République algérienne démocratique et populaire Ministre de l'enseignement supérieur et de la recherche scientifique

Université Saad Dahlab blida 1

Faculté Des Sciences

Département d'Informatique

Mémoire de fin d'études

Pour l'obtention du diplôme de Master en informatique

Option : Sécurité des Systèmes d'Information

Thème :

Mise en œuvre de la gestion des risques : durcissement du niveau de sécurité

Réalisé par :

OUNNOUGHI Fatma Zohra

SERIR Sekoura

Promotrice :

Mme BOUSTIA Nerhimane

Encadré par :

Mr SELMANE Mohammed

Jury:

Mme ARKAM Meriem

Mr SAHNOUNE Zakaria

2020-2021

Remerciement

Tout d'abords à ALLAH l'unique dieu

Tout d'abord, nous devons notre plus profonde gratitude à notre superviseur, M. Selmane Mohammed, pour son soutien enthousiaste, ses conseils savants et sa patience constante tout au long de notre stage. Sa perception du travail bien organisée a été une source d'inspiration continue pour nous.

Deuxièmement, nous tenons à exprimer notre gratitude à nos familles pour leur soutien indéfectible, leur amour et leurs encouragements tout au long de notre vie.

Un merci spécial au père d'Ounnoughi Fatma Zohra, Ounnoughi Kamal Eddine, car ce stage et cette thèse n'auraient pas vu le jour sans lui. Nous lui sommes entièrement dévoués.

Et un grand merci à Mme Choukran Dihia pour tous ses efforts, ses remarques utiles et son grand soutien pendant notre stage.

Nous tenons également à remercier notre professeur Boustia Nerhimane pour son soutien et sa patience tout au long de ce processus, ainsi que pour avoir pris le temps d'examiner et de fournir des commentaires importants sur les ébauches de la thèse.

Enfin, nous tenons à exprimer notre gratitude à nos amis, qui nous ont aidés directement et indirectement au cours de cette thèse.

Abstract

After realizing the importance of risk management, ICOSNET's security department offered us to carry out a risk analysis and management within their company. To illustrate how GRC (Governance, Risk and Compliance) could be applied to analyze risks and all the steps required to resolve additional threats.

To achieve that, we will use the EBIOS (Expression of Needs and Identification of Security Objective) risk management method, in order to assess and deal with the risks associated with ICOSNET servers. This method opts for a structured approach, allowing an exhaustive analysis through the identification of various sub-components or causes of risk.

The main objective of this study is to identify the main security vulnerabilities in the web servers in which we will use the EBIOS method. Then we apply the security measures resulting from our analysis to tighten security and increase its level.

Keywords: risk management, ICOSNET, risk analysis, Governance, Risk and Compliance, threats, EBIOS, identification, web servers, security measures, strengthen security.

Résumé

Après avoir réalisé l'importance de la gestion des risques, le département de sécurité d'ICOSNET nous a proposé de réaliser une analyse et une gestion des risques au sein de leur entreprise. D'illustrer comment la GRC (Gouvernance, risque et conformité) pourrait être appliquée pour analyser les risques et toutes les étapes nécessaires pour résoudre des menaces supplémentaires.

Pour y parvenir, nous utiliserons la méthode de gestion des risques EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité), afin d'évaluer et faire face aux risques associés aux serveurs ICOSNET. Cette méthode opte pour une approche structurée, permettant une analyse exhaustive par l'identification des diverses sous-composantes ou causes de risque.

L'objectif principal de cette étude est d'identifier les principales failles de sécurité dans les serveurs web à travers la méthode EBIOS. Ensuite, nous appliquons les mesures de sécurité résultant de notre analyse pour renforcer la sécurité et augmenter son niveau.

Mots clés : gestion des risques, ICOSNET, analyse des risques, GRC, menaces, EBIOS, l'identification, serveurs web, mesures de sécurité, renforcer la sécurité.

ملخص

بعد إدراك أهمية إدارة المخاطر، عرض علينا قسم الأمن في ICOSNET إجراء تحليل المخاطر داخل شركتهم. لتوضيح كيفية تطبيق الحكم الرشيد و إدارة المخاطر و الامتثال وجميع الخطوات المطلوبة لحل التهديدات الإضافية لشركتهم.

لتحقيق ذلك، سوف نستخدم طريقة EBIOS لإدارة المخاطر، من أجل تحديد و تقييم المخاطر المرتبطة بخوادم ICOSNET و التعامل معها. تختار هذه الطريقة نهجًا منظمًا، مما يسمح بإجراء تحليل شامل من خلال تحديد المكونات الفرعية المختلفة أو أسباب المخاطر.

الهدف الرئيسي من هذه الدراسة هو تحديد نقاط الضعف الأمنية الرئيسية في وخادم الويب التي سنستخدم فيها طريقة EBIOS. ثم نقوم بتطبيق الإجراءات الأمنية الناتجة عن تحليلنا لتشديد الأمن وزيادة مستواه.

الكلمات المفتاحية : إدارة المخاطر ، ICOSNET ، تحليل المخاطر ، الحكم الرشيد و ادارة المخاطر و الامتثال ، التهديدات ، EBIOS، تقييم المخاطر، خوادم الويب ، الإجراءات الأمنية ، تعزيز الأمن.

Sommaire

Liste d'abréviation

GRC : Governance, Risk and Compliance.

SSI : Sécurité des Systèmes d'Informations.

ISMS: Information Security Management System.

IRM: Institute of Risk Management.

FWM: Federal Wildland Fire Management: Policy and Program Review.

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

MEHARI : Méthode Harmonisée d'Analyse des Risques.

CLUSIF : Club de la Sécurité de l'Information Français.

EBIOS : Expression des Besoins et Identification des Objectifs de Sécurité.

DCSSI : Direction Centrale de la Sécurité des Systèmes d'Information.

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

ISO: International Organization for Standardization.

CEI: Commission Electro technique International.

XSS: cross-site scripting.

SQLi: Sql injection.

LAMP: Linux, Apache, MySQL and PHP.

HTTP: Hypertext Transfer Protocol.

SQL : Structured Query Language.

SGBD : Système de gestion de base de données.

CIS: Center for Internet Security.

URL: Uniform Ressource Locator.

OWASP: Open Web Application Security Project.

CRS: Core Rule Set.

PHP: Parser Hypertext Preprocessor.

Liste des figures

Liste des tables

Introduction générale

Aujourd'hui, les technologies de l'information sont utilisées comme base pour soutenir la stratégie commerciale de l'entreprise et améliorer la qualité des services et les processus commerciaux. La croissance exponentielle des nouvelles technologies augmente non seulement les interconnectivités, mais a également intégré Internet dans la vie quotidienne. La manière dont les entreprises sont menées aujourd'hui exige des interconnectivités et des interdépendances croissantes qui nécessitent l'utilisation d'Internet

Pendant son utilisation, la technologie de l'information entraînera des risques. Ce qui nécessite d'attirer l'attention sur la gestion des risques. La gestion des risques peut réduire le risque de processus commerciaux non optimaux, de pertes financières, de dégradation de la réputation de l'entreprise ou de destruction des activités de l'entreprise. Pour réduire les damages aux systèmes d'information du processus commercial de l'entreprise, une évaluation de la gestion des risques doit être effectuée.

Avec son importance croissante, la gouvernance a attiré l'attention ces dernières années des entreprises. Car, il s'agit d'un processus systématique d'identification, d'évaluation et de réponse aux événements susceptibles d'affecter leurs objectifs et répondre aux attentes des parties prenantes internes et externes.

Après avoir pris conscience de l'importance de la gestion des risques, le département de sécurité d'ICOSNET nous propose de réaliser une analyse et une gestion de risque au sein de leur société, d'illustrer comment la GRC (Gouvernance, risque et conformité) pourrait être appliquée afin d'analyser les risques et toutes les étapes nécessaires pour résoudre des menaces supplémentaires.

Dans notre cas d'étude, nous nous concentrerons sur le durcissement de la sécurité des serveurs chez ICOSNET. Il est demandé d'atteindre un niveau de durcissement plus mature.

L'aspect le plus critique du déploiement d'un serveur sécurisé est une planification minutieuse avant l'installation, la configuration et le déploiement. Une planification minutieuse garantira que le serveur est aussi sécurisé que possible et en conformité avec la politique de cybersécurité de l'entreprise. Il est essentiel de la définir au préalable et connaître les menaces à atténuer pour comprendre les raisons des diverses pratiques de sécurité de technique de base.

Pour cela, nous utiliserons la méthode de gestion des risques EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité), afin d'évaluer et traiter les risques associés aux serveurs ICOSNET. Cette méthode opte pour une approche structurée, permettant une analyse exhaustive à travers l'identification de diverses causes de risque. Ses 5 modules peuvent être appliqués de manière quelque peu indépendante, ce qui permet de (re) faire certaines parties de l'analyse.

L'objectif principal de cette étude est d'identifier les principales vulnérabilités de sécurité dans les serveurs web à travers la méthode EBIOS. Puis nous appliquons les mesures de sécurité issues de notre analyse pour durcir la sécurité et augmenter son niveau.

Afin d'illustrer la démarche de notre travail, nous présentons dans ce qui suit l'organigramme du mémoire qui se résume en ces chapitres :

- **Chapitre 1 : « Gestion de risque »** Dans ce chapitre, on va présenter la notion de gestion des risques.
- **Chapitre 2 : « Déploiement de la méthode EBIOS »** Dans ce chapitre, nous allons décrire en détails le déroulement de chaque étape de la méthode EBIOS et la déroulé.
- **Chapitre 3 : « Mise en œuvre des mesures de sécurité »** Dans ce chapitre, nous allons mettre en œuvre les mesures de sécurité décrie dans le chapitre précédent.

Chapitre 1 : Gestion des risques

1. Introduction

La gouvernance, risques et conformité communément appelé GRC (Gouvernance, risque et conformité) est un ensemble de processus et de procédures qui fait référence à une stratégie de gestion de la gouvernance globale d'une organisation, de la gestion des risques d'entreprise et de la conformité aux réglementations pour aider les organisations à atteindre leurs objectifs commerciaux, à faire face à l'incertitude et à agir avec intégrité [1].

GRC comprend trois composants principaux :

- **Gestion de la gouvernance** : S'assurer que les activités organisationnelles, comme la gestion des opérations informatiques, sont alignées de manière à soutenir les objectifs commerciaux de l'organisation.
- **Gestion des risques :** S'assurer que tout risque associé aux activités organisationnelles est identifié et traité d'une manière qui soutient les objectifs commerciaux de l'organisation. Dans le contexte informatique, cela signifie qu'il doit disposer d'un processus complet de gestion des risques informatiques qui s'intègre dans la fonction de gestion des risques d'une organisation.
- **Conformité :** Consiste à s'assurer que les processus internes actuels sont conformes aux règles internes et externes.

Toute entreprise, quelle que soit sa taille fait face à des risques qui peuvent être un obstacle pour sa réussite.

Dans notre projet on se concentre sur la partie de gestion des risques qui est une partie très importante pour toutes les entreprises pour pouvoir identifier, gérer et éviter les possibilités de défaillance.

Dans ce chapitre, on va présenter la notion de gestion des risques.

2. Définition du risque

Les définitions du risque peuvent être trouvées à partir de nombreuses sources, et les suivantes sont les plus citées.

1ere définition : Le sens littéral du mot est le suivant : « une chance ou une possibilité de danger, de perte, de blessure ou d'autres conséquences néfastes ». Dans

[1] Wikipedia contributors. (s. d.). Gouvernance, gestion des risques et conformité. Wikipedia. Consulté le 12 mars 2021, à l'adresse https://fr.wikipedia.org/wiki/Gouvernance,_gestion_des_risques_et_conformité

ce contexte, le risque est utilisé pour signifier des conséquences négatives. Cependant, prendre un risque peut également entraîner un résultat positif [2].

2eme définition : L'institut de gestion des Risques (IRM) a adopté une vision pratique des risques et les a définis comme la combinaison de la probabilité d'un événement et de ses conséquences. Les conséquences peuvent aller du positif au négatif [3].

3eme définition : Le guide international des définitions relatives aux risques (ISO 31000) a défini le risque comme « effet de l'incertitude sur les objectifs ». Un effet peut être positif, négatif ou un écart par rapport à l'attendu. De plus, le risque est souvent décrit par un événement, un changement de circonstances ou une conséquence[4].

Nous pouvons conclure de ces définitions, que le risque est mieux défini en se concentrant sur les risques en tant qu'événements. Autrement dit, pour qu'un risque se matérialise, un événement doit se produire.

3. Les types de risques

Le risque peut avoir des résultats positifs ou négatifs ou peut simplement entraîner une incertitude. Par conséquent, les risques peuvent être considérés comme liés à une opportunité ou à une perte ou à la présence d'incertitude pour une organisation.

Chaque risque a ses propres caractéristiques qui nécessitent une gestion ou une analyse particulière. Dans notre étude, les risques sont répartis en trois catégories selon la norme ISO 31000 : risques de danger (ou purs) ; risques de contrôle (ou d'incertitude) ; risques d'opportunité (ou spéculatifs) [5].

a. Risque de danger :

Les risques de danger sont les risques qui peuvent empêcher la réalisation de la mission de l'entreprise[5]. En règle générale, il s'agit de risques ou de périls de type assurable, y compris : les incendies, les tempêtes, les inondations, les blessures, etc.

Les opérations efficaces normales peuvent être perturbées par la perte, les dommages, les pannes, le vol et d'autres menaces associées à un large éventail de dépendances, comme celles-ci peuvent inclure (par exemple) :

- Humains : Manque de compétences ; Absence inattendue de personnel clé.

[2] Risk. (s. d.). Dans *Oxford English Dictionary*.
[3] IRM. (2002). A Risk Management Standard. https://www.theirm.org/media/4709/arms_2002_irm.pdf
[4] ISO Guide 73. (2009). Risk management – Vocabulary – Guidelines for use in standards, www.iso.org
[5] ISO. (2018). ISO 31000 : 2018 Management du risque. ISO/TC 262. https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:fr

- Locaux : Locaux inadéquats ou insuffisants ; Refus d'accès aux locaux ; dommages ou contamination des locaux.
- Les atouts : Dommages accidentels aux biens matériels ; panne de matériel ; vol ou perte de biens matériels.
- Fournisseur : Perturbation causée par une défaillance du fournisseur ; Livraison de marchandises défectueuse.
- IT : Panne des systèmes matériels informatiques ; Perturbation par un pirate informatique ou un virus informatique.
- Communication : Gestion inadéquate de l'information ; Panne ou perturbation du transport

En général, les organisations auront une tolérance à ces risques, ils doivent être gérés dans les niveaux de tolérance de l'organisation.

b. Risque de contrôle :

Les risques de contrôle sont des risques qui font douter de la capacité à réaliser la mission de l'organisation. Si les protocoles de contrôle sont supprimés, il n'y a aucun moyen d'être certain de ce qui va se passer [5].

Les risques de contrôle sont associés à l'incertitude, et les exemples incluent le potentiel de non-conformité légale et les pertes causées par la fraude. Ils dépendent généralement de la bonne gestion des personnes et de la mise en œuvre réussie des protocoles de contrôle. Bien que la plupart des organisations veillent à ce que les risques de contrôle soient gérés avec soin, ils peuvent néanmoins rester potentiellement importants.

c. Risque d'opportunité :

Lorsqu'une organisation prend délibérément des risques, en particulier des risques commerciaux, afin d'obtenir un rendement positif. Ceux-ci peuvent être considérés comme une opportunité ou un risque spéculatif [5].

Les risques d'opportunité sont délibérément voulus par l'organisation. Ces risques surviennent parce que l'organisation cherche à améliorer la réalisation de la mission.

De nombreuses organisations sont prêtes à investir dans des stratégies commerciales à haut risque en prévision d'un profit ou d'un rendement élevé. Souvent, la même organisation aura une approche opposée des risques de danger et aura une faible tolérance aux dangers.

4. Facteurs de risque

Les facteurs qui donnent lieu à des risques sont les catastrophes et les aléas. La classification peut être divisée en plusieurs types, à savoir les dangers physiques, moraux, et juridiques ou réglementaires. Alors que la classification des causes de risque peut être divisée en plusieurs types, à savoir le risque de bien physique, le risque employé et le risque juridique[6].

Les facteurs de risque peuvent également être classés comme contrôlables ou incontrôlables. Une bonne gestion des risques consiste à déterminer si l'organisation a pris ces facteurs en considération ou non.

5. Gestion des risques (GR)

> *"Une saine gestion des risques est à la base de toutes les activités de gestion. Les risques et incertitudes liés aux activités de gestion doivent être compris, analysés, communiqués et gérés en ce qui concerne le coût de faire ou de ne pas faire une activité." – Federal Wild land Fire Management : Policy and Program Review* [7].

La gestion des risques est un ensemble de processus et d'activités coordonnés qui identifient, surveillent, évaluent, hiérarchisent et contrôlent les risques auxquels une organisation est confrontée.

GR va au cœur de la façon dont une organisation lutte contre les problèmes d'incertitude et de complexité. Il s'agit d'identifier si et quels types de décisions doivent être prises, quand elles doivent être prises, comment elles doivent être prises et qui doit être impliqué.

Les outils et techniques de gestion des risques aideront à gérer les risques de danger, les risques de contrôle et les risques d'opportunité qui pourraient avoir une incidence sur ces dépendances clés.

6. Principes de base de la gestion des risques

La gestion des risques repose sur un ensemble de principes qui sont la base d'une approche réussie de la gestion des risques au sein de toute organisation.

---

[6] SRY Ahmad, "Analysis of User Acceptance of the Application of Information Systems Using the Technology Acceptance Model," Thesis, vol. 4, pp. 924–929, 2012.

[7] National Interagency Fire Center (NIFC). (2009, Février). *Guidance for Implementation of Federal Wildland Fire Management Policy*. https://www.nifc.gov

La liste suivante décrit ce que la gestion des risques devrait être en pratique. Elle comprend également des informations sur ce que la gestion des risques devrait faire ou fournir[8].

a. **Proportionnée :** Les activités de gestion des risques doivent être proportionnelles au niveau de risque auquel l'organisation est confrontée.
b. **Aligner :** Les activités de gestion des risques doivent être alignées sur les autres activités de l'organisation.
c. **Globale :** Pour être pleinement efficace, l'approche de gestion des risques doit être globale.
d. **Intégré :** Les activités de gestion des risques doivent être intégrées à l'organisation.
e. **Dynamique :** Les activités de gestion des risques doivent être dynamiques et adaptées aux risques émergents et changeants.

7. Processus de gestion des risques

La gestion des risques comporte trois étapes du processus, et ce sont : Identification, évaluation et appréciation des risques[9].

a. **Identification des risques :**

Cette phase peut également être appelée (collecte de données); elle ne demande pas beaucoup de main-d'œuvre en termes de bureau de sécurité, mais elle prend beaucoup de temps car l'activité repose principalement sur la collecte de données provenant de différentes parties de l'organisation.

L'intention est d'identifier, de documenter et de communiquer. Elle consiste à déterminer quels risques sont susceptibles d'affecter le projet et à documenter les caractéristiques de chacun. Il s'agit de porter à notre attention leurs facteurs de risque ou leurs événements.

b. **Analyse des risques :**

L'analyse des risques implique la prise en compte des causes et sources des risques, de leurs conséquences positives et négatives et de la probabilité que ces conséquences se produisent, en fonction du nombre de biens analysés et du temps de rotation pour la collecte auprès d'autres services.

[8] ISO. (2018). ISO 31000 : 2018 Management du risque. ISO/TC 262. https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:fr
[9] *Risk Management Plan*. (2015). https://www.phe.gov

Cette phase peut durer de quelques semaines à plusieurs mois. Le principal résultat de cette phase est une matrice contenant toutes les applications, les bases de données, les propriétaires des biens, les contacts techniques, la description des biens et les résultats du score de contrôle.

c. Estimation des risques :

Une fois que toutes les informations nécessaires ont été collectées, l'étape suivante consiste à démarrer les activités d'estimation des risques. Les principales activités de cette phase sont le calcul de l'impact et de la probabilité pour chaque menace. À l'aide de cette formule :

RISQUE = IMPACT x PROBABILITÉ

Par une simple multiplication des valeurs d'impact et de probabilité pour obtenir la valeur de risque final.

d. Évaluation des risques :

La première chose à faire est de donner un sens aux valeurs de risque. Sur la base des résultats de l'activité précédente, tout ce que nous avons vraiment, c'est un tas de chiffres. Le défi est de prendre ces chiffres et de les transformer en quelque chose qui est d'un format plus lisible par l'homme. Cela nous permet de catégoriser chaque risque en catégories de HAUT, MOYEN et FAIBLE.

En utilisant cette technique, il est facile de hiérarchiser les éléments à haut risque pour la correction. Cela ne signifie pas que seuls les éléments à haut risque doivent être corrigés. Le système utilise cette méthode de classification des risques comme une technique de priorisation et ce qui serait par la suite ciblé pour la correction sur la base de cette analyse. Certaines organisations peuvent traiter que des éléments à haut risque tandis que d'autres peuvent choisir de traiter tous les risques dans une certaine mesure.

e. Traitement des risques :

Une fois les risques identifiés et évalués, toutes les techniques de gestion du risque entrent dans une ou plusieurs de ces quatre grandes catégories :

- **Évitement :** L'évitement des risques consiste à éliminer complètement l'activité à risque.
- **Transfert :** Les stratégies de transfert de risque retournent ou partagent la responsabilité de l'exécution d'une activité à risque avec une autre partie.

- **Acceptation :** Une fois que toutes les réponses aux risques raisonnables et rentables ont été prises, une organisation se retrouve avec l'acceptation des risques.
- **Réduction :** Si l'utilisateur choisit de réduire le risque, le système propose une liste de mesures de sauvegarde et de contrôles à mettre en œuvre.

8. Les normes ISO/IEC

Les normes internationales IEC (International Electrotechnical Commission) [10] et ISO (International Organization for Standardization) [11]. Représentent un consensus mondial sur une solution à un problème particulier. Elles définissent des exigences, des spécifications, des lignes directrices ou des caractéristiques dont le respect systématique permet de garantir que des matériaux, produits, processus et services peuvent être utilisés en toute sécurité et sont aptes à l'emploi.

Dans cette section, nous aborderons les normes qui sont souvent cités dans les méthodes de gestion de risques.

a. ISO/IEC 27001

La norme ISO 27001 a été publiée en 2005 sous le titre « ISO / CEI 27001 - Technologies de l'information - Techniques de sécurité - Systèmes de management de la sécurité de l'information - Exigences »[12]. Elle s'adresse aux entreprises de tous secteurs et de toutes tailles.

Il s'agit de la principale norme internationale axée sur la sécurité de l'information, publiée par l'Organisation internationale de normalisation (ISO), en partenariat avec la Commission électrotechnique internationale (CEI). Les deux sont des organisations internationales de premier plan qui élaborent des normes internationales.

L'objectif d'ISO 27001 est de protéger la confidentialité, l'intégrité et la disponibilité des informations dans une entreprise. Cela se fait en découvrant quels problèmes potentiels pourraient survenir avec les informations, puis en définissant ce qui doit être fait pour éviter que de tels problèmes ne se produisent. Par conséquent, l'objectif principal d'ISO 27001 est la gestion des risques : savoir où se trouvent les

[10] Wikipedia contributors. (s. d.). International Organization for Standardization. Wikipedia. Consulté le 10 avril 2021, à l'adressehttps://en.wikipedia.org/wiki/International_Organization_for_Standardization
[11] Wikipedia contributors. (s. d.). International Electrotechnical Commission. Wikipédia. Consulté le 11 avril 2021, à l'adresse https://en.wikipedia.org/wiki/International_Electrotechnical_Commission
[12] International Organization for Standardization, I. S. O. (s. d.).*ISO/IEC 27001:2013*. ISO. https://www.iso.org

risques, puis les traiter systématiquement, à travers la mise en place de contrôles de sécurité.

Cette norme est utilisée dans le monde entier par les organisations, tant commerciales que gouvernementales, comme base pour la gestion de la politique de l'organisation et la mise en œuvre de la sécurité de l'information. Il est conçu pour être suffisamment flexible pour être utilisé par tous les types d'organisations afin de protéger leurs informations de manière systématique et rentable, grâce à l'adoption d'un système de gestion de la sécurité de l'information (SMSI).

b. ISO/IEC 27002

ISO 27002 est une norme internationalement reconnue conçue pour les organisations comme référence pour la mise en œuvre et la gestion des contrôles de sécurité de l'information. Elle fournit des recommandations de bonnes pratiques sur les contrôles de sécurité de l'information à l'usage des personnes chargées de lancer, de mettre en œuvre ou de maintenir les systèmes de gestion de la sécurité de l'information (ISMS) [13].

Cette norme est destinée à être utilisée avec l'ISO 27001, comme cadre pour montrer la conformité aux réglementations lorsque des exigences détaillées ne sont pas fournies.

Les avantages apportés par l'ISO 27002 sont principalement :

- L'établissement de principes généraux pour démarrer, mettre en œuvre, maintenir et améliorer la gestion de la sécurité de l'information dans une organisation;
- La sélection, la mise en œuvre et la gestion des contrôles;
- Une meilleure organisation avec des processus et des mécanismes bien conçus et gérés;
- Conformité à la législation et aux autres réglementations.

La principale différence entre ISO 27001 et ISO 27002, est que ISO 27001 inclut les contrôles de sécurité, tandis que ISO 27002 aborde le même contenu mais plus détaillé et ajoute un guide de mise en œuvre. Souvent, les organisations peuvent obtenir la certification pour ISO 27001 mais pas pour ISO 27002.

[13] International Organization for Standardization, I. S. O. (s. d.).*ISO/IEC 27002:2013*. ISO. https://www.iso.org

c. ISO/IEC 27005

La norme ISO 27005 est une norme internationale de sécurité de l'information a été publiée la première fois par l'Organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (CEI) le 4 juin 2008 en langue anglaise, puis en octobre 2009 en version française. Cette norme est liée à la gestion des risques et à la sécurité de l'information [14].

La norme internationale essentielle ISO 27005 est un processus structuré et systématique permet d'aider les organisations en leur donnant des conseils sur le pourquoi, le quoi et le comment de la gestion des risques de sécurité de l'information à l'appui de leurs objectifs de gouvernance. Permet de décrire comment mener une évaluation des risques de sécurité de l'information. Elle s'appuie sur les concepts généraux spécifiés dans les normes ISO/IEC 27000 et 27001.

1. **Le processus de gestion des risques ISO 27005 :**

L'ISO 27005 ne suis aucune structure de gestion des risques spécifique, elle implique un processus de gestion des risques d'information continu basé sur les phases suivantes (voir la figure 1) :

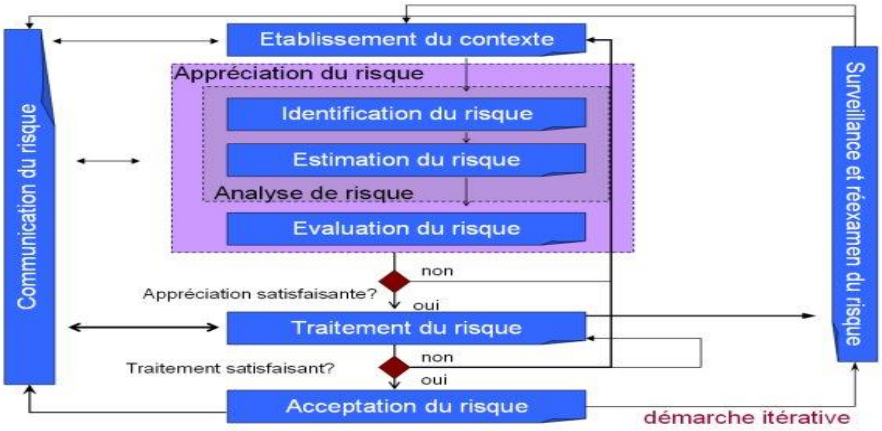


Figure 1 : La démarche de la norme ISO/IEC 27005 [15].

a. **Établissement des contextes** : Cette étape consiste à définir le périmètre d'étude et identifier les biens et les différents critères de base (critère d'impact, critère d'évaluation des risques et les

[14] International Organization for Standardization, I. S. O. (s. d.-c).*ISO/IEC 27005:2011*. ISO. https://www.iso.org

[15] ISO 27005 : gestion des risques pour la sécurité de l'information. (s. d.). Doritique. Consulté le 20 mars 2021, à l'adresse http://www.doritique.fr/Articles/View_Article.php?num_article=73

échelles d'estimation) dans le cadre d'analyse, pour réaliser une bonne analyse des risques.

b. **Identification des risques :** Cette phase permet d'apprécier les différents risques, menaces et vulnérabilités dans le périmètre avec leurs impacts sur le système. Permet aussi d'identifier les mesures de sécurité existantes.

c. **Estimation des risques :** Permet d'estimer le niveau de risque de chaque scénario identifié dans l'étape précédente dans l'entreprise.

d. **L'évaluation des risques :** Plusieurs entreprises choisissent de suivre un processus d'évaluation des risques basé sur les cinq étapes suivante :

   i. Compilation des biens informationnels.
   ii. Identifier les menaces et vulnérabilités applicables à chaque bien.
   iii. Attribuer des valeurs d'impact et de vraisemblance en fonction de critères de risque.
   iv. Évaluer chaque risque par rapport à des niveaux d'acceptabilité prédéterminés.
   v. Hiérarchiser les risques à traiter et dans quel ordre.

e. Traitement des risques: Cette partie consiste à traiter les risques en quatre manières :

   i. Réduire le risque.
   ii. Modifier le risque en appliquant des contrôles de sécurité.
   iii. Éviter le risque.
   iv. Transférer le risque.

f. **Acceptation des risques :** Les entreprises doivent déterminer leurs propres critères d'acceptation des risques en tenant compte

des politiques, des buts, des objectifs et des intérêts des actionnaires existants.

