ERIC ESQUIVEL

Email: redacted@redacted.com | Website: ericesquivel.github.io | LinkedIn: linkedin.com/in/ericesquivel1

EXPERIENCE

AnaVation LLC - Vulnerability Research Intern May 2024 - August 2024

- Developed a Python script using Ghidra's API to disassemble portable executables and collect code complexity metrics; Utilized PyGraphviz to display execution and function call graphs
- Assisted vulnerability researchers in identifying execution flow and potentially high-risk code based on user input test cases
- Built a Docker image featuring a user-friendly frontend that orchestrates all developed tools, enabling users to easily upload binaries for analysis and download output graphs and metrics files.

Security Researcher February 2024 - Present

- Identified improper input sanitization in a Microsoft web application leading to Stored XSS and CSRF affecting millions of users through account takeover
- Documented and reported vulnerability to Microsoft's Bug Bounty Program which led to patching of the vulnerability and recognition on Microsoft's Online Services Acknowledgement page

CERTIFICATIONS

- Certified Red Team Lead (CRTL) [in-progress]
- Certified Red Team Operator (CRTO)
- Practical Network Penetration Tester (PNPT)
- CompTIA Security+

PROJECTS

Active Directory Blog: "The Last Kerberos Read You'll Ever Need" - https://ericesquivel.github.io/posts/kerberos

- Documented, explained, and exploited Microsoft's Kerberos authentication protocol focusing on the steps and details of the protocol
- Demonstrated nearly 20 attacks including variations for different scenarios from both Linux and Windows tools and how they work to help others learn more about Active Directory exploitation

OpsLoader: Cobalt Strike Aggressor Script & Custom Shellcode Loader - https://github.com/EricEsquivel/OpsLoader

- Created a shellcode loader in C that utilizes multiple techniques such as PPID/directory/argument spoofing and Early Bird APC Injection, to fully bypass current Microsoft Defender with Cloud Delivered Protection
- Developed an Aggressor Script which registers a new lateral movement command in Cobalt Strike to automatically place beacon shellcode into the loader, compile and upload it to the target, then execute it

Red Team Operations & Detection Homelab

- Deployed a vulnerable "Game of Active Directory" lab with Elastic in Proxmox to gather in-depth insights on the tactics, techniques, and procedures (TTPs) of various security tools such as Cobalt Strike, and the Impacket suite.
- Documented the behavior of these tools, focusing on understanding their operations under the hood and enhancing detection evasion strategies.

HackTheBox Zephyr Professional Lab

- Conducted a network penetration test for the Zephyr Professional Lab on HackTheBox simulating a realistic corporate environment
- Enumerated and abused Active Directory misconfigurations and vulnerabilities in the network, as well as bypassing Windows Defender and network firewalls to compromise entire domains and pivot to other forests

EDUCATION

The University of Texas at San Antonio Expected Graduation: May 2026

Bachelor's of Business Administration: Cyber Security Honors Student, GPA 3.92

- Led Security+ study groups, conducted technical presentations, and hosted CTF competitions

COMPETITIONS

National Cyber League, Collegiate Cyber Defense Competition, CyberForce, HiveStorm, TracerFIRE, SimSpace