Arya Koner

+91 9732204312 arya.koner07@gmail.com Portfolio LinkedIn Medium

Education

MSC in Cyber Forensic & Cyber Security | Amity University Noida | Noida, UP | **8.41** **PURSUING**
BSC in Cyber Security |S K F G I| Kolkata, West Bengal | **8.86 CGPA** **2023**
12TH (Science) | WBSE | Kuchut P. C. Institution| Purba Bardhaman, West Bengal| **56 AGGREGATE** **2020**

Work Experience

Cyber Security Instructor – MRGS Info way **Feb 2025 – Apr 2025**
Remote- Kolkata, West Bengal

- Cyber Vahini Project – Training female students in cybersecurity fundamentals, VAPT and digital security.

VAPT Tester – Hacktify Cyber Security **Feb 2025 – Mar 2025**
Remote - Mumbi, India

- Performed advanced penetration testing on enterprise networks, leveraging Burp Suite, Nmap and Metasploit to identify critical vulnerabilities, exploit security gaps, and provide comprehensive risk mitigation strategies for enhanced cyber resilience.

Junior Cyber Crime Investigator – EDCI **Aug 2023 – Aug 2024**
Onsite - Kolkata, West Bengal

- Specialized in digital forensics, threat intelligence and incident response, utilizing Autopsy, FTK, EnCase and Wireshark for deep forensic analysis, cyber threat tracing and legal compliant cybercrime investigations.

VAPT Intern – Indian Cyber Security Solutions, West Bengal, India **Mar 2023 – Jun 2023**
On-site - Kolkata, West Bengal

- Conducting network vulnerability assessments and penetration testing using tools like Nmap, Nessus, Burp Suite and Metasploit to identify, exploit and mitigate security risks, ensuring robust cyber defence.

Projects

The Source-Translation Signature: A Multi-Layered Detection Framework for Nim-Compiled Malicious Binaries
In Progress

This research identifies unique compiler artifacts created when Nim code is translated to C/C++ and compiled, forming persistent fingerprints even after obfuscation. By analyzing these structural indicators, it proposes a lightweight, multi-layered framework for detecting Nim-compiled malicious binaries.

BLACKICE AI MCP Agents v1 In Progress

- Advanced AI-Powered Penetration Testing Framework with Autonomous Agents, Intelligent Decision Engine, and 150+ Security Tools

BADNET v1. *GitHub Link*

- Built an AI-powered cyber attack detection and prediction system with real-time monitoring, leveraging ML algorithms (DoS, Probe, R2L, U2R), automated training pipelines, evaluation frameworks, and intuitive CLI-based workflows.

TechnicalSkills

Core Skills: VAPT, Red Teaming, Malware Analysis, Malware Development, Reverse Engineering, Digital Forensics, Incident Response.

Tools & Tech: IDA Pro, Ghidra, Metasploit, Burp Suite, Splunk, Wireshark, Volatility, Python, C/C++, Bash, Linux, Nim

Certifications

CEH V13 AI (pursuing), CEH MASTER (pursuing), COMPTIYA SECURITY PLUS (pursuing), Cisco Cyber Threat Management, Google Cybersecurity,