9. Méthode de gestion des risques

Dans cette partie nous allons présenter quelques méthodes de gestion des risques.

a. OCTAVE :

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) ce que signifie : *évaluation des menaces, les biens et des vulnérabilités critiques sur le plan opérationnel*, est une technique d'évaluation stratégique et de planification de la sécurité basée sur les risques[16]. Cette méthode est conforme aux exigences de la norme ISO 27001.

OCTAVE est ciblé sur les risques organisationnels et se concentre sur les questions stratégiques liées à la pratique. Il s'agit d'une évaluation flexible qui peut être adaptée à la plupart des organisations.

En utilisant l'approche OCTAVE, une organisation prend des décisions de protection des informations en fonction des risques pour la confidentialité, l'intégrité et la disponibilité des biens critiques liés aux informations. Tous les aspects du risque (biens, menaces, vulnérabilités et impact organisationnel) sont pris en compte dans la prise de décision, permettant à une organisation de faire correspondre une stratégie de protection basée sur la pratique à ses risques de sécurité.

b. MEHARI :

MEHARI est une démarche de gestion des risques française qui signifiée : Méthode Harmonisée d'Analyse des Risques. Développée en 1996 par CLUSIF (un club de la sécurité de l'information français), cette méthodologie est une moyenne efficace qui permet l'analyse, l'évaluation des risques, gérer et contrôler la sécurité de systèmes d'information, les différentes ressources informatiques pour tous les types d'organisations[17].

La démarche MEHARI est conforme aux exigences de la norme ISO / CEI 27005 - Norme de gestion des risques liés à la sécurité de l'information.

Les objectifs principaux de la méthodologie MEHARI sont:

[16]OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) - CIO Wiki. (s. d.). CIO WIKI. Consulté le 25 avril 2021, à l'adresse https://cio-wiki.org/wiki/OCTAVE_(Operationally_Critical_Threat,_Asset_and_Vulnerability_Evaluation

[17]*MEHARI 2010 Risk analysis and treatment Guide*. (2010, août). https://mehari.info

- Produire une méthode d'évaluation et de gestion des risques spécifiquement dans le domaine SSI.
- Fournir un ensemble d'outils et d'éléments nécessaires à sa mise en œuvre réussie.
- Permettre une analyse directe et individuelle des situations à risques décrites dans différents cas.
- Fournir un ensemble complet d'outils, en particulier pour la gestion de la sécurité à court, moyen et long terme, conforme à de nombreux niveaux de maturité et actions.

c. EBIOS :

EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) est une démarche française qui signifie : Expression des Besoins et Identification des Objectifs de Sécurité[18].

Cette méthode a été créée en 1995 par La Direction Centrale de la Sécurité des systèmes d'information (DCSSI) du Ministère de la Défense (France), devenue par la suite l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

EBIOS est la méthode d'appréciation et de traitement des risques numériques publiée par ANSSI avec le soutien du Club EBIOS. Permet d'identifier les mesures de sécurité à mettre en œuvre pour les maîtriser [19].

Méthodologie de gestion des risques liés à la sécurité des systèmes d'information qui permet aux entreprises de réaliser une appréciation et un traitement des risques. C'est une méthode qui est reconnue par les différentes administrations françaises, consiste à formaliser les besoins de sécurité et les menaces, et permet d'établir le contexte (périmètre d'étude), l'identification des risques, planifier et suivre le traitement des risques. Cette méthode conforme aux normes ISO/IEC 27001, ISO/IEC 27005.

La méthode EBIOS présente des bases de connaissances génériques pour l'appréciation des vulnérabilités et les risques associées, EBIOS supporte efficacement l'ensemble des actions, notamment la définition de la cible. Cette méthode permet aussi

[18] Agence nationale de la sécurité des systèmes d'information, A. N. S. S. I. (s. d.). EBIOS — Expression des Besoins et Identification des Objectifs de Sécurité. ANSSI. https://www.ssi.gouv.fr
[19] Agence nationale de la sécurité des systèmes d'information, A. N. S. S. I. (s. d.-b). *La méthode EBIOS Risk Manager – Le guide*. ANSSI. https://www.ssi.gouv.fr

de positionner la cible de l'étude vis-à-vis des partenaires de l'organisme et permet d'aboutir à la définition d'un plan de traitement des risques.

Les objectifs d'EBIOS définissent par l'ANSSI comme suit:

- Mettre en place ou renforcer un processus de management du risque numérique au sein d'une organisation.
- Apprécier et traiter les risques relatifs à un projet numérique, notamment dans l'objectif d'une homologation de sécurité.
- Définir le niveau de sécurité à atteindre pour un produit ou un service selon les cas d'usage envisagés et les risques à contrer, dans la perspective d'une certification ou d'un agrément par exemple.

d. Comparaison entre les méthodes :

Nous avons réalisé un tableau comparatif entre les trois méthodes étudiées (OCTAVE, MEHARI, EBIOS) pour mieux choisir la bonne méthode à utiliser dans notre étude, selon ces critères de choix :

- L'origine de la méthode.
- La langue de la méthode.
- La compatibilité avec les normes internationales.
- Facilité d'utilisation.
- La disponibilité de la documentation.
- La disponibilité de la base de connaissance.

Méthode	**Création**	**Origine**	**Langue**	**Compatibilité avec les normes**	**Complexité**	**Documentations**	**Base de connaissance**
EBIOS	1995	France	Français	ISO 31000, 27001, 27005	Faible	Méthodologie complète mise à disposition avec différentes études de cas réalisées afin d'aider à sa mise en place.	Disponible gratuitement.

MEHARI	1996	France	Français	ISO 27001, 27002, 27005	Medium	Méthodologie complète mise à disposition.	Disponible gratuitement.
OCTAVE	1999	États-Unis	Anglais	ISO 31010	Élevée	Méthodologie et documentation complètes disponibles gratuitement mais formation payante.	Disponible mais payante.

Table 1 : Tableau comparatif entre les méthodes de gestion des risques.

e. Choix de la méthode :

C'est à partir du tableau ci-dessus, que nous avons porté notre choix sur la démarche EBIOS pour les raisons suivantes :

- La métrisation de la langue de la méthode "Français".
- La disponibilité des documentations et base de connaissances complète sur la structure de la méthode EBIOS.
- La disponibilité de plusieurs études de cas sur la démarche de cette méthode, ce qui facilite la mise en place de la méthode sur notre périmètre d'étude.
- C'est une méthode claire et facile à concevoir et à appliquer. Chacun peut s'approprier la méthode et adapter son approche selon les sujets étudiés.

EBIOS s'applique à la fois aux systèmes de base (serveur Web) et aux systèmes complexes (système de gestion des ressources humaines interconnectant plusieurs éléments), ou sur des systèmes existants, pour compléter des systèmes d'information ou des sous-systèmes.

10. Conclusion :

Dans cette partie, nous avons pu décrire que le processus de gestion des risques est devenu une priorité absolue pour les entreprises. Son plan comprend de plus en plus des processus d'entreprise pour identifier et contrôler les menaces pesant sur ses biens numériques. C'est pourquoi être capable de comprendre et de contrôler les risques permet aux organisations d'être plus confiantes dans leurs décisions en minimisant les risques et les coûts supplémentaires avant qu'ils ne surviennent.

Nous avons pu comprendre le but des normes ISO les plus utilisées et explorer leurs avantages à suivre les règles de sécurité de l'information. Comme nous avons décrie en profondeur les méthodes de gestion de risque les plus utilisés.

A la fin du chapitre, nous avons pu choisir la méthode la plus adaptée à notre projet. Nous entrerons dans les détails de la suite dans le prochain chapitre.

Chapitre 2 : Déploiement de la démarche EBIOS

1. Introduction

Dans ce chapitre, nous allons décrire en détails le déroulement de chaque étape de la méthode EBIOS. Après nous allons consacrer une partie à la présentation de notre organisme d'accueil.

Ensuite, nous allons dérouler chaque étape de la méthode en profondeur.

2. La démarche EBIOS

Le déploiement de la méthode EBIOS a commencé par de multiples sessions et entretiens entre nous et l'équipe de sécurité d'ICOSNET, posant des questions liées aux éléments essentiels pour chaque critère de sécurité. Ensuite, le niveau de risque est défini de manière incrémentale. Tout d'abord, le potentiel d'attaque est défini, caractérisant un agent menaçant à l'aide d'une méthode d'attaque. Deuxièmement, l'opportunité des menaces est estimée, sur la base du niveau de vulnérabilité. Troisièmement, l'impact est défini, équivalent au maximum de besoins de sécurité suscités pour les actifs concernés par l'impact. Le niveau de risque est défini comme l'ensemble des trois métriques précédentes.

La méthode EBIOS se déroule selon 5 étapes présentant les activités à réaliser dans le cadre d'une étude des risques SSI, qui permet de repérer les évènements redoutés, d'estimer via une étude de risque, identifier les sources de risques qui exploiter les vulnérabilités pour réaliser une menace, et enfin de mettre en place des solutions techniques et organisationnelles permettant de remédier aux vulnérabilités qu'elle peut présenter [20].

Les 5 étapes (que nous allons étudier en détail) sont résumées et représentées ci-dessous (voir la figure 2) :

[20] ANSSI. (2018). EBIOS Risk Manager. SGDSN. https://www.ssi.gouv.fr/uploads/2018/10/guide-methode-ebios-risk-manager.pdf

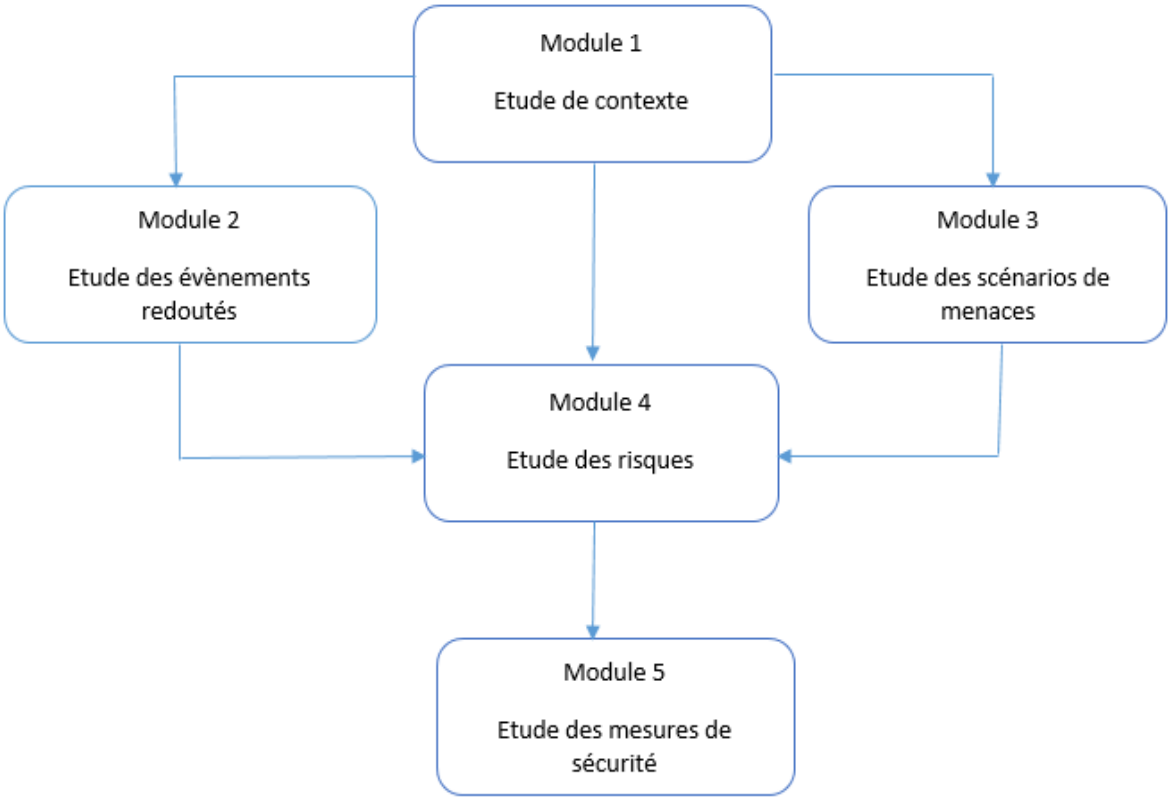


Figure 2 : Démarche générale de la méthode EBIOS.

i. Etude de contexte :

Cette étape consiste à formaliser et définir le cadre de gestion des risques dans lequel notre étude sera effectuée. Ce module permet d'avoir une vue globale sur le système cible pour repérer les informations générales, le contexte d'utilisation, déterminer les entités...etc.

Cette partie est très importante pour la réussite de la gestion des risques car cette réussite dépend de la maîtrise de la méthode avec une bonne connaissance de l'environnement étudié.

Ce module a pour objectif de :

- Identifier le périmètre de l'étude, le détail des équipements, des logiciels et de l'organisation humaine de l'entreprise.
- Identifier également les différentes métriques utilisées, ainsi les biens essentiels et les biens supports.
- Décrire les enjeux de périmètre, ses contraintes spécifiques, le contexte de son utilisation, les missions ou services qu'il doit rendre et les moyens utilisés.

- Collecter les informations et les éléments nécessaires à la gestion des risques pour les réaliser une bonne étude.

L'étape suivante se décompose en 3 activités :

- **Activité 1** : Définir le cadre de la gestion des risques.
- **Activité 2** : Préparer les métriques.
- **Activité 3** : Identifier les biens.

ii. Etude des événements redoutés :

L'étude des événements redoutés consiste à obtenir une liste explicite de tous les événements craints dans le périmètre d'étude pour mesurer leur gravité [20].

Ce module a pour objectif de :

- Repérer l'ensemble des événements redoutés dans le cadre d'étude.
- Décrire les différentes sources des menaces de chaque événement, ainsi que leur impact sur le périmètre d'étude.
- Déterminer les critères de sécurité des biens essentiels.
- Estimer le niveau de chaque événement redouté selon l'échelle de gravité.

L'étape suivante se décompose en une seule activité :

- **Activité 1** : Appréciation des événements redoutés.

iii. Etude des scénarios des menaces :

Cette étape permet de déterminer, estimer les différents scénarios de menaces sur le cadre d'étude [20].

Ce module a pour objectif de :

- Identifier les scénarios des menaces sur l'environnement d'étude.
- Décrire les différentes sources des menaces de chaque scénario, ainsi que leur impact sur le périmètre d'étude.
- Déterminer les critères de sécurité des biens essentiels.
- Estimer le niveau de chaque scénario de menace en utilisant l'échelle de vraisemblance.

L'étape suivante se décompose en une seule activité :

- **Activité 1** : Appréciation des scénarios des menaces.

iv. Etude des risques :

Maintenant que nous avons défini les événements redoutés et les différents scénarios des menaces on peut donc apprécier les risques qui passent sur le périmètre d'étude pour les évaluer et choisir la manière de les traiter [20].

Ce module a pour objectif de :

- Identifier les différents risques sur l'environnement d'étude.
- Évaluer les risques.
- Déterminer la manière de traiter ces risques.

L'étape suivante se décompose en 2 activités :

- **Activité 1** : Appréciation des risques.
- **Activité 2** : Identifier les objectifs de sécurité.

v. Etude des mesures de sécurité :

Cette dernière étape de la méthode consiste à déterminer les moyens de traiter les risques et en proposant les mesures de sécurité à mettre en œuvre [20].

Ce module se divise en 2 activités :

- **Activité 1** : Les mesures de sécurité à mettre en œuvre.
- **Activité 2** : Mettre en œuvre des mesures de sécurité.

3. Organisme d'accueil

Notre projet intitulé « **Mise en œuvre de la gestion des risques : durcissement du niveau de sécurité** » a été proposé par l'entreprise **ICOSNET.**

ICOSNET, est une entreprise de télécommunications présente sur le marché depuis 1999, et dotée d'une équipe pluridisciplinaire.

ICOSNET a su capitaliser une importante expérience et nouer des relations considérables avec les différents acteurs du secteur des TIC à l'échelle nationale et internationale[21].

Dans son optique d'anticipation de la convergence du marché actuel, et la forte croissance des besoins du marché pour se projeter dans l'informatique du futur, et déployer les architectures cloud computing de demain au sein de leurs activités. ICOSNET a lancé son nouveau DATA Center de dernière génération de classement TIER III, Bâtis sur une superficie de 200 m2 au niveau Centre des Affaires El Qods, 6éme niveau de la tour Centrale, 16002, Chéraga, Algérie.

[21]Présentation Icosnet. (s. d.). Icosnet. Consulté le 2 mars 2021, à l'adresse https://icosnet.com.dz/qui-sommes-nous/

ICOSNET se positionne comme un opérateur d'accès internet haut débit, de solutions de télécommunication convergentes et de solutions Cloud. ICOSNET s'impose aujourd'hui sur le marché de la convergence voix et données pour les PME/PMI et les grands comptes multinationaux installés en Algérie.

Une entreprise engagée responsable vis-à-vis de ses clients et employés, elle est considérée comme un opérateur multiservices et offre une large gamme de produits sur trois familles : Accès internet / communication unifiée (services de téléphonie IP) & services Cloud (Data center basé en Algérie).

À l'ère de la digitalisation, ICOSNET se positionne comme un partenaire de choix pour accompagner la transformation numérique des entreprises.

Aujourd'hui beaucoup d'entreprises algériennes et grands groupes internationaux, ont fait confiance à Icosnet [22].

a. Organigramme de l'entreprise

Voici l'organigramme de l'entreprise, notre stage s'est déroulé dans la division technique de l'entreprise.

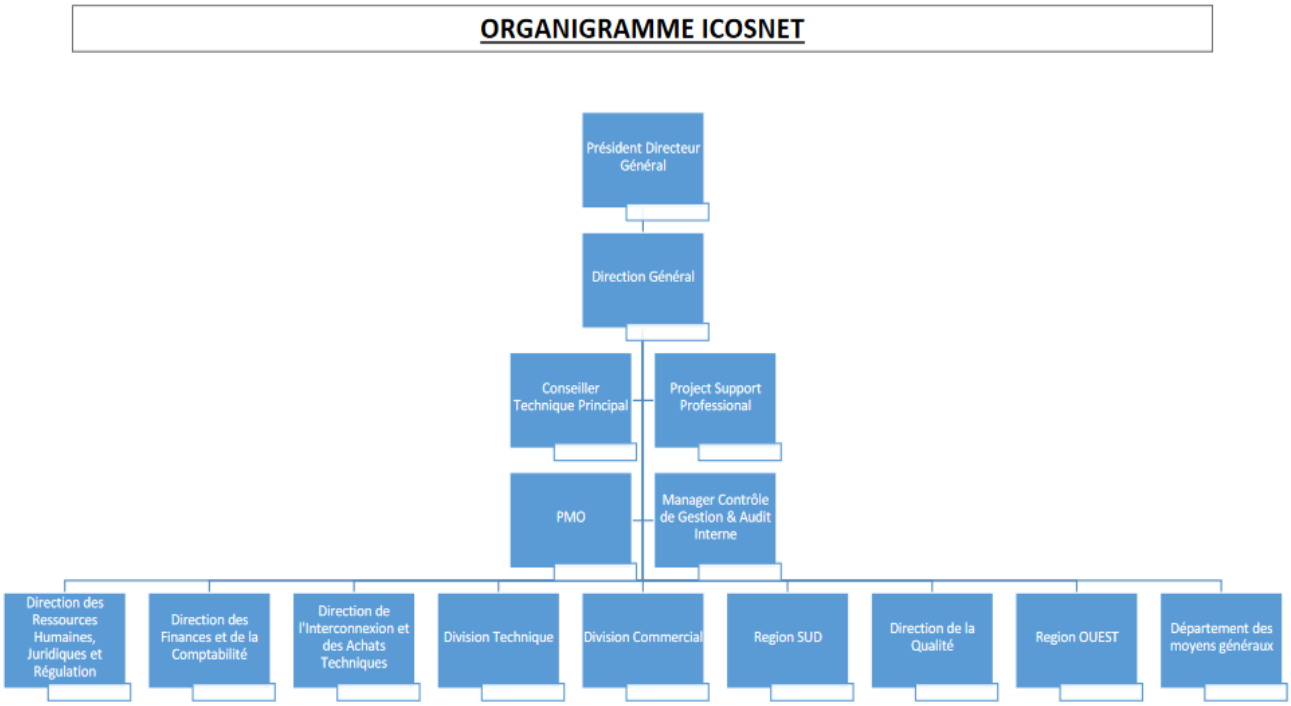


Figure 3 : Organigramme d'ICOSNET.

[22] *Accueil*. (s. d.). Icosnet. Consulté le 2 mars 2021, à l'adresse https://icosnet.com.dz/

4. Déploiement d'EBIOS

Le déploiement de la méthode EBIOS a commencé par de multiples sessions et entretiens entre nous et l'équipe de sécurité d'ICOSNET, posant des questions liées aux éléments essentiels pour chaque critère de sécurité. Ensuite, le niveau de risque est défini de manière incrémentale. Tout d'abord, le potentiel d'attaque est défini, caractérisant un agent menaçant à l'aide d'une méthode d'attaque. Deuxièmement, l'opportunité des menaces est estimée, sur la base du niveau de vulnérabilité. Troisièmement, l'impact est défini, équivalent au maximum de besoins de sécurité suscités pour les actifs concernés par l'impact. Le niveau de risque est défini comme l'ensemble des trois métriques précédentes.

a. Etude du contexte

Cette étape permet d'avoir une vision globale du système d'information cible. Elle définit le périmètre de l'étude, les détails de l'équipement, l'organisation logicielle et humaine de l'entreprise.

i. Définir le cadre de la gestion des risques

L'entreprise ICOSNET, est entre autres une société d'hébergement de serveurs web. Elle dispose d'une division technique qui s'en charge d'héberger le serveur Web du site web de l'entreprise, ainsi que les serveurs Web pour les applications Web de ses clients.

L'hébergement Web est un service de fourniture d'espace en ligne pour le stockage de pages Web. Et ces pages sont mises à la disposition du public via Internet. Chaque serveur est une machine virtuelle connecté à une DMZ, et est accessible via internet.

1. Eléments de contexte :

Pour héberger un serveur web, l'entreprise doit avoir à sa disposition une salle machine appropriée pour la centralisation de l'ensemble de ses machines et ses équipements et ses solutions informatiques. C'est que l'on appelle un Data Center (Centre de données). Chaque machine dispose d'une technologie préinstallée, appelée LAMP. (Linux, apache, maria dB, PHP/phpMyAdmin)

Ainsi, ICOSNET dispose d'un data center au sein de leur local, qui est gérée par la direction informatique.

Et en ce qui concerne les mesures de sécurité prises par la direction, il nous a donc été demandé d'analyser et d'étudier toutes les vulnérabilités possibles puis de trouver leur solution, pour les appliquer ultérieurement.

2. Source de menaces :

Dans cette partie nous allons déterminer les sources de menaces pertinentes vis-à-vis du contexte de périmètre de notre étude. Nous devons donc réfléchir aux origines des risques qui s'agit en effet des sources de menaces que l'on peut redouter, selon la conjoncture sociale, politique, économique, géographique, climatique, etc.

Dans notre cas, nous citons les sources de menaces suivantes :

Type de source de menace	Source
Source humaine interne, malveillante, avec de faibles capacités.	Employé/stagiaire peu sérieux, inconscient.
Source humaine interne, malveillante, avec des capacités illimitées.	Administrateur peu sérieux, maintenance informatique, partenaire, dirigeant, développeur.
Source humaine externe, malveillante, avec de faibles capacités.	Clients.
Source humaine externe, malveillante, avec des capacités illimitées.	Hacker, concurrent, ancien employé désirant se venger, espion, organisation criminel.
Source humaine interne, sans intention de nuire, avec de faibles capacités.	Employé/Stagiaire peu sérieux, peu motivé, maladroit, peu sensibilisé.
Source humaine interne, sans intention de nuire, avec des capacités importantes.	Administrateur peu sérieux, peu motivé.
Source humaine externe, sans intention de nuire, avec de faibles capacités.	Clients, journaliste, visiteur maladroit.
Source humaine externe, sans intention de nuire, avec des capacités importantes.	Fournisseur d’accès internet (ISP).

Sources non humaines.	Animale.
Virus non ciblé.	Malware, virus informatique.
Phénomène naturel.	Incendie, inondation ou infiltration d'eau
Catastrophe naturelle ou sanitaire.	Séisme, pandémie.

Table 2 : Identification des sources de menaces.

ii. Préparer les métriques

1. Les critères de sécurité :

Cette action consiste à choisir les critères de sécurité qui seront étudiés, à produire une définition pour chacun d'eux et à élaborer autant d'échelles de besoins que de critères de sécurité retenus.

Critères de sécurité	**Définition**
Disponibilité	Critère de sécurité où l'utilisateur n'a accès qu'au bien où celui-ci est autorisé.
Intégrité	Critère de sécurité garantissant l'intégrité du bien afin qu'il ne soit pas altéré par un tiers.
Confidentialité	Critère de sécurité qui va garantir la disponibilité d'un bien.

Table 3 : Tableau des critères de sécurité.

2. Échelle de gravité :

L'échelle utilisée pour estimer la gravité d'un événement redouté et des risques qui ont un impact sur la survie ou non de l'entreprise concernée.

Niveau de l'échelle	**Description des niveaux de gravité**
Négligeable	L'entreprise surmontera les impacts sans aucune difficulté.
Limité	L'entreprise surmontera les impacts avec quelques difficultés.

Important	L'entreprise surmontera l'impact avec de grosses difficultés.
Critique	L'entreprise ne surmontera pas les impacts.

Table 4 : Tableau des échelles de gravité.

3. Échelle de vraisemblance :

L'échelle utilisée pour estimer la vraisemblance d'un scénario de menace et des risques.

Niveaux de l'échelle	**Description des niveaux de vraisemblance**
Minime	Cela ne devrait pas se (re)produire.
Significative	Cela pourrait se (re)produire.
Forte	Cela devrait se (re)produire un jour ou l'autre.
Maximale	Cela va certainement se (re)produire prochainement.

Table 5 : Tableau des échelles de vraisemblance.

iii. Identifier les biens

Cette étape a pour but d'identifier les biens au sein du périmètre de l'étude et ainsi de mettre en évidence les éléments nécessaires aux autres activités.

1. Les biens essentiels :

Les biens essentiels représentent le patrimoine informationnel, ou les "biens immatériels", que l'on souhaite protéger.

- Toute information permettant d'identifier l'utilisateur est une information sensible. Ces informations comprennent :
  - Informations personnelles : numéros de sécurité sociale, adresse mail, numéros de permis de conduire et identifiants personnels similaires.
  - Informations financières : telles que les données d'aide financière, les numéros de compte bancaire, les numéros de carte de crédit et des informations similaires.

- Mots de passe : ID utilisateur, mots de passe et codes PIN.

- Informations relatives au contenu Web, telles que :
  - Version PHP.
  - Version serveur Web.
  - Code source.
  - Les pages d'erreurs.
  - Les informations de débogage.
- Toutes les informations auxquelles le serveur Web peut accéder, qui sont distribuées à tous les utilisateurs accédant au site Web public. Ces information peuvent inclure ces fichiers :
  - Fichiers de configuration.
  - Journaux du serveur et fichiers d'audit système.
  - Fichiers temporaires créés par l'application serveur Web.
  - Fichiers liés directement aux mécanismes de sécurité :
    - Fichiers de hachage de mot de passe.
    - Fichiers contenant des informations d'autorisation.

2. **Les biens support :**

Cette étape a pour but de prendre connaissance les composants du système d'information, qu'il s'agisse des biens techniques ou non techniques, supports aux biens essentiels précédemment identifiés.

