Last updated in November 2025

Divakar K

Chennai | k.divakar1626@gmail.com | 9342006729 | TryHackMe | Divakar K | Diva-07

Summary

Cybersecurity-focused B.E. Computer Communication Engineering student with strong skills in networking, Linux, SOC analysis, and penetration testing. Passionate about identifying vulnerabilities, improving security posture, and building real-world security labs. Actively learning modern offensive and defensive techniques to begin a career as a SOC Analyst or Cybersecurity Engineer.

Experience

Role: Penetration Testing (Internship)
Elevate labs

- Assisted in penetration testing and security assessment of web and mobile applications.
- Conducted vulnerability scanning, risk analysis, and reported findings with remediation steps.
- Gained hands-on experience in tools like Burp Suite, Nmap, and OWASP testing methodologies.
- Collaborated with the security team to improve application security posture.

Skills

CyberSecurity : Nmap, Burp Suite, Tenable Nessus, Metasploit Framework, Wireshark, Social Engineering , nikto , OWASP ZAP, sqlmap(basic), Splunk(SIEM), WFuzz, Gobuster, Searchsploit, Hydra, Zeek

Programming: Python, Java, MySQL.

Certifications

CyberSecurity – CISCO

AWS cloud certification

CC (Certified in Cybersecurity) – ISC2 Credit

CCEP - Red Team Leader

AWS Security Encryption

Education

Rajalakshmi Institute of Technology *Sept 2023 – Present*
B.E in Computer and Communication Engineering

Projects

WEB APPLICATION VULNERABILITY SCANNER

- Developed a Python–Flask based vulnerability scanner that uses BeautifulSoup for crawling and automated payload injection to detect XSS, SQLi, and CSRF attacks based on OWASP Top 10 standards. Integrated a simple reporting dashboard for results visualization.
- Tools Used: Python, requests, BeautifulSoup, OWASP top 10 checklist, Flask

Tor GuardNode Prediction — Hackathon Team Project (2025)

- Simulated a Tor network using Chutney for relay-level forensic analysis. Generated traffic data and extracted features for ML training. Built XGBoost model to detect deanonymization patterns. Delivered a compact cybersecurity ML solution with team collaboration.
- Tools Used: Chutney, Tor Expert Bundle, Python, Pandas, Scikit-Learn, XGBoost, JSON, Matplotlib.

SQL INJECTION PLAYGROUND WITH DETECTION ENGINE

- Built a SQL Injection practice lab using Flask/PHP to demonstrate vulnerable vs secure query handling. Developed a Python-based detection engine to identify malicious SQLi payloads and log attack attempts.
- Tools Used: PHP/Flask, SQLite, Python detection tool