Wissal Boutayeb

Étudiante en 4 -ème année d'ingénierie en Cybersécurité | à la recherche d'un stage PFA en Sécurité Informatique.
+212675061125 | wissalboutayeb182@gmail.com | Maroc | LinkedIn | Github

Étudiante en 4 -ème année d'ingénierie en Cybersécurité à L'Université Euro-Méditerranéenne de Fès avec une solide base en sécurité du réseaux informatiques, administration Linux, configuration de serveurs, administration de bases de données, sécurité des systèmes d'information et technologies web sécurisées. Actuellement en apprentissage des méthodologies DevSecOps, je suis À la recherche d'un stage PFA pour approfondir mes compétences en cybersécurité et en sécurité des infrastructures informatiques.

EXPÉRIENCE PROFESSIONNELLE ET ACTIVITÉS EXTRACURRICULAIRES

Stage au Département Informatique, JIFORB Immobilier, Kenitra, Maroc **Juin 2024 – Juillet2024**

- Intégration de Suricata avec Wazuh SIEM Déploiement et configuration de Suricata IDS et Wazuh SIEM.
- Centralisation des alertes et automatisation des réponses aux incidents.
- Amélioration de la corrélation des logs et réduction du temps de détection des menaces.

Formatrice & Organisatrice d'Événements, UEMF Club

- formation et organisation de compétitions CTF.
- Trésorière : Gestion de la planification financière et des ressources pour les activités du club

FORMATION

Université Euro-Méditerranéenne de Fès, Maroc- *Cycle d'Ingénieur, Cybersécurité - GPA: Mention Bien* **Sep 2023 - Juin 2026**

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

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

PROJETS ACADEMIQUE

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

- Installation et configuration de Dionaea, Cowrie et Honeyd pour la simulation d'attaques.
- Analyse des techniques des attaquants à travers la collecte et l'interprétation des logs.
- Renforcement de la sécurité avec AppArmor et Seccomp.
- Intégration de la stack ELK (Elasticsearch, Logstash, Kibana) pour la visualisation des données d'attaques.

Optimisation des Flux de Travail en ML avec JupyterHub et Kubeflow

- Déploiement de JupyterHub avec Kubeflow pour la gestion des workflows ML.
- Conteneurisation avec Docker et orchestration avec Kubernetes.
- Implémentation de Rook Ceph pour un stockage évolutif et performant.

Détection de Menaces avec Snort (Intrusion Detection System)

- Configuration de règles Snort pour identifier les scans de ports et attaques DoS.
- Mise en place d'alertes en temps réel pour une détection proactive.
- Optimisation de la journalisation pour un suivi détaillé des attaques.

Déploiement d'Active Directory sur Windows Server 2012

- Installation et configuration d'AD DS, mise en place de contrôleurs de domaine, DNS, GPOs, et politiques de sécurité pour la gestion des utilisateurs et la stabilité du réseau.

COMPÉTENCES

Compétences techniques :Cybersécurité, Tests de pénétration, Metasploit, Nmap, Burp Suite, Administration Système, Linux, Windows, Sécurité des Systèmes d'Exploitation, Capacités Linux, SELinux, AppArmor, Seccomp, Sécurité Réseau, DevSecOps, Cryptage et Cryptographie, Cloud et Virtualisation

Gestion de base de données :Administration de Bases de Données, MySQL, PL/SQL, Oracle

Langages de programmation :Python, Bash, PHP, NodeJS, C/C++, HTML/CSS, Java, JavaScript

Outils d'automatisation :Outils d'Automatisation, Ansible

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

LANGUES

Français :Avancé
Anglais: Avancé
Espagnol: Notions de Base