KAKARLAMUDI BABI

+91-8106818307
email –kakarlamudibabi1234@gmail.com
LinkedIn -www.linkedin.com/in/babi-kakarlamudi-038649268

SUMMARY

I aspire to excel professionally and broaden my expertise by collaborating with a dynamic and motivated team dedicated to the organization's growth. I am eager to leverage my skills and knowledge effectively within any organizational context.

PRIMARY SKILLS

- Proficient in leveraging Open-Source Intelligence (OSINT) frameworks and various intelligence gathering tools to collect and analyze data from publicly available sources for enhanced situational awareness and threat hunting.
- Solid understanding of networking principles, including the OSI model, TCP/IP protocols, IDS/IPS concepts subnetting, and network infrastructure, which are essential for identifying and mitigating security threats.
- Expertise in applying the Cyber Kill Chain methodology to understand and disrupt the stages of cyber-attacks, from reconnaissance to exfiltration, thereby enhancing defense strategies and incident response.
- Skilled in utilizing the MITRE ATT&CK framework to map adversarial tactics, techniques, and procedures (TTPs), providing a comprehensive approach to threat intelligence and defensive measures.
- Experienced in conducting thorough vulnerability assessments, identifying security weaknesses, and implementing effective management strategies to mitigate risks and improve overall security posture.
- Proficient in performing network and web application penetration testing to identify and exploit vulnerabilities, simulating real-world attacks to enhance security measures and fortify defenses. (OWASP TOP 10)
- Strong understanding of the CIA triad (Confidentiality, Integrity, Availability) and the implementation of various information security controls to protect data and ensure its reliability and availability.
- Familiar with malware and phishing analysis techniques to detect, investigate, and mitigate cyber threats.
- Experienced in analyzing Windows events and logs to detect unusual activities, investigate security incidents, and ensure the integrity and security of systems and knowledge of security monitoring principles, log analysis.
- Comprehensive understanding of Security Operations Centers (SOC) and Security Information and Event Management (SIEM) systems, including their role in monitoring, detecting, and responding to security incidents.

TOOLS

- Scanning & Assessment: Nmap, Nessus, Metasploit Framework, Nikto, Owasp top10, SQL map.
- Monitoring & Analysis: Sysmon, Windows Event Viewer, Splunk, EDR.
- Malware Static Analysis: Exeinfo, PE Studio, Hash Calc, Resource Hacker.
- Malware Dynamic Analysis: Regshot, Process Monitor, Process Explorer, Wireshark.
- Phishing & Spam Analysis: Net craft, Phish Tank, Virus Total.
- Operating System: Parrot Security OS, Kali Linux, Windows.

CERTIFICATIONS

- Certified Ethical Hacker from EC-Council (ECC2976158430).
- VAPT & SOC at Hacking Trainer Institute Unit of Berry 9 It Services PVT LTD.

EDUCATION

- B. Tech in ECE From Rayalaseema university, Kurnool 2024