ABAD Ayoub

Ingénieur Cybersécurité

Maroc ayoub.02.abad@gmail.com 0770859634 linkedin.com/in/abaa-youb Portfolio

Profil

Ingénieur cybersécurité avec **2 ans d'expérience** couvrant l'ensemble du spectre sécurité, de la construction d'infrastructures réseau sécurisées et du durcissement d'environnements cloud, à la détection de menaces en SOC et aux tests de pénétration d'applications. Passionné par le domaine, toujours à creuser davantage à travers les CTFs, le bug bounty ou la veille personnelle. À l'aise à l'intersection de l'offensif et du défensif, avec le souci de comprendre les systèmes en profondeur avant de chercher à les sécuriser.

Experience

- **Ingénieur SecOps @Tessi** *03/03/2025 - Present*
  Oujda, Maroc (Hybride)
  - Surveillance, analyse et investigation des alertes de sécurité (Réseau, SaaS, Email, Endpoint) remontées via les solutions SIEM, NDR, EDR, WAF et IPS/IDS.
  - Veille sur les vulnérabilités critiques (CVE), investigation et analyse d'exposition, et pilotage des actions de remédiation en cas de risque confirmé.
  - Réponse aux questionnaires de cybersécurité (appels d'offres) des clients (posture sécurité, conformité ISO 27001).
  - Conception et développement d'un dashboard en Python interfacé avec l'API IRIS pour la collecte, l'analyse et la visualisation des incidents, alertes et CVEs, avec suivi des KPIs SOC (MTTD, MTTR, sévérité, volumétrie).
  - Intégration et évaluation POC d'une solution NDR en environnement de production : tuning, triage et investigation des alertes, validation de la couverture de détection par simulation d'attaques, analyse comparative avec la solution existante et définition du cadre de décision final.

- **Ingénieur Réseaux & Sécurité (Stage PFE) @Societe Generale ABS** *05/02/2024 - 05/08/2024 (6 mois)*
  Casablanca, Maroc
  - Construction (BUILD) d'une infrastructure réseau sécurisée reliant les réseaux internes des filiales de SG africaines à l'internet public, en intégrant plusieurs couches de sécurité comprenant des Firewalls next-generation et des Proxys pour le filtrage du trafic, l'authentification et le déchiffrement pour l'inspection anti-malware et la prévention des fuites de données (DLP).
  - Configuration des tunnels IPSec VPN pour la connectivité site-à-site.
  - Assistance à la mise en conformité PCI-DSS .
  - Contribution à l'implémentation et au déploiement de solutions EDR et IDS/IPS.
  - Gestion de l'obsolescence HW & SW.
- **Stage Cybersécurité @Tisalabs** *01/07/2023 - 01/09/2023 (2 mois)*
  Cork, Irlande (à distance)
  - Évaluation des vulnérabilités et tests de pénétration (VAPT) · Programmation Python Scripting Bash · Gitlab · Conteneurisation Docker · Sécurité Kubernetes · Travail en méthodologie Agile.

Education

- **École Nationale des Sciences Appliquées d'Oujda (ENSA Oujda)**
  - Diplôme d'Ingénieur d'État en Sécurité Informatique et Cybersécurité 2019 - 2024
    Réseaux informatique · Administration système · C, Shell et Python · Cryptographie · Sécurité mobile · Hacking Éthique · Test de pénétration · Cloud Computing · Big Data · Machine Learning · Audits de sécurité..

Projets récents

- **Cloud-Native DevSecOps Kubernetes Implementation sur AWS EKS pour une application 3-Tier**

  - CI/CD : Conception et implémentation d'une pipeline CI/CD en utilisant Jenkins, AWS, Terraform IaC, Docker pour la conteneurisation, et ArgoCD pour automatiser les déploiements sur Amazon EKS Cluster (Kubernetes).
  - Sécurité : Mise en œuvre des outils de sécurité tels que GitLeaks comme hook pre-commit, OWASP Dependency-Check pour SCA et ZAP pour le scan d'application web (DAST), intégration de plusieurs outils SAST, SonarQube pour la qualité du code, et Trivy pour la sécurité des conteneurs Docker, Kubernetes, et IaC. Utilisation de Vault pour le management des secrets, Prometheus & Grafana pour la supervision, et le stack EFK pour le logging.

