Jared Stemper

JaredAStemper@gmail.com
1.219.286.4440
/Jared-Stemper
/JaredStemper

Experience

Offensive Security Engineer
September 2024 – Present
TikTok USDS — *New York, NY*

- Conducted offensive security tests and assessments to identify vulnerabilities and misconfigurations, providing actionable recommendations to mitigate risks and improve security controls' effectiveness.
- Developed threat models for systems and controls, identifying potential threats and vulnerabilities, and prioritized remediation efforts based on criticality and impact.
- Utilized advanced penetration testing, red teaming, and threat detection techniques to simulate adversarial tactics and assess the robustness of protective, detective, and responsive security controls.
- Automated security testing and monitoring processes to enhance the efficiency and effectiveness of control assessments, ensuring continuous protection against evolving threats.

Offensive Cybersecurity Consultant
July 2021 – July 2024
RSM US LLP — *Chicago, IL*

- Performed **red team**, **physical penetration**, & **network** penetration testing as a technical lead of the close access and network exploitation teams.
- Mentored and led testing across **web application**, **LLM/AI** models, wireless network, social-engineering, cloud penetration testing, & configuration review assessments (AWS).
- Developed **Python** and **Tmux** automation framework to streamline **network penetration testing** organization & automating attacks; reducing start-up time by 85% for testers.
- Built modular scanner and reporting utility with **Python** and **Docker** to asynchronously run security tooling, including **AWS** configuration and code review, before consolidating output into standardized findings for reporting.
- Created a long-range **RFID** badge cloner using microcontroller devices with live credential reading through a **Raspberry Pi** wireless AP.
- Provided actionable remediation recommendations to client executives by delivering breach vector reports, enabling risk reduction & minimizing liability exposure for Fortune 10 technology companies, Fortune 500 financial institutions, & private clients.

Security Software Engineering Intern
May 2020 – Dec 2020
Synopsys — *Bloomington, IN*

- Automated AB-testing analysis through **Python** scripting report comparison, resulting in a 40% reduction in manager analysis time.
- Aggregated assessment data across Netsparker, AppScan, & **BurpSuite** through **Jira** & **PostgreSQL**, facilitating tracking of vulnerability trends.
- Designed & implemented an automated Tableau storyboard for senior managers & C-level to track trends across assessments.

Penetration Security Consulting Intern
Jun 2019 – Aug 2019
RSM US LLP — *Chicago, IL*

- Performed assisted network and web application penetration testing on client engagements.
- Developed Visual Basic macros & Python scripts for automating drafting/draft handling in Excel.
- Measured client compliance within NIST CSF assessments through direct communication with key stakeholders.

Undergraduate Instructor: Intro. to Python Programming
Sep 2018 – Jun 2020
Indiana University — *Bloomington, IN*

- Developed & maintained Python scripts to facilitate autograding of 200+ students.
- Led and assisted instruction for student groups of 20-45 through 55 exercises & labs regarding Python.

Education

B.A. in Computer Science
Aug 2017 – May 2021
Indiana University — *Bloomington, IN*

Relevant Courses: Data Structures, Machine Learning, Relational Databases, Networking, C and Unix, Discrete Mathematics, Linear Algebra

Technical Skills

Certifications: PNPT, SANS GPCS, CompTIA CySA+, AWS Certified Cloud Practitioner
Security: Red Team, Internal/External Network, Web Application, Physical, & Social Engineering Penetration Testing
Languages: C/C++, Python, SQL, JavaScript, HTML/CSS, Unix Bash
Miscellaneous: AWS, Docker, Containerization, Linux, Tenable Nessus, Forklift-certified, Cobalt Strike

Projects

Scylla 2023 - Present
- Orchestration and automation tool developed using Bash and Python to support efficient and consistent internal network penetration testing.

Charybdis 2023 - Present
- Asynchronously scan and ingest data for static code and cloud account configuration testing- spitting out human-readable, highly customizable reporting templates.

PassMasker 2024
- Analyze a list of passwords using novel bucket-sort implementation to improve computation by 40% and provide an analysis of the the passwords into a mask ingestible to hashcat.

Dockerized Metasploitable Lab 2021
- Developed a docker network connecting a Kali OS to a Metasploitable2 OS to facilitate pen testing practice.

Tor Browser Fingerprinting Research 2019
- Measured comparative data sets to determine Tor browser's anti-fingerprinting capabilities and develop an algorithm to bypass controls.

VOLUNTEERING

#HashtagLunchbag Volunteer 2022 - 2024

- Packed lunches to help prepare meals for Pacific Garden Mission homeless shelter.