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 SIEM, Vulnerability Assessment, Identity and Access Management and basics of GRC. Committed to strengthening organizational security and contributing to a safe environment.

EDUCATION

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

SKILLS

- **Vulnerability Scanning & Assessment:** OpenVAS, Tenable Nessus, Acunetix 11, Rapid7 Nexpose
- **Network Analysis & Monitoring:** Wireshark, Nmap, Angry IP Scanner
- **SIEM Monitoring & Detection:** Splunk, IBM Qradar, Metadefender, Wazuh
- **Networking:** OSI Model, TCP/IP Protocols, DHCP, DNS, Firewalls, VPN, Subnet
- **IAM & GRC Tools:** Keycloak, Microsoft Azure AD, Google Cloud IAM, ZenGRC, Google SpreadSheets
- **Other tools:** Google Cloud Platform, John The Ripper, Virus Total, Phish Tool, Microsoft office 365
- **Soft Skills:** 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 Rapid7 Nexpose, recommending remediation strategies that improved overall system security posture.
- 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 , Reporting & Mitigation 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.
- 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.

CERTIFICATIONS

- Currently Pursuing Comptia Security+ Certification by Comptia.
- Certified Cyber Security Professional Certification by IIFIS.
- Progressing SOC L1 Path in Try Hack Me.