Cesar Vaca

contact@cesarspace.online | LinkedIn | cesarspace.online

Education & Certifications

University of Maryland
Bachelor of Science in Cybersecurity Technology
Certifications
Pentest+, *Security+*, *SSCP*, *Network+*, *Linux Essentials*, *Cloud+*, *AWS Certified Cloud Practitioner*

Employment History

Empowered IT Solutions – Poway, CA — *Sep 2023 – Present*
United States Space Force – Schriever Space Force Base, CO — *Oct 2021 – June 2023*
United States Air Force – Beale Air Force Base, CA — *Apr 2019 – Oct 2021*

Experience

Recon & Enumeration

- Performed authenticated and external vulnerability scans across Linux and Windows hosts using Nessus and OpenVAS, validating exposed ports through a SonicWall firewall with Nmap
- Enumerated Active Directory services (SMB, RPC, LDAP, Kerberos, DCE/RPC) with enum4linux-ng and Nmap NSE, confirming anonymous null-session access and extracting the domain SID and OS details
- Profiled wireless targets (SSIDs, BSSIDs, channels, encryption) using a Flipper Zero with an ESP32 Marauder board to scope capture and deauthentication activity
- Operated primarily from Kali Linux, working across Nmap, Wireshark, Burp Suite, Impacket, Aircrack-ng, enum4linux-ng, and kerbrute

Pentesting & Red Teaming

- Executed an Active Directory attack chain: enumerated usernames with kerbrute, tested for AS-REP roasting via Impacket, and identified LDAP signing misconfigurations as NTLM relay preconditions
- Captured WPA2 handshakes and PMKIDs to .pcap by forcing client reconnection with deauthentication (Flipper Zero / ESP32), then cracked the pre-shared keys offline using Aircrack-ng wordlist attacks
- Tested web applications and APIs with Burp Suite, confirming an SSRF via an attacker-controlled callback listener and identifying broken object-level authorization by comparing low-privilege and admin accounts
- Cloned HID Prox (T5577) badges and recovered MIFARE Classic keys with MFKey32 to emulate a multi-technology access fob
- Defined engagement scope and authored technical and executive-summary reports documenting findings, impact analysis, remediations, and detection gaps observed during testing

Scripting, Programming, & Dev Ops

- Built an agentic AI vulnerability-assessment tool (Python, Claude Agent SDK) that runs scoped scans against a single target or full subnet and auto-generates findings reports
- Enforced tool allow-listing and IP-scope validation so the agent only executes approved tools against authorized targets, with encrypted storage for scan data and secrets
- Deployed the agent as a managed background service (start-on-boot, auto-restart on failure), version-controlled with Git across iterations
- Automated security and IT workflows in PowerShell, Bash, and Python, and implemented AES-GCM encryption in JavaScript via the Web Crypto API