- Le serveur Web.
- Matériels (Ordinateurs, routeurs, commutateur/switch, points d’accès, pare-feu...).
- Logiciels (Application, systèmes d’exploitation, base de données…).
- Contenus Web.
- Canaux informatiques et de téléphonie (Wifi, fibre optique, fibre MM, fibre, SM, cuivre...).

- Organisations (Fournisseur d'accès Internet, chefs de service, employés...).
- Supports papiers (Imprimantes, photocopieurs, scanneur...).
- Locaux (Salle machine/réseau, bureaux d'administrateurs).

3. **Les mesures existantes :**

Cette action consiste à recenser l'ensemble des mesures de sécurité existantes sur les biens supports. Mais concernant notre étude, il nous a été demandé de la mener "from scratch".

b. Etude des événements redoutés

Cette étape a pour objectif d'identifier et estimer de manière systématique les éléments constitutifs des risques, en d'autres termes « les événements redoutés » que l'on souhaite éviter concernant le périmètre de l'étude. Cette partie consiste à définir les différents événements redoutés sur le périmètre d'étude avec les sources de menace possibles, en situant les impacts potentiels auxquels est associé un niveau de gravité pour le système cible

i. Appréciation des événements redoutés

Cette activité est représentée sous forme d'un tableau (voir le tableau 6) qui répondre aux questions suivantes :

- Quels sont les événements craints sur le système cible avec leurs impacts sur l'organisme ?
- Quels seraient les plus graves par rapport à leurs critères de sécurité ?

Evénement redouté	Critères	Source de menaces	Impacts	Gravité
Indisponibilité de serveur.	Disponibilité.	- Administrateur peu sérieux. - Employé peu sérieux. - Concurrent. - Partenaire. - Hacker. - Catastrophe naturelle. - Pirate expert. - Développeur web peu sérieux. - Attaques informatiques. - Téléchargement des virus sur la machine de serveur. - Configuration Incorrect.	- Cela peut causer un préjudice grave au client et à la réputation de la société. - Perte de crédibilité. - Perte de confiance vis-à-vis des clients. - Interruption d'activités coûteuses. - Pert d'argent. - l'indisponibilité du site web hébergé. - Perte de données non enregistrées. - Perd des clients.	Critique.
Accès avec privilèges au serveur.	Confidentialité.	- Administrateur peu sérieux. - Concurrent. - Partenaire. - Hacker. - Faille dans le système. - Organisation criminelle. - Pirate. - Attaque informatique.	- Perte de confiance vis-à-vis des clients. - Perte de crédibilité. - Perdre le contrôle de serveur. - Perd des clients. - Fuite d'informations des utilisateurs.	Critique.

Evénement redouté	Critères	Source de menaces	Impacts	Gravité
Indisponibilité de bases de données reliées au serveur.	Disponibilité.	- Administrateur peu sérieux. - Employé peu sérieux. - Concurrent. - Partenaire. - Hacker. - Panne de serveur. - Développeur web peu sérieux. - Attaques informatiques.	- Perte de confiance vis-à-vis des clients. - Impossibilités d'assurer le traitement des sites. - Pert des données et informations personnelles à l'utilisateur. - Pert d'image de marque. - Incapacité à fournir les données demandées par l'utilisateur. - Perd des clients.	Critique.
Accès non autorisé à la base des données relié au serveur.	Confidentialité, Intégrité, Disponibilité.	- Administrateur peu sérieux. - Concurrent. - Partenaire. - Hacker. - Attaques informatiques. - Pirate.	- Perte de confiance vis-à-vis des clients. - Impossibilités d'assurer le traitement des sites. - Pert des données et informations personnelles à l'utilisateur. - Pert d'image de marque. - Bloquer les requêtes.	Critique.
Modification des paramètres réseau utilisés pour le serveur.	Confidentialité, Disponibilité.	- Hacker. - Concurrent. - Partenaire. - Organisation criminelle. - Pirate. - Administrateur peu sérieux. - Employé peu sérieux.	- Fuite d'informations des utilisateurs. - Perte de crédibilité. - Perte de confiance vis-à-vis des clients. -Pert d'image de marque.	Critique.

Evénement redouté	Critères	Source de menaces	Impacts	Gravité
Prise de contrôle de serveur à distance.	Disponibilité, Intégrité, Confidentialité.	- Pirate expert. - Hacker. - Concurrent. - Partenaire. - Organisation criminelle. - Administrateur peu sérieux.	- Risque pour le client et pour la réputation de la société. - Perte de confiance vis-à-vis des clients. - Perte de crédibilité. - Perturbation du fonctionnement interne de l'entreprise. - Interruption de service.	Critique.
Accès aux données sensibles et personnelles du client.	Confidentialité, Intégrité.	- Administrateur peu sérieux. - Employé peu sérieux. - Concurrent. - Partenaire. - Hacker. - Client. - Faille dans le système. - Les ports ouverts. - Attaques informatiques.	- Divulgation du secret de l'information et préjudice pour le client et la réputation de la société. - Perte financière. - Contraintes légales. - Perte de confiance vis-à-vis des clients. - Perte de crédibilité. - Interruption de service.	Critique.

Evénement redouté	Critères	Source de menaces	Impacts	Gravité
- Accès aux données sensibles et confidentielles de l'entreprise.	Confidentialité, Intégrité.	- Administrateur peu sérieux. - Employé peu sérieux. - Concurrent. - Partenaire. - Hacker. - Client. - Faille dans le système. - Les ports ouverts. - Attaques informatiques.	- Divulgation du secret de l'information et préjudice pour le client et la réputation de la société. - Perte financière. - Contraintes légales. - Perte de confiance vis-à-vis des clients. - Perte de crédibilité. - Interruption de service.	Critique.
-Interception des communications circulant dans le réseau privé de serveur.	Confidentialité, Disponibilité.	- Hacker. - Concurrent. - Client. - Pirate. - Administrateur peu sérieux. - Employé peu sérieux. - Attaques informatiques.	- Compromettre la confidentialité des données au niveau LAN. - Perte de crédibilité. - Divulgation du secret de l'information et préjudice pour le client et la réputation de la société.	Critique.

Evénement redouté	**Critères**	**Source de menaces**	**Impacts**	**Gravité**
-Interception et modification des données transitant sur le réseau privé.	Intégrité, Confidentialité.	- Administrateur peu sérieux. - Employé peu sérieux. - Concurrent. - Partenaire. - Hacker. - Faille dans le système.	- Compromettre L'intégrité des données au niveau de serveur de l'entreprise. - Risque pour le client et pour la réputation de la société. - Perte de confiance vis-à-vis des clients. - Perte de crédibilité.	Critique.
Divulgation d'informations.	Confidentialité.	- Administrateur peu sérieux. - Employé peu sérieux. - Concurrent. - Partenaire. - Hacker. - Faille dans le système. - Pirate. - Attaques informatiques.	- Compromettre confidentialité des données au niveau de serveur de l'entreprise. - Perte de confiance vis-à-vis des clients. - Perte de crédibilité. - Pert d'image de marque. - Perturbation du fonctionnement interne de l'entreprise. - Perte de propriété des données.	Critique.

Evénement redouté	Critères	Source de menaces	Impacts	Gravité
Interception de données de réseau WiFi.	Intégrité.	- Administrateur peu sérieux. - Employé peu sérieux. - Partenaire. - Hacker. - Faille dans le système.	- Compromettre l'intégrité des données au niveau LAN. - Écouter les transmissions des différents utilisateurs du réseau Wifi. - Perte de crédibilité.	Limité.
Intrusion d'une personne non autorisée dans le local de serveur.	Confidentialité.	- Visiteur - Client. - Concurrent. - Partenaire.	- Vol. - Mettre en panne le système. - Fuite d'informations.	Limité.
Accès non autorisés à la gestion des utilisateurs.	Disponibilité.	- Administrateur peu sérieux. - Employé peu sérieux. - Concurrent. - Partenaire. - Hacker. - Pirate expert. - Développeur web peu sérieux. -Attaques informatiques. -Téléchargement des virus sur la machine de serveur.	- Perte de confiance vis-à-vis des clients. - Perte de crédibilité. - Pert d'image de marque. - Impact pour l'utilisateur.	Important.

Evénement redouté	Critères	Source de menaces	Impacts	Gravité
Accès à distance sur une application.	Disponibilité, Intégrité, Confidentialité.	- Administrateur peu sérieux. - Employé peu sérieux. - Concurrent. - Partenaire. - Hacker. - Pirate expert. - Développeur web peu sérieux. - Attaques informatiques. - Téléchargement des virus sur la machine de serveur.	- Divulgation du secret de l'information et préjudice pour le client et la réputation de la société. - Perte de confiance vis-à-vis des clients. - Perte de crédibilité. - Interruption de service.	Critique.

Table 6 : Appréciation des événements redoutés

c. Etude des scénarios de menaces

Cette section consiste à identifier et à estimer en termes de vraisemblance les scénarios de menaces pour chaque critère de sécurité qui pesant sur le périmètre de l'étude, et qui peuvent générer des événements effrayants et donc créer des risques Pour ce faire, est étudié les menaces qui peuvent être générées par des sources de menaces et des vulnérabilités exploitables.

i. Appréciation des scénarios de menaces

Cette étape permet d'affiner l'ensemble de scénarios de menaces menée par les étapes précédentes. Cette activité est représentée sous forme d'un tableau (voir le tableau 7) qui répond aux questions suivantes :

- Quelles sont les sources des menaces pertinentes pour l'objet étudié ?
- Quels sont les scénarios de menaces possibles pour chaque critère de sécurité ? Et quels sont les plus vraisemblables ?

Scénarios de menaces	Critères	Source de menaces	Vraisemblance
Pannes matérielles.	Disponibilité.	- Administrateur peu sérieux. - Concurrent. - Partenaire. - Hacker. - Catastrophe naturelle. - Pirate expert. - Développeur web peu sérieux. - Attaques informatiques. - Organisation criminelle.	Significative
Pannes logicielles.	Disponibilité.	- Administrateur peu sérieux. - Concurrent. - Partenaire. - Hacker. - Catastrophe naturelle. - Pirate expert. - Développeur web peu sérieux. - Attaques informatiques. - Organisation criminelle.	Significative.
Accès physique non autorisé au support de stockage. (Espionnage des disques durs)	Disponibilité, Confidentialité.	- Administrateur peu sérieux. - Concurrent. - Partenaire. - Organisation criminelle. - Visiteur maladroit. - Employé maladroit. - Stagiaire.	Significative.

Scénarios de menaces	Critères	Source de menaces	Vraisemblance
Accès physique non autorisé au matériel.	Disponibilité, Confidentialité.	- Administrateur peu sérieux. - Concurrent. - Partenaire. - Organisation criminelle. - Visiteur maladroit. - Employé maladroit. - Stagiaire.	Significative.
Accès non autorisé aux données de session.	Confidentialité., Intégrité.	- Administrateur peu sérieux. - Employé peu sérieux. - Concurrent. - Partenaire. - Hacker. - Catastrophe naturelle. - Pirate expert. - Développeur web peu sérieux. - Attaques informatiques.	Forte.
Indisponibilité du service.	Disponibilité.	- Administrateur peu sérieux. - Employé peu sérieux. - Concurrent. - Partenaire. - Hacker. - Catastrophe naturelle. - Pirate expert. - Développeur web peu sérieux. - Attaques informatiques.	Significative.
Accessibilité de serveur via des ports non nécessaires pour le fonctionnement pour lequel est dédié.	Intégrité, Confidentialité.	- Administrateur peu sérieux. - Employé peu sérieux. - Développeur web peu sérieux.	Forte

Scénarios de menaces	Critères	Source de menaces	Vraisemblance
Mauvaise configuration.	Intégrité.	- Administrateur peu sérieux. - Employé peu sérieux. - Développeur web peu sérieux.	Forte.
Mauvais Hardening (durcissement du système).	Confidentialité, Intégrité, Disponibilité.	- Administrateur peu sérieux. - Employé peu sérieux. - Développeur web peu sérieux.	Significative.
Vol de données (Par manipulation de cookies).	Confidentialité.	- Administrateur peu sérieux. - Employé peu sérieux. - Développeur web peu sérieux.	Minime.
Exploitation des données personnelles ou morales.	Confidentialité, Intégrité.	- Administrateur peu sérieux. - Employé peu sérieux. - Concurrent. - Partenaire. - Hacker. - Catastrophe naturelle. - Pirate expert. - Développeur web peu sérieux. - Attaques informatiques.	Minime.

Scénarios de menaces	Critères	Source de menaces	Vraisemblance
Accès non autorisé aux machines des utilisateurs avec privilèges.	Confidentialité, Intégrité, Disponibilité.	- Administrateur peu sérieux. - Employé peu sérieux. - Concurrent. - Partenaire. - Hacker. - Catastrophe naturelle. - Pirate expert. - Développeur web peu sérieux. - Attaques informatiques. - Organisation criminelle.	Minime.
Dépassement des limites des bases de données.	Disponibilité.	- Administrateur peu sérieux. - Employé peu sérieux. - Développeur web peu sérieux. -Attaques informatiques.	Significative.
Accès non autorisé aux informations d'authentification d'utilisateurs.	Confidentialité, Intégrité, Disponibilité.	- Administrateur peu sérieux. - Employé peu sérieux. - Concurrent. - Partenaire. - Hacker. - Catastrophe naturelle. - Pirate expert. - Développeur web peu sérieux. - Attaques informatiques. - Organisation criminelle.	Significative.

Scénarios de menaces	Critères	Source de menaces	Vraisemblance
Téléchargement des virus et des logiciels malveillants.	Disponibilités, Intégrité, Confidentialité.	- Administrateur peu sérieux. - Employé peu sérieux. - Développeur web peu sérieux. - Stagiaire.	Forte.
Exploiter le réseau.	Disponibilités, Intégrité, Confidentialité.	- Administrateur peu sérieux. - Employé peu sérieux. - Concurrent. - Partenaire. - Hacker. - Faille dans le système.	Significative.
Détournement de l'usage prévu d'un matériel (matériel, papiers, et clés USB laissées sans surveillance, machine de serveur, absence de chiffrement, logiciel, utilisation de comptes génériques, et internet sur postes admin…)	Disponibilités, Intégrité, Confidentialité.	- Administrateur peu sérieux. - Employé peu sérieux. - Partenaire. - Stagiaire. - Client. -Développeur peu sérieux.	Significative.
Composants non appropriés aux conditions d'utilisation ou endommagé.	Disponibilités, Intégrité.	- Administrateur peu sérieux. - Employé peu sérieux. - Partenaire. - Stagiaire. - Client.	Minime.
Partage de mots de passe sans aucun mécanisme de sécurité.	Disponibilités, Intégrité, Confidentialité.	- Administrateur peu sérieux. - Employé peu sérieux. - Partenaire. - Stagiaire. - Client. -Développeur peu sérieux.	Minime.

Scénarios de menaces	Critères	Source de menaces	Vraisemblance
Stockages des données son sécurisation.	Intégrité, Confidentialité.	- Administrateur peu sérieux. - Employé peu sérieux. - Développeur peu sérieux.	Minime.
Modification des éléments (cartes, extensions…) via des connecteurs (ports, slots…). Piégeage d'un matériel (Keylogger…)	Disponibilités, Intégrité, Confidentialité.	- Administrateur peu sérieux. - Employé peu sérieux. - Partenaire. - Stagiaire. - Client.	Minime.
Observation des données interprétables (Observation d'un écran, géolocalisation d'un matériel à partir de son adresse IP, Interception de signaux, papiers…).	Confidentialité.	- Administrateur peu sérieux. - Employé peu sérieux. - Partenaire. - Stagiaire. - Concurrent. - Hacker.	Forte.
Modification, suppression ou disparition d'un logiciel.	Disponibilités, Intégrité, Confidentialité.	- Administrateur peu sérieux. - Employé peu sérieux. - Partenaire. - Stagiaire. - Concurrent. - Hacker.	Significative.
Saturation du canal internet.	Disponibilité.	- Administrateur peu sérieux. - Employé peu sérieux. - Partenaire. - Stagiaire. - Concurrent. - Hacker.	Minime.

Scénarios de menaces	Critères	Source de menaces	Vraisemblance
Accès distant par qui n'utilise aucun mécanisme de chiffrement lors du transport des données de la session.	Confidentialité, Intégrité.	- Administrateur peu sérieux. - Employé peu sérieux. - Partenaire. - Stagiaire. - Concurrent. - Hacker.	Minime.
Incendie ou catastrophe naturelle.	Disponibilités.	- Catastrophe naturelle.	Minime.

Table 7 : Appréciation des scénarios de menaces.

d. Etude de risques

Cette étape permet d'apprécier les risques pesant sur le serveur chez ICOSNET selon leur gravité et vraisemblance. Elle explique aussi comment traiter, estimer, évaluer les risques puis identifier les objectifs de sécurité à atteindre pour les traiter, puis identifier les risques résiduels.

i. Apprécier les risques

Cette partie a pour but d'établir la liste des risques à partir des événements redoutés et des scénarios de menaces précédemment appréciés. La gravité et la vraisemblance ont finalement été estimées (voir le tableau 8). Pour pouvoir compléter le tableau ci-dessous, on répond à la question suivante :

- Quelle est la cartographie des risques selon leur gravité et vraisemblance ?

Gravité	Risque	Vraisemblance
Critique.	- Attaque DDoS (écrasant la capacité d'entretien du web serveur et mettre le serveur indisponible pour les utilisateurs). - Détournement de serveur DNS (un attaquant modifie les configurations DNS pour accéder à des données sensibles). - Attaque par "phishing" où les attaquants montrent de faux sites Web pour voler des informations d'identification des utilisations. - Attaques de piratage de mot de passe de serveur Web. - Des attaques de ''malware'' menant à l'infiltration de logiciels malveillants dans l'infrastructure de l'entreprise. - Exécution d'un logiciel malveillant, qui prendrait le contrôle des droits d'administrateur de l'utilisateur. - Trafiquer le réseau privé d'entreprise. - Attaques de mauvaise configuration des logiciels et des serveurs. - Détournement de session (Le piratage de session / détournement de cookies est une exploitation de la session Web). - Les attaques XSS (Cross-Site Scripting c'est lorsqu'une victime visite une page Web ou une application Web qui exécute le code malveillant).	Maximale.
Critique.	- L'indisponibilité ou défiguration des sites web hébergés par le serveur d'entreprise. - Accès non autorisé aux privilégiés d'admin sur la base des données. - Les détails de connexion volés permettent aux pirates de se connecter et d'effectuer des actions dommageables. - Accès autorisé au système cible de l'utilisateur légitime. - Fuite d'information personnelles des clients et utilisateurs. - Compromettre le serveur Web via diverses attaques telles que le craquage de mot de passe, L'injection SQL basée sur des erreurs de l'administrateur, l'injection de commandes, etc. - Attaques internes par des employés. - Utilisation des logiciels non corrigés. - Prise de contrôle d'un serveur web ou serveur de base des données. - Vol de matériel. - Dommages financiers sur l'entreprise.	Forte.

Gravité	Risque	Vraisemblance
Importante.	- Interception des communications circulant dans le réseau. - Voler des informations sensibles telles que les identifiants de connexion, les détails de carte de crédit, etc. - Accès non autorisé à tout ce qui circule entre un ordinateur d'utilisateur et le web (Telnet). - Attaque d'ingénierie sociale qui vise à obtenir des informations sensibles et confidentielles telles que les noms d'utilisateur, les mots de passe, les numéros de carte de crédit...etc.	Maximale.
Importante.	- La perte de données sensibles par le biais d'employés mal informés sur l'utilisation et la sécurité de ces réseaux. - Interruption des activités qui peut être très coûteuse pour l'entreprise. - Divulgations d'informations sur l'entreprise. - La perte de service. - Accès au serveur de messagerie entre les employées ou serveur de bases de données.	Forte.
Importante.	- Suppression accidentelle des coquilles de sécurité réseau. - L'erreur humaine ou la négligence des administrateurs. - Abus des privilèges.	Significative.
Importante.	- Faille de connexions entre le serveur et la base de données.	Minime.
Limitée.	- Diffusion non autorisée d'informations. - Ouvrir des e-mails HTML malveillants. - Détournement de données.	Forte.

Table 8 : Appréciation des risques.

ii. Identifier les objectifs de sécurité

Cette action consiste à identifier les objectifs de sécurité, c'est-à-dire à choisir la manière dont on va devoir traiter les risques afin que le niveau de risque résiduel devienne acceptable. Cette action doit être réalisée en fonction des critères de gestion des risques retenus.

1. Objectifs de sécurité identifiés

Dans cette partie nous souhaitons essentiellement réduire les risques jugés comme critique, importante et limitée.

Le choix des options de traitement doit être fait au regard :

Options de traitement	Description
Éviter	Changer le contexte de telle sorte qu'on n'y soit plus exposé.
Réduire	Prendre des mesures de sécurité pour diminuer l'impact et/ou la vraisemblance.
Prendre	Assumer les conséquences sans prendre de mesure de sécurité supplémentaire.
Transférer	Partager les pertes occasionnées par un sinistre ou faire assumer la responsabilité à un(des) tiers.

Table 9 : Les options de traitement des risques.

Le tableau suivant répond à la question suivante :

- Comment choisit-on le traitement des risques ?

Les croix correspondent aux premiers choix, les croix entre parenthèses correspondent aux autres possibilités acceptées :

Risque	Évitement	Réduction	Prise	Transfert
- Attaque DDoS.	(X)	X	(X)	(X)
- Détournement de serveur DNS.	(X)	X	(X)	(X)
- Attaque par “phishing”.	(X)	X	(X)	(X)
- Attaques de piratage de mot de passe de serveur Web.		X	(X)	(X)
- Des attaques d’infiltration de logiciels malveillants dans l’infrastructure de l’entreprise.	(X)	X	(X)	(X)
- Exécution d'un logiciel ou code malveillant, qui prendrait le contrôle des droits d'administrateur de l'utilisateur.	(X)	X	(X)	(X)
- Trafiquer le réseau privé d’entreprise.		X	(X)	(X)
- Attaques de mauvaise configuration des logiciels et des serveurs.	(X)	X	(X)	(X)
- Détournement de session (une exploitation de la session Web).	(X)	X	(X)	(X)
- Les attaques XSS.	(X)	X	(X)	(X)

Risque	Évitement	Réduction	Prise	Transfert
- Attaque DDoS.	(X)	X	(X)	(X)
- Détournement de serveur DNS.	(X)	X	(X)	(X)
- L'indisponibilité ou défiguration des sites web hébergés par le serveur d'entreprise.		X	(X)	(X)
- Accès non autorisé aux privilèges d'admin sur la base des données.		X	(X)	(X)
- Vols des détails de connexion.		X	(X)	(X)
- Accès non autorisé au système cible de l'utilisateur légitime.		X	(X)	(X)
- Fuite d'informations personnelles des clients et utilisateurs.		X	(X)	(X)
- Compromettre le serveur Web.	(X)	X	(X)	(X)
- Attaques internes par des employés.	(X)	X	(X)	(X)
- Utilisation de logiciels non corrigés.	(X)	X	(X)	(X)
- Prise de contrôle sur le serveur de base de données.		X	(X)	(X)
- Vol de matériel.	(X)	X	(X)	(X)
- Dommages financiers sur l'entreprise.	(X)	(X)	X	(X)
- Interception des communications circulant dans le réseau local.		X	(X)	
- Vol des informations sensibles.		X	(X)	
- Accès non autorisé à tout ce qui circule entre un ordinateur d'utilisateur et le web (Telnet).		X	(X)	
- La perte de données sensibles par le biais d'employés mal informés sur l'utilisation et la sécurité de ces réseaux.		X	(X)	
- Attaque d'ingénierie sociale qui vise à obtenir des informations sensibles et confidentielles.	(X)	X	(X)	(X)
- Interruption des activités qui peut être très coûteuse pour l'entreprise.		X	(X)	

Risque	Évitement	Réduction	Prise	Transfert
- Attaque DDoS.	(X)	X	(X)	(X)
- Détournement de serveur DNS.	(X)	X	(X)	(X)
- Divulgations d'informations sur l'entreprise.		X	(X)	
- La perte de service.		X	(X)	
- Accès au serveur de messagerie entre les employées ou serveur de bases de données.	(X)	X	(X)	(X)
- Suppression accidentelle des coquilles de sécurité réseau.		X	(X)	(X)
- L'erreur humaine ou la négligence des administrateurs.		X	(X)	(X)
- Abus des privilèges.		X	(X)	(X)
- Faille de connexions entre le serveur et la base de données.	(X)	(X)	X	(X)
- Diffusion non autorisée d'informations.		(X)	X	
- Ouvrir des e-mails HTML malveillants.		X	(X)	
- Détournement de données.		(X)	X	

Table 10 : Objectifs de sécurité identifiés.

2. Risques résiduels identifiés

À l'issue de l'identification des objectifs de sécurité, cette étape mis en évidence les risques résiduels suivants :

Risque résiduels	Gravité	Vraisemblance
- Exécution d'un logiciel malveillant, qui prendrait le contrôle des droits d'administrateur de l'utilisateur.	Critique.	Maximale.
- Attaque DDoS (écrasant la capacité d'entretien du web serveur et mettre le serveur indisponible pour les utilisateurs).	Critique.	Maximale.

Risque résiduels	Gravité	Vraisemblance
- Détournement de serveur DNS (un attaquant modifie les configurations DNS pour accéder à des données sensibles).	Critique.	Maximale.
- Attaque par “phishing” où les attaquants montrent de faux sites Web pour voler des informations d'identification des utilisations.	Critique.	Maximale.
- Compromettre le serveur Web via diverses attaques telles que le craquage de mot de passe, L’injection SQL basée sur des erreurs de l'administrateur, l'injection de commandes, etc.	Critique.	Forte.
- Les attaques XSS (Cross-Site Scripting c’est lorsqu’une victime visite une page Web ou une application Web qui exécute le code malveillant).	Critique.	Maximale.
- Voler des informations sensibles telles que les identifiants de connexion, les détails de carte de crédit, etc.	Importante.	Maximale.
- Accès non autorisé à tout ce qui circule entre un ordinateur d’utilisateur et le web.	Importante.	Maximale.
- Détournement de données.	Limitée.	Forte.
- Interception des communications circulant dans le réseau.	Importante.	Maximale.
- La perte de données sensibles par le biais d’employés mal informés sur l’utilisation et la sécurité de ces réseaux.	Importante.	Forte.
- Suppression accidentelle des coquilles de sécurité réseau.	Importante.	Significative.
- L'erreur humaine ou la négligence des administrateurs.	Importante.	Minime.
- Diffusion non autorisée d’informations.	Limitée.	Forte.
- Faille de connexions entre le serveur et la base de données.	Importante.	Minime.

Table 11 : Les risques résiduels.

e. Etude des mesures de sécurité :

Cette dernière étape fournit des outils pour évaluer les risques identifiés dans l'étape 2 et analysés successivement dans l'étape 3 et, pour déterminer les moyens de les traiter, et décider d'accepter ou non les risques résiduels.

i. Les mesures de sécurité à mettre en œuvre

Cette étape a pour but de déterminer les mesures de sécurité adéquates pour atteindre les objectifs de sécurité identifiés.

Mesures de sécurité	**Bien supports concernés**
- Choisir le système d'exploitation approprié pour le serveur Web. - Corriger et mettre à niveau le système d'exploitation. - Supprimer ou désactiver les services et applications inutiles. - Configurer l'authentification des utilisateurs du système d'exploitation. - Configurer les contrôles d'accès sur les ressources. - Tester la sécurité du système d'exploitation. - Configuration, protection et analyse des fichiers journaux. - Utiliser des systèmes de détection d'intrusion (IDS) basés sur l'hôte et/ou des vérificateurs d'intégrité des fichiers pour détecter les intrusions et vérifier le contenu Web. - IDS basé sur l'hôte utilisé pour les serveurs Web qui fonctionnent principalement SSL / TLS.	- Système d'exploitation.
- Installation sécurisée du serveur Web: ● Installer le logiciel serveur sur un hôte dédié. ● Installer les services Internet minimaux requis. ● Supprimez tous les exemples de documents, scripts et code exécutable. ● Supprimer ou désactiver tous les services installés par l'application serveur Web mais non requis (par exemple, FTP).	- Serveur Web.

