Muhil

Chennai, TN
+918754303593, muhilm6@gmail.com
LinkedIn, GitHub

Summary

Ambitious final-year Cybersecurity student with a strong foundation in security operations, threat analysis, and incident response. Certified in CompTIA Security+, Network+, and AWS CLF-C02. Ranked in the top 1% on TryHackMe (uid: lasthacker), demonstrating advanced hands-on skills in threat detection, log analysis, and vulnerability assessment. Eager to contribute to defensive security operations and continuous improvement as a Cybersecurity Analyst.

Practical Projects

- **Home Lab SIEM Implementation** – Set up a **Wazuh-based SIEM system** integrated with a Linux and Windows home lab. Configured log forwarding, built detection rules, and conducted real-time threat correlation and alerting.
- **SOC Operations with TryHackMe** – Analyzed phishing attacks, suspicious logs, and threat actor behavior using a simulated SOC environment. Practiced **incident response**, **alert triaging**, and **threat hunting.**
- **SOAR & EDR Integration Lab** – Built a lab integrating **Security Orchestration, Automation, and Response (SOAR)** tools with **Endpoint Detection and Response (EDR)** to simulate and analyze **advanced threat detection** and **automated incident response workflows**.
- **Cowrie Honeypot with Slack Alerts** – Deployed and customized a **Cowrie SSH honeypot** to collect **attacker data**, automated **Slack alerting**, and developed initial **incident response** procedures.
- **Safecode-scanner –** Created a **web-based tool** (Python/HTML) for **scanning codebases** to identify **common security issues and vulnerabilities**, demonstrating an understanding of **secure coding practices** and **vulnerability assessment**.

Publications

IEEE Conference Paper
“Evaluating and Exploiting Security Vulnerabilities in Large Language Models (LLMs) for Offensive Penetration Testing”
To be presented at IEEE ICCPCT 2025**, August 2025**

Skills & tools

Security Tools: Wireshark, Burp Suite, Metasploit, Nessus, Nmap, YARA, Wazuh
Programming Languages: Python, Bash, C++
Operating Systems: Kali Linux, Ubuntu, Windows
Core Areas: Threat Hunting, SOC Analysis, Reverse Engineering, Secure Networking

Certifications

- CompTIA Security+
- CompTIA Network+
- AWS Certified Cloud Practitioner (CLF-C02)
- NPTEL (Programming in Java, Computer Architecture)

Education

B.Tech in Computer Science with Specialization in Cybersecurity **CGPA: 9.7/10**
SRM Institute of Science and Technology, Chennai
September 2022 – Present

12th (CBSE) **Percentage: 78.4%**
Shrishti Vidyashram, Vellore
June 2018 – June 2019

10th (CBSE) **GPA: 9.8/10**
Shrishti Vidyashram, Vellore
June 2016 – June 2017

Experience

Singapore Armed Forces **Mar 2020 - Jan 2022**
Signaller · Communication Specialist *Singapore*

- Operated and maintained secure communication systems for the 35th Combat Engineers, ensuring real-time, encrypted transmissions under mission-critical scenarios.
- Troubleshot system and protocol failures, enhancing operational uptime and showcasing readiness for high-pressure security environments.
- Independently managed radio frequency equipment and encrypted protocols, building a strong foundation in communication and cybersecurity practices.