

AEDAN (AT) TAYLOR

aedan.e.taylor@gmail.com ◇ [linkedin.com/in/secureighty](https://www.linkedin.com/in/secureighty) ◇ github.com/secureighty ◇ infosec.exchange/@secureighty

EDUCATION

Computing Security BS, Rochester Institute of Technology

Fall 2023

EXPERIENCE

Penetration Tester & Red Teamer

May 2023 - November 2024

[OCD Tech](#)

Remote

- Conducted Penetration Tests and Red Team Engagements against enterprise clients and delivered professional reports in a team setting. Discovered multiple critical severity vulnerabilities using Burp Suite, Nessus, and manual Python scripting and fuzzing.
- Built and operated technical infrastructure to assist with penetration testing workflows including Greenbone Vulnerability Manager (OpenVAS), ReconFTW, Hashtopolis, Evilginx, and more.
- Provided preliminary incident response advising and log analysis for client blue teams.

Security Analyst

January 2022 - June 2022

[FM](#)

Johnston, RI

- Triaged alerts in a SIEM (Security Information and Event Manager), correlating activity with multiple technologies including CrowdStrike, Varonis, Palo Alto PAN-OS, Palo Alto Wildfire, and Securonix.
- Created and refined correlation search alerts in Splunk.
- Conducted Purple Team validation testing and assessed the security posture of workstations and servers within the ecosystem.
- Trained other analysts and oversaw their work.

PROJECTS

Blog and External Publications - secureighty.me/blog

Blog dedicated to sharing security research, CTF writeups, and links to guest publications on other organizations' websites.

Security Research, Community Outreach

CTF Challenge Authorship - [Writeups and Dev Process Presentation](#)

Wrote web security focused Capture The Flag challenges for use in competition. Publicly presented writeups and development process in RIT's Security Club, RITSEC.

Web Security, Python, Flask, Selenium, Public Speaking

Bug Bounty and Vulnerability Disclosure Research - hackerone.com/secureighty

Researched and responsibly disclosed vulnerabilities through platforms including Hackerone, Bugcrowd, Responsible Disclosure, and emails directly to company points of contact. Recognized by Palo Alto Networks and CrowdStrike.

Web Security, ZAPProxy, Burpsuite, OWASP

ACCOMPLISHMENTS

- Winner of UB-Lockdown Fall 2021 - Windows Lead for RIT's winning team in University of Buffalo's blue team cyber defense competition. Decrypted ransomware on an FTP server.
- RITSEC Research Presentations - Presenter for RIT's Security Club, presenting on a range of topics including a MITRE ATT&CK technique, Web Application Firewalls, and Game Hacking.
- ISTS Black Team "Weird OS" Lead - Set up a Miracle Linux box to run in RITSEC's Information Security Talent Search, designed to open as many clock applications as possible on boot using Packer, Ansible, and Terraform.