Mesures de sécurité	Bien supports concernés
- Corriger et mettre à niveau l'application serveur Web. - Configuration des contrôles d'accès au système d'exploitation de l'hôte du serveur Web. ● Définir une matrice complète d'accès au contenu Web qui identifie les dossiers et fichiers du répertoire de documents du serveur Web qui sont restreints et lesquels sont accessibles (et par qui). ● Utiliser l'authentification des utilisateurs, les signatures numériques et d'autres mécanismes cryptographiques, le cas échéant. - Configuration du répertoire de contenu Web sécurisé. ● Dédier un seul disque dur ou une seule partition logique au contenu Web et établir des sous-répertoires associés exclusivement pour les fichiers de contenu du serveur Web. - Installer un logiciel de vérification de l'intégrité des fichiers pour protéger les fichiers de configuration du serveur Web, les fichiers de mots de passe et le contenu Web. - Définir un répertoire unique pour tous les scripts ou programmes externes exécutés dans le cadre du contenu Web. - Configurer l'IDS pour surveiller le trafic réseau du trafic vers et depuis le serveur Web après le pare-feu. - Tester la sécurité de l'application serveur Web et du contenu Web. - Sauvegarde fréquente des informations critiques. - Configuration de SSL / TLS, Garantir que l'accès via le port TCP 80 est désactivé. - Configurer le pare-feu de tel sorte qu'il bloque tout le trafic entrant vers le serveur Web à l'exception des ports TCP 80 (HTTP) et / ou 443 (HTTPS utilisant SSL / TLS). - Configurer le pare-feu de tel sorte qu'il informe l'administrateur réseau ou Web de toute activité suspecte par un moyen approprié.	

Mesures de sécurité	Bien supports concernés
- Configurer le pare-feu de tel sorte qu'il bloque (en conjonction avec IDS) les adresses IP ou les sous-réseaux qui, selon l'IDS, attaquent le réseau organisationnel.	
- S'assurer qu'aucun fichier classifié ou donnée sensible n'est disponible sur ou via un serveur Web public. - Limiter les téléchargements aux répertoires qui ne sont pas lisibles par le serveur Web. - Utilisation de noms de chemin explicites (c.-à-d. Ne repose pas sur la variable de chemin). - Conserver une copie protégée et faisant autorité du contenu Web de l'organisation.	- Page Web.
- Remplacer le protocole "Telnet" par le protocole SSH afin d'assurer un accès distant sécurisé. - Le serveur Web doit être situé dans une zone démilitarisée ou sous-traité à une organisation qui protège correctement le pare-feu. - La DMZ ne doit pas être située sur la troisième (ou plus) interface du pare-feu. - Utilisation de commutateurs réseau sur le segment de réseau du serveur Web pour se protéger contre les écoutes "eavesdropping" clandestines du réseau. - Configuration des commutateurs réseau en mode haute sécurité pour vaincre l'usurpation d'identité et les attaques d'empoisonnement. - Configuration des commutateurs réseau pour envoyer tout le trafic sur le segment de réseau à l'hôte IDS (basé sur le réseau).	- LAN.
- Installer le système de gestion de base de données et le configurer en toute sécurité. - Créer et sécuriser des comptes utilisateurs dans la base de données.	- Serveur de base de données.

Mesures de sécurité	**Bien supports concernés**
- Développer des contrôles d'accès appropriés pour les comptes utilisateurs. ● Les utilisateurs doivent fournir au moins deux formes d'authentification. (un identifiant d'utilisateur et un mot de passe ainsi qu'une carte à puce, un badge, un jeton ou une forme quelconque de biométrie.) ● S'assurer que les données ou autres ressources ne sont accessibles que de manière autorisée, en utilisant la matrice de contrôle d'accès pour la base de données. ● Masquer les structures de données et les données elles-mêmes que l'utilisateur ne devrait pas voir à l'aide des vues. - Développer et appliquer des normes pour les programmes d'applications qui accèdent à la base de données. - Crypter les données sensibles - S'assurer que les connexions réseau aux données sont sécurisées. - Mettre en place des mécanismes d'audit appropriés pour la base de données - Protéger la base de données contre les intrus en identifiant et en se protégeant contre les menaces de sécurité. - Appliquer des mises à jour de sécurité si nécessaire.	
- Sensibilisation des employés vers la sécurité physique. - Mise en place de mesures de sécurité physique comme les zones d'entrée et les zones réglementées. - Barrières de sécurité pour restreindre le périmètre de l'organisation. - Les asphyxiants incendie peuvent être utilisés pour les zones sensibles au feu comme les salles de serveurs et les salles de sécurité.	- Matériels. - Canaux informatiques. - Supports papiers. - Locaux.
- Former et informer les employés des risques liés à l'usage du réseau LAN. - Réquisitionner un certain type de personnel (par exemple, administrateurs système et Web, webmestre, administrateurs réseau, responsables de la sécurité des systèmes d'information). - Compétences et formation requises. - Exigences individuelles (niveau d'effort requis pour des types de	- Organisations.

Mesures de sécurité	Bien supports concernés
personnel spécifiques) et collectives de main-d'œuvre (niveau d'effort global).	

Table 12 : Les mesures de sécurité à mettre en œuvre.

ii. Mettre en œuvre les mesures de sécurité

Cette étape consiste à savoir déterminer les traitements appropriés des risques, les planifier et suivre leur mise en œuvre. Les échelles à utiliser :

Difficulté	Terme
Faible.	Quotidien.
Faible.	Trimestre.
Moyenne.	Année.
Élevée.	3 ans.

Table 13 : L'échelle à utiliser pour la mise en œuvre des mesures de sécurité.

Le plan d'action trié par terme et par difficulté en précise le responsable, est établi comme suit :

Mesure de sécurité	Responsable	Difficulté	Terme
- Corriger et mettre à niveau le système d'exploitation.	Direction informatique.	Faible.	Quotidien.
- Supprimer ou désactiver les services et applications inutiles.	Direction informatique.	Faible.	Trimestre.
- Configurer l'authentification des utilisateurs du système d'exploitation.	Direction informatique.	Faible.	Trimestre.
- Configurer les contrôles d'accès sur les ressources.	Direction informatique.	Faible.	Trimestre.
- Tester la sécurité du système d'exploitation.	Direction informatique.	Faible.	Trimestre.
- Configuration, protection et analyse des fichiers journaux.	Direction informatique.	Faible.	Quotidien.

Mesure de sécurité	Responsable	Difficulté	Terme
- Utiliser des systèmes de détection d'intrusion (IDS) pour détecter les intrusions et vérifier le contenu Web.	Direction informatique.	Moyenne.	Quotidien.
- IDS basé sur l'hôte utilisé pour les serveurs Web qui fonctionnent principalement SSL / TLS.	Direction informatique.	Élevée.	Quotidien.
- Installer les services Internet minimaux requis.	Direction informatique.	Moyenne.	Trimestre.
- Supprimez tous les exemples de documents, scripts et code exécutable	Direction informatique.	Moyenne.	Trimestre.
- Supprimer ou désactiver tous les services installés par l'application serveur Web mais non requis (par exemple, FTP).	Direction informatique.	Moyenne.	Trimestre.
- Corriger et mettre à niveau l'application serveur Web.	Direction informatique.	Faible.	Quotidien.
- Configuration des contrôles d'accès au système d'exploitation de l'hôte du serveur Web.	Direction informatique.	Moyenne.	Trimestre.
- Configuration du répertoire de contenu Web sécurisé.	Direction informatique.	Faible.	Trimestre.
- Installer un logiciel de vérification de l'intégrité des fichiers pour protéger les fichiers de configuration du serveur Web, les fichiers de mots de passe et le contenu Web.	Direction informatique.	Faible.	Trimestre.
- Définir un répertoire unique pour tous les scripts ou programmes externes exécutés dans le cadre du contenu Web.	Direction informatique.	Faible.	Trimestre.

Mesure de sécurité	Responsable	Difficulté	Terme
- Configurer l'IDS pour surveiller le trafic réseau vers et depuis le serveur Web après le pare-feu.	Direction informatique.	Moyenne	Trimestre.
- Sauvegarde fréquente des informations critiques.	Direction informatique.	Faible.	Quotidien.
- Configuration de SSL / TLS, et garantir que l'accès via le port TCP 80 est désactivé.	Direction informatique.	Faible.	Quotidien.
- S'assurer que le pare-feu bloque tout le trafic entrant vers le serveur Web à l'exception des ports TCP 80 (HTTP) et / ou 443 (HTTPS utilisant SSL / TLS).	Direction informatique.	Faible.	Quotidien.
- Configurer le pare-feu de tel sorte qu'il bloque tout le trafic entrant vers le serveur Web à l'exception des ports TCP 80 (HTTP) et / ou 443 (HTTPS utilisant SSL / TLS).	Direction informatique.	Faible.	Quotidien.
- Configurer le pare-feu de tel sorte qu'il informe l'administrateur réseau ou Web de toute activité suspecte par un moyen approprié.	Direction informatique.	Faible.	Quotidien.
- Configurer le pare-feu de tel sorte qu'il bloque (en conjonction avec IDS) les adresses IP ou les sous-réseaux qui, selon l'IDS, attaquent le réseau organisationnel.	Direction informatique.	Faible.	Quotidien.
- S'assurer qu'aucun fichier classifié ou donnée sensible n'est disponible sur ou via un serveur Web public.	Direction informatique.	Faible.	Quotidien.
- Limiter les téléchargements aux répertoires qui ne sont pas lisibles par le serveur Web.	Direction informatique.	Faible.	Trimestre.

Mesure de sécurité	Responsable	Difficulté	Terme
- Utilisation de noms de chemin explicites (c.-à-d. Ne repose pas sur la variable de chemin).	Direction informatique.	Faible.	Trimestre.
- Conserver une copie protégée et faisant autorité du contenu Web de l'organisation.	Direction informatique.	Faible.	Trimestre.
- Remplacer le protocole "Telnet" par le protocole SSH afin d'assurer un accès distant sécurisé.	Direction informatique.	Faible.	Trimestre.
- Le serveur Web doit être situé dans une zone démilitarisée ou sous-traité à une organisation qui protège correctement le pare-feu.	Organisation.	Faible.	Trimestre.
- La DMZ ne doit pas être située sur la troisième (ou plus) interface du pare-feu.	Direction informatique.	Faible.	Trimestre.
- Utilisation de commutateurs réseau sur le segment de réseau du serveur Web pour se protéger contre les écoutes clandestines "eavesdropping" du réseau.	Direction informatique.	Faible.	Trimestre.
- Configuration des commutateurs réseau en mode haute sécurité pour vaincre l'usurpation d'identité et les attaques d'empoisonnement.	Direction informatique.	Faible.	Trimestre.
- Configuration des commutateurs réseau pour envoyer tout le trafic sur le segment de réseau à l'hôte IDS (basé sur le réseau).	Direction informatique.	Faible.	Trimestre.

Mesure de sécurité	Responsable	Difficulté	Terme
- S'assurer que les données ou autres ressources ne sont accessibles que de manière autorisée, en utilisant la matrice de contrôle d'accès pour la base de données.	Direction informatique.	Faible.	Quotidien.
- Créer et sécuriser des comptes utilisateurs dans la base de données.	Direction informatique.	Faible.	Trimestre.
- Installer le système de gestion de base de données et le configurer en toute sécurité.	Direction informatique.	Moyenne.	Trimestre.
- Développer des contrôles d'accès appropriés pour les comptes utilisateurs.	Direction informatique.	Moyenne.	Trimestre.
- Masquer la structure de données et les données elles-mêmes que l'utilisateur ne devrait pas voir à l'aide des vues.	Direction informatique.	Moyenne.	Trimestre.
- S'assurer que les connexions réseau aux données sont sécurisées.	Direction informatique.	Faible.	Quotidien.
- Mettre en place des mécanismes d'audit appropriés pour la base de données.	Direction informatique.	Moyenne.	Trimestre.
- Protéger la base de données contre les intrus en identifiant et en se protégeant contre les menaces de sécurité.	Direction informatique.	Faible.	Quotidien.
- Appliquer des mises à jour de sécurité si nécessaire.	Direction informatique.	Faible.	Quotidien.
- Mise en place de mesures de sécurité physique.	Organisation.	Moyenne.	Année.
- Sensibilisation des employés vers la sécurité physique.	Organisation.	Moyenne.	Année.
- Former et informer les employés des risques liés à l’usage du réseau LAN.	Organisation.	Élevé.	3 ans.

Mesure de sécurité	Responsable	Difficulté	Terme
- Réquisitionner un certain type de personnel (par exemple, administrateurs système et Web, webmestre, administrateurs réseau, responsables de la sécurité des systèmes d'information).	Organisation.	Moyenne.	Année.
- Compétences et formation requises.	Organisation.	Moyenne.	Année.
- Exigences individuelles et collectives de main-d'œuvre.	Organisation.	Faible.	Quotidien.

Table 14 : Le plan d'action trié par terme et difficultés.

5. Conclusion

Dans ce chapitre, notre étude est entrée dans une couverture exhaustive avec la détermination de concepts, d'objectifs et d'exigences de sécurité. Elle a pris en compte toutes les entités techniques et non techniques. Dans la première étape de la méthode, nous avons traité l'analyse du contexte en termes de décomposition pertinente. Nous avons ensuite mené à la fois une analyse des besoins de sécurité et une analyse des menaces dans leur nature conflictuelle aux étapes 2 et 3. Enfin, aux étapes 4 et 5, nous avons diagnostiqué les risques et indiqué les mesures pour les couvrir et rendu explicites et connus les risques résiduels.

Chapitre 3 : Mise en œuvre des mesures de sécurité

1. Introduction

Dans ce chapitre nous allons passer en revue toutes les mesures de sécurité résultant de notre analyse antérieure, et nous allons sécuriser les entités internes et externes du système d'exploitation et du serveur d'ICOSNET. Ces mesures consistent à augmenter le niveau de sécurité et le durcir.

2. Installation sécurisée de LAMP

Icosnet nous a donné une machine virtuelle avec un système d'exploitation préinstallé appelé CentOS, et ils nous ont demandé de mettre en place le pack LAMP comme environnement de travail.

LAMP est un ensemble de logiciels open source pour héberger des sites Web et des applications Web. LAMP est un acronyme et il se compose du système d'exploitation Linux, du serveur HTTP Apache, du système de gestion de base de données relationnelle MySQL et du langage de programmation PHP.

Nous commençons ce chapitre, par l'installation de LAMP en toute sécurité et appliquerons toutes les configurations nécessaires.

a. Composants de LAMP

i. Linux :

Un système d'exploitation de type Unix ordinateur assemblé sous le modèle de développement et de distribution des logiciels libres et gratuits.

ii. Apache :

Apache est le serveur Web résident. Comme Linux, il est open-source. Apache traite les demandes, puis pousse les ressources Web via HTTP vers le domaine public.

Apache gère un grand pourcentage de sites Web sur Internet. L'une des raisons est le nombre de fonctionnalités qu'il offre. Ceux-ci peuvent aller de la prise en charge du langage de programmation côté serveur aux schémas d'authentification.

iii. MySQL :

MySQL est un système de gestion de base de données (SGBD) multithread et multi-utilisateurs SQL, c'est la base de données de la pile LAMP. C'est un système de gestion de base de données relationnelle qui est principalement utilisé pour stocker des données d'application.

MariaDB est un fork de MySQL développé par la communauté, dirigé par ses développeurs d'origine. Il s'agit d'une base de données open source d'entreprise pour le traitement transactionnel, analytique ou hybride transactionnel/analytique à grande échelle. En préservant les données historiques et en optimisant les analyses en temps réel tout en continuant à traiter les transactions, MariaDB Platform offre aux entreprises les moyens de créer des avantages concurrentiels et de monétiser les données.

iv. PHP :

Un langage de script côté serveur conçu pour le développement Web, mais également utilisé comme langage de programmation à usage général. PHP est préféré en raison de son efficacité. Les commandes PHP peuvent éventuellement être intégrées directement dans un document source HTML plutôt que d'appeler un fichier externe pour traiter les données.[23]

b. Les Avantages de LAMP

Le moyen le plus efficace de développer une application Web simple à complexe au niveau de l'entreprise consiste à utiliser un LAMP car il contient des fonctionnalités de personnalisation, de flexibilité et de sécurité puissantes et rentables.

Tous les composants de la pile LAMP sont des logiciels open source facilement disponibles en version gratuite.

Possibilités de développer et déployer des projets basés sur LAMP sans payer de frais de licence pour la distribution du logiciel

[23]Wikipedia contributors. (s. d.). PHP.Wikipedia.Consulté le 12 mai 2021, à l'adresse https://en.wikipedia.org/wiki/PHP

L'utilisation de PHP et MySQL facilite la correction rapide des erreurs et effectue des modifications car les utilisateurs ont un accès complet à la source.

c. Sécuriser LAMP sur CentOS

i. Linux :

Pour commencer, nous avons installé la distribution linux CentOS, pour sa sécurité et sa standardisation car elle facilite le dépannage et la maintenance.

Il est dédié à l'hébergement des serveurs car il permet d'économiser de l'argent, d'obtenir des performances et des caractéristiques de sécurité plus élevées. Il est également sécurisé et rapide car Centos n'exécute que les versions les plus basiques et les plus stables des programmes logiciels, ce qui réduit le risque de plantage du système.

Nous avons seulement besoin de le tenir à jour à tout moment. Nous devons nous assurer de configurer notre système pour installer automatiquement non seulement les mises à jour de sécurité, mais également les mises à jour des packages.

Pour activer les mises à jour automatiques, nous devons installer le package **DNF-automatic RPM** en exécutant cette commande :

dnf install dnf-automatic

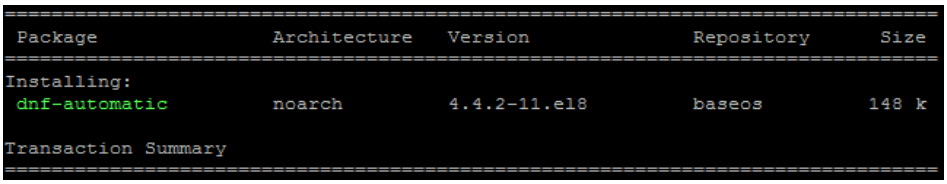


Figure 4 : Installation du dnf-automatic.

La prochaine étape consiste à configurer les mises à jour dnf-automatic. Le fichier de configuration se trouve dans */etc/dnf/automatic.conf*. Nous devons ouvrir le fichier et définir les valeurs requises pour répondre à nos exigences logicielles.

vim /etc/dnf/automatic.conf

Nous pouvons ensuite configurer dnf-automatic pour télécharger les nouvelles mises à jour et nous alerter via motd ("message du jour") en activant la fonctionnalité apply_updates dans le fichier de configuration et en envoyant emit_via à motd.

```
# Whether updates should be downloaded when they are available, by
# dnf-automatic.timer. notifyonly.timer, download.timer and
# install.timer override this setting.
download_updates = yes

# Whether updates should be applied when they are available, by
# dnf-automatic.timer. notifyonly.timer, download.timer and
# install.timer override this setting.
apply_updates = yes


[emitters]
# Name to use for this system in messages that are emitted.  Default
# hostname.
 system_name = frontend.selfcare.icosnet.com

# How to send messages.  Valid options are stdio, email and motd.  I
# emit_via includes stdio, messages will be sent to stdout; this is
# to have cron send the messages.  If emit_via includes email, this
# program will send email itself according to the configured options
# If emit_via includes motd, /etc/motd file will have the messages.
emit_via = motd
```

Figure 5 : Configuration du dnf-automatic.

Enfin, nous pouvons maintenant exécuter dnf-automatic, en activant une minuterie système (system timer) pour planifier les mises à jour automatiques DNF pour notre machine CentOS 8.

systemctl enable --now dnf-automatic.times

```
[root@frontend icosnet]# systemctl enable --now dnf-automatic.timer
Created symlink /etc/systemd/system/timers.target.wants/dnf-automatic.timer → /u
sr/lib/systemd/system/dnf-automatic.timer.
```

Figure 6 : Exécution du dnf-automatic.

La prochaine étape que nous devons faire est de vérifier les différents services avec les minuteries que nous avons sur notre système.

```
[root@frontend icosnet]# systemctl list-timers *dnf-*
NEXT                         LEFT     LAST PASSED UNIT                ACTIVATES
Thu 2021-06-17 06:46:19 CET  10h left n/a  n/a    dnf-automatic.timer dnf-autom>
n/a                          n/a      n/a  n/a    dnf-makecache.timer dnf-makec>
```

Figure 7 : Vérification des différents services.

ii. Apache :

Apache est disponible dans les référentiels logiciels par défaut de CentOS, ce qui signifie que vous pouvez l'installer avec le gestionnaire de packages **dnf**.

sudo dnf install httpd

Une fois installé, nous pouvons maintenant vérifier la version d'Apache en exécutant la commande **rpm**. Elle imprime un tableau d'informations telles que la version, la date de sortie, la version et l'architecture du package.

rpm -qi httpd

```
[root@frontend icosnet]# rpm -qi httpd
Name        : httpd
Version     : 2.4.37
Release     : 39.module_el8.4.0+778+c970deab
Architecture: x86_64
Install Date: Wed 09 Jun 2021 10:17:57 PM CET
Group       : System Environment/Daemons
Size        : 4488436
License     : ASL 2.0
Signature   : RSA/SHA256, Thu 20 May 2021 03:28:12 PM CET, Key ID 05b555b38483c65d
Source RPM  : httpd-2.4.37-39.module_el8.4.0+778+c970deab.src.rpm
Build Date  : Thu 20 May 2021 05:34:04 AM CET
Build Host  : x86-01.mbox.centos.org
Relocations : (not relocatable)
Packager    : CentOS Buildsys <bugs@centos.org>
Vendor      : CentOS
URL         : https://httpd.apache.org/
Summary     : Apache HTTP Server
Description :
The Apache HTTP Server is a powerful, efficient, and extensible
web server.
```

Figure 8 : Les informations d'Apache.

Maintenant que tout est défini, nous pouvons démarrer le service Web Apache HTTP, en exécutant la commande systemctl suivante :

sudo systemctl start httpd

Et pour permettre à Apache de démarrer automatiquement au démarrage du système, nous utilisons cette commande :

sudo systemctl enable httpd

Pour confirmer si le service est en cours d'exécution, nous exécutons uniquement :

sudo systemctl status httpd

À partir du résultat de la commande, le statut « active » en vert indique que le serveur Web Apache est opérationnel.

```
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor prese>
  Drop-In: /usr/lib/systemd/system/httpd.service.d
           └─php-fpm.conf
   Active: active (running) since Thu 2021-06-17 15:50:17 CET; 1h 10min ago
     Docs: man:httpd.service(8)
 Main PID: 1205 (httpd)
   Status: "Running, listening on: port 80"
    Tasks: 213 (limit: 2587)
   Memory: 15.5M
   CGroup: /system.slice/httpd.service
```

Figure 9 : Le statut d'Apache.

iii. MySQL :

Nous pouvons installer MariaDB Server juste à partir de cette ligne de commande :

sudo yum install mariadb-server

Une fois l'installation terminée, nous démarrons le service systemd pour MariaDB Server en utilisant systemctl, de la même manière que le serveur Apache :

sudo systemctl start mariadb.service

sudo systemctl enable mariadb.service

Pour confirmer si le service est en cours d'exécution, nous exécutons uniquement :

sudo systemctl status mariadb.service

```
● mariadb.service - MariaDB 10.3 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; enabled; vendor pre>
   Active: active (running) since Thu 2021-06-17 15:50:18 CET; 1h 22min ago
     Docs: man:mysqld(8)
           https://mariadb.com/kb/en/library/systemd/
 Main PID: 1345 (mysqld)
   Status: "Taking your SQL requests now..."
    Tasks: 30 (limit: 2587)
   Memory: 12.1M
   CGroup: /system.slice/mariadb.service
           └─1345 /usr/libexec/mysqld --basedir=/usr
```

Figure 10 : Le statut de MariaDB.

Pour terminer l'installation, nous avons des pratiques de sécurité spécifiques que nous devons toujours suivre. Voici les étapes à suivre pour aider à renforcer le serveur MariaDB :

sudo mysql_secure_installation

Cette commande nous permet d'améliorer la sécurité de notre installation MySQL de la manière suivante :

1. Définir un mot de passe pour les comptes root. (dans notre cas, nous avons déjà défini le mot de passe et nous ne voulons pas le changer).

```
Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password ensures that nobody can log into the MariaDB
root user without the proper authorisation.

You already have a root password set, so you can safely answer 'n'.

Change the root password? [Y/n] n
 ... skipping.
```

Figure 11 : Définition d'un mot root.

2. Supprimer les comptes root accessibles depuis l'extérieur de l'hôte local.

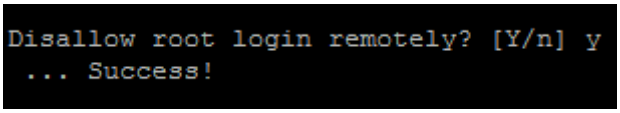


Figure 12 : Suppression des comptes root.

3. Supprimer les comptes d'utilisateurs anonymes.

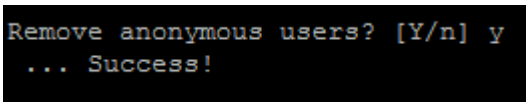


Figure 13 : Suppression des comptes anonymes.

4. Supprimer la base de données de test (à laquelle tous les utilisateurs peuvent accéder par défaut, même les utilisateurs anonymes) et les privilèges qui permettent à quiconque d'accéder aux bases de données dont les noms commencent par test.

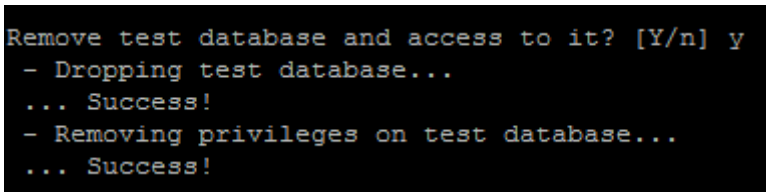


Figure 14 : Suppression de la base de données « test ».

iv. PHP :

Le dernier composant de LAMP que nous devons installer est PHP. Nous allons installer la dernière version de PHP en utilisant le référentiel Remi.

1. Tout d'abord, nous installons le référentiel EPEL qui permet d'accéder facilement aux packages d'installation des logiciels couramment utilisés.

sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm

2. Ensuite, nous installons yum-utils et activons remi-repository à l'aide de la commande ci-dessous.

sudo dnf install dnf-utils http://rpms.remirepo.net/enterprise/remi-release-8.rpm

3. Après l'installation réussie de yum-utils et Remi-packages, nous recherchons les modules PHP disponibles en téléchargement en exécutant cette commande :

sudo dnf module list php

4. Ensuite, nous activons le module PHP 7.4 en exécutant :

sudo dnf module enable php:remi-7.4

5. Et enfin, nous installons la dernière version à l'aide de cette commande :

sudo dnf module install php 7.4

6. Une fois que nous avons complètement installé PHP 7.4, nous devons démarrer et activer PHP-FPM au démarrage.

sudo systemctl start php-fpm

sudo systemctl enable php-fpm

7. Pour vérifier son statut, nous exécutons la commande :

sudo systemctl status php-fpm

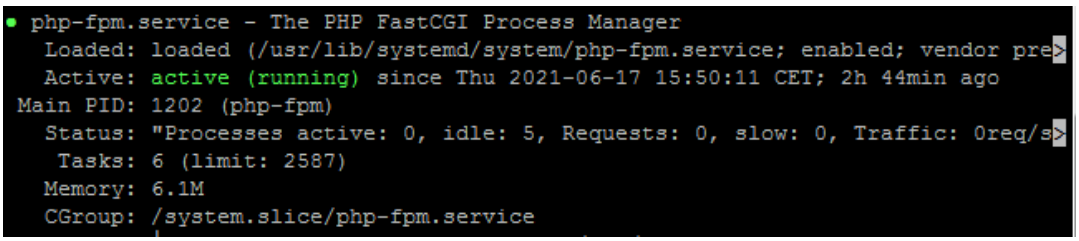


Figure 15 : Le statut de PHP.

3. Durcissement de système d'exploitation Linux

a. Introduction

Le durcissement est un processus de sécurisation d'un système et un ensemble d'outils, de techniques et de bonnes pratiques pour réduire la vulnérabilité des applications technologiques, des systèmes, de l'infrastructure, du micro logiciel et d'autres domaines.

La sécurisation du système Linux est une tâche difficile et longue pour les administrateurs système, mais il est nécessaire de renforcer la sécurité du linux pour améliorer le niveau de sécurité du système et le protéger contre les attaquants et des pirates[24].

Dans cette partie du chapitre nous allons présenter les étapes qui on a appliqué pour le renforcement du notre système. Nous commençons par effectuer l'installation de la bonne manière avec une bonne partition, nous avons donc une base solide. L'étape suivante consiste à réaliser des mesures de sécurité physique pour empêcher les

[24] ANSSI. (2019, February). *Recommandation de configuration d'un système GNU/LINUX*. https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf

personnes non autorisées d'accéder au système en premier lieu. Enfin, nous appliquons un ensemble de mesures de sécurité communes.

