# RAPPORT DE STAGE II

Filière : **Cybersécurité et Confiance Numérique (CCN)**

3ème année Cycle Ingénieur

---

# Développement d'un Scan Web avec Greenbone Vulnerability Management (GVM)

---

Réalisé à : Le Centre National pour la Recherche Scientifique et Technique (CNRST)
du 1er juillet 2025 au 30 août 2025


**Réalisé par :**
Karim Badreddine

**Encadré par :**
M. Redouane MERROUCH


Année universitaire : 2024-2025

# Remerciement

Je tiens à exprimer ma profonde gratitude à mon encadrant au sein de **MARWAN**, **M. Redouane Merrouch**, pour son accueil chaleureux, sa disponibilité et ses précieux conseils tout au long de ce stage. Son expertise technique et sa vision stratégique ont largement contribué à l'aboutissement de ce projet.

Mes remerciements s'adressent également à l'ensemble de l'équipe **MARWAN** pour leur soutien constant, leur esprit de collaboration et les échanges enrichissants qui ont jalonné cette expérience. Leur implication et leur partage d'expérience ont été déterminants pour la réussite du projet.

Je souhaite aussi remercier le **Centre National pour la Recherche Scientifique et Technique (CNRST)** pour m'avoir offert l'opportunité de réaliser ce stage au sein d'un environnement aussi stimulant, au cœur des enjeux de la cybersécurité dans le secteur académique marocain.

Enfin, j'adresse un remerciement particulier à mes collègues et camarades pour leurs encouragements, leurs retours constructifs et leur aide précieuse, qui ont contribué à enrichir cette expérience professionnelle et humaine.

# Résumé

Ce rapport de stage présente une analyse approfondie de la conception et du développement d'une plateforme web permettant aux universités marocaines connectées au réseau **MARWAN** de lancer, planifier et suivre des scans de vulnérabilités à l'aide du moteur **Greenbone Vulnerability Management (GVM/OpenVAS)**.

En tant qu'étudiant à l'**ENSA El Jadida**, filière **Cybersécurité et Confiance Numérique**, j'ai eu l'opportunité d'effectuer un stage au sein du **Centre National pour la Recherche Scientifique et Technique (CNRST)**, plus précisément dans la division **MARWAN**, chargée de la gestion du réseau académique et de recherche marocain.

Ce projet s'inscrit dans un contexte où la sécurité des infrastructures réseau est devenue une priorité stratégique pour les universités, face à la multiplication des cyberattaques et des vulnérabilités non corrigées. L'objectif principal a été de fournir un outil centralisé, accessible et sécurisé, permettant aux établissements d'effectuer eux-mêmes des audits de sécurité tout en optimisant le temps de traitement et la standardisation des rapports.

Le rapport est structuré en plusieurs chapitres présentant le contexte institutionnel, la problématique, les solutions techniques retenues, ainsi que la méthodologie de mise en œuvre. Une attention particulière est portée à l'intégration de **GVM/OpenVAS** dans un environnement Docker, à l'automatisation des tâches via une API, et à la conception d'une interface web intuitive. Ce travail met en lumière comment l'utilisation d'outils open source peut renforcer la posture de cybersécurité des institutions tout en restant économiquement viable.

**Mots-clés** : cybersécurité, GVM, OpenVAS, scan de vulnérabilités, MARWAN, CNRST, réseau universitaire, Docker, API, interface web.

# Abstract

This internship report provides an in-depth analysis of the design and development of a web platform enabling Moroccan universities connected to the **MARWAN** network to launch, schedule, and monitor vulnerability scans using the **Greenbone Vulnerability Management (GVM/OpenVAS)** engine. As a student at **ENSA El Jadida**, majoring in **Cybersecurity and Digital Trust**, I had the opportunity to carry out an internship within the **Centre National pour la Recherche Scientifique et Technique (CNRST)**, specifically in the **MARWAN** division, responsible for managing the Moroccan academic and research network.

This project addresses the growing need for robust network security in universities, as cyberattacks and unpatched vulnerabilities become increasingly frequent. The primary goal was to provide a centralized, accessible, and secure tool enabling institutions to conduct their own security audits while improving efficiency and standardizing reporting.

