

Tyler Boire

Email: tyler.boire@gmail.com
Website: <https://tylerboire.github.io>
GitHub: <https://github.com/TylerBoire>

Communication Skills:

- Consulting for businesses up to Fortune 50 space.
- Experience in interacting with technical and management audiences
- Provide written and verbal guidance on improving security posture.
- Write documentation and guidance on technical processes & policy.

Security Strategy:

- Defense-in-depth models
- Kill-chain analysis and interdiction.
- Firewall config review and best practices layer 4 and 7
- Network logging and alerting
- Least privileged models
- Knowledge of multiple firewall, IDS and IPS vendors
- Experience with multiple EDR, AV, and Network security products
- Experience with PCI-DSS, HIPAA, ISO 27001, NIST 800-53

DFIR:

- Host, Network, and Memory forensics
- File recovery and slack space analysis
- Static and Dynamic Malware Analysis
- Experience building Incident Response plans
- IOC and Threat Intelligence aggregation
- Log analysis

Offensive Security:

Network and Host recon:

- Port, Host and Service discovery
- Vulnerability identification
- OSINT and Confidential document discovery
- Password leak identifications

Exploitation:

- OWASP Top 10 familiarity
- Use and modification of public exploits
- LLMNR & WPAD poisoning
- Kerberos and Service Principal Name abuse.
- Password Cracking using curated dictionaries and rule sets
- Phishing

Physical:

- Lock picking
- Door bypass
- Camera placement considerations

Wireless Analysis:

- WPA cracking attacks including PKMID
- Client Beacon Attacks
- Signal leakage testing
- Evil twin
- Rogue AP

Post exploitation:

- Shell persistence
- Credential harvesting
- Pivoting between network segments
- Power user identification/hunting
- Privilege escalation
- Identifying incident response and countermeasures
- Living off the land

Work Experience

January 2018 – Present	Penetration Tester at Verizon <ul style="list-style-type: none">• Provide customers with Internal, External and Wireless penetration tests• Identify and reinforce good security practices deployed in customer networks• Provide customers with detailed reports regarding their vulnerabilities• Help maintain infrastructure used in day to day operations• Work towards automating common tasks and procedures• Designed and implement repeatable and reliable gold images for consultant laptops and VMs
June 2016 – January 2018	Threat Specialist at Palo Alto Networks <ul style="list-style-type: none">• False positive and false negative verdict determination<ul style="list-style-type: none">– Sandbox dynamic analysis, URL categorization, C2 communication detection• Coverage for emerging vulnerabilities and malware variants• Triage reports of perceived product vulnerabilities• IPS signature development, improvement, and tuning• Aided in identification and signatures for various malware families.• Automated information gathering via internal REST APIs with Python• Maintained internal replication lab
December 2015 – May 2016	Network Admin & Researcher at Leahy Center for Digital Investigation <ul style="list-style-type: none">• Maintained network functionality• Oversaw junior admins and maintained critical infrastructure• Performed vulnerability assessments and inventory tracking• Improved documentation on existing procedures• Researched forensic uses for JTAG/ChipOff techniques• Provided consultation on Amazon Alexa research
June 2015 – April 2016	Incident Response Intern at Dell Secureworks <ul style="list-style-type: none">• 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.
Dec 2012 – Nov 2016	Sr.Helpdesk/Helpdesk at Champlain College <p>Responsible for immediate response to classroom issues, directing other techs to complete tickets and long term projects.</p>
Sept 2013 – May 2014	Teaching Assistant at Champlain College <p>Responsible for ensuring labs ran smoothly and working 1-on-1 with students who had questions during class.</p>
May 2013 – Aug 2013	Network Operations Center Technician at Westelcom <p>Worked in the Network Operation Center, providing over the phone support to customers.</p>

Education

May 2016	Bachelor's degree in Computer Networking & Information Security, Champlain College Specialization in Cybersecurity & Minor in Digital Forensics
May 2012	College prep courses, Clinton Community College