Nikhil Kumar

Aspiring Cyber Security Analyst

GitHub: nikhilkumar0102

LinkedIn: nikhil-kumar-professional

Email: nikhilkumar01.name@gmail.com

Phone number: +917903953826

VIT Bhopal University

Entry-Level **Cybersecurity Analyst** with a B.Tech in **Cybersecurity & Digital Forensics** and hands-on experience in **penetration testing**, **SOC operations**, and **threat detection**. Proficient in using tools like **Wireshark**, **Nmap**, **Burp Suite**, and **Splunk** to perform **vulnerability assessments**, **incident response**, and **malware analysis**. Certified through programs from IBM and TryHackMe, with a strong foundation in **Python scripting** for developing custom security tools.

Education

Vellore Institute of Technology, Bhopal *June 2022 – Ongoing*

B.Tech, Computer Science (Cybersecurity & Digital Forensics) *Cumulative CGPA: **8.15/10***

Training and Certifications

- **Software Security Testing:** Certified in vulnerability analysis and penetration testing against OWASP Top 10 and NIST frameworks, using tools like Nessus, OWASP ZAP, and Burp Suite. Experience includes static/dynamic analysis and generating reports with CVSS scoring.
- **IBM - Cybersecurity Analyst SOC skills:** Demonstrated proficiency in threat intelligence, SIEM, incident response, network defence, and compliance.
- **TryHackMe Advent of Cyber 2024:** Gained hands-on SOC experience in threat detection, web security, and infrastructure defence.
- **Practical Labs CTFs (TryHackMe & CyberDefenders):** Strengthened skills in incident response, threat hunting, and vulnerability analysis through practical labs.

Practical Projects

Linux-CIS-Audit Tool || ***(Python, google-generativeai, rich, python-dotenv)***

- **Developed** an AI-enhanced tool for **auditing Debian-based Linux systems** using **CIS Benchmarks**.
- **Generated** detailed **security posture scores** and provided expert explanations and actionable recommendations for system hardening using Google's Gemini API.

NetScan_ || ***(python-nmap, prompt-toolkit, tqdm, colorama, tabulate)***

- **Created** a **network scanning tool** leveraging **Nmap** for efficient host discovery, **port scanning**, and service enumeration.
- **Designed** the tool for **network administrators** and **security professionals** with both command-line and interactive modes.
- **Enabled** detailed reporting and scan history tracking to support **vulnerability detection**.

PassGenius || ***(Python Security Suite)*** || ***(zxcvbn-python, rich, PyYAML, HIBP API)***

- **Developed** a **CLI tool** for **advanced password auditing** and offensive security, providing robust, pattern-based strength analysis.
- **Proactively detected** compromised credentials and **automated** custom wordlist generation for **penetration testing**.
- **Supported vulnerability assessment** workflows with detailed reporting and analysis.

Skills

Language & Programming: C++, Python, Linux Shell Scripting, SQL

Cloud & Networking: AWS (IAM, EC2, S3, VPC, CloudTrail, Security Groups), LAN Troubleshooting