The report is structured into several chapters covering the institutional context, the problem statement, the technical solutions adopted, and the implementation methodology. Special focus is given to the integration of **GVM/OpenVAS** in a Docker environment, the automation of tasks via an API, and the development of an intuitive web interface. This work highlights how open-source tools can strengthen the cybersecurity posture of institutions while remaining cost-effective.

**Keywords:** cybersecurity, GVM, OpenVAS, vulnerability scanning, MARWAN, CNRST, university network, Docker, API, web interface.

# Table des matières

# Table de figure

# Table de tableaux

# Table des abreviations

| | |
|---|---|
| CNRST | Centre National pour la Recherche Scientifique et Technique |
| MARWAN | Moroccan Academic and Research Wide Area Network |
| GVM | Greenbone Vulnerability Management |
| OpenVAS | Open Vulnerability Assessment System |
| VM | Virtual Machine |
| API | Application Programming Interface |
| CIDR | Classless Inter-Domain Routing |
| IP | Internet Protocol |
| VPN | Virtual Private Network |
| HTML | HyperText Markup Language |
| CSS | Cascading Style Sheets |
| JS | JavaScript |
| PDF | Portable Document Format |
| UI | User Interface |

# Introduction générale

Dans le cadre de mon Stage de 4ème Année, j'ai manifesté un vif intérêt pour un stage au **CNRST** (*Centre National pour la Recherche Scientifique et Technique*). Actuellement en quatrième année à l'**ENSAJ** dans la filière **Cybersécurité et Confiance Numérique**, cette expérience pratique de deux mois m'a permis de m'immerger dans le domaine de la **cybersécurité réseau**, en particulier à travers l'intégration d'outils open source pour l'audit de sécurité.

De nos jours, les organisations, en particulier celles gérant des infrastructures critiques comme le réseau universitaire marocain **MARWAN** (*Moroccan Academic and Research Wide Area Network*), sont confrontées à un nombre croissant de menaces et vulnérabilités. La nécessité de disposer d'outils centralisés et automatisés pour détecter, analyser et suivre les failles de sécurité est devenue un enjeu stratégique majeur.

Mon projet de stage s'inscrit précisément dans ce contexte : la **conception et le développement d'une plateforme web** permettant aux **universités et institutions connectées au réseau MARWAN** de lancer, de manière autonome, des scans de vulnérabilités à l'aide du moteur **Greenbone Vulnerability Management (GVM)**, basé sur **OpenVAS**. L'objectif est de fournir un outil simple, accessible via un navigateur, capable d'automatiser des analyses de sécurité et de générer des rapports exploitables pour les équipes techniques de chaque université.

Cette solution repose sur l'installation et la configuration de GVM dans un environnement virtualisé sécurisé, l'intégration d'une interface web interagissant avec l'API de GVM, et la mise en place d'un processus de scan automatisé. Elle vise à améliorer l'efficacité des opérations de sécurité, à réduire le temps de détection des vulnérabilités et à renforcer la posture de sécurité globale des établissements membres du réseau MARWAN.

Dans le **premier chapitre** « *Contexte et objectifs du stage* », nous présentons le CNRST et la division MARWAN, le contexte du projet, la problématique rencontrée et les objectifs poursuivis.

Dans le **deuxième chapitre** « *État de l'art et choix technologiques* », nous exposons les concepts clés liés à la gestion des vulnérabilités, les fonctionnalités de GVM/OpenVAS, et une comparaison avec d'autres solutions existantes.

Dans le **troisième chapitre** « *Conception et mise en œuvre* », nous détaillons l'architecture technique de la plateforme, les étapes de déploiement et d'intégration avec GVM, ainsi que les choix de développement.

Enfin, dans le **quatrième chapitre** « *Tests, résultats et perspectives* », nous présentons les scénarios de test réalisés, l'analyse des résultats obtenus, les problèmes rencontrés, et les perspectives d'amélioration de la solution.

