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

Contents

Abstract

Chapter 1

Introduction Générale

1.1 La cybersécurité

est la pratique consistant à protéger les systèmes, les réseaux et les données contre tout accès, utilisation, divulgation, perturbation, modification ou destruction non autorisés.
C'est un domaine critique dans le monde d'aujourd'hui, car notre dépendance à l'égard de la technologie ne cesse de croître.

Les serveurs sont des composants essentiels de toute infrastructure de cybersécurité. Ils fournissent un emplacement central pour le stockage et le traitement des données et peuvent être utilisés pour héberger des applications et des services utilisés par les employés, les clients et les partenaires.

Ce travail fournira une introduction à la cybersécurité et aux serveurs.
Il couvrira les sujets suivants :

- Les bases de la cybersécurité
- Les différents types de serveurs
- Les défis de sécurité associés aux serveurs
- Les bonnes pratiques de sécurisation des serveurs

À la fin de ce travail, vous aurez une compréhension de base de la cybersécurité et des serveurs.
Vous serez en mesure d'identifier les risques de sécurité associés aux serveurs et vous serez en mesure de mettre en place les meilleures pratiques pour protéger vos serveurs.

1.1.1 Pourquoi la cybersécurité est-elle importante ?

La cybersécurité est importante car elle protège notre infrastructure critique, nos informations personnelles et nos actifs financiers. Ces dernières années, un certain nombre de cyberattaques très médiatisées ont causé des dommages importants.
Par exemple, l'attaque du ransomware WannaCry en 2017 a infecté plus de 200 000 ordinateurs dans 150 pays.
L'attaque a causé des milliards de dollars de dégâts et perturbé des services essentiels tels que les hôpitaux et les écoles.

1.2 Qu'est-ce qu'un serveur ?

Un serveur est un ordinateur qui fournit des ressources à d'autres ordinateurs sur un réseau.
Les serveurs peuvent être utilisés pour stocker des données, exécuter des applications et fournir des services tels que la messagerie électronique, le partage de fichiers et l'impression.

1.2.1 Les défis de sécurité associés aux serveurs

Les serveurs sont une cible courante pour les cyberattaques car ils contiennent des données précieuses et sont souvent connectés à Internet.
Certains des défis de sécurité associés aux serveurs incluent :

- Malware : un malware est un logiciel conçu pour endommager un système informatique. Les logiciels malveillants peuvent être utilisés pour voler des données, installer des portes dérobées ou perturber les opérations.

- Phishing : Le phishing est un type d'attaque d'ingénierie sociale qui est utilisé pour inciter les utilisateurs à révéler leurs informations personnelles, telles que des mots de passe ou des numéros de carte de crédit.

- Attaques par déni de service (DoS) : les attaques DoS sont conçues pour submerger un serveur de trafic, le rendant indisponible pour les utilisateurs légitimes.

•Violations de données : Les violations de données sont des incidents au cours desquels des données sensibles sont volées dans un système informatique. Les violations de données peuvent avoir un impact significatif sur les entreprises, car elles peuvent entraîner des pertes financières, la perte de clients et une atteinte à la réputation.

1.2.2 Les meilleures pratiques pour sécuriser les serveurs :

Il existe un certain nombre de meilleures pratiques qui peuvent être utilisées pour sécuriser les serveurs. Certaines des meilleures pratiques les plus importantes incluent :

•Maintenez vos logiciels à jour : les mises à jour logicielles incluent souvent des correctifs de sécurité qui peuvent aider à protéger votre serveur contre les vulnérabilités connues.

•Utilisez des mots de passe forts : Les mots de passe doivent comporter au moins 12 caractères et doivent inclure un mélange de lettres majuscules et minuscules, de chiffres et de symboles.

•Activer l'authentification à deux facteurs : L'authentification à deux facteurs ajoute une couche de sécurité supplémentaire en demandant aux utilisateurs de saisir un code sur leur téléphone en plus de leur mot de passe.

•Utilisez un pare-feu : Un pare-feu peut aider à protéger votre serveur contre tout accès non autorisé. Sauvegardez vos données régulièrement : Des sauvegardes régulières peuvent aider à minimiser les dommages causés par une violation de données.

