Yimaj Ahmed

1552 Dover Creek Ln Lawrenceville, GA 30045 | 470-209-5746 | yahmedgt@gmail.com | U.S. Citizen

Summary

Cybersecurity professional with a Bachelor's degree in Computer Engineering from the Georgia Institute of Technology with concentrations in Cybersecurity and Cloud Computing. Driven to enhance security through analyzing complex threats and reverse engineering malware. Proficient in penetration testing, network analysis, and risk assessment. Actively seeking to leverage my technical acumen and passion for cybersecurity to contribute to the mission of dynamic cyber defense and threat intelligence.

Education

Georgia Institute of Technology | Atlanta, GA *January 2020 – May 2024*
Bachelor of Science in Computer Engineering, Honors
Concentrations: Cybersecurity and Distributed System & Software Design

Certifications

CompTIA Security+ *July 2024*
Google Cybersecurity Certificate *May 2023 – August 2023*

Skills

Cybersecurity: Reverse Engineering Malware, Security Information and Event Management (SIEM) Tools, Data Loss Prevention (DLP), Threat Modeling, VPNs, VLANs, AD/LDAP, Encryption, Digital Forensics, Information Security, Memory Analysis, Network Analysis, Penetration Testing, Vulnerability Scanning, Firewall Configuration and Management, Incident Response, Risk Management
Programming: Python, Java, C, C++, SQL, Assembly, Verilog, VHDL, Software Debugging, Automation
Software: IDA Pro, OllyDBG, Wireshark, Altera Quartus II, Nmap, GitHub, MATLAB, Metasploit, Burp Suite, CrowdStrike, VMware
Cloud Computing: AWS, Database Management, Spark, MapReduce, Hadoop, DevOps, Machine Learning and AI, Cloud Security
Technical Support: Linux, Microsoft Office, Teams, Google Suite, Ticketing Systems, Operating Systems, Networking Concepts, ISO

Projects

Reverse Engineering Malware Project *Spring 2024*
The aim of this project was to gain hands-on experience in reverse engineering and analyzing a variety of malware samples to understand their behavior, attack mechanisms, and potential impact on systems.

- Reverse-engineered and analyzed a diverse set of malware samples, including Michelangelo.1, DOS-7, SQLSlammer, Lucius, and Harulf, to understand their code, structure, and functionality. Utilized IDA Pro and OllyDbg to dissect malware samples.

Network Monitoring and Scanning Project *Summer 2024*
The goal of this project was to develop and execute a network monitoring and scanning system to analyze network traffic, identify devices, and assess network security.

- Installed and configured Wireshark and Nmap to monitor and analyze network traffic and perform network scans.
- Analyzed network packets using Wireshark to observe traffic patterns, identify protocols, and detect anomalies.
- Executed network scans with Nmap to discover active devices, open ports, and services, assessing network exposure and vulnerabilities, and documented the findings into a comprehensive report.

Building a Security Operations Center (SOC) with Microsoft Sentinel | Cybersecurity *Summer 2024*
The goal of this project was to deploy and configure a Security Information and Event Management (SIEM) system using Microsoft Sentinel, enabling real-time monitoring and response to security threats.

- Set up an Azure VM with RDP ports to simulate a security vulnerability.
- Connected VM event logs to Log Analytics and created custom alerts for RDP sign-ins.
- Monitored logs continuously to simulate a SOC environment and provided security recommendations.

Experience

Mastercard | Remote *Summer 2024*
Cyber Security Analyst Intern Experience
A global technology company in the payments industry, providing secure and innovative payment solutions for consumers worldwide

- Analyzed and identified areas of the business that needed more robust security training and implemented those procedures
- Aided in identifying and reporting security threats such as phishing.

Clifford Chance Law Firm | Remote *Spring 2023*
Cyber Security Intern
A prominent multinational law firm known for its expertise in providing comprehensive legal services globally.

- Assisted various clients with legal issues relating to cyber breaches, and Notified stakeholders about data breaches.
- Provided guidance on responding to an ICO Dawn Raid to the managing partner of online travel companies.
- Formulated defensive strategies for a client with data center operations to respond to data breaches.