GUBBALA JAYA KUMAR

jayak0776@gmail.com | +91 8919753805 | Rajahmundry India

GITHUB | LINKDIN | PORTFOLIO

LEETCODE | HACKER RANK

EDUCATION

PRAGATI ENGINEERING COLLEGE | B.Tech |Information Technology — **SEP 2022 - CURRENT**

CGPA: 7.9/10 — SURAMAPALEM, AP

B.V.C COLLEGE OF EINGINEERING | Diploma | Mechanical Engineering — **AUG 2019 – MAY 2022**

PERCENTAGE: 89% — Rajahmundry, AP

PROFESSIONAL SUMMARY

- Cybersecurity enthusiast with hands-on experience in real-time threat detection using Snort, Splunk, and Wireshark.
- Trained as an SOC Analyst under Deloitte's cybersecurity training program at SDI Bhubaneswar (via I Aspire Mind Foundation).
- Proficient in monitoring, analyzing, and correlating logs for suspicious activity across Linux and Windows environments.
- Skilled in detecting brute-force, port scanning, and MITM attacks using open-source IDS tools.
- Knowledgeable in network protocols, TCP/IP, ARP spoofing, and OSI model for effective packet inspection and traffic analysis.
- Familiar with Splunk dashboards and alerts; currently building skills in correlation searches.
- Good understanding of cybersecurity fundamentals, including incident response, malware behavior, and endpoint monitoring.
- Technical background in full-stack development and cloud platforms (AWS), supporting a holistic view of IT infrastructure security.
- Eager to contribute to a SOC team and grow in the field of cyber threat detection and defense.

SKILLS

- **CYBERSECUIRTY SKILLS:**
  - Security Information and Event Management (SIEM): Splunk and Sentinal
  - Intrusion Detection & Prevention Systems (IDS/IPS): Snort, Suricata
  - Security Operations Center (SOC) Monitoring
  - Network Security & Packet Analysis: Wireshark
  - Log Analysis
  - Firewall Configuration & Management
  - Penetration Testing (Basic): Metasploit, Nmap
  - Endpoint Security: Velociraptor
  - MITM & Spoofing Attack Analysis: Ettercap, arpspoof
- **TECHNICAL SKILLS:**
  - Operating Systems: Linux (Ubuntu/Kali), Windows
  - Programming/Scripting: Python, Java
  - Cloud Security Basics: AWS IAM, EC2 Security
  - Web Development: HTML, CSS, JS, React, Tailwind CSS, Spring Boot
  - ServiceNow: Instance, Tables, Fields, Records, Scripting (UI and Data Polices, Business rules, UI Actions, Client Scripts), Service Catalog and Others

CERTIFICATIONS AND CERTIFICATES

- **SERVICENOW |** Certified System Administrator
- **SERVICENOW |** Certified Application Developer
- **AMAZON WEB SERVICE |** Certified Cloud Practitioner.
- **CYBERSECURITY FUNDAMENTALS |** Cisco Cybersecurity Certificate | AICTE Certificate

- **PYTHON | WEB DEVELOPMENT|** Hacker Rank and Infosys Springboard, Coincent and Internshala | Simplilearn

PROJECTS

1. Real-Time SSH Brute-Force Attack Detection using Snort & Splunk

- Configured Snort with custom rules to detect repeated SSH login attempts.
- Integrated Snort alerts into Splunk for real-time monitoring and alert generation.
- Built basic dashboards in Splunk to visualize and track attack patterns.

2. Nmap Port Scan Detection using Snort and Splunk

- Used Snort's preprocessor and rules to detect SYN scans and TCP scans from Nmap.
- Parsed alerts through Splunk and created dashboards for visual analysis of scans.
- Demonstrated proactive threat identification using open-source tools.

3. ARP Spoofing and MITM Attack Demonstration

- Executed ARP spoofing attacks using arpspoof and GUI-based MITM with Ettercap.
- Captured traffic using Wireshark to inspect credential leaks and session hijacks.
- Documented the entire attack lifecycle and mitigation strategies.

4. Basic Threat Detection Using Splunk from System Logs

- Collected Linux system logs (auth.log, syslog) using Splunk Universal Forwarder.
- Created correlation searches to flag unusual user behavior and failed login attempts.
- Demonstrated log ingestion, filtering, and alert creation.

5. Web Development Projects | Dental Management System | Portfolio | Mini projects

INTERNSHIP

SOC Analyst Training | SDI Bhubaneswar (Deloitte) | I Aspire Mind Foundation

Cybersecurity-specific training aligned with real-world SOC environments

- Learned fundamentals of Security Operations Center (SOC) workflows.
- Practiced log analysis, incident triage, and basic alert investigation.
- Hands-on with tools like Snort and Splunk for intrusion detection and monitoring.

Introduction to Networking for Cyber Professionals | Zscaler Academy - Virtual Internship

Focused training on core networking concepts relevant to cybersecurity

- Gained foundational understanding of networking protocols (TCP/IP, DNS, HTTP/S).
- Explored real-world scenarios involving secure web gateways and network segmentation.
- Learned how modern enterprise networks are secured using zero-trust principles.

AWS Cloud Virtual Internship | AICTE - EDUSKILLS

Practical exposure to cloud infrastructure and basic security configurations

- Deployed and managed virtual servers using Amazon EC2, and configured storage with AWS S3.
- Explored IAM roles, policies, and access control for user authentication and permission management.
- Understood shared responsibility model, encryption options, and cloud monitoring via CloudWatch.
- Developed awareness of cloud-based attack surfaces and the importance of cloud security best practices.

HOBBIES

Playing and Watching Cricket | Coding and Programming | Gaming | Watching Movies & Web Series