

Akshay Yuvan

[in](#) LinkedIn | [+91 709599562](#) | [M](mailto:akshayyuvan123@gmail.com) akshayyuvan123@gmail.com | [GitHub](#)

Education

B.Tech in CSE with Cyber Security **Vellore Institute of Technology** *Chennai* **09/2022 - Current**
(Expected Graduation:05/2026)

- Major in Computer Science & Engineering
- Maintaining a CGPA: 9.2 / 10.0 (till 6th Semester)

Experience

Cyber Security Virtual Internship **ShadowFox** *Remote* **09/2025 to 10/2025**

- Conducted security assessments across **6+ controlled lab scenarios**, performing service discovery, directory enumeration, and network traffic analysis to identify insecure configurations and potential credential exposure.
- Analysed **100+ packet capture events** to detect plaintext data leakage patterns and validated secure transport mechanisms, contributing to improved security hardening recommendations.
- Executed **multiple controlled exploitation simulations** within sandboxed virtual environments to understand attacker paths and document mitigation strategies.
- Delivered **4+ structured Proof-of-Work security reports** covering scope, methodology, findings, severity classification, and remediation steps, all of which were reviewed and mentor-validated.

Projects

Cyber Security **Web Application Security Assessment Report (Lab Target)** Project Report

- Completed an end-to-end security assessment on **1 vulnerable web application**, identifying **10+ exposure points** across service discovery, access control, and data handling.
- Documented findings using **severity-based classification** and provided **actionable remediation steps**, resulting in a structured assessment report suitable for audit review.

Network Traffic & Credential Exposure Analysis Security Analysis Report

- Analysed **100+ packet capture events** to detect plaintext credential leakage patterns and insecure communication flows.
- Assessed risks across **multiple traffic scenarios** and proposed **secure-by-default configurations**, reducing interception risk in simulated environments.

Pentesting Lab Walkthrough + Remediation Plan Lab Walkthrough

- Performed guided penetration testing across **3+ controlled lab scenarios**, identifying common misconfigurations and weak authentication paths. Developed a remediation plan with **step-by-step patch recommendations** and documented methodology, outcomes, and evidence in a format suitable for hand-off.

Skills:

- **Programming Languages:** Python, C, C++, JavaScript, Bash (Basics)
- **Cyber Security & Networking:** Web Application Security Fundamentals, Network Security Basics, Vulnerability Assessment, Traffic & Packet Analysis, Authentication & Session Security, Encryption Fundamentals, Threat & Attack Surface Analysis
- **Security Tools & Platforms:** Nmap, Wireshark, Burp Suite (Basics), Metasploit (Lab Environment), Kali Linux, TryHackMe, VeraCrypt
- **Databases & Systems:** MySQL (Basics), Linux (Command Line), Virtual Machines (VMware / VirtualBox)
- **Version Control & Deployment:** Git, GitHub
- **Languages:** English, Tamil, Telugu

Course Works:

- **Core:** Computer Networks, Data Structures and Algorithms, Object Oriented Programming, Operating Systems, DBMS.

Achievements & Certifications:

- Google Cybersecurity Professional Certificate - Demonstrated foundational understanding of security principles, threat identification, incident response concepts, network security, and risk management practices.
- CTF Challenge Winner (University): Secured a top position in a Capture The Flag (CTF) competition by successfully solving challenges related to web security, basic cryptography, and network reconnaissance in a controlled environment.
- Active Participation in Security Labs & Challenges: Regularly engaged in hands-on security challenges and lab-based exercises, strengthening practical skills in vulnerability identification, traffic analysis, and remediation documentation.