Notre objectif c'est d'atteindre un niveau de durcissement élevé sur notre système, pour réaliser notre but on a commencé de niveau minimal jusqu'à le niveau élevé selon le les étapes de schéma ci –dessus (voir la figure 17) :

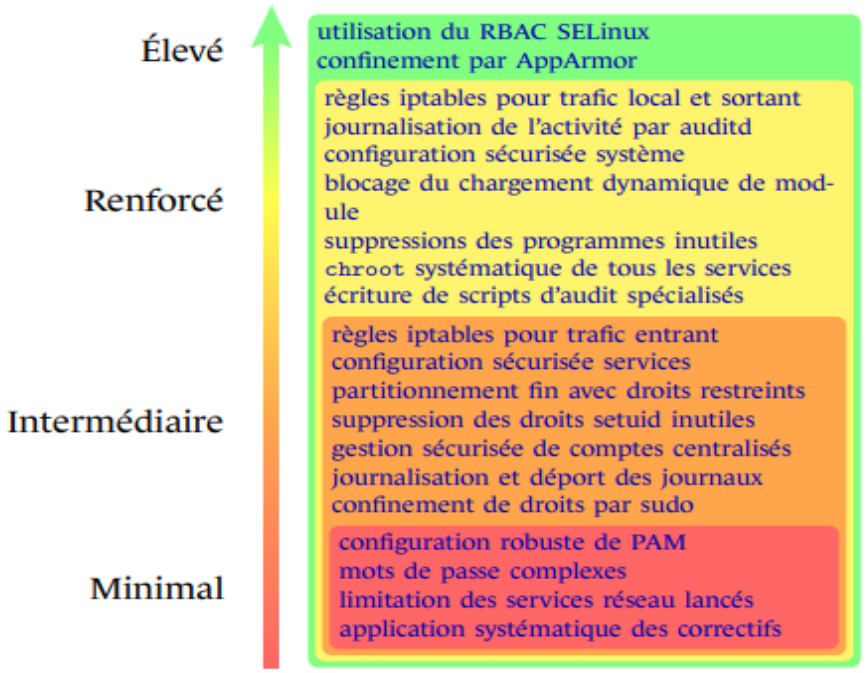


Figure 16 : Niveaux de sécurité système[25].

b. Sécurité relative à un système GNU/Linux

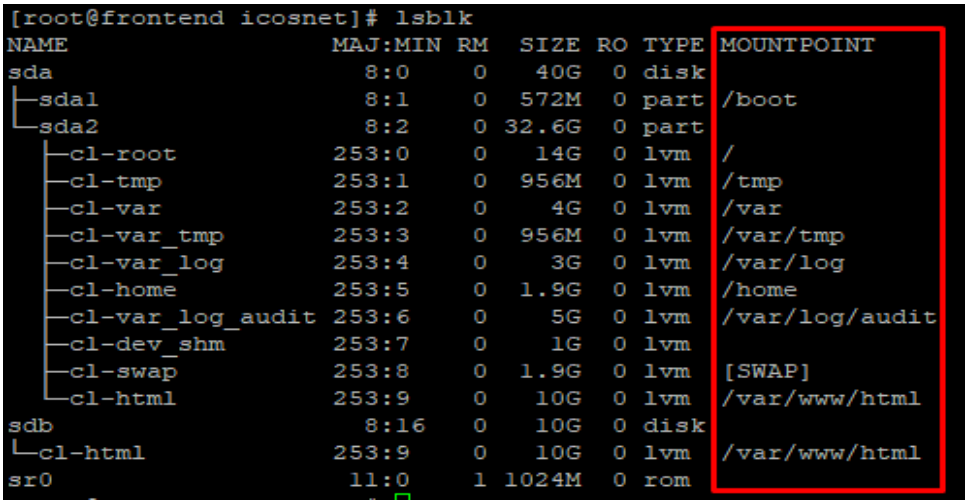
Du point de vue d'un professionnel de la sécurité informatique, un grand nombre de distributions classiques de Linux sont dans leur configuration initiale mal sécurisées et la plupart des paquets fournis sont dépassés au moment de l'installation, pour cela le durcissement de Linux commence dès la phase de l'installation du système. Généralement il existe un certain nombre d'étapes à réaliser lors de l'installation afin de s'assurer de l'intégrité de notre système et d'identifier les risques potentiels.

[25] ANSSI. (2019, February). *Recommandation de configuration d'un système GNU/LINUX*. https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf

i. Partitionnement du disque :

Il est important d'avoir des partitions différentes pour obtenir une plus grande sécurité des données en cas de sinistre. En créant différentes partitions, les données peuvent être séparées et regroupées. Lorsqu'un accident inattendu se produit, seules les données de cette partition seront endommagées, tandis que les données des autres partitions survivront.

L'administrateur de sécurité chez l'entreprise Icosnet à effectuer la partition suivante du disque (voir la figure 18) :



```
[root@frontend icosnet]# lsblk
NAME                  MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda                     8:0    0   40G  0 disk
├─sda1                  8:1    0  572M  0 part /boot
└─sda2                  8:2    0 32.6G  0 part
  ├─cl-root           253:0    0   14G  0 lvm  /
  ├─cl-tmp            253:1    0  956M  0 lvm  /tmp
  ├─cl-var            253:2    0    4G  0 lvm  /var
  ├─cl-var_tmp        253:3    0  956M  0 lvm  /var/tmp
  ├─cl-var_log        253:4    0    3G  0 lvm  /var/log
  ├─cl-home           253:5    0  1.9G  0 lvm  /home
  ├─cl-var_log_audit  253:6    0    5G  0 lvm  /var/log/audit
  ├─cl-dev_shm        253:7    0    1G  0 lvm
  ├─cl-swap           253:8    0  1.9G  0 lvm  [SWAP]
  └─cl-html           253:9    0   10G  0 lvm  /var/www/html
sdb                     8:16   0   10G  0 disk
└─cl-html           253:9    0   10G  0 lvm  /var/www/html
sr0                    11:0    1 1024M  0 rom
```

Figure 17 : Partitionnement du disque.

Après avoir vu cette liste, les utilisateurs malveillants peuvent exploiter des partitions telles que /tmp, /var/tmp et /dev/shm pour stocker et exécuter des programmes indésirables. Donc nous avons proposé de sécuriser chaque partition par des différentes options de montage pour restreindre ce qui peut être fait sur les fichiers du système.

Le tableau ci -dessus présente la description de différentes options utilisées :

Options	Description
Nodev	Interdit les périphériques.
Nosuid	Interdit les bits setuid ou setgid.
noexec	Interdit l'exécution de tout binaire.

Table 15 : Options de restrictions sur les fichiers.

Pour un bon renforcement du serveur linux nous avons choisi de réaliser la sécurisation de chaque partition du système par des options recommandé par le club “CIS Benchmark” [26] résumé dans le tableau suivant :

Partition	Description	Options
/	Partition racine, contient le reste de l’arborescence.	Defaults
/boot	Contient le noyau et le chargeur de démarrage. Pas d’accès nécessaire une fois le boot terminé (sauf mise à jour).	Defaults
/tmp	un répertoire accessible en écriture dans le monde utilisé pour le stockage temporaire par tous les utilisateurs et quelques applications.	defaults, nodev, nosuid, noexec.
/var	utilisé par les démons et autres services système pour stocker temporairement données dynamiques. Certains répertoires créés par ces processus peuvent être accessibles en écriture dans le monde entier.	Defaults, noexec
/var/tmp	est un répertoire accessible en écriture dans le monde utilisé pour le stockage temporaire par tous utilisateurs et certaines applications.	defaults, nodev, nosuid, noexec
-/var/log - /var/log/audit	est utilisé par les services système pour stocker les données de journal.	defaults, noexec
/home	Le répertoire est utilisé pour prendre en charge les besoins de stockage sur disque des utilisateurs locaux.	defaults, nodev

Table 16 : Partions recommandés par CIS.

[26]CIS.(2021, May).*CIS CentOS linux 8 benchmark.*

Pour effectuer à chaque partition sa fonction nous devons suivre les étapes suivantes :

- Tour d'abord, nous devons accéder au fichier **/etc/fstab** qui est un fichier de configuration système, et contient tous les disques disponibles avec les partitions et leurs options, nous utilisons cette commande :

vim /etc/fstab

- Ensuite nous devons ajouter pour chaque partition ses options pour mieux sécuriser les fichiers du serveur linux : nous devons apporter quelques modifications aux fichiers de configuration principales du système.

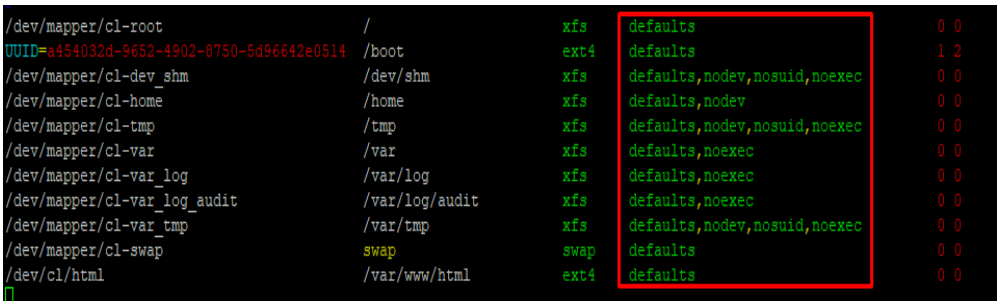


Figure 18 : Application des modifications sur les fichiers systèmes.

- Maintenant, après avoir modifié ce fichier, nous avons exécuté la commande suivante pour mettre à jour systemd :

systemctl daemon-reload

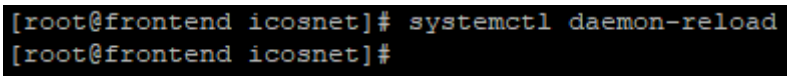


Figure 19 : Mise à jour du systemd.

- Pour vérifier les modifications apportées sur le fichier, nous exécutons uniquement :

cat /etc/fstab

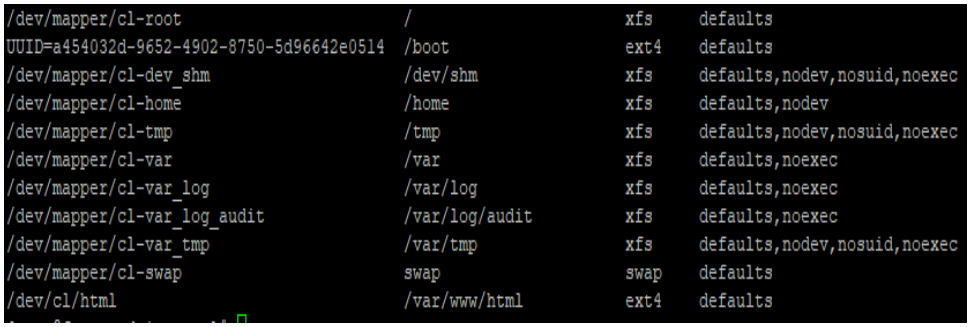


Figure 20 : Vérification de la modification.

ii. Mettre à jour le système :

La première chose à faire après le premier démarrage est de mettre à jour le système car c'est une tâche très critique, en particulier lorsqu'il s'agit d'installer des mises à jour de sécurité. Cela garantit que le système reste sûr, stable et vous tient au courant des dernières menaces de sécurité.

Pour mettre le système à jour nous avons exécuté la commande suivante :

yum update

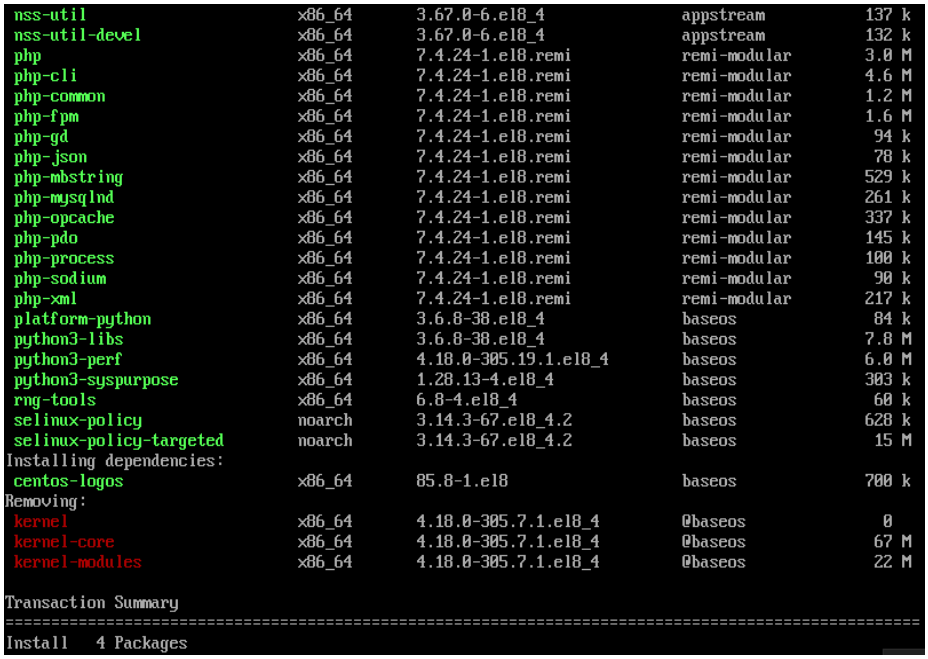


Figure 21 : Mise à jour du système.

On peut aussi vérifier les mis à jour disponible sur le système avec la commande :

yum check – update

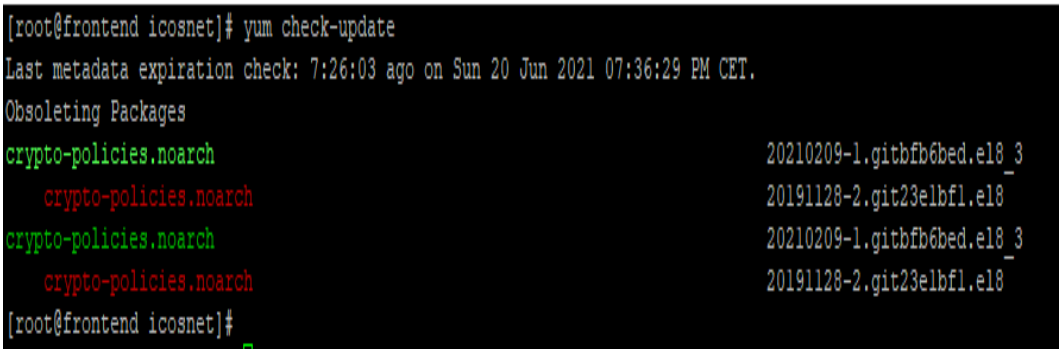


Figure 22 : Vérification des mises à jour système.

iii. Désactiver les systèmes de fichiers inutilisés :

La suppression de la prise en charge des types de système de fichiers inutiles réduit la surface d'attaque locale du système car un certain nombre de types de systèmes de fichiers peu courants sont pris en charge sous Linux. Si un système de fichiers type n'est pas nécessaire, il doit être désactivé.

D'après la recommandation CIS (Center for Internet Security) concernant le benchmark CentOS 8 Linux les fichiers système qu'on doit désactiver sont :

1. Cramfs :

Le système de fichiers cramfs (compressed ROM/RAM file system) n'est pas utilisé, donc la recommandation donnée par CIS est de désactiver définitivement ce fichier de système.

Pour désactiver cramfs, les étapes qu'il faut exécuter sont:

- Définir une certaine ligne de configuration qui se place dans /etc/modprobe.d :

  cd /etc/modprobe.d

- Ensuite, nous avons créé un nouveau fichier :

  vim cramfs.conf

- Après, nous avons implémenté la configuration suivante qui permet de désactiver cramfs sur ce fichier:

```
install cramfs /bin/true
```

Figure 23 : Désactivation de cramfs.

- Maintenant, nous devons exécuter la commande suivante pour décharger le module cramfs:

```
[root@frontend modprobe.d]# rmmod cramfs
```

Figure 24 : Décharger le module cramfs.

- Enfin, nous avons exécuté les commandes suivantes pour vérifier que le module cramfs est désactivé:

  modprobe -n -v cramfs

  lsmod | grep cramfs

```
[root@frontend modprobe.d]# modprobe -n -v cramfs
install /bin/true
[root@frontend modprobe.d]# lsmod | grep cramfs
[root@frontend modprobe.d]# _
```

Figure 25 : Vérification que le module cramfs est désactivé.

2. vFat :

Ce système n'est pas utilisé car le format de vFAT est principalement utilisé sur les anciens systèmes Windows et les périphériques USB portables, lecteurs ou modules flash.

Pour désactiver vFAT, les étapes qu'il faut exécuter sont :

1. Définir une certaine ligne de configuration qui se place dans /etc/modprobe.d:

   cd /etc/modprobe.d

2. Créer un nouveau fichier :

   vim vfat.conf

```
[root@frontend icosnet]#  cd /etc/modprobe.d
[root@frontend modprobe.d]# vim vfat.conf
```

Figure 26 : Création d'un nouveau fichier.

3. Implémenter la configuration suivante qui permet de désactiver vFat sur ce fichier :

```
install vfat /bin/true
```

Figure 27 : Désactivation de vFat.

4. Exécuter la commande suivante pour décharger le module vFat :

```
[root@frontend modprobe.d]# rmmod vfat
```

Figure 28 : Décharger vFat.

5. Exécuter les commandes suivantes pour vérifier que le module vFat est désactivé:

   modprobe -n -v vfat

   lsmod | grep vfat

```
[root@frontend modprobe.d]# modprobe -n -v vfat
insmod /lib/modules/4.18.0-305.17.1.el8_4.x86_64/kernel/fs/fat/fat.ko.xz
install /bin/true
[root@frontend modprobe.d]# lsmod | grep vfat
[root@frontend modprobe.d]#
```

Figure 29 : Vérification de la désactivation de vFat.

6. De même manier nous avons désactivé les systèmes des fichiers suivantes :
    - Le montage des systèmes de fichiers squashfs.
    - Le montage des systèmes de fichiers udf.
    - Le montage automatique.
    - Le stockage USB.

iv. Désactiver les services inutilisés :

Il est toujours conseillé de désactiver les services inutilisés ou inutiles sur le serveur linux. En effet, plus le nombre de services en cours d'exécution n'est élevé, plus le nombre de ports ouverts sur le système peuvent être exploité par un attaquant pour accéder à notre serveur. De plus, les meilleures pratiques de sécurité recommandent de désactiver les services inutilisés et de se débarrasser de tous les services non sécurisés en cours d'exécution sur votre système.

Pour désactiver les différents services inutiles dans le système nous devons suivre les étapes suivantes :

1. Toute d'abord, nous avons affiché tous les services disponibles sur le système avec la commande suivante :

systemctl list-unit-files

Figure 30 : Les services disponibles.

2. D'après l'administrateur de la sécurité de l'entreprise Icosnet, nous devons vérifier les services suivants :

   a. Les services **xinetd, telentclient** et **openldap-clients** ne sont pas installé :

```
[root@frontend icosnet]# rpm -q xinetd
package xinetd is not installed
[root@frontend icosnet]#
[root@frontend icosnet]# rpm -q telent
package telent is not installed
[root@frontend icosnet]#
[root@frontend icosnet]# rpm -q openldap-clients
package openldap-clients is not installed
[root@frontend icosnet]#
```

Figure 31 : Vérification des services non installés.

3. Désactiver le service avahi :

systemctl --now disable avahi-daemon.service

```
[root@frontend icosnet]# systemctl --now disable avahi-daemon.service
Removed /etc/systemd/system/multi-user.target.wants/avahi-daemon.service.
Removed /etc/systemd/system/sockets.target.wants/avahi-daemon.socket.
Removed /etc/systemd/system/dbus-org.freedesktop.Avahi.service.
Warning: Stopping avahi-daemon.service, but it can still be activated by:
  avahi-daemon.socket
```

Figure 32: Désactivation du service avahi.

v. Configuration des paramètres réseaux :

Certains paramètres de la configuration réseau IP du système doivent être modifiés de manière à renforcer sa robustesse vis-à-vis des attaques potentielles. Comme c'est souvent le cas, les paramètres par défaut permettent de prendre nativement chargé beaucoup de fonctionnalités[27].

Pour une configuration appropriée des paramètr1es réseaux on accède au fichier de configuration **/etc/sysctl.conf** et désactiver et ignorer les services suivants :

- Nous désactivons le routage source :

```
net.ipv4.conf.all.accept_source_route=0
net.ipv4.conf.default.accept_source_route=0
```

Figure 33 : Désactivation du routage source

[27]Guide technique relatif à la sécurité du serveur Linux. (2014). Direction générale de la sécurité des systèmes d'information. https://www.dgssi.gov.ma/sites/default/files/attached_files/guide_linux-v14-12-2015.pdf

- Après, nous désactivons aussi l'acceptation et l'envoi de paquets ICMP redirigés :

```
net.ipv4.conf.all.accept_redirects=0
net.ipv4.conf.default.accept_redirects=0
```

Figure 34 : Les paquets ipv4 à 0.

```
net.ipv6.conf.all.accept_redirects=0
net.ipv6.conf.default.accept_redirects=0
```

Figure 35 : Les paquets ipv6 à 0.

- Nous enregistrions les paquets martiens suspects :

```
net.ipv4.conf.all.log_martians=1
net.ipv4.conf.default.log_martians=1
```

Figure 36 : Enregistrer des paquets martiens suspects.

- Ignorer Les requêtes ICMP de diffusion :

```
net.ipv4.icmp_echo_ignore_broadcasts=1
net.ipv4.icmp_echo_bold_ignore_broadcasts=1
```

Figure 37 : Ignorer Les requêtes ICMP de diffusion.

- Ignorer les fausses réponses ICMP :

```
net.ipv4.icmp_ignore_bogus_error_responses=1
net.ipv4.icmp_echo_bold_ignore_broadcasts=1
```

Figure 38 : Ignorer les fausses réponses ICMP.

- Mettre « **net.ipv4.conf.all.rp_filter »** et « **net.ipv4.conf.default.rp_filter »** sur 1 force le noyau Linux pour utiliser le filtrage du chemin inverse sur un paquet reçu pour déterminer si le paquet était validé.

```
net.ipv4.conf.all.rp_filter=1
net.ipv4.conf.default.rp_filter=1
```

Figure 39 : Filtrage du chemin inverse.

vi. Sécurisation locale du système

1. Gestion des comptes et des utilisateurs :

Linux est un système d'exploitation multi-utilisateurs, tous les utilisateurs doivent posséder un compte usager pour pouvoir y accéder. De plus, ils doivent être identifiés afin d'assurer la confidentialité. Un tel système impose des contraintes de sécurité qui n'existent pas sur un système mono-utilisateur.

La gestion des comptes représente une partie primordiale dans la sécurité des systèmes. Avec une mauvaise gestion des utilisateurs et de leurs droits, de nombreux systèmes pourraient être corrompus. Il est donc crucial de mettre en place les techniques appropriées de gestion des comptes utilisateurs pour protéger l'accès au système. Pour une configuration sécurisée de la gestion des comptes, nous avons procéder comme suit :

- Afficher la liste des comptes utilisateur root et supprimer les comptes inutilisés :

```
[root@frontend ~]# lid -g wheel
 root(uid=0)
 admin(uid=1002)
[root@frontend ~]#
```

Figure 40 : La liste des comptes.

- Supprimer le répertoire d'origine de l'utilisateur « admin » ainsi que son compte :

```
[root@frontend icosnet]# userdel -r admin
[root@frontend icosnet]#
```

Figure 41 : Suppression de l'utilisateur admin.

- Afficher la liste des comptes pour vérifier la suppression de compte « admin » :

```
[root@frontend ~]# lid -g wheel
 root(uid=0)
[root@frontend ~]#
```

Figure 42 : Vérification de la suppression du compte root.

- Désactiver le compte super-utilisateur (root) : C'est le compte le plus important sur le système, son UID égal à 0. Ce compte dispose des droits d'accès administratifs.

Il est recommandé de désactiver le compte root entièrement et d'ajouter des comptes d'administration nominatifs qui peuvent effectuer les tâches d'administrations en utilisant la commande sudo suivie d'une authentification.

- Avant de désactiver le compte root nous devons créer un nouveau compte pour l'administrateur du système. Pour créer un compte administratif nous avons exécuté les commandes suivantes :

useradd icosnet

passwd icosnet

```
[root@frontend ~]#
[root@frontend ~]# useradd icosnet
[root@frontend ~]#
[root@frontend ~]# passwd icosnet
Changing password for user icosnet.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@frontend ~]#
```

Figure 43 : Création d'un nouveau compte root.

- Après que le compte est créé, nous devons donner le privilège sudo pour le compte créé :

```
[root@frontend ~]# usermod -G wheel icosnet
[root@frontend ~]#
```

Figure 44 : Donner le privilège sudo au compte.

- Maintenant on affiche la liste des comptes :

```
[root@frontend ~]# lid -g wheel
 root(uid=0)
 icosnet(uid=1002)
```

Figure 45 : La nouvelle liste.

- Enfin, nous nous somme connecter au compte créé avec la commande suivante :

su –icosnet

```
[root@frontend ~]# su - icosnet
Last login: Sun Jun 20 19:00:00 CET 2021 on pts/0
[icosnet@frontend ~]$
```

Figure 46 : Connexion au nouveau compte.

- Maintenant que nous avons créé un nouveau compte pour l'administrateur, on peut désactiver le compte « root » avec la commande suivante :

usermod –L root

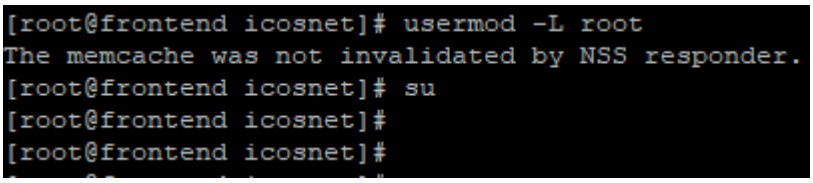


Figure 47 : Désactivation du compte root.

2. Sécurité des mots de passe :

Une bonne gestion des mots de passe permet un accès sécurisé au système. Il est nécessaire de choisir et d'utiliser des mots de passe robustes, c'est-à-dire difficiles à retrouver à l'aide d'outils automatisés et à deviner par une tierce personne.

Pour fixer une politique pour notre gestion des mots de passe nous avons modifié le fichier ***/etc/login.defs*** pour plus sécuriser les comptes du système**.**

- Toute d'abord, nous devons accéder au fichier ***/etc/login.defs*** avec la commande suivante :

vim /etc/login.defs

- Ensuite, nous devons modifier les paramètres suivants :
  - PASS_MAX_DAYS : Nombre maximum de jours pendant lesquels un mot de passe peut être utilisé.
  - PASS_MIN_DAYS : Nombre minimum de jours autorisés entre les changements de mot de passe.
  - PASS_MIN_LEN : Longueur minimale du mot de passe acceptable.
  - PASS_WARN_AGE : Nombre de jours d'avertissement avant l'expiration d'un mot de passe.

```
# Password aging controls:
#
PASS_MAX_DAYS 90
PASS_MIN_DAYS 7
#       PASS_MIN_LEN    Minimum acceptable password length.
PASS_WARN_AGE 7
#
PASS_MAX_DAYS 90
PASS_MIN_DAYS 7
PASS_MIN_LEN    5
PASS_WARN_AGE 7

#
# Min/max values for automatic uid selection in useradd
#
UID_MIN                  1000
UID_MAX                 60000
```

Figure 48 : Modification des paramètres du mot de passe.

- Pour le cryptage des mots de passe nous avons choisi l'algorithme **« SHA512 » :**

```
# Use SHA512 to encrypt password.
ENCRYPT_METHOD SHA512
```

Figure 49 : Cryptage du mot de passe.

3. Sécurité des mots de passe dans PAM :

Il est important d'avoir une bonne gestion et une bonne configuration de la politique des mots de passe sur notre système. Il est d'abord important de déterminer ce qu'est un mot de passe fort, communément, il doit suivre les recommandations suivantes :

- Comprend au moins huit caractères.
- Ne contient ni votre nom d'utilisateur, ni votre vrai nom, ni le nom de la société.
- Ne contient pas de mot entier.
- Contient des caractères provenant de chacune des quatre catégories suivantes (minuscule, majuscule, chiffre, caractères spéciaux).
- ous Linux, nous pouvons gérer ces recommandations dont le fichier PAM.

PAM (Les modules d'authentification enfichables Linux) est une suite de bibliothèques qui permet à un administrateur système Linux de configurer des méthodes pour authentifier les utilisateurs[28].