En suivant ces meilleures pratiques, vous pouvez aider à protéger vos serveurs contre les cyberattaques.

1.3 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

1.4 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.

1.5 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 ?

1.6 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 .

1.7 Techniques

Pour ce travail la technique appropriée sera :

1.7.1 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 ...

1.7.2 La Recherche Documentaire :

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

1.7.3 La Recherche Expérimentale :

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

1.8 Limitation

Dans ce travail nous allons nous limiter a utiliser :

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

1.9 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 .

Chapter 2

Les Serveurs

2.1 Définitions

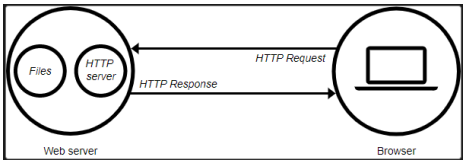
Les serveurs sont des ordinateurs ou des systèmes informatiques qui fournissent des services ou des ressources à d'autres ordinateurs ou utilisateurs sur un réseau. Ils peuvent être utilisés pour stocker des données, héberger des sites Web, exécuter des applications et bien plus encore. Il existe différents 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. Dans ce point ci-après nous allons la plupart des sortes de serveurs les plus repandus

Sortes De Serveur

1. Serveur Web
2. Serveur de Messagerie
3. Serveur de fichiers

4. Serveur de base de données
5. Serveur d'applications
6. Serveur de virtualisation
7. Serveur DNS
8. Serveur de sauvegarde
9. Serveur de jeu
10. Serveur de médias

2.2 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.

2.2.1 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.

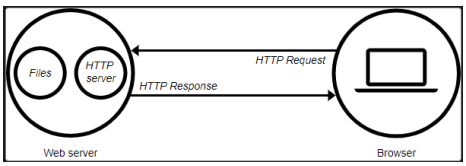
• Vulnérabilités du serveur HTTP : Les serveurs HTTP tels que Apache, Nginx et IIS peuvent être vulnérables à des attaques telles que les dénis de service (DoS) et les dénis de service distribués (DDoS).

• 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.

Il est important de mettre en place des mesures de sécurité adéquates pour protéger les serveurs web contre ces vulnérabilités potentielles, telles que la mise à jour régulière de la sécurité du système et l'utilisation de logiciels de sécurité pour détecter et prévenir les attaques potentielles.
Les développeurs de sites web doivent également être conscients des meilleures pratiques de sécurité, telles que la validation des entrées utilisateur et l'utilisation de l'encodage pour se protéger contre les attaques XSS.

2.3 Serveurs de Messageries



Un serveur de messagerie est un type de serveur qui est utilisé pour envoyer et recevoir des courriers électroniques (e-mails). Les serveurs de messagerie sont essentiels pour le fonctionnement du courrier électronique car ils sont responsables de la distribution des messages entre les différents utilisateurs.

Il existe deux types principaux de serveurs de messagerie : le serveur SMTP (Simple Mail Transfer Protocol) et le serveur POP (Post Office Protocol).

Le serveur SMTP est utilisé pour envoyer des courriers électroniques. Lorsqu'un utilisateur envoie un e-mail, le client de messagerie envoie le message au serveur

SMTP, qui se charge de le transférer au serveur de messagerie du destinataire.

Le serveur POP est utilisé pour récupérer les courriers électroniques sur le serveur de messagerie. Les clients de messagerie utilisent le protocole POP pour se connecter au serveur de messagerie et récupérer les messages qui leur sont destinés.

Il existe également un autre protocole appelé IMAP (Internet Message Access Protocol) qui est utilisé pour accéder aux messages sur le serveur de messagerie sans les télécharger sur l'ordinateur local. IMAP permet aux utilisateurs de se connecter à leur boîte de réception depuis n'importe quel ordinateur ou appareil connecté à Internet.

Les serveurs de messagerie peuvent être configurés pour fournir des fonctionnalités supplémentaires telles que la sécurité des messages, la gestion des spams et des virus, la gestion des listes de diffusion, etc. Les serveurs de messagerie sont également souvent intégrés à des suites de collaboration pour permettre le partage de calendriers, de contacts, de tâches, etc.

