NIKHIL SHAKYA

LinkedIn: linkedin.com/in/nikhilshakya0905/ Email: nikhilshakya0905@gmail.com
GitHub: github.com/Nikhil0905/ Mobile: +91-9872408318

SKILLS

- Languages: Python, C/C++, Bash, SQL, Solidity basics, PowerShell basics
- Frameworks: HTML, Flask, OWASP Top 10
- Tools/Platforms: Linux, Windows, AWS, MySQL, Burp Suite, Metasploit, Active Directory, Splunk, Wazuh, Git/GitHub, Docker, Jenkins, Remix IDE, Cursor AI, Antigravity, MCP, Notion
- Core Concepts: Networking, Linux & Windows Internals, Web Application Pentesting, Cloud, DevOps, Security Operations Centre, Digital Forensics, Blockchain, Operating Systems, Data Structure & Algorithm, Analytical Reasoning, DBMS
- Soft Skills: Leadership, Analytical Thinking, Adaptability, Collaboration & Teamwork, Attention to Detail, Documentation & Reporting

INTERNSHIPS

Cyber Security Intern | Techvanto Jun 2025 – Jul 2025

- Developed SmartNetIDS, a machine learning–based Network Intrusion Detection System for real-time anomaly detection and proactive identification of common cyber threats.
- Conducted security assessments and penetration testing on live projects, utilizing tools such as Nmap, Wireshark, and Metasploit to identify vulnerabilities in networks and web applications.
- Solved 60+ labs and gained hands-on experience in network security, web application security, and incident response, applying practical techniques to simulate and mitigate real-world attacks.

PROJECTS

ForgeOps | Link Apri 2026 - May 2026

- Tech-Stack: Docker, Jenkins, Gitea, Nexus, Prometheus, Grafana, Python, Flask, Nginx, Bash
- Architected an offline-first DevOps platform tailored for air-gapped and low-connectivity environments, enabling uninterrupted CI/CD workflows without reliance on external cloud infrastructure or SaaS-based tooling.
- Integrated 13 containerized services into a unified self-hosted ecosystem supporting source control, automated pipelines, artifact management, deployment orchestration, monitoring, and rollback capabilities to improve infrastructure resilience and deployment reliability.
- Devised a Python-based synchronization and observability framework with Flask REST APIs that automated repository replication, deployment auditing, infrastructure health tracking, and operational monitoring through a centralized real-time dashboard.

Behavioral Malware Analysis | Link May 2026

- Tech-Stack: Wazuh, Sysmon, Process Monitor, Regshot, Autoruns, Windows 10, AWS EC2
- Constructed and configured a complete malware sandbox infrastructure from the ground up using Wazuh SIEM, Sysmon, and KVM/QEMU to perform behavioral malware analysis in a controlled Windows 10 environment.
- Investigated a Trojan.NoEscape/AsyncRAT-style malware sample by correlating Sysmon telemetry, registry hive diffs, and alerts, uncovering 497+ security events, 185 executable drops, and 54+ DLL hijack indicators aligned with MITRE ATT&CK techniques.
- Uncovered advanced attack behaviors, including FodHelper UAC bypass, PowerShell-based payload staging, runtime .NET compilation, and DLL search-order hijacking, while compiling a DFIR-style incident report with IOCs, attack-chain reconstruction, and actionable detection recommendations.

InsightOps | Link Feb 2026 – Mar 2026

- Tech-Stack: Splunk, Python, Flask, REST APIs, MITRE ATT&CK, Windows Server, Linux, KVM/QEMU
- Engineered an AI-assisted SOC intelligence system integrated with Splunk that transforms raw alerts into multi-stage incidents across Windows and Linux using MITRE ATT&CK-aligned detection logic.
- Formulated a deterministic risk-scoring model (0 - 100) and orchestrated a 6-stage Python pipeline (REST + HEC) to ingest, correlate, and enrich alerts with contextual explanations via a Flask monitoring interface.
- Optimized analyst triage by reducing alert noise by ~80 - 90% (20 - 30 alerts into 1 incident) and reported incidents (high-risk ≥ 75) with scores reaching 100 for multi-stage attack chains.

CERTIFICATIONS

- Security+ Certified | CompTIA — May 2026
- Certified Blue Team Practitioner (CBTP) | SecOps Group — Mar 2026
- Quick Heal Certified Digital Forensics Investigator (QHDFI) | QuickHeal — Mar 2026
- Network+ Certified | CompTIA — Jan 2025

ACHIEVEMENTS

- Maintain technical blogs covering Labs, CTFs, project breakdowns, and practical learning experiences | Medium — Since Apr 2025
- Ranking Top 2% Gobally | TryHackMe — Since Jan 2024
- Solved 400+ programming problems across all online coding platforms and courses | Codolio | NeoColab — Apr 2026
- Participated in 15+ CTF events at the University, National, and international levels | CTF — Apr 2026

EDUCATION

Lovely Professional University — Punjab, India
Bachelor of Technology (Hons.) - CSE with specialization in Cybersecurity and Blockchain | CGPA: 8.70 — Since Aug 2023

Kendriya Vidyalaya 3 Base Repair Depot, Air Force Station — Chandigarh, India
Intermediate - PCM with Computer Science | Percentage: 86 — Apr 2022 – Mar 2023
High School - CBSE | Percentage: 93.6 — May 2020 – Apr 2021