

VARUN RAJ V

+91 8148792490 | varun2003raj@gmail.com | Kanyakumari, Tamil Nadu, India
[linkedin.com/in/varun2003raj](https://www.linkedin.com/in/varun2003raj) | github.com/varun2003raj

PROFESSIONAL SUMMARY

Entry-level IT professional and cybersecurity enthusiast seeking internship or entry-level opportunities in Cyber Security, SOC Analysis, Networking, IT Support, or System Administration. Skilled in networking fundamentals, Linux and Windows administration, virtualization, and cybersecurity tools with hands-on lab experience. Eager to contribute to security monitoring, system protection, and IT operations.

EDUCATION

B.E. – Computer Science Engineering (Cyber Security)	2022 – 2026
<i>Dhanalakshmi Srinivasan College of Engineering, Coimbatore CGPA: 7.9 Minor: Indian Administration (Honours)</i>	
Higher Secondary (12th Grade)	2022
<i>S.N.M. Hindu Vidyalaya Matric Hr. Sec. School, Kanyakumari 67%</i>	
Secondary (10th Grade)	2020
<i>S.N.M. Hindu Vidyalaya Matric Hr. Sec. School, Kanyakumari 69%</i>	

TECHNICAL SKILLS

Cybersecurity Tools: Nmap, Wireshark, Burp Suite, Nessus, Metasploit, DVWA, Metasploitable 2
Security Concepts: SQL Injection (SQLi), Cross-Site Scripting (XSS), Vulnerability Assessment, Penetration Testing
Operating Systems: Linux (User/Permission/Group Management), Windows Administration, VirtualBox, VMware
Networking: IP Addressing, DNS, DHCP, TCP/UDP, Network Scanning, Traffic Analysis
Programming: Python (Basic), Java (Basic), PowerShell (Basic)
Platforms: PortSwigger Web Security Academy, picoCTF, DVWA Labs

EXPERIENCE

Cyber Security Intern – Novitech	March 2024 (10 Days)
- Set up virtual lab environments using VirtualBox for cybersecurity practice and testing - Performed network discovery using Angry IP Scanner and network scanning using Nmap - Analyzed network traffic and inspected packets using Wireshark - Gained hands-on understanding of core cybersecurity operations and industry tools	

PROJECTS

AI-Based Phishing & Scam Detection System	Final Year Project
- Developed a mobile-based system to detect phishing and scam messages in real time - Classified messages as Safe, Suspicious, or Phishing using a multi-factor scoring system - Implemented rule-based logic combined with a TensorFlow Lite model for deep text analysis - Analyzed text patterns and embedded malicious links to improve detection accuracy	
Hybrid Honeypot System	FITA Academy
- Developed a hybrid honeypot using Python, Flask, SQLite, and Cowrie SSH Honeypot to monitor and analyze malicious activities in a controlled environment - Detected and logged Brute Force, SQL Injection (SQLi), XSS, and Command Injection attacks using Cowrie SSH Honeypot integration - Built a centralized monitoring dashboard to visualize web server and SSH honeypot logs; analyzed attacker behavior and payloads	
Secure Authentication Monitoring System	FITA Academy
- Developed a secure user authentication system using Python, Flask, SQLite, and BCrypt password hashing - Integrated CAPTCHA-based verification to reduce automated login attempts and bot activity - Designed monitoring mechanisms to detect Brute Force, SQL Injection (SQLi), and XSS attempts; logged events for incident analysis	
Cybersecurity Lab – DVWA & Metasploitable 2	Self-Directed
- Performed vulnerability scanning, enumeration, and exploitation in a controlled lab environment - Tested SQLi and XSS vulnerabilities using Nmap, Burp Suite, and Metasploit Framework	

CERTIFICATIONS

- Master Program in Ethical Hacking & Cyber Security – FITA Academy (May 2026)