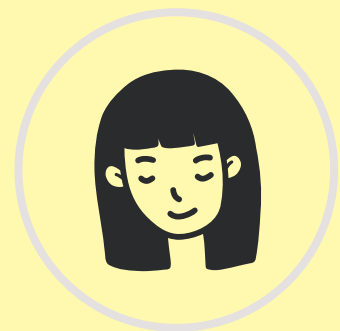


# SSL-TLS

Cours de CyberSecurity



**Ikram KOUIBAATI**

---



**Annabelle BOSSE**

---



# Table de matières

## Key Points

---

- ☐ Introduction
- ☐ Considérations légales et éthiques
- ☐ Concept et Objectifs
- ☐ Explication des Diagrammes
- ☐ Benchmark des Solutions Existantes
- ☐ Démonstration du Code
- ☐ Implémentation et Développement
- ☐ Tests et Validation
- ☐ Workflow GitHub Actions
- ☐ Conclusion

# Introduction

## Problématique

Certains serveurs utilisent encore des versions obsolètes et des suites de chiffrement faibles.

## Objectif du Projet

- Créer un outil capable de détecter ces vulnérabilités.
- Simplifier l'analyse grâce à l'automatisation du scan et la génération d'un rapport détaillé.

## CONTEXTE

La sécurisation des communications en ligne repose sur les protocoles SSL/TLS.








## Considérations Légales

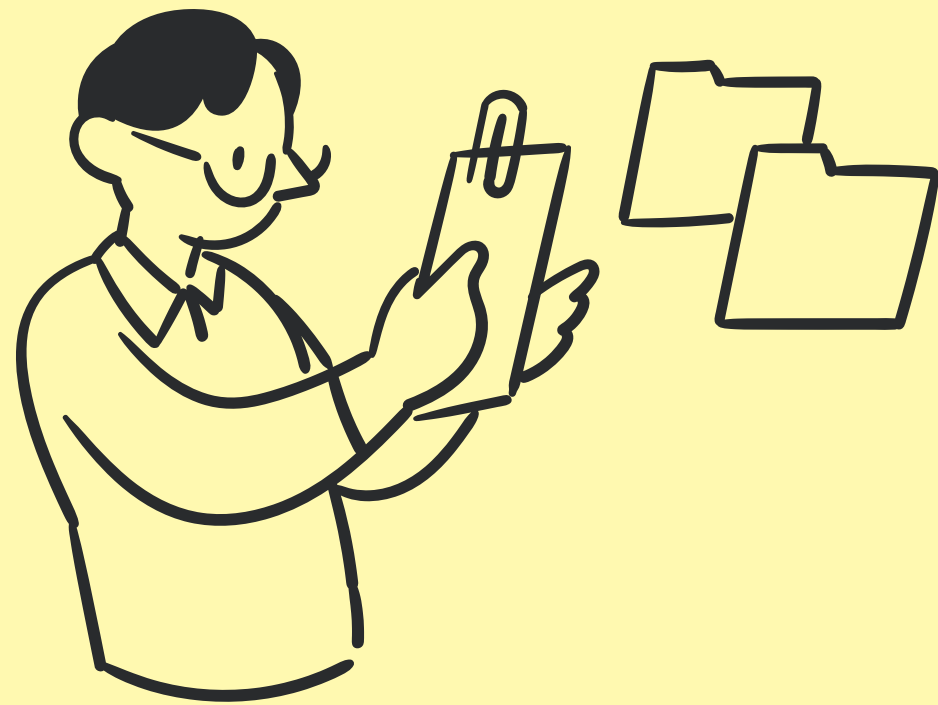
-  Respect de la Législation en Cybersécurité
-  Autorisation et Consentement
-  Protection des Données



## 2. Considérations Éthiques

-  Renforcement de la Sécurité
-  Utilisation Responsable
-  Partage des Bonnes Pratiques





