Jonathan Beierle

jonathan@beierle.win | beierle.win | linkedin.com/in/Jonathan-beierle/

EXPERIENCE

X-Force Threat Intelligence Malware Reverse Engineering Intern, IBM — May 2025 – August 2025

- Wrote YARA rules to identify and track malware ingested from various feeds and incident response investigations
- Created Python-based malware configuration parsers using static and dynamic extraction utilities such as MWCP, Dragodis, and x64Dbg to automatically extract crucial information and provide actionable intelligence to clients
- Investigated several popular open source CobaltStrike UDRLs including AceLdr, ElusiveMice, and BokuLoader
- Produced high level reports for clients that communicated key findings from malware investigations
- Prepared an executive-level presentation that explains complex technical concepts at an accessible level

Network Engineering Intern, HEB — Summers 2022 - 2024 (8 months)

- Wrote several Python-based network automation applications that were used to automatically shut down switchports and dynamically discover port profiles across 1000+ devices
- Analyzed data-center network traffic to evaluate the fail-over time of various networking devices
- Updated switch firmware to mitigate security vulnerabilities identified in threat intelligence publications

ACTIVITIES

Co-Captain, Collegiate Cyber Defense Competition (CCDC) — December 2023 – March 2025

- Competed 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 Microsoft security baselines, Group Policy, Registry modifications, and proper access controls
- Wrote documentation and PowerShell scripts regarding the configuration and security of Windows systems
- Coled a team of 8 people that achieved 3rd place in the Southwest CCDC regional competition

National SimSpace Cyber Cup — March 2024, March 2025

- 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
- Identified TTPs to track adversarial activity across a simulated enterprise environment
- Coordinated with a team of 6 people to detect and respond to various active threats

Co-Captain, Department of Energy (DoE) CyberForce Competition — February 2024 – November 2024

- Responded to 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) and Windows Defender Application Control (WDAC)

Infrastructure Lead, UTSA Cyber Competitions Lab — January 2024 – December 2024

- Directed a team of 8 people to coordinate infrastructure development and maintenance
- Assisted with the setup and security of laboratory equipment, including a domain controller, email server, four Proxmox hypervisors, and 25 Windows workstations

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: 3.98

PROJECTS

COMmander: github.com/HullaBrian/COMmander — May 2025 – June 2025

- .NET tool that uses ETW to monitor for suspicious RPC and COM based activity based on a configurable ruleset
- Detects attacks such as PetitPotam, DCSync, and remote SAM dumping in real-time

Krueger: beierle.win/2024-12-20-Weaponizing-WDAC-Killing-the-Dreams-of-EDR/ — December 2024

- Novel research detailing the use of WDAC to remotely disable EDR drivers and services
- Used YARA signatures and Group Policy to provide and recommend detections and mitigations