

Kamlesh Kumar

Phone No: +91 6266314789 | Kamleshsande85@yahoo.com | [LinkedIn](#) | [GitHub](#) | DOB : 22-08-2000

ASPIRING NETWORK & SECURITY ENGINEER

Aspiring Network Engineer with a strong foundation in networking concepts, including routing, switching, subnetting, and network performance monitoring. Proficient in Python and Linux, with exposure to Wireshark, Nmap, Metasploit, and basic routing/switching. Currently preparing for the CompTIA Network+ and Security+ certifications, with a dual focus on optimizing enterprise networks and securing network infrastructure from evolving threats.

EDUCATION

Master of Computer Applications (MCA) (Ongoing)

Pandit Ravi Shankar Shukla University, Raipur — CGPA: 7.5 (Expected July 2025)

Bachelor of Science (B.Sc.) in Computer Science

Shaheed Nand Kumar Patel University, Raigarh — CGPA: 7.35 (2021–2023)

High School (10th) – 85% (2017) | Higher Secondary (10+2) – 331/500 (2020)

CORE TECHNICAL SKILLS

Networking Tools & Protocols: Wireshark, Nmap, Packet Tracer, TCP/IP, DHCP, DNS, ARP, VLANs

Cybersecurity: SIEM (Splunk/QRadar), EDR (CrowdStrike), Log Analysis (ELK), Network Forensics (Wireshark), Threat Intel (MITRE ATT&CK), Incident Response.

Operating Systems: Linux (Kali, Debian), Windows

Programming & Scripting: Python (automation & network tools), Bash

Virtualization & Labs: VirtualBox, VMware, TryHackMe, picoCTF

PROJECTS & TOOLS BUILT

Enterprise Network Design and Security Audit - CCNA exam prep project for hands-on experience in network design, security, routing, switching, and IP addressing. [GitHub](#)

Implementation and Detection of Ransomware Attacks - This project focuses on ransomware attacks—demonstrating how they encrypt files, how they operate, and methods to detect and prevent them using different algorithms and techniques. [GitHub](#)

IP Scanner Tool - CLI tool for converting domain to IP with WHOIS and port scan capabilities. [GitHub](#)

Wireshark Analysis - Captured and analyzed live packets to understand HTTP/DNS/ARP traffic flow.

Directory Brute Force Tool - Simulated directory discovery in pentest scenarios using Python + wordlists.

OPEN SOURCE CONTRIBUTIONS

Created "**2700 Networking Questions**" repository to help CompTIA Network+ (N10-009) aspirants, covering protocols, security, troubleshooting, and wireless concepts. [GitHub](#)

EXPERIENCE (INTERNSHIPS)

Vault-Tec Security – Cybersecurity Intern (Sep–Nov 2024) [Certificate](#)

- Built password generation & validation tools.
- Explored IP reconnaissance and info-gathering tools.

ShadowFox Cybersecurity – Intern (Oct 2024) [Certificate](#)

- Trained on Wireshark, Metasploit, Veracrypt, Aircrack-ng.
- Performed live recon in lab scenarios.

Acmegrade – Cybersecurity Intern (Jul–Sep 2024) [Certificate](#)

- OSINT gathering, social engineering simulation, and protocol analysis.

CERTIFICATIONS

CISCO : [Networking Basics](#)

Amazon : [AWS Educate Getting Started with Networking](#)

Google : [The Bits and Bytes of Computer Networking](#)

NPTEL: Ethical Hacking [Certificate](#)

NPTEL: Practical Cybersecurity [Certificate](#)

CompTIA Network+ – Preparation in progress

CompTIA Security+ – Preparation in progress

CYBER LABS & LEARNING PLATFORMS

[TryHackMe Profile](#) – Completed beginner to intermediate rooms (King of the Hill, Passive Recon)

[picoCTF](#) – Practicing reverse engineering and cryptography challenges