# Guide d'Installation et Configuration - Scanner de Vulnérabilités (SAE302)

Ce document détaille la procédure pour installer le scanner sur une machine virtuelle Linux (Debian/Ubuntu), configurer le serveur Web Apache en proxy inverse, et lancer le backend Java.

## 1. Environnement de la Machine Virtuelle

La machine virtuelle utilisée pour ce projet est basée sur le système d'exploitation Linux. Ce choix offre une plateforme robuste et flexible, essentielle pour les tâches de développement et d'administration système liées au SAE.

## 2. Outils Installés

Deux outils principaux ont été installés et configurés sur la VM Linux pour répondre aux besoins spécifiques du SAE : Nmap et un serveur web.

### 2.1. Nmap (Network Mapper)

Nmap est un utilitaire d'exploration de réseau et un outil de sécurité/audit.

- Rôle dans la SAE **:** Nmap a été utilisé pour :
    - Vérifier les ports ouverts sur d'autres machines cibles .
    - Identifier les services et les versions des applications en cours d'exécution.
    - Tester la connectivité et la visibilité de la VM sur le réseau.

Pour installer Nmap, les commandes utilisés sont les suivantes :

- Debian/Ubuntu **:** sudo apt update puis sudo apt install nmap

```
dm300753@debian:~$ su
Mot de passe :
root@debian:/home/dm300753# apt-get update
Atteint : 1 http://security.debian.org/debian-security trixie-security InRelease
Atteint : 2 http://deb.debian.org/debian trixie InRelease
Atteint : 3 http://deb.debian.org/debian trixie-updates InRelease
Lecture des listes de paquets... Fait
```

```
root@debian:/home/dm300753# apt install nmap
Installation de :
  nmap

Installation de dépendances :
  liblinear4  nmap-common

Paquets suggérés :
  liblinear-tools  liblinear-dev  ncat  ndiff  zenmap

Sommaire :
  Mise à niveau de : 0. Installation de : 3Supprimé : 0. Non mis à jour : 0
Taille du téléchargement : 6 364 kB
  Espace nécessaire : 27,5 MB / 13,7 GB disponible

Continuer ? [O/n] 
```

appuyez sur o + entrée

```
Réception de : 1 http://deb.debian.org/debian trixie/main amd64 liblinear4 amd64 2.3.0+dfsg-5+b2 [41,7 kB]
Réception de : 2 http://deb.debian.org/debian trixie/main amd64 nmap-common all 7.95+dfsg-3 [4 392 kB]
Réception de : 3 http://deb.debian.org/debian trixie/main amd64 nmap amd64 7.95+dfsg-3 [1 931 kB]
6 364 ko réceptionnés en 0s (24,3 Mo/s)
Sélection du paquet liblinear4:amd64 précédemment désélectionné.
(Lecture de la base de données... 137993 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../liblinear4_2.3.0+dfsg-5+b2_amd64.deb ...
Dépaquetage de liblinear4:amd64 (2.3.0+dfsg-5+b2) ...
Sélection du paquet nmap-common précédemment désélectionné.
Préparation du dépaquetage de .../nmap-common_7.95+dfsg-3_all.deb ...
Dépaquetage de nmap-common (7.95+dfsg-3) ...
Sélection du paquet nmap précédemment désélectionné.
Préparation du dépaquetage de .../nmap_7.95+dfsg-3_amd64.deb ...
Dépaquetage de nmap (7.95+dfsg-3) ...
Paramétrage de liblinear4:amd64 (2.3.0+dfsg-5+b2) ...
Paramétrage de nmap-common (7.95+dfsg-3) ...
Paramétrage de nmap (7.95+dfsg-3) ...
Traitement des actions différées (« triggers ») pour man-db (2.13.1-1) ...
Traitement des actions différées (« triggers ») pour libc-bin (2.41-12) ...
```

## 2.2. Installation des services (Java & Apache)

### 2.2.1 Installation d'Apache sur Debian

Connectez-vous à votre terminal et exécutez les commandes suivantes en tant que `root` ou avec `sudo` :

Bash

```
# Mise à jour des dépôts
sudo apt update

# Installation d'Apache
sudo apt install apache2 -y

# Activation des modules nécessaires pour la redirection (Proxy) vers Java
sudo a2enmod proxy
sudo a2enmod proxy_http

# Redémarrage d'Apache pour appliquer les modules
sudo systemctl restart apache2
```

#### 2.2.1.1 Installation de Java

sudo apt install default-jdk -y

### 2.2.2 Déploiement des fichiers

Apache sert par défaut les fichiers situés dans `/var/www/html`.

1. Telecharger SAE302-main sur le github : https://github.com/JohanAbd/SAE302
2. Copiez les fichiers au bon endroit : cp -R /SAE302-main/www /var
3. Assurez-vous que les permissions sont correctes :

```
sudo chown -R www-data:www-data /var/www/html
sudo chmod -R 755 /var/www/html
sudo chmod -R 755 /var/www
```

### 2.2.3 Configuration du Proxy Apache

Il faut dire à Apache : *"Si une requête arrive sur `/api`, envoie-la au programme Java"*.

1. Créez un fichier de configuration : `sudo nano /etc/apache2/sites-available/sae302.conf`
2. Collez la configuration suivante :

```
Apache
<VirtualHost *:80>
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html

    # Redirection des appels API vers le backend Java (port 8080)
```

```
    ProxyPreserveHost On
    ProxyPass /api http://127.0.0.1:8080/api
    ProxyPassReverse /api http://127.0.0.1:8080/api

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

3. Activez le site et désactivez celui par défaut :

```
sudo a2ensite sae302.conf
sudo a2dissite 000-default.conf
sudo systemctl reload apache2
```

## 2.3. La base de données

sudo apt-get install sqlite3

Se placer dans `/var/www :`

sqlite3 bd.db < init_db.sql

chmod 666 /var/www/bd.db

# 3. Lancement du Site Web

## 3.1 Se placer au bon endroit

Bien se placer dans `/var/www`.

cd /var/www

## 3.2 Compiler les fichiers

Avant de **lancer** (`java`), il faut **compiler** (`javac`). Pour que cela fonctionne, tu dois avoir tes bibliothèques (JAR) dans un dossier `libs`.

Exécute cette commande pour compiler tout le projet d'un coup :

javac -cp ".:libs/*" *.java

*Si cette commande réussit, tu verras apparaître des fichiers `.class` dans ton dossier.*

### 3.3 Lancer le serveur

Une fois compilé, lance la commande :

java -cp ".:libs/*" WebServer

Tu devrais voir apparaître sur la console :
“Backend Java API démarré sur le port 8080
Le site est accessible via Apache : http://localhost”

Le site est aussi accessible sur http://IP:80

## 3. Vérification du fonctionnement

1. **Accès au site** : Ouvrez un navigateur sur `http://[IP_DE_VOTRE_VM]`.
2. **Connexion** : Utilisez les identifiants configurés (admin / admin123).
3. **Scan** : Lancez un scan sur une IP (ex: `192.168.1.1`).
4. **Résultats** : Allez sur la page des vulnérabilités. Si elles s'affichent avec les bordures de couleur (rouge, orange, vert), la configuration est réussie.