AUSTIN HEATH

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

one2bla.me
Willing to relocate
Clearance: Top Secret (TS/SCI) w/ FSP

EXPERIENCE

Microsoft Atlanta, GA
Software Engineer, Site Reliability *March 2023 – Present*

- Designed a resilient system using Azure Data Factory, various Microsoft IaC products, and existing cross domain solutions to empower 3 engineering teams with the ability to replicate critical security data to the Azure Government clouds, increasing the accuracy of 5 security services.
- Championed the delivery of AI-driven adversary emulation to the Azure Government clouds, enabling incident response teams to proactively assess the fidelity of security services provided by Microsoft Security.

U.S. Army Cyber Command Fort Eisenhower, GA
Senior Security Software Engineer *February 2018 – February 2023*

- 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.
- 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.
- 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.
- Hosted 12 monthly training events covering reverse-engineering and exploit development techniques, increasing the organization's number of trained security researchers by 25%.
- 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.
- 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.

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*

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)
Azure Fundamentals (AZ-900)

TECHNICAL SKILLS

Cloud Providers: Azure
Applications: VMware, VirtualBox, Vagrant, Ghidra, IDAPro, BinaryNinja, BinDiff
Languages: Python, C/C++, C#, x86, amd64, MIPS, ARM, PowerPC, TileGX, PowerShell
Developer Tools: Git, GitHub Actions, Azure DevOps, Jupyter, Docker, QEMU, GDB, WinDbg, angr, AFL, KLEE
Libraries: gRPC, OpenMP/MPI, libvirt, libcurl, POX, Mininet, OpenFlow, LLVM, Z3, NumPy, SciPy, pandas, pwntools

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.

VOLUNTEERING AND COMMUNITY SERVICE

Mentor January 2024 – Present
Blacks in Cybersecurity *Atlanta, GA*

Provided mentorship to junior cybersecurity professionals in the Black community.

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