Shawn Webb
lattera@gmail.com - https://www.linkedin.com/in/shawnwebb/

SENIOR SECURITY ENGINEER

SUMMARY OF QUALIFICATIONS:

Experienced and innovative senior information security engineer with fifteen years of experience, specializing in secure development practices in malicious environments. Offensive and defensive security researcher diligently focused on the intersection between information security and human rights.

Programming languages: C, shell scripting, go, python, some java, some php
Development environments: tmux + vim
Operating systems: Linux, Windows, FreeBSD, HardenedBSD
Special skills: Exploit mitigation development, offensive and defensive information security research, human rights research
Spoken languages: English (native), Spanish (fluent)

PROFESSIONAL EXPERIENCE:

BlackhawkNest, Inc May 2020 – Present
Senior Security Engineer / Project Manager

- Development of proprietary performant indexed packet capture suite of utilities.
- Leader and guide of the BlackhawkNest development team.
- Systems and services integration.
- Lead technical architect and developer of a new threat intelligence ecosystem which includes extended detection and response (XDR) capabilities that can be deployed across an entire organization.

Emerald Onion Aug 2017 – Present
Advisory Board Member – Volunteer

- Remotely maintain human rights-focused infrastructure in a malicious environment.
- Advise the team on the technical aspects of running securely anonymization and anti-censorship software.

The HardenedBSD Project / HardenedBSD Foundation Corp Apr 2014 – Present
Co-founder / Lead Security Engineer – Volunteer

- Founder and President of HardenedBSD Foundation Corp (2018 - present), a tax-exempt not-for-profit 501(c)(3) charitable organization.
- Co-implemented the most robust Address Space Layout Randomization (ASLR) implementation found in the BSDs.
- Built and maintain a mixed IPv4 and IPv6 build and mirror infrastructure.
- Perform system and network administration.
- Implement various security hardening technologies and exploit mitigations.

    - Kernel module hardening
    - Process tracing/debugging hardening
    - Runtime linker (RTLD) hardening
    - grsecurity Trusted Path Execution (TPE)
    - Robust fix for CVE-2021-4034
    - Implemented and upstreamed to FreeBSD hypervisor containerization
    - Numerous other features
- Public relations and open source community management, including working with the FreeBSD development community.
- Financial and business management and development.
- Manage and assist teams of talented developers from across the globe.
- Offensive and defensive information security research to prove robustness of HardenedBSD's innovations.
- Designed and implemented a secure and scalable operating system updating mechanism.
- Deployed a novel human rights-focused infrastructure, enabling the development and deployment of the operating system to be fully performed behind various mixnets.
    - HardenedBSD became the first enterprise operating system in 2020 with its entire infrastructure fully reachable via Tor Onion Services.
- Delivered multiple presentations at various international conferences covering various aspects of HardenedBSD and information security in general.
- Integrated SafeStack into HardenedBSD, making HardenedBSD the first enterprise operating system to ship with SafeStack enabled by default.
- Integrated non-Cross-DSO Control Flow Integrity (CFI) into HardenedBSD, making HardenedBSD the first open source enterprise operating system to ship with CFI.
- Deeply integrated llvm's variable auto initialization feature, making HardenedBSD the first enterprise operating to ship with a complete ecosystem with variable auto initialization feature enabled and applied by default.

OPNsense Aug 2016 – Apr 2021

Core Team Member – Volunteer

- Ported HardenedBSD's PaX ASLR, PaX SEGVGUARD, and other exploit mitigation and security hardening technologies to OPNsense.
- Helped the OPNsense team fully migrate their open source firewall appliance base operating system from FreeBSD to HardenedBSD.

G2, Inc / Huntington Ingalls Industries Jan 2015 – May 2020

Senior Security Engineer

- Lead and manage the IT and information security needs of day-to-day operations.
- Research and support human rights efforts globally.
    - Mentored two interns who focused on misinformation, disinformation, malware and human rights—and the intersection between them.

- Manage an enterprise environment consisting of Windows, Linux, and BSD systems.
- Advocate for and publisher of several open source information security tools.
- Developed an automated and portable blackbox penetration and fuzz testing environment and infrastructure for NIST CSD.
- Developed a method to ingest, transform, and distribute batches of large data quickly in an air-gapped environment.
- Helped kick off a dense storage technology (Row6) by applying performance testing metrics and development resources.
- Developed and maintained the infrastructure for a cybersecurity streaming analytics platform.
- Lead developer for an innovative intrusion prevention system that integrates with General Dynamics Trusted Cybersecurity Sensors.
- Migrated the business from Checkpoint firewall to OPNsense.
    - Ensured the seamless transition from Checkpoint's policy-based rules to OPNsense's firewall-based rules.
    - Unique network consisting of over forty VLANs with various requirements in a DoD contracting environment.
- Spoke at various international conferences regarding various information security technologies.

Sourcefire VRT / Cisco Systems Jul 2012 – Jan 2015
Senior Research Engineer

- ClamAV development.
- Offensive and defensive information security research, focusing on malware.
- Helped maintain ClamAV's infrastructure, serving around 40 million ClamAV installations globally.

Wayfair Apr 2011 – May 2012
Software Engineer / Security Analyst

- Developed and deployed a web-based technique for rapid deployment of development infrastructure on FreeBSD by integrating ZFS, jails, FreeBSD's virtualized networking stack, and Drupal.

The Boyer Company May 2010 – May 2012
Network Administrator

- Upgraded and maintained servers and infrastructure on an as-needed basis.

rFocus Aug 2007 – Apr 2011
Software Engineer / Security Analyst

- Built web applications for various clients.
- Analyzed the security of services, applications, and networks.

PROFESSIONAL PUBLICATIONS:

- PoC||GTFO

- Presented at various international conferences, including: BloomCon, BSDCan, BSidesCharm, DEF CON, EuroBSDcon, NYC*BUG, Utah OpenWest, and vBSDcon.