Garrett McGuire

garrettcmcguire@gmail.com (770) 367-3261 @ garrett-mcguire www.garrettmcguire.com

Objective

I am actively seeking an internship or full-time position in the field of cybersecurity. I am eager to apply my passion and technical skills in information security and programming that I have developed throughout my bachelor's degree in software engineering/cybersecurity.

Education

KENNESAW STATE UNIVERSITY **// MAY 2021- MAY 2024**

- *Bachelor of Science in Software-Engineering (3.9 GPA) /* **Order of the Sword & Shield National Honor Society of Homeland Security**
- *Minor: Cyber-security*
- Relevant coursework: Intro to Cybersecurity Principles, Programming 1 & 2 (C++), Intro to SWE, Discrete Comp. Structures, Probability & Data Analysis, Client systems security, Op systems concepts and admin, Database systems, Technical Writing, Professional Practices and Ethics.

CERTIFICATIONS: COMPTIA - SECURITY+, TCMSECURITY - PRACTICAL JUNIOR MALWARE RESEARCHER (PJMR)

- **Online Initiatives**: Practical Windows Forensics, Practical Ethical Hacking, OSINT Fundamentals, Python 201, pursuing PNPT certification.
- **CTFs**: NCL: ranked top 6% out of 3,500 teams, NCAE national team finals 8th place, 2x US Cyber Games & NSA Codebreaker competitor.

Skills

- **Technical Skills**: Java, C++, C, Python, Bash, Assembly, SQL, Linux, ELK Stack, Splunk, Snort, Wireshark, VMs, Web Exploitation, Intelligence Analysis, Malware Analysis, Reverse Engineering, Exploit Development, Dark Web Research, PCAP analysis, Windows Forensics.
- **Soft Skills:** Excellent oral and written communication, Lifelong learner, Reliable, Consistent, Organized, Detail oriented, Strategic thinker.

Projects

Honey Pot ELK Stack SIEM – Writeup Available - https://medium.com/@garrettcmcguire

- A VM deployed and specifically configured as a honeypot to attract global online attacks. Implemented and customized the ELK stack as a SIEM solution for organizing the collected data. Leveraged Suricata rules for alerts and Kibana as a visual tool to display the attack information.

Threat Intelligence Feed – Discord bot

- Developed a Python-based bot that aggregates and updates real-time threat intelligence feeds from multiple sources. Implemented integration with Discord to automatically post relevant threat information and alerts to a designated channel. Improved situational awareness by providing timely updates on emerging threats and vulnerabilities.

Leadership

Microsoft Student Learn Ambassador (KSU/Atlanta) – April 2023 – Present

Vice President – Information Systems Security Association (KSU) – January 2022 – February 2023

- Organized events for our 300+ member club at KSU and collaborated with a team to teach classes on malware analysis and CTFs.

Experience

Cyber Threat Intelligence Intern– Center for Internet Security: MS-ISAC - September 2022 - Present

- Performed intelligence analysis, generated reports, and conducted malware analysis. Collaborated in the development of a Python script that automates the detection of CTAs (Cyber Threat Actors) selling initial access to members. This solution improved efficiency by reducing the daily time investment from over 30 minutes to just 2 minutes while enhancing the effectiveness of the results obtained.

Client Technical Support – Fiserv – April 2022 – September 2022

- Established the commercial center team, working in close collaboration to provide support to Republic Bank. Efficiently configured and tested new workstations for a team of 40 members. Provided effective troubleshooting for customers' technical hardware and software issues.