VISHAL KUMAR

Phone: +91-6299641204 | Email: vishal630488@gmail.com | LinkedIn: linkedin.com/in/vishal-kumar

PROFESSIONAL SUMMARY

Cybersecurity Analyst with strong hands-on experience in network security, ethical hacking, and penetration testing. Proficient in identifying and reporting real-world vulnerabilities, with a proven track record of responsibly disclosing critical issues—such as a misconfigured Grafana instance found during reconnaissance on Cloudie.hk. Adept at working across platforms like Windows, Kali Linux, and Arch Linux. Experienced with tools like Nmap, Wireshark, Burp Suite, Metasploit, and others. Skilled in Python, C++, Rust, and Assembly, with a keen interest in malware analysis and reverse engineering. Certified in foundational cybersecurity concepts from Palo Alto and practical threat-hunting labs via TryHackMe.

EDUCATION

- Bachelor of Technology (B.Tech) in Cybersecurity
- Parul University | 2024- 2028 (Ongoing)

CERTIFICATIONS

- Palo Alto Networks Cybersecurity Foundation Certificate
- TryHackMe Certification - Completed multiple hands-on labs

TECHNICAL SKILLS

Operating Systems: Windows, Kali Linux, Arch Linux

Languages: Python, C++, Rust, Assembly

Cybersecurity Tools:

- Reconnaissance & Scanning: Nmap, Nikto, Shodan
- Vulnerability Analysis: Nessus, OpenVAS, Burp Suite
- Exploitation: Metasploit, SQLmap
- Packet Analysis: Wireshark, Tcpdump
- Web Security: OWASP ZAP, Dirb, Gobuster
- Other: GDB, Radare2, Ghidra, VirtualBox, Docker

PROJECTS & RESEARCH

- Grafana Misconfiguration Vulnerability Disclosure:
  - Discovered an unsecured Grafana instance during pentesting and reported it to Cloudie.hk.
  - Drafted a professional disclosure email outlining risks and remediation.

- Keylogger with Remote Logging and Stealth Mode:
  - Developed a cross-platform keylogger with anti-VM and Telegram/Cloudflare Tunnel-based log exfiltration.
- Red Team Simulation Setup:
  - Simulated a red team engagement using Empire, Cobalt Strike, and custom payloads.
- Network Monitoring & Packet Analysis Tool:
  - Created a Python tool for logging traffic metadata and detecting suspicious patterns.

ACHIEVEMENTS

- Completed multiple real-world hacking labs on TryHackMe
- Reported live vulnerability in production environment
- Built advanced tools for red teaming and threat emulation