NIKHIL KUMAR

Cyber Security Analyst

Address: Ahmedabad, Gujarat | **LinkedIn** | **Github** | **Phone**: **7903953826** | **Email**: nikhilkumar01.name@gmail.com

EDUCATION

Vellore Institute Of Technology Bhopal (VITB) || B-Tech: Computer Science and Engineering (CSDF) (CGPA 8.15) **2022-2026**

Kendriya Vidyala No.1 Shahibaugh, Ahmedabad || Class 10th (85%) || Class 12th (80%)

TECHNICAL SKILLS

Technical Skills: Python, HTML/CSS, Kali Linux, AWS, Vulnerability Assessment, Penetration Testing, Wireshark , Nmap , Burp Suite, Splunk, Web Security Testing, API Security Testing.

EXPERIENCE

ELEVATE LABS || CYBERSECURITY INTERNSHIP (REMOTE) — Aug 2025 - Sep 2025

- Executed foundational Vulnerability Scanning and Phishing Email Analysis.
- Configured Firewall rules and utilized VPNs for network access control and security.
- Conducted packet analysis using Wireshark for network traffic inspection and forensics.
- Developed secure applications (Chat App) and practiced strong password management techniques.
- Addressed endpoint security by remediating suspicious browser extensions

HACK SECURE || CYBERSECURITY INTERNSHIP (REMOTE) — Apr 2025 - May 2025

- Performed Blue Team tasks: threat detection, incident response, and malware analysis in simulated SOC environments.
- Used Wireshark, Splunk, ELK Stack, SQLMap, and VirusTotal for scanning, sniffing, and vulnerability testing.
- Executed SQL injection, XSS testing, port scanning, and directory brute-forcing for application security validation.
- Investigated ransomware using Sysmon and Splunk; mapped attacker behavior and analyzed CVEs.
- Strengthened skills in SIEM, log analysis, packet inspection, and network forensics.

ACADMIC PROJECTS

LINUX SECURITY AUDIT TOOL - CIS BENCHMARK — Sep’ 25

- Developed an automated security auditing tool in **Python 3** to assess the vulnerability posture of **Debian Linux systems** by validating configurations against the **CIS Benchmark**.
- Engineered checks for critical controls by parsing system outputs **(e.g., sshd -T, findmnt)**, verifying file permissions (**/etc/shadow**), and ensuring secure SSH policies **(PermitRootLogin).**
- Expanded audit coverage to include logging & auditing (verifying auditd service status) and complex firewall rule analysis, including checks for UFW and **nftables** default-deny policies.
- Integrated the **Google Gemini API** to provide **AI-enhanced analysis** and **generate context-aware remediation steps** for failed security controls, transforming standard results into actionable intelligence.

PASSGENIUS - INTERACTIVE PASSWORD SUITE — Aug’ 25

- A command-line tool (CLI) built in Python that acts as a complete suite for auditing and testing password security.
- It uses the **zxcvbn-python** library to perform a "**pattern-based**" strength check. This is an advanced method that looks for common words, names, dates, or keyboard patterns (like qwerty), not just character types.
- It uses the **HIBP (Have I Been Pwned) API** to check if a password has already been exposed in a known data breach.
- It helps penetration testers (ethical hackers) by automatically creating custom lists of potential passwords (wordlists) to test a system's defenses.
- It uses the **rich library** to present its findings in detailed, color-coded, and easy-to-read reports directly in the terminal.
- It uses **PyYAML** to manage settings, such as API keys or tool preferences.

CERTIFICATIONS

- Cyber Security Analyst (IBM)
- Advent SOC (TryHackMe)
- Software Security Testing (Packt)
- Network fundamentals (EC-Council)
- Automate Cybersecurity Tasks with Python (Coursera)
- Play It Safe: Manage Security Risks (Coursera)