Aaron Cowley

Security Engineer

396 N 100 W Apt 8 Provo Utah

aaron.d.cowley@outlook.com

(916) 430-6668

github.com/aaroncowley
linkedin.com/in/aaron-cowley-3a091b126

Education

M.S. Technology (Cybersecurity Emphasis) | Brigham Young University, Provo Utah | Aug 2021
GPA:4.0

B.S. Cybersecurity | Brigham Young University, Provo Utah | Aug 2019
GPA:3.32

Skills

Languages : Python, C/C++, Golang, Javascript, C#, SQL, Java

Defensive Cybersecurity : Splunk, Splunk Phantom, Elastic Stack, Zeek IDS, Snort

Penetration Testing : Tennable Nessus, Burp Suite, Kali Linux, Metasploit

Forensics : Volatility, Autopsy, FTK Imager, Malware Reverse Engineering

Systems Administration : Amazon AWS, Azure, Git, Docker, Ansible

Extra-Curricular

Bug Bounty Hunter on Hackerone & BugCrowd

BYU CCDC (Collegiate Cyber Defense Competition) Linux & Web Team Lead

BYU ITSEC Club Vice President

Deloitte CTF 2nd Place

HackTheBox Rank of Hacker

Work Experience

Dec'19 - Now Graduate Cybersecurity Research Assistant
BYU, Provo UT
·Thesis on deploying vulnerable blockchains as "vulnerability as a service" Cybersecurity teaching tools
·Reseaching automated red team scripts for defensive cybersecurity training
·Created and Manages Academic Research Lab's SOC using Splunk, Zeek IDS, Splunk Phantom and custom Python integrations
·Teaches and prepares coursework for defensive and offensive Cybersecurity classes

May'19 - Now ICS Security Engineer Intern
Idaho National Laboratory, Idaho Falls ID
·Assessed security of US DOE Industrial Control Systems and developed automated remediations in Python
·Deployed SIEM tools and wrote custom Python integrations for ICS devices
·Produced automated threat feed integration for SCADA system defense
·Developed novel threat model and remediation for critical ICS Vulnerability that was presented on Capitol Hill to demonstrate INLs cyber response capabilities
·Used Python to automate threat remediation and reporting software

Sep'18 - Sep'19 Cybersecurity Research Assistant
BYU, Provo UT
·Web Applications & Linux lead for CCDC (Collegiate Cyber Defense Competition) team
·BYU Student Red Team Member
·TA and Mentor for Cybersecurity courses
·Developed Penetration Testing coursework for Cybersecurity major as an undergrad

Jan'17 - Sep'18 Student Full-Stack Developer
BYU, Provo UT
·Managed 14 of BYU Humanities multi-platform websites
·Reduced code complexity and decreased load time by 10% through self-written upgrades
·Discovered and patched SQLi and XSS vulnerabilities in live University websites

Publications

Jan 2020 Dynamic Intrusion Deception in a Cloud Environment
Chia-Chi Teng, Aaron Cowley, Russel Havens

Projects & Contributions

June 2019 Open source contribution to Structured Threat Intelligence Graph, a gui for creating and visualizing STIXv2 threat intelligence objects with a graph database
github.com/idaholab/STIG