de crédit.

**7. Utiliser les normes du moindre privilège pour l'accès aux données.** Les utilisateurs ne doivent avoir accès aux données de cartes de crédit que si cela est nécessaire à l'exercice de leurs fonctions. Les menaces internes risquent d'exposer les données de cartes de crédit. Par conséquent, seuls les employés qui ont besoin d'un accès pour exercer leur fonction doivent y avoir accès. Dans certains cas, une partie du numéro de carte de crédit peut être masquée pour renforcer la sécurité. Par exemple, le personnel du service clientèle peut voir les quatre derniers chiffres d'un numéro de carte de crédit mais pas le numéro complet, tandis que le service de facturation peut voir le numéro complet pour aider les clients à modifier leur numéro de carte dans le dossier.

**8. Enregistrer les demandes d'accès avec l'identifiant de l'utilisateur qui récupère les données de la carte de crédit.** Qu'il s'agisse d'un compte compromis ou d'un initié malveillant, l'enregistrement de chaque demande d'accès avec l'identifiant de l'utilisateur laisse une piste d'audit. Les enquêteurs et les forces de l'ordre utilisent les pistes d'audit pour identifier un acteur malveillant, et elles aident les équipes de réponse aux incidents à identifier l'étendue des dommages et les consommateurs affectés par une violation de données.

**9. Limiter l'accès physique aux données des cartes de crédit.** Les serveurs qui stockent les données des cartes de crédit doivent être dotés de mesures de sécurité physique appropriées. Pour les organisations qui stockent des données de carte de crédit dans le cloud, le fournisseur de cloud doit fournir des politiques conformes aux normes PCI-DSS. La sécurité physique doit également consigner les demandes d'accès à l'infrastructure afin de créer une piste d'audit.

**10. Consigner et surveiller les demandes d'accès aux ressources réseau stockant des données de cartes de crédit.** La surveillance de l'accès aux données est une composante de

plusieurs règlements de conformité. Les journaux et la surveillance vont de pair avec la sécurité et la protection des données. Les journaux suivent les événements de demande d'accès et les outils de surveillance utilisent ces événements pour identifier les anomalies qui déclenchent des notifications envoyées aux administrateurs. Les analystes utilisent la surveillance pour réagir rapidement aux incidents en cours afin de les contenir et de limiter les dommages causés par une violation.

**11. Tester les systèmes et les procédures de sécurité.** Il arrive que les systèmes de sécurité tombent en panne ou qu'ils ne fonctionnent pas comme prévu. Il est donc important que les administrateurs testent régulièrement les contrôles de sécurité dans l'ensemble de l'environnement. Certaines organisations organisent des événements de sécurité au cours desquels elles offrent des prix aux employés qui trouvent des ressources vulnérables. En plus des tests annuels, les administrateurs doivent examiner la documentation relative à la conformité PCI-DSS afin d'y déceler tout changement.

**12. Documenter les politiques de sécurité et les distribuer aux employés.** Les employés ne peuvent pas suivre les politiques de sécurité s'ils ne savent pas quelles politiques ils doivent suivre. La norme PCI-DSS exige des employeurs qu'ils documentent les politiques de sécurité afin que les employés puissent faire référence à ce qui doit être fait et identifier les moyens appropriés de traiter les données des clients.

## **4. Entités concernées par la conformité à la norme PCI DSS**

Étant donné que la norme PCI DSS s'applique à toute organisation qui accepte, traite, stocke ou transmet des données de titulaires de cartes, les types d'organisations suivants doivent démontrer leur conformité à la norme :

- **Commerçants** de toutes tailles : Toute entité qui accepte, traite, stocke ou transmet des données de carte de paiement, que ce soit en ligne, en magasin ou par tout autre moyen de vente.
- **Fournisseurs de points de vente (PDV)** : Les entreprises qui fournissent des services de traitement de paiement ou qui ont accès aux données de carte de paiement, y

compris les processeurs de paiement, les passerelles de paiement, les fournisseurs d'hébergement et les prestataires de services de sécurité.

- **Institutions financières**

En outre, toute organisation qui stocke, traite ou transmet des données de carte de paiement est tenue de se conformer à la norme PCI DSS, quel que soit son secteur d'activité. Cela peut inclure des entités telles que les institutions financières, les organismes gouvernementaux et les organisations à but non lucratif, entre autres[3].

## **5. Avantages de la norme PCI-DSS**

Le maintien de la conformité à la norme PCI-DSS demande un effort considérable, mais les bénéfices qui en découlent sont nombreux. La majorité de ces avantages ont un impact positif sur vos revenus. Il est donc essentiel de suivre ces directives et de protéger les données des titulaires de cartes en appliquant les exigences de sécurité définies dans la norme PCI-DSS.

Les avantages comprennent :

**1. Renforcement de la confiance des clients :** Les clients sont rassurés de savoir que leurs données sont sécurisées, et le respect de la norme PCI-DSS démontre que votre organisation comprend les mesures nécessaires pour protéger les informations relatives aux cartes de crédit.

**2. Prévention des violations de données :** Dans un monde où la cybersécurité est une priorité cruciale, toute organisation stockant des données sensibles, telles que les informations de carte de crédit, doit mettre en place des mesures de sécurité robustes pour éviter les violations de données. Chaque exigence de la norme PCI-DSS contribue à prévenir les cyberattaques potentielles qui pourraient compromettre les revenus de votre entreprise.

**3. Conformité aux normes internationales :** Le Conseil de sécurité PCI-DSS rassemble des sociétés de cartes de crédit du monde entier pour élaborer et mettre à jour les directives de sécurité. De nombreuses parties prenantes, y compris certains fournisseurs et prestataires de services marchands, peuvent exiger que votre entreprise reste conforme à la norme PCI-DSS pour mener des transactions commerciales avec elles.

**4. Aide à la mise en place de contrôles de sécurité adéquats :** Face à la multitude d'options de cybersécurité disponibles, il est souvent difficile de déterminer les meilleures pratiques à adopter. Les lignes directrices de la norme PCI-DSS orientent les entreprises dans la bonne direction, en fournissant des directives claires sur les contrôles de sécurité nécessaires pour protéger efficacement les données des cartes de crédit.

**5. Alignement avec d'autres normes de conformité :** De nombreuses organisations doivent respecter plusieurs normes de conformité, telles que HIPAA et RGPD. En appliquant les principes de sécurité de la norme PCI-DSS, votre entreprise peut également rester conforme à ces autres normes, simplifiant ainsi le processus de conformité globale.

## **6. Quels sont les impacts du non-respect de la norme PCI DSS**

La non-conformité à la norme PCI-DSS entraîne des conséquences graves. Après une violation des données, une organisation pourrait se retrouver à payer des millions de dollars en frais de violation et en frais juridiques associés aux recours collectifs. Voici les cinq principales conséquences :

**1. Amendes mensuelles :** Les environnements non conformes mettent en danger les données des cartes de crédit des consommateurs, ce qui justifie l'imposition de frais mensuels élevés en cas de violation de la norme PCI-DSS. Les pénalités varient en fonction du niveau du commerçant, mais elles vont généralement de **5 000** à **100 000** dollars par mois.

**2. Compromission du système et violations des données :** Une sécurité insuffisante crée des vulnérabilités qui peuvent entraîner des violations des données. Les violations des données entraînent des coûts considérables en termes de réponse aux incidents, d'enquêtes, de perte de confiance des clients et de litiges.

**3. Litiges :** Les violations graves des données entraînent un stress financier pour les consommateurs, et les recours collectifs leur permettent d'obtenir réparation. Les



organisations doivent assumer les frais juridiques et tout règlement après une violation des données.

**4. Atteinte à la réputation de la marque :** Si une organisation est connue pour sa mauvaise sécurité, les clients se tourneront vers ses concurrents. Une atteinte à la réputation de la marque affecte la fidélité et la confiance des clients.

**5. Perte de revenus :** Lorsque les clients choisissent des concurrents en raison de l'atteinte à la réputation de la marque, l'organisation subit une perte de revenus, y compris les coûts associés aux litiges.

Par exemple, une violation de données impliquant **34 millions** de cartes de paiement s'est soldée par un procès de 8 millions de dollars en 2019 .

## 7. Meilleures pratiques pour la conformité PCI-DSS

La plupart des meilleures pratiques de la norme PCI-DSS suivent ses exigences, mais les organisations peuvent mettre en place des politiques supplémentaires pour renforcer la sécurité [8].

Voici quelques pratiques supplémentaires que les organisations devraient envisager :

- **Maintenir les logiciels à jour :** Les développeurs publient régulièrement des mises à jour pour corriger les failles de sécurité de leurs logiciels. Il est donc crucial de maintenir toutes les applications à jour afin d'éviter de laisser l'infrastructure vulnérable.
- **Utiliser la tokenisation des données des cartes de crédit :** La tokenisation, similaire au chiffrement, remplace les données sensibles par des données non sensibles tout en conservant certains éléments des données d'origine pour permettre la poursuite des opérations commerciales. Cela ajoute une couche de sécurité supplémentaire aux données sensibles.
- **Attribuer un identifiant unique à chaque utilisateur et ressource :** En plus de donner des noms d'utilisateur uniques aux utilisateurs, chaque composant qui accède

aux données devrait avoir son propre identifiant unique. Cela facilite le suivi des demandes et renforce la traçabilité des activités.

- **Protéger les mots de passe :** Il est essentiel de demander à tous les utilisateurs de stocker leurs mots de passe de manière sécurisée. L'utilisation de gestionnaires de mots de passe est fortement recommandée pour éviter les mauvaises pratiques de stockage des mots de passe et renforcer la sécurité des comptes.
- **Effectuer des tests de pénétration des logiciels et des configurations réseau :** Les tests de pénétration, effectués par des experts en sécurité ou des pirates éthiques, permettent d'identifier les vulnérabilités potentielles dans les logiciels et les configurations réseau. Cela aide l'organisation à détecter et à corriger les problèmes de sécurité avant qu'ils ne soient exploités par des attaquants.

## 8. Conclusion

En conclusion, la norme PCI DSS est une pierre angulaire de la cybersécurité pour toute organisation traitant des données de paiement. Adopter et maintenir cette conformité est non seulement une obligation réglementaire, mais également une stratégie proactive pour assurer la protection et la pérennité des entreprises dans le paysage numérique actuel, tels que la prévention des violations de données, le renforcement de la confiance des clients et l'alignement avec d'autres normes de sécurité, dépassent largement les efforts nécessaires pour maintenir cette conformité. Par ailleurs, le non-respect de ces exigences peut entraîner des conséquences financières et juridiques sévères, ainsi qu'une atteinte à la réputation de l'entreprise.

# Chapitre 3 : L'audit de sécurité informatique

---

## Introduction

L'évolution technologique et les changements environnementaux posent de multiples défis au système d'information d'une entité. Ces défis découlent de la nécessité de concilier les besoins informatiques de l'entité tout en respectant les réglementations en matière de technologie informatique. Assurer la cohérence entre les processus informatiques et les normes en vigueur relève ainsi du domaine de l'audit informatique.

L'audit informatique vise à garantir l'alignement des systèmes d'information avec les objectifs stratégiques de l'entité ainsi qu'avec les réglementations et les meilleures pratiques du secteur. Il s'agit d'une évaluation systématique et indépendante des processus, des contrôles et des politiques informatiques pour assurer leur efficacité, leur sécurité et leur conformité.

Dans un environnement informatique en constante évolution, les auditeurs informatiques jouent un rôle crucial en identifiant les vulnérabilités, en proposant des recommandations d'amélioration et en fournissant une assurance quant à la fiabilité et à l'intégrité des systèmes d'information.

En résumé, l'audit informatique est essentiel pour garantir **la fiabilité, la sécurité** et la **conformité** des systèmes d'information dans un contexte où les défis technologiques et réglementaires sont de plus en plus complexes.

## 1 . Définition d'un audit

En informatique, le terme « audit » est apparu dans les années 70 et a été utilisé de manière relativement aléatoire. Par la suite, un audit de sécurité du système d'information est considéré comme une mission d'évaluation de la conformité par rapport à une politique de sécurité ou, à défaut, par rapport à un ensemble de règles de sécurité[5].

Une mission d'audit ne peut être réalisée que si l'on définit au préalable un référentiel, qui consiste en un ensemble de règles organisationnelles, procédurales et/ou 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 référentiel doit être :

- **Complet** : il doit mesurer l'ensemble des caractéristiques, en ne se limitant pas exclusivement aux niveaux système, réseau, télécoms ou applicatif, mais en couvrant également les aspects techniques et organisationnels.
- **Homogène** : chaque caractéristique mesurée doit avoir un poids cohérent avec l'ensemble.
- **Pragmatique** : il doit être aisé à quantifier et à contrôler, un aspect 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.

## 2. Rôle et Objectif de l'Audit

Une mission d'audit poursuit plusieurs objectifs. Nous pouvons notamment énumérer les suivants :

- Identifier les écarts par rapport aux bonnes pratiques de sécurité.
- Proposer des actions pour améliorer le niveau de sécurité du système d'information.

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

Des risques supplémentaires, notamment l'efficacité, l'efficience et la fiabilité d'un système d'information, peuvent être résolus par l'identification régulière et l'évaluation des risques au sein d'une entité, c'est-à-dire par la surveillance.

### 3. Relation entre l'Audit Informatique et PCI DSS :

L'audit informatique selon la norme ISO 27001:2022 et la conformité au standard PCI DSS partagent plusieurs points de convergence, bien qu'ils aient des objectifs et des domaines d'application différents. Voici un aperçu des principaux aspects de leur relation :

- **Convergence des Objectifs :**

Les deux normes visent à assurer la sécurité des informations et des données sensibles. Tandis que l'ISO 27001 est une norme de gestion de la sécurité de l'information axée sur la mise en place d'un système de management de la sécurité de l'information (SMSI), PCI DSS est spécifiquement conçu pour sécuriser les transactions par carte de crédit.

- **Recoupement des Exigences :**

Malgré leurs différences, de nombreuses exigences de sécurité des données spécifiées par PCI DSS sont également couvertes par les contrôles de sécurité de l'ISO 27001. Par exemple, la protection des données sensibles, la gestion des accès, la surveillance des systèmes, et la gestion des incidents sont des aspects communs traités par les deux normes.

- **Coopération et Synergie :**

En pratique, les organisations peuvent tirer parti d'une approche intégrée de la conformité en utilisant les principes et les contrôles de sécurité de l'ISO 27001 pour renforcer leur conformité à PCI DSS. En intégrant les exigences des deux normes, les entreprises peuvent rationaliser leurs efforts de conformité et garantir une protection optimale des informations et des données des clients.

- **Audit et Vérification :**

Les processus d'audit internes et externes sont essentiels pour évaluer la conformité à la fois à l'ISO 27001 et à PCI DSS. Les audits aident à identifier les lacunes de sécurité, à évaluer l'efficacité des contrôles mis en place et à recommander des actions correctives pour améliorer la sécurité globale des systèmes d'information et des transactions par carte de crédit.

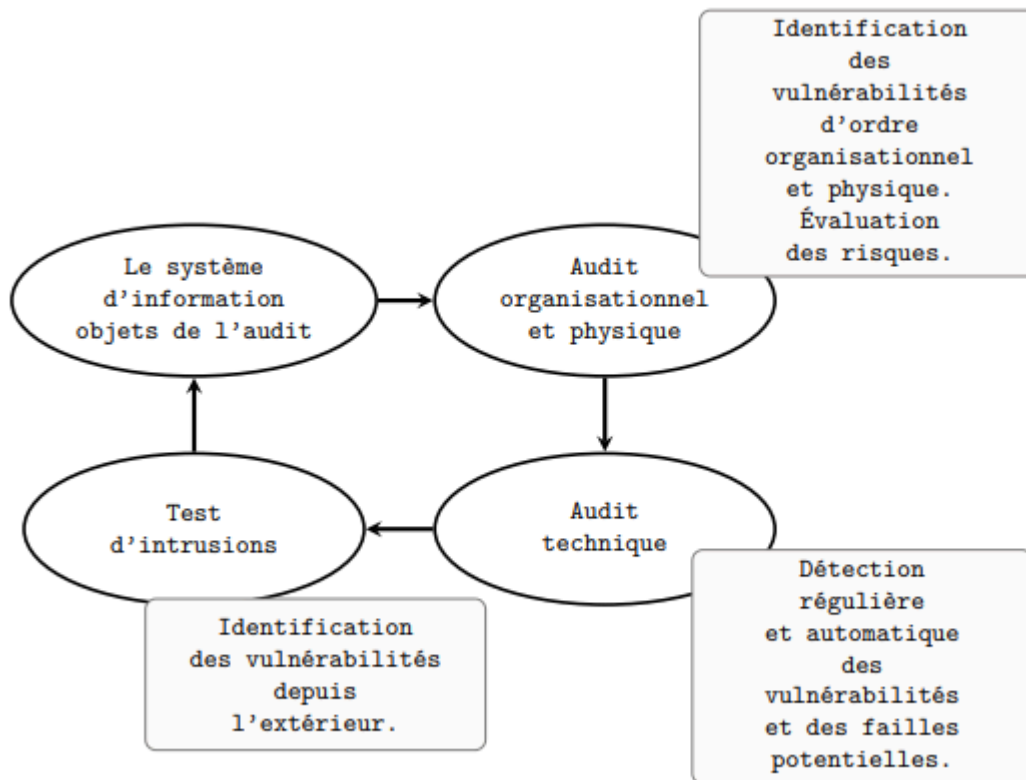
En conclusion, bien que l'audit informatique selon l'ISO 27001 et la conformité à PCI DSS soient distincts dans leur portée et leurs objectifs, ils se complètent mutuellement dans la promotion d'une culture de sécurité robuste et dans la protection des données sensibles contre les menaces potentielles.

