Atelier 3 : Mise en place d'un WAF avec NGINX/NAXSI sur OPNsense

Un **Web Application Firewall** (WAF) est un type de pare-feu qui protège le serveur d'applications Web dans le backend contre diverses attaques. Le WAF garantit que la sécurité du serveur Web n'est pas compromise en examinant les paquets de requête HTTP / HTTPS et les modèles de trafic Web.

L'objectif de cet atelier est de comprendre les concepts clés du pare-feu applicatif web (WAF) et d'acquérir les compétences nécessaires pour configurer et gérer efficacement le pare-feu applicatif web (WAF) NAXSI sur OPNsense, afin de protéger un serveur web contre les cyberattaques, tout en maîtrisant les concepts de sécurité et de gestion des règles de filtrage des requêtes."

Préparation :

Chaque groupe dispose de machines virtuelles accessibles via l'interface Proxmox à l'adresse suivante :

http://10.25.24.100:8006

Les machines :

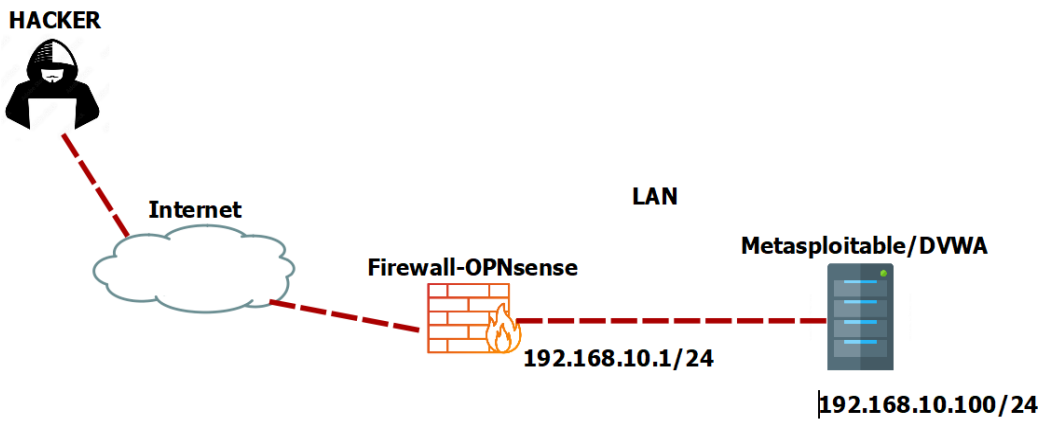
- OPNsense
- Linux (Debian)
- Metasplpitable

Chaque étudiant possède un compte personnel avec les identifiants suivants :

- **Nom d'utilisateur** : Nom de famille en majuscules
- **Mot de passe** : Date de naissance au format **JJMMAAAA** (jour, mois, année)

Avant de commencer l'atelier assurez-vous de bien configurer l'infrastructure ci-dessous

Chaque groupe utilise un LAN différent : 192.168.X.0/24 dans cet exemple le groupe 1 par exemple utilise le 192.168.10.0/24



Installation et Configuration de Nginx

NGINX est un serveur web de périphérie haute performance, caractérisé par une faible utilisation de la mémoire et des fonctionnalités essentielles pour construire une infrastructure web moderne et efficace.

Les capacités de NGINX incluent : serveur HTTP, proxy inverse HTTP et mail, mise en cache, équilibrage de charge, compression, limitation du débit des requêtes, multiplexage et réutilisation des connexions, déchargement SSL et diffusion de médias en HTTP

Etape 1 : Installation de Nginx

Installer d'abord les MàJ. && Installer Ensuite le plugin Nginx sur OPNsense : **System > Firmware > Plugins**

Tapez nginx dans le champ de recherche pour trouver le plugin NGINX.

Cliquez sur l'icône + à côté de os-nginx pour installer le plugin. Vous serez ensuite redirigé vers l'onglet du menu Mise à jour

Avant d'activer le service **NGINX**, il est nécessaire de modifier les paramètres de l'interface graphique (**GUI**) d'**OPNsense** afin d'éviter tout conflit de port entre **NGINX** et **Lighttpd**, le processus chargé de servir l'interface Web

Naviguer vers : **Système > Paramètres > Administration**.

Activer le protocole HTTP

Modifier le paramètre du port TCP de 443 ou 80 à un autre port, comme **8080**.

