Rayan Khalil

Aspiring Cybersecurity Professional

✉ rayankh642@gmail.com ☎ +961 81885759

Beirut, Lebanon linkedin.com/in/rayan-khalil067

Motivated third-year cybersecurity student with a solid academic background and hands-on experience in ethical hacking, network security, programming, and digital forensics. Actively participating in Capture The Flag (CTF) competitions and lab environments to simulate real-world attack scenarios and enhance threat detection and response skills. Having a keen interest in both red team and blue team operations, with strong analytical thinking, attention to detail, and a collaborative mindset. Eager to contribute to a forward-thinking security team by applying technical knowledge, problem-solving abilities, and a passion for learning to help secure and harden systems in real-world environments.

Education

BS, Computer and Network Security,
University of Sciences and Arts in Lebanon | Expected Graduation: June 2026

Relevant Courses:

- Ethical Hacking and Penetration Testing (Kali Linux, Nmap, Nikto, Metasploit, Burp Suite)
- Digital Forensics
- Computer Networking (Routing and Switching, Scaling and Connecting Networks)
- Advanced Programming (Python)
- OOP (Java)
- Database Management Systems
- Web Application Security
- Computer Security (CIA Triad, Cryptography, Hash Functions)
- Operating Systems (Ubuntu)

Languages

Arabic (Native) English (Near-Native Proficiency)

Skills

Penetration Testing & Vulnerability Assessment
Proficient in identifying and exploiting system weaknesses using tools like Kali Linux, Metasploit, and Burp Suite. Familiar with OWASP Top 10 and common attack vectors in web and network environments.

Digital Forensics
Knowledgeable in forensic analysis and evidence handling. Capable of tracing breaches and investigating attack origins using open-source tools.

Containerization & Lab Simulations
Utilizes Docker to build isolated environments for security testing and exploit simulations.

Web Application Development
experienced in full-stack web development with a strong foundation in HTML, CSS, Javascript, JQuery, Python Flask.

Database Management
Proficient in working with MySQL databases and writing queries

Security Information and Event Management (SIEM)
Hands-on experience with Wazuh for log analysis and threat detection.

Computer Networking & Network Security
Solid understanding of network protocols, subnetting, firewalls, and packet analysis using tools like Wireshark. Able to design and secure basic network architectures.

Cryptography & Data Protection
Familiar with cryptographic principles including symmetric/asymmetric encryption, hashing, digital signatures, and SSL/TLS protocols.

Programming and Scripting
Experienced in writing efficient code using Python, Java, and JavaScript as well as applying OOP principles

Projects and Cybersecurity Training

> **Security Solutions Project**

- **Implemented Wazuh, an open-source SIEM, in a Docker-based environment** to monitor and respond to real-world cyberattacks
- **Simulated 10 attack scenarios** including brute force, reverse shell, privilege escalation, ARP spoofing, and remote code execution using tools like Hydra, Netcat, Nmap, and Metasploit
- **Configured Wazuh's core components**—Manager, Agent, Indexer, and Dashboard—on a single-node stack, with the agent installed on a Dockerized Ubuntu target
- **Leveraged features such as intrusion detection, file integrity monitoring, log analysis, and automated IP blocking** through Active Response to validate Wazuh's real-time detection and response capabilities.

> **University Campus Network Project**

Designed and implemented a comprehensive, secure, and scalable network topology for a university campus environment. Configured 3 routers, 12 switches, 3 servers, and over 40 hosts across multiple departments using Cisco Packet Tracer.
Key implementations included:

- **VLAN segmentation and inter-VLAN routing** for traffic isolation and enhanced security.
- **DHCP configuration** for dynamic IP management.

- **Access Control Lists (ACLs)** to enforce network security policies.
- **SSH-enabled remote switch/router management** and secure router-on-a-stick topology.
- **Realistic deployment of services** (Web, FTP, Email servers) and detailed IP addressing schemes.

> **Capture The Flag Competitor,** *Semicolon Academy | June 1st 2025*

Currently undergoing training with Semicolon Academy for Lebanon's first CTF competition in collaboration with Google Developers Group (GDG) Coast Lebanon, covering a wide array of topics including **web and application security, infrastructure exploitation, reverse engineering, cryptography** and **real-world attack simulations.**

> **Cybersecurity Bootcamp Trainee,** *Hash Academy | April 2025 - August 2025*

Actively undergoing hands-on training in both offensive and defensive security. The online program covers:

- **Penetration Testing & Red Team Tactics:**

Full kill chain exploration including reconnaissance (OSINT, Nmap), enumeration (Active Directory, NetBIOS, SMB, DNS), exploitation (SQLi, RCE, LFI, XXE), post-exploitation, lateral movement, and pivoting.

- **Web & Mobile Security:**

In-depth analysis of client-side and server-side vulnerabilities (XSS, CSRF, access control flaws, path traversal), Android app reverse engineering, and instrumentation using Frida.

- **Security Tool Development:**

Building security tools from scratch using Python to automate scanning, exploitation, and defensive tasks.

- **Blue Team & Defensive Security:**

SIEM integration (Wazuh), IDS/IPS, EDRs, firewalls, digital forensics, and incident response strategies.

- **Security Frameworks & Industry Standards:**

Exposure to MITRE ATT&CK, CIS, NIST, Zero Trust, and real-world attack detection.

- **Capstone Projects, CTFs and Hands-on Labs** as part of the training