JULIAN PEÑA

[redacted] | [redacted] | [redacted]| linkedin.com/in/julian-pena/

RELEVANT EXPERIENCE

CrowdStrike

Security Engineer Intern Jun. 2024 – Present

- Spearheaded the development of novel detections surrounding identity attacks and abuse of Active Directory Certificate Services (AD CS), Microsoft System Center Configuration Manager (SCCM), and MS Exchange Online
- Introduced a previously untested exploitation technique to the internal red team, resulting in a high-severity penetration test finding and driving new detection engineering efforts
- Briefed incident response leadership on tracked eCrime actor TTPs, the current state of detection coverage, and strategies to improve detections

Booz Allen Hamilton

Red Team Operator Intern Feb. 2023 – Aug. 2023

- Built custom shellcode loaders and post-exploitation tools to evade various commercial AV/EDR products
- Utilized C2 frameworks including Cobalt Strike and Mythic on red team engagements
- Utilized SpecterOps' GhostWriter tool to track clients, projects, assets and findings, and leveraged the automatic reporting features to reduce team workload

Cyber Intelligence Analyst Intern Jun. 2022 – Jun. 2024

- Reverse engineered malware samples from APT groups to accurately emulate real adversaries for incident response training sessions
- Developed execution plans for incident response training, outlining various TTPs/IOCs and the timeline of execution to improve client detections of attacks in simulated corporate environments
- Deployed a custom vulnerable Active Directory lab with AWS to train fellow interns on initial access and post-exploitation strategies

Clear Tech LLC

Security Control Assessor Intern Nov. 2021 – Jun. 2022

- Implemented NIST controls and maintained documents certifying compliance with NIST SP 800-171r2/800-171a
- Deployed and maintained Identity and Access Management systems to include Multi-Factor Authentication (MFA) and Role Based Access Control (RBAC) controls
- Researched Azure Active Directory from an offensive-security standpoint and mitigated attack vectors regarding the abuse of default configurations
- Created and managed Azure AD InTune and Conditional Access Policies according to DISA STIGs and CIS Benchmarks for device compliance

LICENSES AND CERTIFICATIONS

- Zero-Point Security: Certified Red Team Operator (CRTO) Obtained: Apr. 2024
- Offensive Security Certified Professional (OSCP) Obtained: Oct. 2021

EDUCATION

University of Texas at San Antonio, San Antonio, TX Expected Graduation: May, 2026

Bachelor of Science, Computer Science

ACHIEVEMENTS

- 2023-2024: Collegiate Penetration Testing Competition (CPTC): Central Region Champion (1st Place)
- 2023: Cal Poly Pomona SWIFT: King of The Hill (KoTH) (1st Place)
- 2023: Collegiate Cyber Defense Competition (CCDC): Southwest Regionals (3rd Place)
- 2022-2023: Collegiate Penetration Testing Competition (CPTC): Global Finalist