Activer Nginx dans Services **> Nginx > Configuration>enable**

Etape 2 : Ajout d'un Upstream Server

Upstream Server : représente le serveur web réel qui héberge l'application.

Allez dans Services > Nginx > Configuration

Accédez à l'onglet **Upstream** Servers

Cliquez sur + pour ajouter un serveur :

Description : WebServer

IP address : 192.168.10.100 (Adresse de serveur DVWA)

Port : 80

Server Priority : 1

Maximum Connections. 10000

Maximum Failures. 6

Fail Timeout. 6

Etape 3 : Ajout Upstream

Upstream : L'ensemble des serveurs backend configurés pour gérer les requêtes.

Allez dans Services > Nginx > Configuration

Accédez à l'onglet Upstreams

Description: WebServer_backend.

Server Entries: WebServer

Load Balancing Algorithm: Vous pouvez sélectionner un algorithme d'équilibrage de charge. Les options disponibles sont **Weighted Round Robin** et **IP Hash**..

Keepalive: Définit le nombre maximal de connexions inactives conservées dans le cache de chaque processus worker et active le cache des connexions pour le serveur upstream. Pour le désactiver, laissez le champ vide ou définissez-le sur **0**. Le support **Keepalive** doit également être activé dans les paramètres de l'emplacement (location).

Enable TLS (HTTPS): Décochez cette option pour ne pas utiliser TLS

TLS: Servername override: ce champ impose un nom d'hôte spécifique pour la connexion backend au lieu de transmettre le nom d'hôte de la connexion en aval à la connexion en amont.

TLS: Supported Versions: Vous pouvez sélectionner les versions TLS prises en charge

TLS: Session Reuse:

TLS: Trusted Certificate: Vous pouvez sélectionner les certificats de confiance installés sur OPNsense.

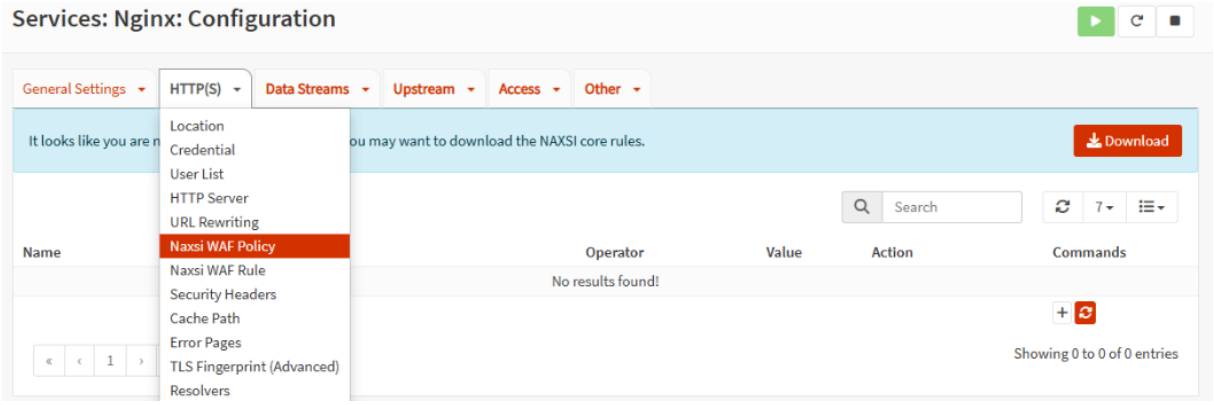
PS : Dans mon cas je n'ai pas utilisé le TLS.

Etape 4 : Télécharger les règles de NAXSI (WAF)

NAXSI signifie **Nginx Anti XSS & SQL Injection**. Techniquement, c'est un **module tiers pour Nginx**, disponible sous forme de package pour de nombreuses plateformes de type UNIX.

Par défaut, ce module lit un **ensemble de règles simples et lisibles** contenant **99 % des modèles connus** impliqués dans les vulnérabilités des sites web.

Par exemple, les caractères **<**, **|** ou le mot-clé **drop** ne sont normalement pas censés faire partie d'une **URI**.



Etape 5 : Création d'une Location

La Location définit ce qui sera redirigé vers le serveur Upstream. Les règles du WAF doivent être appliquées à une location. Voici les étapes pour ajouter une location :

Allez dans la page **Services > Nginx > Configuration.**

Cliquez sur le menu déroulant HTTP(S) en haut de la page.

Sélectionnez le menu Location

Description : WebServer_Location

URL Pattern : / pour désigner la racine de Web server ou bien donner un chemin différent.

