

Logan Goins

[REDACTED] | [REDACTED] | <https://linkedin.com/in/ljgoins> | [REDACTED]

SUMMARY

Offensive security practitioner with extensive experience in penetration-testing and security analytics. Passionate, motivated, client-centric, and a continuous learner. Thorough and strong methodological approach to penetration-testing, specializing in internal network testing, and Active Directory exploitation, with the ability to deliver effective and comprehensive reports to improve organizational security posture.

EXPERIENCE

Penetration Tester – Active Directory Exploitation Specialist - Global Finalist

August 2023-January 2024

Global Collegiate Penetration Testing Competition (CPTC) 9

- Improving technical teamwork and penetration testing skills through life-like simulated penetration testing engagements. Involving the proposal response to a Request for Proposal (RFP), a professional report, deliverables, injects, and simulated client interactions.
- Acquired skills regarding the practical exploitation of vulnerabilities on a variety of systems and infrastructure and how to report them effectively to the client.

CERTIFICATIONS

Offensive Security Certified Professional (OSCP)

Certified Red Team Operator (CRTO)

CompTIA Cybersecurity Analyst+ (CySA+)

CompTIA Security+

Expires: April 2026

Expires: April 2026

EDUCATION

Bachelor of Business Administration (BBA) in Cybersecurity (currently enrolled)

The University of Texas at San Antonio - San Antonio, TX

Organizations:

Computer Security Organization (CSA): Secretary – 350+ Members

CompTIA Student Chapter: Member

Console Cowboys: Member

PROJECTS

Development: HeadHunter. - <https://github.com/shellph1sh/HeadHunter>

HeadHunter is a Command & Control (C2) framework with asynchronous, beacon based encrypted communications along with custom agents and a server bundled agent generator with cross compilation capabilities.

- Demonstrated knowledge of custom offensive security tooling development and the C programming language through the creation of an encrypted C2 framework including compatible Windows and Linux agents.
- Demonstrated knowledge of red team operations and offensive security tooling

Development: Bypassing CrowdStrike Falcon with Cobalt strike

- Used ThreatCheck and Ghidra to identify flagged bytes in the Cobalt strike artifacts.
- Utilized the Cobalt strike Artifact Kit to manually modify key Cobalt strike utilities to bypass signature-based, and in memory detection, including a shellcode XOR decryption routine.
- Leveraged a custom malleable C2 profile to strip strings from compiled artifacts, and customized Beacon to better hide in memory.
- Modified a simple shellcode loader which bypasses static and sandbox-oriented detections for loading the Cobalt strike stager.

ACHIEVEMENTS

- CPTC Global Finalist @ CPTC9, New York
- 1st Place @ CPTC9 U.S. Central Regionals, Tennessee
- 3rd Place @ National SimSpace CyberCup Red Team Competition