

Jack Trigg

Red Teamer, Active Public Trust Clearance

Tampa, FL | jacktrigg.com | jacktrigg00@gmail.com | linkedin.com/in/jtrigg | github.com/johntrigg

PROFESSIONAL SUMMARY

Ambitious, driven, and dependable cybersecurity professional with several years of relevant experience. Continuously seeking improvement and growth, from education, certification, and most importantly, hands-on practical real-world experience. Proven track record in streamlining and standardization of existing routines, playbooks, and workflows. Other interests include chess, piano, media analysis, and cooking.

AREAS OF EXPERTISE

- Incident Response
- Azure & AWS
- Kali Linux
- Metasploit
- Red Teaming
- Reporting & Technical Writing
- Mitre ATT&CK
- Docker
- OWASP Top 10
- Windows Defender XDR/EDR
- Burp Suite
- MSSQL/MySQL
- Python
- Vulnerability Remediation
- Bash
- PowerShell

PROFESSIONAL EXPERIENCE

Maveris

Red Team Operator, Remote

January 2025 - Ongoing

- Worked in a collaborative red team of over forty people, focusing on uncovering vulnerabilities within the Department of Veteran Affairs processes, technologies, and networks. Attack surface area was massive, with regular scanning, parsing, analysis, and exploitation of tens of thousands of endpoints, including extensive AWS, Azure,
- Accomplished objectives (finding how a threat actor could access veteran PII or PHI on a given system) every operational cycle, ahead of schedule.

University of South Florida

Graduate Research Assistant, Hybrid

January 2024 - January 2025

- Developing explainable AI models in Python to enhance the transparency and interpretability of malware classification processes.
- Led a project focused on industrial cybersecurity and cyber-physical systems (ICS/SCADA) to design and deliver educational materials, fostering a deeper understanding of these critical areas among students. Included **simulated phishing initial access** and **security testing of a power plant**. The project was estimated to reach **over a hundred students**.

Airline Tariff Publishing Co. (ATPCO),

Security Operations Analyst, Remote

June 2023 - August 2024

- **Coordinated with a team** on projects related to maintaining a strong information security posture for the company, with a **focus on vulnerability remediation, full-stack incident response, and systematic hardening**.
- Integrated a DevOps workflow by managing tasks through Jira tickets, driving progress with weekly sprints, and maintaining comprehensive documentation on Confluence.
- Led a campaign to fully implement Microsoft Authenticator 2FA, replacing SMS 2FA, by coordinating with multiple departments to communicate with **hundreds of targeted individuals**.
- Conducted a web application penetration test on a WordPress instance, uncovering **over 15 issues**, including 2 high-risk vulnerabilities. Worked with a team to remediate.
- Enabled the incident-response process. Worked in full-stack incident remediation, resolving over **120 high-priority incidents and alerts**. Notable incidents include **compromise of an AWS instance**, and an **attempted login to a honeytoken account**.

27 Virtual,

Enterprise Virtualization Automation Engineer, Remote

June 2022 - July 2023

- Developed PowerShell scripts utilizing VMWare's PowerCLI library that **automated the deployment, reversions, and cleanup** of up to 90 VMWare certification class lab kits, which consisted of several networked VMs. **Reduced the deployment times of lab kits by up to 70%** by reducing the need for manual oversight and involvement in the process.
- Revitalized the deployment process of environments through VMWare's virtualization suite, including vSphere, vCenter, and Horizon, that consisted of **100s** of virtual machines for VMWare education and certification classes.
- Tasked with the **validation and troubleshooting** of lab kits. Created accompanying documentation for finding, remediating, and preventing future errors.

EDUCATION & CERTIFICATIONS

Certified Red Team Operator (CRTO)

(Expected) March 2026

University of South Florida, Master's, Graduated with Honors

M.S. in Cybersecurity - May 2025

Offensive Security Certified Professional (OSCP)

September 2024

University of South Florida, Bachelor's, Graduated with Honors

B.S. in Cybersecurity - December 2023

TCM Security Practical Network Penetration Tester (PNPT)

October 2023

TCM Security Practical Junior Penetration Tester (PJPT)

September 2023

Hack The Box Genesis ProLab

September 2023

COMMUNITY INVOLVEMENT, COMPETITIONS, & PROJECTS

Home Lab Maintainer

Ongoing

- Designed a home lab hosted on **ProxMox** consisting of a **honeypot running Cowrie**, that recorded SSH logins, and let simulated attackers run commands in a virtualized environment, sending information to a server running **Wazuh EDR**. Other uses include a self-hosted Discord music bot, file storage server, and more.

Cybersecurity Guest Speaker - Broadcast Technology Exposium, SBE Chapter 39

November 2025

- Invited to give an hour-long **presentation and Q&A** about the **modern state of cybersecurity, best practices, developing/emerging trends**, and how to prepare for the future.

SouthEast Collegiate Penetration Testing Competition 10 (SECPTC 10)

November 2024

- Placed **2nd** by under 1%, qualifying for globals. Participated as **co-captain** in the South East Collegiate Penetration Testing Competition (SECPTC) 2024 in Augusta, Georgia, **leading team strategy and communication**, contributing to team's competitive performance against top institutions.
- **Spearheaded written proposal** for team's entry into SECPTC, **showcasing leadership in team coordination and strategic planning**, gained valuable experience in real-world penetration testing scenarios.
- Led and organized the report writing effort, the most critical phase of the competition.

Adversary Wars CTF @ DEFCON 32

August 2024

- Placed **2nd** in a CTF at DEFCON 32, out of 78 teams over 100 players. Challenges were mostly focused on **Web Exploitation, penetration testing, OSINT, threat intelligence, and forensics**.

USF CyberHerd Cybersecurity Competition Team

CPTC Co-Captain, Injects & Communication Captain, Red Team Teacher

June 2023 - June 2025

- Founding member and CPTC co-captain of the USF CyberHerd team. Attend weekly practices after work hours and on weekends to practice for cybersecurity competitions such as CCDC, CPTC, and CyberForce, and more.
- Particular focus on **handling injects, incident response, and handling business matters** in the context of a competition, such as writing full **penetration test reports** for CPTC, creating **incident response reports** for CCDC, and handling **presentations and injects for CCDC**. General focus in a versatile range of areas otherwise, such as **web exploitation, data forensics, and incident remediation**.