Match type : none

URL Rewriting : Nothing selected

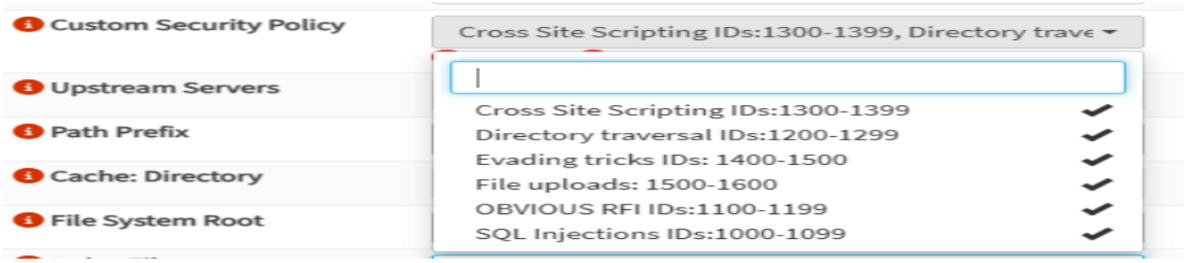
Enable Security Rules. Cocher pour activer les règles

Mode learning mode : Cochez cette option pour activer le mode d'apprentissage, ce qui signifie que rien n'est bloqué mais tout est enregistré. Lors de l'utilisation du WAF pour la première fois, cette option est avantageuse. Vous pouvez ajouter des listes blanches jusqu'à ce que les faux positifs cessent pendant la phase d'apprentissage.

Block XSS Score : None

Block SQL injection Score : None

Custom Security Policy :



Upstream Servers : WebServer_Backend

Etape 6 : Création d'un HTTP Server

Accédez à Services > Nginx > Configuration > HTTP Server

Cliquez sur + pour ajouter un serveur :

Nom du serveur : 192.168.10.100

Locations : WebServer_Location

TLS Certificate : Web GUI TLS Certifacte

Sauvegarder la configuration et recharger NGINX

Etape 7 : Validation de votre solution.

Lancer la machine Metaspoitable.

http:// IP_WAN/dvwa

Quel est le nom et le pwd ?

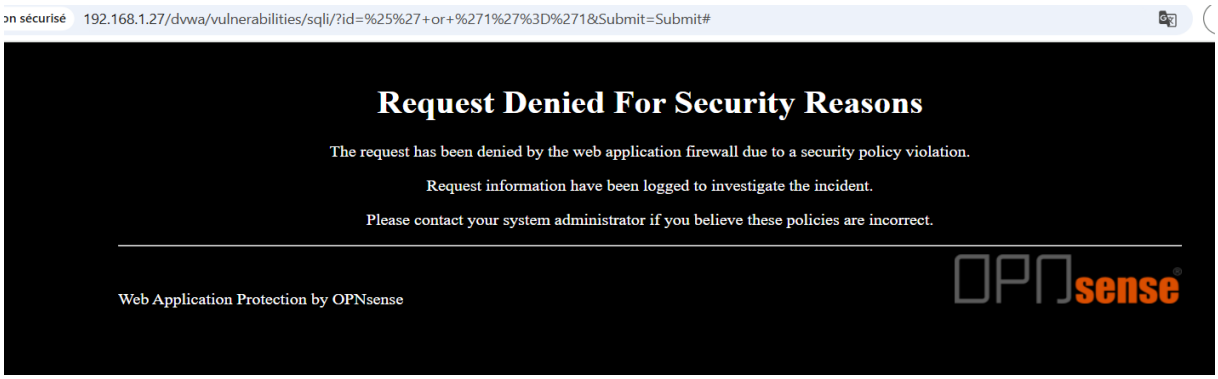
Mettez le niveau de sécurité en mode faible pour tester les commandes de bases de SQL injection.

Injection sql : `%' or '1'='1`

Injection sql : `'UNION SELECT table_name, NULL FROM information_schema.tables -`

XSS Stored : <script>alert("Hack"+document.cookie);</script>

Résultats :



Conclusion

À la fin de cet atelier, vous avez appris à configurer un Web Application Firewall (WAF) en utilisant NGINX/NAXSI sur OPNsense. Vous avez installé NGINX, ajouté des upstreams, activé NAXSI, créé des règles de filtrage et testé leur efficacité. Cette configuration renforce la sécurité de votre serveur web contre les attaques courantes comme SQL injection.
