AUSTIN J. HEATH

+1 601-596-2842 | austin@heath.codes | https://austin.heath.codes
https://github.com/one2blame | https://linkedin.com/in/austinjheath
Clearance: TS/SCI with CI Poly

EXPERIENCE

Senior Security Researcher June 2021 – Present
U.S. Army Cyber Command - Cyber Solutions Development *Fort Gordon, GA*

- Managed a team of 12 security researchers using tools like IDAPro, BinDiff, LLVM, and QEMU, to research, discover, and exploit vulnerabilities in embedded devices and Windows applications, saving the organization over $1mil in expected costs when compared to similar vendor solutions.
- Developed a shellcode library using C, Python, and CMake, enabling 20 developers to cross-compile ubiquitous shellcodes for Intel, ARM, MIPS, and PowerPC processor architectures, eliminating duplicate shellcodes across 9 exploit development projects.
- Triaged 5 public vulnerability disclosures, releasing 7 bespoke exploit tools, providing initial access to computer networks of interest for 6 operations teams across 3 organizations and 4 uniformed services.
- Instructed 5 operations teams on the effective use of exploit tools, increasing stakeholder interaction and influencing organizational policy to emphasize consistent stakeholder engagement.
- Hosted 12 monthly training events covering reverse-engineering and exploit development techniques, increasing the organization's number of trained security researchers by 25%.
- Overhauled the organization's technical documentation process using Markdown, LaTeX, Pandoc, CMake, and Python, enabling developers to better detect documentation errors prior to release.

Junior Security Researcher January 2019 – May 2021
U.S. Army Cyber Command - Cyber Solutions Development *Fort Gordon, GA*

- Redesigned the organization's binary obfuscation methods using LLVM, rendering obfuscated artifacts unrecognizable compared to the original, inhibiting reverse-engineering efforts and preventing developers from spending 40 hours manually obfuscating existing projects.
- Implemented 11 modules for a Python exploit framework, automating common operator tasks and reducing 50% of human interaction, increasing mission efficiency for 5 operations teams.
- Automated the organization's compilation, testing, release, and deployment process by integrating existing projects into GitLab CI, expediting tool development and release for 3 developer teams.
- Obfuscated web-based malware written in PHP using open source software and designed command, control, and configuration mechanisms using Python, enabling 3 operations teams across 2 uniformed services to maintain persistent access to web targets of interest.

EDUCATION

Georgia Institute of Technology Atlanta, GA
Master of Science, Computer Science (Specialization: Computing Systems), 4.0 GPA *December 2022*

U.S. Army Cyber Center of Excellence Augusta, GA
Cyber Basic Officer Leader Course, Distinguished Honor Graduate *December 2018*

Mississippi State University Starkville, MS
Bachelor of Science, Computer Engineering, 3.61 GPA *December 2017*

CERTIFICATIONS

Offensive Security Certified Professional (OSCP)
Certified Information Systems Security Professional (CISSP)
GIAC Reverse Engineering Malware (GREM)
CompTIA Security+ (Sec+)
Certified Ethical Hacker (CEH)
Cisco Certified Network Associate (CCNA)

PROJECTS

Splinter Shell | https://github.com/one2blame/splintershell | *Python, Scapy, Scikit-learn, amd64* April 2021 - Present
Employed unsupervised learning techniques to train a machine learning model on a corpus of packet captures, classifying normal and malicious network traffic and encoding shellcodes to bypass intrusion prevention systems.

The Dark Arts | https://one2bla.me/the-dark-arts/ | *C, Python, Ghidra, pwntools, angr* July 2020 - Present
Composed a blog to catalogue my adventures in reverse-engineering and binary exploitation, serving as a training resource for junior security researchers.

Constraint-based Variable Analyzer | https://github.com/one2blame/cs6340 | *C++, LLVM, Z3* October 2021
Transformed programs into LLVM intermediate representation (IR), derived Datalog facts from the instructions, and designed a reaching definition and live variables analysis using Z3.

Data Dependency Tracker | https://github.com/one2blame/cs6747 | *Python, Ghidra* July 2021
Wrote Python scripts to parse Ghidra disassembly, generating control flow graphs and data dependency tracking for functions in malware specimens.

Stock Trading Robot | https://github.com/one2blame/cs7646 | *Python, NumPy, pandas* April 2022
Employed reinforcement learning to train a model on historical stock metrics, assessing the trading robot's performance on out-of-sample data, outperforming a manual trading strategy by 30%.

Multi-class Random Forest | https://github.com/one2blame/cs6601 | *Python, NumPy* July 2022
Improved upon existing multi-class classification tree and random forest implementations, achieving a classification accuracy of 84% on out-of-sample data.

Extensible MapReduce Framework | https://github.com/one2blame/cs6210 | *C++, gRPC, Protobuf* April 2020
Designed an extensible, distributed system to MapReduce a large corpus of data, applying data sharding and load balancing to enhance performance.

Distributed File System | https://github.com/one2blame/cs6200 | *C++, gRPC, Protobuf* November 2019
Engineered a concurrent server capable of handling clients initiating asynchronous gRPC requests to upload and download files.

SDN Firewall | https://github.com/one2blame/cs6250 | *Python, Mininet, OpenFlow, POX* March 2021
Constructed an emulated network to test software-defined network firewall rules, programming real-time traffic inspection to enforce access controls.

TECHNICAL SKILLS

Languages: Python, C/C++, x86, amd64, MIPS, ARM, PowerPC, TileGX, Java, PHP, JavaScript
Libraries: gRPC, OpenMP/MPI, libvirt, libcurl, POX, Mininet, OpenFlow, LLVM, Z3, NumPy, SciPy, pandas, pwntools
Developer Tools: Git, GitLab CI, Atlassian Bamboo, Jupyter, Docker, QEMU, GDB, WinDbg, angr, AFL, KLEE
Applications: VMware, VirtualBox, Vagrant, Ghidra, IDAPro, BinaryNinja, BinDiff
Frameworks: Metasploit, WordPress

VOLUNTEERING AND COMMUNITY SERVICE

Mentor February 2022 – May 2022
Grovetown High-school Robotics Club *Grovetown, GA*
Mentored high-school students on robotics mechanical engineering, setup of electrical components, and development of Arduino code for controller logic. Lead the Grovetown High-school Robotics Club to take 1st place in the Central Savannah River Area (CSRA) Fully Wired high-school robotics competition.

Volunteer May 2021 - July 2021
Air Force Association CyberPatriot *Augusta, GA*
Moderated a Virtual CyberPatriot Summer Camp via Zoom and provided instruction to high-school students on techniques to harden the security posture of various Linux distributions.

Volunteer August 2019 – March 2020
Girls Who Code *Augusta, GA*
Facilitated club meetings and taught 6th - 12th grade girls Python game development.

ACHIEVEMENTS AND AWARDS

CISA President's Cup Cybersecurity Competition - 3rd Place 3 x Army Achievement Medals