

Ilias Belharda

Cybersecurity Engineer



📍 Morocco

✉️ belharda.ilias@gmail.com

📞 +212 600102919

🔗 LinkedIn ilias belharda

Portfolio : <https://ilias-belharda.github.io/>

I am a cybersecurity engineer with strong technical expertise in system and network security, reverse engineering, and cyber defense. Holder of Fortinet, Cisco, and Huawei certifications, with hands-on experience in APT simulation, phishing, and forensic analysis. Active in university clubs and social initiatives, combining solid technical skills with teamwork, leadership, and adaptability.

Technical Skills

- **Offensive Security:** Pentesting, SQL Injection, phishing, reconnaissance
- **Defensive Security:** Wazuh, Suricata, AD Hardening, IDS/IPS
- **Forensics & Analysis:** Reverse engineering, sandboxing, forensics
- **Tools:** SQLMap, Meterpreter, Nessus, Wireshark, Sage, Burp Suite
- **Networking:** Nmap, OSINT, SMB, Secure connections
- **Systems:** Windows Server, Linux, VMware/VirtualBox

Certifications

- Fortinet: FCSS – OT Security 7.2 Self-Paced
- Cisco Networking Academy : Introduction to IoT and Digital Transformation
- 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 : Professional
- Anglais : Professional
- Arabe : Native

Engagements & Activities

- Member of TEDxUIR
- Membre of Social Impact club: humanitarian actions (e.g.: Morocco earthquake 2023)
- Company visits: Maroclear, Casablanca Stock Exchange, Thales ...
- Membr of the trading club

Education

2023 – 2025 | Master's Degree in Cybersecurity – Université Internationale de Rabat (UIR), Rabat

2020 – 2023 | Integrated Preparatory Classes, Computer Science Track – UIR, Rabat

Professional Experience

AXA GBS – Final Year Internship (6 months)

Feb 2025 – Aug 2025 | Rabat

Project : *Simulation of an APT attack on an Active Directory infrastructure and implementation of defense measures – Graduated with High Honors*

- Designed and deployed a virtualized test infrastructure
- Conducted full APT simulation (reconnaissance, phishing, SQLi, exploitation, persistence, lateral movement, SMB)
- Implemented countermeasures: Wazuh, Suricata IPS, hardening, anti-phishing, AD strengthening
- Tools used: SQLMap, Meterpreter, Nessus, Suricata, Wazuh
- **Security incident management with SIEM platform:**
 - Alert reception, classification, and escalation
 - Incident response procedures (analysis, prioritization, documentation)
 - Collaboration with network and security teams

TBEM – Assistant engineer intern (5 weeks)

Jul 2024 – Aug 2024, Rabat

- Vulnerability analysis and participation in information system security hardening

Milroad – Technician intern (5 weeks)

Aug 2024 – Sep 2024, Safi

- Router/switch configuration, network troubleshooting, security documentation

NTSI Tanger – Worker intern (4 weeks)

Jul 2022 – Aug 2022, Tanger

- Used Sage for commercial management
- Performed technical tasks related to networking

Academic Projects

Dark Web Analysis & Exploit Reverse Engineering

- Analyzed exploit forums on the Selfless Web
- Created a secure sandbox environment
- Reverse engineered downloaded content
- Assessed security risks and provided recommendations

Phishing Attack

- Developed a Spotify clone to simulate a phishing attack and raise awareness

Browser Forensics

- Analyzed browsing history with Browser History Examiner
- Extracted and correlated user activities

NoSQL Injection

- Delivered technical presentation and live demonstration
- Exploited vulnerabilities in NoSQL databases