# Chapter 1

# Contexte et objectifs du stage

# Introduction

Ce chapitre présente le cadre général du projet, en commençant par une présentation détaillée du CNRST, division MARWAN, sa problématique et sa solution.

# 1 Presentation de l'organisme d'accueil

Notre stage de 4ème année s'est déroulé au sein du **Centre National pour la Recherche Scientifique et Technique (CNRST)**, et plus précisément dans la division **MARWAN** (Moroccan Academic and Research Wide Area Network).

## 1.1 Présentation du CNRST

Le Centre national de Recherche Scientifique et Technique « CNRST » est un établissement public érigé par l'état pour soutenir et développer la recherche au Maroc en offrant des structures de mutualisation et permettre l'accès à l'information. Plus encore le CNRST dessine par actions successives, une politique de coordination de la recherche, qui pourrait utilement renforcer et orienter la dynamique actuelle du système de recherche scientifique national.

En effet, ces actions sont destinées à promouvoir, renforcer et valoriser la recherche dans les universités, les établissements de recherche et les établissements de formation des cadres. Les actions entreprises par le CNRST consistent à développer les activités de service et de la recherche au sein des unités propres, à renforcer les compétences de son personnel à travers un programme de formation continue et à améliorer sa gouvernance.

Il est à noter que le 1er aout 2001 la loi n°80 00 relative au Centre National pour la Recherche Scientifique et Technique (CNRST) a été promulguée.

## 1.2 Mission du CNRST

Comme tout autre organisme le CNRST a plusieurs missions, en effet il doit :

- Procéder à l'évaluation et assurer le suivi de toutes les activités de recherche ou de services dans lesquelles il est impliqué.
- Effectuer des prestations de services au profit des opérateurs de recherche et contribuer à la valorisation et au transfert des résultats de recherche.
- Mettre en œuvre des programmes de recherche et de développement technologique dans le cadre des choix et priorités fixés par l'autorité gouvernementale de tutelle.
- Apporter son concours au renforcement de l'infrastructure nationale de recherche.
- Créer des synergies entre les différentes équipes de recherche qui travaillent sur des thématiques prioritaires (réseaux, pôles de compétence).
- Etablir des conventions ou contrats d'association, dans le cadre des activités de recherche ou des services, avec les établissements et organismes de recherche publics ou privés.

## 1.3 Unités et services

Le CNRST est constitué de deux départements. Un département administratif et un autre scientifique qui s'articule sur quatre divisions :

