Logan Goins

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

EXPERIENCE

Offensive Security Consultant Co-op (X-Force Red) May 2024 - Present
IBM

- Shadowed multiple internal network and web application assessments, gaining hands-on security testing expertise and improving vulnerability detection/communication skills.
- Engineered a novel solution for stealthy Active Directory enumeration. The project involved reversing and implementing eight protocol layers and authentication mechanisms from scratch, with plans to conduct a public release of the tooling for community contribution.
- Conducted extensive research and review of Windows protocol documentation, ensuring full interoperability with the Impacket suite.
- Conducted a research presentation to IBM Security and X-Force executives, while streamed to the entirety of the X-Force department.

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: Spring 2026
The University of Texas at San Antonio - San Antonio, TX

PROJECTS

Krueger: Windows Offensive Security Tooling –
https://github.com/logangoins/Krueger

- Designed a portable .NET application with the ability to remotely kill Endpoint Detection and Response (EDR) services on remote Windows hosts as apart of lateral movement procedures using weaponized Windows Defender Application Control (WDAC).
- Engineered a solution for portably installing the WDAC policy on a remote target when executed from memory. This was accomplished by embedding the policy inside of the executed .NET assembly.
- Utilized PInvoked Windows API calls to create custom authentication tokens and trigger remote shutdowns of target devices over Remote Procedure Call (RPC).

Cable: Active Directory Offensive Security Tooling –
https://github.com/logangoins/Cable

- Created a simple .NET application capable of interacting with Active Directory environments, with the intended use case of being executed in memory through a C2 channel.
- Developed custom methods for enumerating Active Directory Domain Services (ADDS), Active Directory Certificate Services (ADCS), Domain Controllers in the environment, and Domain/Forest Trust relationships.
- Engineered processes for exploiting Active Directory Discretionary Access Control List (DACL) focused attack vectors. This includes abusing write primitives on LDAP objects, such as the ability to write Resource-Based Constrained Delegation (RBCD).

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.
- Presented our findings and provided recommendations in a professional manner during a dedicated executive presentation.