KRANTHI KUMAR MANDA

(813) 318-1595 | Tampa, Florida | kranthikumar.manda@outlook.com | https://linkedin.com/in/kranthi-kumar-manda | My blog

EDUCATION

The University of Tampa **May 2024**
Master of Science: Cybersecurity CGPA: 3.8

Rajiv Gandhi University of Knowledge Technologies **July 2021**
Bachelor of Technology: Computer Science CGPA: 3.42

WORK EXPERIENCE

Resilience Inc **Tampa, USA**
Cyber Security Analyst **June 2024–Present**

- Performed detailed vulnerability assessments using Nuclei, Burp Suite, OWASP ZAP, Nikto, and Nessus, identifying critical security risks and enhancing overall Application Security.
- Managed and prioritized vulnerabilities using Nessus, driving remediation efforts to mitigate high-risk threats and reduce the organization's attack surface as part of Vulnerability Management.
- Conducted in-depth research on XSS, security headers, and application entry points, contributing to improved Threat Analysis and Compliance with industry standards.
- Utilized tools like Nikto for security assessments and attended sessions on EDR (Endpoint Detection and Response) tools to integrate advanced detection and response capabilities into the Resilience Security Operations.
- Conducted comprehensive vulnerability assessments using Nuclei, Burp Suite, OWASP ZAP, and Nessus, identifying and mitigating security risks.

Infosys Ltd **Hyderabad, India**
Automation Test Engineer (QA) **Aug 2021–Oct 2022**

- Developing automated test scripts using programming languages such as Java (Selenium Java).
- Develop and maintain automated testing frameworks that can be used across different applications.
- Planning and executing automated tests to ensure that the software products meet the desired quality standards.
- Analyze the test results and report the issues to the development team.
- Document the testing process, including test plans, test cases, and test scripts.
- Work with the DevOps team to integrate automated testing into the continuous integration and delivery process.

Meebuddy Pvt.Ltd **Nuzvid, India**
Penetration Tester Internship **Aug 2019–Aug 2020**

- Conducted penetration testing on Meebuddy's infrastructure and performed vulnerability assessments on web application and servers, identifying and remediating 7 critical vulnerabilities to enhance overall security posture.
- Verified SSL authentication for secure application development on Web Servers, ensuring robust encryption standards and mitigating the risk of data breaches.
- Analyzed systems for potential vulnerabilities arising from improper configuration and operational errors, resulting in the identification and remediation of 4 vulnerabilities.
- Executed white/gray box penetration testing on applications using Kali Linux, uncovering, and addressing 3 high-risk vulnerabilities to fortify data protection.
- Utilized NMAP to port scan servers and closed unnecessary ports, reducing the attack surface and minimizing the risk of unauthorized access and resolving 5 network security vulnerabilities.

CERTIFICATIONS

- Certified Ethical Hacker (CEH Master)
- AWS Certified Cloud Practitioner
- CompTIA Security+
- Qualys Certified Specialist (VMDR)

SKILLS

- Proficient in **network traffic analysis** using **Wireshark and tcpdump**.
- Experienced in **vulnerability assessment and management** using **Qualys**.
- Skilled in **malware analysis**, identity and access management (**IAM**), and Web application security (**OWASP**).
- Hands-on experience with SIEM platforms **splunk** and IBM Qradar, IDS/IPS logs for **log analysis**.
- Familiar with the **MITRE ATTACK** framework for threat detection and response.
- Knowledgeable in networking concepts(OSI Model) and proficient in penetration testing methodologies and tools.
- Utilized **JIRA** as a ticketing tool for incident management and tracking.

PROJECTS

Vulnerability management with Qualys (Project Link: check here)

- Installed and configured Qualys to perform vulnerability scans on Windows 10 host.
- Implemented vulnerability management functions on home lab networks:
  - Discover, Prioritize, Assess, Report, Remediate and verify.
- Conducted vulnerability assessments and remediated them accordingly.

Malware traffic analysis using Wireshark (Project Link: check here)

- Conducted an in-depth investigation into network traffic patterns, leading to the detection and analysis of a sophisticated Trojan attack originating from a Russian server.
- Leveraged Wireshark for network traffic analysis and log investigation, demonstrating advanced skills with tools.
- Advised on and implemented a comprehensive defense strategy, emphasizing intrusion and endpoint security measures to safeguard against cyber threats.

Cyber Competition - Blue team defense (Project Link: check here)

- Participated in a Capture the Flag competition during a Penetration Testing course in master's program.
- Implemented and managed firewall rules to enhance network security and control access to hosts.
- Strengthened security by blocking SSH access to hosts, reducing attack surface and mitigating potential risks.
- Closed all unnecessary ports on systems to minimize exposure and prevent unauthorized access.
- Improved system security by identifying and removing unnecessary user accounts with weak passwords, reducing the risk of unauthorized access and potential breaches.
- Developed comprehensive understanding of defensive strategies and tactics in a cybersecurity environment.

ACHIEVEMENTS

- Secured 2nd position at Spartan CTF Winner, demonstrating proficiency in cybersecurity tactics and strategies, EC-Council, December 2023.
- Achieved 1st position at OWASP Q2 Chapter CTF Winner, showcasing expertise in web application security through offensive and defensive cybersecurity techniques, OWASP Tampa, April 2023.
- Actively participated in numerous Capture the Flag (CTF) competitions and consistently excelled in challenges hosted by platforms such as HackTheBox and TryHackMe.