Ilias Belharda

Ingénieur en Cybersécurité

Rabat-Salé-Kénitra
belharda.ilias@gmail.com
+212(0) 600102919
LinkedIn ilias belharda

Ingénieur en cybersécurité avec une expertise technique dans la sécurité des systèmes, des réseaux et le reverse engineering. Titulaire de certifications Fortinet, Cisco et Huawei, j'ai mené des projets concrets en simulation d'attaque APT, phishing, et forensic. Impliqué dans plusieurs clubs universitaires et actions sociales, je combine des compétences techniques solides avec un esprit d'équipe, de leadership et une forte capacité d'adaptation.

Compétences techniques

• Cybersécurité offensive : Pentest, SQLi, phishing, reconnaissance
• Défensive : Wazuh, Suricata, AD Hardening, IDS/IPS
• Analyse & forensic: Reverse engineering, sandboxing, forensics
• Outils : SQLMap, Meterpreter, Nessus, Wireshark, Sage, Burp Suite
• Réseaux : Nmap, OSINT, SMB, Wireshark, sécurité des connexions
• Systèmes : Windows Server, Linux, VMware/VirtualBox

Certifications

• Fortinet: FCSS – OT Security 7.2 Self-Paced
• Cisco Networking Academy : Introduction à l'IoT et à la transformation digitale
• Cisco Networking Academy : Introduction to IoT (Course Completion)
• Huawei : HCIA-IoT V3.0 – 2024-05-23
• Red Hat System Administration I 9.0

Langues

• Français : Bilingue
• Anglais : Avancé
• Arabe : Maternelle
• Espagnol : Débutant

Engagements & Activités

• Membre actif de TEDxUIR
• Membre du club Social Impact : participation à des actions humanitaires (ex. : séisme 2023)
• Visites d'entreprises : Maroclear, Bourse de Casablanca, sociétés technologiques
• Membre du club de trading

Formation Académique

2023 – 2025 : Master en Cybersécurité - *Université Internationale de Rabat (UIR), Rabat*
2020–2023 : Classes Préparatoires Intégrées, filière Informatique - *Université Internationale de Rabat, Rabat*

Expérience Professionnelle

AXA GBS – Stage de fin d'études (6 mois)
Février 2025 – Août 2025 | Rabat
Sujet : Simulation d'une attaque APT sur une infrastructure Active Directory et mise en place de mesures de défense – Mention Très Honorable
• Conception d'une infrastructure virtualisée de test
• Simulation complète d'une attaque APT (reconnaissance, phishing, SQLi, exploitation, persistance, mouvement latéral, SMB)
• Mise en place de contre-mesures : Wazuh, Suricata IPS, durcissement, anti-phishing, renforcement AD
• Utilisation d'outils : SQLMap, Meterpreter, Nessus, Suricata, Wazuh
• **Gestion des incidents de sécurité via une plateforme SIEM avec une équipe** :
– Réception, classification et escalade des alertes de sécurité
– Suivi des procédures de réponse aux incidents (analyse, priorisation, documentation)
– Collaboration avec les équipes réseau et sécurité pour le traitement des incidents

TBEM – Stage assistant ingénieur (5 semaines)
07/2024 – 08/2024, Rabat
• Analyse de vulnérabilités et participation au renforcement de la sécurité des SI

Milroad – Stage technicien (5 semaines)
08/2024 – 09/2024, Safi
• Configuration de routeurs/switches, dépannage réseau, documentation sécurit

NTSI Tanger – Stage ouvrier (4 semaines)
07/2022 – 08/2022, Tanger
• Utilisation de Sage pour gestion commerciale
• Tâches techniques liées aux réseaux

Projets académiques

Analyse du Dark Web & Reverse Engineering d'exploits
Analyse de forums d'exploit du dark web sur le Web Selfless
• Création d'un environnement sandbox
• Reverse engineering de contenus téléchargés
• Évaluation des risques de sécurité et recommandations

Phishing Attack
• Développement d'un clone de Spotify pour simuler une attaque de phishing et sensibiliser aux cybermenaces.

Browser Forensics
• Analyse des historiques de navigation avec Browser History Examiner
• Extraction et corrélation d'activités utilisateur

NoSQL Injection
• Présentation et démonstration technique en binôme
• Exploitation de vulnérabilités dans des bases de données NoSQL