

# Jonathan Beierle

[REDACTED] | [REDACTED] | [beierle.win](mailto:beierle.win) | [linkedin.com/in/Jonathan-beierle/](https://www.linkedin.com/in/Jonathan-beierle/)

## SUMMARY

Information security specialist with extensive experience in network security and incident response. Highly motivated, client-centric, and life-long learner. Exhaustive approach to security implementation and research, with the ability to deliver clear, concise, and detailed reports.

## EXPERIENCE

### Network Engineering Intern, HEB

Summer 2024, 2023, 2022 (8 months)

- Updated switch firmware to mitigate security vulnerabilities
- Contributed to several internally written network automation applications that were used to automatically shut down switchports and dynamically discover port profiles across 1000+ devices
- Ran audits on store infrastructure to maintain network performance, reliability, and security

### National SimSpace Cyber Cup

March 2024

- Used various security tools such as Elastic, Splunk, and Security Onion to detect and respond to a variety of threats including LSASS dumping, lateral movement, and C2 operations
- Responded and documented security incidents in a simulated enterprise network
- Coordinated with a team of 6 people to respond to various active threats

### Co-Captain, Department of Energy (DoE) CyberForce Competition

February 2024 - Present

- Detected and responded to various security incidents within a simulated network such as C2 operations, stored credential access, and data exfiltration
- Configured Active Directory environments to maximize security without compromising usability using utilities such as Group Policy Objects (GPOs), Windows Defender Application Control (WDAC), and Local Administrator Password Solution (LAPS)

### Infrastructure Lead, UTSA Cyber Competitions Lab

January 2024 - Present

- Created Group Policy Objects to harden an Active Directory network with 25 workstations and 4 hypervisors
- Assisted with the setup and security of laboratory equipment, including a domain controller, email server, four Proxmox hypervisors, and 25 Windows workstations

### Co-Captain, Collegiate Cyber Defense Competition (CCDC)

December 2023 - Present

- Competed in a simulated, high-stress competition to secure a network of devices against active adversaries while sustaining critical business operations
- Hardened and configured Microsoft Windows machines in an Active Directory environment using Group Policy, Registry modifications, and proper access controls
- Wrote extensive documentation regarding configuration of various Windows operating systems
- Coordinated with several specialized team members to effectively compete

### TracerFIRE Competition

November 2023

- Leveraged the ELK stack, Sysmon logs, and other methods of log aggregation to investigate a simulated cyber-attack against a fictitious organization
- Analyzed lateral movement in a network by simulated advanced persistent threats (APTs)

## CERTIFICATIONS

CompTIA Security+

Expires January 2027

CompTIA Network+

Expires January 2027

## EDUCATION

University of Texas at San Antonio (UTSA)

Expected Graduation: December 2025

Bachelor of Science in Computer Science

GPA: 3.96

## PROJECTS

Windows Hardening Research: [github.com/HullaBrian/Windows-Hardening](https://github.com/HullaBrian/Windows-Hardening)

March 2024 - Present

- Research and documentation on Windows security – including GPOS, Windows Defender Application Control (WDAC), and Sysmon.

HashScout: [github.com/HullaBrian/HashScout](https://github.com/HullaBrian/HashScout)

June 2024

- Python application to recursively hash every file in a directory or .zip for use in forensics investigations