Tyler J. Boire

https://tylerboire.github.io/ tylerboire@gmail.com

Conferences & CTFs:

OSCP (In Progress), Defcon 22 and 23, JailbreakCon, MITRE CTF, CSAW, NECCDC

- Attended training on Android Malware Analysis, Reversing and Exploitation at DC23
- BurlingPwn CTF team member
- Defended enterprise-like network from professional pen-testers at NECCDC.

Projects:

- Kippo Honey Pots
- Automating post exploitation information gathering in Bash
- Automated Android and Windows Malware triage & analysis in Python.

Education:

BS Computer Networking & Information Security — Champlain College 2012-2016

Specialization in Cyber-Security & Minor in Digital Forensics

General Education — Clinton Community College 2011-2012

GenEd credits and college prep classes.

Experience:

Threat Specialist, Palo Alto Networks — 06/16-Now

Customer facing support for all threat prevention and detection features of the Palo Alto Networks Platform:

- Determined false positive & false negative verdicts for IPS, sandbox dynamic analysis verdicts, URL categorization, and C2 communication detection.
- Assisted in creating coverage for emerging vulnerabilities & malware variants.
- Aided in identification and signatures for various malware families.
- Automated information gathering via internal REST APIs with Python.
- Interpreted commodity scan results against the Palo Alto Networks platform.
- Assisted in IPS signature development, improvement, and tuning.
- Worked with customers in establishing best practices configuration for individual environments.
- Maintained internal replication lab

Network Admin & Researcher, Leahy Center for Digital Investigation — 12/15-05/16

Maintained network functionality and researched forensic uses for JTAG to bypass full disk encryption on android phones

- Oversaw junior admins and maintained critical infrastructure
- Performed vulnerability assessments and inventory tracking
- Implemented log aggregation using GreyLog2
- Improved documentation on existing procedures
- Researched forensic uses for JTAG/ChipOff techniques
- Provided JTAG documentation for our director to use in active investigations.
- Provided consultation on Amazon Alexa research.

Intern, Dell SecureWorks — 06/15-04/16

Consolidated and reworded best practice and remediation suggestions.

- Aided the Threat Intelligence department in analyzing a kill chain for Threat Group 3390
- Reported on threat assessments of hostile countries and capabilities based on OSINT.
- Consolidated and reworked best practice and remediation suggestions.
- Reviewed SANS GCIH material with new hires prep for their test.

Sr.Helpdesk/Helpdesk, Champlain College — 12/12-11/16

Teaching assistant, Champlain College — 09/13-05/14

NOC technician, Westelcom — 05/13-08/13