Caleb **Stewart**

Software Engineer · Penetration Tester · Reverse Engineer

Arlington, VA

caleb.stewart94@gmail.com | calebstewart | caleb.stewart | calebjstewart | calebjstewart

Summary

Software Engineering and Cyber Security Expert with Electrical Engineering background. More than 10 years software development experience in many languages from x86 and ARM Assembly to Python. Experience in SOC, Incident Response and Red Team roles. Passion for building elegant tools and frameworks to automate and simplify operations.

Work Experience

Huntress Labs

Arlington, VA

Security Researcher

Jul 2021 - Present

- Technical expert performing static and dynamic binary analysis of malicious payloads.
- Research and development of new features for Huntress platform to extend detection and response capabilities.
- Testing partner software to identify, disclose and remediate potential vulnerabilities.

DoD Cyber Protection Team

Fort Meade, MD

Technical Director

Jun 2020 - Jul 2021

- Lead the research and development of capabilities and tools supporting DoD missions in cyberspace.
- Developed and deployed software and hardware load-out for deployable incident response teams.
- Developed incident response scenarios to provide analyst training and improve mission effectiveness.
- Qualified Mission Commander and Host Analyst.

Coast Guard Cyber Protection Team

Washington, DC

Mission Element Lead

Feb 2019 - Jun 2020

- First responder for numerous network security incidents threatening National Critical Infrastructure
- Developed SOP and training requirements for incoming personnel.
- Procured, configured and deployed state of the art incident response hardware platform.

Coast Guard Security Operations Center

Washington, DC

Infrastructure Support Branch Lead

Nov 2017 - Nov 2018

- Operation and Maintenance of all network defence infrastructure including Intrusion Prevention and Detection Systems, Data-Loss Prevention, Web Content Filter, and Firewalls.
- Battle Watch Captain supervising security and operational control over all IT systems across the Coast Guard.

Coast Guard Cutter Berthlof

Alameda, CA

Combat Information Center Officer

May 2016 - Nov 2017

- Responsible for combat and communications equiment and operational planning.
- Assistant Command Security Officer - managed physical, information and operational security programs for entire crew.

National Security Agency

Fort Meade, MD

Internship

Jun 2015 - Jul 2015

- Applied systems-programming expertise to reverse engineer unknown software and catalog all code-paths for further analysis.
- Performed static and dynamic analysis on malware to identify and report all observed activity.

Certifications

Dec 2018	**Offensive Security Certified Professional (OSCP),** Certification ID: OS-101-017541	*Offensive Security*
Oct 2020	**Exploit Researcher and Advanced Penetration Tester (GXPN),** Certification ID: 9192230	*GIAC*
Dec 2019	**Offensive Security Certified Expert (OSCE),** Certification ID: OS-CTP-11344	*Offensive Security*
Feb 2020	**Offensive Security Web Expert (OSWE),** Certification ID: OS-AWAE-02880	*Offensive Security*
Mar 2020	**Certified Professional Penetration Tester (eCPPT),** Certification ID: 9831814	*eLearnSecurity*
Feb 2020	**Offensive Security Wireless Professional (OSWP),** Certification ID: OS-BWA-036075	*Offensive Security*
Dec 2018	**Certified Information Systems Security Professional (CISSP),** Certification ID: 703304	*ISC2*
Feb 2021	**Offensive Security Experience Penetration Tester (OSEP),** Certification ID: OSEP-10202	*Offensive Security*
Mar 2021	**Certified Exploit Developer (eCXD),** Certification ID: 9573003	*eLearnSecurity*

Notable Projects

CVE Credits

https://cve.mitre.org

Reported

Disclosed and assisted in remediation of the following CVE IDs: CVE-2021-42258, CVE-2021-42344, CVE-2021-42345, CVE-2021-42346, CVE-2021-42571, CVE-2021-42572, CVE-2021-42573, CVE-2021-42741, CVE-2021-42742.

pwncat

github.com/calebstewart/pwncat

Creator — *Python, C, C#*

Full featured agentless C2 platform built on top of a basic shell providing stable interactive sessions as well as an extensive pluggable API for automated enumeration, persistence, privilege escalation, and report generation.

Katana

github.com/johnhammond/katana

Co-Creator — *Python*

Automated Capture the Flag (CTF) problem solver. Implements a multi-threaded problem identification and solution framework capable of automatically solving cyber security challenges from a variety of categories.

CTF4Hire

github.com/ctf4hire

Lead System Engineer, Challenge Developer — *Python, Kubernetes, C, Assembly, GKE*

Designed and implemented scalable automated event infrastructure utilizing Kubernetes on Google Cloud Platform supporting over 5000 simultaneous players with personally assigned challenge machines. Held events for multiple worldwide conferences and companies including HackerOne, BSidesBoston and GrimmCon.

StewieOS

github.com/calebstewart/stewieos

Creator — *x86 Assembly, C*

Demonstrated expertise in low-level software and hardware programming. Designed and implemented POSIX-like kernel for the x86 family of processors. Full multitasking support. Custom device drivers for common hardware as well as implementations of common userland utilities.

Education

U.S. Coast Guard Academy

New London, CT

B.S. In Electrical Engineering — *Jun 2012 - May 2016*