AUSTIN HEATH

+1 601-596-2842 | austin@heath.codes

https://austin.heath.codes

Willing to relocate

Clearance: Top Secret (TS/SCI) with CI Polygraph

EXPERIENCE

Senior Reverse Engineer 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, Ghidra, LLVM, and QEMU, to research, discover, and exploit vulnerabilities in embedded devices and Windows applications, enabling the organization to avoid costs procuring similar vendor solutions, resulting in a significant savings.
- 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.
- Hosted 12 monthly training events covering reverse-engineering and exploit development techniques, increasing the organization's number of trained security researchers by 25%.

Reverse Engineer February 2018 – 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.
- 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.

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, 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.

EDUCATION

Georgia Institute of Technology Atlanta, GA

Master of Science, Computer Science (Specialization: Computing Systems), 4.0 GPA *December 2022*

Mississippi State University Starkville, MS

Bachelor of Science, Computer Engineering, 3.61 GPA *December 2017*

TECHNICAL SKILLS

Languages: Python, Lua, C/C++, Java, x86, x86_64, MIPS, ARM, PowerPC, TileGX
Security Tools: Metasploit, Wireshark, TShark, IDAPro, Ghidra, BinaryNinja, BinDiff
Developer Tools: Git, GitLab CI, CMake, Docker, GDB, WinDbg, QEMU, LLVM, KLEE, AFL, angr

CERTIFICATIONS

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