

Logeshwar M

linkedin.com/in/logeshwar-m-84682a263 / logeshwar516@gmail.com / 9344540477

Summary

Cybersecurity Enthusiast with practical experience in threat detection, incident response, and malware analysis. Proficient in SIEM platforms including Wazuh, AWS cloud security services, and security automation through scripting. Demonstrated skills in penetration testing and capture-the-flag exercises using Hack The Box and TryHackMe platforms. Strong background in network security, digital forensics, and security frameworks including MITRE ATT&CK methodology. Seeking to contribute technical expertise in a Security Operations Center environment while advancing skills in 24/7 threat monitoring and response operations.

Experience

SonicWall

Malware researcher Intern, Bangalore

- Conducted comprehensive **static** and **dynamic** analysis of malware samples of 10+ including **PE** and **non-PE** file formats to identify malicious behaviors, persistence mechanisms, and network communication patterns
 - Performed reverse engineering using **OllyDbg** and **x64dbg** debuggers to trace program execution flows, analyze custom packing techniques, and examine Windows API call sequences
 - Analyzed portable executable file structures including **headers**, **sections**, Import Address Tables, and Export Address Tables to support malware classification and signature development
 - Developed Indicators of Compromise reports and **YARA** detection rules for threat intelligence teams, enhancing organizational malware detection capabilities and security posture
-

Technical Skills

- **SIEM & Detection:** Wazuh, incident response (triage, containment, RCA), threat hunting, log analysis
 - **Security Tools:** Nessus, Nmap, Wireshark, Burp Suite, Metasploit, Linux os
 - **Frameworks & Standards:** MITRE ATT&CK, OWASP Top 10, NIST, ISO 27001
 - **Programming & Scripting:** Python (automation), PowerShell (Windows security), Bash (Linux automation), JavaScript (web testing)
 - **Malware Analysis & Forensics:** Static & dynamic analysis, YARA rule creation, PE/Registry/MFT analysis, ATT&CK mapping
 - **Reverse Engineering:** OllyDbg, x64dbg, Ghidra, IDA free, API call tracing, custom packer analysis, PE internals (headers, sections, IAT/EAT), IOC/YARA development
 - **Networking:** TCP/IP, DNS, VPNs, firewalls, HTTPS/TLS, OSI model
 - **Cloud Platforms:** AWS (S3, EC2, Lambda, IAM, CloudWatch, DynamoDB), identity access management
 - **Offensive Security:** HackTheBox & TryHackMe – exploitation, privilege escalation, forensic labs, vulnerability scanning
-

projects

Malware Analysis and Detection System (2025)

Tech Stack: Python, React.js, FastAPI, Ubuntu, Windows Sandbox, YARA, AWS (DynamoDB & S3), Scikit-learn, Volatility3, Sysmon, Tshark

Focus Areas: Malware analysis (static & dynamic), threat detection, ML-based classification, cloud integration, and automated security pipelines

- Built a **web-based malware analysis platform** with **static & dynamic analysis** for .exe files.
- Integrated **YARA** rule for real-time threat detection.

- Designed **isolated VMs (Ubuntu & Windows)** for secure malware execution.
- Automated **signature database updates**, reducing detection time by **40%**.
- Built an **AI-powered malware detection system** integrating **Machine Learning models** for threat classification.
- Extracted **15+ memory forensic features** using **Volatility3** and trained ML models for **malware behavior analysis**.
- **GitHub link:** <https://github.com/7ogeshwar/MalwareAnalysis>

Steganography Tool (2023)

- Built a **Java-based steganography tool** for securely hiding text within images.
- Developed a **decoder algorithm** to extract hidden messages with **100% accuracy**.
- Improved encryption techniques, enhancing data security by **60%**.
- **GitHub link:** github.com/7ogeshwar/STEGNOGRAPHY

Serverless Website(2024)

- Developed a serverless website using **AWS S3** Utilized AWS S3 for static file storage and Lambda for backend logic.
- Created API endpoints with API Gateway for dynamic interactions.
- Managed data storage with DynamoDB for scalability and efficiency.
- Implemented a fully serverless architecture for cost-effective, scalable hosting

Education

MCA(master of computer application)

CEG Anna university, chennai

04/2025

With CGPA : 7.3

BCA(computer application)

Hindustan College of Arts & Science, chennai

05/2023

with CGPA : 8.5

Certificates

- (ISC2) in cc final assessment with 3 years valid **Relevant Skills:** Cybersecurity Fundamentals, ThreatDetection, Risk Management, Incident Response, Network Security
- **Cybersecurity Job Simulation – Mastercard (2025)** Conducted a **phishing email simulation** to assess security awareness. Analyzed phishing simulation results, identifying key **security gaps**.

Achievements

- **Proficiency Award:** Recognized for outstanding academic performance in BCA.
- **National Quiz Competition:** Achieved 2nd place in a National Symposium Computer Science Technical Quiz Competition at Vels Institute of Technology, Chennai, showcasing expertise in technical concepts and problem-solving skills.

Soft Skills

Problem-solving, Analytical Thinking, Collaboration, collaboration skills, communication skills, customer oriented, analytical