2.3.1 Quelques vulnérabilités Sur Les Serveurs de Messageries

Il existe plusieurs vulnérabilités potentielles qui peuvent affecter les serveurs de messagerie. Voici quelques exemples :

•Injection de code : Les attaquants peuvent exploiter des vulnérabilités dans le serveur de messagerie pour injecter du code malveillant dans les e-mails, qui peuvent ensuite être utilisés pour exécuter des attaques de phishing, des attaques de logiciels malveillants ou d'autres types d'attaques.

• Attaques de force brute : Les attaquants peuvent tenter de deviner les identifiants de connexion des utilisateurs en utilisant des attaques de force brute, qui impliquent l'utilisation de programmes pour tester toutes les combinaisons de noms d'utilisateur et de mots de passe possibles.

• Attaques par déni de service (DoS) : Les attaquants peuvent lancer des attaques par déni de service (DoS) contre le serveur de messagerie pour le rendre indisponible, ce qui peut empêcher les utilisateurs d'accéder à leurs e-mails ou de les envoyer.

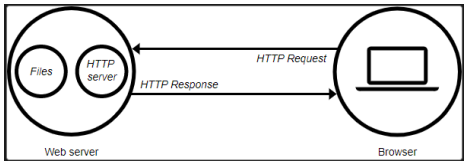
•Vulnérabilités de sécurité : Les serveurs de messagerie peuvent avoir des vulnérabilités de sécurité connues qui peuvent être exploitées par les attaquants pour accéder à des données sensibles, tels que des courriels confidentiels ou des informations d'identification.

•Vulnérabilités de configuration : Les serveurs de messagerie peuvent avoir des vulnérabilités de configuration qui peuvent être exploitées par les attaquants

pour accéder à des données sensibles, tels que des listes de contacts, des calendriers et des tâches.

Il est important de mettre en place des mesures de sécurité adéquates pour protéger les serveurs de messagerie contre ces vulnérabilités potentielles, telles que la mise à jour régulière de la sécurité du système et l'utilisation de logiciels de sécurité pour détecter et prévenir les attaques potentielles.
Les utilisateurs doivent également être éduqués sur les meilleures pratiques de sécurité, telles que la création de mots de passe forts et l'utilisation de l'authentification à deux facteurs pour protéger leurs comptes de messagerie.

2.4 Serveur de fichiers



Un serveur de fichiers est un type de serveur qui stocke des fichiers et des dossiers, et permet à des utilisateurs de les accéder et de les partager via un réseau. Les serveurs de fichiers peuvent être configurés pour fournir différentes fonctionnalités, telles que :

1. Partage de fichiers : Les utilisateurs peuvent accéder aux fichiers stockés sur le serveur et les partager avec d'autres utilisateurs du réseau.
2. Gestion des droits d'accès : Les administrateurs peuvent définir des autorisations d'accès pour chaque utilisateur ou groupe d'utilisateurs, afin de contrôler qui peut accéder à quels fichiers.
3. Sauvegarde de données : Les serveurs de fichiers peuvent être configurés pour effectuer des sauvegardes régulières des fichiers stockés, afin de protéger les données contre la perte ou la corruption.
4. Synchronisation de fichiers : Les utilisateurs peuvent synchroniser des fichiers entre le serveur de fichiers et leur ordinateur local, pour assurer une cohérence des données.
5. Accès à distance : Les utilisateurs peuvent accéder aux fichiers stockés sur le serveur de fichiers à partir d'un emplacement distant en utilisant un client de connexion sécurisé.
6. Stockage en nuage : Les serveurs de fichiers peuvent être configurés pour stocker des fichiers dans le cloud, ce qui permet aux utilisateurs d'y accéder à partir de n'importe où avec une connexion Internet.

7. Accès multiplateforme : Les serveurs de fichiers peuvent être configurés pour fournir un accès multiplateforme aux utilisateurs, ce qui permet aux utilisateurs d'accéder aux fichiers à partir de différents systèmes d'exploitation tels que Windows, Mac OS ou Linux.

Les serveurs de fichiers sont couramment utilisés dans les entreprises pour stocker et partager des fichiers entre les employés, mais ils peuvent également être utilisés dans des environnements domestiques pour stocker et partager des fichiers entre les membres de la famille.