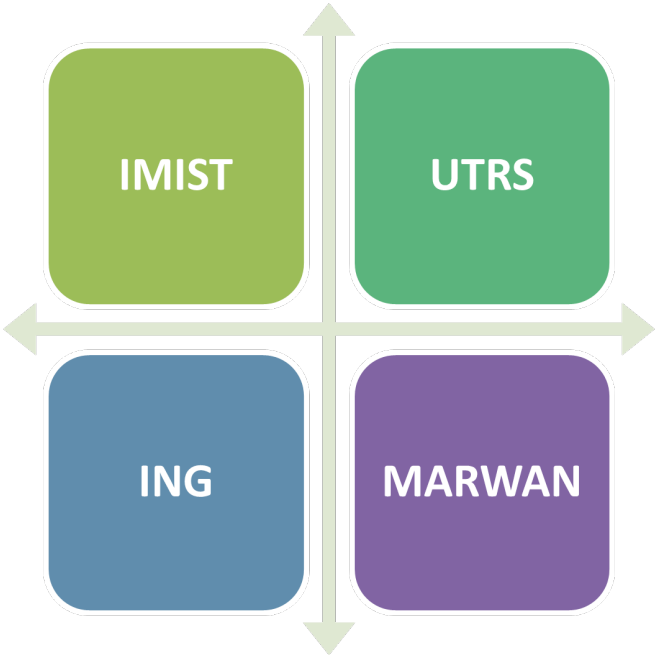


Figure 1.1: Le département scientifique du CNRST

- **IMISIT:** L'institut Marocain de l'information Scientifique et Technique relève du CNRST en sa qualité d'opérateur de la recherche, il est chargé actuellement de la documentation et de la diffusion de l'information scientifique.
- **UATRS:** Les Unités d'Appui Techniques à la Recherche Scientifique. Elles mettent à la disposition de la communauté scientifique un parc d'instrumentation à la fine pointe de la technologie et proposent des prestations analytiques couvrant les domaines de la chimie, de la biologie et des matériaux.
- **ING:** L'Institut National de Géophysique est chargé d'assurer la surveillance et l'alerte sismique du territoire national, 24H/24 et 7j/7.
- **MARWAN:** Moroccan Academic and Research Wide Area Network créé en 1998, est le Réseau National de l'Enseignement et de la Recherche. Il a pour objectif de mettre en place une infrastructure d'information et de communication entre les établissements de formation et d'enseignement.

## 1.4 Présentation de MARWAN

MARWAN est la division chargée de la gestion du réseau national dédié aux universités et institutions d'enseignement et de recherche marocaines, en effet elle a pour objectif de répondre aux besoins de ces établissements et de leur assurer une infrastructure de communication haut débit, fiable et perfomante avec une interconnexion avec Internet et autres réseaux internationnaux équivalents.
La division MARWAN offre plusieurs autres services , en effet elle a mis en place des services aux profit des universités comme :

- **MAGRID:** Qui est un centre de calcul de haute performance et qui doit répondre aux besoins des universités en terme de puissance de calcul et de capacité de stockage.
- **EDUROAM:** Qui vise à offrir un accès sans fil sécurisé, aux personnels et aux étudiants des établissements d'enseignement supérieur et de recherche, et ceci à un niveau mondial, sur l'ensemble des sites adhérents.
- **EDUIDM:** C'est le service de la fédération d'identité.
- **Certificat**, **IPV6**, **VisioConférence** ...

