Rayan Fakhreddine

Beirut, Lebanon
+96181920481 rayanmfakhreddine@gmail.com rayanfakhreddine rayanfakhreddine

Education

American University of Beirut **August 2022 – Expected May 2026**
Bachelor of Engineering in Computer Science & Engineering; *Beirut, Lebanon*

- GPA: 3.88
- Relevant Coursework: Computing Networks & Services, Ethical Hacking I and II, Internet Security Lab, Operating Systems, Cryptography & Network Security, Digital Forensics & Incident Response

Experience

Threat Intelligence Intern **Jul 2025 - Aug 2025**
ABSEGA *Beirut, Lebanon*

- Analyzed TTPs of adversaries (e.g., Scattered Spider, NoName057) and those targeting Lebanese Finance/Healthcare.
- Authored formal CTI reports using OSINT and threat intel platforms (OTX, VT) to correlate infrastructure.
- Developed a Python automation tool for domain reputation enrichment and security risk evaluation.
- Presented technical findings to senior mentors, translating intelligence into stakeholder-ready documentation.

Teaching Assistant - Ethical Hacking II **Jan 2026 - May 2026**
American University of Beirut *Beirut, Lebanon*

- Assisting in the instruction of advanced penetration testing techniques, including Active Directory (AD) attacks, pivoting, and post-exploitation.
- Guiding students through lab environments and evaluating lab assignments.

Projects

Digital Forensics & Incident Response Case Study (Windows) | *Sp. Tp. in DFIR* **December 2025**

- Led forensic analysis on 3 systems in a 6-endpoint Windows environment using triage and timeline analysis.
- Correlated thousands of logs (Sysmon, Security, Application) to reconstruct a multi-stage attack chain.
- Reconstructed a multi-stage attack chain spanning initial access, persistence, lateral movement, and defense evasion.
- Identified 10+ IOCs, including registry persistence and malicious binaries; mapped findings to MITRE ATT&CK.
- Co-authored a formal incident report tailored for executive, IT, and DFIR audiences, including technical findings and prioritized remediation steps.

Linux & Active Directory Penetration Testing | *Ethical Hacking 2* **May 2025**

- Executed full-cycle engagements against Linux servers and Active Directory environments.
- Performed reconnaissance, vulnerability exploitation, lateral movement, and privilege escalation.
- Produced comprehensive remediation reports detailing vulnerability impact and mitigation steps.

Secure Banking Microservices App | *Flask, Docker* **November 2025**

- Secured a 7-service architecture against OWASP Top 10 vulnerabilities using JWT-based RBAC, Argon2id credential hashing, and robust defenses against SQLi, XSS, and CSRF.
- Hardened deployment via Docker network segmentation and least-privilege service access.
- Integrated OWASP ZAP into the CI pipeline for automated vulnerability scanning (SQLi, XSS, SSRF).

Centralized Security Monitoring | *Wazuh, Ubuntu, Windows* **December 2024**

- Deployed Wazuh SIEM architecture to monitor network endpoints and centralize log management.
- Configured agents for real-time threat detection, alerting, and automated integrity monitoring.
- Configured File Integrity Monitoring (FIM) to track unauthorized file modifications.
- Integrated VirusTotal API for real-time malware detection and hash scanning..

Skills

Hard Skills: Python (4yrs), C++, Bash, Batch, PowerShell, git, GitHub, Docker
Soft Skills: Problem-Solving, Communication, Leadership, Strategic Thinking, Creativity, Teamwork, Analytical Thinking
Languages: English (Fluent), Arabic (Native)

Extra-Curricular Activities

IEEE Technical Advisor & Semicolon University Ambassador **Aug 2025 - May 2026**

- Co-organized **Cybersecurity Day 2025**; led a **Hack The Box (HTB) workshop** for 50+ students.