2.4.1 Quelques vulnérabilités Sur Les Serveurs de Fichier

Il existe plusieurs vulnérabilités potentielles qui peuvent affecter les serveurs de fichiers. Voici quelques exemples :

1. Vulnérabilités de sécurité : Les serveurs de fichiers peuvent avoir des vulnérabilités de sécurité connues qui peuvent être exploitées par les attaquants pour accéder à des données sensibles, telles que des fichiers confidentiels ou des informations d'identification.

2. Vulnérabilités de configuration : Les serveurs de fichiers peuvent avoir des vulnérabilités de configuration qui peuvent être exploitées par les attaquants pour accéder à des données sensibles, telles que des fichiers de configuration ou des répertoires de fichiers.

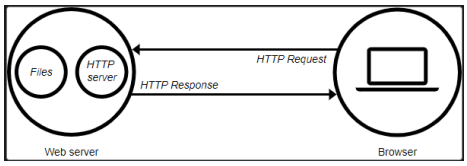
3. Attaques par déni de service (DoS) : Les attaquants peuvent lancer des attaques par déni de service (DoS) contre le serveur de fichiers pour le rendre indisponible, ce qui peut empêcher les utilisateurs d'accéder aux fichiers hébergés sur ce serveur.

4. Attaques de force brute : Les attaquants peuvent tenter de deviner les identifiants de connexion des utilisateurs en utilisant des attaques de force brute, qui impliquent l'utilisation de programmes pour tester toutes les combinaisons de noms d'utilisateur et de mots de passe possibles.

5. Fuites de données : Les serveurs de fichiers peuvent être vulnérables aux fuites de données, qui peuvent se produire lorsque des données sensibles sont stockées de manière inappropriée ou lorsque des utilisateurs non autorisés y ont accès.

Il est important de mettre en place des mesures de sécurité adéquates pour protéger les serveurs de fichiers contre ces vulnérabilités potentielles, telles que la mise à jour régulière de la sécurité du système et l'utilisation de logiciels de sécurité pour détecter et prévenir les attaques potentielles. Les utilisateurs doivent également être éduqués sur les meilleures pratiques de sécurité, telles que la création de mots de passe forts et l'utilisation de l'authentification à deux facteurs pour protéger leur accès aux fichiers stockés sur le serveur de fichiers.

2.5 Serveur de Base de Données



Un serveur de base de données est un type de serveur qui stocke des données et fournit des services pour gérer ces données. Il permet aux utilisateurs de stocker, d'organiser, d'accéder et de gérer des données de manière efficace et sécurisée.

Les serveurs de base de données sont utilisés pour stocker des informations sur des produits, des clients, des transactions financières, des employés, des stocks, etc. Ils sont également utilisés pour alimenter des applications qui nécessitent un accès rapide et efficace aux données, telles que les sites web, les applications mobiles, les systèmes de gestion de la relation client (CRM), les systèmes de gestion de la chaîne d'approvisionnement (SCM), etc.

Les serveurs de bases de données peuvent être configurés pour fournir différentes fonctionnalités, telles que :

1. Langage de requête : Les serveurs de bases de données prennent en charge des langages de requête tels que SQL (Structured Query Language) pour interroger et récupérer les données stockées.

2. Gestion des transactions : Les serveurs de bases de données prennent en charge la gestion des transactions pour garantir l'intégrité des données et éviter les conflits.

3. Gestion des utilisateurs et des droits d'accès : Les administrateurs peuvent définir des autorisations d'accès pour chaque utilisateur ou groupe d'utilisateurs, afin de contrôler qui peut accéder à quelles données.

4. Sauvegarde et restauration : Les serveurs de bases de données peuvent être configurés pour effectuer des sauvegardes régulières des données stockées, afin de protéger les données contre la perte ou la corruption.

5. Réplication des données : Les serveurs de bases de données peuvent être configurés pour répliquer les données sur plusieurs serveurs, pour améliorer la disponibilité et la redondance des données.

6. Sécurité des données : Les serveurs de bases de données peuvent être configurés pour fournir des fonctionnalités de sécurité avancées, telles que le chiffrement des données, l'authentification à deux facteurs, etc.