## 4. Processus d'audit de sécurité du cycle de vie des systèmes d'information

Le processus d'audit de sécurité du cycle de vie des systèmes d'information comprend plusieurs étapes essentielles pour évaluer et garantir la sécurité des systèmes informatiques tout au long de leur existence.

- **Planification de l'Audit :** Cette étape implique la définition des objectifs, du périmètre et des ressources nécessaires pour l'audit. Le plan d'audit doit prendre en compte les risques potentiels et les exigences de conformité applicables.
- **Collecte d'Informations :** L'auditeur rassemble des informations sur l'infrastructure, les applications, les politiques de sécurité, les contrôles en place et les processus opérationnels liés aux systèmes d'information.
- **Évaluation des risques :** L'évaluation des risques permet d'identifier les menaces potentielles, les vulnérabilités et les impacts associés aux systèmes d'information. Cette analyse permet de prioriser les domaines à auditer et les contrôles de sécurité à évaluer.
- **Analyse des contrôles de sécurité :** L'auditeur examine les contrôles de sécurité en place pour déterminer leur efficacité à atténuer les risques identifiés. Cela comprend l'évaluation des politiques, des procédures, des technologies et des pratiques de gestion des risques.
- **Tests et Vérifications :** Des tests techniques et des vérifications sont effectués pour évaluer la robustesse des contrôles de sécurité. Cela peut inclure des tests de pénétration, des scans de vulnérabilité, des évaluations de conformité et des analyses de sécurité des applications.
- **Identification des faiblesses :** Les faiblesses et les lacunes dans les contrôles de sécurité sont identifiées et documentées. Cela peut inclure des problèmes de configuration, des vulnérabilités logicielles, des lacunes dans les processus de gestion des identités et des accès, etc.
- **Rapport d'Audit :** Un rapport d'audit détaille les résultats de l'évaluation de sécurité, y compris les faiblesses identifiées, les recommandations pour améliorer la sécurité et les mesures correctives recommandées. Ce rapport est généralement remis à la direction de l'entreprise pour examen et action corrective.

- **Suivi et Réévaluation** : Après la mise en œuvre des mesures correctives, un suivi est effectué pour vérifier leur efficacité. De plus, des audits périodiques sont recommandés pour maintenir la conformité et la sécurité continues des systèmes d'information.



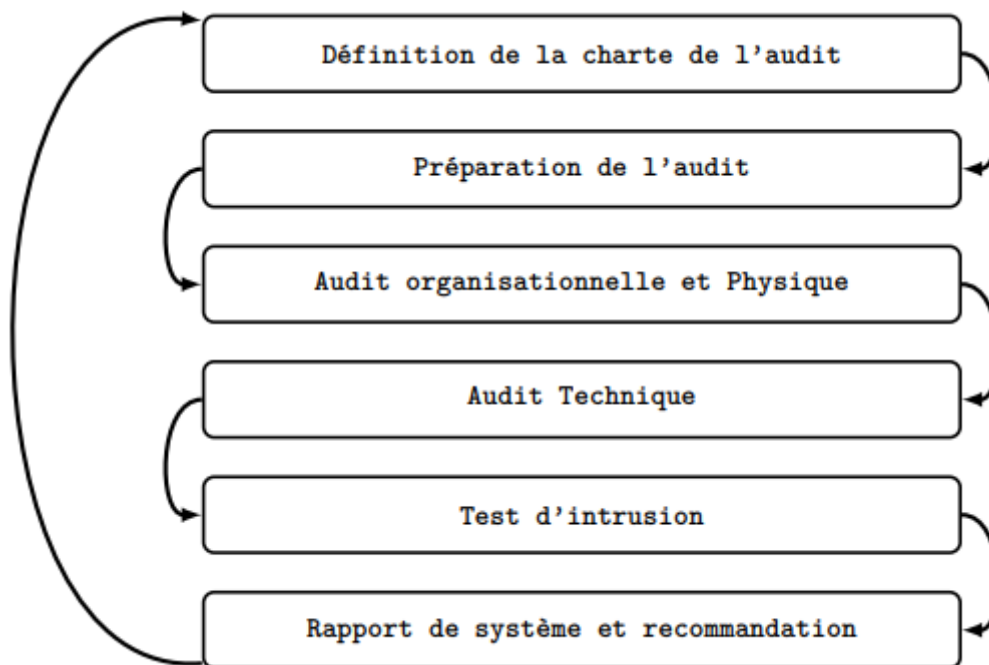
**Figure 3.1** : Le cycle de vie d'audit de sécurité

En suivant ce processus d'audit de sécurité du cycle de vie des systèmes d'information, les organisations peuvent identifier et atténuer les risques de sécurité, assurant ainsi la protection des données et la résilience des infrastructures informatiques.

## 5. Processus de mise en œuvre d'une mission d'audit de sécurité des systèmes d'information

Comme mentionné précédemment , nous avons suivi les étapes de l'audit de sécurité des systèmes d'information se déroulant généralement . Toutefois, il est crucial de souligner l'importance d'une phase préparatoire [6] .

Nous avons présentons l'ensemble du processus d'audit dans la figure suivante :



**Figure 3.2 :** Schéma du processus d'audit

### 5.1 Élaboration de la Charte d'Audit

Avant d'entreprendre toute mission d'audit, il est impératif de rédiger une charte d'audit. Cette dernière vise à définir clairement la nature de l'audit, ses domaines d'intervention, ses limites et modalités, ainsi que les responsabilités des parties prenantes, tout en établissant les



principes régissant les relations entre les auditeurs et les audités. De plus, elle précise les compétences professionnelles et éthiques requises des auditeurs [7].

## **5.2 Préparation de l'audit**

Nous avons dans cette étape, également appelée phase de pré-audit, revêt une importance cruciale dans la réalisation de l'audit sur le terrain. En synthèse, cette étape permet de :

- Définir un référentiel de sécurité, en fonction des exigences et des attentes des responsables du site audités, ainsi que du type d'audit envisagé.
- Élaborer un questionnaire d'audit sécurité à partir du référentiel et des objectifs de la mission.
- Planifier les entretiens et recueillir les informations nécessaires auprès des personnes impliquées.

En effectuant ces étapes préliminaires avec rigueur et méthode, il est possible de garantir une conduite efficace et efficiente de l'audit sur le terrain, tout en assurant une compréhension approfondie des enjeux et des objectifs de la mission d'audit [7].

## **5.3 Audit Organisationnel et Physique**

### **- Objectif :**

Dans cette étape, l'objectif est d'analyser l'aspect physique et organisationnel de l'organisme cible à auditer. Nous examinons donc les aspects de gestion et d'organisation de la sécurité, tant sur les plans organisationnels, humains que physiques [7].

Les objectifs visés par cette étape sont les suivants :

- Obtenir une vue d'ensemble de l'état de sécurité du système d'information.
- Identifier les risques potentiels sur le plan organisationnel.

### **- Déroulement :**

Pour mener à bien cette étape de l'audit, il est nécessaire de suivre une approche méthodologique basée sur un ensemble de questions préétablies. Ce questionnaire doit être adapté aux réalités spécifiques de l'organisme à auditer. À la suite de cette étape et en utilisant une métrique appropriée, l'auditeur peut évaluer les failles et évaluer le niveau de maturité en termes de sécurité de l'organisme, ainsi que sa conformité par rapport à la norme de référence de l'audit.

Dans notre contexte, cet audit se basera sur la norme **ISO/27001:2022** comme référentiel.

## **5.4 Audit Technique**

### **- Objectif :**

Nous avons dans cette étape de l'audit sur le terrain intervient en deuxième position après l'audit organisationnel. L'audit technique suit une approche méthodique, allant de la découverte et de la reconnaissance du réseau audité jusqu'à l'exploration des services réseau actifs et vulnérables.

Cette analyse doit mettre en lumière les failles, les risques et les conséquences éventuelles d'intrusions ou de manipulations illicites de données. Pendant cette phase, l'auditeur peut également comparer les résultats obtenus lors des entretiens avec les constatations techniques. Il évalue également la robustesse de la sécurité du système d'information et sa capacité à protéger les aspects de confidentialité, d'intégrité, de disponibilité et d'autorisation des données.

Cependant, l'auditeur doit veiller à ce que les tests effectués n'affectent pas la continuité de service du système audité.

### **- Déroulement :**

L'audit technique sera réalisé selon une succession de phases respectant une approche méthodique. Il permet la détection des types de vulnérabilités suivantes :

- Les erreurs de programmation et d'architecture.

- Les erreurs de configuration des composants logiques installés, tels que les services (ports) ouverts sur les machines, la présence de fichiers de configuration installés par défaut, l'utilisation des comptes utilisateurs par défaut.
- Les problèmes au niveau du trafic réseau (flux ou trafic non répertorié, écoute réseau,...).
- Les problèmes de configuration des équipements d'interconnexion et de contrôle d'accès réseau.
- Les principales phases de l'audit technique sont les suivantes :

#### **Phase 1 : Audit de l'Architecture du Système**

- Reconnaissance du réseau et du plan d'adressage.
- Sondage des systèmes.
- Sondage réseau.
- Audit des applications.

#### **Phase 2 : Analyse des Vulnérabilités**

- Analyse des vulnérabilités des serveurs en exploitation.
- Analyse des vulnérabilités des postes de travail.

#### **Phase 3 : Audit de l'Architecture de Sécurité Existante**

Cette phase comprend l'audit des éléments suivants :

- Firewalls et règles de filtrage.
- Routeurs et ACLs (Liste de contrôle d'accès).
- Sondes et passerelles antivirales.
- Stations proxy.
- Serveurs DNS, d'authentification.
- Commutateurs.
- Politique d'usage de mots de passe.

### **5.5 Audit Intrusif**

Cet audit vise à évaluer la réaction des installations techniques face à des attaques. Il permet également de sensibiliser les parties prenantes, y compris la direction, les équipes sur

site et les utilisateurs, en fournissant des rapports détaillant les failles identifiées, les tests effectués (scénarios et outils utilisés) ainsi que les recommandations pour remédier aux insuffisances détectées.

## **5.6 Rapport d'Audit**

À la clôture des phases précédentes d'audit sur le terrain, l'auditeur est chargé de rédiger un rapport de synthèse sur sa mission d'audit. Cette synthèse doit mettre en lumière les défaillances constatées. Tout autant qu'il est crucial de mettre en évidence les problèmes, il est tout aussi important de proposer des solutions. Par conséquent, l'auditeur est également invité à formuler des recommandations afin de remédier aux lacunes identifiées. Ces recommandations doivent prendre en compte à la fois l'audit organisationnel et physique, ainsi que l'audit technique et intrusif [7].

## **6 . 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). Initialement, cette méthode se concentrait uniquement sur l'analyse des risques. Elle a ensuite évolué pour permettre une gestion globale de la sécurité des organismes, même dans des environnements ouverts et géographiquement répartis.

MEHARI a été adoptée par des milliers d'organisations à travers le monde et reste la méthode la plus utilisée en France, particulièrement dans le secteur industriel. L'utilisation et la distribution de son logiciel sont libres, et diverses bases de connaissances sont disponibles pour faciliter son application. Des études de cas illustrent également la méthode pour en simplifier l'usage [11].

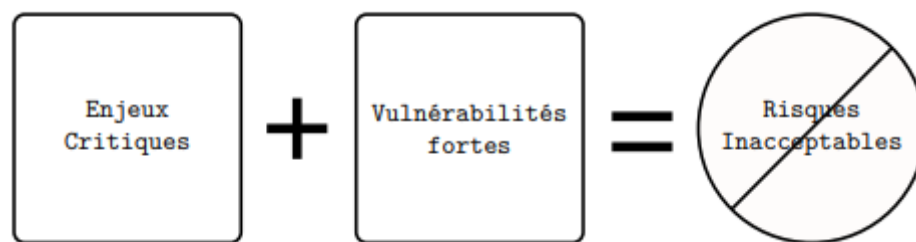
Contrairement à la méthode EBIOS, MEHARI repose sur des scénarios de risques permettant d'identifier les risques potentiels au sein de l'organisation. Elle est définie comme une boîte à outils conçue pour la gestion de la sécurité. En fonction des besoins, des orientations, des politiques de l'organisation, ou simplement des circonstances, MEHARI assure qu'une solution d'évaluation des risques appropriée puisse être élaborée. La méthode est présentée sous la forme d'un ensemble de modules, centrés sur l'évaluation et la gestion des risques.

## 6.1 Principe de fonctionnement

La méthode MEHARI prend en compte les informations de l'entreprise pour développer un plan qui définit les points à protéger. MEHARI permet 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 allie la rigueur d'une analyse des risques formellement liée au niveau de vulnérabilité du système d'information à l'adaptabilité de la gravité des risques étudiés. La présence ou l'absence de mesures de sécurité influence la probabilité de survenance d'un sinistre et son impact. L'interaction de ces mesures contribue à réduire la gravité des risques jusqu'au niveau choisi.



**Figure 3.3 :** Enjeux critique + Vulnérabilités fortes = Risques inacceptables

## 6.2 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 des risques. MEHARI vise à fournir des outils et des méthodes pour sélectionner les mesures de sécurité les plus pertinentes pour une entreprise donnée.

Les différentes phases de la méthode ont pour objectif :

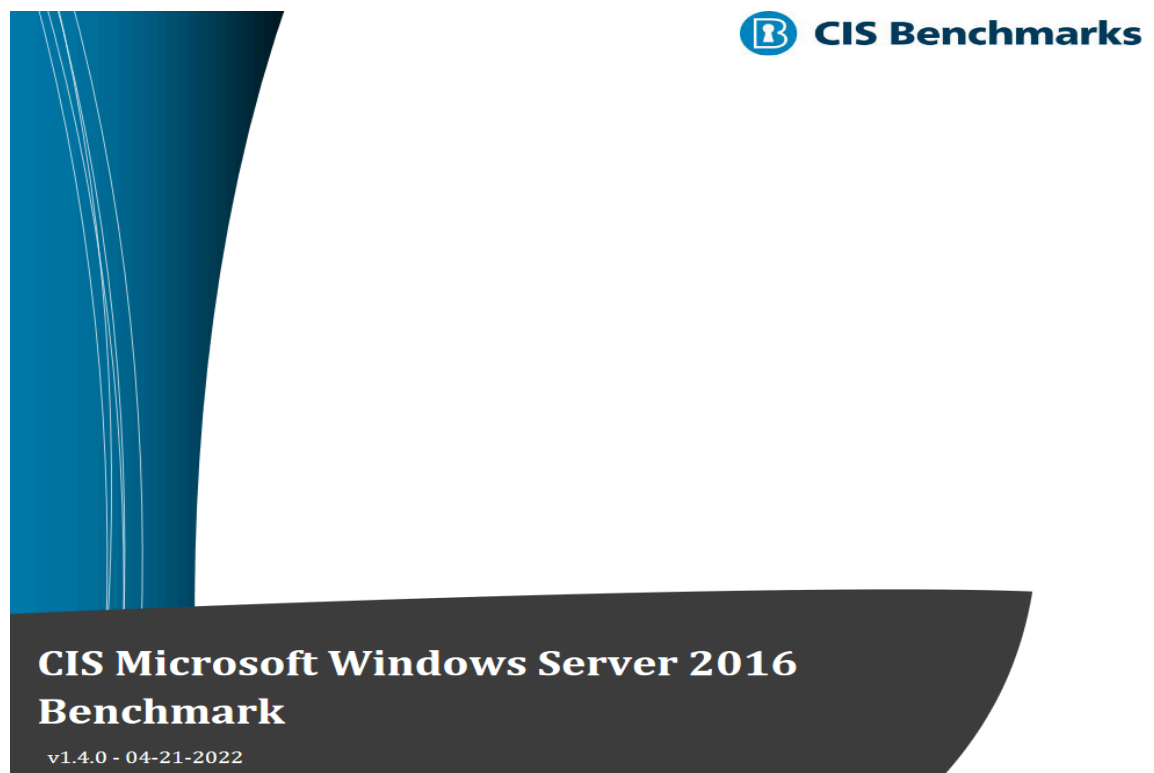
- **Établir le contexte de l'entreprise :** Comprendre l'environnement dans lequel l'entreprise opère, ses objectifs, et ses contraintes.

