Tareq Abu Khashabeh

(+962) 795711044 | tareq.abukhashabeh@gmail.com | Tareq-Abukhashabeh | Portfolio | Linkedin

Summary

Motivated and detail-oriented Cybersecurity student with a strong foundation in Blue Team operations, SOC analysis, and automation. Passionate about detecting, analyzing, and responding to real-world security incidents through hands-on projects, automation, and CTF competitions. Skilled in Python, Bash scripting, and network analysis tools, with experience in log analysis, intrusion detection, threat monitoring, and security automation. Quick learner with a proactive mindset, continuously expanding knowledge in incident response, SIEM tools, defensive security techniques, and automated threat detection workflows.

Projects

NarrowAI — GitHub Repo

January 2025 – May 2025

- Built an AI-powered reconnaissance tool integrating WHOIS, DNS, subdomain enumeration, email harvesting, and Nmap scanning.
- Integrated Gemini AI chatbot for interactive analysis, vulnerability assessments, and exploit suggestions.
- Built a full dashboard for visualizing scan results and managing reconnaissance data.
- Automated report delivery to users and enabled remote tool execution directly from Telegram.
- Integrated a CVE feed from trusted sources to surface real-time vulnerability data per scan.
- Implemented a database to store and retrieve historical scan results for tracking and comparison.

Automated Malware Analysis — In Progress

March 2026

- Built a fully automated malware analysis pipeline from file submission to final verdict with zero manual analyst involvement.
- Integrated VirusTotal, MalwareBazaar, and AlienVault OTX for parallel OSINT threat intelligence enrichment.
- Leveraged Cuckoo, ANY.RUN, and Hybrid Analysis sandboxes for dynamic behavioral analysis and runtime monitoring.
- Automated the full analysis workflow using n8n, delivering a complete verdict in under 5 minutes.
- Generates detailed threat reports with IOC extraction, MITRE ATT&CK mapping, and weighted risk scoring.
- Implemented automated alerts and incident response tickets via email, Discord, MISP, and TheHive based on verdict.

RedRecon — GitHub Repo

2025

- Built a Python-based active and passive reconnaissance tool for security assessments and CTF competitions.
- Performs passive OSINT via HackerTarget and crt.sh APIs for subdomain enumeration.
- Conducts multi-threaded active port scanning with service banner grabbing across common ports.
- Detects WAF presence (Cloudflare, Sucuri, AWS, Akamai) and server technology fingerprinting.
- Outputs structured, color-coded reports using Rich for fast visual triage.

ScanX — GitHub Repo

April 2025

- Designed and developed an advanced Bash-based network reconnaissance tool for scanning, vulnerability detection, and web intelligence gathering.
- Automated scanning of IP ranges to detect open ports and services using Nmap.
- Integrated Whois and DNS lookups for enhanced recon.
- Added modules to detect weak HTTP headers, outdated software, and default configurations.
- Logged scan results into structured reports for further analysis.
- Used in CTF and lab simulations to identify exploitable misconfigurations.

Courses Platform — Live Site

2025

- Built and launched a free cybersecurity education platform using HTML, CSS, and JavaScript.
- Features structured video lessons and quizzes to help students learn cybersecurity hands-on.
- Publicly accessible and designed to make quality cybersecurity education available to everyone.

Fake Email Detector — GitHub Repo

March 2025 – April 2025

- Developed a Chrome extension that detected 92% of phishing attempts in testing across 500+ sample emails, improving detection accuracy compared to existing tools by 15%.

Education

B.Sc. in Cybersecurity Al-Zaytoonah University of Jordan — Amman, Jordan
Expected Graduation: 2026 | GPA: 88.6

Certifications

- Certified Cybersecurity Technician (CCT) — 2025
- Certified Cisco Basic Networks
- Certified Cisco Ethical Hacking
- SOC L1 (TryHackMe)

Leadership & Activities

Founder & Team Leader — ZSC (Cybersecurity Club), Al-Zaytoonah University of Jordan

2025 – Present

- Founded and lead the university's Cybersecurity Club, overseeing all members and club activities.
- Organize and host cybersecurity events, workshops, and CTF competitions for students.
- Represent the club officially within the university and the broader security community.

Team Leader & CTF Organizer — RedX, Al-Zaytoonah University of Jordan

2025 – Present

- Founded and led the RedX Team, mentoring members in cybersecurity and ethical hacking.
- Organized and hosted a Capture The Flag (CTF) competition for students.
- Designed and implemented both the frontend and backend of the CTF platform.
- Managed server deployment, configuration, and hosting directly on a personal device.
- Ensured high availability and scalability for multiple participants during the event.

Core Team — GDGZUJ (Google Developer Group), Al-Zaytoonah University of Jordan

2025 – Present

- Serve as a technical member on the core team of the university's Google Developer Group chapter.
- Build and present technical projects and demos at community events.
- Deliver tech talks and workshops on development and security topics for students.

Skills

Area	Level
Security	Advanced
Automation	Basic
Networking	Intermediate
Python	Intermediate
Java	Intermediate
Computer Tech	Intermediate
Front End (HTML, CSS, JavaScript)	Intermediate
Bash Scripting	Basic
MySQL	Basic