Les serveurs de bases de données sont couramment utilisés dans les entreprises pour stocker et gérer des données importantes, mais ils peuvent également être utilisés dans des environnements domestiques pour stocker et gérer des données personnelles telles que les finances, les contacts, les photos, etc.

2.5.1 Quelques vulnérabilités Sur Les Serveurs de Base De Donnes

Il existe plusieurs vulnérabilités potentielles qui peuvent affecter les serveurs de bases de données. Voici quelques exemples :

1. Injection SQL : Les attaquants peuvent exploiter des vulnérabilités dans le serveur de base de données pour injecter du code SQL malveillant, qui peut permettre aux attaquants de prendre le contrôle du serveur de base de données, de modifier ou de supprimer des données, ou encore d'accéder à des informations confidentielles.

2. Vulnérabilités de sécurité : Les serveurs de bases de données peuvent avoir des vulnérabilités de sécurité connues, telles que la configuration par défaut de mots de passe faibles, qui peuvent être exploitées par les attaquants pour accéder à des données sensibles.

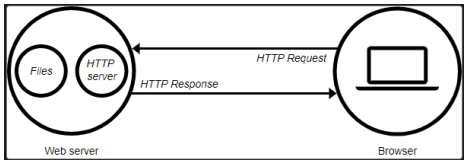
3. Attaques par déni de service (DoS) : Les attaquants peuvent lancer des attaques par déni de service (DoS) contre le serveur de base de données pour le rendre indisponible, ce qui peut empêcher les utilisateurs d'accéder aux données stockées sur ce serveur.

4. Vulnérabilités de configuration : Les serveurs de bases de données peuvent avoir des vulnérabilités de configuration qui peuvent être exploitées par les attaquants pour accéder à des données sensibles, telles que des informations de connexion ou des fichiers de configuration.

5. Fuites de données : Les serveurs de bases de données peuvent être vulnérables aux fuites de données, qui peuvent se produire lorsque des données sensibles sont stockées de manière inappropriée ou lorsque des utilisateurs non autorisés y ont accès.

Il est important de mettre en place des mesures de sécurité adéquates pour protéger les serveurs de bases de données contre ces vulnérabilités potentielles, telles que la mise à jour régulière de la sécurité du système et l'utilisation de logiciels de sécurité pour détecter et prévenir les attaques potentielles. Les développeurs de bases de données doivent également être conscients des meilleures pratiques de sécurité, telles que la validation des entrées utilisateur et l'utilisation de l'authentification à deux facteurs pour protéger l'accès aux données stockées sur le serveur de bases de données.

2.6 Serveur d'Application



Un serveur d'application est un type de serveur qui héberge des applications et fournit des services d'application aux clients. Les serveurs d'application sont essentiels pour les entreprises qui développent et déploient des applications commerciales, car ils fournissent une plateforme pour exécuter et gérer ces applications de manière efficace et sécurisée.

Les serveurs d'application peuvent être utilisés pour héberger une grande variété d'applications, telles que les applications de commerce électronique, les applications de gestion de contenu, les applications de gestion de la relation client (CRM), les applications de gestion de la chaîne d'approvisionnement (SCM), les applications de collaboration, etc.

Les serveurs d'application peuvent fournir différentes fonctionnalités, telles que :

1. Gestion de la connectivité : Les serveurs d'application peuvent gérer la connectivité entre les applications et les différents systèmes d'information, tels que les bases de données, les systèmes de fichiers, les services web, etc.
2. Gestion des transactions : Les serveurs d'application peuvent gérer les transactions pour garantir l'intégrité des données et éviter les conflits.
3. Gestion de la sécurité : Les serveurs d'application peuvent fournir des fonctionnalités de sécurité avancées pour protéger les applications et les données contre les menaces potentielles.
4. Gestion des sessions : Les serveurs d'application peuvent gérer les sessions pour assurer la continuité des services aux utilisateurs lorsqu'ils passent d'une page à l'autre ou lorsqu'ils se connectent à l'application à partir de différents appareils.
5. Gestion des performances : Les serveurs d'application peuvent surveiller et optimiser les performances de l'application pour assurer une expérience utilisateur rapide et fluide.