- **Identifier les actifs et les menaces** : Recenser les ressources importantes et les menaces potentielles qui pourraient les affecter.
- **Analyser les risques** : Évaluer la probabilité et l'impact des menaces identifiées sur les actifs de l'entreprise.
- **Définir les mesures de sécurité** : Proposer et prioriser les actions nécessaires pour traiter les risques identifiés.

Ces phases permettent de créer un cadre structuré pour la gestion de la sécurité de l'information, en assurant que les décisions sont basées sur une compréhension claire des risques et des besoins spécifiques de l'entreprise.

## 7. Référence CIS Microsoft Windows Server 2016

Nous avons utilisé le CIS (Center for Internet Security) Microsoft Windows Server 2016 Benchmark pour évaluer et renforcer la sécurité de notre infrastructure informatique. Ce benchmark fournit des lignes directrices et des recommandations pour configurer et sécuriser les systèmes Windows Server 2016.



**Figure 3.4** – CIS Microsoft Windows Server 2016 Benchmark

L'utilisation du CIS Microsoft Windows Server 2016 Benchmark vise à atteindre les objectifs suivants :

- **Évaluer la sécurité des serveurs Windows Server 2016** en identifiant les configurations sécurisées et les pratiques recommandées.
- **Renforcer la posture de sécurité** des serveurs en appliquant les recommandations du benchmark.
- **Assurer la conformité aux standards de sécurité** en suivant les meilleures pratiques reconnues au niveau international.

## 7.1 Méthodologie

Pour réaliser cette évaluation de sécurité, nous avons suivi les étapes ci-dessous en utilisant le benchmark CIS Microsoft Windows Server 2016 comme référence :

1. **Analyse des configurations actuelles** : Audit des configurations existantes sur les serveurs Windows Server 2016 pour identifier les écarts par rapport aux recommandations CIS.
2. **Application des recommandations** : Mise en œuvre des recommandations du benchmark pour aligner les configurations des serveurs avec les meilleures pratiques de sécurité.
3. **Vérification et validation** : Revue des configurations après application des recommandations pour s'assurer qu'elles respectent les directives du benchmark.
4. **Documentation** : Rédaction des résultats de l'évaluation et des mesures correctives appliquées.

## 7.2 Principales Recommandations du Benchmark CIS

Les recommandations du CIS Microsoft Windows Server 2016 Benchmark couvrent plusieurs domaines clés de la sécurité, notamment :

- **Gestion des comptes et des accès** :
  - Désactiver les comptes invités.
  - Renforcer les politiques de mot de passe et d'authentification.

- Limiter les droits d'administration et utiliser des groupes restreints.
- **Configurations du système :**
  - Activer les mises à jour automatiques.
  - Désactiver les services non essentiels.
  - Configurer les paramètres de sécurité locaux et de groupe.
- **Audit et surveillance :**
  - Configurer les journaux de sécurité pour enregistrer les événements critiques.
  - Mettre en place une surveillance continue des systèmes.
- **Protection des données :**
  - Utiliser le chiffrement pour protéger les données sensibles.
  - Configurer les sauvegardes automatiques et sécurisées.
- **Sécurité réseau :**
  - Configurer les pare-feu pour contrôler le trafic entrant et sortant.
  - Désactiver les protocoles et services réseau non sécurisés.

## 7.3 Politique de mot de passe

**1.1.5 (L1) S'assurer que 'Les mots de passe doivent répondre à des exigences de complexité' est défini sur 'Activé' (Automatisé)**

Applicabilité du profil :

- Niveau 1 - Contrôleur de domaine
- Niveau 1 - Serveur membre

Description :

Ce paramètre de stratégie vérifie tous les nouveaux mots de passe pour s'assurer qu'ils répondent aux exigences de base pour des mots de passe forts.

Lorsqu'elle est activée, cette politique exige que les mots de passe répondent aux exigences minimales suivantes :

- Ne pas contenir le nom de compte de l'utilisateur ou des parties du nom complet de l'utilisateur dépassant deux caractères consécutifs
- Avoir au moins six caractères de longueur



- Contenir des caractères provenant de trois des catégories suivantes :
- Caractères majuscules anglais (A à Z)
- Caractères minuscules anglais (a à z)
- Chiffres en base 10 (0 à 9)
- Caractères non alphabétiques (par exemple, !, \$, #, %)

Une catégorie générale de tout caractère Unicode ne relevant pas des quatre catégories précédentes. Cette cinquième catégorie peut être spécifique à la région.

Chaque caractère supplémentaire dans un mot de passe augmente exponentiellement sa complexité. Par exemple, un mot de passe alphabétique en minuscules de sept caractères aurait  $26^7$  (environ  $8 \times 10^9$  ou 8 milliards) combinaisons possibles. À 1 000 000 tentatives par seconde (une capacité de nombreux utilitaires de craquage de mots de passe), il ne faudrait que 133 minutes pour le casser. Un mot de passe alphabétique sensible à la casse de sept caractères à  $52^7$  combinaisons. Un mot de passe alphanumérique sensible à la casse sans ponctuation de sept caractères a  $62^7$  combinaisons. Un mot de passe de huit caractères a  $26^8$  (ou  $2 \times 10^{11}$ ) combinaisons possibles. Bien que cela puisse sembler un grand nombre, à 1 000 000 tentatives par seconde, il ne faudrait que 59 heures pour essayer toutes les combinaisons possibles. Rappelez-vous, ces temps augmenteront considérablement pour les mots de passe qui utilisent des caractères ALT et d'autres caractères spéciaux du clavier tels que "!" ou "@". L'utilisation appropriée des paramètres de mot de passe peut aider à rendre difficile une attaque par force brute.

L'état recommandé pour ce paramètre est : **Activé**

Control		Set Correctly	
		Yes	No
<b>1</b>	<b>Account Policies</b>		
<b>1.1</b>	<b>Password Policy</b>		
1.1.1	(L1) Ensure 'Enforce password history' is set to '24 or more password(s)' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2	(L1) Ensure 'Maximum password age' is set to '365 or fewer days, but not 0' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.3	(L1) Ensure 'Minimum password age' is set to '1 or more day(s)' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.4	(L1) Ensure 'Minimum password length' is set to '14 or more character(s)' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.5	(L1) Ensure 'Password must meet complexity requirements' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.6	(L1) Ensure 'Store passwords using reversible encryption' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

**Table 3.1 :** Tableau de Politique de mot de passe

## 7. Conclusion

La mise en place de toute approche visant à tester la sécurité des systèmes d'information devrait résulter d'une réflexion préalable afin d'envisager les solutions les plus appropriées. Cette démarche doit prendre en considération les besoins spécifiques de l'organisation, tant sur le plan organisationnel que technique.

# Chapitre 4 : Réalisation

---

## Introduction

Dans le cadre de la mission d'audit réglementaire confiée à notre société, Audit Technique, nous nous concentrons sur la phase de réalisation de l'audit. Cette étape cruciale englobe la mise en œuvre des procédures d'audit planifiées, la collecte des preuves et la documentation des observations pertinentes. L'objectif est de nous assurer que les activités de l'entité auditée sont conformes aux exigences réglementaires en vigueur et de vérifier l'efficacité des contrôles internes en place.

Au cours de cette phase, nos auditeurs ont suivi une méthodologie rigoureuse, basée sur les normes internationales d'audit, pour garantir l'objectivité et la fiabilité des conclusions tirées. Ils ont utilisé une combinaison de techniques d'audit, telles que les entretiens, les examens documentaires, les tests de contrôle et les analyses de données, afin d'obtenir une compréhension approfondie des processus de l'entité auditée.

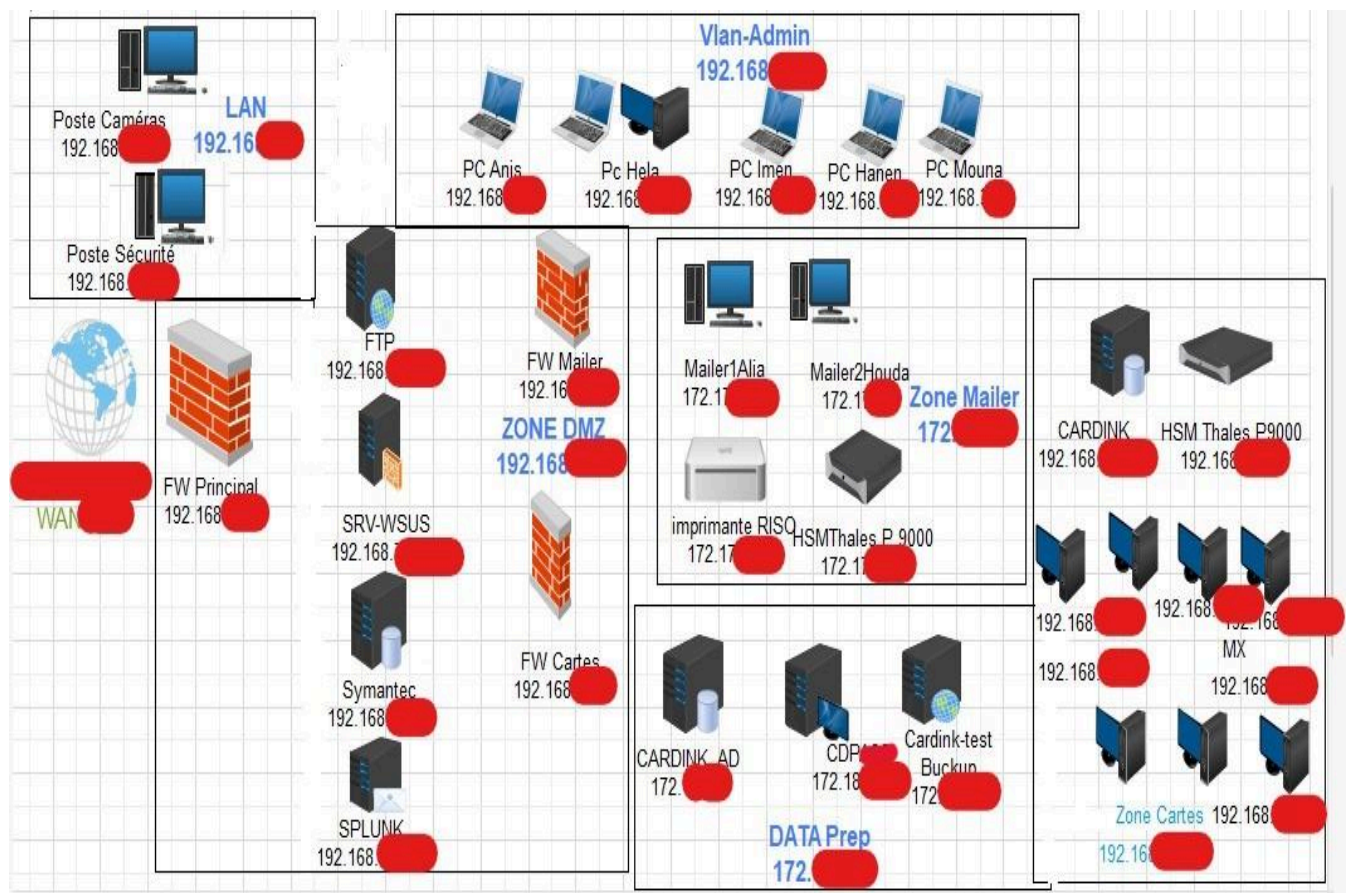
## 1 .Présentation du périmètre

Dans le cadre de l'audit de l'infrastructure de l'entreprise, le périmètre d'audit englobe l'ensemble des composants, systèmes et réseaux faisant partie intégrante de l'infrastructure informatique de l'entreprise. Cela inclut les serveurs, les postes de travail, les périphériques réseau, les dispositifs de stockage de données, les équipements de réseau, ainsi que les logiciels et applications utilisés.

Cette section décrit l'étendue de l'audit, en se concentrant spécifiquement sur le réseau local de l'entreprise, pour évaluer les vulnérabilités internes et la robustesse de la sécurité du système d'information.

Durant cette étape, nous allons procéder à une inspection du réseau afin de déterminer sa topologie, d'identifier les hôtes connectés et les équipements réseau. Pour

réaliser cette tâche, nous commençons par un recueil des données concernant les équipements inventoriés.



**Figure 4.1 :** Infrastructure de l'entreprise lors de l'audit

Cette figure montre le périmètre de société inclut les éléments suivants :

**flux de données WAN :**

- Cette adresse IP est utilisée pour la sortie des flux de données sur le réseau WAN, assurant la connectivité externe de l'entreprise.

● **Zone DMZ :**

- **Firewall Principal :** Le firewall principal protège le réseau interne contre les menaces extérieures et contrôle le trafic entrant et sortant pour garantir la sécurité des données sensibles.
- **Firewall Mailer :** Firewall dédié à la protection des services de messagerie.
- **Firewall Cartes :** Firewall dédié à la protection des applications et des données industrielles liées aux cartes

- **Serveur FTP** : Utilisé pour le transfert de fichiers entre différents segments du réseau et avec des partenaires externes.
- **Serveur SRV-WSUS** : Serveur de mises à jour Windows Server Update Services pour gérer les mises à jour des systèmes d'exploitation.
- **Serveur Symantec** : Serveur de sécurité pour la gestion des antivirus et autres solutions de sécurité Symantec.
- **Serveur Splunk** : Utilisé pour la collecte, le monitoring et l'analyse des données machine générées par les applications, les systèmes et les infrastructures IT.
- **Zone LAN :**
  - **Poste de contrôle caméra** : Ordinateur dédié à la surveillance des caméras de sécurité.
  - **Poste de sécurité** : Poste de travail utilisé par le personnel de sécurité pour le monitoring et la gestion des systèmes de sécurité.
- **VLAN-Admin :**
  - Comprend 5 postes de travail utilisés par le personnel administratif de la société. Ce VLAN est segmenté pour offrir une sécurité renforcée et une gestion centralisée des ressources administratives.
- **Zone Mail :**
  - **2 postes d'employés** : Postes de travail utilisés par les employés pour les communications internes et externes.
  - **Imprimante** : Périphérique de sortie utilisé par les employés pour imprimer des documents.
  - **HSM Thales** : Module matériel de sécurité utilisé pour la protection des clés cryptographiques et le chiffrement des données sensibles.
  - **Zone de messagerie de la société But** : Assure la segmentation du réseau pour les services de messagerie, garantissant ainsi une meilleure sécurité et une gestion efficace du trafic.
- **Zone DATA Prep :**
  - **Serveur CARDINK AD** : Serveur Active Directory pour la gestion des utilisateurs et des ressources de l'entreprise.
  - **CDP de la société** : Serveur de sauvegarde et de restauration des données critiques.

- **Cardink-test backup** : Serveur de tests et de sauvegarde pour les applications Cardink.
- **Zone Industry(Zone Carte) :**
  - **Serveur Cardink** : Serveur principal pour les opérations industrielles liées aux cartes.
  - **HSM Thales** : Module matériel de sécurité pour la protection des clés cryptographiques et le chiffrement des données critiques.
  - **7 postes de travail** : Postes de travail utilisés par les employés pour les opérations industrielles.

## 2. Présentation des échelles utilisées

L'évaluation des risques est classée selon quatre niveaux :

Niveau de risque	Description
<b>Mineur</b>	Faible risque pour le système d'information, nécessitant une correction à long terme.
<b>Important</b>	Risque modéré pour le système d'information, nécessitant une correction à moyen terme.
<b>Majeur</b>	Risque significatif pour le système d'information, nécessitant une correction à court terme.
<b>Critique</b>	Risque extrêmement élevé pour le système d'information, nécessitant une correction immédiate ou imposant un arrêt immédiat du service.

