Configuration d'un WAF avec mod_security

Introduction

Un Web Application Firewall (WAF) est un pare-feu spécifique qui protège les applications web contre des menaces telles que les injections SQL, les attaques XSS (Cross-Site Scripting) et d'autres vulnérabilités. mod_security est un module open-source pour Apache HTTP Server qui permet de détecter et bloquer ces attaques.

L'objectif de ce TP est d'installer et de configurer mod_security pour sécuriser une application web et de tester sa capacité à détecter et bloquer les attaques.

Objectifs

1. Installer mod_security sur un serveur Apache.
2. Configurer mod_security pour qu'il analyse et bloque les attaques web.
3. Tester la configuration de mod_security avec des attaques simulées.
4. Analyser les logs générés par mod_security pour voir les attaques détectées.

Étapes réalisées

1. Installation de mod_security sur Apache :

1. **Installer le module mod_security** :
    - Sur une machine Ubuntu, vous pouvez installer mod_security avec la commande suivante :

        sudo apt update

        sudo apt install libapache2-mod-security2

2. **Vérifier l'installation** :
    - Après l'installation, vérifiez que le module mod_security est bien chargé avec la commande :

        apache2ctl -M | grep security

Vous devriez voir security2_module dans la sortie.

3. **Activer le module mod_security** :
    - Si le module n'est pas activé par défaut, vous pouvez l'activer avec la commande suivante :

        sudo a2enmod security2

    - Redémarrez ensuite le serveur Apache :

```
sudo systemctl restart apache2
```

2. Configuration de mod_security :

1. **Renommer le fichier de configuration recommandé** :
    - mod_security fournit un fichier de configuration recommandé qui doit être utilisé :

```
sudo mv /etc/modsecurity/modsecurity.conf-recommended /etc/modsecurity/modsecurity.conf
```

2. **Éditer le fichier de configuration de mod_security** :
    - Ouvrez le fichier de configuration mod_security :

```
sudo nano /etc/modsecurity/modsecurity.conf
```

    - Modifiez la directive SecRuleEngine pour activer le blocage des attaques :

```
SecRuleEngine On
```

3. **Appliquer les règles de sécurité par défaut** :
    - mod_security utilise un ensemble de règles de sécurité par défaut qui doivent être activées pour protéger les applications web contre les attaques courantes.
    - Vous pouvez utiliser les règles de l'OWASP ModSecurity Core Rule Set (CRS) en installant le paquet suivant :

```
sudo apt install modsecurity-crs
```

    - Activez ces règles en les incluant dans le fichier de configuration mod_security :

```
IncludeOptional /usr/share/modsecurity-crs/base_rules/*.conf
```

4. **Redémarrer Apache pour appliquer les modifications** :
    - Redémarrez Apache pour prendre en compte les nouvelles configurations :

```
sudo systemctl restart apache2
```

3. Test de la configuration de mod_security :

1. **Effectuer un test de sécurité avec une attaque simulée** :
    - Pour tester si mod_security détecte les attaques, vous pouvez essayer de générer une injection SQL ou un XSS.

- Par exemple, essayez d'accéder à l'application web avec une URL qui tente une injection SQL :

  http://votreserveur/index.html?foo=' OR 1=1 --

- **mod_security** devrait bloquer cette requête et enregistrer l'événement dans les logs.

2. **Effectuer un test de Cross-Site Scripting (XSS)** :
   - Essayez une requête contenant un script malveillant :

     http://votreserveur/index.html?foo=<script>alert('XSS')</script>

   - Cette requête devrait être bloquée par mod_security.

4. Analyse des logs générés par mod_security :

1. **Consulter les logs de mod_security** :
   - mod_security génère des logs pour chaque attaque détectée. Par défaut, ces logs sont enregistrés dans le fichier :

     /var/log/apache2/modsec_audit.log

   - Vous pouvez afficher les logs avec la commande :

     sudo cat /var/log/apache2/modsec_audit.log

   - Le fichier contiendra des informations sur les requêtes bloquées, y compris le type d'attaque détecté et l'URL concernée.
2. **Vérification des événements enregistrés** :
   - Recherchez des événements spécifiques liés à des attaques, comme des injections SQL ou des XSS. Par exemple :

     sudo grep "SQL Injection" /var/log/apache2/modsec_audit.log

Résultats obtenus

1. mod_security a été installé et configuré sur le serveur Apache avec succès.
2. Les règles de sécurité par défaut ont été activées, y compris celles de l'OWASP CRS.
3. Les attaques simulées, telles que l'injection SQL et le XSS, ont été détectées et bloquées par mod_security.
4. Les logs ont bien enregistré les événements liés aux attaques détectées.

Conclusion

Ce TP m'a permis de comprendre comment configurer un Web Application Firewall (WAF) avec mod_security pour protéger une application web contre les attaques courantes. J'ai appris à activer des règles de sécurité, à tester la configuration avec des attaques simulées, et à analyser les logs générés par mod_security pour identifier les attaques bloquées.