

Jared Stemper

✉ JaredAStemper@gmail.com **in** [/Jared-Stemper](#)
☎ 1.219.286.4440 **o** [/JaredStemper](#)

EXPERIENCE

Offensive Security Engineer <i>TikTok USDS</i>	September 2024 – Present New York, NY
<ul style="list-style-type: none">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 <i>RSM US LLP</i>	July 2021 – July 2024 Chicago, IL
<ul style="list-style-type: none">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 <i>Synopsys</i>	May 2020 – Dec 2020 Bloomington, IN
<ul style="list-style-type: none">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 <i>RSM US LLP</i>	Jun 2019 – Aug 2019 Chicago, IL
<ul style="list-style-type: none">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 <i>Indiana University</i>	Sep 2018 – Jun 2020 Bloomington, IN
<ul style="list-style-type: none">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 <i>Indiana University</i>	Aug 2017 – May 2021 Bloomington, IN
<i>Relevant Courses: Data Structures, Machine Learning, Relational Databases, Networking, C and Unix, Discrete Mathematics, Linear Algebra</i>	

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
<ul style="list-style-type: none">Orchestration and automation tool developed using Bash and Python to support efficient and consistent internal network penetration testing.	
PassMasker	2024
<ul style="list-style-type: none">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.	
Tor Browser Fingerprinting Research	2019
<ul style="list-style-type: none">Measured comparative data sets to determine Tor browser's anti-fingerprinting capabilities and develop an algorithm to bypass controls.	

VOLUNTEERING

#HashtagLunchbag Volunteer	2022 – 2024
<ul style="list-style-type: none">Packed lunches to help prepare meals for Pacific Garden Mission homeless shelter.	