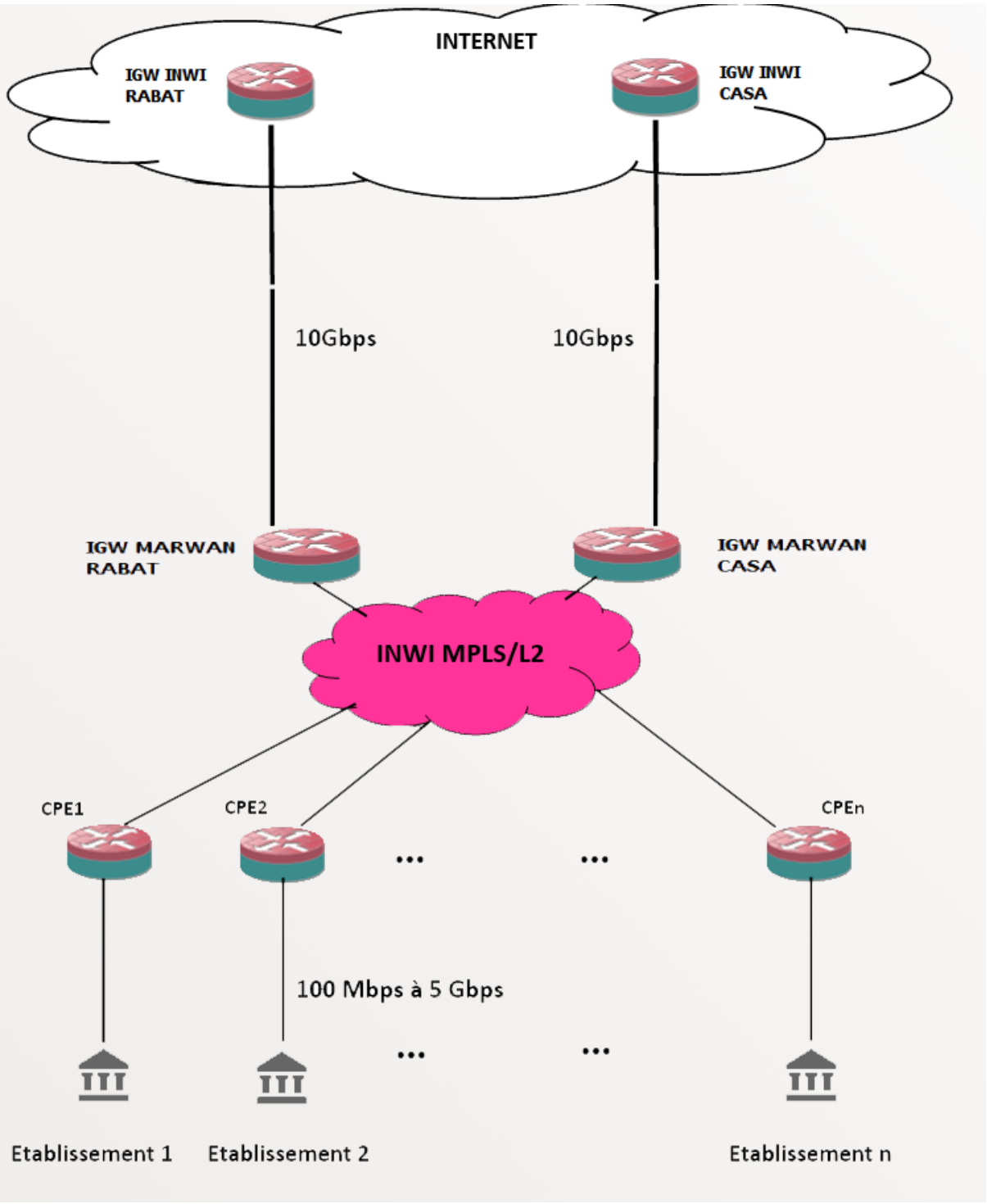


Figure 1.2: Architecture du réseau MARWAN

## 2 Contexte et enjeux de la cybersécurité réseau

Dans un monde numérique en constante évolution, les réseaux académiques et de recherche constituent des infrastructures stratégiques. Ils interconnectent des milliers d'utilisateurs et hébergent des données sensibles (scientifiques, académiques et administratives).

Le réseau MARWAN, en tant que cœur de la communication universitaire nationale, est exposé à un large éventail de menaces : attaques par déni de service, intrusions, compromission de serveurs, et exploitation de vulnérabilités non corrigées.
Ces menaces peuvent avoir des impacts critiques : interruption des services éducatifs, exfiltration de données confidentielles ou encore atteinte à la réputation des institutions.

Dans ce contexte, il devient impératif pour MARWAN et le CNRST de se doter d'outils de **gestion des vulnérabilités**, capables de détecter, analyser et rapporter efficacement les failles de sécurité afin de renforcer la résilience du réseau.

## 3 Problématique du projet

Actuellement, les scans de vulnérabilités sont souvent réalisés de manière ponctuelle et nécessitent une expertise technique importante. Les universités, en tant que « clients » du réseau MARWAN, doivent disposer d'une solution centralisée leur permettant de lancer des analyses de sécurité de manière autonome et contrôlée.

La problématique principale est donc :

- Comment concevoir une **plateforme web intuitive** permettant aux universités de déclencher des scans réseau ?
- Comment intégrer et automatiser le moteur **GVM (OpenVAS)** au sein de cette plateforme pour assurer la détection efficace des vulnérabilités ?
- Comment garantir la **sécurité**, la traçabilité et la performance des opérations dans un environnement partagé entre plusieurs institutions académiques ?

## 4 Objectifs et résultats attendus

L'objectif global du projet est de développer une plateforme web de scan de vulnérabilités intégrée au moteur **GVM (OpenVAS)**.

Les objectifs spécifiques sont :

- Installer et configurer GVM dans un environnement virtualisé sécurisé.
- Concevoir une interface web simple permettant aux universités de lancer des scans sur leurs propres infrastructures.
- Automatiser l'exécution des scans et la génération de rapports.
- Permettre la visualisation et l'export des résultats (HTML, PDF, XML).

- Mettre en place des mécanismes de contrôle d'accès pour garantir une utilisation sécurisée.

Les résultats attendus incluent une première version fonctionnelle de la plateforme, capable de réaliser des scans basiques sur des adresses IP ou des sous-réseaux, et de restituer les résultats sous forme de rapports exploitables.

