Ahmed Shili

Applying for Junior Penetration Tester position at Hack4Job LTD

ahmed.shili.sec@gmail.com | (+216) 96 493 747 | linkedin.com/in/ahmedshili | github.com/shili-ahmed
| credly.com/users/ahmed-shili | Ariana, Tunisia | UTC+1 (Open to remote work; flexible across time zones)

Summary

Curious and methodical **Penetration Tester**, I specialize in identifying **systemic weaknesses** across **web apps**, **infrastructure**, **wireless networks**, and **Active Directory** environments. I craft **custom exploits** to **prove** and **prioritize** them. I blend **static analysis** with **dynamic debugging** to **reverse engineer x86 binaries** and expose **vulnerabilities** often missed by others. My toolkit includes **Burp Suite**, **Nmap**, **Nessus**, and custom **Python/Bash scripts**, enabling me to **accelerate triage**, **reduce noise**, and **reproduce exploit chains** with precision.

I work best with **remote-first**, **globally distributed teams**, collaborating to deliver **concise**, **bilingual (EN/FR) reports** tailored to both **technical** and **executive audiences**. I always bring **clarity**, **speed**, and **ethical integrity** to every test — whether it's **scoping engagements**, **chaining misconfigurations**, or **advising developers** on mitigation.

Experience

El-Khawarizmi Computing Center (CCK) — SOC Analyst Intern

Mar 2025 – Sep 2025 (6 months) | Manouba University Campus

- Built real-time Power BI dashboards to monitor Fortigate and IDS/IPS logs, improving detection and incident triage times.
- Correlated Splunk and ELK alerts with threat intelligence to validate indicators and evidence for investigations.
- Tuned detection rules and enriched logs to reduce noise and focus on attacker-aligned behaviors to support red team validation and post-exploitation analysis.

El-Khawarizmi Computing Center (CCK) — Penetration Tester Intern

Jul 2024 – Aug 2024 (1 month) | Manouba University Campus

- Conducted black-box and authenticated application tests using Burp Suite (manual + scanner), WPScan and Nessus to find injection, authentication, and session flaws.
- Performed host and network discovery (Nmap), vulnerability validation, and produced remediation-focused reports with reproduction steps and risk ratings.
- Automated repetitive checks with Python scripts to reliably reproduce findings and reduce manual verification time.

Smart Tunisian Technopark (S2T) — Web3 Systems Engineer Intern

Mar 2022 – Jun 2022 (4 months) | El Ghazala Technology Park

- Reviewed smart contracts and integrated OpenZeppelin patterns to reduce exploit surface; applied threat modelling to decentralized components.
- Developed secure deployment practices and automated checks for configuration drift—skills that translate to secure code review and supply-chain assessments.

El-Khawarizmi Computing Center (CCK) — Software Engineer Intern

Feb 2021 – Jun 2021 (4 months) | Manouba University Campus

- Implemented secure web application features and hardened server configurations; participated in code reviews to spot injection and auth issues.

El-Khawarizmi Computing Center (CCK) — Identity Systems Engineer Intern

Mar 2019 – Jun 2019 (4 months) | Manouba University Campus

- Designed federation and identity flows (SAML, LDAP) and hardened authentication paths—experience relevant to Active Directory and identity-focused red team tests.

Tunisian Civil Aviation and Airports Authority (OACA) — Network Security Intern

Jan 2018 – Feb 2018 & Jul 2018 – Aug 2018 (2 months total) | Tunis-Carthage International Airport

- Applied secure access controls via **Active Directory** and monitored traffic with **Wireshark** to troubleshoot and harden systems.
- Secured network devices and implemented basic network hardening practices that later informed internal/external network pentests.