- **Suivi des échecs de connexion RDP avec carte mondiale dans Azure Sentinel (SIEM)**

  - Utilisation d'un script PowerShell personnalisé pour extraire des métadonnées depuis l'Observateur d'événements Windows et les transmettre à une API tierce afin d'obtenir des données de géolocalisation
  - Configuration d'un espace de travail Log Analytics dans Azure pour ingérer des journaux personnalisés contenant des informations géographiques (latitude, longitude, État/province et pays)
  - Configuration d'un classeur (workbook) Azure Sentinel (SIEM cloud de Microsoft) afin d'afficher les données d'attaques globales (force brute RDP) sur une carte mondiale en fonction de la localisation physique et de l'intensité des attaques

- **Automatisation de Pentest des applications web et des APIs par des scripts bash**

  - Création de scripts bash pour rationaliser les tâches répétitives dans le cadre de tests de pénétration et de programmes de bug bounty, englobant des activités telles que la reconnaissance, détection de WAF et des technologies utilisées (WordPress, GraphQL), mécanismes de bypass, fuzzing, spidering, scan des secrets, LFI, SQLi, XSS, etc.

- **Audit de Sécurité du Code Source d'Applications web (PHP, NodeJs ..)**

  - Réalisé une analyse approfondie du code source de plusieurs applications pour identifier les vulnérabilités, en mettant l'accent sur les entrées utilisateur, l'authentification, la gestion des erreurs et la logique métier critique.
  - Effectué des tests et débogages locaux approfondis pour confirmer les vulnérabilités critiques, analyser leurs causes racines, évaluer leur impact sur la sécurité, identifier les zones sensibles et proposer des mesures préventives.
  - Proposé des solutions sécurisées incluant la validation stricte des entrées utilisateur, les bonnes pratiques de codage sécurisé, des audits de code réguliers et l'utilisation de bibliothèques fiables pour atténuer les risques.

Réalisations et Certifications

- Top 1% sur TryHackMe, Certifications: Web Fundamentals, Pre-Security, Jr. Pentester, Pentest+, Cyber Defense).
- HackTheBox: Senior Web Penetration Tester (67% Progress)
- HackTheBox: SOC Analyst (50% Progress)
- Obtenu la 3ème place lors d'une compétition CTF organisée par l'université.
- CloudGuru : Azure Security Engineer (AZ-500), et AWS Cloud Practicioner AWS Security Fundamentals

Compétences Techniques et Intérêts

Compétences Techniques: Pentest des Applications Web, Recon, OSINT, Python, Bash Scripting, AWS, Microsoft Azure, Azure Active Directory, Kubernetes, Secrets Management, CI/CD, SAST, DAST, Threat Modeling, SCA , DevSecOps, Sécurité Réseaux, PCI-DSS, ISO 27001, NIST, SOC, SIEM, Monitoring & Logging, Digital Forensics (Linux, Windows & Android) ...

Tools: Burp Suite, Shodan, OWASP Zap, Postman, Wireshark, nmap, nuclei, CrackMapExec, Bloodhound, volatility, Ghidra, IDA, SQLMap, Kali Linux tools, Metasploit, Nessus, OpenVAS, Git, SonarQube, ELK Stack, Trivy, Sophos, Lansweeper, Palo Alto...

Compétences Comportementales : Adaptabilité, Collaboration, Curiosité d'apprendre, l'écoute, la patience ...

Langues

Arabe: Native **Anglais**: Avancé **Français**: Avancé