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

Infosys Ltd **Hyderabad, India**
Security Operations Center Analyst (SOC) **Aug 2021–Oct 2022**

- Monitored SIEM (Splunk enterprise security, IBM Qradar), Palo Alto firewalls and IDS/IPS logs, detecting enterprise threats and initiating investigations, resulting in the identification, and triaging of incidents with a 30% increase in threat identification efficiency.
- Utilized Microsoft Defender for endpoint detection and response (EDR), leveraging advanced threat intelligence and behavioral analytics to swiftly detect, investigate, and remediate security incidents, enhancing overall endpoint security posture.
- Analyzed phishing emails identified through SIEM alerts and Proofpoint sandbox to assess potential threats and identify indicators of compromise (IOCs).
- Collaborated with security incident response teams and conducted root cause analyses and developed governance documents to educate clients on proactive security measures, mitigating the impact of security incidents and enabling preventive actions.
- Managed JIRA tickets and documentation, ensuring accurate and thorough records of incidents, investigations, and remediation efforts.

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 financial data protection.
- Utilized NMAP to port scan servers and closed unnecessary ports, reducing the attack surface and minimizing the risk of unauthorized access.
- Performed live packet data capture with Wireshark to examine security gaps, identifying 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 and Brim for network traffic analysis and log investigation, demonstrating advanced skills in cybersecurity 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 (CTF) cyber-competition during a Penetration Testing course in a cybersecurity 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 competitive 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.
- Coordinated and conducted 5 engaging security awareness sessions for approximately 100 employees as a part of Infosys cybersecurity training program in 2022.
- Actively participated in numerous Capture the Flag (CTF) competitions and consistently excelled in challenges hosted by platforms such as HackTheBox and TryHackMe.