Bibungsarth Islary

Trivandrum, India
☎ +91-7002969318 ✉ bibungsarthislary@gmail.com
linkedin.com/in/bibungsarth github.com/Bibungsarth

Summary

I am a dedicated cybersecurity professional with a BSc in Computer Science, currently pursuing an MSc in Computer Science specializing in Cyber Security. I have a solid foundation in AI, Cyber Security, Ethical Hacking, and Penetration Testing, with hands-on experience in log analysis, malware detection, and security risk assessment. Proficient in utilizing industry-standard tools like Splunk and the ELK Stack for log management and threat analysis, I also excel in both dynamic and static analysis techniques to effectively identify and mitigate security threats. Skilled in vulnerability assessment and penetration testing using tools such as Burp Suite, OWASP ZAP, and advanced manual testing, I am prepared to contribute significantly in a client-facing role, enhancing security operations and driving proactive threat mitigation strategies.

Education

Digital University Kerala (formerly IIITMK) **Sept 2023 – Present**
MSc in Computer Science, Specialization in Cyber Security *Trivandrum, India*
Coursework includes: Computer Networks, Ethical Hacking, AI in Cyber Security, Malware Analysis

Lalit Chandra Bharali College **Aug 2020 – Jul 2023**
BSc in Computer Science *Guwahati, India CGPA: 7.5/10*
Core subjects: Data Structures, Operating Systems, DBMS, Computer System Architecture, Microprocessors

Technical Skills

Cybersecurity: Endpoint Protection, Malware Analysis, Vulnerability Assessment, Penetration Testing

Security Tools: Burp Suite, OWASP ZAP, Nessus, Nmap

Operating Systems: Windows, Linux (Ubuntu, Kali Linux)

Programming: Python, JavaScript, HTML/CSS, SQL

Soft Skills: Critical Thinking, Analytical Skills, Communication, Team Collaboration

Languages: English, Hindi, Assamese

Projects

Headless Browser Detection System **2024**
Developed a JavaScript-based system to detect headless browsers by analyzing browser behavior, identifying anomalies in rendering, screen dimensions, and timing discrepancies, thus strengthening web security.

Penetration Testing with Adversarial AI
Implemented a penetration testing framework using Adversarial Neural Networks (ANN). This project involved simulating attacks using adversarial AI to identify vulnerabilities and improve system defenses by iterating based on attack feedback. The framework utilized TensorFlow and adversarial datasets for robust threat simulation and mitigation.

Additional Information

Willing to work in rotational shifts to support 24/7 security operations. Continuously updating knowledge of evolving cybersecurity threats and techniques. Excellent written and verbal communication skills, well-suited for client-facing roles.