ARAVIND CHINTHAKINDI

Hyderabad, Telangana, India
arvdchinthakindi@gmail.com | linkedin.com/in/aravind-chinthakindi | github.com/arvdch | arvdch.github.io

PROFESSIONAL SUMMARY

Detail-oriented Cybersecurity student with hands-on experience in penetration testing, vulnerability assessment, digital forensics, and blue team operations. Completed internship performing web application security testing and network enumeration. Proficient in SIEM platforms, security tooling, and CTF competitions on TryHackMe and HackTheBox. Developed open-source security tools in Python and deployed a SOC lab with Splunk for log management and threat detection. Seeking an internship or entry-level role in cybersecurity, SOC analysis, or penetration testing.

EDUCATION

Bachelor of Technology (B.Tech) — Computer Science & Engineering (Cybersecurity) *2023 – Present*

Jawaharlal Nehru Technological University Hyderabad (JNTUH) Hyderabad, India

- Specialization in Cybersecurity covering network security, digital forensics, threat detection, and incident response
- Completed team capstone project: SOC Home Lab using Splunk for SIEM and enterprise-grade log management
- Relevant coursework: Network Security, Ethical Hacking, Operating Systems, Cryptography, Cloud Security

PROFESSIONAL EXPERIENCE

Cybersecurity Intern *June 2025 – June 2025*

JD Infotech Hyderabad, India

- Conducted vulnerability assessments and penetration testing on web applications using VulnHub lab environments
- Identified and exploited web application vulnerabilities including Cross-Site Scripting (XSS), SQL Injection (SQLi), and Insecure Direct Object Reference (IDOR)
- Performed reconnaissance and information gathering using Nmap, theHarvester, dig, and WhatWeb
- Executed SMB, FTP, and SSH service enumeration and brute-force attacks using Hydra and John the Ripper
- Practiced privilege escalation techniques and post-exploitation analysis on Linux target machines
- Analyzed HTTP header security misconfigurations and documented actionable remediation recommendations
- Operated security tools including Burp Suite, sqlmap, ffuf, Enum4linux, and curl for application testing
- Produced professional vulnerability reports with risk ratings, technical findings, and remediation steps

PROJECTS

HEXFORGE — Python File Forensics Tool *April 2026*

Personal Open-Source Project github.com/arvdch/hexforge

- Designed and built a Python-based binary forensics tool for CTF challenges and real-world file analysis
- Implemented file signature detection, metadata extraction, steganography detection, and embedded file carving
- Automated file scanning workflows previously requiring multiple manual tools, improving analysis speed and accuracy
- Published detailed technical writeup on security blog documenting architecture, usage, and forensic methodology

SOC Home Lab — SIEM and Log Management with Splunk *July 2025*

Academic Team Project (JNTUH) Hyderabad, India

- Architected and deployed a Security Operations Center (SOC) lab environment simulating enterprise detection capabilities
- Configured Splunk SIEM for real-time log ingestion, event correlation, alerting, and custom dashboard creation
- Designed log management pipelines and detection rules for identifying common attack patterns and anomalies
- Documented full lab setup, architecture diagrams, and detection use-cases on personal security research blog

CERTIFICATIONS & SECURITY ACTIVITIES

CTF Competitor — TryHackMe & HackTheBox *2023 – Present*

Platforms: TryHackMe, HackTheBox

- Actively compete in Capture The Flag (CTF) challenges focused on digital forensics, reverse engineering, web exploitation, and privilege escalation
- Authored technical CTF writeup for MYTHX: AN ENDGAME PROTOCOL with detailed attack chain analysis and methodology
- Applied hands-on skills including binary analysis, network traffic analysis, malware analysis, and steganography

Cybersecurity Research Blog *April 2025 – Present*

arvdch.github.io

- Maintain a public security blog with technical writeups on CTF solutions, tool development, and home lab projects
- Topics include blue team detection, SIEM operations, digital forensics, penetration testing, and Python security tooling
- Demonstrates ongoing self-development, technical communication skills, and commitment to the security community

TECHNICAL SKILLS

Penetration Testing Tools: Burp Suite, Nmap, sqlmap, ffuf, Hydra, John the Ripper, Enum4linux, Metasploit, theHarvester, WhatWeb

SIEM & SOC: Splunk, log ingestion, event correlation, alert tuning, custom dashboards, log management pipelines

Digital Forensics: File signature analysis, metadata extraction, steganography detection, file carving, Binwalk, Volatility

Network Security: Wireshark, packet analysis, TCP/IP, SMB, FTP, SSH enumeration, IDS/IPS

Programming & Scripting: Python (security tool development), Bash scripting, curl

Operating Systems: Arch Linux, Kali Linux, Ubuntu, Windows

Security Concepts: Vulnerability assessment, privilege escalation, post-exploitation, reconnaissance, threat detection, incident response

Platforms & Tools: TryHackMe, HackTheBox, VulnHub, GitHub, CTF lab environments

PROFILES & ONLINE PRESENCE

LinkedIn: https://linkedin.com/in/aravind-chinthakindi

GitHub: https://github.com/arvdch

Security Blog: https://arvdch.github.io

HEXFORGE Project: https://github.com/arvdch/hexforge