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

- Worked in active IBM X-Force Red client assessments and learned from the best offensive security professionals in the industry on a variety of assessment types, including internal network and web application security tests.
- Attended practical and custom 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, then utilized that knowledge to assist in client assessments.
- Performed research into Active Directory underlying protocols and built an accompanying custom and novel tool to assist in preforming internal network assessments through a new method of enumeration.

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 - https://logan-goins.com/2024-02-03-CS/

- 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.

Lab Environment: Active Directory Certificate Services (AD CS) - A Beautifully Vulnerable and Mis-configurable Mess - https://logan-goins.com/2024-05-04-ADCS/

- Configured, explained, exploited, and documented a full-scale Active Directory environment focusing on Active Directory Certificate Services (ADCS) vulnerabilities ESC1-ESC14 originally discovered by SpecterOps.
- Understood and recreated ADCS misconfigurations and vulnerabilities on a Domain Controller (DC) and Certification Authority (CA) configuration level and created expansive documentation as a source for others to learn from.

COMPETITIONS

Collegiate Penetration Testing Competition (CPTC 9)

- Achieved 1st place in the CPTC9 U.S. central region competition held at Tennessee Tech University.
- Proceeded to the CPTC9 global competition in Rochester New York against the top 15 teams in the world.
- Specialized in Active Directory exploitation and compromised full-scale internal network environments.
- Created a detailed report covering findings, business impact, and compliance violations for an executive audience.