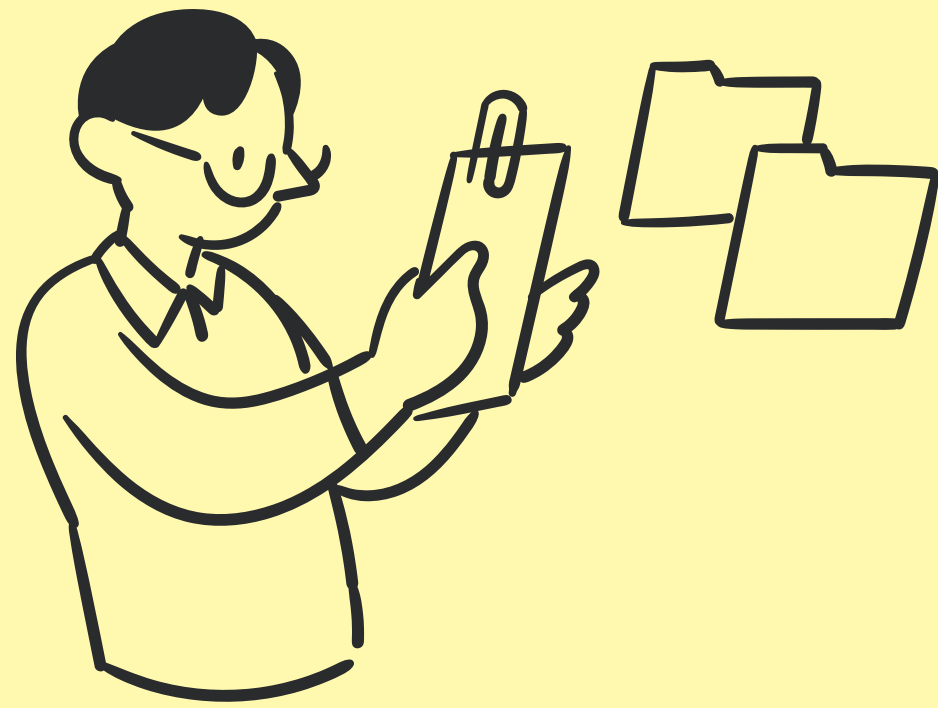
# Benchmark des Solutions Existantes

**Pourquoi Créer une Nouvelle Solution ?**

## Solutions existantes

---

- ☐ **SSL Labs de Qualys :**
  - Analyse détaillée des configurations SSL/TLS.
  - Limité à une utilisation en ligne, pas d'intégration dans des workflows automatisés.
- ☐ **SSLscan :**
  - Outil en ligne de commande rapide et léger.
  - Nécessite des compétences techniques avancées.
- ☐ **DigiCert Vulnerability Scanner :**
  - Analyse les certificats TLS pour détecter les vulnérabilités.
  - Spécifique aux certificats DigiCert, pas de scan des ports.
- ☐ **SSL.com Best Practices :**
  - Guide théorique avec recommandations pour une configuration sécurisée.
  - Pas d'outil de scan intégré.



# Benchmark des Solutions Existantes

Pourquoi Créer une Nouvelle Solution ?

## 2. Limites des Outils Existants :

---

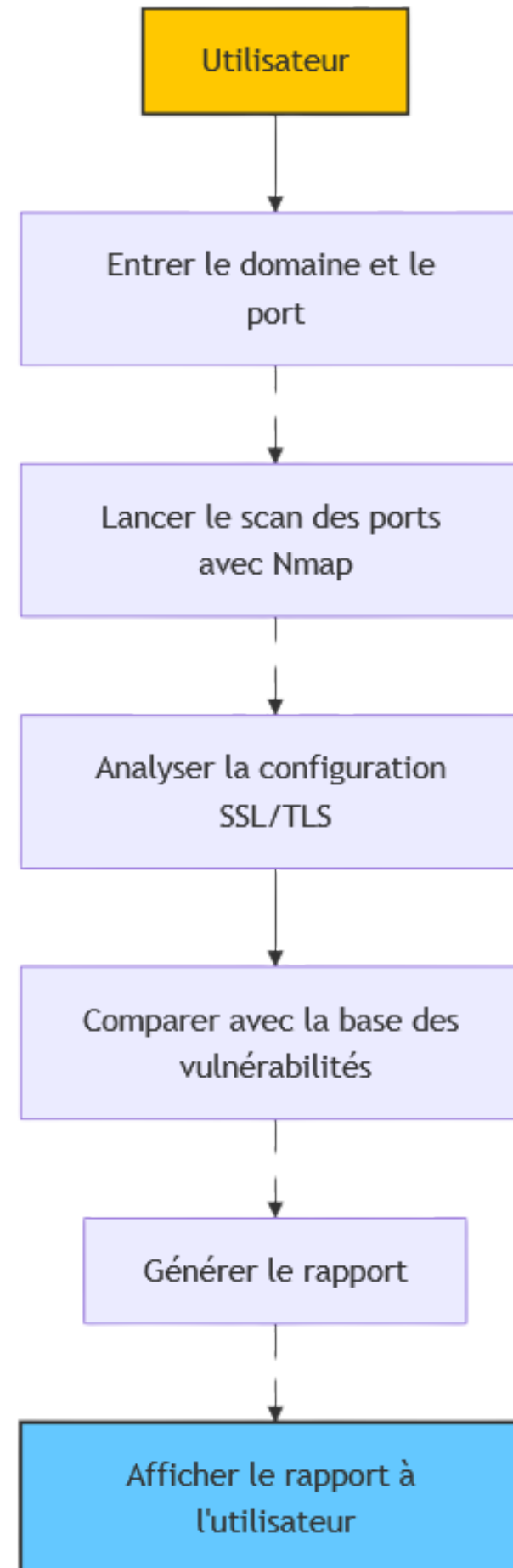
- ✗ Peu d'options pour une intégration dans des pipelines CI/CD.
- ✗ Manque d'automatisation pour les tests récurrents.
- ✗ Interfaces parfois complexes et non adaptées aux non-experts.