**Table 4.1** : L'échelle de risque

Le niveau de risque d'une vulnérabilité est calculé en fonction de sa difficulté d'exploitation et de son impact potentiel sur le système d'information. La table suivante illustre les différents niveaux de risque associés à la difficulté d'exploitation d'une vulnérabilité :

Difficulté d'exploitation	Description
<b>Difficile</b>	Exploitation de vulnérabilités non publiées nécessitant une expertise en sécurité des systèmes d'information et le développement d'outils spécifiques et ciblés.
<b>Elevée</b>	Exploitation de vulnérabilités publiques nécessitant des compétences en sécurité des systèmes d'information et le développement d'outils simples.
<b>Modérée</b>	Exploitation nécessitant des techniques simples et des outils disponibles publiquement.
<b>Facile</b>	Exploitation triviale, ne nécessitant ni outil ni compétence particulière.

**Table 4.2 :** Le niveau de risque d'une vulnérabilité

Ainsi une description des niveaux d'impact technique CVSS de la vulnérabilité, en complément de l'évaluation des risques .

Cette échelle évalue l'impact des incidents sur le métier, en attribuant une valeur en fonction de la gravité :

Niveau De Risque	Score	
<b>Critique</b>	<b>9.0 -&gt; 10</b>	<b>INACCEPTABLE</b>
<b>Élevée</b>	<b>7.0 -&gt; 8.9</b>	ACCEPTABLE SOUS CONDITIONS
<b>Moyen</b>	<b>4.0 -&gt; 6.9</b>	MODERE
<b>Faible</b>	<b>0.1 -&gt; 3.9</b>	ACCEPTABLE
<b>Pas de Risque</b>	<b>0</b>	ACCEPTABLE

**Table 4.3 :** Échelle de gravité métier

### 3. Outil d'audit utilisés

Dans le contexte du test de pénétration (pentest), l'utilisation de divers outils se révèle indispensable pour conduire avec succès les différentes phases de l'évaluation de sécurité. Ces outils revêtent une importance capitale en automatisant des tâches spécifiques, en identifiant des vulnérabilités, et en fournissant des informations cruciales qui permettent aux professionnels de la sécurité d'atteindre les objectifs du pentest de manière efficace. Ce chapitre théorique explore quelques-uns des principaux outils de pentesting utilisés, offrant un aperçu essentiel pour la compréhension approfondie de ce processus d'évaluation de la sécurité.

Outils	Version utilisée	Licence	Fonctionnalités	Composantes du SI objet de l'audit
Microsoft Windows	11 Pro 64Bit	OEM	OS Windows développé par Microsoft, exploitant le noyau Windows NT	L'application Web, ServeurWeb , Web service
Kali Linux	V 2022.1	GNU General Public License	OS ; boîte d'outils pour tester la sécurité des systèmes d'information et des infrastructure réseau.	L'application Web, ServeurWeb , Web service,
OWASP ZAP	V2.11.1	Open source	(Zed Attack Proxy) Scanner de sécurité d'applications Web open source.	L'application Web, ServeurWeb
Nmap	V7.91	GNU GPL	Analyse et d'interception de flux réseaux	Web service, ServeurWeb
WireShark	V 3.6.2	GNU General Public License version 2	Sondage et de reconnaissance du réseau	L'application Web, ServeurWeb
Subgraph Vega	1.0	Open source	Vega est un scanner et une plateforme pour tester le Niveau de sécurité des applications Web	Application Web
Zenmap	V7.92	GNU GPL	Analyse et d'interception de flux réseaux	Web service, Serveur Web, ServeurWeb
Nessus	V10.1.0-X64	Open source 16 @IP	Analyse de vulnérabilités	Serveur, PC, Réseau

**Table 4.3 :** Outil d'audit utilisés

### 4 . Etat de maturité de la sécurité du système d'information

Pour évaluer la maturité de la sécurité du système d'information, nous avons utilisé dans ma tâche le référentiel ISO 27001:2022, en particulier les contrôles énumérés dans l'annexe A. Cette section présente une analyse détaillée des contrôles vérifiés et la maturité



associée pour chaque domaine du référentiel d'audit de la sécurité des systèmes d'information.

### Mesures de Sécurité Technologiques (Annexe A.1, Module 8)

Dans le cadre de l'annexe A.1, module 8, nous avons examiné en détail les mesures de sécurité technologiques.

l'application des mesures techniques basées sur les normes ISO 27001:2022 est essentielle pour assurer une protection robuste des systèmes d'information. En intégrant des technologies comme les pare-feu, les systèmes d'alarme, les caméras et les systèmes de sécurité des portes, et en suivant un SMSI rigoureux, les entreprises peuvent réduire significativement leurs risques et renforcer leur sécurité globale. Les mesures de sécurité technologiques de l'annexe A.1, module 8, fournissent un cadre supplémentaire pour évaluer et améliorer continuellement la sécurité de l'information.

Ces mesures de sécurité sont cruciales pour assurer la protection des informations et des systèmes contre les accès non autorisés .

**Table 4.4 :** Terminaux finaux des utilisateurs

Article		Exigence	Moyen de vérification (recommandations sans s'y limiter)	Vérifications à effectuer	Niveau de Conformité
8. Mesures de sécurité technologiques					
8.2	Droits d'accès privilégiés	L'attribution et l'utilisation des droits d'accès privilégiés doivent être limitées et gérées.	<ul style="list-style-type: none"> <li>• Revue du processus d'attribution des droits privilégiés et la conformité de sa mise en œuvre avec la politique de contrôle d'accès,</li> <li>• Revue des comptes d'accès privilégiés,</li> <li>• Revue des logs des accès,</li> <li>• Interview des administrateurs systèmes, réseaux, BD et applications et des responsables métier pour l'identification des droits d'accès privilégiés et des conditions de leur expiration.</li> </ul>	<ul style="list-style-type: none"> <li>• Si les utilisateurs qui ont besoin de droits d'accès privilégiés pour chaque système ou processus (par exemple, les systèmes d'exploitation, les systèmes de gestion de bases de données et les applications) sont identifiés,</li> <li>• Si les droits d'accès privilégiés sont attribués aux utilisateurs au besoin et au cas par cas, conformément à la politique de contrôle d'accès et en respectant le principe du « moindre privilège »,</li> <li>• Si les exigences d'expiration des droits d'accès privilégiés ont été définies et mises en œuvre,</li> <li>• Si des mesures sont mises en place pour s'assurer que les utilisateurs ont conscience de leurs droits d'accès privilégiés et savent quand ils sont en mode d'accès privilégié (par exemple l'utilisation d'identités utilisateur spécifiques, de paramètres d'interface utilisateur ou même d'un matériel spécifique),</li> <li>• Si les exigences d'authentification relatives aux droits d'accès privilégiés sont plus élevées que les exigences relatives aux droits d'accès normaux,</li> </ul>	

**Table 4.5 :** Droits d'accès privilégiés

Article		Exigence	Moyen de vérification (recommandations sans s'y limiter)	Vérifications à effectuer	Niveau de Conformité
8. Mesures de sécurité technologiques					
8.3	Restriction d'accès aux informations	L'accès aux informations et autres actifs associés doit être restreint conformément à la politique spécifique à la thématique du contrôle d'accès qui a été établie.	<ul style="list-style-type: none"> <li>• Revue de la politique de contrôle d'accès,</li> <li>• Revue des identités des utilisateurs,</li> <li>• Revue de la matrice des rôles d'accès,</li> <li>• Interview des administrateurs</li> </ul>	<ul style="list-style-type: none"> <li>• Si les restrictions d'accès sont basées sur des exigences individuelles de l'application métier et conformément à la politique de contrôle d'accès définie,</li> <li>• Si des mécanismes de configuration pour contrôler l'accès aux informations dans les</li> </ul>	

**Table 4.6 :** Restriction d'accès aux informations

Article		Exigence	Moyen de vérification (recommandations sans s'y limiter)	Vérifications à effectuer	Niveau de Conformité
8. Mesures de sécurité technologiques					
8.11	Masquage des données	Le masquage des données doit être utilisé conformément à la politique spécifique à la thématique du contrôle d'accès de l'organisation et d'autres politiques spécifiques à une thématique associées, ainsi qu'aux exigences métier, tout en prenant en compte la législation applicable.	<ul style="list-style-type: none"> <li>• Revue de la politique de contrôle d'accès,</li> <li>• Revue des procédures de masquage des données,</li> <li>• Interview du DSI et du responsable métier,</li> <li>• Revue des comptes d'accès privilégiés,</li> <li>• Revue des logs des accès.</li> </ul>	<ul style="list-style-type: none"> <li>• Si des procédures de masquage des données sont mises en place conformément à la politique de contrôle d'accès et aux exigences métier, tout en prenant en compte les exigences d'ordre légal,</li> <li>• Si ces procédures sont mises en œuvre et permettent de limiter l'exposition de données sensibles, notamment les données à caractère personnel, et de se conformer aux exigences légales, statutaires, réglementaires et contractuelles,</li> <li>• Si l'accès aux outils de masquage des données n'est possible qu'aux utilisateurs autorisés,</li> <li>• Si les restrictions d'accès ou l'utilisation des données traitées sont mises en place.</li> </ul>	

**Table 4.7 :** Masquage des données

## 5. Audit organisationnelles et physiques

Nous avons visé à obtenir une vision qualitative et quantitative des différents facteurs de la sécurité informatique du site audité et à identifier les points critiques du système d'information. L'audit fonctionnel sera réalisé en se basant sur des entretiens avec le responsable et sur des observations effectuées sur le site.

### ❖ Méthodologie

L'audit fonctionnel a été réalisé en se basant sur :

- **Entretiens** : Discussions avec le responsable de la sécurité informatique.
- **Observations** : Examen des pratiques et infrastructures physiques sur le site.

### ❖ Organisationnelles

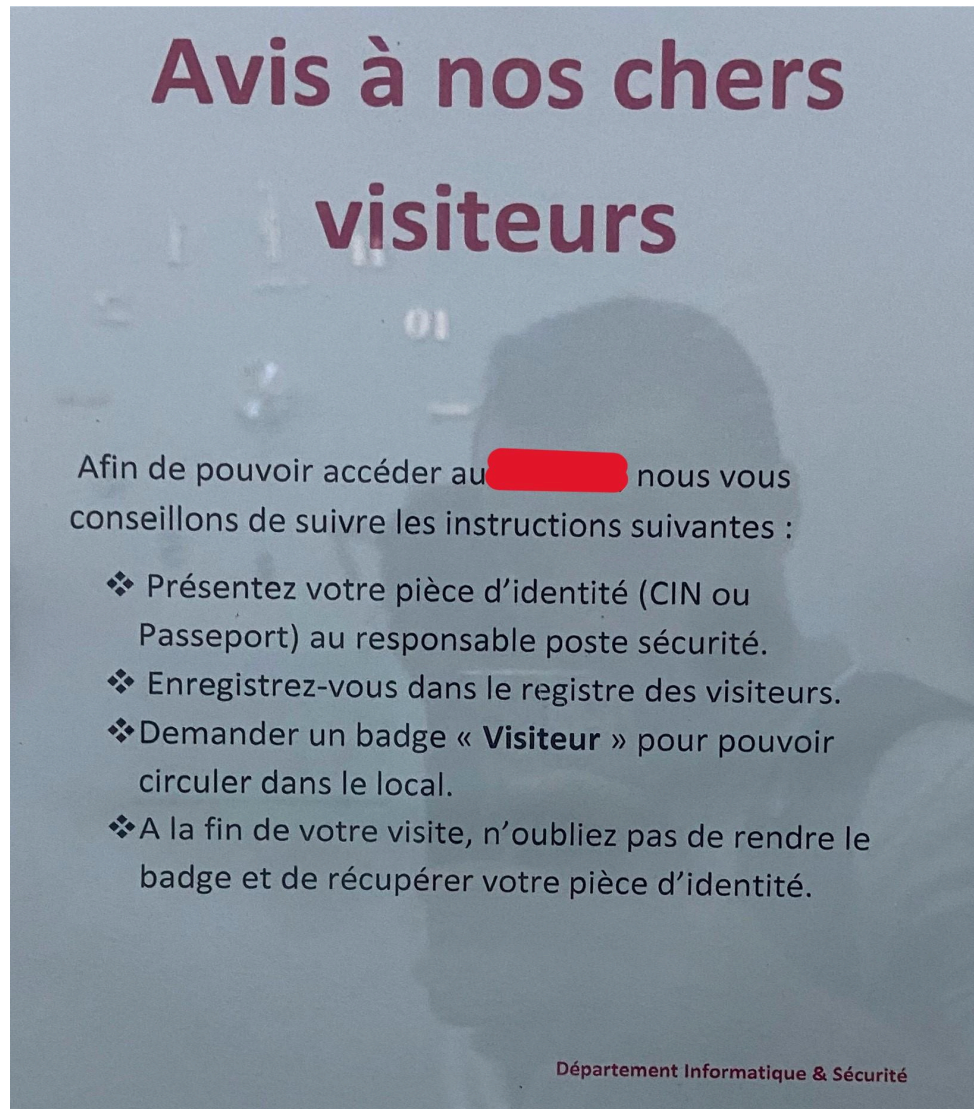
Dans cette tâche, nous avons vérifié les aspects organisationnels de l'audit de cette société. Dans la première partie.

Nous avons observé un **générateur** à l'extérieur de la société.



**Figure 4.2** : générateur à l'extérieur de la société

Ensuite, dans la zone de sécurité, notée 24/24, nous avons constaté qu'il y avait de nombreuses procédures en place. À l'entrée, des avis pour les visiteurs étaient bien visibles. Vous pouvez voir ces observations illustrées dans la figure ci-dessous :



**Figure 4.3:** Exemples d'observations de chers visiteurs

Ces observations mettent en lumière la nécessité d'une amélioration continue dans la gestion des actifs physiques et des processus organisationnels pour renforcer la sécurité globale du site.





## ENGAGEMENT DE CONFIDENTIALITE VISITEUR

Les locaux que vous allez visiter sont spécialisés dans la personnalisation de produits de haute sécurité (Cartes et codes confidentiels). Nous vous souhaitons la bienvenue et vous saurions gré de veiller à ce que les procédures et règles de sécurité suivantes soient pleinement respectées.

### Les règles de sécurité

- Pour visiter les ateliers de production, vous devez absolument être accompagnés d'un membre du personnel [REDACTED]
- Il est strictement interdit d'emporter tout document, produit ou objet appartenant à [REDACTED] sans l'accord préalable du management de [REDACTED] et sans remplir le « Bon de Sortie » disponible dans l'administration.
- Il est interdit d'utiliser les appareils photographiques et les téléphones mobiles lors de la visite des ateliers du site [REDACTED]

### Protection de l'information

Lors de votre visite, vous pouvez avoir accès à des informations confidentielles et dont la divulgation pourrait être préjudiciable [REDACTED] et à ses clients.

Nous vous demandons de bien vouloir signer cet accord à travers lequel vous vous engagez à :

- ✓ Ne pas divulguer ou utiliser, sans l'autorisation écrite du Management [REDACTED] aucune des informations dont vous auriez connaissance.
- ✓ Respecter toutes les règles de sécurité [REDACTED]
- ✓ N'accéder qu'aux renseignements nécessaires et autorisés par [REDACTED] et n'utiliser ces renseignements que dans le cadre de votre visite;
- ✓ N'écrire sur quelque support que ce soit aucune information sensible telle que n° de carte, n° de compte, n° de chèque, clés informatiques, et informations clients des fichiers ou états éditiques.

Fait à Tunis, le : 12/06/2024

Nom et prénom : Ben Ammar Nader

Signature Précédée de la mention

"Lu et approuvé"

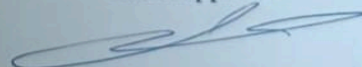


Figure 4.5: Engagement de confidentialité visiteur

### ❖ Physique

Dans la section audit physique, nous avons présenté un exemple de sécurité physique, notamment **la zone de la salle mailler**. Il convient de noter que les zones mailler ne sont pas accessibles à tous les visiteurs et employés, mais uniquement au personnel spécifique de cette société.



Pour accéder à la salle mailer, nous avons passé par plusieurs étapes. La zone mailer comprend (le serveur CARDINK AD, le CDP de la société et le Cardink-test backup). Nous avons franchi **3 sas** et **contrôleur d'accès** pour accéder à cette zone.