# 5 Méthodologie adoptée

Pour atteindre ces objectifs, la méthodologie suivie s'articule en plusieurs étapes :

- **Étude bibliographique** : analyse des concepts liés à la gestion des vulnérabilités et comparaison des solutions existantes.
- **Mise en place de l'environnement** : installation d'Ubuntu Server, configuration de Docker et déploiement de GVM.
- **Conception de la plateforme** : définition de l'architecture technique (frontend, backend, intégration API).
- **Développement et intégration** : implémentation des modules de scan et de reporting.
- **Tests et validation** : lancement de scans expérimentaux, vérification de la performance et de la fiabilité des résultats.

Cette méthodologie garantit un équilibre entre **recherche théorique** et **implémentation pratique**, assurant ainsi la réussite du projet.

# Conclusion

Ce projet de chatbot intelligent pour MARWAN, combinant fine-tuning de LLM et RAG, représente une solution innovante pour répondre aux défis opérationnels et techniques du support utilisateur.

# Chapter 2

# État de l'art et choix technologiques

# 1 Gestion des vulnérabilités : concepts et enjeux

La gestion des vulnérabilités est un processus essentiel en cybersécurité visant à identifier, analyser, prioriser et corriger les faiblesses présentes dans un système d'information. Une vulnérabilité est une faille de sécurité dans un logiciel, un système d'exploitation ou une configuration pouvant être exploitée par un attaquant pour compromettre la confidentialité, l'intégrité ou la disponibilité des données.

Les étapes typiques de la gestion des vulnérabilités incluent :

- **Identification** : utilisation d'outils de scan pour détecter les failles connues.
- **Évaluation** : classification des vulnérabilités selon leur criticité (basée sur le score CVSS – Common Vulnerability Scoring System).
- **Remédiation** : application de correctifs (patching), reconfiguration des systèmes, ou mise en place de mesures compensatoires.
- **Suivi** : vérification continue pour s'assurer que les vulnérabilités ont été corrigées.

Les enjeux principaux sont : la protection des données sensibles, la réduction du risque d'intrusions, la conformité réglementaire et l'amélioration de la résilience des infrastructures critiques.


Figure 2.1: Cycle de vie de la gestion des vulnérabilités

# 2 Présentation de Greenbone Vulnerability Management (GVM) et OpenVAS

Greenbone Vulnerability Management (GVM) est une solution open source de gestion des vulnérabilités reposant sur le moteur de scan OpenVAS (Open Vulnerability Assessment System). Elle utilise une base de tests appelée **NVTs (Network Vulnerability Tests)** permettant d'identifier des milliers de failles connues.

## Architecture de GVM

Un déploiement standard de GVM est composé de plusieurs modules :

- **OpenVAS Scanner** : le moteur qui exécute les tests de vulnérabilité.
- **Greenbone Vulnerability Manager (gvmd)** : gestion des configurations, des scans et des résultats.
- **Greenbone Security Assistant (GSA)** : interface web pour l'administration et le lancement de scans.
- **Feed NVTs** : base de données de vulnérabilités mise à jour régulièrement.

