Wissal BOUTAYEB

Étudiante en 5e année d'ingénierie en cybersécurité | À la recherche d'un stage PFE en sécurité informatique à partir du 1er février 2026

0675061125 | wissalboutayeb182@gmail.com | Maroc | LinkedIn | Github

PROFIL

Élève ingénieure en troisième année du cycle d'ingénierie en cybersécurité à l'Université Euro-Méditerranéenne de Fès (UEMF), passionnée par la **sécurisation des systèmes d'information**, la cybersécurité offensive et défensive. Motivée, rigoureuse et curieuse, j'aime relever les défis techniques liés à la détection des menaces et à l'analyse de vulnérabilités. Je suis à la recherche d'un **stage de fin d'études (PFE) de six mois à partir du 1er février** pour approfondir mes compétences pratiques en cybersécurité.

EXPÉRIENCES PROFESSIONNELLES

Stagiaire Analyste Cybersécurité, CBI, Casablanca, Maroc **juill 2025-Oct 2025**

Déploiement d'une Solution DLP (Data Loss Prevention)

Piloté le déploiement d'une solution DLP basée sur **Microsoft Purview** pour renforcer la protection des données sensibles de l'organisation.

- **Conduit une analyse approfondie des risques** liés aux fuites potentielles de données au sein du système D'information.
- **Cartographié et identifié les flux critiques** de données à protéger
- **Classifié les données sensibles** selon leur niveau de criticité et défini des mesures de sécurité adaptées (audit, alerte, blocage).
- **Configuré et personnalisé les politiques DLP** sur les principaux canaux de communication (e-mails, web, endpoints, supports amovibles,etc).
- **Implémenté des règles de détection de contenu sensible** (données personnelles, documents internes confidentiels etc).
- **Réalisé des tests de scénarios de fuite** pour évaluer et optimiser l'efficacité des politiques de prévention.
- **Analysé les journaux d'événements (logs)** et **ajusté** les règles de sécurité en fonction des alertes détectées.

Stagiaire au Département Cybersécurité, JIFORB, Rabat, Kénitra, Maroc **juill 2024-août 2024**

Intégration de **Wazuh SIEM** et **Suricata IDS** pour la Détection des Menaces en Temps Réel

- **Installé, configuré et optimisé** la solution **Wazuh SIEM** pour la centralisation et la corrélation des événements de sécurité.
- **Déployé et configuré Suricata (IDS)** pour l'analyse approfondie du trafic réseau et la détection d'activités Malveillantes.
- **Intégré Suricata à Wazuh** afin d'assurer une **détection et corrélation des menaces en temps réel**

FORMATION

Université Euro-Méditerranéenne de Fès, Maroc, **Morocco** - *Cycle d'Ingénieur, Cybersécurité - (GPA: Mention Bien)* **Sept 2023 -En cours**

Université Euro-Méditerranéenne de Fès, Maroc, **Morocco** - *Classes Préparatoires Intégrée, Classes Préparatoires Intégrée - (GPA: Mention Très Bien)* **Sept 2021- Juin 2023**

Lycée Mohammed V Qualifiant de Meknès - *Baccalauréat, Sciences Physiques - (GPA: Mention Très Bien)* **Sept 2020 – Juin 2021**

PROJETS ACADEMIQUES

Déploiement de Honeypots pour l'Analyse et la Défense contre les Attaques

- Déployé et configuré **des honeypots** (**Dionaea**, **Cowrie**, **Honeyd**) pour simuler des cibles attractives et capturer des **Attaques**.
- Collecté et analysé les logs d'attaque pour caractériser les techniques adverses (exploits, malware, tentatives de connexion etc).
- Renforcé la sécurité des environnements honeypot via **AppArmor** et **Seccomp** pour limiter les risques d'évasion.
- Intégré **la stack ELK** (**Elasticsearch**, **Logstash**, **Kibana**) pour l'indexation et la visualisation centralisée des données D'attaque.

Détection de Menaces avec Snort (Intrusion Detection System)

- Installé et configuré Snort (**IDS**) pour identifier les scans de ports, attaques **DoS** et autres activités malveillantes.
- **Défini** des règles et **mis en place** des alertes en temps réel pour assurer une détection proactive
- Optimisé la journalisation pour un suivi détaillé des attaques.

Déploiement d'Active Directory sur Windows Server 2022

- Installé et configuré Active Directory Domain Services (AD DS) et mis en place des contrôleurs de domaine
- Configuré les **GPO** et appliqué **des politiques de sécurité** pour centraliser la gestion des comptes, permissions et baseline de sécurité.

Simulation d'une Attaque Evil Twin et Mise en Place d'un Système de Détection en Temps Réel via ELK Stack

- Créé **un point d'accès rogue** (**Hostapd** + **Dnsmasq**) pour simuler un Evil Twin et déployer un portail captif.
- **Intercepté le trafic** via **ARP spoofing et DNS spoofing** avec **Ettercap**
- Collecté, centralisé et visualisé en temps réel les données d'attaque via la stack **ELK**

COMPÉTENCES

Tests de pénétration : Nmap, Metasploit, Wireshark, Burp Suite, etc.
Sécurité des systèmes d'exploitation : Linux (SELinux, AppArmor, Seccomp), Windows & Active Directory
Administration systèmes et réseaux : Administration Linux, Sécurité réseau
DevSecOps & Automatisation : Ansible**,** Docker, Kubernetes, Keycloak
Cryptage et cryptographie, cloud et virtualisation
Supervision : Wazuh, ELK (Elasticsearch, Logstash, Kibana)
IDS/IPS : Suricata, Snort
Monitoring & Alerting: Zabbix
Pare-feu & Sécurité Réseau : Palo Alto
Administration des bases de données : MySQL, PL/SQL, Oracle
Langages de programmation : Python, PHP, C/C++, HTML/CSS/JavaScript, Java

COMPÉTENCES PERSONNELLES **:** Adaptabilité, Travail en Équipe et Collaboration, Gestion du Temps, Travail sous pression

LANGUES

Arabe : Langue maternelle
Français : Courant
Anglais : Intermédiaire
Espagnol : Notions de base