RÉPUBLIQUE DÉMOCRATIQUE DU CONGO
MINISTÈRE DE L'ENSEIGNEMENT
SUPÉRIEUR ET UNIVERSITAIRE

" MISE EN PLACE D'UN SYSTÈME DE SECURITE DANS UN SERVEUR WEB "

Par :**Tshibangu Ntumba Kenny**

Travail de fin d'études présenté en vue de l'obtention du grade
de licencié en Sciences Informatiques

Option : Réseau et Infrastructure

Année Académique 2022-2023

Table des matières

Introduction Générale

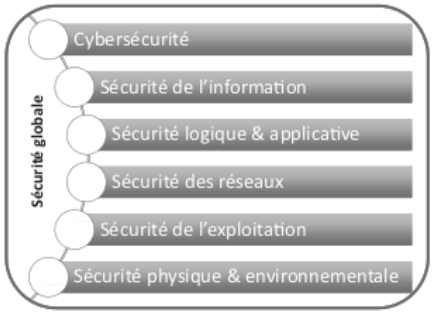
0.1 Quelques petites Définition

0.1.1 La Securite Informatique

La sécurité informatique est l'ensemble des mesures techniques, organisationnelles et juridiques mises en place pour protéger les systèmes informatiques, les réseaux et les données contre les attaques, les pertes ou les altérations. Elle vise à garantir la confidentialité, l'intégrité et la disponibilité des informations stockées sur les systèmes informatiques, ainsi que la protection de la vie privée et des droits de propriété intellectuelle.

La sécurité informatique englobe un large éventail de domaines, tels que la sécurité des réseaux, la sécurité des systèmes d'exploitation, la sécurité des applications, la sécurité des données, la sécurité physique, la gestion des identités et des accès, la conformité aux normes de sécurité, la surveillance et la détection des incidents de sécurité, ainsi que la réponse aux incidents de sécurité.

La sécurité informatique est devenue un enjeu majeur dans le monde numérique d'aujourd'hui, où les attaques informatiques sont de plus en plus sophistiquées et fréquentes. La mise en place d'une politique de sécurité informatique efficace est donc essentielle pour protéger les systèmes informatiques et les données sensibles contre les menaces potentielles et assurer la continuité des activités des organisations qui les utilisent.



La sécurité informatique englobe plusieurs domaines d'applications :

- sécurité physique et environnementale ;
- sécurité de l'exploitation ;
- sécurité des réseaux ;
- sécurité logique, sécurité applicative et sécurité de l'information ;
- cybersécurité.

0.1.2 La Cyber Sécurité

La cybersécurité, également appelée sécurité informatique ou sécurité des technologies de l'information, est l'ensemble des mesures techniques, organisationnelles et juridiques mises en place pour protéger les systèmes informatiques, les réseaux et les données contre les attaques, les pertes ou les altérations. Elle vise à garantir la confidentialité, l'intégrité et la disponibilité des informations stockées sur les systèmes informatiques, ainsi que la protection de la vie privée et des droits de propriété intellectuelle.

La cybersécurité concerne la sécurité informatique et des réseaux des environnements connectés à Internet et accessibles via le cyberespace. Elle peut être mise en défaut, entre autres, par des cyberattaques informatiques. Du fait de l'usage extensif d'Internet, de nouvelles menaces sont apparues générant des risques additionnels dont les impacts, de niveaux d'importance variables, peuvent affecter les individus, les organisations ou les États.

La cybersécurité est devenue un enjeu majeur dans le monde numérique d'aujourd'hui, où les attaques informatiques sont de plus en plus sophistiquées et fréquentes. Elle est essentielle pour protéger les systèmes informatiques et les données sensibles contre les menaces potentielles et assurer la continuité

des activités des organisations qui les utilisent. La cybersécurité est également importante pour protéger les utilisateurs finaux, tels que les consommateurs et les employés, contre les risques de vol d'identité, de fraude en ligne et d'autres formes de cybercriminalité.

Les points essentiels englobés par la cybersécurité comprennent :

1. La confidentialité :

la protection des données contre les accès non autorisés. Cela inclut la protection des données personnelles, des secrets commerciaux, des informations financières et autres informations sensibles.

2. L'intégrité :

la protection des données contre les altérations non autorisées. Cela inclut la garantie que les données sont exactes et fiables.

3. La disponibilité :

la garantie que les systèmes, les réseaux et les données sont accessibles et fonctionnent correctement, et que les interruptions de service sont minimisées.

4. L'authenticité :

la garantie que les utilisateurs sont bien ceux qu'ils prétendent être, et que les données sont bien celles qu'elles prétendent être.

5. La non-répudiation :

la garantie qu'une personne ne peut pas nier avoir effectué une action ou avoir envoyé des données.

6. La résilience :

la capacité des systèmes et des réseaux à résister aux attaques et à récupérer rapidement en cas d'incident.

7. La conformité :

le respect des lois, des réglementations et des normes en matière de sécurité informatique.

8. La sensibilisation :

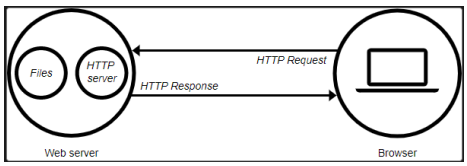
l'éducation et la formation des utilisateurs pour qu'ils comprennent les risques liés à la sécurité informatique et les meilleures pratiques à suivre pour les éviter.

