NAWAF ALKATHERI

Riyadh, Saudi Arabia
+966 53 929 3414 eng.nawafalkatheri@gmail.com linkedin.com/in/nawaf-a-3969a4217 github.com/NawafAlk

Summary

Cybersecurity graduate (B.E. Computer Science Engineering — Cyber Security, First Class with Distinction) with CompTIA Security+ and eJPT certifications. Hands-on experience in penetration testing, SIEM monitoring, and digital forensics — including building ForensAI, an AI-powered forensics platform integrating LLM analysis with rule-based risk scoring — with a Top-3 finish at the Resillion CTF competition. Seeking a SOC Analyst / Cybersecurity Analyst role.

Education

GITAM University **Graduated Apr. 2026**
Bachelor of Computer Science Engineering (Cyber Security) *Bangalore, India*

First Class with Distinction

Projects

ForensAI — AI-Powered Digital Forensics Platform | *Python, PySide6, Groq API, SleuthKit* **June 2025**

- Built a cross-platform disk-image forensics platform (E01/EWF, raw) supporting acquisition with on-the-fly hashing (MD5 / SHA1 / SHA256), NTFS/FAT32 file-system analysis, Windows registry examination, and file carving across 13 formats with confidence scoring.
- Integrated an LLM analysis layer (Groq API, Llama 3.3 70B) that explains file artifacts, registry keys, and timestamp anomalies, and generates deleted-file overwrite narratives from cluster-level recovery analysis.
- Designed a hybrid risk engine combining 28 deterministic forensic rules (0–100 severity scores) with AI contextual re-evaluation and natural-language artifact search.
- Engineered chain-of-custody controls: an immutable JSONL audit trail with SHA-256 hash chaining covering every risk assessment and AI interaction.

Network Scanner | *Python, Networking* **Apr 2024**

- Developed a network scanning tool for host discovery and service enumeration.
- Implemented ICMP and TCP-based scanning techniques with customizable scan options.
- Performed automated device identification and basic network analysis for security assessment workflows.

Certifications

CompTIA Security+ (SY0-701) | *CompTIA* **Aug 2024**

eLearnSecurity Junior Penetration Tester (eJPT) | *INE Security* **Oct 2022**

Achievements

Top 3 — Resillion CTF Competition **2025**

1st Place — Open Hackathon, GITAM University **2026**

1st Place — Final-Year Project Award (ForensAI) **2026**

Skills

SIEM & Security Monitoring: Splunk, Log Analysis, Alert Triage, Threat Detection

Network & Traffic Analysis: Wireshark, Nmap, TCP/IP Protocol Analysis

Operating Systems & Scripting: Linux Administration, Bash, Python (Security Automation, Log Parsing), Windows Event Log Analysis

Security Operations: Incident Response, Digital Forensics & Evidence Integrity, Vulnerability Assessment, Penetration Testing Fundamentals (eJPT Certified)

Frameworks & Standards: MITRE ATT&CK, NIST Incident Response (SP 800-61), NCA Essential Cybersecurity Controls (ECC) – Familiarity

Languages: Arabic (Native), English (Proficient)