**Figure 4.6: avant entre du SAS**



**Figure 4.7: Sortie du SAS**

Pour passer à travers les SAS, les étapes suivantes ont été suivies :

1. **Identification** : Présentation d'une carte d'identité ou d'un badge d'accès pour authentifier l'identité de la personne.
2. **Autorisation** : Vérification des autorisations d'accès spécifiques à chaque SAS, généralement par un agent de sécurité ou un système de contrôle d'accès.
3. **Ouverture** : Si les autorisations sont valides, les portes du SAS sont déverrouillées pour permettre à la personne de passer.
4. **Fermeture** : Une fois que la personne a franchi le SAS, les portes se referment derrière elle pour maintenir la sécurité de la zone restante.

Ces étapes sont conçues pour contrôler strictement l'accès à une zone sécurisée et garantir que seules les personnes autorisées y entrent.

Dans la salle mailer, nous avons remarqué plusieurs éléments importants pour la sécurité



**Figure 4.8:** la salle mailer

- **Contrôleur d'accès du SAS :** Un dispositif permettant de contrôler l'accès à la salle depuis les SAS précédents, assurant ainsi que seules les personnes autorisées peuvent y entrer.
- **Système de détection incendie :** Des dispositifs d'incendie en cas de tout départ de feu, garantissant la sécurité en cas d'urgence.
- **Coffre-fort hautement classifié :** Un coffre-fort sécurisé contenant des éléments sensibles tels que des clés, des disques de sauvegarde de données Mastercard et Visa, ainsi que d'autres données confidentielles. L'accès à ce coffre-fort est strictement limité et contrôlé.

La présence de ces dispositifs de sécurité dans la salle mailer renforce la protection des données sensibles et des actifs critiques de l'entreprise.



## **6 . Taxonomies des failles techniques**

Dans le cadre de l'audit technique, cette étude organisationnelle et physique permet d'avoir une vue globale de l'état de sécurité du système d'information et d'identifier les risques potentiels. À cette étape, nous passons à la recherche des vulnérabilités afin d'analyser le niveau de protection de l'infrastructure face aux attaques, notamment celles qui exploitent ces vulnérabilités.

Nous avons effectué des tests de pénétration (pentest) externes BlackBox , internes et audit de configuration pour évaluer la sécurité du système d'information de l'organisme audité. Les résultats sont présentés ci-dessous, organisés selon les domaines du référentiel d'audit de la sécurité des systèmes d'information[9].

### **6.1 Scan de Vulnérabilités de PCI DSS**

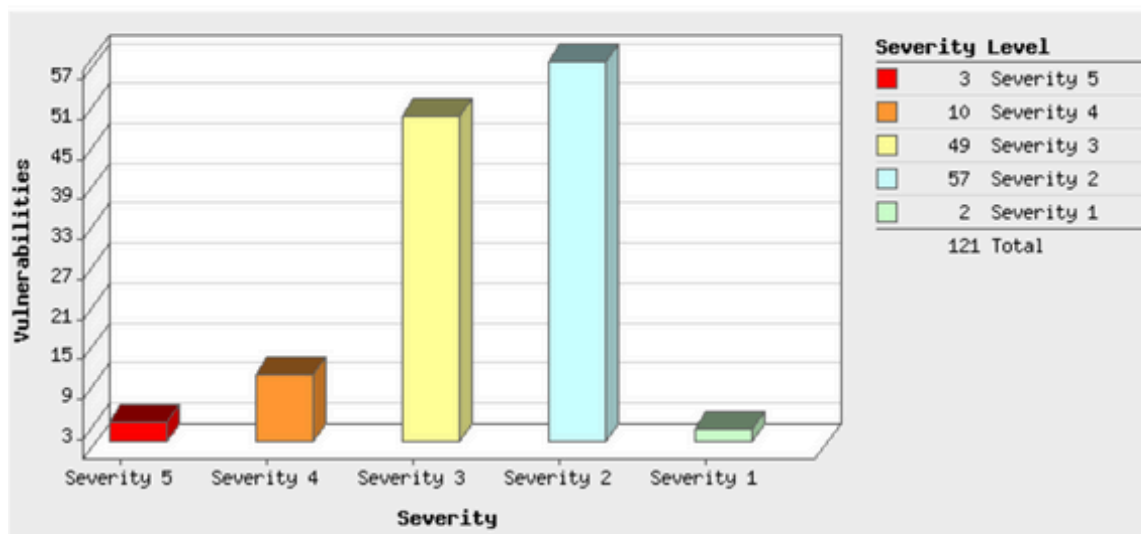
Dans le cadre de analyse des vulnérabilités , j'ai lancé un scan de vulnérabilités conforme aux normes PCI DSS afin de détecter et d'afficher l'état des vulnérabilités présentes. Pour ce faire.

Nous avons utilisé Qualys, une plateforme de sécurité informatique (cloud) qui fournit des solutions de gestion des vulnérabilités, de conformité et de sécurité informatique. En tant que fournisseur de services d'évaluation approuvé (ASV) pour la norme PCI DSS, Qualys permet aux entreprises de détecter, évaluer et remédier aux vulnérabilités présentes dans leurs systèmes et réseaux. Ses outils automatisés aident à identifier les failles de sécurité, à assurer la conformité réglementaire et à protéger les données sensibles contre les cyberattaques. La plateforme présente les vulnérabilités par gravité, facilitant ainsi la priorisation des actions correctives.

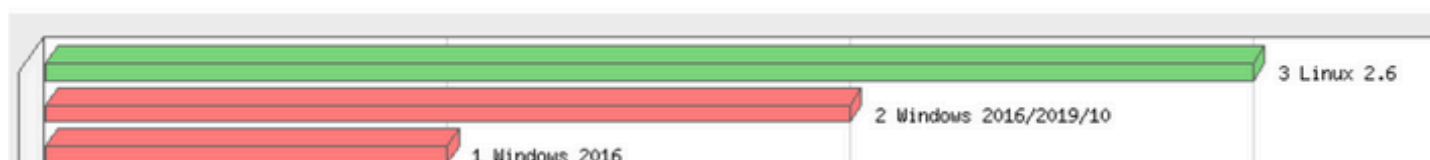
Le scan a permis d'identifier plusieurs vulnérabilités critiques, majeures et mineures au sein de l'infrastructure auditée.

Voici un résumé des résultats :

## Vulnerabilities by Severity



## Operating Systems Detected



**Figure 4.9 : Résultats de scan des vulnérabilités PCI DSS**

Le scan de vulnérabilités effectué avec l'ASV scanner de Qualys a permis d'identifier et de classer efficacement les vulnérabilités présentes dans notre infrastructure :

- **3 vulnérabilités critiques**
- **10 vulnérabilités élevées**
- Le reste sont des informations mineures et des services/protocoles détectés.

Grâce à cette évaluation, nous avons pu prioriser les mesures correctives et améliorer significativement la sécurité des données de paiement, assurant ainsi notre conformité aux normes PCI DSS.

Par la suite, je vais mesurer les vulnérabilités des parties les plus sensibles du réseau local pour identifier rapidement les failles réellement dangereuses. Grâce à l'utilisation d'outils

spécialisés, je pourrai générer des rapports efficaces et exploitables, facilitant ainsi une sécurisation rapide et efficace du système.

## 6.1 Pentest externe :

Dans le cadre de notre mission d'audit technique pour la conformité PCI DSS , nous avons réalisé un test d'intrusion externe (Pentest) afin d'identifier les vulnérabilités potentielles et de renforcer la sécurité des systèmes traitant les données de cartes bancaires.

### Identification des ports ouverts

Nous allons maintenant exécuter une analyse du réseau à l'aide de nmap pour déterminer quels ports TCP sont ouverts et quel service ils exécutent.

```
(daruis@kali)-[~]
$ sudo nmap -p- -v -v [redacted]
Starting Nmap 7.94SVN ( https://nmap.org ) [redacted] 13:11 EDT
Initiating Ping Scan at 13:11
Scanning [redacted] [4 ports]
Completed Ping Scan at 13:11, 0.15s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:11
Completed Parallel DNS resolution of 1 host. at 13:11, 0.39s elapsed
Initiating SYN Stealth Scan at 13:11
Scanning 41.226.1.142 [65535 ports]
SYN Stealth Scan Timing: About 13.55% done; ETC: 13:14 (0:03:18 remaining)
SYN Stealth Scan Timing: About 28.33% done; ETC: 13:15 (0:02:57 remaining)
SYN Stealth Scan Timing: About 41.68% done; ETC: 13:15 (0:02:41 remaining)
Discovered open port 4500/tcp on 41.226.1.142
SYN Stealth Scan Timing: About 32.64% done; ETC: 13:18 (0:04:59 remaining)
SYN Stealth Scan Timing: About 40.02% done; ETC: 13:18 (0:04:36 remaining)
SYN Stealth Scan Timing: About 47.29% done; ETC: 13:18 (0:03:59 remaining)
SYN Stealth Scan Timing: About 53.15% done; ETC: 13:18 (0:03:35 remaining)
SYN Stealth Scan Timing: About 59.34% done; ETC: 13:18 (0:03:12 remaining)
SYN Stealth Scan Timing: About 65.36% done; ETC: 13:18 (0:02:44 remaining)
SYN Stealth Scan Timing: About 71.71% done; ETC: 13:19 (0:02:18 remaining)
SYN Stealth Scan Timing: About 77.40% done; ETC: 13:19 (0:01:52 remaining)
SYN Stealth Scan Timing: About 82.98% done; ETC: 13:19 (0:01:26 remaining)
SYN Stealth Scan Timing: About 88.40% done; ETC: 13:19 (0:01:00 remaining)
SYN Stealth Scan Timing: About 94.04% done; ETC: 13:19 (0:00:31 remaining)
Completed SYN Stealth Scan at 13:20, 544.04s elapsed (65535 total ports)
Nmap scan report for [redacted]
Host is up, received echo-reply ttl 241 (0.052s latency).
Scanned at 2024-05-26 13:11:05 EDT for 544s
Not shown: 65533 filtered tcp ports (no-response)
PORT      STATE SERVICE REASON
113/tcp   closed ident  reset ttl 50
4500/tcp  open  sae-urn syn-ack ttl 63

Read data files from: /usr/bin/../../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 544.76 seconds
Raw packets sent: 197016 (8.669MB) | Rcvd: 472 (18.872KB)
```

Figure 4.10 : Scan tous les ports TCP

Le résultat du scan de tous les ports TCP avec Nmap montre qu'un port est ouvert, le port **4500**, et qu'un port est fermé, le port **113**, comme indiqué dans les résultats de Nmap.

Nous allons maintenant utiliser `nmap` pour déterminer quels ports **UDP** sont ouverts et quel service ils exécutent.

```
(daruis@kali)-[~]
$ sudo nmap -sU -p- [REDACTED]
Starting Nmap 7.94SVN ( https://nmap.org ) at [REDACTED] EDT
Stats: 0:02:41 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 4.01% done; ETC: 13:47 (1:04:09 remaining)
Stats: 0:10:02 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 14.53% done; ETC: 13:49 (0:59:03 remaining)
Stats: 0:11:28 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 16.55% done; ETC: 13:50 (0:57:49 remaining)
Stats: 0:24:54 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 76.19% done; ETC: 13:13 (0:07:47 remaining)
Nmap scan report for [REDACTED]
Host is up (0.050s latency).
Not shown: 65534 open|filtered udp ports (no-response)
PORT      STATE SERVICE
123/udp   open  ntp

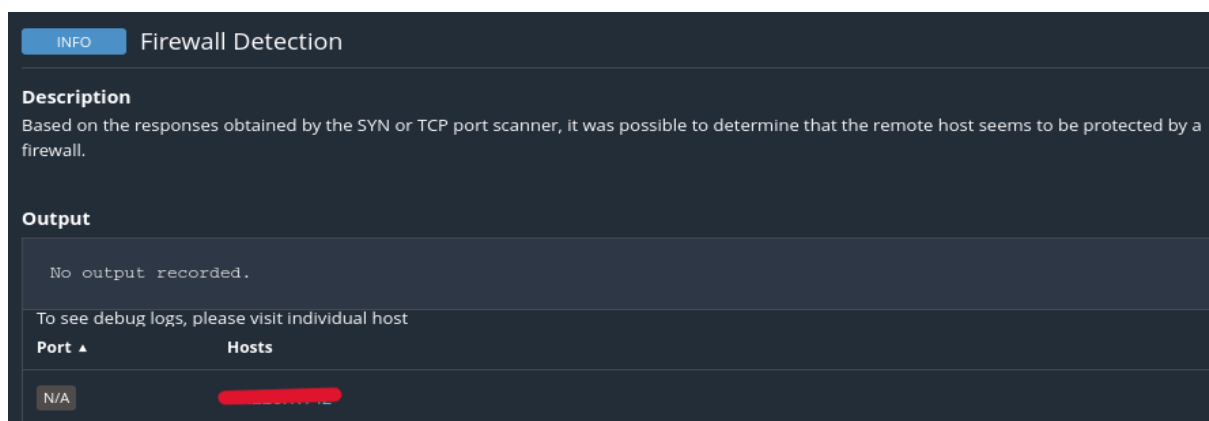
Nmap done: 1 IP address (1 host up) scanned in 1520.46 seconds
```

**Figure 4.11** : Scan tous les ports UDP

Le résultat du scan de tous les ports UDP avec Nmap montre qu'un port est ouvert, le port **123**, comme indiqué dans les résultats de nmap.

## → Divulgarion des informations sensible

Lors de l'analyse de la sécurité de réseau, a détecté la présence d'un pare-feu avec **Nessus**.



**Figure 4.12** : détecté la présence d'un pare-feu

Dans cette partie, nous allons vérifier si le port du pare-feu est ouvert en effectuant un scan.

```
(daru@kali)-[~]
$ sudo nmap -v -sU -p 500 -T1 192.168.1.1 -Pn

Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 17:14 EDT
Initiating Parallel DNS resolution of 1 host. at 17:14
Completed Parallel DNS resolution of 1 host. at 17:14, 0.48s elapsed
Initiating UDP Scan at 17:14
Scanning 192.168.1.1 [1 port]
Completed UDP Scan at 17:15, 45.04s elapsed (1 total ports)
Nmap scan report for 192.168.1.1
Host is up.

PORT      STATE      SERVICE
500/udp   open|filtered isakmp

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 45.58 seconds
Raw packets sent: 8 (1.124KB) | Rcvd: 0 (0B)
```

Figure 4.13 : Scan port pare-feu

Après ce scan, le résultat montre que le port 500 du pare-feu est **ouvert/filtré**.  
Nous allons maintenant utiliser Nmap pour afficher les informations en utilisant diverses techniques d'évasion de pare-feu [10].  
Voici **exemple** de Commandes utilisées :

DESCRIPTION	COMMANDE	EXPLICATION
Utilisation de paquets IP fragmentés	nmap 192.168.1.1 -f	Demande que le scan (y compris les scans ping) utilise de petits paquets IP fragmentés, rendant la détection plus difficile pour les filtres de paquets.
Scan à partir d'une IP usurpée	nmap -S www.microsoft.com 192.168.1.1	Scanne cible en utilisant l'adresse IP de Microsoft (les options -e eth0 et -Pn peuvent être nécessaires).
Ajout de données aléatoires aux paquets envoyés	nmap --data-length 200 192.168.1.1	Ajoute des données aléatoires aux paquets envoyés pour rendre la détection plus difficile.
Définir votre propre taille d'offset	nmap 192.168.1.1 -mtu 32	Permet de spécifier la taille des fragments pour augmenter les chances de contourner les dispositifs de sécurité.

Table 4.8 : Évasion de pare-feu et Usurpation

Après avoir utilisé ces commandes pour afficher des informations détaillées sur l'infrastructure réseau, nous avons réussi à identifier **le modèle et la version du pare-feu**.

Cependant, il est important de noter que ces détails spécifiques sont considérés comme des informations hautement confidentielles et ne seront pas divulgués dans ce rapport, conformément aux exigences de confidentialité liées à l'audit.

