Jean Romero

San Antonio, TX | Open to Relocation | (786) 861-6985
jeanralvarez212@gmail.com jean-carlos-romero JeanRA88 heretek.dev HTB: Jean8895 (Top 3%)

Summary

OSCP+ certified penetration tester focused on Active Directory and internal-network attacks — Top 3% on HackTheBox (49+ machines rooted across HTB, TryHackMe, and OffSec PG) and a delivered internal-network pentest with a CVSS-scored report. Backed by Tier 2 SOC experience at a critical-infrastructure utility for a detection-aware offensive approach.

Certifications

- OSCP+ — OffSec Certified Professional+ (OffSec, 2026)
- eCPPT — Certified Professional Penetration Tester (INE, 2026)
- OffSec AD Pentest Skill Path • MITRE ATT&CK: Lateral Movement (OffSec, 2026)
- CEH v12 — EC-Council (2025) • eJPT — INE (2025) • CompTIA Security+ (2025) • ISC2 CC (2025)

Technical Skills

Penetration Testing: Network & Web App Pentesting, Vulnerability Assessment, Report Writing, Ethical Hacking
Offensive Tools: Burp Suite, Metasploit, Nmap, BloodHound, Hydra, Wireshark, John the Ripper, SQLMap, Gobuster, Responder
Attack Techniques: AD Attacks (Kerberoasting, DCSync, AS-REP), Privilege Escalation, Lateral Movement, Pivoting & Tunneling, Credential Harvesting, AV Evasion, SQLi, XSS
Defensive / SIEM: Microsoft Sentinel (KQL), Defender for Endpoint, Live Response, MITRE ATT&CK, ServiceNow, ICS/OT Monitoring, NERC CIP
Methodologies: OWASP Top 10, MITRE ATT&CK, PTES, NIST, Cyber Kill Chain
Scripting & Environments: Python, Bash, KQL, Git; Kali Linux, Windows Server, Active Directory, Docker, VirtualBox

Experience

Blackswan Cybersecurity, LLC **Jul 2025 – Present**
SOC Analyst II — Tier 2 (Client: CPS Energy) *San Antonio, TX*

- Defended ~8,000 IT/OT/ICS assets at a critical-infrastructure electric and gas utility, triaging 10–20 escalated alerts daily with zero critical misses across assigned shifts.
- Performed Tier 2 investigation and escalation in Microsoft Sentinel (KQL), Defender for Endpoint, and Live Response, mapping adversary activity to MITRE ATT&CK and refining detection playbooks to streamline triage.
- Led a 3-analyst team as night-shift lead, owning incident triage across overnight coverage before transitioning to day shift.
- Maintained NERC CIP compliance documentation and audit readiness through structured evidence collection and incident tracking in ServiceNow.

Projects & Labs

Internal Network Penetration Test — Blackswan Cybersecurity | *Scoped client engagement* **2025**

- Executed the full attack lifecycle — reconnaissance, enumeration, exploitation, and privilege escalation — against in-scope hosts and network services using Nmap and Metasploit, within defined rules of engagement.
- Surfaced 7 vulnerabilities (1 critical, 6 high) and authored a CVSS-scored professional report with an executive summary and prioritized remediation.

Penetration Testing Labs & Research | *HackTheBox · TryHackMe · OffSec PG* **Jan 2024 – Present**

- Rooted 49+ machines across HackTheBox (Top 3% globally), TryHackMe, and OffSec Proving Grounds, with a focus on Active Directory attack paths — Kerberoasting, DCSync, BloodHound, and lateral movement.
- Completed OffSec PEN-200 (OSCP+): pivoting, buffer overflows, client-side attacks, and antivirus evasion in enterprise lab environments.

Education & Training

OffSec — PEN-200 (OSCP+ Curriculum) **2026**
Penetration Testing with Kali Linux — OSCP+ exam earned