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

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

- Zero-Point Security Certified Red Team Operator (CRTO) 2024
- TCM-Security Practical Network Penetration Tester (PNPT) 2024
- CompTIA A+ 2023
- CompTIA Security+ 2022

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

Cobalt Strike Aggressor Script

- Created an Aggressor Script which registers a new lateral movement command in Cobalt Strike to upload a stageless Beacon to the target and execute it
- Created additional quality of life features using Aggressor Script to aid in operations

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

Penetration Testing Homelab

- Setup homelab using PfSense, layer 3 switch, WireGuard VPN, and Proxmox server hosting a vulnerable "Game of Active Directory" environment to practice AD attacks, C2 frameworks, and Microsoft Defender AV evasion

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

EXTRACURRICULARS

Competed in: National Cyber League, Collegiate Cyber Defense Competition, CyberForce, HiveStorm, TracerFIRE, SimSpace competitions