Education

Private International Polytechnic School of Tunis (Polytech INTL) — 2023–2025
Master's Level Engineering Degree in Computer Science, Networks and Multimedia | *EUR-ACE Accredited*
Tunis Higher School of Communications (SUP'COM) — 2021–2022
Professional Master's Degree in Operational Cybersecurity
Higher Institute of Computer Science (ISI) — 2020–2022
Professional Master's Degree in Open Source Software Engineering
Higher Institute of Technological Studies in Communications of Tunis (ISET'COM) — 2016–2019
Applied Bachelor's Degree in Siences of Information Computer Technologies | Major : Security

Skills

Core Penetration Testing Tools: Burp Suite Professional (Repeater, Intruder, Scanner, Extender), Nmap, Nessus, Metasploit Framework, sqlmap, OWASP ZAP, Nikto, Gobuster, Dirb, Amass, Kali Linux

Web & Application Security: OWASP Top 10 manual testing, API testing (Postman + Burp), authentication & session testing, XSS, SQLi, CSRF, XXE, SSRF exploitation, basic secure code review (PHP, JavaScript, Python, Java)

Network & System Testing: Wireshark, tcpdump, Linux & Windows privilege escalation, credential access techniques, lateral movement

Reverse Engineering – x86/x64 Focus: Ghidra (primary), IDA Pro Free, x86/x64 assembly reading and analysis, binary patching, debugging with x64dbg and Immunity Debugger, stack layout, calling conventions, common binary protections (ASLR, DEP, stack canaries)

Exploit Development: buffer overflows, format string basics, simple ROP, custom exploit development with Python + pwntools, modifying public PoCs, writing reliable proof-of-concept exploits

Scripting & Automation: Python (requests, pwntools, automation & reporting), Bash/Zsh, writing simple Burp extensions and custom tools

Reporting & Communication: detailed technical reports, executive summaries, reproducible PoCs, CVSS scoring, clear remediation advice, strong written and spoken English

Languages: Arabic (Native), French (Fluent), English (Fluent)

Certifications:

- **Certified Ethical Hacker (CEH)** - relevant for offensive fundamentals.
- **Cisco CyberOps Associate / CyberOps** (security operations knowledge aiding triage and detection).
- **HCIA Security (Huawei Certified ICT Associate)** (Network defense, access control, and enterprise security architecture)
- MTA: Security Fundamentals (Microsoft Technology Associate)
- Cybersecurity Basics (edX)
- Programming Foundations: Web Security
- AWS: Getting Started with Cloud Security
- AWS Academy Graduate — Cloud Foundations
- Microsoft Azure Fundamentals (AZ-900), Azure Data Fundamentals (DP-900), Azure AI Fundamentals (AI-900)
- IT Specialist – Python, JavaScript, Software Development (Certiport) — useful for scripting and secure code review.

Projects

- Intrusion Detection System with ELK & Suricata (2024–2025) — Built a lab-based IDS on CentOS with **Suricata** and **ELK Stack** to monitor traffic, automate log analysis, and demonstrate faster detection of network threats.
- Windows 7 Forensics Analysis with Autopsy (2024–2025) — Recovered deleted files and artifacts from a compromised VM using **Autopsy** and **SIFT Workstation**, reinforcing skills in digital forensics and incident response.
- Keylogger Demonstration Tool (2024–2025) — Developed a proof-of-concept keylogger in a controlled lab with **pynput** and **smtplib**, highlighting exfiltration risks and strengthening understanding of attacker techniques.

Additional notes

- **Open to working with globally distributed, remote-first teams** across time zones.
- **Legally authorized to work remotely for foreign companies** under Tunisia’s SUARL status, with the ability to **invoice internationally** and remain fully compliant with local tax and social security regulations.
- **No visa sponsorship required**. Fully equipped to contribute remotely without relocation or work authorization in the client’s country.
- Comfortable **scoping**, **remote engagements**, working with clients to define **rules of engagement**, and explaining **technical risk** to engineering and leadership teams.
- **Active learner**: follow public **exploit databases** and **research trackers**; automate **repeatable verification** to increase **throughput** while reducing **false positives**.