Les serveurs d'application sont souvent utilisés en conjonction avec d'autres outils de développement et de déploiement, tels que les serveurs web, les bases de données, les outils de développement intégrés (IDE), les systèmes de contrôle de version, etc.

2.6.1 Quelques vulnérabilités Sur Les Serveurs d'Application

Il existe plusieurs vulnérabilités potentielles qui peuvent affecter les serveurs d'application. Voici quelques exemples :

1. Vulnérabilités de sécurité : Les serveurs d'application peuvent avoir des vulnérabilités de sécurité connues, telles que des failles dans les algorithmes de chiffrement ou des vulnérabilités dans les bibliothèques tierces, qui peuvent être exploitées par les attaquants pour accéder à des données sensibles ou prendre le contrôle du serveur.

2. Attaques par déni de service (DoS) : Les attaquants peuvent lancer des attaques par déni de service (DoS) contre le serveur d'application pour le rendre indisponible, ce qui peut empêcher les utilisateurs d'accéder aux applications hébergées sur ce serveur.

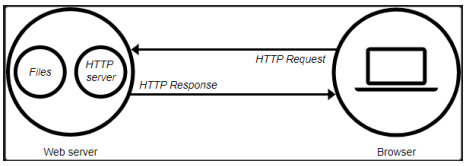
3. Injection de code : Les attaquants peuvent exploiter des vulnérabilités dans le serveur d'application pour injecter du code malveillant dans les applications, qui peuvent ensuite être utilisées pour exécuter des attaques de phishing, des attaques de logiciels malveillants ou d'autres types d'attaques.

4. Vulnérabilités de configuration : Les serveurs d'application peuvent avoir des vulnérabilités de configuration qui peuvent être exploitées par les attaquants pour accéder à des données sensibles, telles que des informations de connexion ou des fichiers de configuration.

5. Fuites de données : Les serveurs d'application peuvent être vulnérables aux fuites de données, qui peuvent se produire lorsque des données sensibles sont stockées de manière inappropriée ou lorsque des utilisateurs non autorisés y ont accès.

Il est important de mettre en place des mesures de sécurité adéquates pour protéger les serveurs d'application contre ces vulnérabilités potentielles, telles que la mise à jour régulière de la sécurité du système et l'utilisation de logiciels de sécurité pour détecter et prévenir les attaques potentielles.
Les développeurs d'applications doivent également être conscients des meilleures pratiques de sécurité, telles que la validation des entrées utilisateur et l'utilisation de l'authentification à deux facteurs pour protéger les applications hébergées sur le serveur d'application.

2.7 Serveur DNS



Un serveur DNS (Domain Name System) est un type de serveur qui permet de traduire les noms de domaine en adresses IP. Les noms de domaine sont des identificateurs textuels, tels que "google.com" ou "facebook.com", qui sont plus faciles à mémoriser que les adresses IP numériques qui identifient les ordinateurs et les serveurs sur Internet.

Lorsqu'un utilisateur entre un nom de domaine dans son navigateur web, le navigateur envoie une requête DNS au serveur DNS pour obtenir l'adresse IP correspondante. Le serveur DNS répond alors avec l'adresse IP, qui est utilisée pour établir la connexion avec le serveur web correspondant.

Les serveurs DNS sont essentiels pour le fonctionnement d'Internet, car ils permettent aux utilisateurs d'accéder aux sites web et aux services en ligne en utilisant des noms de domaine plutôt que des adresses IP numériques. Les serveurs DNS sont également utilisés pour acheminer le courrier électronique et pour fournir d'autres services de réseau.

Les serveurs DNS peuvent être configurés pour fournir différentes fonctionnalités, telles que :

1. Caching de requêtes : Les serveurs DNS peuvent mettre en cache les réponses aux requêtes DNS précédentes pour accélérer les temps de réponse et réduire la charge sur le réseau.

2. Résolution de noms de domaine : Les serveurs DNS peuvent résoudre les noms de domaine en adresses IP en utilisant des bases de données de noms de domaine et des serveurs racines.

3. Redirection de domaine : Les serveurs DNS peuvent être configurés pour rediriger les requêtes vers d'autres serveurs DNS, en fonction des besoins.