## ● Preuve

Les vulnérabilités affectant les pare-feu **Fortinet FortiGate version 5** peuvent toucher plusieurs versions spécifiques de cette gamme.

```
Nmap scan report [REDACTED]
Host is up (0.038s latency).
Not shown: 999 filtered tcp ports (no-response), 997 open|filtered udp ports (no-response)
PORT      STATE SERVICE VERSION
500/udp   open  isakmp  Fortinet FortiGate v5
| ike-version:
|   vendor_id: Fortinet FortiGate v5
|   attributes:
|     Dead Peer Detection v1.0
|   XAUTH
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: OpenBSD 4.X
OS CPE: cpe:/o:openbsd:openbsd:4.0
OS details: OpenBSD 4.0, OpenBSD 4.3
Network Distance: 12 hops
Service Info: OS: Fortigate v5; Device: Network Security Appliance; CPE: cpe:/h:fortinet:fortigate
```

**Figure 4.14 :** Version de Firewall

Les vulnérabilités affectant les pare-feu **Fortinet FortiGate version 5** peuvent toucher plusieurs versions spécifiques de cette gamme. Voici une liste des versions affectées par certaines des vulnérabilités connues :

### 1. CVE-2019-15705

- **Nom :** Improper Certificate Validation
- **Description :** La validation incorrecte des certificats SSL/TLS peut permettre des attaques de type Man-in-the-Middle (MitM).
- **Impact :** Les communications sécurisées peuvent être interceptées et modifiées par des attaquants, compromettant la confidentialité et l'intégrité des données.

## 2. CVE-2016-4962

- **Nom** : Request Remote Code Execution
- **Description** : Vulnérabilité dans le traitement de certaines requêtes HTTPS qui permet l'exécution de code arbitraire.

## 3. CVE-2018-13382 - Authentication Bypass

- **Description** : Une faille dans la méthode d'authentification permet à un attaquant de contourner le mécanisme d'authentification à deux facteurs (2FA).
- **Impact** : Un attaquant pourrait accéder au système avec des privilèges élevés sans les informations d'authentification correctes, compromettant potentiellement l'ensemble du réseau.

## 4. CVE-2016-7496

- **Nom** : Authentication Bypass in Web Management Interface
- **Description** : Vulnérabilité de contournement d'authentification dans l'interface web d'administration.

## 5. CVE-2016-7545

- **Nom** : Command Injection via Management Interface
- **Description** : Vulnérabilité due à une validation insuffisante des entrées permettant l'exécution de commandes arbitraires sur le système.

## 6. CVE-2016-1909

- **Nom** : Remote Code Execution via HTTP Request
- **Description** : Permet l'exécution de code arbitraire à distance par un attaquant non authentifié via une requête malveillante.

<b>Nom de la vulnérabilité</b>	<b>Remote Code Execution (RCE)</b>
<b>Risque</b>	<b>Critique</b>
<b>Score CVSS</b>	<b>9.8</b>
<b>Description</b>	Cette vulnérabilité permet à un attaquant non authentifié d'exécuter du code arbitraire à distance sur les appareils <b>Fortinet FortiGate</b> utilisant la version 5 du firmware. Cette faille est causée par une validation insuffisante des entrées dans le composant de gestion de configuration du pare-feu.
<b>Eléments impact</b>	Pare-feu

**Table 4.9** : Remote Code Execution

<b>Vecteur d'attaque (AV)</b>	<b>Distance (D)</b>
<b>Complexité de l'attaque (AC)</b>	<b>Faible (L)</b>
<b>Privilège requis (PR)</b>	<b>Aucun (N)</b>
<b>Interaction avec l'utilisateur (UI)</b>	<b>Aucun (N)</b>
<b>Portée (S)</b>	<b>Inchangée (U)</b>

**Table 4.10 : Métriques d'Exploitabilité de Remote Code Execution**

<b>Impact sur la confidentialité (C)</b>	<b>Elève (H)</b>
<b>Impact sur l'intégrité (I)</b>	<b>Elevé (H)</b>
<b>impact sur la disponibilité (A)</b>	<b>Faible (L)</b>

**Table 4.11 : Métriques d'Impact de Remote Code Execution**

La divulgation de détails sensibles, tels que le modèle **Fortinet FortiGate** et la **version 5** du pare-feu et **portée 500**, peut exposer votre infrastructure à des risques de sécurité accrus. Il est essentiel de traiter ces informations avec la plus grande confidentialité et de limiter leur accès aux parties autorisées et concernées par l'audit. En garantissant la confidentialité de ces données, vous protégez la sécurité et l'intégrité de votre réseau contre les menaces potentielles.

## **6.2 Pentest interne :**

Dans le cadre d'audit de sécurité, nous avons effectué un test d'intrusion interne, également connu sous le nom de Pentest. L'objectif principal de ce Pentest était d'identifier les éventuelles vulnérabilités au sein de votre infrastructure interne, en mettant un accent particulier sur les systèmes traitant les données sensibles des cartes bancaires. Ce processus



nous a permis d'évaluer la robustesse de vos mesures de sécurité internes et de recommander des actions correctives pour renforcer votre posture de sécurité.

### 6.2.1 Évaluation de la Sécurité de la Zone DMZ

Nous allons maintenant effectuer une analyse du réseau à l'aide de NESSUS et Nmap pour déterminer quels ports sont ouverts et quel service ils exécutent.

<input type="checkbox"/> Host ▾	Ports
<input type="checkbox"/> 192.168.1.1	135, 139, 445, 1025, 1026, 1027, 1028, 1029, 1030, 1031
<input type="checkbox"/> 192.168.1.2	135, 139, 445, 49664, 49665, 49666, 49667, 49668, 49669, 49677
<input type="checkbox"/> 192.168.1.3	135, 139, 445, 49664, 49665, 49666, 49667, 49668, 49669, 49671

**Figure 4.15** : Scan des port ouvert avec Nessus

Par la suite, nous allons utiliser d'autres méthodes de scan, notamment le scan des ports ouverts avec Nmap, pour afficher des résultats complémentaires.

Nous avons maintenant lancé un scan de vulnérabilités de la **zone DMZ** pour évaluer la sécurité de cette zone avec **Nessus**. Ce scan a pour objectif de détecter les failles potentielles et les vulnérabilités qui pourraient mettre en danger l'infrastructure de la zone DMZ.

Filter ▾	Search Hosts	3 Hosts
<input type="checkbox"/> Host	Vulnerabilities ▾	
<input type="checkbox"/> 192.168.1.1	11 90	×
<input type="checkbox"/> 192.168.1.2	10 3 80	×
<input type="checkbox"/> 192.168.1.3	46	×

**Figure 4.16** : Scan de vulnérabilités de zone DMZ

Après l'utilisation de Nessus, plusieurs vulnérabilités ont été identifiées et classées selon leur gravité. Nous avons ensuite procédé à une vérification de ces vulnérabilités en suivant l'ordre de priorités de notre société. Cette approche systématique nous permet de cibler d'abord les failles les plus critiques et de garantir une amélioration progressive et continue de la sécurité de notre infrastructure.

Nous avons continué notre audit de sécurité en utilisant Nmap pour détecter les ports ouverts sur notre réseau. Les résultats du scan ont révélé des informations supplémentaires qui **n'avaient pas été identifiées** par d'autres outils comme Nessus.

Voici les nouveaux résultats du scan Nmap :

```
Not shown: 65518 filtered tcp ports (no-response)
PORT      STATE SERVICE      REASON
21/tcp    open  ftp          syn-ack ttl 64
135/tcp   open  msrpc        syn-ack ttl 64
139/tcp   open  netbios-ssn  syn-ack ttl 64
443/tcp   open  https        syn-ack ttl 64
445/tcp   open  microsoft-ds syn-ack ttl 64
990/tcp   open  ftps         syn-ack ttl 64
1025/tcp   open  NFS-or-IIS   syn-ack ttl 64
1026/tcp   open  LSA-or-nterm syn-ack ttl 64
1028/tcp   open  unknown      syn-ack ttl 64
1029/tcp   open  ms-lsa       syn-ack ttl 64
1030/tcp   open  iad1         syn-ack ttl 64
1031/tcp   open  iad2         syn-ack ttl 64
5985/tcp   open  wsman        syn-ack ttl 64
8089/tcp   open  unknown      syn-ack ttl 64
8530/tcp   open  unknown      syn-ack ttl 64
8531/tcp   open  unknown      syn-ack ttl 64
47001/tcp  open  winrm        syn-ack ttl 64
```

**Figure 4.17 :** Scan des port ouvert avec NMAP

Nous allons chercher à obtenir des informations détaillées sur le modèle et la version du serveur **FTP**. Pour ce faire, nous avons utilisé Nmap avec des scripts de détection de version.

```

(daruis@kali)-[~]
└─$ sudo nmap -p 21 -Pn -sV -v -v 192.168.1.111
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-05 06:05 EDT
NSE: Loaded 46 scripts for scanning.
Initiating Parallel DNS resolution of 1 host. at 06:05
Completed Parallel DNS resolution of 1 host. at 06:05, 0.03s elapsed
Initiating SYN Stealth Scan at 06:05
Scanning 192.168.1.111 [1 port]
Discovered open port 21/tcp on 192.168.1.111
Completed SYN Stealth Scan at 06:05, 0.05s elapsed (1 total ports)
Initiating Service scan at 06:05
Scanning 1 service on 192.168.1.111: 21/tcp
Completed Service scan at 06:05, 11.18s elapsed (1 service on 1 host)
NSE: Script scanning 192.168.1.111.
NSE: Starting runlevel 1 (of 2) scan: $DIR." HTTP/1.0\n";
Initiating NSE at 06:05
Completed NSE at 06:05, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan:
Initiating NSE at 06:05
Completed NSE at 06:05, 0.00s elapsed
Nmap scan report for 192.168.1.111
Host is up, received user-set (0.0074s latency).
Scanned at 2024-06-05 06:05:11 EDT for 11s

PORT      STATE SERVICE REASON
21/tcp    open  ftp     syn-ack ttl 64
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

```

Figure 4.18 : service info de version et os de serveur FTP

- Test d'Exploitation par Brute Force

Nous avons ensuite effectué une attaque par force brute sur le serveur FTP identifié dans la zone DMZ en utilisant l'outil **Hydra** de Kali Linux.

Voici les étapes et les résultats :

```

(daruis@kali)-[~]
└─$ hydra -t 4 -L /usr/share/wordlists/rockyou.txt -P /usr/share/wordlists/rockyou.txt -vV 192.168.1.111 ftp

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-06-05 06:14:19
[DATA] max 4 tasks per 1 server, overall 4 tasks, 205761782671201 login tries (l:14344399/p:14344399), ~51440445
[DATA] attacking ftp://192.168.1.111:21/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target 192.168.1.111 - login "123456" - pass "123456" - 1 of 205761782671201 [child 0] (0/0)
[ATTEMPT] target 192.168.1.111 - login "123456" - pass "12345" - 2 of 205761782671201 [child 1] (0/0)
[ATTEMPT] target 192.168.1.111 - login "123456" - pass "123456789" - 3 of 205761782671201 [child 2] (0/0)
[ATTEMPT] target 192.168.1.111 - login "123456" - pass "password" - 4 of 205761782671201 [child 3] (0/0)
[ATTEMPT] target 192.168.1.111 - login "123456" - pass "iloveyou" - 5 of 205761782671201 [child 2] (0/0)
[ATTEMPT] target 192.168.1.111 - login "123456" - pass "princess" - 6 of 205761782671201 [child 0] (0/0)
[ATTEMPT] target 192.168.1.111 - login "123456" - pass "1234567" - 7 of 205761782671201 [child 1] (0/0)
[ATTEMPT] target 192.168.1.111 - login "123456" - pass "rockyou" - 8 of 205761782671201 [child 3] (0/0)
[ATTEMPT] target 192.168.1.111 - login "123456" - pass "12345678" - 9 of 205761782671201 [child 0] (0/0)
[ATTEMPT] target 192.168.1.111 - login "123456" - pass "abc123" - 10 of 205761782671201 [child 1] (0/0)
[ATTEMPT] target 192.168.1.111 - login "123456" - pass "nicole" - 11 of 205761782671201 [child 3] (0/0)
[ATTEMPT] target 192.168.1.111 - login "123456" - pass "daniel" - 12 of 205761782671201 [child 2] (0/0)
[ATTEMPT] target 192.168.1.111 - login "123456" - pass "babygirl" - 13 of 205761782671201 [child 2] (0/0)
[ERROR] Not an FTP protocol or service shutdown: 550 No connections allowed from your IP
[ERROR] Not an FTP protocol or service shutdown: 550 No connections allowed from your IP
[VERBOSE] Retrying connection for child 1 length: ".$LENGTH."\\n\\n";
[VERBOSE] Retrying connection for child 3
[ERROR] Not an FTP protocol or service shutdown: 550 No connections allowed from your IP

```

Figure 4.19 : Brute Force de FTP

- **Résultats des Attaques par Force Brute**

Après avoir lancé les attaques par force brute sur le serveur FTP, nous avons observé que le **serveur a bloqué** les tentatives d'accès après **13 échecs** consécutifs. Les tests effectués ont montré que le serveur FTP est **efficacement protégé contre les attaques** par force brute, grâce à des mesures de sécurité telles que le blocage des tentatives après un certain nombre d'échecs. Cela démontre que le serveur FTP dans la zone DMZ est bien configuré et résistant aux tentatives d'exploitations courantes.

**Conclusion :** Efficace.

### 6.2.1 Mécanisme / politique d'accès défaillant

Nous avons découvert une vulnérabilité critique liée aux imprimantes connectées au réseau de la zone DMZ. Habituellement, ces imprimantes ne devraient pas être **accessibles** depuis cette zone, car elles sont censées être isolées dans la zone Mailer.

Malgré **l'isolation** attendue des imprimantes, notre analyse réseau a révélé leur présence et leur accessibilité depuis la zone DMZ. Cela indique une possible mauvaise configuration ou une faille dans la segmentation du réseau.

<b>Nom de la vulnérabilité</b>	<b>Mécanisme de gestion d'accès :</b> identification et authentification de mauvaise qualité
<b>Risque</b>	<b>Élevée</b>
<b>Score CVSS</b>	<b>8.5</b>
<b>Description</b>	L'application permet des attaques par <b>force brute</b> ou d'autres attaques automatisées. Elle autorise également l'utilisation de mots de passe par défaut, faibles ou bien connus, par exemple "Password1" ou "admin/admin".
<b>Éléments impact</b>	Imprimante

**Table 4.12 :** Mécanisme de gestion d'accès

<b>Vecteur d'attaque (AV)</b>	<b>Local (L)</b>
<b>Complexité de l'attaque (AC)</b>	<b>Faible (L)</b>
<b>Privilège requis (PR)</b>	<b>Aucun (N)</b>
<b>Interaction avec l'utilisateur (UI)</b>	<b>Aucun (N)</b>
<b>Portée (S)</b>	<b>Inchangée (U)</b>

**Table 4.13 :** Métriques d'Exploitabilité de Mécanisme de gestion d'accès

<b>Impact sur la confidentialité (C)</b>	<b>Elève (H)</b>
<b>Impact sur l'intégrité (I)</b>	<b>Elevé (H)</b>
<b>impact sur la disponibilité (A)</b>	<b>Faible (L)</b>

**Table 4.14 :** Métriques d'Impact de Mécanisme de gestion d'accès

## **Risques Techniques et Métier**

Bien que cela représente un risque élevé pour l'administration de l'application en soi, cela signifie qu'un attaquant pourrait utiliser une **attaque par force brute** (le principe général de l'attaque par force brute étant de tester l'ensemble des mots de passe possibles) pour obtenir les informations d'identification de l'administrateur ou d'un modérateur. Ensuite, l'attaquant pourrait accéder à la liste d'administration.

