CINCHANA S

✉ cinchanas121@gmail.com

📞 +91 7019816594

📍 Shimoga , India

🔗 LinkedIn : https://www.linkedin.com/in/cinchanas/

🖥 Portfolio : https://cinchu27.github.io/

👤 GitHub : https://github.com/cinchu27

SUMMARY

CEH-certified cybersecurity graduate with a strong interest in Red Teaming and Vulnerability Assessment & Penetration Testing (VAPT). Hands-on experience in network scanning, web application security testing. Passionate about offensive security, reconnaissance, exploitation techniques, and continuous skill development through labs and real-world inspired projects.

TECHNICAL SKILLS

- **Programming Languages:** C, Python, SQL

- **Web application penetration testing:** Burp Suite, SQL-Map, OWASP ZAP, Wireshark

- **Vulnerability scanning:** OpenVas, Nessus

- **Exploitation tools :** Metasploit, brute force, dictionary attacks

- **Operating System:** Linux, Windows

- **Network Penetration Testing & Reconnaissance**

INTERNSHIP EXPERIENCE

Trainee Software Engineer
AiROBOSOFT Products and Services   Feb 2024 – April 2024
Bengaluru, India
- Collaborated with cross-functional team members to understand requirements and implement **AI-based software solutions**.
- Gained hands-on exposure to **software development life cycle (SDLC)** practices, debugging, and performance analysis.

VAPT Intern
CyArt Tech   Dec 2025 – Current
Remote, India
- Assisted in **Vulnerability Assessment and Penetration Testing (VAPT)** for web applications and network environments, including reconnaissance and scanning using **Nmap**.
- Identified common **web application vulnerabilities**, security misconfigurations, and potential attack vectors under supervision.
- Documented findings and gained hands-on exposure to **risk assessment and remediation practices**.

Projects:-

1. **IDS Traffic Simulation**

- Designed and implemented a Python (Scapy)–based network traffic generator to simulate TCP SYN scans and test intrusion detection scenarios.
- Installed, configured, and tuned Snort IDS on Ubuntu, including custom rule creation and threshold-based port scan detection.
- Analyzed and validated IDS alerts using Wireshark packet analysis, correlating TCP flags, IP addresses, and ports to confirm detection accuracy.

2. **Networking and Security Operations (SIEM, Forensics & Traffic Analysis)**

- Designed and executed a network security operations lab involving traffic capture, protocol troubleshooting, and attack simulation using Wireshark, Kali Linux, and Ubuntu.
- Simulated an SSH brute-force attack, performed network forensics to identify repeated TCP SYN packets, failed SSH handshakes, and correlated findings with /var/log/auth.log.
- Implemented SIEM monitoring using the ELK Stack (Elasticsearch, Logstash, Kibana) to correlate failed SSH login events, build timelines, identify IOCs, and conduct threat hunting.

3. **Vulnerability Assessment & Penetration Testing (VAPT)**

- Performed lab-based VAPT on Metasploitable2 (VirtualBox) using Kali Linux, identifying and exploiting SQL Injection, XSS, Path Traversal, SMB exposure, and SSH user enumeration with Nmap, OpenVAS, and OWASP ZAP.
- Evaluated risks using CVSS v3.1 and delivered a structured VAPT report, documenting findings with Dradis CE and Excel/Google Sheets.

CERTIFICATIONS

- **Certified Ethical Hacker (CEH v13)** – EC-Council

- **TISA – Certified Information Security Auditor** – TEXIAL

- **Web Design for Everybody** – University of Michigan

- **Introduction to Cybersecurity** – Cisco Networking Academy

- **Networking Basics -** Cisco Networking Academy

EDUCATION

Bachelor of Engineering (B.E) : Computer Science   2024 | CGPA: 9.0

Malnad College of Engineering , Hassan, Karnataka.

ADDITIONAL INFORMATION

- **Practice Platforms:** TryHackMe , Portswigger
- **Languages:** English, Kannada, Hindi
- **Interests:** Red Team Operations, Penetration Testing, Security Automation, Ethical Hacking