Ces points essentiels sont interconnectés et doivent être pris en compte dans toute stratégie de cybersécurité efficace.

0.1.3 Quelques mots sur les Serveurs

Les serveurs sont des ordinateurs ou des systèmes informatiques qui fournissent des services ou des ressources à d'autres ordinateurs ou utilisateurs sur un réseau. Ils peuvent être utilisés pour stocker des données, héberger des sites Web, exécuter des applications et bien plus encore. Il existe différents types de serveurs, tels que les serveurs de fichiers, les serveurs de messagerie, les serveurs de bases de données et les serveurs de jeux en ligne. Les serveurs sont souvent utilisés pour fournir des services à distance, ce qui permet aux utilisateurs d'y accéder à partir de n'importe où dans le monde.

0.1.4 Les Serveurs Web



Les serveurs Web sont des ordinateurs ou des programmes informatiques qui fournissent des pages Web aux clients qui les demandent via un navigateur Web. Ils sont utilisés pour héberger des sites Web et distribuer du contenu en ligne. Les serveurs Web peuvent exécuter différents types de logiciels, tels que Apache, Nginx, Microsoft IIS et bien d'autres. Les pages Web sont généralement créées en utilisant des langages de programmation Web tels que HTML, CSS et JavaScript. Les serveurs Web peuvent également exécuter des applications Web, telles que des forums en ligne, des blogs, des magasins en ligne et bien plus encore.

0.1.5 Quelques vulnérabilités Sur Les Serveurs Web

Il y a plusieurs vulnérabilités qui peuvent affecter un serveur web, en voici quelques exemples :

• Injection SQL : Cette vulnérabilité permet à un attaquant d'injecter du code SQL malveillant dans une requête pour détourner le contrôle de la base de données.

• Cross-site scripting (XSS) : Cette vulnérabilité permet à un attaquant d'injecter du code malveillant dans une page Web pour voler des informations d'authentification ou d'autres données sensibles.

• Vulnérabilités du serveur HTTP : Les serveurs HTTP tels que Apache, Nginx et IIS peuvent être vulnérables à des attaques telles que les dénis de service (DoS) et les dénis de service distribués (DDoS).

• Mauvaise configuration : Une mauvaise configuration du serveur web peut permettre aux attaquants d'accéder aux fichiers sensibles ou d'exécuter du code malveillant.

• Vulnérabilités du CMS : Les systèmes de gestion de contenu tels que WordPress et Drupal peuvent être vulnérables à des attaques telles que les injections SQL et les attaques de force brute.

0.2 Contexte de recherche

Ce travail s'appuie sur les différents domaines de la Cybersécurité qui actuellement est déjà devenu un des points plus important dans le domaine de l'informatique Une Solution simple et pratique peut être proposée ; Pour rendre le serveur Plus sur et plus sécurisé

0.3 Solution technique

La solution la plus proche et la moins vorace en ressource serait de mettre en place un système de securite qui respecte le nécessaire des normes de securites dans un serveur web actuel.

0.4 Problématique

Sur un Serveur web il existe plusieurs sortes de vulnérabilités par lesquels on peut facilement y accéder Comme :

•**L'injection SQL :** en bref c'est une attaque qui consiste a insérer du code SQL malveillant dans les entrées d'un formulaires ...

• **Cross-Site Scripting(XSS) :** Comme son nom l'indique c'est une faille de securite qui permet un attaquant d'injecter du code malveillant dans une page web ou de faire une redirection vers un site frauduleux

Et j'en passe ;

Voici les quelques questions que nous allons nous poser tout au long de ce travail :

– Quel est le descriptif d'un bon système de securite ?

– Quels sont les systèmes de securites que nous allons utiliser ?

– Sur quel type de serveur web ce système sera efficace ?

0.5 Méthodologie

Pour arriver a une solution plausible nous allons utiliser une procédure qui va nous permettre d'installer des machines virtuelles ; différentes machines virtuelles configurée de différentes façon ; et tester différentes approches de sécurisation de serveurs et même essayer de les combinées pour voir si le résultat est solide .

0.6 Techniques

Pour ce travail la technique appropriée sera :

0.6.1 La Recherche sur Internet :

Parcourir les différents sites et forums qui proposent des travaux similaires aux miens , des vidéos et tutoriels pour les différentes configurations a faire pour ce travail ...

0.6.2 La Recherche Documentaire :

Utiliser les différents livres,revues ,archives ; Qui , en les utilisant pourront m'aider a atteindre mon but , ma solution solide .

0.6.3 La Recherche Expérimentale :

Faire des petites expérimentation sur mes machines virtuelles configurées comme des serveurs web

0.7 Limitation

Dans ce travail nous allons nous limiter a utiliser :

(En fonction de l'évolution de mon travail ce point va se remplir).

0.8 Objectif

L'objectif visé dans ce travail est de pouvoir mettre en place un système de securite capable de remplir le travail nécessaire qui est actuellement demandé sur les serveurs web ;

De configurer un serveur web assez performant pour remplir les prérequis nécessaire qui sont demandés par la communauté des développeurs Web qui sont majoritairement amenés a utiliser les Serveurs Web Pour héberger leurs sites internet .

Chapitre 1

Prochain Chapitre