Logan Goins

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

SUMMARY

OSCP, CySA+, and Security+ certified student at UTSA with extensive practical experience in penetration-testing and offensive security. Client-centric and a continuous learner. Global Collegiate Penetration Testing Competition (CPTC) global finalist and regional champion, active member of the Cybersecurity community at UTSA through a multitude of organizations. Officer in the Computer Security Association (CSA), and creator of the HeadHunter Command & Control (C2) framework.

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

Relevant Coursework:
Unlocking Cyber: Cybersecurity case studies, hands-on labs, industry tools of the trade.
Programming Languages I with Scripting: Python Programming, Functions, IPO, Loops, OOPs, Recursion
Red Team Operations and Tactics: Red team mindset, best practices, and industry tools.

CERTIFICATIONS

Offensive Security Certified Professional (OSCP) December 2023
CompTIA Cybersecurity Analyst+ (CySA+) April 2023
CompTIA Security+ April 2023

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.

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.