Pour la configuration de Pam nous devons suivre les étapes suivantes :

- Vérifier que les exigences de création de mot de passe sont conformes à la politique de l'organisation avec la commande suivante :

vim /etc/pam.d/system-auth

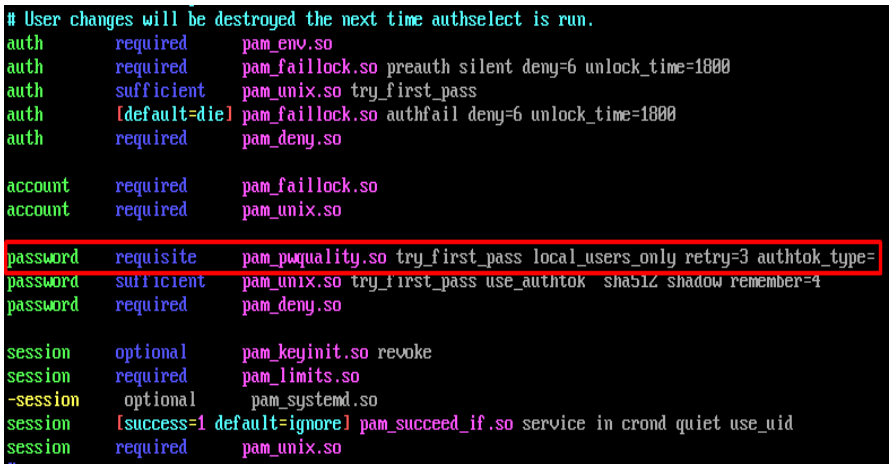


Figure 50 : Vérification la politique du mot de passe.

- D'après le fichier de configuration **/etc/pam.d/system-auth** le module PAM n'est pas configuré, donc on ajoute la ligne suivante pour sécuriser les mots de passe contre les différentes attaques:
    - D'abord nous nous somme accéder au fichier **/etc/pam.d/system-auth** et accéder à la ligne contenant les **pam_pwquality.so** modules, après commenter la ligne.

Figure 51 : Mise en commentaire l'ancienne configuration.

[28]Wikipedia contributors. (s. d.-e). Linux PAM. Wikipedia. Consulté le 25 juin 2021, à l'adresse https://en.wikipedia.org/wiki/Linux_PAM

- Ensuite, nous avons remplacé la ligne par la suivante :

```
password    requisite     pam_pwquality.so try_first_pass local_users_only retry=3 authtok_type= min
len=8 lcredit=-1 ucredit=-1 dcredit=-1 ocredit=-1 enforce_for_root
```

Figure 52 : Nouvelle configuration du mot de passe.

i. **minlen=8**– définit la longueur minimale du mot de passe à 8 caractères.

ii. **lcredit=-1** -Définit le nombre minimum de lettres minuscules que le mot de passe doit contenir à au moins un.

iii. **ucredit=-1**-Définit le nombre minimum de lettres majuscules sur un mot de passe à au moins un.

iv. **dcredit=-1** – Définit le nombre minimum de chiffres à contenir dans un mot de passe à au moins un.

v. **ocredit=-1**– Définissez le nombre minimum d'autres symboles tels que @, #, ! $ % etc sur un mot de passe à au moins un.

vi. **enforce_for_root** – Garantit que même si c'est l'utilisateur root qui définit le mot de passe, les stratégies de complexité doivent être appliquées.

- En tant qu'utilisateur root, nous essayons de changer le mot de passe d'utilisateur « icosnet » avec un mot de passe qui ne correspond pas aux informations d'identification définies dans PAM (Par exemple mote de passe « icosnet »).

vii. Voici un exemple de la création du mot de passe avant la configuration PAM :

```
[root@frontend icosnet]# passwd icosnet
Changing password for user icosnet.
New password:
BAD PASSWORD: The password contains less than 1 digits
Retype new password:
passwd: all authentication tokens updated successfully.
```

Figure 53 : Résultat avant PAM.

- Après la configuration du PAM :

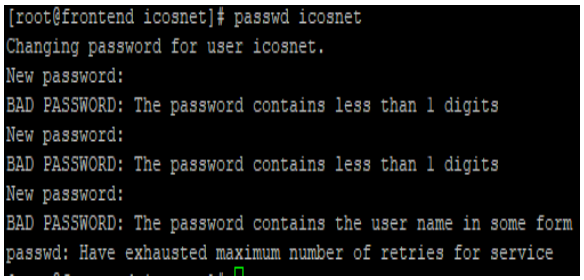


Figure 54 : Résultat après PAM.

vii. Gestion des accès

1. Accès physique au système :

La sécurité des accès physiques au système est une étape très importante pour protéger la configuration physique d'un système Linux. La configuration de notre système en toute sécurité dès le début facilite la mise en œuvre ultérieure de paramètres de sécurité supplémentaires.

La sécurité physique du système repose en premier lieu sur l'emplacement et l'environnement physique où est installé le serveur. Cela permet d'empêcher l'accès non autorisé ainsi que les dommages de tout genre pouvant affecter le serveur. Les mesures suivantes permettent de contrôler l'accès au système :

- Limiter l'accès physique à l'emplacement de serveur et mettre en place diverses mesures de sécurité. Il est recommandé de discuter des mesures de protection en place pour le système et de s'assurer qu'elles répondent aux besoins.
- Verrouillé de manière sécurisée la salle dédiée aux serveurs, si possible dans un emplacement central du bâtiment, avec un accès uniquement accordé à ceux qui ont besoin de maintenir physiquement le serveur.
- Il est également recommandé de garder les racks de serveurs ou les boîtiers verrouillés.

2. Sécurisation du chargeur de démarrage grub2 :

Le GRUB est le système qui va s'occuper du menu de démarrage de notre système quand nous installons un OS Linux. Le GRUB est un outil qui permet de détecter les différents systèmes d'exploitation présents sur la machine et de les lister au démarrage de celle-ci pour nous orienter vers quel OS démarré[29]. C'est un outil que l'on peut optimiser afin de mettre en place une meilleure protection de notre machine. Il est recommandé de protéger la configuration du chargeur de démarrage par un login et un mot de passe pour empêcher toute tentative de connexion avec le mode single ou bien le changement des paramètres pendant le démarrage. Pour ce faire, on ajoute une directive de Nom et mot de passe dans le fichier de configuration du GRUB en suivant les étapes suivantes :

1. Rentrer dans le fichier de la configuration grub **/etc/grub.d**.
2. Copier le contenu de fichier «40_custom » dans un nouveau fichier 40**_custom-ori**.
3. Gérer un mot de passe crypté pour le chargeur de démarrage.

```
[root@frontend icosnet]# cd /etc/grub.d
[root@frontend grub.d]#
[root@frontend grub.d]# ls
00_header             10_linux              20_ppc_terminfo   41_custom
00_tuned              10_reset_boot_success 30_os-prober      README
01_users              12_menu_auto_hide     30_uefi-firmware
08_fallback_counting  20_linux_xen          40_custom
[root@frontend grub.d]#
[root@frontend grub.d]# cp 40_custom 40_custom-ori
[root@frontend grub.d]#
[root@frontend grub.d]# ls
00_header             10_linux              20_ppc_terminfo   40_custom-ori
00_tuned              10_reset_boot_success 30_os-prober      41_custom
01_users              12_menu_auto_hide     30_uefi-firmware  README
08_fallback_counting  20_linux_xen          40_custom
[root@frontend grub.d]#
[root@frontend grub.d]#
[root@frontend grub.d]# grub2-mkpasswd-pbkdf2
Enter password:
Reenter password:
PBKDF2 hash of your password is grub.pbkdf2.sha512.10000.4E374085D51AC2DD53C6D22
6B3951B59CAED40C085290CC1ED1B8CA73D6F401A703CB519720A0DE1B8D08DF6271DFC382718395
412292EF75CC7CAC5B6C5D798.0F40EEA884BD21B16A6F04F706A9AA05984832AD83C2EE31F9CDF1
4205187ABA443BE47656473929E24D7C9DBB295AEA1784DE8B32B630DB4E1FC81A6BCD633C
[root@frontend grub.d]#
```

Figure 55 : Création d'un mot de passe de boot.

[29]Dorigny, M. (s. d.). Sécuriser l'édition du GRUB | Commandes et Système. IT-Connect. Consulté le 21 juin 2021, à l'adresse https://www.it-connect.fr/securiser-ledition-du-grub

4. Ajouter le mot de passe crypté et un nom d'utilisateur dans le fichier **40_custom** avec la commande suivante :

```
[root@frontend grub.d]# vim  40_custom
```

Figure 56 : Configurer le fichier custom partie 1.

5. Accéder au fichier de la configuration grub2 et copier le contenu du fichier grub.cfg dans le fichier **grub.cfg -ori**.

```
set superusers="icosnet"
password_pbkdf2 icosnet grub.pbkdf2.sha512.10000.8DD24031507BA30E09E7B84EFFC9715B5CF02525752C72BC0F1
0B2BC73DC4B3C7A44DBBA32DED872E24073200A8C337846F798910AA59A12F93C69932F1BF895.EE0F001B7881E309831D26
81C2F4F2293086D59A086B21A968283FE3E499D77D6012A0944A709A101DE6E43E32A4BFC93F006C23A0D09928BD1D37AF81
84566B
```

Figure 57 : Configuration du fichier custom partie 2.

6. Mettre à jour le fichier de configuration du grub avec la commande suivante :

grub2-mkconfig -o /boot/grub2/grub.cfg

```
[root@frontend grub.d]# cd /boot/
[root@frontend boot]#
[root@frontend boot]# ls
config-4.18.0-193.28.1.el8_2.x86_64                 initramfs-4.18.0-193.28.1.el8_2.x86_64.img
config-4.18.0-305.3.1.el8.x86_64                    initramfs-4.18.0-240.22.1.el8_3.x86_64.img
efi                                                 initramfs-4.18.0-305.3.1.el8.x86_64.img
grub2                                               loader
initramfs-0-rescue-772c3f0e80bc473cbfd6e4f30d376351.img  lost+found
[root@frontend boot]#
[root@frontend boot]# cd grub2/
[root@frontend grub2]#
[root@frontend grub2]# ls
device.map  fonts  grub.cfg  grubenv  i386-pc
[root@frontend grub2]# cp grub.cfg grub.cfg
cp: 'grub.cfg' and 'grub.cfg' are the same file
[root@frontend grub2]#
[root@frontend grub2]# cp grub.cfg grub.cfg-ori
[root@frontend grub2]#
```

Figure 58 : Mise à jour de la configuration du grub.

```
[root@frontend grub2]# grub2-mkconfig -o /boot/grub2/grub.cfg
Generating grub configuration file ...
done
```

Figure 59 : Génération de la nouvelle configuration.

7. Vérifier que les informations de l'authentification sont enregistrées dans le fichier **grub.cfg** :

```
[root@frontend grub2]# vi /boot/grub2/grub.cfg
```

Figure 60 : Vérification des informations d'authentification.

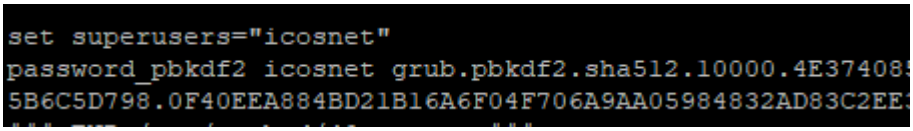


Figure 61 : Information d'authentification.

8. Enfin, pour s'assurer que la configuration est bien réussite. On redémarre le système et ont vérifié que le système du démarrage est verrouillé avec un nom et mot de passe :

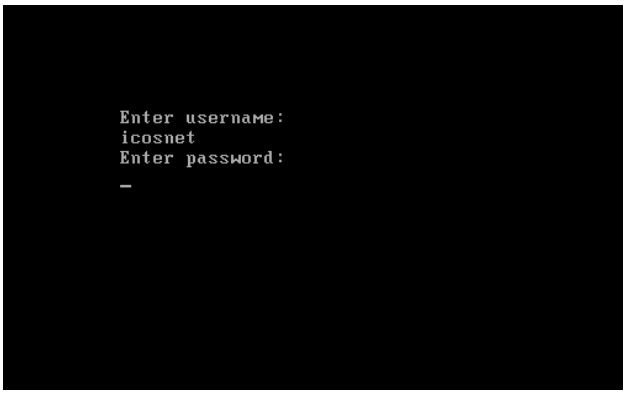


Figure 62 : Vérification du mot de passe de boot partie 1.

Figure 63 : Vérification du mot de passe de boot partie 2.

3. Droits d'accès au fichier :

Les droits d'accès définissent la possession d'un fichier ou d'un répertoire à un utilisateur et à un groupe d'utilisateurs. Ils gèrent aussi quelles actions les utilisateurs ont le droit d'effectuer sur les fichiers (lecture, écriture et exécution), selon qu'ils sont propriétaire du fichier, membre du groupe propriétaire du fichier ou ni l'un ni l'autre. La

possession et la gestion des permissions associées s'effectuent individuellement avec chaque fichier.

Les personnes partageant l'accès aux fichiers présentent un risque d'exposer des informations classifiées ou même de perdre des données si d'autres utilisateurs

Non autorisé accèdent à leurs fichiers ou répertoires. Pour résoudre ce problème, on applique les droits d'accès sur les fichiers critique du système comme suit :

Voici la liste des fichiers à protéger :

- **/etc/passwd** : contient des informations de compte d'utilisateur qui sont utilisées par de nombreux systèmes utilitaires et doivent donc être lisibles pour que ces utilitaires fonctionnent.
- **/etc/passwd-** : contient les informations de sauvegarde du compte utilisateur.
- **/etc/shadow** : utilisé pour stocker les informations sur les comptes d'utilisateurs qui sont essentielles à la sécurité de ces comptes, tels que le mot de passe haché et d'autres éléments de sécurité informations.
- **/etc/shadow-** : est utilisé pour stocker des informations de sauvegarde sur les comptes d'utilisateurs qui sont critiques pour la sécurité de ces comptes, comme le mot de passe haché et d'autres éléments de sécurité informations.
- **/etc/gshadow** : est utilisé pour stocker les informations sur les groupes qui sont critiques pour le la sécurité de ces comptes, comme le mot de passe haché et d'autres informations de sécurité.
- **/etc/gshadow-** : est utilisé pour stocker des informations de sauvegarde sur les groupes qui sont critiques pour la sécurité de ces comptes, tels que le mot de passe haché et d'autres éléments de sécurité informations.

- **/etc/group** : contient une liste de tous les groupes valides définis dans le système.

Et voici les types des droits :

- **r** : droit de lecture (read).
- **w** : droit d'écriture (write)**.**
- **x** : droit d'exécution (eXecute).

Pour commencer nous effectuons les droites de lectures, et d'écriture pour le root et lecture sur les autres fichiers **/etc/passwd** avec les commandes suivantes :

1. La commande **chown** pour changer le propriétaire à **root** et la commande **chmod** pour changer les droits de fichiers au l'écriture pour le root, et au lecture pour les autres fichiers **:**

chown root:root /etc/passwd

chmod 644 /etc/passwd

```
[root@frontend icosnet]# chown root:root /etc/passwd
[root@frontend icosnet]#  chmod 644 /etc/passwd
[root@frontend icosnet]#
```

Figure 64 : Changement des droits sur les fichiers.

2. Ensuite, nous avons vérifié les droits d'accès du fichier **/etc/passwd** :

```
[root@frontend icosnet]# stat /etc/passwd
  File: /etc/passwd
  Size: 1551            Blocks: 8          IO Block: 4096   regular file
Device: fd00h/64768d    Inode: 226886      Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2021-06-21 14:12:37.774230915 +0100
Modify: 2021-06-20 19:39:27.748935730 +0100
Change: 2021-06-21 14:59:51.894602397 +0100
 Birth: -
[root@frontend icosnet]#
```

Figure 65 : Vérification des droits d'accès.

3. Après, nous avons effectué les droites de lectures et d'écriture pour le root et de lecture pour les autres utilisateurs sur le fichier **/etc/passwd** :

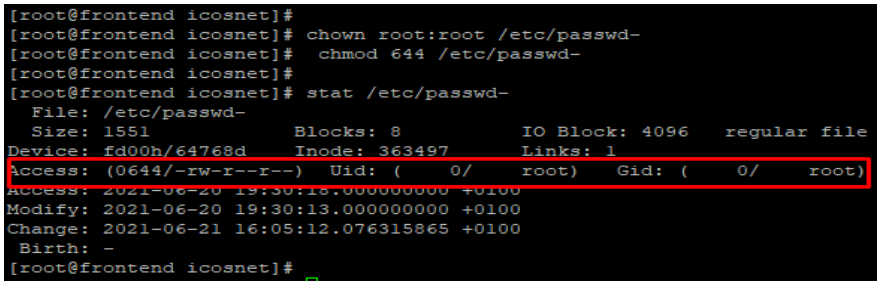


Figure 66 : Effectuer les droites d'accès.

4. Nous avons éliminé tous les droits sur le fichier **etc/shadow** et **etc/shadow –** donc personne ne peut lire, écrire ou exécuter sur ces fichiers :

Figure 67 : Elimination des droits précédents, partie 1.

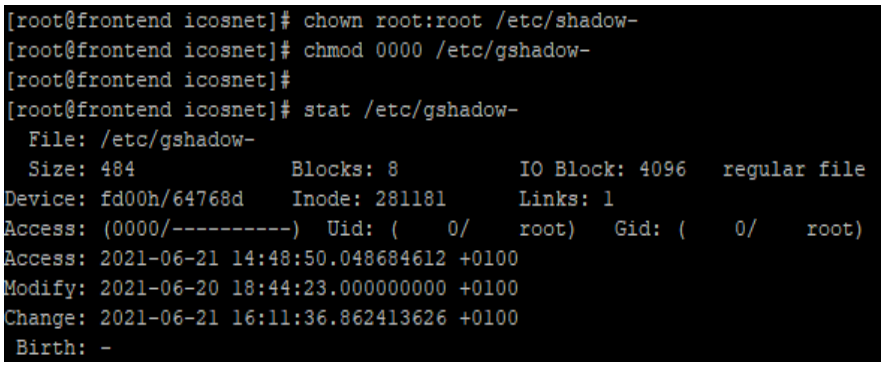


Figure 68 : Eliminations des droites précédentes, partie 2.

5. Ensuite, nous devons éliminer tous les droits sur le fichier **etc/gshadow** et **etc/gshadow** – donc personne ne peut lire, écrire ou exécuter sur ces fichiers (voir la figure 70):

```
[root@frontend icosnet]# chown root:root /etc/gshadow
[root@frontend icosnet]# chmod 0000 /etc/gshadow
[root@frontend icosnet]#
[root@frontend icosnet]# stat /etc/gshadow
  File: /etc/gshadow
  Size: 492             Blocks: 8          IO Block: 4096   regular file
Device: fd00h/64768d    Inode: 226881      Links: 1
Access: (0000/----------)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2021-06-20 18:53:43.516630192 +0100
Modify: 2021-06-20 18:53:20.609566599 +0100
Change: 2021-06-21 15:58:51.263226892 +0100
 Birth: -
[root@frontend icosnet]#
```

Figure 69 : Élimination des droits sur le fichier etc/gshadow et etc/ gshadow partie 1.

```
[root@frontend icosnet]# chown root:root /etc/gshadow-
[root@frontend icosnet]# chmod 0000 /etc/gshadow-
[root@frontend icosnet]#
[root@frontend icosnet]# stat /etc/gshadow-
  File: /etc/gshadow-
  Size: 484             Blocks: 8          IO Block: 4096   regular file
Device: fd00h/64768d    Inode: 281181      Links: 1
Access: (0000/----------)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2021-06-21 14:48:50.048684612 +0100
Modify: 2021-06-20 18:44:23.000000000 +0100
Change: 2021-06-21 16:00:26.248674567 +0100
 Birth: -
[root@frontend icosnet]#
```

Figure 70 : Élimination des droits sur le fichier etc/gshadow et etc/ gshadow partie 2.

6. Après, nous avons effectué les droites de lectures, d'écriture pour le root et de lecture pour les autres sur le fichier **/etc/group** :

```
[root@frontend icosnet]# chown root:root /etc/group
[root@frontend icosnet]# chmod 644 /etc/group
[root@frontend icosnet]#
[root@frontend icosnet]# stat /etc/group
  File: /etc/group
  Size: 622             Blocks: 8          IO Block: 4096   regular file
Device: fd00h/64768d    Inode: 226888      Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2021-06-20 18:53:20.551568969 +0100
Modify: 2021-06-20 18:53:20.447573221 +0100
Change: 2021-06-21 16:17:10.462233624 +0100
 Birth: -
[root@frontend icosnet]#
```

Figure 71 : Effectuer les droites lectures, écriture sur le fichier /etc/group.

viii. Mise en place d'un système de filtrage (Iptables)

Par défaut, notre serveur peut communiquer librement avec internet. Si un service est mal configuré il pourrait alors être accessible depuis l'extérieur, ce qui engendre des risques pour notre serveur.

La solution consiste à utiliser un pare-feu, pour n'autoriser qu'un nombre spécifié de ports ouverts et filtrer les paquets transférés sur le réseau. Heureusement pour nous linux dispose d'un système de pare-feu intégré : IpTables.

IpTables est une structure de table générique qui définit des règles et des commandes dans le cadre du netfilter pour filtrer les différents « packages » du système. Le filtrage des paquets consiste à transmettre ou à bloquer des paquets sur une interface réseau en fonction des adresses, des ports ou des protocoles de la source et de la destination[30].

1. Installer Iptables :

Iptables est préinstallé dans la plupart des distributions Linux. Cependant, voici les étapes :

1. Nous exécutons les commandes suivante une par une:

sudo yum update

sudo yum install iptables

```
[root@frontend icosnet]# yum update
Last metadata expiration check: 1:17:16 ago on Tue 22 Jun 2021 08:04:26 PM CET.
Dependencies resolved.
Nothing to do.
Complete!
[root@frontend icosnet]# yum install iptables
Last metadata expiration check: 1:20:47 ago on Tue 22 Jun 2021 08:04:26 PM CET.
Package iptables-1.8.4-17.el8.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[root@frontend icosnet]#
```

Figure 72 : Installation d'Iptables.

2. Après, nous vérifions l'état de notre configuration actuelle d'iptables en exécutant :

sudo iptables -L

[30]Brown, K. (2020, août 27).The Beginner's Guide to iptables, the Linux Firewall.How-To Geek.https://www.howtogeek.com/177621/the-beginners-guide-to-iptables-the-linux-firewall/

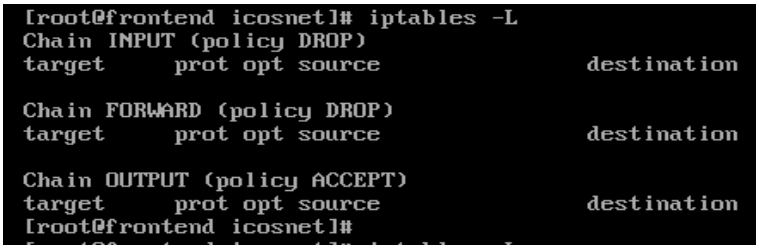


Figure 73 : La table par défaut d'Iptables.

2. Configuration d'Iptables :

Après l'installation réussite d'iptables nous allons appliquer les règles suivantes sur notre pare-feu :

3. Nous autorisons tout le trafic sortant de notre la machine. Le trafic sortant ne pourra théoriquement pas être dangereux.

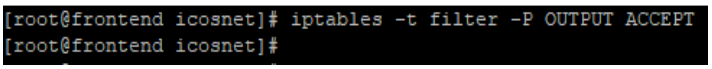


Figure 74 : Autorisation du trafic sortant.

4. Nous autorisons les connexions déjà établies car les données qui sont en état "établies" ont été autorisées par une des règles du trafic entrant du pare-feu.

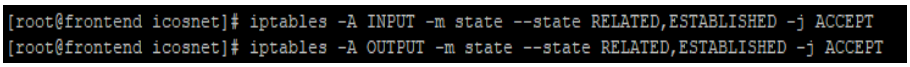


Figure 75 : Autorisation les connexions déjà établies.

5. Ensuite, nous autorisons le trafic entrant et sortant sur l'interface de bouclage réseau (IP : 127.0.0.1)

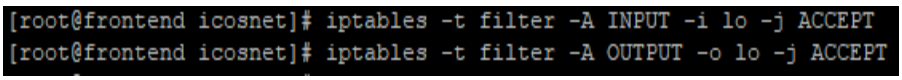


Figure 76 : Autorisation du trafic sur l'interface de bouclage.

6. Nous pouvons aussi autoriser le ping sur et depuis le serveur.

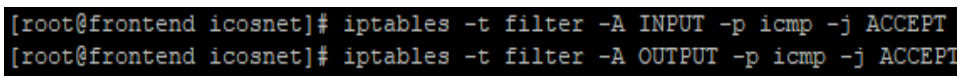


Figure 77 : Autorisation du ping sur et depuis le serveur.

7. Maintenant, nous pouvons autoriser l'ouverture de certain port. Nous commençons par le port SSH en entrant et en sortant.

```
[root@frontend icosnet]# iptables -t filter -A INPUT -p tcp --dport 22 -j ACCEPT
[root@frontend icosnet]# iptables -t filter -A OUTPUT -p tcp --sport 22 -j ACCEPT
```

Figure 78 : Autorisation du port SSH.

8. Après, nous autorisons le port 25 entrant et sortant pour autoriser le protocole d'envoi d'emails.

```
[root@frontend icosnet]# iptables -t filter -A INPUT -p tcp --dport 25 -j ACCEPT
[root@frontend icosnet]# iptables -t filter -A OUTPUT -p tcp --sport 25 -j ACCEPT
```

Figure 79 : Autorisation du trafic sur le port 25.

9. Ensuite, nous autorisons le trafic sur le port 110 pour autoriser le protocole de récupération d'émail.

```
[root@frontend icosnet]# iptables -t filter -A INPUT -p tcp --dport 110 -j ACCEPT
[root@frontend icosnet]# iptables -t filter -A OUTPUT -p tcp --sport 110 -j ACCEPT
```

Figure 80 : Autorisation du trafic sur le port 110.

10. Nous autorisons aussi le trafic sortant sur le port 53 pour accepter les requêtes DNS effectuées par le serveur (TCP et UDP).

```
[root@frontend icosnet]# iptables -t filter -A OUTPUT -p tcp --sport 53 -j ACCEPT
[root@frontend icosnet]# iptables -t filter -A OUTPUT -p udp --sport 53 -j ACCEPT
[root@frontend icosnet]# iptables -t filter -A OUTPUT -p tcp --dport 53 -j ACCEPT
[root@frontend icosnet]# iptables -t filter -A OUTPUT -p udp --dport 53 -j ACCEPT
```

Figure 81 : Autorisation du trafic sortant du port 53 partie 1.

11. Comme nous pouvons autoriser le trafic entrant sur le port 53 pour accepter les requêtes DNS envoyées par les clients et reçues par le serveur (TCP et UDP).

```
[root@frontend icosnet]# iptables -t filter -A INPUT -p tcp --dport 53 -j ACCEPT
[root@frontend icosnet]# iptables -t filter -A INPUT -p udp --dport 53 -j ACCEPT
```

Figure 82 : Autorisation du trafic entrant du port 53 partie 2.

12. Après cela, nous autorisons les protocoles HTTP et HTTPS en entrant/sortant (Serveur Web : HTTP (80) et HTTPS sécurisé par SSL (443 ou 8443).

```
[root@frontend icosnet]# iptables -t filter -A OUTPUT -p tcp --sport 80 -j ACCEPT
[root@frontend icosnet]# iptables -t filter -A OUTPUT -p tcp --sport 443 -j ACCEPT
[root@frontend icosnet]#
[root@frontend icosnet]# iptables -t filter -A INPUT -p tcp --dport 80 -j ACCEPT
[root@frontend icosnet]# iptables -t filter -A INPUT -p tcp --dport 443 -j ACCEPT
[root@frontend icosnet]# iptables -t filter -A INPUT -p tcp --dport 8443 -j ACCEPT
```

Figure 83 : Autorisation des protocoles http et https.

13. Ensuite, pour sécuriser notre serveur des différentes attaques (comme script-kiddies et DDOS etc....) nous avons ajouté des règles pour bloquer les paquets nuls qui sont simplement des paquets de reconnaissance. Ces modèles d'attaque utilisent ces paquets pour essayer de voir comment nous avons configuré le pare-feu et découvrir des faiblesses.

```
[root@frontend icosnet]# iptables -A INPUT -p tcp --tcp-flags ALL NONE -j DROP
```

Figure 84 : Blocage des paquets nuls.

14. Après, nous allons bloquer tous les paquets XMAS qui sont également des paquets de reconnaissance.

```
[root@frontend icosnet]# iptables -A INPUT -p tcp --tcp-flags ALL ALL -j DROP
```

Figure 85 : Blocage de tous les paquets XMAS.