- **Preuve**

preuve qui démontre la réussite d'un exploit, et cette preuve a été imprimée à la fois avant et après l'événement ou l'exploit

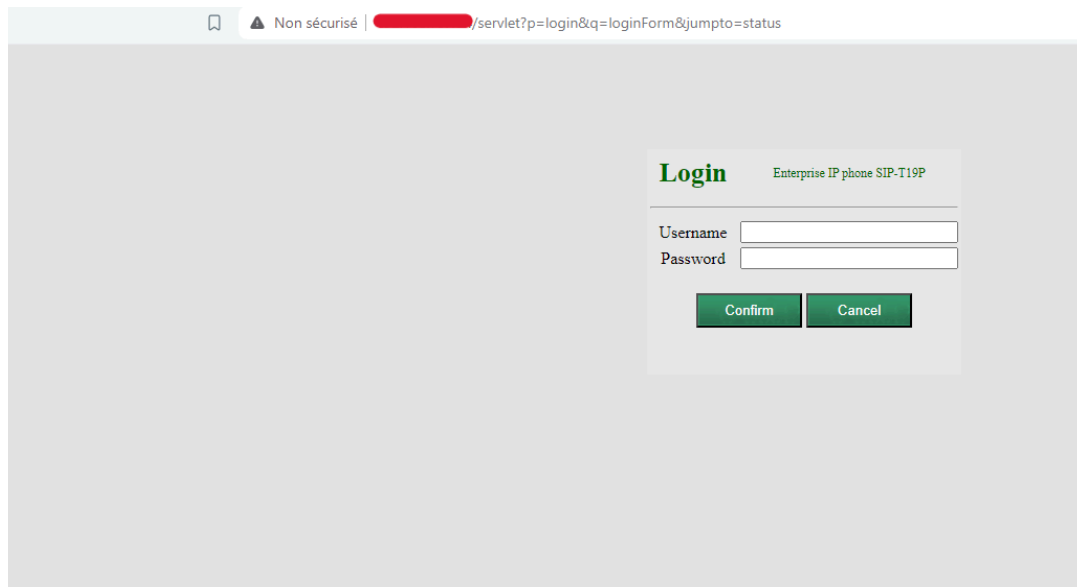


Figure 4.20 : Interface login d'Imprimante

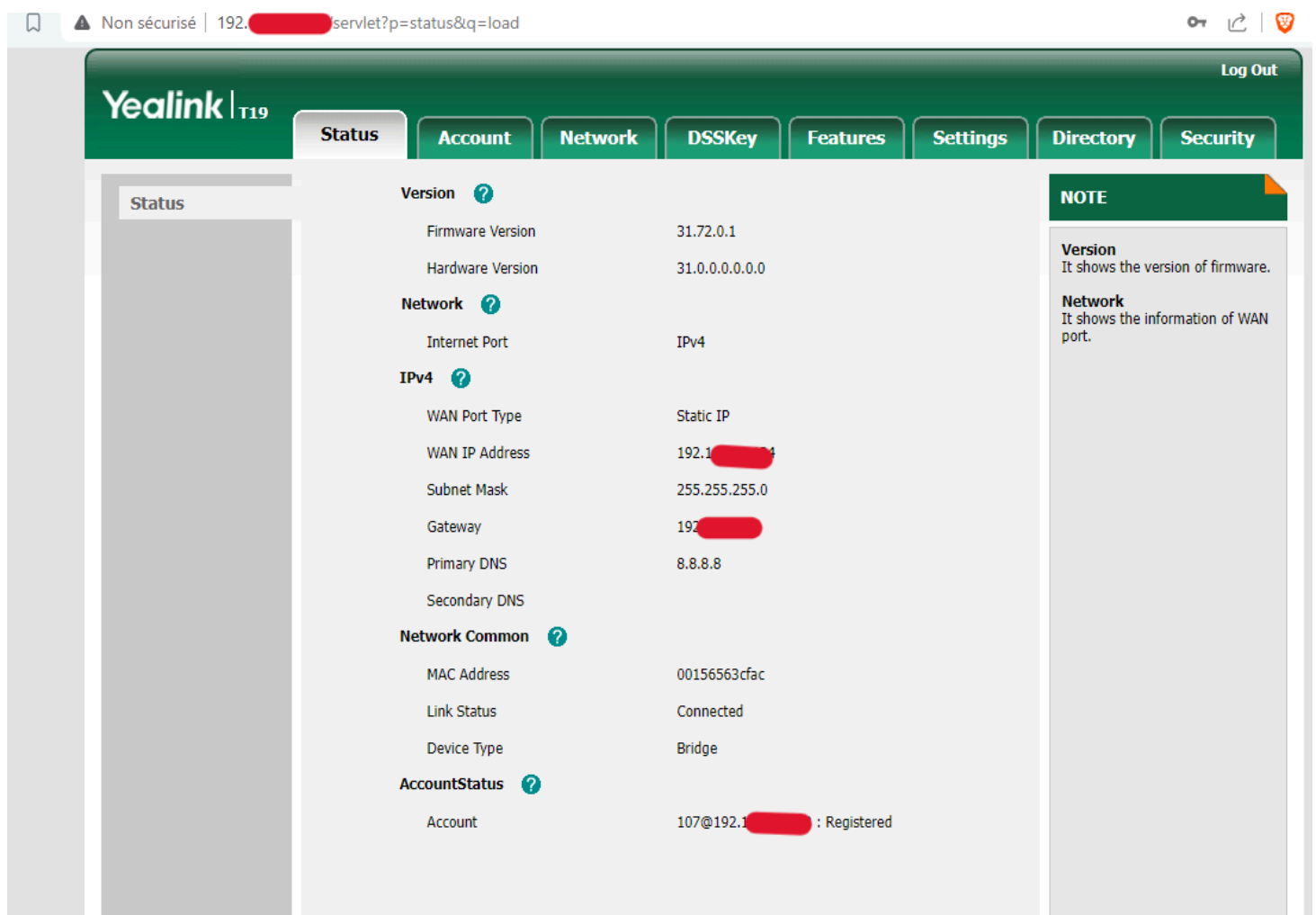
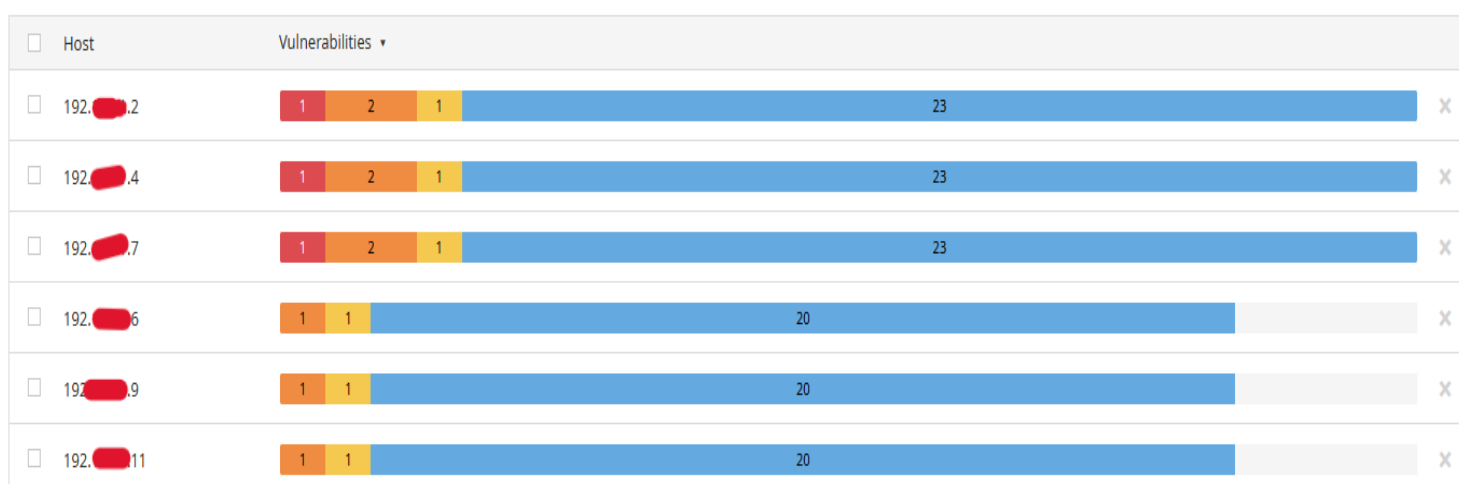


Figure 4.21 : Preuve de réussite de l'exploitation imprimant

Cette réussite souligne l'importance critique de sécuriser tous les périphériques connectés au réseau, y compris les appareils apparemment moins critiques tels que les imprimantes. L'exploitation réussie des imprimantes met en lumière les risques potentiels de sécurité associés à ces périphériques souvent négligés et souligne la nécessité de mettre en œuvre des mesures de sécurité appropriées pour les protéger contre les attaques potentielles.

## 6.2.2 Évaluation de la Sécurité de la Zone LAN

Nous avons suivi un processus rigoureux pour identifier et traiter des vulnérabilités critiques de notre réseau local (LAN). Nous avons lancé un scan de sécurité sur **la zone LAN** en utilisant l'outil Nessus.



**Figure 4.22** : Résultat de scan de zone LAN

Nessus a identifié plusieurs vulnérabilités, dont une particulièrement critique sur un **switch** spécifique. Nous avons confirmé que la vulnérabilité signalée sur la switch était bien réelle et **critique**. Cette vulnérabilité pourrait potentiellement être exploitée pour compromettre la sécurité du réseau.

<b>Nom de la vulnérabilité</b>	<b>Mauvaise configuration de sécurité</b>
<b>Risque</b>	<b>Élevée</b>
<b>Score CVSS</b>	<b>9.0</b>
<b>Description</b>	des fonctionnalités inutiles sont activées ou installées (ex : des ports, des services, des pages, des comptes ou des privilèges inutiles)
<b>Eléments impact</b>	Switch

**Table 4.15 : Mauvaise configuration de sécurité**

<b>Impact sur la confidentialité (C)</b>	<b>Elève (H)</b>
<b>Impact sur l'intégrité (I)</b>	<b>Elevé (H)</b>
<b>impact sur la disponibilité (A)</b>	<b>Faible (L)</b>

**Table 4.16 : Métriques d'Impact de Mauvaise configuration de sécurité**

- **Preuve**

preuve qui démontre la réussite d'un exploit, et cette preuve a été commutateur à la fois avant et après l'événement ou l'exploit et les informations sensibles .



HP (J998) Switch

J998

Username

Password

Log In

**Figure 4.23 : Interface login de Switch**



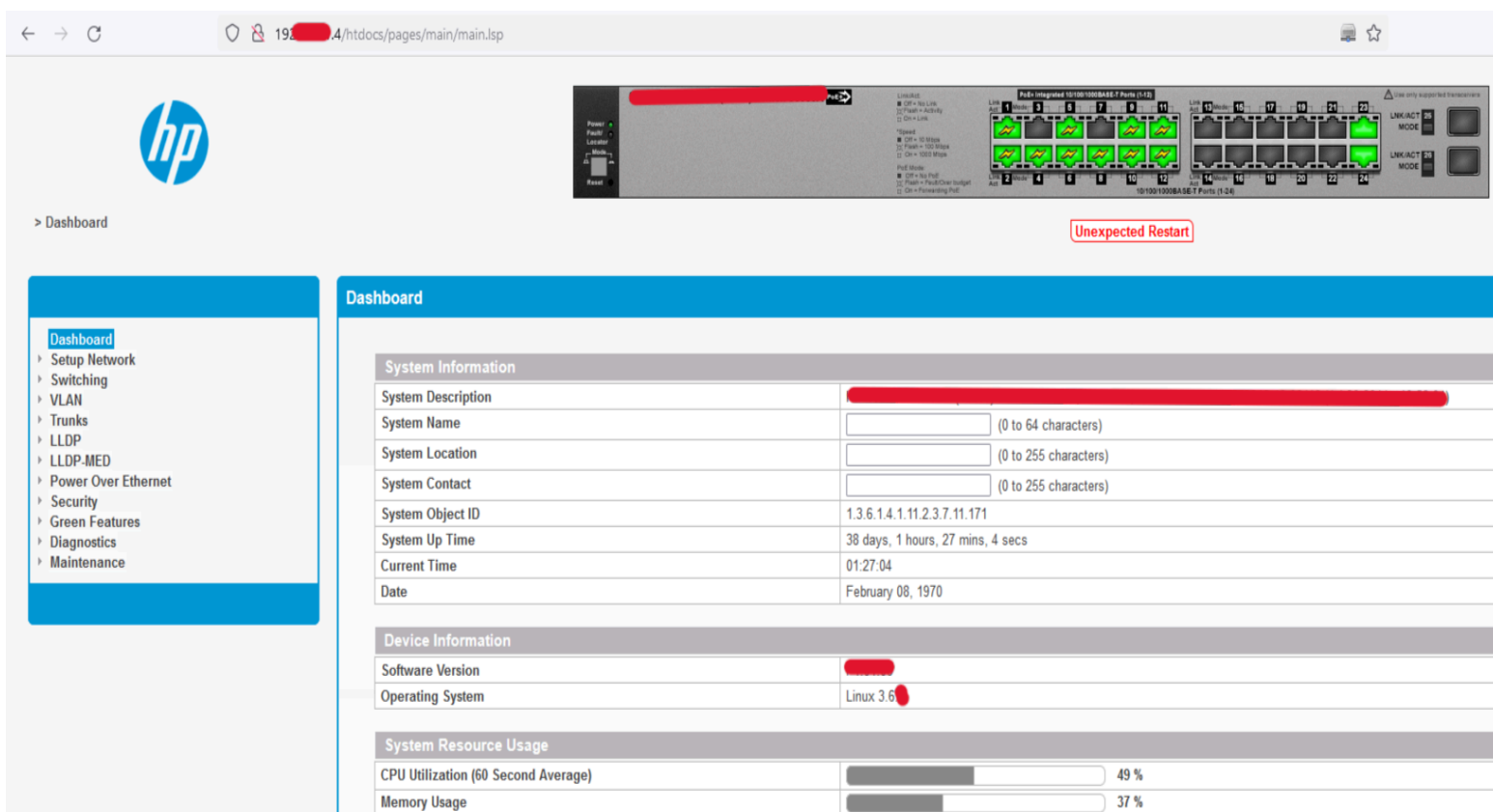


Figure 4.24 : Preuve de réussite de l'exploitation Switch

Cette réussite souligne l'importance critique de sécuriser tous les périphériques connectés au réseau.

## 6.3 audit de configuration

L'audit de configuration vise à utiliser le CIS Microsoft Windows Server 2016 Benchmark à évaluer la conformité des configurations actuelles des systèmes et des équipements par rapport aux standards et aux bonnes pratiques de sécurité **accès privilégié** et **analyse de la politique de mot de passe**. Cette étape est cruciale pour identifier les écarts potentiels et les configurations inadéquates pouvant être exploitées par des attaquants.

### **6.3.1 Accès privilégié**

Pour mieux comprendre le processus d'examen des comptes administrateur au niveau des applications, nous avons interrogé le directeur informatique de la société . Il a été constaté que la société dispose de procédures formelles pour l'examen et le suivi périodique des comptes administrateurs.

Nous avons rencontré le chef du service informatique ,Chef de projet, afin de mieux comprendre le processus d'examen des comptes administrateurs au niveau d'Active Directory (AD).

#### **1. Méthode d'Évaluation**

**Méthode :** Enquête et inspection

#### **2. Résultats de l'Évaluation**

##### **Contrôles de Révocation des Accès :**

Suite à l'entretien avec le directeur des systèmes d'information et à l'examen du schéma décrivant la procédure de révocation d'accès aux programmes et aux données, nous avons estimé que les contrôles encadrant la révocation des accès aux applications informatiques étaient efficacement conçus.

##### **Contrôles d'Accès à AD :**

Après avoir interrogé le directeur des systèmes d'information et examiné le processus de contrôle, nous avons conclu que les contrôles régissant l'accès à AD étaient globalement bien conçus. Cependant, nous avons identifié quelques recommandations mineures et des ajustements de configuration nécessaires pour renforcer l'efficacité du dispositif de contrôle.

##### **Efficacité Opérationnelle :**

En appliquant notre jugement professionnel, nous avons décidé qu'aucun test d'efficacité opérationnelle ne devait être effectué.

#### **3. Conclusion du Contrôle**

**Conclusion :** Efficace

### **6.3.2 - Analyse de la politique d'usage des mots de passe**

Les méthodes d'authentification utilisées sont les mots de passe au niveau des postes de travail et des serveurs.

#### **1. Méthode d'Évaluation**

**Méthode :** Enquête et inspection

#### **2. Résultats de l'Évaluation**

Nous remarquons les points suivants avec chef du service informatique concernant la politique d'usage des mots de passe :

- Pour les serveurs, routeurs et tous les autres équipements réseau, les mots de passe sont robustes en termes de nombre de caractères et de combinaison de minuscules, majuscules, chiffres, lettres et caractères spéciaux.
- Au niveau des postes de travail, chaque utilisateur est responsable de la définition de son mot de passe.
- Certains mots de passe (au niveau des postes) ressemblent aux noms des utilisateurs ou sont trop courts (moins de **14 caractères**), ce qui ne constitue pas une bonne pratique de sécurité.
- Une sensibilisation des utilisateurs sur les bonnes pratiques de sécurité est en cours de mise en place, ainsi qu'une procédure de contrôle a priori.
- Absence d'une charte d'utilisation qui spécifie aux utilisateurs leurs obligations de protection de leurs postes.
- Absence d'une politique définissant notamment la typologie des mots de passe autorisés, la longueur des mots de passe, les délais d'expiration, la technique de génération, et la fréquence de renouvellement des mots de passe.

