Abdelhakim Hani

+212 633826704 | han.23hani@gmail.com | Portfolio

abdelhakim-hani | Abdelhakim-hani | tryhackme |

Objective

I aim to leverage my cybersecurity skills to contribute to innovative projects focused on securing network infrastructures, proactively detecting intrusions, and managing risks. My goal is to play an active role in protecting information systems while gaining hands-on experience in a demanding professional environment.

Experience

- **Menara Holding [🌐]** *July 2025 - September 2025*
  PFA Internship Marrakech, Morocco
  - Implemented an intelligent system for detecting XSS attacks using machine learning.
  - Applied vectorization techniques (TF-IDF) and learning algorithms (Logistic Regression, Random Forest, SVM, Deep Learning).
  - Enhanced detection against obfuscated payloads and advanced malicious injection variations.
- **COPAG [🌐]** *March 2024 - August 2024*
  Internship Taroudant, Morocco
  - Developed a web and mobile application for commercial management for COPAG.
  - Designed the full project following modeling best practices, including UML diagrams.
  - Selected technologies: Angular for frontend and Spring Boot for backend.

Education

- **International University of Rabat** *Ongoing*
  Engineering Cycle – Cybersecurity Rabat, Morocco
  - 5th Year
- **Ibn Zohr University, Faculty of Sciences** *2023*
  Bachelor's Degree in Fundamental Studies Agadir, Morocco
  - Major: Mathematics and Computer Science
- **Ibn Soulaiman Roudani High School** *2018*
  Baccalauréat – Mathematical Sciences A Taroudant, Morocco

Projects

- **Academic Project: Implementation of a C2 Architecture on GNS3** *2025*
  Tools: GNS3, Python, Metasploit, Virtual Machines, Linux (Kali/Ubuntu), Wireshark
  - Developed a full Command & Control (C2) architecture enabling centralized management of agents in a simulated network.
  - Implemented automated attack scenarios (exfiltration, reconnaissance, persistence).
  - Designed and configured an advanced network topology on GNS3 with reliable communication between compromised hosts and the C2 server.
  - Applied traffic analysis techniques using Wireshark to identify network behavior and compromise indicators.
- **Final Year Project: Automatic Detection of Gastrointestinal Bleeding from WCE Images** *February 2023 - June 2023*
  Tools: Python, CNN (TensorFlow/Keras), Random Forest, OpenCV, Google Colab
  - Built an intelligent system for automatic detection of gastrointestinal bleeding from Wireless Capsule Endoscopy (WCE) images.
  - Implemented a Convolutional Neural Network (CNN) and Random Forest model for medical image analysis.
  - Designed an accurate and robust model contributing to faster and more reliable assisted diagnosis.
- **Session Hijacking: Analysis and Exploitation in a Controlled Environment** *2025*
  Tools: Burp Suite, Wireshark, Python
  - Analyzed and exploited vulnerabilities related to session hijacking in a secure lab environment.
  - Reproduced attacks (session fixation, cookie theft) and implemented defensive countermeasures.
  - Produced security hardening recommendations for web applications.
- **Honeypot: Deployment and Attack Analysis with SIEM Integration** *2025*
  Tools: Cowrie, Suricata, ELK Stack
  - Deployed an interactive honeypot to capture and analyze malicious activities.
  - Integrated Suricata and ELK for correlation, alerting, and visualization.

- ◦ Performed attacker behavioral analysis and produced detailed reports.

- **Secure Network Topology on GNS3/pfSense** *2025*
  Tools: GNS3, pfSense, VLAN, DMZ, VPN
  - ◦ Designed a secured network architecture including VLAN segmentation, DMZ, and VPN tunnels.
  - ◦ Configured firewalls, NAT rules, IDS/IPS, and access policies.
  - ◦ Simulated attack scenarios to validate architecture robustness.

SKILLS

- **Programming Languages:** Python, Bash, PowerShell, Java, C/C++, JavaScript
- **Penetration Testing:** Reconnaissance, exploitation, post-exploitation, Web testing (XSS, SQLi, CSRF, LFI/RFI, SSRF), network/system testing (AD, Wi-Fi, services/ports)
- **Pentest Tools:** Nmap, Metasploit, Burp Suite, Hydra, John the Ripper, Nikto, SQLmap
- **Cyber Defense & SOC:** Wazuh, Microsoft Sentinel, CrowdStrike, Defender, SIEM (Splunk, Graylog), EDR/XDR
- **Intrusion Detection & Monitoring:** Snort, Suricata, Zeek, ELK Stack, Wireshark
- **Vulnerability Management:** Nessus, OpenVAS, CVE/CVSS, exploit analysis
- **System & Server Security:** Linux & Windows hardening, Apache/Nginx security
- **Cloud Security:** Azure, AWS, Google Cloud — IAM, policies, storage security, network security
- **Virtualization & Infrastructure:** VMware ESXi, OpenStack, Proxmox, Hyper-V, VirtualBox, Docker, Containerization
- **Networking & Infrastructure:** TCP/IP, DNS, DHCP, HTTP/HTTPS, VPN, VLAN, firewalls, IDS/IPS
- **API Security:** JWT, OAuth2, OpenID Connect, API hardening
- **Cryptography:** AES, RSA, ECC, hashing (SHA, MD5), HMAC, digital signatures
- **DevOps & Version Control:** Linux Administration, Git/GitHub, CI/CD basics, automation scripting
- **Data Science & ML:** TensorFlow, Keras, Scikit-learn, Pandas, NumPy, OpenCV
- **Compliance & Standards:** ISO 27001, NIST, OWASP Top 10, GDPR, CIS Benchmarks

CERTIFICATIONS

- **Cloud Security Foundations (In progress)**
- **AWS – Introduction to Amazon Web Services** *Nov 2025*
- **SQL Injection Attacks** *Nov 2025*
- **Improve IT Security Through Monitoring** *Oct 2025*
- **Red Hat System Administration** *Oct 2025*
- **Virtualize Your Work Environments** *Oct 2025*
- **Cisco Ethical Hacker** *2025*

ADDITIONAL INFORMATION

Languages:

- French (Advanced)
- Arabic (Native)
- English (Advanced)

Interests:

- Professional chess player
- Participation in CTF competitions and cybersecurity challenges
- Attack simulation (VMs, Kali Linux, Metasploit)
- Continuous learning on new vulnerabilities