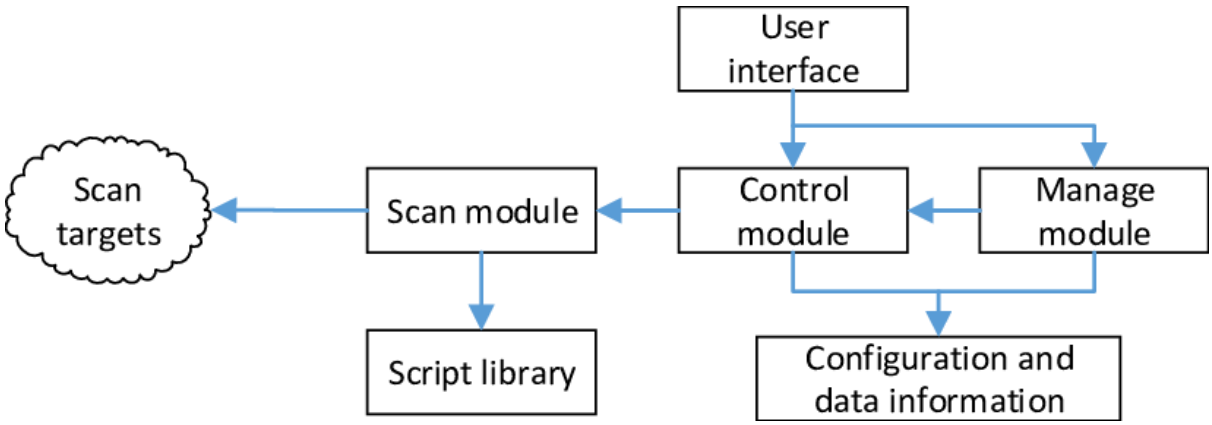


Figure 2.2: Architecture de GVM/OpenVAS

# 3 Comparaison avec d'autres outils (Nessus)

Pour justifier le choix de GVM, il est utile de le comparer à un outil propriétaire très utilisé : **Nessus**.

| **Critère** | **GVM / OpenVAS (Greenbone)** | **Nessus (Tenable)** |
|---|---|---|
| **Licence** | Open source, gratuit | Propriétaire, payant (sauf version limitée Nessus Essentials) |
| **Base de vulnérabilités** | NVT Feed (Greenbone Community / Enterprise) | Base Tenable, mise à jour payante |
| **Interface utilisateur** | Web (GSA) + API | Web + API |
| **Automatisation** | Oui (scripts, API REST) | Oui (intégrations avancées) |
| **Popularité** | Très utilisé en académique et institutions publiques | Très utilisé en entreprise |
| **Coût** | Gratuit (communautaire) | Abonnement annuel (licences commerciales) |
| **Support** | Communauté + version entreprise | Support professionnel complet |

Table 2.1: Comparaison entre GVM/OpenVAS et Nessus

# 4 Raisons du choix de GVM pour le projet

Le choix de GVM pour ce projet s'explique par plusieurs raisons :

- Solution **open source et gratuite**, adaptée au contexte académique.
- **Mises à jour régulières** via les feeds communautaires et professionnels.
- **Flexibilité d'intégration** grâce à son API, idéale pour une intégration dans la plateforme web.
- **Adéquation au contexte institutionnel** : largement adopté dans les universités et organismes publics.
- **Support communautaire actif**, facilitant l'installation et le dépannage.

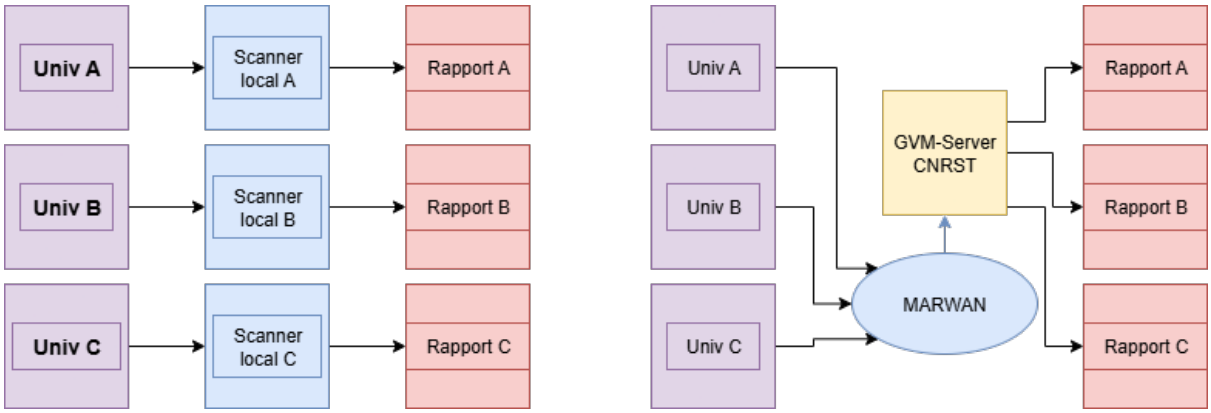


Figure 2.3: Comparaison entre scanning centralisé via GVM et scanning manuel par université