15. Finalement nous bloquons les paquets envoyés par l'attaquant de syn-flood.

```
[root@frontend icosnet]# iptables -A INPUT -p tcp ! --syn -m state --state NEW -j DROP
```

Figure 86 : Blocage des paquets envoyés par l'attaquant de syn-flood.

3. Enregistrer la configuration :

Maintenant que nous avons configuré notre pare-feu nous pouvons lister les règles d'Iptables avec la commande suivante :

Iptables -l –n

```
[root@frontend icosnet]# iptables -L -n
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:22
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp spt:22
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:22
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:80
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:443
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:8443
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:25
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:110
DROP       tcp  --  0.0.0.0/0            0.0.0.0/0           tcp flags:0x3F/0x00
DROP       tcp  --  0.0.0.0/0            0.0.0.0/0           tcp flags:!0x17/0x02 state NEW
DROP       tcp  --  0.0.0.0/0            0.0.0.0/0           tcp flags:0x3F/0x3F
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:53
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:53

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp spt:22
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp spt:80
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp spt:443
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp spt:25
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp spt:110
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp spt:53
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp spt:53
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:53
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:53
[root@frontend icosnet]#
```

Figure 87 : La nouvelle table Iptables.

Maintenant nous pouvons enregistrer notre configuration du pare-feu :

```
[root@frontend icosnet]# iptables-save | sudo tee /etc/sysconfig/iptables
# Generated by iptables-save v1.8.4 on Tue Jun 22 23:30:37 2021
*filter
```

Figure 88 : Enregistrement d'Iptables.

Le fichier de configuration iptables sur CentOS se trouve dans */etc/sysconfig/iptables*. La commande ci-dessus a enregistré les règles que nous avons créées dans ce fichier (voir la figure 90).

Juste pour être sûr que tout fonctionne, nous avons redémarré le pare-feu :

```
[root@frontend icosnet]# service iptables restart
Redirecting to /bin/systemctl restart iptables.service
```

Figure 89 : Redémarrage du Pare-feu.

ix. Mise en place d'outil de prévention d'intrusion (Fail2ban)

1. Définition :

Fail2ban est une application d'analyse des journaux qui surveille les journaux système pour détecter les symptômes d'une attaque automatisée sur notre système.

Lorsqu'une tentative de compromission est localisée, à l'aide des paramètres définis, Fail2ban ajoute une nouvelle règle à Iptables pour bloquer l'adresse IP de l'attaquant, soit pour une durée déterminée, soit de manière permanente. Fail2ban peut également nous alerter par e-mail qu'une attaque est en cours.

Fail2ban se concentre principalement sur les attaques brute force sur SSH, bien qu'il puisse être configuré pour fonctionner pour tout service qui utilise des fichiers journaux et peut être soumis à un compromis.[31]

2. L'installation de Fail2ban :

- Premièrement, nous devons s'assurer que notre système est à jour et que le référentiel EPEL est installé (voir la figure 91) :

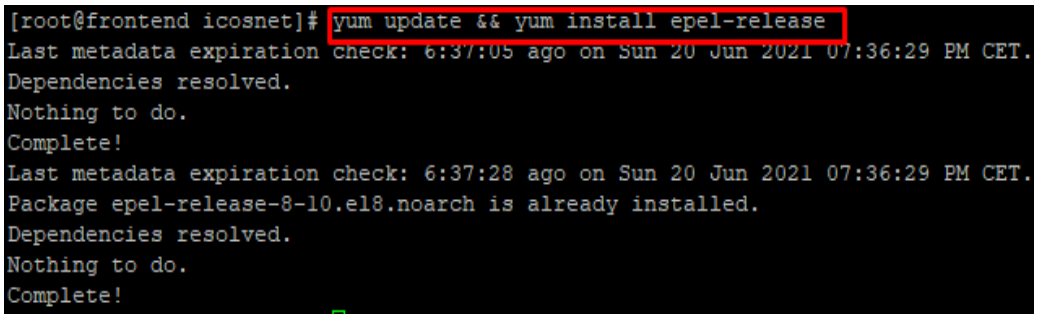


Figure 90 : Vérification d'état du système.

- Après avoir vérifié le système, nous pouvons maintenant installer Fail2Ban, avec la commande entrée sur la figure suivante :

[31]Fail2ban. (s. d.). Fail2ban. Consulté le 10 juin 2021, à l'adresse https://www.fail2ban.org/wiki/index.php/Main_Page

```
[root@frontend icosnet]# yum install fail2ban
Last metadata expiration check: 6:49:35 ago on Sun 20 Jun 2021 07:36:29 PM CET.
Dependencies resolved.
================================================================================
 Package            Arch    Version                                 Repo       Size
================================================================================
Installing:
 fail2ban           noarch  0.11.2-1.el8                            epel       19 k
Installing dependencies:
 esmtp              x86_64  1.2-15.el8                              epel       57 k
 fail2ban-firewalld noarch  0.11.2-1.el8                            epel       19 k
 fail2ban-sendmail  noarch  0.11.2-1.el8                            epel       22 k
 fail2ban-server    noarch  0.11.2-1.el8                            epel      459 k
 libesmtp           x86_64  1.0.6-18.el8                            epel       70 k
 liblockfile        x86_64  1.14-1.el8                              appstream  32 k
 python3-pip        noarch  9.0.3-19.el8                            appstream  20 k
 python3-setuptools noarch  39.2.0-6.el8                            baseos    163 k
 python3-systemd    x86_64  234-8.el8                               appstream  81 k
 python36           x86_64  3.6.8-2.module_el8.4.0+790+083e3d81      appstream  19 k
Enabling module streams:
 python36                   3.6

Transaction Summary
================================================================================
Install  11 Packages

Total download size: 960 k
Installed size: 2.4 M
Is this ok [y/N]: y
```

Figure 91 : Installation du Fail2Ban.

- Une fois l'installation terminée, nous devons installer **Sendmail** pour que l'administrateur puisse consulter les rapports envoyés par Fail2ban :

```
[root@frontend icosnet]# yum install sendmail
Last metadata expiration check: 1:33:49 ago on Mon 21 Jun 2021 05:12:05 PM CET.
Dependencies resolved.
================================================================================
 Package                    Architecture              Version
================================================================================
Installing:
 sendmail                   x86_64                    8.15.2-34.el8
Installing dependencies:
 procmail                   x86_64                    3.22-47.el8

Transaction Summary
================================================================================
Install  2 Packages

Total download size: 948 k
Installed size: 2.0 M
Is this ok [y/N]: y
Downloading Packages:
(1/2): procmail-3.22-47.el8.x86_64.rpm
(2/2): sendmail-8.15.2-34.el8.x86_64.rpm
--------------------------------------------------------------------------------
Total
Running transaction check
Transaction check succeeded.
```

Figure 92 : Installation du Sendmail.

- Ensuite, il suffit juste de démarrer et activer Fail2ban et de même pour Sendmail :

```
[root@frontend icosnet]# systemctl start fail2ban
[root@frontend icosnet]# systemctl enable fail2ban
Created symlink /etc/systemd/system/multi-user.target.wants/fail2ban.service →
usr/lib/systemd/system/fail2ban.service.
[root@frontend icosnet]# systemctl start sendmail
[root@frontend icosnet]# systemctl enable sendmail
Created symlink /etc/systemd/system/multi-user.target.wants/sendmail.service →
usr/lib/systemd/system/sendmail.service.
Created symlink /etc/systemd/system/multi-user.target.wants/sm-client.service
/usr/lib/systemd/system/sm-client.service.
[root@frontend icosnet]#
```

Figure 93 : Démarrage de Fail2ban et Sendmail.

- Maintenant Fail2ban est active, comme nous pouvons le voir sur la figure suivante :

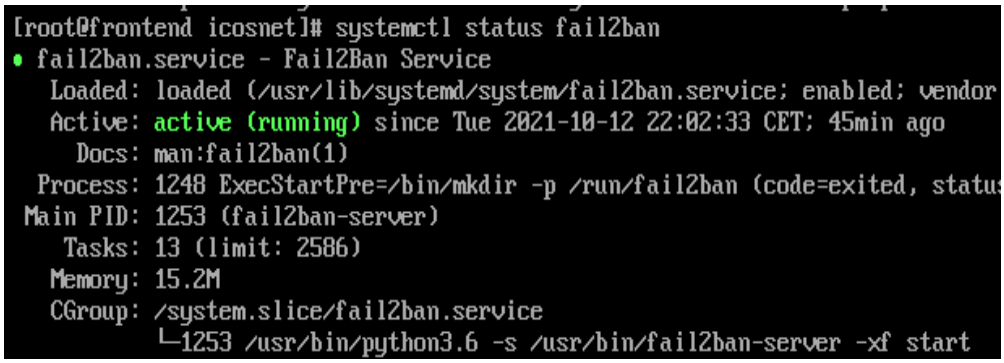


Figure 94 : Vérification du statut fail2ban.

3. La configuration de Fail2ban :

Le fichier de configuration global pour le serveur fail2ban est **/etc/fail2ban/fail2ban.conf**. Cependant, il n'est pas recommandé de modifier ce fichier directement, car il sera probablement écrasé ou amélioré en cas de mise à jour du package à l'avenir. Donc nous créons une copie fail2ban.conf en fail2ban.local.

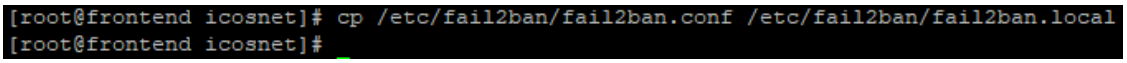


Figure 95 : Création d'une copie fail2ban.

- Fail2ban conserve les fichiers de configuration dans le répertoire **/etc/jail.local**. Mais nous devons créer une copie de ce fichier en tant que **jail.local**.

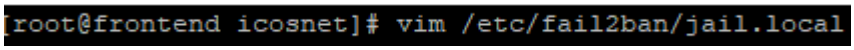


Figure 96 : Création du fichier jail.local partie 1.

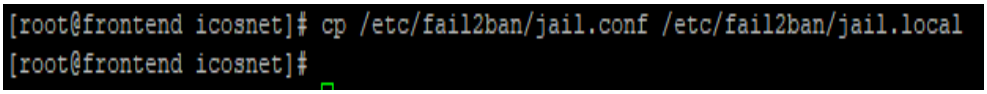


Figure 97: Création du fichier jail.local partie 2.

- Nous devons maintenant apporter des modifications nécessaires au fichier **jail.local** pour créer des règles d'interdiction. Nous avons modifié certains paramétré par défaut selon nos besoins.

```
# ignorecommand = /path/to/command <ip>
ignorecommand =

# "bantime" is the number of seconds that a host is banned.
bantime  = 20m

# A host is banned if it has generated "maxretry" during the last "findtime"
# seconds.
findtime  = 20m

# "maxretry" is the number of failures before a host get banned.
maxretry = 3

# "maxmatches" is the number of matches stored in ticket (resolvable via tag
maxmatches = %(maxretry)s
```

Figure 98 : Ajouter des paramètres au fichier jail.local partie 1.

```
destemail = icosnet@localhost

# Sender email address used solely for some actions
sender = fail2ban

# E-mail action. Since 0.8.1 Fail2Ban uses sendmail MTA for the
# mailing. Change mta configuration parameter to mail if you want to
# revert to conventional 'mail'.
mta = sendmail
```

Figure 99 : Ajout des paramètres au fichier jail.local partie.

- Voici la liste des paramètres qui nous devons prendre en considération :
    - **bantime** : Cela spécifie la durée pendant laquelle un hôte distant est banni en secondes.
    - **maxretry** : Il s'agit du nombre de tentatives de connexion infructueuses avant que l'hôte ne soit bloqué/interdit.
    - **findtime** : Durée en secondes pendant laquelle un hôte sera bloqué après avoir réalisé les tentatives maxtry.
    - **banaction** : L'action d'interdiction.
    - **Backend** : Le système utilisé pour récupérer les fichiers journaux.
    - **destmail** : Pour envoyer un Email à l'admin avec des informations sur l'IP bannie.

- Notre configuration implique que lorsqu'une l'adresse IP enregistre 3 tentatives d'authentification infructueuses au cours des 5 dernières minutes, elle sera alors bannie pendant 20 min, et en même temps Fail2ban envoie un email à l'administrateur d'Icosnet.
- Après avoir terminé la configuration, nous allons descendre dans le même fichier jail.local et nous choisissons de protéger SSH en ajoutant la ligne suivante dans la section de [sshd] :

enabled =true

```
[sshd]
enabled = true
port    = ssh
logpath = %(sshd_log)s
backend = %(sshd_backend)s
```

Figure 100 : Activation de SSH dans le fichier jail.local.

- Ensuite, après avoir effectué toutes les modifications, nous avons enregistré notre fichier et nous avant redémarrer le service Fail2ban à l'aide de la commande suivante :

systemctl restart fail2ban

- Après avoir configuré **fail2ban** pour sécuriser **sshd**, nous pouvons afficher l'état actuel du serveur fail2ban, nous exécutons les commandes suivantes :

```
[root@frontend icosnet]# fail2ban-client status
Status
|- Number of jail:      1
`- Jail list:   sshd
[root@frontend icosnet]#
```

Figure 101 : L'état actuel du serveur fail2ban.

- Et enfin, nous essayons le fonctionnement de fail2ban en testons SSH avec les mauvaises informations d'identification

avec l'adresse IP de notre machine « 192.168.16.1». Après trois tentatives erronées, Fail2ban a bloqué cette IP via Iptables avec « rej » et ICMP. Nous pouvons voir les règles dans Iptables après avoir bloqué l'adresse IP comme ci-dessous :

```
[root@frontend icosnet]# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
f2b-sshd   tcp  --  anywhere             anywhere             multiport dports ssh
ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTABLISHED
ACCEPT     all  --  anywhere             anywhere
ACCEPT     icmp --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:domain
ACCEPT     udp  --  anywhere             anywhere             udp dpt:domain
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:https
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:pcsync-https
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ftp-data
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ftp
ACCEPT     tcp  --  anywhere             anywhere             tcp dpts:50000:50100

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTABLISHED
ACCEPT     all  --  anywhere             anywhere
ACCEPT     icmp --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere             tcp spt:ssh
ACCEPT     tcp  --  anywhere             anywhere             tcp spt:domain
ACCEPT     udp  --  anywhere             anywhere             udp spt:domain
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:domain
ACCEPT     udp  --  anywhere             anywhere             udp dpt:domain
ACCEPT     udp  --  anywhere             anywhere             udp spt:ntp
ACCEPT     tcp  --  anywhere             anywhere             tcp spt:http
ACCEPT     tcp  --  anywhere             anywhere             tcp spt:https
ACCEPT     tcp  --  anywhere             anywhere             tcp spt:ftp
ACCEPT     tcp  --  anywhere             anywhere             tcp spt:ftp-data
ACCEPT     tcp  --  anywhere             anywhere             tcp spts:50000:50100

Chain f2b-sshd (1 references)
target     prot opt source               destination
RETURN     all  --  anywhere             anywhere
```

Figure 102 : Les règles d'Iptables après avoir bloqué la tentative de connexion.

- Nous pouvons surveiller les adresses IPs échouées et interdit à l'aide de la commande suivante :

Fail2ban-client statussshd

```
[root@frontend icosnet]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     2
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
   |- Currently banned: 0
   |- Total banned:     1
   `- Banned IP list:
```

Figure 103 : Statut de Fail2ban.

- Une fois que nous avons complètement testé fail2ban, nous devons accéder au boite des emails de compte «Icosnet » pour vérifier que fail2ban à envoyer une alerte de ban.

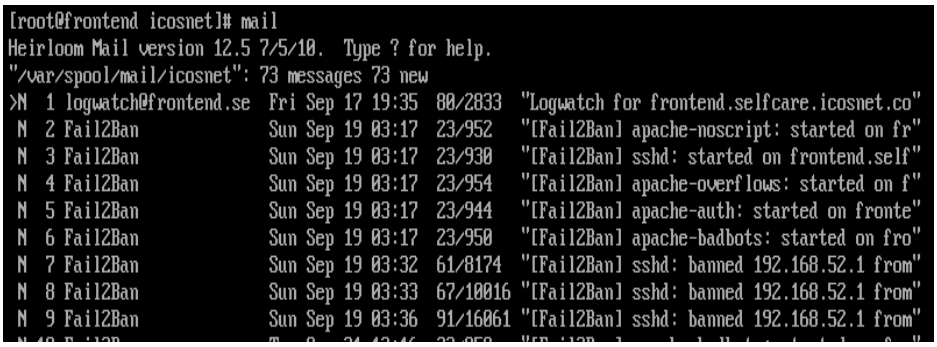


Figure 104 : Boite email du compte Icosnet.

- Finalement, voici l'émail envoyé par fail2ban :

Figure 105 : L'émail envoyé par Fail2ban.

x. Mise en place d'un analyseur de journaux (LogWatch)

LogWatch est un outil de gestion des journaux qui surveille et analyse les fichiers journaux d'un système et génère un rapport quotidien qui résume et rend compte l'activité des journaux du système. Ce rapport nous aidera à identifier si des erreurs ou des avertissements ont été signalés sur le système.[32]

1. Installation de LogWatch :

- Pour installer LogWatch, il faut juste entrer la commande suivante :

yuminstall –y logwatch

```
[root@frontend icosnet]# yum install -y logwatch
Last metadata expiration check: 7:13:45 ago on Sun 20 Jun 2021 07:36:29 PM CET.
Dependencies resolved.
================================================================================
 Package                                    Architecture
================================================================================
Installing:
 logwatch                                   noarch
Installing dependencies:
 mailx                                      x86_64
 perl-Date-Manip                            noarch
 perl-Sys-CPU                               x86_64
 perl-Sys-MemInfo                           x86_64

Transaction Summary
================================================================================
Install  5 Packages

Total download size: 1.8 M
Installed size: 13 M
Downloading Packages:
(1/5): mailx-12.5-29.el8.x86_64.rpm
(2/5): logwatch-7.4.3-9.el8.noarch.rpm
(3/5): perl-Sys-CPU-0.61-14.el8.x86_64.rpm
(4/5): perl-Sys-MemInfo-0.99-6.el8.x86_64.rpm
(5/5): perl-Date-Manip-6.60-2.el8.noarch.rpm
--------------------------------------------------------------------------------
Total
Running transaction check
Transaction check succeeded.
Running transaction test
```

Figure 106 : L'installation de LogWatch.

- Maintenant, nous configurons LogWatch pour analyser les fichiers log des services SSH, http, et sudo. Toute la configuration de Logwatch est gérée dans un seul fichier qui est le fichier "**/usr/share/logwatch/default.conf/logwatch.conf "**, nous avons accédée a ce fichier avec la commande suivante :

[32]Logwatch - ArchWiki. (s. d.). Archlinux.Consulté le 12 juin 2021, à l'adresse https://wiki.archlinux.org/title/Logwatch

```
[root@frontend icosnet]# vim /usr/share/logwatch/default.conf/logwatch.conf
```

Figure 107 : Accès au fichier de configuration de LogWatch.

- Ensuite, nous modifions certains paramètres par défaut du fichier en fonction de nos besoins. En définissons la sortie de LogWatch sous forme d'email :

```
Output = mail
#To make Html the default formatting Format = html
Format = text
#To make Base64 [aka uuencode] Encode = base64
Encode = none

# Default person to mail reports to.  Can be a local account or a
# complete email address.  Variable Output should be set to mail, or
# --output mail should be passed on command line to enable mail feature.
MailTo = icosnet@localhost
# When using option --multiemail, it is possible to specify a different
# email recipient per host processed.  For example, to send the report
# for hostname host1 to user@example.com, use:
#Mailto_host1 = user@example.com
# Multiple recipients can be specified by separating them with a space.

# Default person to mail reports from.  Can be a local account or a
# complete email address.
MailFrom = Logwatch
```

Figure 108 : Configuration du format d'email.

- Nous avons modifié aussi les paramètres suivants :
  - **Range** : Pour envoyer le rapport d'hier (yesterday).
  - **Detail** : Pour envoyer le rapport complet sur les journaux des services sélectionnés (Low).
  - **Service** : Nous avons choisi de surveiller les services http,sudo, et sshd.

```
Range = yesterday

# The default detail level for the report.
# This can either be Low, Med, High or a number.
# Low = 0
# Med = 5
# High = 10
Detail = Low


# The 'Service' option expects either the name of a filter
# (in /usr/share/logwatch/scripts/services/*) or 'All'.
# The default service(s) to report on.  This should be left as All for
# most people.
Service = sudo
Service = http
Service = sshd
```

Figure 109 : Modification supplémentaires.

- Enfin, Après l'enregistrement de fichier nous devons tester le fonctionnement de Logwatch à travers les étapes suivantes :
    - Nous commençons par entrer la commande suivante pour envoyer le rapport à l'administrateur du système :

logwatch

```
[root@frontend icosnet]# logwatch
You have new mail in /var/spool/mail/icosnet
[root@frontend icosnet]#
```

Figure 110 : Envoie du rapport au système.

- Selon le résultat de la commande, le rapport a été envoyé à l'administrateur par email. Nous accédons aux emails du root « Icosnet » pour s'assurer que le message de LogWatch a été reçu, en utilisant la commande :

mail

```
N 23 logwatch@frontend.se  Tue Sep 21 13:06  53/2003  "Logwatch for frontend.selfcare.icosnet.co"
```

Figure 111 : Affichage du résultat de l'envoie d'un rapport par LogWatch.

- Voici un exemple de rapport envoyé par LogWatch pour surveiller les journaux de service sudo:

```
From root@frontend.selfcare.icosnet.com  Tue Sep 21 13:06:24 2021
Return-Path: <root@frontend.selfcare.icosnet.com>
Date: Tue, 21 Sep 2021 13:06:17 +0100
To: icosnet@frontend.selfcare.icosnet.com
From: logwatch@frontend.selfcare.icosnet.com
Subject: Logwatch for frontend.selfcare.icosnet.com (Linux)
Auto-Submitted: auto-generated
Precedence: bulk
Content-Type: text/plain; charset="iso-8859-1"
Status: R


 ################### Logwatch 7.4.3 (04/27/16) ####################
        Processing Initiated: Tue Sep 21 13:06:16 2021
        Date Range Processed: yesterday
                              ( 2021-Sep-20 )
                              Period is day.
        Detail Level of Output: 0
        Type of Output/Format: mail / text
        Logfiles for Host: frontend.selfcare.icosnet.com
 ##################################################################

 --------------------- SSHD Begin ------------------------

 SSHD Started: 2 Time(s)

 ---------------------- SSHD End -------------------------
```

Figure 112 : Exemple d'un rapport LogWatch.

- LogWatch fonctionne souvent mieux lorsqu'il est configuré pour s'exécuter quotidiennement pour envoyer ou enregistrer un rapport à afficher plus tard. Ceci peut être réalisé en configurant Logwatch pour qu'il s'exécute en tant que tâche « **cron** » en utilisant la commande suivante :

```
[root@frontend icosnet]# crontab -e
```

Figure 113 : Configuration de LogWatch en tant que tache cron.

- Nous devons ajouter une ligne pour Logwatch dans le fichier « **crontab** ». Le code suivant est configuré pour exécuter Logwatch à 00h30 chaque jour :

```
30 0  * * *          /usr/sbin/logwatch
```

Figure 114: Ajout d'un timer à LogWatch.

xi. Mise en place d'un outil d'audit de sécurité (Lynis)

L'audit périodique de la sécurité du système d'exploitation est un moyen essentiel pour identifier les vulnérabilités et veiller à ce que les mesures de sécurité existantes soient efficaces. Il existe différents outils que l'on peut utiliser afin d'évaluer le niveau de sécurité de notre système. Pour cela nous avons choisi la mise en place de Lynis pour surveiller le durcissement de notre serveur Linux.[33]

Lynis est un outil de sécurité open source qui peut effectuer une analyse approfondie de la sécurité du système afin d'évaluer le profil de sécurité du système. Il génère un rapport de sécurité récapitulatif et synthétique de l'état du système. En raison de sa simplicité et de sa flexibilité, Lynis peut être utilisé pour atteindre les objectifs suivants :

- Audit de sécurité.
- Détection de vulnérabilité.
- Durcissement du système.

[33]*Lynis - Security auditing and hardening tool for Linux/Unix. (s. d.-b). Cisofy. Consulté le 16 juin 2021, à l'adresse https://cisofy.com/lynis/*

1. Installation du Lynis :

- Pour installer Lynis, il faut juste entrer la commande :

yum install –y lynis

```
[root@frontend icosnet]# yum install lynis
Last metadata expiration check: 3:02:31 ago on Tue 22 Jun 2021 12:44:45 PM CET.
Dependencies resolved.
================================================================================
 Package        Architecture     Version                Repository      Size
================================================================================
Installing:
 lynis          noarch           3.0.1-1.el8            epel           293 k

Transaction Summary
================================================================================
Install  1 Package
```

Figure 115 : L'installation Lynis.

- Avant d'exécuter Lynis nous devons vérifier son installation:

```
[root@frontend icosnet]# lynis show version
3.0.1
```

Figure 116 : Vérification de l'installation de lynis.

- Pour exécuter un audit système de base avec Lynis, nous devons exécuter la commande ci-dessous :

Lynis audit system

- Lorsqu'il s'exécute, il affiche diverses vérifications et résultats sur avec l'écriture dans le fichier journal et les rapports :

```
[+] Initializing program
------------------------------------
  - Detecting OS...                                           [ DONE ]
  - Checking profiles...                                      [ DONE ]

  ---------------------------------------------------
  Program version:           3.0.6
  Operating system:          Linux
  Operating system name:     CentOS Linux
  Operating system version:  8
  Kernel version:            4.18.0
  Hardware platform:         x86_64
  Hostname:                  frontend
  ---------------------------------------------------
  Profiles:                  /etc/lynis/default.prf
  Log file:                  /var/log/lynis.log
  Report file:               /var/log/lynis-report.dat
  Report version:            1.0
  Plugin directory:          /usr/share/lynis/plugins
  ---------------------------------------------------
  Auditor:                   [Not Specified]
  Language:                  en
  Test category:             all
  Test group:                all
  ---------------------------------------------------
  - Program update status...                                  [ SKIPPED ]
```

Figure 117 : Exécution de Lynis.

- Lynis peut afficher OK ou AVERTISSEMENT avec OK, ce qui signifie que les vérifications sont correctes, mais s'il affiche AVERTISSEMENT, un problème est identifié dans le système qui nécessite une attention particulière. Il peut afficher aussi des suggestions pour trouver comment mettre en œuvre divers durcissements du système.
- Voici le résultat final de l'analyse du Lynis sur notre système :

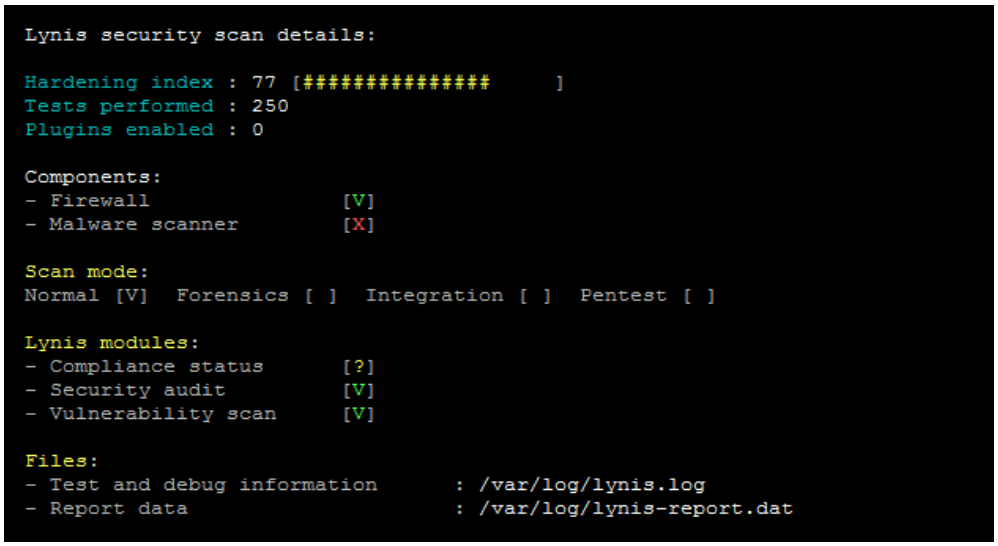


Figure 118 : Résultat du scan.

