ERIC ESQUIVEL

redacted@redacted.com | ericesquivel.github.io | 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
- 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

Microsoft Bug Bounty February 2024

- Identified improper input sanitization causing Stored XSS and CSRF, risking account takeover for millions of users.
- Received 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

Bypassing CrowdStrike Falcon & Microsoft Defender for Endpoint EDR

- Developed a shellcode loader in C utilizing multiple techniques to fully bypass CrowdStrike Falcon and Microsoft Defender for Endpoint (MDE) to load Havoc C2 shellcode and execute commands
- Utilized Indirect Syscalls, DLL unhooking, anti-sandbox, drip allocation, custom implementations for common functions, RC4 decryption with SystemFunction032, and removed unnecessary imports from the IAT

Cobalt Strike Aggressor Script - github.com/EricEsquivel/OpsLoader

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

Red Team Operations & Detection Homelab

- Deployed an Active Directory lab with Elastic in Proxmox to gather in-depth insights into 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

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

- Documented, explained, and exploited Microsoft's Kerberos authentication protocol and detailed it in depth
- Demonstrated nearly 20 attacks including variations for different scenarios from both Linux and Windows tools

HackTheBox Zephyr Professional Lab

- Conducted a network penetration test for the Zephyr Professional Lab simulating a 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

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

EXTRACURRICULARS

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