Introduction Générale

Pour Rappel mon sujet c'est la :"Mise en Place d'un système de securite dans un Serveur WEB"

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.

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 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 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.

0.1.3 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