Anandhu B

✉ **anandhub75@gmail.com** | ☎ **+91-9444679569** | 📍 **Chennai, India** | in LinkedIn

Professional Summary

Certified Ethical Hacker (CEH) and Certified Penetration Testing Professional (C|PENT) with hands-on experience in SOC operations, threat detection, incident response, and vulnerability management. Proficient in tools such as Elastic (ELK), Splunk, Wireshark, Nessus, Fortinet, and Sophos. Skilled in log analysis, forensics, and rule tuning, with a strong analytical mindset and a passion for staying ahead of evolving cyber threats.

Skills

Cybersecurity: Threat Hunting, Incident Response, Vulnerability Management, Risk Assessment, Penetration Testing
Tools & Technologies: Splunk, Wireshark, Nessus, Burp Suite, Nmap, Metasploit, Sqlmap, Accunetix, Hydra, Gobuster, Wfuzz, ExtraHop RevealX NDR, Sophos XDR.
Frameworks & Standards: MITRE ATT&CK, OWASP Top 10, ISO 27001
Other Skills: SIEM, IDS/IPS, Linux Security, Privilege Escalation, Firewalls

Experience

Trainee – Cybersecurity
Futurenet Technologies | Sept 2025 – Present

- Conducting log analysis, alert triage, and investigations using the Elastic (ELK) Stack.
- Managing log onboarding and ingestion from Windows, Linux, Firewall, and AV sources.
- Deploying and maintaining Elastic Agents and Fleet Servers across client systems.
- Performing packet capture, memory analysis, and threat correlation during incidents.
- Creating and tuning KQL/EQL detection rules to enhance alert accuracy.
- Conducting vulnerability scans with Nessus and Holm Security, validating findings, and implementing fixes through patching and configuration hardening.
- Supporting Active Directory and Google Workspace security operations.
- Assisting in incident containment, eradication, and documentation.
- Preparing SOC reports on incidents, trends, and key observations.

Security Analyst Trainee
Tracelay Networks | Bangalore, India | Feb 2025 – Aug 2025

- Conducted a thorough analysis using cybersecurity tools, including Microtrend Vision One XDR, ExtraHop RevealX NDR, Sophos XDR, IBM X-Force, and Cybereason EDR.
- Conducted research on different types of Incident Response solutions.
- Conducted research on different types of malware.

Cyber Security Analyst Intern
Cyber Secured India | Mumbai, India | Aug 2024 - Dec 2024

- Conducted vulnerability assessments and penetration testing on web applications and networks.
- Utilized tools like Wireshark, Metasploit, Splunk, and Burp Suite for security assessments.
- Developed detailed incident reports and remediation plans for identified vulnerabilities.

- Participated in weekly knowledge-sharing sessions to enhance team understanding of evolving cyber threats.

Graduate Trainee
CMA-CGM | Chennai, India | Mar 2023 - Nov 2023

- Gained experience in shipping and logistics security.
- Managed and streamlined sales, service, and marketing activities in Salesforce.
- Ensured compliance with cybersecurity best practices in logistic operations.

Projects

Aero-Online Book Selling Platform

- Developed a secure e-commerce platform for book sales.
- Won an intercollege competition for innovation in security measures.

Education

B.Tech in Information Technology Vel Tech High Tech Engineering College | 2018 - 2022 | **CGPA: 8.2**

Certifications

- **Certified Ethical Hacker (CEH)** | EC-Council | Mar 2021 - Mar 2024
- **Certified Penetration Testing Professional (C|PENT)** | EC-Council | Jul 2024 - No Expiry

Achievements

- **IOT Hackathon - World Record Achiever** | Inspireo Tech & Microsoft Research (Mar 2021)
- **Editor / Publisher - College Cyber Security Magazine** (2020 - 2021)
- **DEFCON CTF 2022 Participant** (Nov 2022)

Languages

- **English:** Native or Bilingual Proficiency
- **Hindi:** Full Professional Proficiency
- **Malayalam:** Native or Bilingual Proficiency
- **Tamil:** Full Professional Proficiency

Tools & Software

Nmap, Sqlmap, Wireshark, Burp Suite, Accunetix, GoBuster, Wfuzz, Nuclei, Curl, Hydra, Splunk