Logan Goins

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

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/reporting skills.
- Engineered a novel solution for stealthy Active Directory enumeration. The project involved reversing and implementing eight protocol layers and authentication mechanisms from scratch.
- Delivered an internal presentation to X-Force and IBM Security executives.
- Released the tooling/research for community contribution: https://securityintelligence.com/x-force/stealthy-enumeration-of-active-directory-environments-through-adws/
- Contributed to internal network penetration testing methodology documentation.

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 in Cybersecurity Expected Graduation: Spring 2026
The University of Texas at San Antonio - San Antonio, TX
Activities:

- CPTC 2023-2024 Regional Champion and Global Finalist
- Computer Security Association (CSA) Competitions Coordinator
- National SimSpace Red Team Competition 3rd place
- UTSA RowdyCon KoTH 1st place and Panel Speaker

PROJECTS

SoaPy: Active Directory Offensive Security Tooling – https://github.com/xforcered/SoaPy

- Designed a custom solution and created associated tooling for stealthy interaction with LDAP through Active Directory Web Services (ADWS) intended be used from an internal Linux host through a proxy.
- Created numerous novel implementations of native Active Directory technologies for Linux to accomplish this, including but not limited to NMF (.NET Message Framing Protocol), NNS (.NET Negotiate Stream protocol), and NBFSE (.NET Binary Encoding Format: SOAP Extension).

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

- Implemented an operationally efficient way to perform account takeover on Active Directory objects through strong explicit certificate mapping.

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

- Designed a portable way to remotely kill Endpoint Detection and Response (EDR) services on remote Windows hosts for 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.

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

- 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).