ARAVIND CHINTHAKINDI

Detection Engineering • SIEM & SOC Operations • Cloud Security (Foundations)

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

PROFESSIONAL SUMMARY

Cybersecurity undergraduate specializing in detection engineering and SIEM operations, with hands-on Splunk/SPL experience building correlation searches and alerts that detect brute-force attacks, web enumeration, and host-based threats via Sysmon. Completed a penetration testing internship covering web application security, network enumeration, and incident response documentation, gaining attacker-technique knowledge that directly strengthens detection logic. Developing foundational cloud security skills through advanced coursework in IAM, cloud architecture, and the shared responsibility model. Active CTF competitor ranked in the top 15% on TryHackMe. Seeking an entry-level role in detection engineering, SOC analysis, or cloud security.

TECHNICAL SKILLS

SIEM & Detection Engineering: Splunk, SPL (Search Processing Language), correlation searches, alert tuning, custom dashboards, log management pipelines

Security Monitoring & Log Analysis: Sysmon event analysis, Windows/Linux log analysis, authentication anomaly detection, web log analysis (HTTP status codes & methods), Wireshark/packet analysis

Cloud Security (Foundations): IAM concepts, shared responsibility model, cloud architecture security principles (coursework)

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

Offensive Security: Burp Suite, Nmap, Metasploit, sqlmap, Hydra, John the Ripper

Programming & Operating Systems: Python, Bash | Linux (Kali, Ubuntu, Arch), Windows

PROFESSIONAL EXPERIENCE

Cybersecurity Intern **June 2025**

JD Infotech *Hyderabad, India*

- Conducted vulnerability assessments on VulnHub web apps, exploiting XSS, SQLi, and IDOR vulnerabilities using Burp Suite, sqlmap, and ffuf
- Performed reconnaissance and information gathering using Nmap, theHarvester, dig, and WhatWeb to map attack surfaces
- Executed SMB, FTP, and SSH service enumeration and brute-force attacks using Hydra, John the Ripper, and Enum4linux
- Practiced privilege escalation techniques and post-exploitation analysis on Linux target machines
- Analyzed HTTP header security misconfigurations and documented actionable remediation recommendations
- Produced professional vulnerability reports with risk ratings, technical findings, and remediation steps for stakeholders

PROJECTS

SOC Home Lab — SIEM & Detection Engineering with Splunk **July 2025**

Academic Team Project, JNTUH *Hyderabad, India*

- Built Splunk correlation searches on Apache access logs; detected 8 authentication failures across 2 source IPs indicating credential-based attacks
- Developed SPL detection queries that surfaced ~100 HTTP 404 errors from 2 IPs, flagging active web enumeration and directory scanning
- Monitored traffic baselines peaking at 1,250 requests/minute using time-series panels to detect sudden volume anomalies
- Designed a 9-panel custom Splunk dashboard covering auth failures, unauthorized access, suspicious HTTP methods, error levels, and URI analysis
- Ingested Sysmon event logs for host-based detection of anomalous process creation, execution patterns, and lateral movement indicators

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 that previously required multiple manual tools, improving analysis speed and accuracy
- Published a detailed technical writeup documenting architecture, usage, and forensic methodology

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
- Relevant coursework: Network Security, Ethical Hacking, Operating Systems, Cryptography, Cloud Security

SECURITY ACTIVITIES & ACHIEVEMENTS

CTF Competitor — TryHackMe & HackTheBox **2023 – Present**

- Ranked in the top 15% of TryHackMe users; actively compete in CTF challenges focused on digital forensics, reverse engineering, web exploitation, and privilege escalation
- Authored a technical CTF writeup for “MYTHX: An Endgame Protocol” with detailed attack chain analysis; applies hands-on skills across challenges including binary analysis, network traffic analysis, malware analysis, and steganography

Cybersecurity Research Blog **April 2025 – Present**

arvdch.github.io

- Maintain a public security blog covering CTF write-ups, detection engineering, SIEM operations, and home lab projects