Jagadeesh Varma Kakarlapudi

+1(832)9082143 | jagadeeshvarmasce@gmail.com | LinkedIn | GitHub | Portfolio

PROFESSIONAL SUMMARY

Cybersecurity graduate student with hands-on experience in intrusion detection, SIEM tools, and threat analysis. Skilled in Snort, ELK Stack, Splunk, and Nessus, with a solid foundation in SOC workflows, NIST standards, and incident response. Eager to contribute to a security operations team.

EDUCATION

University of Houston, Houston, TX. *August 2023 - May 2025*

Masters in Cybersecurity *GPA - 3.90*

Data & network security, Data science for Cybersecurity, Design data analytic solutions, cryptography, SOC, and advanced SOC Analysis, Risk management.

GVP College of Engineering, India. *August 2019 - July 2023*

Bachelor of Technology Electronics and Communication Engineering *GPA - 3.20*

EXPERIENCE

Research Assistant: *GITAM (Deemed to be University), Visakhapatnam, India* *November 2022 - August 2023*

- Configured and secured Linux-based lab systems, reducing system vulnerabilities by 30% and maintaining a secure testing environment compliant with institutional policies.
- Assisted in analyzing network traffic patterns and researching detection techniques using open-source tools.
- Developed and standardized threat analysis workflows, reducing onboarding time by 25% and enhancing audit readiness.

Cybersecurity Intern: *AICTE (Supported by PALO ALTO)* *March 2022 - May 2022*

- Participated in hands-on security labs involving network defense, vulnerability scanning, and threat intelligence, which enhanced the organization's ability to identify and mitigate potential threats.
- Collaborated with a team to simulate cyber-attack scenarios and develop incident response strategies. Created reports on vulnerabilities and provided recommendations to mitigate identified threats.

PROJECTS

Log Analysis, Intrusion Detection & Prevention system with Snort:

- Configured and deployed Snort IDS in multiple operational modes, engineering custom detection rules to identify FTP, SMTP, DNS, Telnet, and HTTP traffic patterns with 100% accuracy across 200+ packet samples
- Implemented real-time traffic monitoring and alert generation system, successfully detecting 26 connection attempts while optimizing rule specificity to reduce false positives
- Integrated Snort with Wireshark for packet-level analysis, validating detection accuracy through controlled SSH and web traffic, enhancing forensic and visibility capabilities.
- **Technologies:** Snort IDS, Ubuntu Linux, Wireshark, Apache2, SSH

ML-Based Intrusion Detection using UNSW-NB15 Dataset (Coursework Project)

- Developed a network intrusion detection system using the UNSW-NB15 dataset and machine learning models (Random Forest, SVM, Logistic Regression). Implemented optimized feature selection improving threat detection accuracy by 15%.
- Built a Python-based command-line tool for anomaly detection with CSV export, and generated HTML reports featuring visualizations and statistical summaries for streamlined threat analysis.
- **Technologies:** Python, Scikit-learn, Pandas, NumPy, Matplotlib/Seaborn, HTML/CSS, CSV, Random Forest, SVM, Logistic Regression, UNSW-NB15 Dataset

Firewall Security Configuration and Testing:

- Designed and tested host-based firewall configurations in a Kali-Ubuntu virtual lab using UFW, iptables, Nmap, and Wireshark to simulate and analyze real-world traffic filtering, port control, and protocol behavior.
- **Technologies:** Ubuntu, Kali Linux, UFW, iptables, Nmap, Wireshark

SKILLS

SIEM & Log Management: Splunk (Hands-on), ELK Stack (Elasticsearch, Logstash, Kibana), Azure Sentinel.

IDS/IPS & Monitoring tools: Snort, Suricata, Zeek, Security Onion, Wireshark, TCPdump.

Vulnerability Scanning & Assessment: Nessus, OpenVAS, Nmap, Burp Suite, Nikto, Metasploit.

Programming & Operating Systems: Python, C, HTML, Bash, Ubuntu, Kali Linux, CentOS, Windows, MacOS.

Security Frameworks & Compliance: ISO27001, NIST 800-53, NIST 800-61, NIST Risk Management(RMF), HIPAA, FISMA.

Cloud & Network Security: Microsoft Azure, VPN, VLAN, IPsec.

Soft Skills: Analytical Thinking, Attention to Detail, Team Collaboration, Communication.

Productivity & Documentation: Microsoft 365, Google Workspace, Technical Writing & Reporting.

CERTIFICATIONS

EC-Council Certified Ethical Hacker CEHv11

Palo Alto Networks Cybersecurity Professional

SIEM Splunk Hands-On Guide

Google Cybersecurity Professional

IBM Cybersecurity Analyst Professional

Microsoft MTA: Security Fundamentals