Samyukta Kurikala

Boston, MA | samyuktakurikala.netlify.app | samyuktakurikalawork@outlook.com | samyukta-kurikala

Education

MS in Cybersecurity, Northeastern University **Sep. 2024 – Dec. 2026**
Coursework: Information System Forensics, Network Security, Software Vulnerabilities and Securities **GPA: 3.75**

BTech in Computer Science, SRM Institute of Science and Technology **Sep. 2020 – Jun. 2024**
Coursework: Computer Networks, Network Security, Operating Systems **GPA: 9.21**

Technical Skills

Tools & Platforms: Wireshark, Burp Suite, Volatility, Autopsy, Splunk, Security Onion
Languages/Scripts: Python, Bash, PowerShell, SQL
Frameworks/Standards: MITRE ATT&CK, NIST CSF, ISO 27001, OWASP Top 10
Core Skills: Malware Forensics, Memory Analysis, Log Analysis, IR Playbooks, Threat Hunting, Vulnerability Management

Projects

Enterprise SOC Environment | ELK Stack, MITRE ATT&CK, NIST CSF, Logstash **In Progress**

- Deployed ELK Stack SIEM with NIST CSF-aligned dashboards and MITRE ATT&CK technique detection, implementing correlation rules for T1110, T1078, and T1083 attack patterns.
- Configured multi-source log ingestion and automated alerting with framework-based incident classification, reducing alert noise through strategic rule tuning and technique-specific detection logic.

Secure Instant Messaging Application | Python, ECDH, AES-GCM **2025**

- Built a command-line chat app with encrypted messaging, session key rotation, and secure login, supporting real-time communication.
- Applied ECDH key exchange and AES-GCM encryption, enabling zero-knowledge password proofs and tamper-proof logs.

Information System Forensics - Case Studies | Volatility, Wireshark, Autopsy **2025**

- Conducted 4 detailed case studies focusing on memory analysis, malware forensics, browser forensics, and cloud artifact analysis.
- Applied tools like Volatility, Wireshark, and Autopsy to identify indicators of compromise and recommend incident response measures.
- Maintained detailed chain-of-custody documentation and demonstrated practical proficiency in analyzing digital evidence.

Experience

Cybersecurity Project Intern | DRDO **Aug. 2023 – Nov. 2023**

- Developed and deployed an end-to-end encrypted video transmission system over Wi-Fi, using AES encryption and PyCrypto, to safeguard sensitive communications.
- Implemented frame shuffling and real-time anti-tampering checks, achieving zero successful MITM attack attempts in laboratory testing.

Network Security Intern | MSN Laboratories **Jun. 2023 – Jul. 2023**

- Monitored and analyzed network traffic using Wireshark/tcpdump, reducing false positives in alert triage by 20%.
- Configured VLAN segmentation and firewall rules, decreasing unauthorized access attempts by 35%.
- Reviewed firewall logs and escalated 15+ critical incidents, improving detection-to-response time by 30%.

Certifications

CompTIA Security+ Completed
Google Cybersecurity Professional Certificate In Progress
ISC2 CC In Progress

Community

- Top 50 Globally – WiCyS Target Cyber Defense Challenge (Tier 1)
- SimSpace Cyber Range Challenge: Ranked 6th place (Threat detection, log analysis, SOC coordination)
- Contributor to WiCyS VDP program; Head of Finance & FOSS contributor @ null NEU
- Attendee: Boston Security Meetup, DEFCON Boston, Boston Hackers