Jagadeesh Varma Kakarlapudi

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

PROFESSIONAL SUMMARY

Cybersecurity professional with a Master's degree and hands-on experience in intrusion detection, threat analysis, and vulnerability assessments. Skilled in Snort, ELK Stack, Nessus, and Python, with a strong foundation in SIEM, incident response, and security frameworks. Committed to continuous improvement, clear communication, and delivering effective security solutions.

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 *Nov 2022 – Aug 2023*

- Configured and maintained secure Linux-based lab environments, supporting system setup, troubleshooting, and research-driven cybersecurity operations.
- Researched emerging cybersecurity technologies and documented technical procedures to support project continuity and cross-team collaboration

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

- Participated in hands-on security labs focused on 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 (7 FTP, 19 SMTP) 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

Cyber Threat Analyst Project - 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

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

Vulnerability Assessment & Penetration Testing: Nessus, Nikto, Wireshark, Burp Suite, Metasploit, TCP dump, Nmap, OpenVAS.

IDS/IPS & Monitoring tools: Snort, Suricata, Zeek, Security Onion, ElastAlert, Event Viewer.

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

Cloud & Visualization: Microsoft Azure, Docker, Kubernetes, VPN, VLAN, IPsec, PuTTY.

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

Productivity & Documentation: Microsoft 365, Google Workspace(Sheets, Docs), WinRAR, 7Zip, Technical Documentation.

Soft Skills: Attention to detail, Analytical Thinking, Team Coordination, Communication, Adaptability.

CERTIFICATIONS

EC-Council Certified Ethical Hacker CEHv11

Google Cybersecurity Professional

Palo Alto Networks Cybersecurity Professional

IBM Cybersecurity Analyst Professional

SIEM Splunk Hands-On Guide

Microsoft MTA: Security Fundamentals