AARON TI

mcdulltii@gmail.com • Portfolio https://mcdulltii.github.io • Github https://github.com/mcdulltii • Singapore

Having a curious mindset towards computer science, I always seek for new directions to gain more knowledge. From binary exploits to web development, computer renders to assembly, these are some of the fields within computer science that I have worked on. Being passionate about developing my skills and knowledge in computer science, I actively take up a myriad of opportunities to learn as much as I can.

SKILLS

- High & Low Level Programming
- Malware Analysis & Reverse Engineering
- Full Stack & Mobile App Development
- DevOps
- 3D Design & Rendering
- VR & AR App Development

EXPERIENCE

Coding

- Python, C, C#, C++, Rust, Golang, Javascript, Java, Assembly, Nim

Technologies/Environment

- Windows, Linux, OpenGL, Web frameworks, Docker, Kubernetes, OpenCV, Huggingface, Cinema4D, Blender, Unity, UnrealEngine

EMPLOYMENT HISTORY

Cyber Security Engineer Intern at Centre for Strategic Infocomm Technologies (CSIT) **Sep 2024 – Present**

- Creating custom Linux user mode and kernel mode antivirus tools

Cyber Security Engineer Intern at watchTowr **Apr 2024 – Jul 2024**

- Adapted T-Pot architecture with modular vulnerable honeypot containers with ELK packetbeat integration and dashboard alerts.
- Assisted in automating continuous assurance and adversary sight through code runners.
- Finetuned the GPT3.5 model and prompt engineered to automate manual laborous tasks.

DevSecOps Intern at GuardRails **Oct 2022 – Dec 2022**

- Used Semgrep to quickly find and prevent security issues in various technologies.
- Integrated Semgrep into the organization’s CI/CD pipeline, helping to enforce security standards and protect against OWASP Top 10 vulnerabilities.

Threat and Incident Specialist at MINDEF - Military Security Department (MSD) **Apr 2020 – Apr 2022**

- Reviewed violations of computer security procedures and developed mitigation plans.
- Delved into malware analysis and threat hunting, in turn, researching and developing computer forensic tools.
- Analyzed malicious obfuscation methods, researched and reverse-engineered malicious samples for further understanding of their procedures.

Software Developer at Helloholo **Nov 2020 – Jan 2021**

- Developed and implemented interactive AV design and integrated VR technologies with corporate visions.
- Experimented with new technologies (Virtual Reality, Augmented Reality, and Mixed Reality), and assisted in developing software compatible with Extended Reality devices.
- Introduced Oculus development for simulation and AR technology.

Intern at Institute of High Performance Computing (IHPC) A*STAR **May 2017 – Jan 2018**

- Using high-performance simulation software to understand the behavior of light and electromagnetic waves in both dielectric materials as well as metals.
- Coordinated effectively with a team of 4 members possessing skills in high-performance computing.

PROJECTS

Badminton AI Robot **Jun 2023 – Apr 2024**

- Stereo calibration of cameras to take photos of incoming shuttlecocks.
- Object detection model to retrieve position from stereo images.
- Uses (Robot Operating System) ROS 2 to communicate with badminton robot, to predict and move to the shuttlecock's landing position to receive it.

Diagram Sketch AI **Sep 2023 – Apr 2024**

- Uses YOLOv8 object detection model to train and detect shapes and texts within handwritten diagrams.
- Optical Character Recognition to transcribe text from diagram images.
- Visualize detected shapes and texts digitally within a DrawIO frontend.

SourceSync **Aug 2022 – Apr 2023**

- Syncing of source codes with Ghidra decompiled pseudocodes.
- Compares two AST trees using depth-first preorder walk and fuzzy hashing.
- Match simplified AST tree nodes and get function line matchings within each function bound.

obfDetect **Aug 2021 – Oct 2021**

https://github.com/mcdulltii/obfDetect

- Automatically detects obfuscated code and other state machines in binary samples.
- IDA Scripting to perform heuristic calculations on function Abstract Syntax Trees (AST).
- Detects function anomalies and obfuscated assembly code based on heuristic complexities.

COURSES / CERTIFICATIONS

AWS Academy Cloud Foundations

- Gives an overall understanding of cloud computing concepts, independent of specific technical roles.
- Provides a detailed overview of cloud concepts, AWS core services, security, architecture, pricing, and support.

AWS Academy Cloud Architecting

- Covers the fundamentals of building IT infrastructure on AWS and helps students gain the skills they need to pursue the AWS Certified Solutions Architect – Associate certification.

Advanced Malware Analysis Techniques by Kaspersky

https://xtraining.kaspersky.com/courses/advanced-malware-analysis-techniques

- Analyze modern complicated code samples, from receiving the initial artifact, all the way to producing a technical description of the attacker's TTPs with IOCs.
- Produce static decryptors for real-life scenarios and then continue with in-depth analysis of the malicious code.
- Analyze malicious documents that are typically used to deliver initial payloads and know how to extract them.
- Ensure damage assessment and incident response efforts are accurate and effective.

Targeted Malware Reverse Engineering by Kaspersky

https://xtraining.kaspersky.com/courses/targeted-malware-reverse-engineering

- Analyze real-life malware used in the wild by APT groups.
- Reverse-engineer malicious documents and exploits.
- Approach reverse engineering programs written in several programming or scripting languages (C, .NET, Delphi, Powershell, JavaScript, C++) and compiled for different architectures (x86, x64) with different compilers or operating systems (Windows, Linux).
- Handle obfuscated or encrypted content in malicious software.

Reverse Engineering 101 by Kaspersky

https://xtraining.kaspersky.com/courses/reverse-engineering-101

- Gain the initial knowledge needed for malware analysis.
- Analyze executables generated by different compilers to be more familiar with "esoteric" executables.

EDUCATION

Singapore Institute of Technology and University of Glasgow **2022 – Present**

- Undergraduate in Computing Science.
- Actively seeking out connections and job opportunities to broaden my horizon.

Singapore Institute of Technology **2019 – 2022**

- Undergraduate in Information Security, as part of the Work-Study programme in the Cyber NSF Scheme.
- Building on my computing knowledge in the varying fields of computer science, such as Information Security and Interactive Simulation.
- Delved into the niche topics within computer science as part of Capture-The-Flag (CTF) teams both locally and overseas. Some of the niche topics that I have explored are the makings of malware and reverse engineering.

Anglo-Chinese Junior College **2017 – 2018**

- GCE A-Levels (Further Mathematics, H2 Mathematics, H2 Physics).
- Expressed my passion for computer science by developing real-time computer vision models in my school's computing CCA.
- Created 3D models and textures, computer renders, and shaders in several modeling/texturing applications.