Nikhil Kumar
Aspiring Cyber Security Professional
nikhilkumar01.name@gmail.com | +91 7903953826 | github.com/nikhilkumar0102 | LinkedIn
VIT Bhopal University, MP

Education

Bachelor of Technology (B.Tech) Jun 2022 - Ongoing
Vellore Institute of Technology, Bhopal
Computer Science and Engineering (Cybersecurity & Digital Forensics)
CGPA: 8.15/10

Training and Certifications

- **Packet - Software Security Testing:** Vulnerability analysis and software security testing. Proficient in using tools like Nessus, OWASP ZAP, and Burp Suite to perform static/dynamic analysis and penetration testing against OWASP Top 10 and NIST frameworks. Experienced in authoring clear, actionable reports with CVSS scoring.
- **IBM Cybersecurity Analyst:** Gained SOC analyst skills in threat intelligence, SIEM, incident response, network defense, and compliance using real-world tools and case studies.
- **TryHackMe – Advent of Cyber 2024:** Hands-on with IAM, DLP, OWASP Top 10, privilege escalation, malware analysis, cryptography, threat hunting, and digital forensics.
- **EC-Council Network Security:**Networking protocols, identity theft analysis, cyber-attack mitigation, and practical use of Zeek for traffic monitoring.

Practical Projects

- **PassGenius (Python Security Suite):** Developed a CLI-based password security toolkit using Python and argparse to promote secure credential practices. The tool features an advanced analyzer that evaluates password strength with the zxcvbn library and cross-references credentials against the Have I Been Pwned (HIBP) API for breach detection. It also includes a secure password generator and a custom wordlist generator, which leverages NLTK for contextual analysis, to simulate targeted password attacks during penetration tests.
- **NetScan (Python Tool):** Developed a CLI-based network security tool using Python that wraps Nmap to automate network discovery and vulnerability assessment. The tool performs service/OS detection, identifies known vulnerabilities based on software versions, and generates detailed reports. It also features a scan history database for tracking and comparing results over time.
- **Phishing Simulation (IBM Internship):** Conducted a social engineering exercise using Zphisher on Kali Linux to demonstrate modern credential harvesting techniques. Analyzed the attack lifecycle and presented a report on effective threat mitigation strategies, focusing on user education and defensive security controls to reduce organizational risk.
- **Advanced Network Scanning (Guide):** Authored a knowledge base for ethical hacking and Red Team operations, documenting advanced network reconnaissance and evasion techniques. This research details methodologies for executing stealth scans (TCP/UDP), bypassing firewall/IDS/IPS defenses, and performing OS fingerprinting with the Nmap Scripting Engine (NSE), demonstrating a comprehensive understanding of the penetration testing lifecycle and modern threat actor tactics.

Professional Experience

Cybersecurity Intern – Hack Secure Apr 2025 - May 2025 (Remote)

- 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.

Technical Skills

- **Programming Languages:** C++ | Python | Linux Shell Scripting
- **Cybersecurity Tools:** Wireshark | Nmap | OSINT | Nessus | Burp Suite
- **Networking:** VLAN Setup | Cisco Router Configuration | LAN Troubleshooting
- **Soft Skills:** Project Management | Leadership | Adaptability | Emotional Intelligence