U.S.Puri Jagannadh

jagannadhulapalli@gmail.com | +91 9133014476 | Tapeswaram, Andhra Pradesh, India | Linkedin

Profile Summary

Motivated Cybersecurity Trainee with a strong foundation in networking and Operating systems, skilled in Ethical Hacking, vulnerability scanning and Network Security. Committed to strengthening organizational security and contributing to a safe digital environment.

Education

Bachelor of Technology in Electronics and Communication Engineering Sep 2021 – May 2025
Godavari Institute of Engineering & Technology, Rajahmundry, AP, India

Skills

- **Languages:** Basics of Python
- **Cybersecurity Tools:** OpenVAS, Splunk, Wireshark, Nmap, Acunetix 11, Virus Total, Nessus, Wazuh
- **Networking:** OSI Model, TCP/IP, DNS, Firewall, VPN
- **OS:** Kali Linux, Windows 11
- **Soft Skills:** Problem Solving, Team Collaboration, Communication, Documentation & Reporting

Work Experience

Cyber Security Analyst Intern Oct 2025 – Present
Company: Digit-Defense, Madhapur, Hyderabad

- Conducted threat analysis and security monitoring using SIEM tools (Splunk, Wazuh) to detect anomalies, reduce false positives, and support incident response efforts.
- Performed vulnerability assessments and risk prioritization with OpenVAS and Qualys, recommending remediation strategies that improved overall system security posture.
- Enhanced incident investigation workflow, cutting resolution delays by 18% through optimized log analysis.
- Collaborated with IT teams to implement access controls, patch management, and endpoint security measures, reducing exposure to malware and unauthorized access attempts.

Projects

Vulnerability Assessment & Penetration Testing (VAPT) on a Web Application Aug 2025 – Sep 2025

- Conducted end-to-end security assessment on a demo application, uncovering 18+ vulnerabilities with CVSS scoring. Executed port scanning using Nmap, achieving 95% accuracy in service detection across multiple endpoints.
- Documented findings in a professional VAPT report, boosting remediation speed by 25% for developers.
- Correlated results with CVSS metrics, enhancing vulnerability prioritization efficiency by 40%.
- Strengthened security posture by recommending patch strategies that decreased threat surface by 20%.

Centralized SIEM Threat Detection & Response Using Splunk and Wireshark Sep 2025 – Oct 2025

- Established SIEM environment using Splunk, enabling centralized monitoring of 50K+ log entries daily. Simulated cyber-attacks via Kali Linux (DoS, phishing) validating SOC response efficiency by 35%.
- Captured malicious packets with Wireshark, improving incident detection accuracy by 28%. Applied Maltego for threat intelligence, mapping 25+ suspicious domains and attacker IPs.
- Detected repeated login failures and port scans, enabling responsive defense against credential attacks. Produced real-time dashboard with 100% uptime, ensuring continuous security visibility.

Key Achievements

- Detected 15 high-risk vulnerabilities through advanced threat analysis, strengthening overall system defense.
- Monitored network traffic, reducing incident response time by 30% with early detection strategies.
- Investigated suspicious domains and IPs, improving accuracy in threat detection and prevention.

Certifications

- Certified Cyber Security Professional Certification by IIFIS.
- Network Defense Essentials by EC-Council.
- Comptia Security+ Certification by Comptia.