Logan Goins

[REDACTED] | https://logan-goins.com | 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 Testing Intern (X-Force Red) May 2024-August 2024
IBM

- Participated in active IBM X-Force Red client engagements while working with the best offensive security professionals in the industry on a variety of assessment types, including web application security tests and internal network penetration tests.
- Attended bootcamps covering a variety of penetration-testing and offensive security topics including web application, internal network, external network, and mobile penetration testing taught by Sr. Penetration Testing Consultants.
- Performed active research into Microsoft Active Directory exploitation and built an accompanying custom and novel tool leveraging the impacket suite to assist in preforming Active Directory focused assessments.

CERTIFICATIONS

Offensive Security Certified Professional (OSCP)
Certified Red Team Operator (CRTO)
CompTIA Cybersecurity Analyst+ (CySA+) Expires: April 2026
CompTIA Security+ Expires: April 2026

EDUCATION

Bachelor of Business Administration (BBA) in Cybersecurity Expected Graduation: May 2026
The University of Texas at San Antonio - San Antonio, TX

PROJECTS

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.

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 an understanding of core C2 functionality

COMPETITIONS

Collegiate Penetration Testing Competition (CPTC 9)

- Achieved 1st place in the CPTC9 U.S. central region competition held at Tennessee Tech University
- Specialized in Active Directory exploitation and compromised a full-scale environment
- Created a detailed report detailing findings, business impact, and compliance violations for an executive audience.