Nikhil Kumar

Aspiring Cyber Security Professional
github.com/nikhilkumar0102|LinkedIn/nikhil-kumar-professional

Email: nikhilkumar01.name@gmail.com
Phone number: +91 7903953826
VIT Bhopal University, MP

Motivated cybersecurity enthusiast with hands-on experience in ethical hacking, blue teaming, and system security. Skilled in threat detection, incident response, and vulnerability assessment. Experienced in documenting labs and technical workflows to support learning and knowledge sharing.

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

Intermediate ***Jul 2013 - Jul 2022***

Kendriya Vidyalaya, Ahmedabad

- Class 12th (Senior Secondary): 80% || Class 10th (Secondary): 85%

Training and Certifications

- **IBM Cybersecurity Analyst**: Gained SOC analyst skills in threat intelligence, SIEM, incident response, network defence, and compliance using real-world tools and case studies.
- **Google Cybersecurity Certificate:** Linux, MySQL, Python, network security, risk management, incident response (Wireshark, Splunk).
- **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

- **Advanced Network Scanning (Guide):** Authored a compact guide on Nmap, Netdiscover, stealth scanning, firewall evasion, and enumeration for cybersecurity learners.
- **NetScan (Python Tool):** Built a CLI-based Nmap wrapper for automated scanning, service detection, and scan history management.
- **CyberDefenders Labs:** Solved blue team labs simulating SOC tasks like malware analysis, forensics, and threat detection.
- **TryHackMe Labs:** Completed hands-on CTFs on scanning, privilege escalation, forensics, and web exploitation.
- **Lab Write-ups:** Documented challenges from TryHackMe and CyberDefenders, highlighting tools, attack paths, and fixes.
- **Web Portfolio:** Designed a responsive site using HTML/CSS/JS, hosted on GitHub Pages to showcase frontend skills.

Professional Experience

Cybersecurity Intern – Hack Secure ***April 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