Mukund Rao, B.Tech.

Phone: +91-7004128536

Email: mukundrao9852@gmail.com

LinkedIn: linkedin.com/in/mukund-rao-36293a251/

INTRODUCTION

Cybersecurity enthusiast with hands-on experience in network attacks, threat detection, and malware analysis. Actively pursuing CEH and eJPT to deepen offensive security skills.

CORE EXPERTISE & SKILLS

- Pentesting & Detection Stack: Nmap, Wireshark, Burp Suite, SQLMap, aircrack-ng, arpspoof; ARP Poisoning, MITM, SQLi, XSS; Python scripting; MITRE ATT&CK, OWASP Top 10.
- Technical Expertise: Hands-on experience with Kali Linux & Offensive Security, Javascript Code Debugging and Log Analysis.
- Software Skills: Python, C++, Javascript Debugging, SQL database management, MERN (HTML, CSS, Javascript), Java (basic).

EDUCATION

Vellore Institute of Technology | *B.Tech in Computer Science* | Bhopal, MP 2022-26

- Final Year; CGPA: 8.02/10.00

KEY CERTIFICATIONS

- Google's Professional Cybersecurity Certificate: Learned Blue Teaming and basic cybersecurity principles.
- EC Council C|EH (Certified Ethical Hacker): Enrolled and actively studying under direct guidance from EC Council.
- INE eJPT (Junior Penetration Tester): Enrolled and studying from official INE prep material under guidance of Alexis Ahmed.
- IBM Cybersecurity Analyst: Learned Blue Teaming, SIEM, Logs, OWASP 10 etc. in detail.
- IBM Generative AI: Learned all principles of AI and APIs. Made various projects.

PROFESSIONAL EXPERIENCE

NULLCLASS | *SOC Analyst Internship* - Remote June 2025 - July 2025

- Completed extensive training.
- Contributed to 3+ key projects including malware analysis and intrusion detection systems.
- Wrote detailed analysis reports summarizing threats and detection outcomes.

Amroha Police Cybersecurity Internship | *APCSIP-2025* - Amroha, UP June 2025 - June 2025

- Two week internship under IPS Officers of UP Police.
- Selected by screening test, awaiting offer letter.

PROJECTS

Custom Correlation Rules in ELK Stack June 2025

- Built and tested 6+ detection rules for credential stuffing, DNS tunneling, and PowerShell exploitation across 3 lab environments.
- Used Filebeat, Logstash, and Kibana to ingest, parse, and visualize attack patterns.
- Created alerts using custom logic and plotted behaviors to MITRE ATT&CK.

HawkEye Stealer – Red & Blue Team Analysis June 2025

- Analyzed a malware PCAP with 40+ network packets to extract 15+ IOCs and mapped 7+ TTPs to MITRE ATT&CK.
- Simulated attacker behavior and documented SMTP-based data theft using HawkEye.
- Performed forensic labs and charted detection to ELK and MITRE techniques.

PenTesting, ARP Poisoning and MitM Attacks Nov 2024

- Performed 3+ network-based attacks including ARP poisoning and MitM across 2 virtual machines in a lab setup.
- Used Kali Linux to attack 2 Windows VMs with tools like arpspoof and airmon-ng.

Hospital Management Website October 2024

- Built a cloud-based platform for doctors and patients to share medical records securely with a team.
- Integrated AI chatbot and security features using OWASP Top 10 practices to protect PII & SPII data.

LABS

- **TryHackMe Labs:** Completed 35+ cybersecurity rooms along with 'Intro to Cybersecurity' & 'Cybersecurity 101' career paths.
- **Practical Labs | INE eJPT**: 30% of 158 practical labs completed. Ongoing SkillCheck CTFs.
- **Practical Labs | EC Council C|EH**: 50% of 20 practical labs completed. Ongoing.
- **Hawkeye Lab | Cyberdefenders**: 100% Completed.