4. Sécurité DNS : Les serveurs DNS peuvent implémenter des fonctionnalités de sécurité avancées, telles que DNSSEC (DNS Security Extensions), pour protéger contre les attaques de DNS spoofing et de DNS cache poisoning.

5. Load balancing : Les serveurs DNS peuvent être utilisés pour répartir la charge entre plusieurs serveurs web en redirigeant les requêtes vers différents serveurs en fonction des besoins.

Les serveurs DNS sont souvent gérés par les fournisseurs de services Internet (ISP), les entreprises et les organisations gouvernementales. Les utilisateurs peuvent également configurer leur propre serveur DNS pour fournir une résolution de noms de domaine personnalisée ou pour améliorer la sécurité et la performance de leur réseau local.

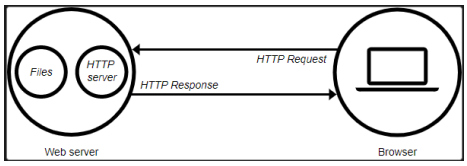
2.7.1 Quelques vulnérabilités Sur Les Serveurs DNS

Il existe plusieurs vulnérabilités potentielles qui peuvent affecter les serveurs de DNS (Domain Name System). Voici quelques exemples :

1. Attaques par déni de service (DoS) : Les attaquants peuvent lancer des attaques par déni de service (DoS) contre le serveur de DNS pour le rendre indisponible, ce qui peut empêcher les utilisateurs d'accéder aux noms de domaine associés à ce serveur.
2. Vulnérabilités de sécurité : Les serveurs de DNS peuvent avoir des vulnérabilités de sécurité connues qui peuvent être exploitées par les attaquants pour accéder à des données sensibles, telles que des informations de connexion ou des fichiers de configuration.
3. Attaques de cache poisoning : Les attaquants peuvent exploiter des vulnérabilités dans le serveur de DNS pour modifier le contenu du cache DNS, ce qui peut rediriger les utilisateurs vers des sites web malveillants.
4. Vulnérabilités de configuration : Les serveurs de DNS peuvent avoir des vulnérabilités de configuration qui peuvent être exploitées par les attaquants pour accéder à des données sensibles, telles que des informations de connexion ou des fichiers de configuration.
5. Fuites de données : Les serveurs de DNS peuvent être vulnérables aux fuites de données, qui peuvent se produire lorsque des données sensibles sont stockées de manière inappropriée ou lorsque des utilisateurs non autorisés y ont accès.

Il est important de mettre en place des mesures de sécurité adéquates pour protéger les serveurs de DNS contre ces vulnérabilités potentielles, telles que la mise à jour régulière de la sécurité du système et l'utilisation de logiciels de sécurité pour détecter et prévenir les attaques potentielles. Les administrateurs de DNS doivent également être conscients des meilleures pratiques de sécurité, telles que la mise en place de politiques de sécurité strictes pour l'accès au serveur de DNS et la configuration correcte du serveur de DNS pour minimiser les risques d'attaques de cache poisoning.

2.8 Serveur de Jeu



Un serveur de jeu est un type de serveur qui permet de fournir des services de jeu en ligne à des joueurs du monde entier. Les serveurs de jeu sont utilisés pour héberger des jeux multijoueurs en ligne, tels que les jeux de tir à la première personne, les jeux de stratégie en temps réel, les jeux de rôle en ligne massivement multijoueurs (MMORPG), les jeux de sport en ligne, etc.

Les serveurs de jeu offrent des fonctionnalités telles que :

1. 1. Hébergement de jeux multijoueurs : Les serveurs de jeu sont utilisés pour héberger des jeux multijoueurs en ligne pour permettre aux joueurs de jouer ensemble sur Internet.

2. Gestion des joueurs : Les serveurs de jeu peuvent gérer les joueurs, les scores, les classements et les statistiques de jeu, ainsi que les opérations de modération pour assurer un environnement de jeu sécurisé et équitable.

3. Optimisation des performances : Les serveurs de jeu peuvent être optimisés pour offrir des performances de jeu optimales, telles que des temps de latence réduits et une faible latence pour une expérience de jeu fluide.