- Et pour vérifier les différentes suggestions données par Lynis on exécute la commande suivante :

grep -i "^suggestion" /var/log/lynis-report.dat

```
suggestion[]=LYNIS|This release is more than 4 months old. Check the website or
suggestion[]=AUTH-9229|Check PAM configuration, add rounds if applicable and exp
suggestion[]=AUTH-9230|Configure minimum encryption algorithm rounds in /etc/log
suggestion[]=AUTH-9230|Configure maximum encryption algorithm rounds in /etc/log
suggestion[]=AUTH-9282|When possible set expire dates for all password protected
suggestion[]=AUTH-9328|Default umask in /etc/profile or /etc/profile.d/custom.sh
suggestion[]=STRG-1846|Disable drivers like firewire storage when not used, to p
suggestion[]=NAME-4404|Add the IP name and FQDN to /etc/hosts for proper name re
suggestion[]=FIRE-4513|Check iptables rules to see which rules are currently not
suggestion[]=HTTP-6643|Install Apache modsecurity to guard webserver against web
suggestion[]=SSH-7408|Consider hardening SSH configuration|Compression (set YES
suggestion[]=SSH-7408|Consider hardening SSH configuration|LogLevel (set INFO to
suggestion[]=SSH-7408|Consider hardening SSH configuration|MaxAuthTries (set 4 t
suggestion[]=SSH-7408|Consider hardening SSH configuration|MaxSessions (set 10 t
suggestion[]=SSH-7408|Consider hardening SSH configuration|PermitRootLogin (set
suggestion[]=SSH-7408|Consider hardening SSH configuration|Port (set 22 to )|-|
suggestion[]=SSH-7408|Consider hardening SSH configuration|TCPKeepAlive (set YES
suggestion[]=SSH-7408|Consider hardening SSH configuration|AllowAgentForwarding
suggestion[]=LOGG-2154|Enable logging to an external logging host for archiving
suggestion[]=ACCT-9622|Enable process accounting|-|-|
suggestion[]=ACCT-9626|Enable sysstat to collect accounting (no results)|-|-|
suggestion[]=TOOL-5002|Determine if automation tools are present for system mana
suggestion[]=FILE-7524|Consider restricting file permissions|See screen output o
suggestion[]=KRNL-6000|One or more sysctl values differ from the scan profile an
suggestion[]=HRDN-7222|Harden compilers like restricting access to root user onl
suggestion[]=HRDN-7230|Harden the system by installing at least one malware scan
```

Figure 119 : Suggestions par Lynis.

4. Apache2 Hardening

Dans cette partie du chapitre, nous couvrirons les principales étapes de sécurisation de votre serveur Web Apache.

a. Masquage de la version Apache et l'identité du système d'exploitation :

Apache affiche par défaut la version de notre serveur web Apache installé sur notre serveur avec le nom du système d'exploitation. Il affiche également les informations sur les modules Apache installés.

Apache affiche par défaut la version de notre serveur web Apache installé sur notre serveur avec le nom du système d'exploitation. Il affiche également les informations sur les modules Apache installés.

Cela peut constituer une menace majeure pour la sécurité de notre serveur Web ainsi que de notre système d'exploitation. Pour empêcher Apache de ne pas afficher ces informations au public, nous devons apporter quelques modifications au fichier de configuration principal d'Apache.

- Premièrement, nous devons désactiver « ServerSignature ».
- Deuxièmement, dire à Apache de se renvoyer lui-même en tant que produit dans l'en-tête de réponse du serveur à chaque demande de page. « ServerTokensProd ».

```
# Supplemental configuration
ServerSignature Off
ServerTokens Prod
```

Figure 120 : Configuration du ficher Apache.

Nous pouvons le tester maintenant et vérifier si des informations sont affichées dans l'en-tête, et remarquer que rien ne s'affiche.

```
[root@frontend icosnet]# curl --head http://127.0.0.1
HTTP/1.1 403 Forbidden
Date: Mon, 21 Jun 2021 13:58:49 GMT
Server: Apache
X-Frame-Options: DENY
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Referrer-Policy: same-origin
Content-Type: text/html; charset=iso-8859-1
```

Figure 121 : Vérification de l'en-tête.

b. Désactivation de la liste des répertoires :

Par défaut Apache liste tout le contenu du répertoire racine du document en l'absence de fichier d'index. Si nous essayons d'accéder à Apache via http://localhost/selfcare_icosnet, qui représente le dossier du site web d'Icosnet. On remarque qu'il affiche tout.

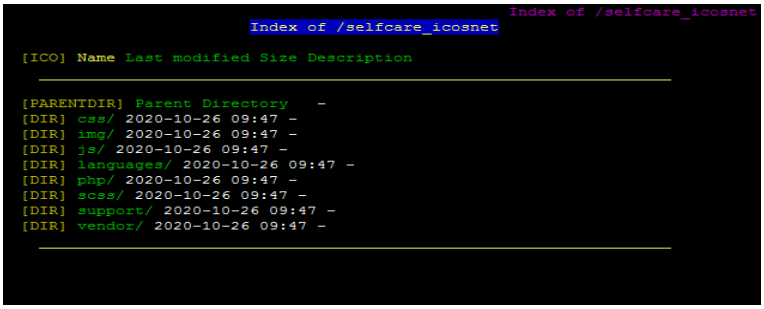


Figure 122 : Test d'accès au répertoire.

Nous pouvons le désactiver en utilisant "Options directive" dans le fichier de configuration pour un répertoire spécifique. Ainsi, le visiteur ne peut pas voir les fichiers et dossiers sous la racine ou le sous-répertoire.

```
<Directory "/var/www/html/selfcare_icosnet/">
Options -Indexes
Order deny,allow
Deny from all
</Directory>
```

Figure 123 : Configuration des directives.

Une fois la configuration du fichier terminée, nous pouvons essayer d'y accéder à nouveau via le navigateur Lynx. Une fois la configuration du fichier terminée, nous pouvons essayer d'y accéder à nouveau via le navigateur. Tous les fichiers sont désormais inaccessibles.

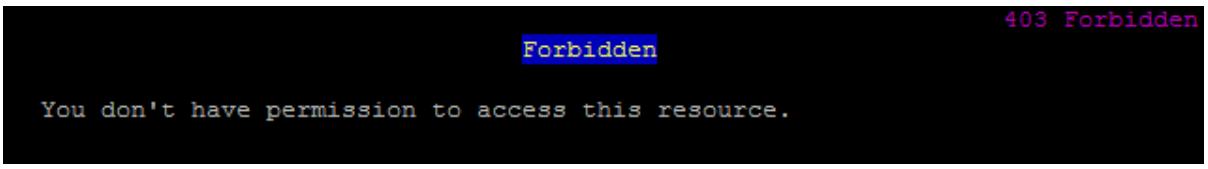


Figure 124 : Test d'accès au répertoire après la modification.

c. Exécution d'Apache en tant qu'utilisateur et groupe distincts

La configuration par défaut d'Apache est de s'exécuter en tant que "daemon". Il est efficace d'utiliser un utilisateur distinct non privilégié pour Apache. L'idée ici est de protéger les autres services en cours d'exécution en cas de faille de sécurité.

```
User http-web
Group http-web
```

Figure 125 : Configuration d'Apache en tant qu'utilisateur.

d. Installation des modules mod_security et mod_evasive

i. Mod_security :

Mod_security est un moteur de détection et de prévention des intrusions open source pour les applications Web qui s'intègre de manière transparente au serveur Web. Il fonctionne comme un pare-feu pour nos applications Web et nous permet de surveiller le trafic en temps réel, ainsi que de protéger notre serveur Web contre les attaques par force brute ou (D)DoS.[34]

Pour installer mod_security il suffit d'exécuter la commande : ***yum install*** mod_security puis de redémarrer notre serveur Apache.

Pour tester le mod_security module, nous exécutons la commande suivante : ***httpd -M | grep security***

```
[root@frontend icosnet]# httpd -M | grep security
security3 module (shared)
```

Figure 126 : Le status de mod_security.

Maintenant que l'installation de mod_security est terminée et vérifiée, on doit le configurer car il a besoin de règles pour fonctionner.

Tout d'abord, nous devons installer un Core Rule Set (CRS) afin d'utiliser mod_security. Le CRS fournit un serveur Web avec un ensemble de règles sur la façon de se comporter dans certaines conditions. La société de développement mod_security fournit un CRS gratuit appelé OWASP (Open Web Application Security Project) qui peut être téléchargé en exécutant les commandes suivantes :

sudo mkdir /etc/httpd/conf.d/modsecurity.d

sudo cd /etc/httpd/conf.d/modsecurity.d

[34] *mod_security*. (s. d.). Modsecurity.Consulté le 08 juin 2021, à l'adresse https://www.modsecurity.org/

sudo wget https://github.com/SpiderLabs/owasp-modsecurity-crs/tarball/master

sudo tar -xvf master

sudo mv SpiderLabs-owasp-modsecurity-crs-* owasp-modsecurity-crs

```
[root@frontend icosnet]# cd /etc/httpd/conf.d/modsecurity.d
[root@frontend modsecurity.d]# ls
modsecurity.conf  owasp-crs  projetrules.conf  rules.conf  unicode.mapping
```

Figure 127 : Installation de OWASP.

Ensuite, dans le répertoire OWASP CRS installé, nous trouvons un exemple de fichier avec des règles **crs-setup.conf.example**. Nous devons copier son contenu dans un nouveau fichier nommé **crs-setup.conf**.

```
LICENSE
README.md
SECURITY.md
crs-setup.conf
crs-setup.conf.example
```

Figure 128 : Fichier des règles OWASP.

Maintenant, nous informons Apache d'utiliser ce fichier avec le module. Nous pouvons le faire en éditant le fichier de configuration principal d'Apache "/**etc/httpd/conf/httpd.conf**" en ajoutant les lignes suivantes :

```
<IfModule security2_module>
        Include /etc/httpd/conf.d/modsecurity.d/owasp-crs/crs-setup.conf
        Include /etc/httpd/conf.d/modsecurity.d/owasp-crs/rules/*.conf
</IfModule>
```

Figure 129 : Configuration de mod_security dans le fichier config d'Apache.

Une fois que tout est configuré correctement, nous allons tester mod_security avec les règles OWASP en envoyant des requêtes malveillantes au serveur Web Apache et voir si les requêtes sont bloquées ou non.

Tous d'abord, nous allons tester comment mod_security protège le serveur Web Apache de quelques attaques malveillantes. Sur un navigateur chrome. Nous entrons les urls suivantes pour tester l'attaque XSS :

1. Si un attaquant essaye d'entrer un url qui contient un script d'attaque XSS, mod_security bloque l'url et une page « Forbidden » sera affichée :

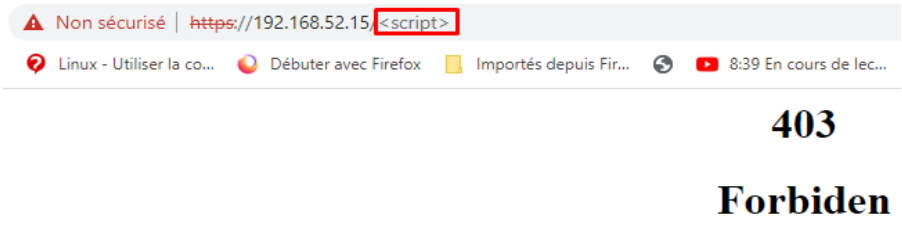


Figure 130 : Test sur le fonctionnement de mod_securité.

2. Ensuite, nous vérifions que mod_security envoi des alertes dans le fichier des logs de mod_security avec la commande suivante :

tail -f /var/log/httpd/modsec_audit.log

Une alerte d'une attaque XSS s'affiche dans le fichier "**modsec_audit.log**" comme suite :

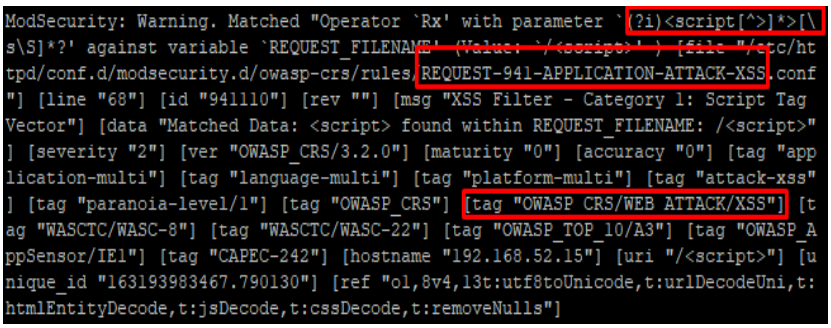


Figure 131 : Alerte d'attaque XSS.

3. Et si nous testons avec une injection sur une commande, nous aurons ce résultat (voir la figure 133) :

Figure 132 : Injection sur la commande.

4. Et si nous testons avec une injection SQL, nous aurons ce résultat :

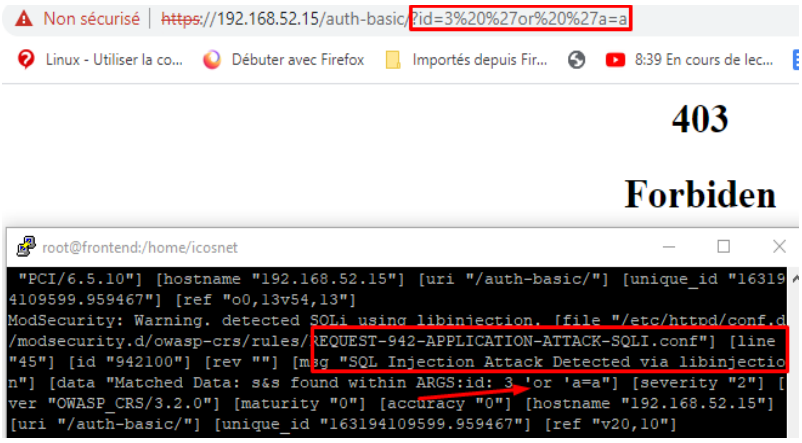


Figure 133 : Injection SQL.

ii. Mod_evasive :

Mod_evasive empêche les attaques DDOS de faire autant de dégâts par la façon dont il traite les requêtes. Cette fonctionnalité lui permet de gérer la force brute HTTP et l'attaque DDos.[35]

Nous devons également le configurer. Pour cela, il faut modifier le fichier de configuration d'Apache (voir la figure 131).

[35] *mod_evasive*. (s. d.). Debian Wiki.Consulté le 09 juin 2021 A l'adresse https://wiki.debian.org/fr/Apache/mod_evasive

```
#mod_evasive config
<IfModule mod_evasive24.c>
DOSHashTableSize 3097
DOSPageCount 2
DOSSiteCount 50
DOSPageInterval 1
DOSSiteInterval 1
DOSBlockingPeriod 10
DOSEmailNotify z.ounnoughi@gmail.com
DOSLogDir "/var/log/mod_evasive"
</IfModule>
# Load config files in the "/etc/httpd/conf.d" directory, if any.
IncludeOptional conf.d/*.conf
LoadModule security3_module /usr/lib64/httpd/modules/mod_security3.so
LoadModule evasive20_module   /usr/lib64/httpd/modules/mod_evasive24.so
```

Figure 134 : Ajouter le mod_evasive dans la configuration d'Apache.

- DOSHashTableSize : nombre de nœuds de niveau supérieur pour la table de hachage de chaque enfant.
- DOSPageCount : nombre de demandes pour la même page par intervalle de page avant qu'une adresse IP ne soit bloquée.
- DOSSiteCount : nombre de demandes pour un objet par le même client par intervalle de site avant que l'adresse IP ne soit bloquée.
- DOSPageInterval : intervalle utilisé dans le seuil de nombre de pages (mesuré en secondes).
- DOSSiteInterval : intervalle utilisé dans le seuil de nombre de sites (mesuré en secondes).
- DOSBlockingPeriod : période (en secondes) pendant laquelle une IP est bloquée. Pendant ce temps, toutes les demandes provenant de l'adresse IP affectée reçoivent une redirection 403.

Une fois que tout est configuré correctement, nous pouvons tester pour voir si le module fonctionne correctement. Nous utiliserons le script test.pl écrit par les développeurs de mod_evasive pour tester mod_evasive.

```
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
```

Figure 135 : Test sur le fonctionnement de mod_evasive partie 2.

```
Sep 27 00:58:50 frontend mod_evasive[40874]: Blacklisting address 192.168.52.15: possible DoS attack.
Sep 27 00:58:50 frontend mod_evasive[40874]: Blacklisting address 192.168.52.15: possible DoS attack.
```

Figure 136 : Test sur le fonctionnement de mod_evasive partie 1.

a. Sécuriser Apache avec des certificats SSL :

Nous pouvons sécuriser toutes nos communications de manière cryptée sur Internet avec un certificat SSL. Grâce à cette technologie, les serveurs peuvent envoyer en toute sécurité des informations à leurs clients sans que leurs messages soient interceptés ou lus par un tiers.

Sur cette partie, nous allons créer et utiliser un certificat SSL auto-signé avec le serveur web Apache.

1. Tout d'abord, nous devons ouvrir les ports http et https et dans notre cas nous l'avons déjà fait précédemment sur notre configuration Iptables. Nous pouvons vérifier les ports ouverts à l'aide de la commande "nmap rhel8".
2. Ensuite, nous devons installer mod_ssl, un module Apache qui prend en charge le cryptage SSL. Une fois l'installation terminée, nous devons redémarrer le serveur httpd et ainsi le module mod_ssl est activé et prêt à être utilisé. Nous pouvons le faire en utilisant ces commandes :

   sudo dnf install mod_ssl

   sudo systemctl restart httpd
3. Nous pouvons maintenant passer à la génération d'un nouveau certificat SSL. Le certificat stockera des informations de base sur notre site et sera accompagné d'un fichier clé qui permet au serveur de gérer en toute sécurité les données cryptées. Nous pouvons le créer la commande openssl :

sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/pki/tls/private/apache-selfsigned.key -out /etc/pki/tls/certs/apache-selfsigned.crt

4. Nous serons amenés à une invite où nous pourrons entré des informations sur notre serveur. La ligne la plus importante est celle qui demande le « Common Name ». Nous avons besoin de l'IP du serveur. Il est important que ce champ corresponde à tout ce que nous mettons dans la barre d'adresse de notre navigateur pour accéder au site. Et voici le résultat (voir la figure 133) :

```
[root@frontend ~]#     openssl req -x509 -nodes -days 365 -newkey rsa:204
8 -keyout /etc/pki/tls/private/apache-selfsigned.key -out /etc/pki/tls/ce
rts/apache-selfsigned.crt
Generating a RSA private key
................+++++
...+++++
writing new private key to '/etc/pki/tls/private/apache-selfsigned.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a D
N.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:dz
State or Province Name (full name) []:Algiers
Locality Name (eg, city) [Default City]:Algiers
Organization Name (eg, company) [Default Company Ltd]:ICOSNET
Organizational Unit Name (eg, section) []:Division Technique
Common Name (eg, your name or your server's hostname) []:127.0.0.1
Email Address []:z.ounnoughi@gmail.com
```

Figure 137 : Génération d'un certificat SSL.

5. Maintenant que nous avons notre certificat auto-signé et notre clé disponible, nous devons mettre à jour notre configuration Apache pour l'utiliser. Nous allons créer un fichier dans le répertoire /etc/httpd/conf.d avec la configuration suivante :

```
<VirtualHost *:443>
    ServerName 127.0.0.1
    DocumentRoot  /var/www/html/selfcare_icosnet
    SSLEngine on
    SSLCertificateFile /etc/pki/tls/certs/apache-selfsigned.crt
    SSLCertificateKeyFile /etc/pki/tls/private/apache-selfsigned.key
</VirtualHost>
```

Figure 138 : Création d'un fichier de configuration de SSL.

6. On peut alors vérifier la configuration pour les erreurs de syntaxe par la commande suivante :

sudo apachectl config test

Actuellement, notre configuration ne répond qu'aux requêtes HTTPS sur le port 443. Nous allons la configurer pour qu'elle réponde également sur le port 80 en ajoutant un bloc correspondant à ces requêtes, si nous voulons forcer le chiffrement de tout le trafic.

```
<VirtualHost *:80>
    ServerName selfcare_icosnet
    Redirect / https://127.0.0.1/
</VirtualHost>
```

Figure 139 : Ajout de la configuration sur le port 80.

7. Nous sauvegardons et fermons ce fichier lorsque nous avons terminé, puis testons à nouveau notre syntaxe de configuration, et rechargeons Apache.
8. Nous pouvons tester la nouvelle fonctionnalité de redirection en visitant notre site avec http://127.0.0.1. Il devrait être redirigé vers https:// automatiquement.

Figure 140 : Test sur la redirection vers https.

5. Conclusion

Dans ce dernier chapitre, nous sommes passés à la prochaine étape nécessaire, qui consiste à augmenter le niveau de sécurité des serveurs d'Icosnet. Nous avons passés en revue toutes les mesures résultant de notre analyse antérieure, et nous avons sécurisé les entités internes et externes de leur système d'exploitation et de leur serveur. Et même fourni des outils supplémentaires pour renforcer leur sécurité.

Conclusion

Dans ce travail, notre motivation a été essentiellement de prouver que le processus de gestion des risques est devenu une priorité absolue pour les entreprises. La GRC s'est avéré non seulement un sujet important dans le monde des affaires et de la technologie, mais elle peut également aider une entreprise à gérer son système d'informations, à démontrer sa conformité et à réduire les risques. La gestion des risques a créé de la valeur et est devenue partie intégrante du processus organisationnel. Comme elle fait également partie du processus décisionnel et doit être adapté à chaque entreprise.

Notre travail a commencé par présenter dans un premier temps notre structure d'accueil Icosnet, pour bien connaître l'entreprise ainsi que son environnement, notamment ses serveurs car ils sont notre principal intérêt.

Nous avons ensuite fourni un chapitre entier sur la gestion des risques, ses facteurs, ses principes et son processus de manière approfondie. Nous avons donné un aperçu des différentes normes standard qui initient la mise en œuvre d'un processus de gestion des risques de sécurité de l'information.

Plus loin dans notre étude, nous avons examiné différentes méthodes et stratégies de gestion des risques en décrivant les caractéristiques structurelles des normes et des méthodes mises en œuvre dans le système de gestion de la sécurité de l'information pour nous aider à choisir la méthode la plus précise et la plus appropriée pour notre projet. Notre choix s'est porté sur Ebios, car non seulement il permet d'évaluer les risques numériques et d'identifier les mesures de sécurité à prendre pour les maîtriser, il est également compatible avec les 2 normes les plus importantes pour notre étude (ISO 27001 et 27005).

A l'aide d'EBIOS, notre étude est entrée dans une couverture exhaustive avec la détermination de concepts, d'objectifs et d'exigences de sécurité. Elle a pris en compte toutes les entités techniques et non techniques. Dans la première étape de la méthode, nous avons traité l'analyse du contexte en termes de décomposition pertinente. Nous avons ensuite mené à la fois une analyse des besoins de sécurité et une analyse des menaces dans leur nature conflictuelle aux étapes 2 et 3. Enfin, aux étapes 4 et 5, nous avons diagnostiqué les risques et indiqué les mesures pour les couvrir et rendu explicites et connus les risques résiduels.

Après avoir établi notre processus de gestion des risques, nous sommes passés à la prochaine étape nécessaire, qui consiste à augmenter le niveau de sécurité des serveurs d'Icosnet. Nous avons également passés en revue toutes les mesures résultant de notre analyse antérieure, et nous avons sécurisé les entités internes et externes de leur système d'exploitation et de leur serveur. Et même fourni des outils supplémentaires pour renforcer leur sécurité.

Enfin, nous avons pu atteindre notre objectif et renforcer la sécurité des serveurs d'Icosnet, et atteindre un niveau intermédiaire. Tout en fournissant une étude qui peut aider les futurs projets de l'entreprise.

Il est clair que ce stage effectué au sein de l'entreprise Icosnet nous a permis d'enrichir nos connaissances et compétences théoriques dans le domaine de la sécurité de l'information et de les mettre en pratique dans le monde professionnel. De plus, cela nous a permis de maîtriser parfaitement la gestion des risques et de visualiser facilement les solutions aux menaces.

Bibliographie

[1] Wikipedia contributors. (s. d.). Gouvernance, gestion des risques et conformité. Wikipedia. Consulté le 12 mars 2021, à l'adresse https://fr.wikipedia.org/wiki/Gouvernance,_gestion_des_risques_et_conformité

[2] Risque. (s. d.). Dans *Oxford English Dictionary*.

[3] Institute of Risk Management (IRM).(2002). *A Risk Management Standard*.https://www.theirm.org

[4] ISO Guide 73. (2009). Risk management – Vocabulary – Guidelines for use in standards, www.iso.org

[5] SRY Ahmad, "Analysis of User Acceptance of the Application of Information Systems Using the Technology Acceptance Model," Thesis, vol. 4, pp. 924–929, 2012.

[6] National Interagency Fire Center (NIFC).(2009, février).*Guidance for Implementation of Federal Wildland Fire Management Policy*.https://www.nifc.gov

[7] *Risk Management Plan*. (2015). https://www.phe.gov

[8] Wikipedia contributors. (s. d.). International Organization for Standardization. Wikipedia. Consulté le 10 avril 2021, à l'adressehttps://en.wikipedia.org/wiki/International_Organization_for_Standardization

[9] Wikipedia contributors. (s. d.). International Electrotechnical Commission.Wikipedia. Consulté le 11 avril 2021, à l'adresse https://en.wikipedia.org/wiki/International_Electrotechnical_Commission

[10] International Organization for Standardization, I. S. O. (s. d.).*ISO/IEC 27001:2013*. ISO.https://www.iso.org

[11] International Organization for Standardization, I. S. O. (s. d.).*ISO/IEC 27002:2013*. ISO.https://www.iso.org

[12] International Organization for Standardization, I. S. O. (s. d.-c).*ISO/IEC 27005:2011*. ISO.https://www.iso.org

[13] OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) - CIO Wiki. (s. d.). CIO WIKI. Consulté le 25 avril 2021, à l'adresse https://cio-wiki.org/wiki/OCTAVE_(Operationally_Critical_Threat,_Asset_and_Vulnerability_Evaluation

[14] *MEHARI 2010 Risk analysis and treatment Guide*. (2010, août). https://mehari.info

[15] Agence nationale de la sécurité des systèmes d'information, A. N. S. S. I. (s. d.). EBIOS — Expression des Besoins et Identification des Objectifs de Sécurité. ANSSI. https://www.ssi.gouv.fr

[16] Agence nationale de la sécurité des systèmes d'information, A. N. S. S. I. (s. d.-b). *La méthode EBIOS Risk Manager – Le guide*. ANSSI. https://www.ssi.gouv.fr

[17] Présentation Icosnet. (s. d.). Icosnet. Consulté le 2 mars 2021, à l'adresse https://icosnet.com.dz/qui-sommes-nous/

[18] *Accueil*. (s. d.). Icosnet. Consulté le 2 mars 2021, à l'adresse https://icosnet.com.dz/

[19] Wikipedia contributors. (s. d.). PHP.Wikipedia. Consulté le 12 mai 2021, à l'adresse https://en.wikipedia.org/wiki/PHP

[20] ANSSI. (2019, February). *Recommandation de configuration d'un système GNU/LINUX*. https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf

[21] CIS.(2021, May).*CIS CentOS linux 8 benchmark*.

[22] Guide technique relatif à la sécurité du serveur Linux. (2014). Direction généralle de la sécurité des systèmes d'information. https://www.dgssi.gov.ma/sites/default/files/attached_files/guide_linux-v14-12-2015.pdf

[23] Wikipedia contributors. (s. d.-e). Linux PAM. Wikipedia. Consulté le 25 juin 2021, à l'adresse https://en.wikipedia.org/wiki/Linux_PAM

[24] Dorigny, M. (s. d.). Sécuriser l'édition du GRUB | Commandes et Système. IT-Connect. Consulté le 21 juin 2021, à l'adresse https://www.it-connect.fr/securiser-ledition-du-grub

[25] Brown, K. (2020, août 27). The Beginner's Guide to iptables, the Linux Firewall.How-To Geek.https://www.howtogeek.com/177621/the-beginners-guide-to-iptables-the-linux-firewall/

[26] Fail2ban. (s. d.). Fail2ban. Consulté le 10 juin 2021, à l'adresse https://www.fail2ban.org/wiki/index.php/Main_Page

[27] Logwatch - ArchWiki. (s. d.). Archlinux. Consulté le 12 juin 2021, à l'adresse https://wiki.archlinux.org/title/Logwatch

[28] Lynis - Security auditing and hardening tool for Linux/Unix. (s. d.-b). Cisofy. Consulté le 16 juin 2021, à l'adresse*https://cisofy.com/lynis/*

[29] *mod_security*. (s. d.). Modsecurity. Consulté le 08 juin 2021, à l'adresse https://www.modsecurity.org/

[30] *mod_evasive*. (s. d.). Debian Wiki. Consulté le 09 juin 2021 A l'adresse https://wiki.debian.org/fr/Apache/mod_evasive