Sécurisation d'un serveur Apache

[sommaire]

1. **Objectifs**

- Connaitre le rôle des modules de Tomcat.
- Etre capable de sécuriser serveur web Tomcat

- **Présentation**

  - Sécuriser un système informatique est une tâche rigoureuse, d’autant plus quand ledit système est connecté au réseau Internet. En effet, le réseau mondial grouille de pirates qui nuisent au bon fonctionnement de vos systèmes.
  - La sécurité se fera tout d'abord au niveau du serveur Web pour protéger celui-ci d'attaques extérieures comme le DDOS par exemple, mais aussi pour ne pas géner d'éventuels utilisateurs qui en parallèle utilisent la même machine pour d'autres raisons: Limiter Apache dans la consommation des ressources disponibles et permettre ainsi aux autres utilisateurs/applications de la machine de travailler/fonctionner correctement.

- **Récupérer des informations sur ce serveur**

  1. **Présentation**

  - Une solution pour pirater un serveur pour un hacker est déjà de récupérer des informations sur ce serveur. Cela lui permettra de s'orienter sur tel ou tel solution d'attaque.
  - Pour récupérer des informations sur le serveur, sa version, la distribution (Linux, Microsoft) sur laquelle tourne le serveur Apache, la version php et les modules, ...Il suffit de faire un **telnet sur l'ip** du serveur sur le **port 80** (celui utilisé normalement pour le protocole http)
  - Pour activer telnet sur Windows:

- **Réalisation**

  - Exécuter l'invite de commande (`Démarrer -> Exécuter -> cmd`)
  - Taper la commande:`telnet localhost 80`

apcpedagogie.com

- Résultat:

- Le résultat de cette commande montre à un pirate tous les informations nécessaires pour le serveur Apache.

Changer le port d’écoute du SSH

1. **Définitions**

- **SSH**, ou **Secure Socket Shell**, est un protocole réseau qui permet aux administrateurs d'accéder à distance à un ordinateur, en toute sécurité.
- **SSH** désigne à la fois le protocole de réseau cryptographique et les utilitaires qui mettent en oeuvre ce protocole.
- Assurez-vous de garder vos dépendances à jour, et utilisez des outils comme **Gemnasium** pour obtenir des notifications automatiques lorsqu'une vulnérabilité est annoncée dans l’un de vos composants.

- **Sécurisation**

    - Par défaut et conventionnellement, le Secure Shell ou SSH écoute sur le port 22. Mais cette convention facilite la tâche des pirates. Ainsi, ils testent tout de suite ce port s’ils veulent accéder au serveur.

Utiliser exclusivement le TLS en administration

1. **Présentation**

- Le protocole **TLS** est conçu pour fournir trois services essentiels à toutes les applications qui s'exécutent au-dessus de lui: le chiffrement, l'authentification et l'intégrité des données.
- Techniquement, vous n'êtes pas obligé d'utiliser les trois dans chaque situation. Vous pouvez décider d'accepter un certificat sans valider son authenticité, mais vous devez être bien conscient des risques de sécurité et des implications de le faire. En pratique, une application Web sécurisée tirera parti des trois services.

1. **Cryptage**

- Un mécanisme pour masquer ce qui est envoyé d'un hôte à un autre.

apcpedagogie.com

- **Authentification**
  - Un mécanisme pour vérifier la validité du matériel d'identification fourni.
- **Intégrité**
  - Un mécanisme pour détecter la falsification et la falsification des messages.

- **Sécurisation**
  - Lorsque le protocole **SSL** a été normalisé par l'IETF, il a été renommé en Transport Layer Security (**TLS**). Beaucoup utilisent les noms TLS et SSL de manière interchangeable, mais techniquement, ils sont différents, car chacun décrit une version différente du protocole.
  - Pendant que vous administrez votre serveur, des millions de pirates tentent de soutirer des données sensibles comme votre mot de passe, par exemple. Ainsi, il est conseillé d'opter exclusivement le TLS (Transport Layer Security) pour l'administration. Avec des données chiffrées, impossible à cracker.

Fichier de configuration

- Suivant la distribution, le fichier de configuration principal d'Apache peut se situer sous `/etc/httpd/conf/httpd.conf` `/etc/apache2/apache2.conf`

Outils de sécurité du site Web

- Une fois que vous pensez que vous avez fait tout ce que vous pouvez alors il est temps de tester la sécurité de votre site Web. Le moyen le plus efficace de le faire est l'utilisation de certains outils de sécurité de site Web, souvent appelés tests de pénétration ou test de stylo pour faire court.
- Il existe de nombreux produits commerciaux et gratuits pour vous aider avec cela. Ils fonctionnent de la même manière que les scripts que les hackers utiliseront en ce qu'ils testent tous les exploits connus et tentent de compromettre votre site en utilisant certaines des méthodes mentionnées précédemment telles que l'injection SQL.
- Quelques outils gratuits qui valent la peine d'être regardés :
  - Netsparker (édition communautaire gratuite et version d'essai disponible). Bon pour tester l'injection SQL et XSS OpenVAS . Revendique être le scanner de sécurité Open Source le plus avancé. Bon pour tester les vulnérabilités connues, scanne actuellement plus de 25 000. Mais il peut être difficile à configurer et nécessite l'installation d'un serveur OpenVAS qui ne fonctionne que sur * nix. OpenVAS est la fourche d'un Nessus

apcpedagogie.com

avant qu'il ne devienne un produit commercial à source fermée.
- SecurityHeaders.io (vérification en ligne gratuite). Un outil pour signaler rapidement les en-têtes de sécurité mentionnés ci-dessus (tels que CSP et HSTS) qu'un domaine a activés et correctement configurés.
- Xenotix XSS Exploit Framework Un outil de OWASP (Open Web Application Security Project) qui comprend un grand choix d'exemples d'attaques XSS, que vous pouvez exécuter pour confirmer rapidement si les entrées de votre site sont vulnérables dans Chrome, Firefox et IE.
- Les résultats des tests automatisés peuvent être décourageants, car ils présentent une multitude de problèmes potentiels. L'important est de se concentrer d'abord sur les problèmes critiques. Chaque problème rapporté vient normalement avec une bonne explication de la vulnérabilité potentielle. Vous constaterez probablement que certaines des problématiques moyennes / faibles ne sont pas un problème pour votre site.

Source:

- https://www.oneteam.tn/comment-securiser-votre-site-web/

Sommaire du cours Administration et sécurité des sites web

Source : https://apcpedagogie.com/securisation-dun-serveur-apache · téléchargé le 04/11/2026 · © APC Pédagogie · apcpedagogie.com

apcpedagogie.com