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

Network Vulnerability Assessment and Reporting Aug 2025 – Sep 2025

Tools: OpenVAS, Nessus, Nmap, Angry IP Scanner, Wireshark **Environment:** Kali Linux, Windows 11

- Conducted a comprehensive vulnerability assessment on a simulated local network using OpenVAS and Nessus.
- Utilized Nmap and Angry IP Scanner to identify live hosts, open ports, and network services.
- Captured and analyzed network traffic using Wireshark to detect suspicious packets and potential intrusion attempts.
- Generated risk-based vulnerability reports, prioritized findings based on CVSS scores, and suggested mitigation strategies.
- Improved overall network security posture by patching identified vulnerabilities and re-validating results.

Centralized SIEM Monitoring ,Threat Detection & Response Sep 2025 – Oct 2025

Tools: Splunk, Wazuh, IBM QRadar, VirusTotal **Environment:** Kali Linux, Windows 11

- Set up a SIEM environment using Wazuh integrated with Splunk for centralized log collection and analysis.
- Monitored system and network logs to identify potential security incidents such as brute-force attempts and malware activity.
- Used IBM QRadar to simulate incident correlation and create custom alerts based on event severity.
- Investigated suspicious files and URLs through VirusTotal for malware verification.
- Documented incident handling steps, response procedures, and lessons learned in a security report.

Certifications

- Currently Pursuing Comptia Security+ Certification by Comptia.
- Network Defense Essentials by EC-Council.
- Certified CyberSecurity Professional Certification by IIFIS.