## 3. Pourquoi Créer un Nouveau Scanner

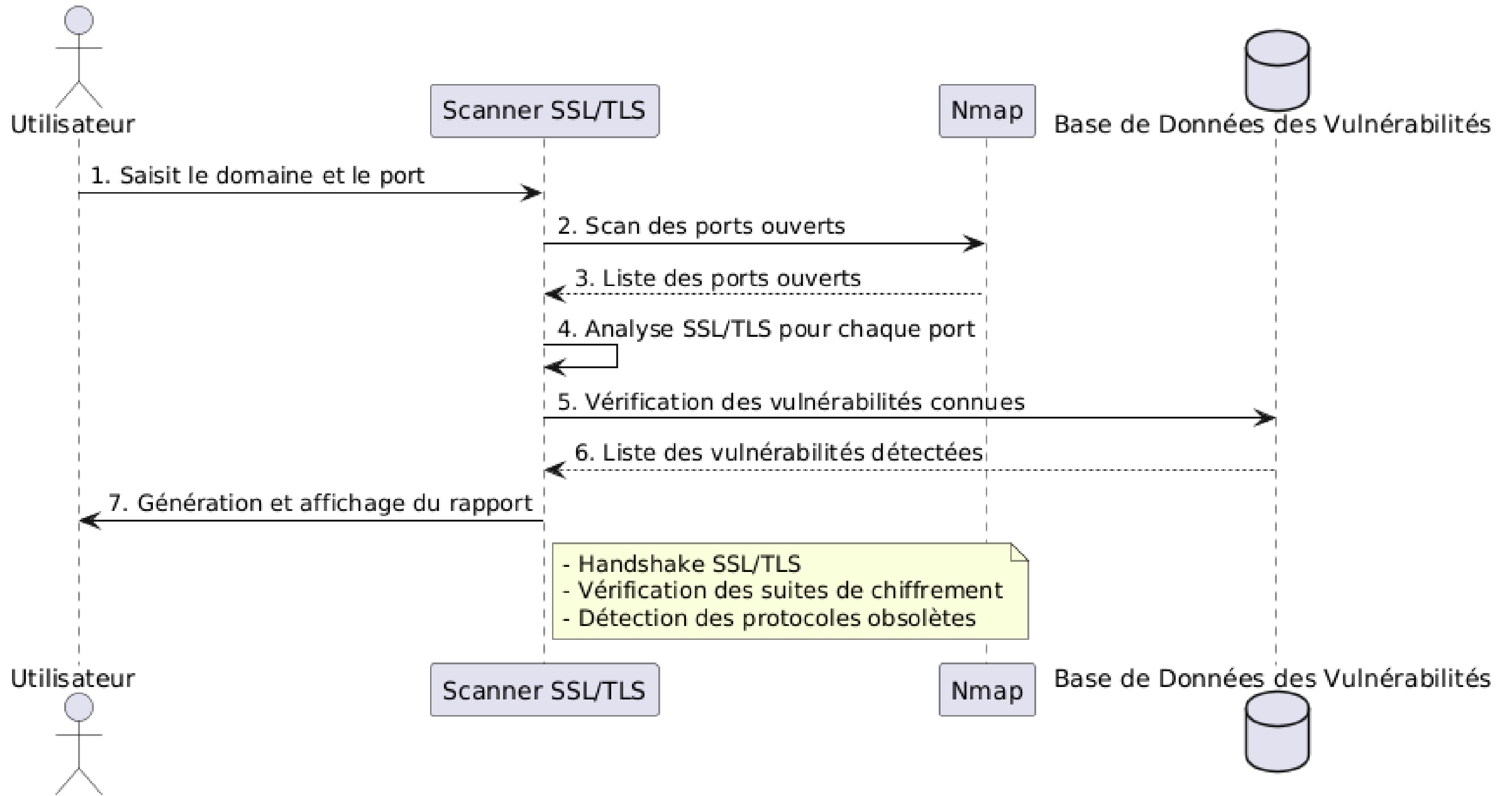
---

- ✓ Automatisation.
- ⚡ Performance
- 📋 Rapport Personnalisé
- 💻 Accessibilité

# Diagramme de Workflow (Vue Globale du Processus)

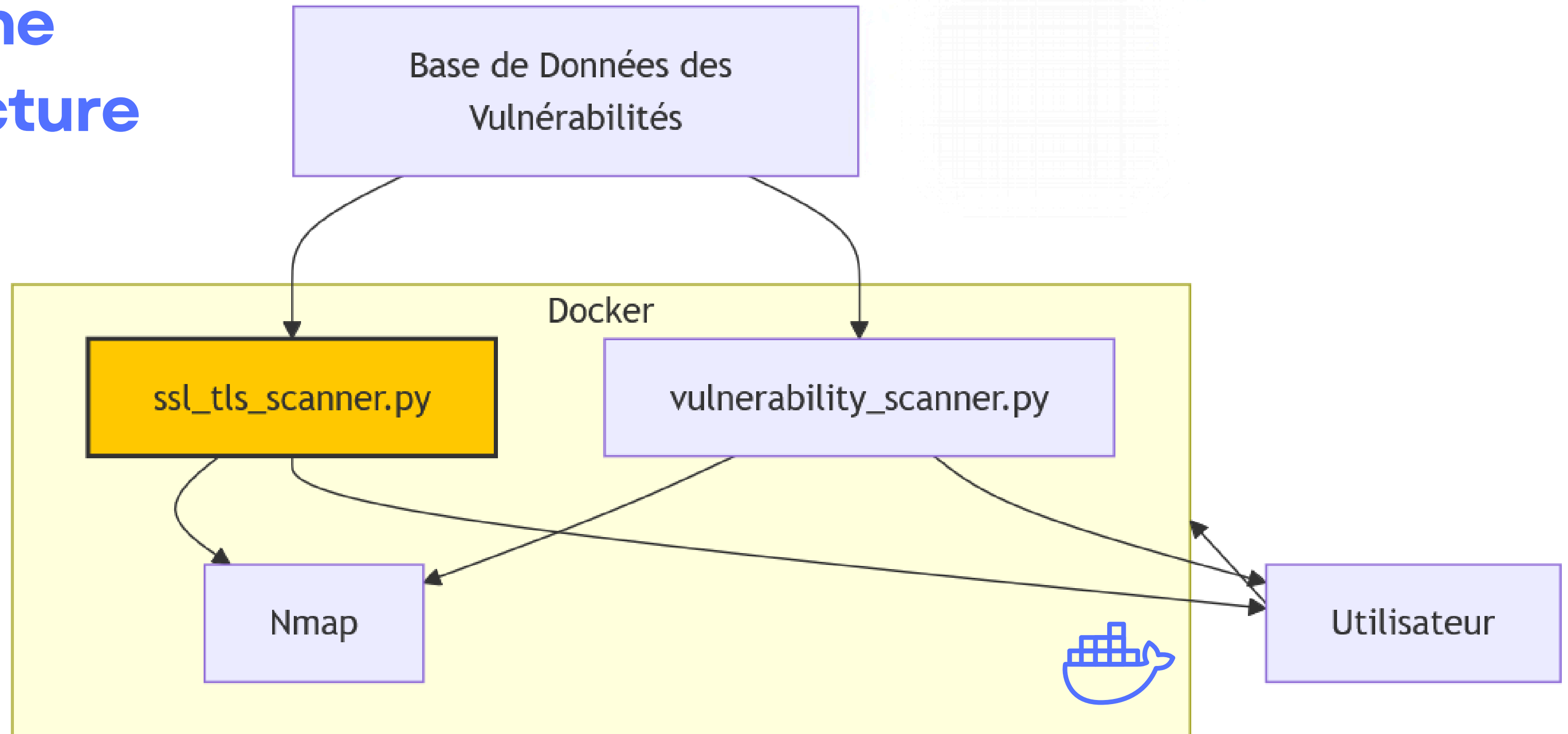


# Diagramme de Séquence





# Diagramme d'architecture



# Développement du Scanner SSL/TLS



## Technologies Utilisées :

---

- ☐ **Langage : Python 3.10**
- ☐ **Modules Principaux :**
  - ssl et socket pour le handshake SSL/TLS
  - OpenSSL pour la gestion des certificats
  - nmap pour le scan des ports ouverts

## Fonctionnalités Principales :

---

- ☐ **Analyse SSL/TLS**
- ☐ **Vérification des Vulnérabilités**
- ☐ **Scan des Ports**
- ☐ **Génération de Rapports**