#### **3. Conclusion du Contrôle**

**Conclusion :** Non Efficace

### 6.3.3 - Analyse du Firewall

Cette étape consiste à déterminer si le firewall fonctionne correctement. Le rôle du firewall est de contrôler l'accès selon une politique spécifique adaptée à ses huit interfaces. La démarche adoptée consiste à auditer le firewall, les règles de filtrage et les mécanismes de log.

#### 1. Méthode d'Évaluation

**Méthode :** Enquête et inspection

#### 2. Résultats de l'Évaluation

Lors d'une réunion avec le chef du service informatique, j'ai pu, à l'aide de la checklist, identifier les vulnérabilités suivantes du firewall :

- Absence d'une procédure de test périodique des vulnérabilités du firewall ainsi que des tests de pénétration pour vérifier la résistance du système contre les attaques.
- Absence d'un rapport d'audit à long terme présentant l'historique des incidents survenus au niveau du firewall (violation des ACLs, crash par débordement du tampon).
- L'administration n'est pas informée en temps réel des événements les plus critiques.

#### 3. Conclusion : Non Efficace

## 7. Recommandations

Après avoir terminé l'évaluation technique, les outils de scan et les tests techniques effectués ont permis de déceler des failles de sécurité et des vulnérabilités dans les différents composants du système d'information. Par la suite, je vais proposer des recommandations techniques à mettre en œuvre pour pallier les insuffisances et les défaillances détectées.

Pour renforcer la sécurité des systèmes et se conformer aux exigences PCI DSS, les recommandations suivantes ont été formulées :

- **Mise à jour et patching** : Appliquer régulièrement les mises à jour de sécurité et les correctifs pour tous les systèmes et applications.
- **Configuration sécurisée** : Revoir et renforcer les configurations des systèmes, en particulier les pare-feu et les systèmes de détection d'intrusion.
- **Formation et sensibilisation** : Sensibiliser les employés aux bonnes pratiques de sécurité et aux risques associés aux vulnérabilités identifiées.
- **Revue de la politique de sécurité** : Mettre à jour les politiques de sécurité pour inclure les meilleures pratiques et les recommandations spécifiques issues du pentest.

#### → Mécanisme de gestion d'accès :

- **Mots de Passe Forts** : Remplacer les mots de passe par défaut par des mots de passe forts et uniques pour chaque imprimante.
- **Authentification Multi-Facteurs (MFA)** : Si possible, implémenter des mécanismes d'authentification multi-facteurs pour l'accès aux imprimantes.
- **Segmentation Réseau** : Isoler les imprimantes dans un segment réseau distinct avec des contrôles d'accès stricts pour limiter l'accès aux seuls utilisateurs autorisés.
- **Surveillance et Journalisation** : Activer la surveillance et la journalisation des accès et des modifications sur les imprimantes pour détecter toute activité suspecte.
- **Mises à jour de sécurité** : S'assurer que les imprimantes sont régulièrement mises à jour avec les derniers correctifs de sécurité fournis par le fabricant.
- **Formation des Utilisateurs** : Sensibiliser les utilisateurs à l'importance de ne pas utiliser les identifiants par défaut et de choisir des mots de passe robustes.

#### → Politique d'usage des mots de passe :

- **Utilisation de mots de passe robustes** : Veillez à ce que tous les mots de passe, en particulier ceux des serveurs et des équipements réseaux et de sécurité, soient robustes et changés régulièrement.
- **Expiration des mots de passe** : Une bonne politique de sécurisation des accès par mot de passe consiste également à définir un délai d'expiration des mots de passe. Il

est par exemple possible de définir le renouvellement des mots de passe tous les 15, 30 ou 45 jours.

- **Confidentialité des mots de passe** : Ne divulguez jamais un mot de passe, surtout pas en l'envoyant par courrier électronique.
- **Stockage des mots de passe** : Évitez de noter le mot de passe quelque part ou de le laisser exposé (sur un écran, sous le clavier, dans un fichier non protégé, etc.).
- **Changements réguliers et historiques des mots de passe** : Proposez des changements réguliers tout en bloquant la possibilité d'utiliser des mots de passe déjà employés.
- **Audit de la politique de mots de passe** : Définissez la fréquence des audits afin de vous assurer que la politique est bien respectée. Des outils tels que LophtCrack, John the Ripper ou Crack permettent de contrôler régulièrement la robustesse des mots de passe.

#### → **Au niveau Firewall :**

- **Enregistrement des connexions** : Effectuer un enregistrement détaillé de toutes les traces de connexions bloquées ou autorisées par le firewall.
- **Statistiques d'usage** : Établir des statistiques sur l'usage du firewall pour analyser les tendances et les anomalies.
- **Mises à jour et patches** : Vérifier régulièrement et automatiquement les derniers patches et mises à jour à partir du site du constructeur pour garantir que le firewall est à jour.
- **Rapport d'audit à long terme** : Établir un rapport d'audit à long terme présentant l'historique des incidents survenus au niveau du firewall, y compris les violations des ACL et les crashes dus à des débordements de tampon.
- **Documentation des règles de filtrage** : Définir un document ou une spécification des règles de filtrage contenant une description de l'utilité de chaque filtre/règle.
- **Configuration du firewall** : Définir un document précisant la configuration du firewall et le suivi des modifications de cette configuration pour maintenir une traçabilité et assurer la cohérence des réglages.

## → Divulgence d'Informations Personnelles :

- **Analyse approfondie** : Effectuez une analyse approfondie pour identifier les points d'accès vulnérables où la divulgation d'informations personnelles a été détectée. Cela peut inclure une évaluation complète des entrées utilisateur, des sorties système, et des interactions avec les bases de données.
- **Correction Immédiate** : Mettez en œuvre des correctifs rapides pour sécuriser les points d'accès vulnérables. Assurez-vous que les données sensibles ne sont plus exposées dans les réponses du serveur. Cela peut nécessiter des ajustements au niveau du code, des configurations du serveur, ou des politiques de sécurité.
- **Politiques de Sécurité Renforcées** : Revoir et renforcer les politiques de sécurité de l'application. Intégrez des contrôles de sécurité supplémentaires, tels que des filtres de données, des mécanismes de cryptage robustes, et des validations strictes, pour prévenir toute divulgation accidentelle d'informations personnelles.

## → Mauvaise configuration de sécurité

Pour remédier à la mauvaise configuration de sécurité, notamment en ce qui concerne les fonctionnalités inutiles activées ou installées, telles que des ports, des services, des pages, des comptes ou des privilèges non nécessaires, voici les recommandations à suivre :

- **Analyse des Services et Ports** :
  - Effectuer un audit complet des services et ports actuellement activés sur tous les systèmes.
  - Désactiver ou fermer tous les services et ports qui ne sont pas nécessaires au fonctionnement de l'infrastructure.
- **Gestion des Comptes** :
  - Réaliser une revue périodique des comptes utilisateurs et administrateurs.
  - Supprimer ou désactiver les comptes qui ne sont plus utilisés ou nécessaires.
  - Assurer que chaque compte a des privilèges minimaux nécessaires à ses fonctions (principe du moindre privilège).
- **Contrôle des Privilèges** :

- Mettre en place une politique stricte de gestion des privilèges.
- Réduire les privilèges des comptes utilisateur à ce qui est absolument nécessaire pour leurs tâches.
- Utiliser des comptes distincts pour les tâches administratives et non-administratives.
- **Revue des Pages Web et Services Exposés :**
  - Effectuer un inventaire des pages web et services exposés à l'internet ou à des réseaux non sécurisés.
  - Désactiver ou restreindre l'accès aux pages et services qui ne sont pas essentiels.
- **Mises à Jour et Patches :**
  - Assurer que tous les systèmes et applications sont à jour avec les derniers patches de sécurité.
  - Mettre en place un processus régulier de gestion des patches pour garantir que les nouvelles vulnérabilités sont rapidement corrigées.
- **Configuration Sécurisée par Défaut :**
  - Revoir et appliquer les configurations de sécurité par défaut recommandées par les fabricants et les meilleures pratiques de l'industrie.
  - Documenter et valider les configurations pour chaque système et application.
- **Formation et Sensibilisation :**
  - Former les administrateurs et les utilisateurs aux bonnes pratiques de sécurité, y compris la gestion des configurations et des privilèges.
  - Sensibiliser les utilisateurs sur les risques associés à la mauvaise configuration de sécurité.
- **Surveillance Continue :**
  - Mettre en place des outils de surveillance pour détecter toute activité anormale ou non autorisée.
  - Réaliser des audits réguliers pour s'assurer que les configurations restent sécurisées et conformes aux politiques définies.



## **8. Conclusion**

Le contrôle de la sécurité réseau, tant interne qu'externe, fait partie intégrante de la démarche sécuritaire d'une société. Comme nous l'avons détaillé, ce contrôle devient aussi complexe que les techniques mises en place contre les attaques. Les tests d'intrusion sont un outil essentiel pour les entreprises afin de découvrir les vulnérabilités de leurs systèmes face aux cyberattaques. Bien que les tests d'intrusion internes ne doivent pas être négligés, les menaces internes sont beaucoup moins courantes, ce qui en fait une priorité moindre.

Nous avons approfondi notre compréhension du déroulement d'une mission d'audit informatique à travers toutes ses étapes, dans le but de garantir que la gouvernance des technologies de l'information de l'entreprise auditée est correctement mise en place. En outre, nous avons analysé les vulnérabilités ainsi que les faiblesses organisationnelles et techniques, et avons fourni des recommandations adéquates pour remédier aux insuffisances de contrôle interne informatique détectées dans le système d'information de l'entité auditée.

# 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 dans le cadre d'une mission d'audit réglementaire pour une société de l'industrie des cartes bancaires. C'est pourquoi nous avons concentré notre travail sur deux parties distinctes : la partie théorique et la partie pratique.

La partie théorique consistait à passer en revue les notions d'audit du système de management de la sécurité de l'information (SMSI), ainsi que les normes et référentiels pertinents. Nous avons utilisé **des checklists** basées sur l'ISO 27001 et le PCI DSS. Nous avons également exploré les politiques et méthodes d'audit essentielles dans ce domaine.

La partie pratique, quant à elle, a impliqué la réalisation d'une infrastructure pour une entreprise afin d'effectuer un **test d'intrusion**. Cette approche nous a permis d'évaluer concrètement la gestion de la sécurité de l'information. En théorie comme en pratique, la notion de sécurité de l'information a pris une importance considérable 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, ainsi qu'aux dommages matériels et autres, les entreprises trouvent désormais essentiel de se munir d'une variété de moyens pour protéger leurs ressources d'information. Depuis longtemps, la sécurité des systèmes informatiques, et plus généralement des systèmes d'information, était considérée comme un aspect secondaire par les sociétés. Cependant, une prise de conscience progressive a mis la sécurité des systèmes d'information (SSI) au premier plan. La raison principale est liée à la multitude d'incidents et aux pertes graves qui en résultent, causant des impacts significatifs pour les entreprises. La trilogie confidentialité, intégrité, disponibilité détermine la valeur d'une information. L'exemple du test d'intrusion que nous avons effectué nous a permis d'apprécier la gestion de la sécurité de l'information. Nous savons qu'un système, quel qu'il soit, n'est jamais assuré à **100 %** contre les diverses menaces ou risques, qui sont de plus en plus nombreux avec les nouvelles technologies de l'information. Par conséquent, la sécurité de l'information est cruciale pour toute entreprise qui veut maintenir son activité et son image de marque dans le monde des affaires actuel.

En conclusion, il est essentiel de s'atteler à réduire au maximum les risques pouvant survenir et ainsi préserver les différents systèmes d'informations.

# Webographie

---

- [1] IT cybersec expert : <https://it-cybersec.expert/> consulté le 25/02/2024.
- [2] ANCS : <https://www.ancs.tn/fr/audit/cadre-juridique> ,Cadre juridique et règlementaire de la mission d'audit , consulté le 02/03/2024.
- [3] PCI DSS : <https://www.pcisecuritystandards.org> ,des normes de sécurité ,consulté le 10/03/2024.
- [4] ISO 27001 :2022 : <https://www.iso.org/> , La famille norme ISO 27k , consulté le 07/04/2024.
- [5] Information security management systems Requirements:  
<https://www.iso.org/obp/ui#iso:std:iso-iec:27001:ed-2:v1> , consulté le 07/04/2024.
- [6] Référentiel d'Audit de la Sécurité des Systèmes d'Information :  
[https://www.ancs.tn/sites/default/files/Referentiel\\_Audit%203.1.pdf](https://www.ancs.tn/sites/default/files/Referentiel_Audit%203.1.pdf) ,consulté le 07/04/2024.
- [7] Méthodologies d'audit : <https://www.ancs.tn/fr/audit/methodologies> , consulté le 10/03/2024.
- [8] Politique d'audit au sein de votre entreprise : <https://openclassrooms.com/fr/courses/1756306-planifiez-une-politique-daudit-au-sein-de-votre-entreprise/6381281-determinez-le-cadre-legislatif-et-normatif-des-audits> , consulté le 10/03/2024.
- [9] OWASP : [https://owasp.org/www-project-web-security-testing-guide/v41/3-The\\_OWASP\\_Testing\\_Framework/1-Penetration\\_Testing\\_Methodologies](https://owasp.org/www-project-web-security-testing-guide/v41/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies) ,consulté le 20/05/2024
- [10] Outils Pentest infrastructure: <https://github.com/ESD-academy/Outils/tree/master/Pentest%20infra> , consulté le 22/04/2024.
- [11] MÉHARI : <https://clusif.fr/services/management-des-risques/les-fondamentaux-de-mehari/> , , consulté le 15/05/2024.

# Annexes

## Annexe A

<b>8</b>		<b>Mesure de sécurité</b>
<b>8.1</b>	Terminaux finaux des utilisateurs	<b>Mesure de sécurité</b> Les informations stockées, traitées ou accessibles via les terminaux finaux des utilisateurs, doivent être protégées.
<b>8.2</b>	Droits d'accès privilégiés	<b>Mesure de sécurité</b> L'attribution et l'utilisation des droits d'accès privilégiés doivent être limitées et gérées.
<b>8.3</b>	Restriction d'accès aux informations	<b>Mesure de sécurité</b> L'accès aux informations et autres actifs associés doit être restreint conformément à la politique spécifique à la thématique du contrôle d'accès qui a été établie.
<b>8.4</b>	Accès aux codes source	<b>Mesure de sécurité</b> L'accès en lecture et en écriture au code source, aux outils de développement et aux bibliothèques de logiciels doit être géré de manière appropriée.
<b>8.5</b>	Authentification sécurisée	<b>Mesure de sécurité</b> Des technologies et procédures d'authentification sécurisées doivent être mises en œuvre sur la base des restrictions d'accès aux informations et de la politique spécifique à la thématique du contrôle d'accès.
<b>8.6</b>	Dimensionnement	<b>Mesure de sécurité</b> L'utilisation des ressources doit être surveillée et ajustée selon les besoins de dimensionnement actuels et prévus.
<b>8.7</b>	Protection contre les programmes malveillants(malware)	<b>Mesure de sécurité</b> Une protection contre les programmes malveillants doit être mise en œuvre et renforcée par une sensibilisation appropriée des utilisateurs.
<b>8.8</b>	Gestion des vulnérabilités techniques	<b>Mesure de sécurité</b> Des informations sur les vulnérabilités techniques des systèmes d'information utilisés doivent être obtenues, l'exposition de L'organisation à ces vulnérabilités doit être évaluée et des mesures appropriées doivent être prises

<b>8.9</b>	Gestion des configurations	<b>Mesure de sécurité</b> Les configurations, y compris les configurations de sécurité, du matériel, des logiciels, des services et des réseaux, doivent être définies, documentées, mises en œuvre, surveillées et révisées.
<b>8.10</b>	Suppression des informations	<b>Mesure de sécurité</b> Les informations stockées dans les systèmes d'information, les terminaux ou tout autre support de stockage doivent être supprimées lorsqu'elles ne sont plus nécessaires.
<b>8.11</b>	Masquage des données	<b>Mesure de sécurité</b> Le masquage des données doit être utilisé conformément à la politique spécifique à la thématique du contrôle d'accès de l'organisation et d'autres politiques spécifiques à une thématique associée, ainsi qu'aux exigences métier, tout en prenant en compte la législation applicable.