REPUBLIQUE DU BENIN
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR
ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE D'ABOMEY CALAVI

INSTITUT DE FORMATION ET DE RECHERCHE EN INFORMATIQUE

01 BP 526 Cotonou – Bénin
Tel : +229 95 028 070 / 53 973 060
https://www.ifri-uac.bj
Courriel : contact@ifri.uac.bj

PLAN DE REDACTION DU MEMOIRE

Pour l'obtention du

Diplôme de Licence en Informatique
Option : Sécurité Informatique

THEME

Intégration de Snort avec un SIEM Wazuh pour la protection du serveur web de l'ABMS

Nom et prénoms de l'étudiant :
ZINZINDOHOUE Sèdjro Ottmare Josèphina

Sous la supervision de :
SAHO Nelson

Année Académique : 2024 - 2025

PLAN DU MÉMOIRE

I - INTRODUCTION GÉNÉRALE

- Contexte et problématique.
- Objectifs du mémoire.
- Présentation de l'entreprise.

II - DÉVELOPPEMENT

Chapitre 1 : Revue de littérature

- **1.1 La sécurité des serveurs web**
  - Les menaces actuelles sur les serveurs web.
  - Le Top 10 OWASP 2025 : présentation et pertinence.
  - Choix sur l'injection SQL et le brute force.
- **1.2 Les systèmes de détection d'intrusion (IDS)**
  - Définition et types d'IDS.
  - Présentation de Snort : architecture et fonctionnement.
  - Les règles Snort.
- **1.3 Les systèmes SIEM**
  - Définition et rôle d'un SIEM.
  - Présentation de Wazuh : architecture et fonctionnement.
  - Intégration IDS/SIEM : état de l'art.

Chapitre 2 : Analyse, choix techniques et implémentation

- **2.1 Présentation de l'environnement de travail**
  - Présentation de la structure d'accueil.
  - Contraintes rencontrées (absence de logs serveur).
  - Justification du choix des attaques via OWASP 2025.
- **2.2 Architecture de la solution proposée**
  - Topologie du réseau de test.
  - Outils et technologies retenus.
  - Environnement de virtualisation.

- **2.3 Installation et configuration de Snort**
  - Installation de Snort.
  - Configuration des règles de détection (SQL, Brute Force).
  - Tests de fonctionnement.
- **2.4 Installation et configuration de Wazuh**
  - Installation du serveur Wazuh.
  - Intégration de Snort comme source d'alertes.
  - Configuration des tableaux de bord.

Chapitre 3 : Présentation des résultats et perspectives

- **3.1 Simulation des attaques**
  - Simulation de l'injection SQL.
  - Simulation de l'attaque par brute force.
  - Outils utilisés pour les simulations.
- **3.2 Analyse des résultats**
  - Alertes générées par Snort.
  - Corrélation et visualisation dans Wazuh.
  - Analyse des logs et des tableaux de bord.
- **3.3 Évaluation de la solution**
  - Points forts de l'architecture déployée.
  - Limites identifiées.
- **3.4 Perspectives**
  - Améliorations possibles.
  - Pistes d'évolution.

III - CONCLUSION GÉNÉRALE

- Bilan du projet.
- Justification du choix des vecteurs d'attaque retenus.
- Recommandations et perspectives futures.