4. Gestion de la bande passante : Les serveurs de jeu peuvent gérer la bande passante pour optimiser les performances de jeu et éviter les problèmes de lag ou de décalage.

5. Gestion des mises à jour : Les serveurs de jeu peuvent gérer les mises à jour de jeu pour maintenir les joueurs à jour avec les dernières fonctionnalités et correctifs de bugs.

Les serveurs de jeu sont utilisés par les développeurs de jeux pour héberger leurs jeux en ligne et fournir des services de jeu en ligne à des millions de joueurs dans le monde entier. Les serveurs de jeu peuvent être exploités directement par les développeurs de jeux ou par des fournisseurs de services tiers spécialisés dans l'hébergement de serveurs de jeu. Les serveurs de jeu sont essentiels pour les jeux multijoueurs en ligne, car ils permettent aux joueurs de jouer ensemble sur Internet, offrant ainsi une expérience de jeu immersive et sociale.

Il existe plusieurs vulnérabilités potentielles qui peuvent affecter les serveurs de jeu. Voici quelques exemples :

1. Vulnérabilités de sécurité : Les serveurs de jeu peuvent avoir des vulnérabilités de sécurité connues qui peuvent être exploitées par les attaquants pour

accéder à des données sensibles, telles que des informations de compte de joueur ou des données de paiement.

2. Attaques par déni de service (DoS) : Les attaquants peuvent lancer des attaques par déni de service (DoS) contre le serveur de jeu pour le rendre indisponible, ce qui peut empêcher les joueurs d'accéder au jeu ou de jouer en ligne.

3. Exploits de jeu : Les attaquants peuvent exploiter des vulnérabilités dans le code du jeu pour gagner un avantage injuste sur les autres joueurs, ou pour perturber le jeu pour tous les autres joueurs.

4. Vulnérabilités de configuration : Les serveurs de jeu peuvent avoir des vulnérabilités de configuration qui peuvent être exploitées par les attaquants pour accéder à des données sensibles, telles que des informations de connexion ou des fichiers de configuration.

5. Fuites de données : Les serveurs de jeu peuvent être vulnérables aux fuites de données, qui peuvent se produire lorsque des données sensibles sont stockées de manière inappropriée ou lorsque des utilisateurs non autorisés y ont accès.

Il est important de mettre en place des mesures de sécurité adéquates pour protéger les serveurs de jeu contre ces vulnérabilités potentielles, telles que la mise à jour régulière de la sécurité du système et l'utilisation de logiciels de sécurité pour détecter et prévenir les attaques potentielles. Les développeurs de jeux doivent également être conscients des meilleures pratiques de sécurité, telles que la validation des entrées utilisateur et l'utilisation de l'authentification à deux facteurs pour protéger les comptes de joueur. Les administrateurs de serveurs de jeu doivent également surveiller les activités suspectes et mettre en place des politiques de sécurité strictes pour minimiser les risques d'attaques.

Constat

Si vous remarquez bien que sur tout les serveurs que je viens de citer nous voyons que les attaques comme :

1. L'Attaque Par Déni de Service (DoS).

2. Vulnérabilité de Configuration.

3. Fuites de données.

4. Vulnérabilité de Sécurité .

Dans ce le chapitre qui suit nous allons essayer de parler des méthodes, manières par lesquelles nous pouvons éviter de tomber dans les pièges d'attaques citées ci-hauts .

Chapter 3

La CyberSécurité et La Sécurité Informatique

3.1 La CyberSécurité

3.1.1 Définition

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.

3.2 La Sécurité Informatique

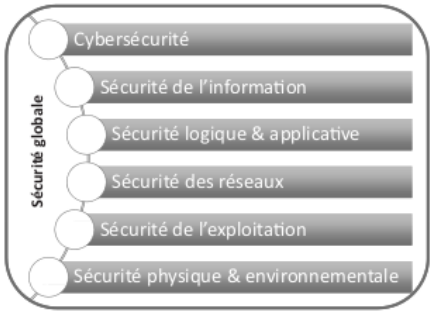
3.2.1 Définition

3.3 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 ;

Chapter 4

La Configuration Du Serveur Web (ISS) Et La Sécurisation de ce dernier