James Hasewinkle

Senior Penetration Tester

San Antonio, Texas | Phone: 210.364.7546 | Email: jhasewinkle@proton.me
Website: https://www.linkedin.com/in/james-hasewinkle-194988116/

Summary

Senior Offensive Security Consultant with 5+ years of experience conducting internal/external, web, mobile, cloud, and physical penetration tests across enterprise, industrial, retail, and commercial environments. Specializes in adversary emulation, social engineering, mobile testing, and covert physical intrusion. Skilled in Windows, Linux, Active Directory, AWS/Azure, and full-stack exploitation. Known for clear technical writing, client communication, and delivering high-impact red team engagements from planning to executive reporting.

Experience

Senior Penetration Tester — Zyston LLC — Dallas, TX | Dec 2020 – November 2025

- Led and executed 100+ offensive security engagements including internal/external infrastructure tests, cloud assessments, web/mobile testing, and full red-team operations.
- Performed high-impact physical penetration tests (badge cloning, lock bypass, tailgating, covert camera access, and alarm evasion) for industrial, retail, and corporate environments.
- Built internal frameworks for external attack surface mapping, phishing infrastructure, and repeatable red team tradecraft.
- Conducted complex Active Directory attacks including Kerberoasting, AS-REP Roasting, constrained delegation abuse, and lateral movement using Cobalt Strike, Sliver, and Impacket tooling.
- Delivered spear-phishing and multi-stage SE campaigns achieving high credential-capture rates; executed BEC/BPC-style attacks for business process compromise evaluations.
- Identified critical vulnerabilities including RCE, authentication bypass, broken access control, SSRF, SQLi, deserialization flaws, cloud IAM escalation paths, and insecure mobile API behavior.
- Drafted detailed technical reports and executive summaries, translating highly technical findings into clear recommendations for engineering teams and C-suite leadership.
- Mentored junior analysts and shaped internal testing standards, methodology, and documentation processes.

Cyber Security Analyst — Zyston LLC — Dallas, TX | Jan 2019 – Dec 2020

- Investigated and triaged security incidents using SIEMs including Splunk, QRadar, and AlienVault.
- Analyzed host-based telemetry from CrowdStrike Falcon, Carbon Black, and Sumo.
- Performed threat hunting activities, wrote intelligence briefs, and assisted incident response cases.
- Trained new analysts on triage methodology, detection logic, and attacker behavior patterns.

Cyber Security Intern — Decypher Tech Ltd. — San Antonio, TX | Summer 2016

- Assisted with web, internal, and external penetration tests across multiple industries.
- Documented findings in Dradis and produced testing narratives for IT departments and executives.
- Supported log aggregation and incident response using an ELK stack during a breach investigation.

Tools & Technologies

Cobalt Strike • Sliver • Burp Suite Pro • CrackMapExec / NetExec • Impacket
Evil-WinRM • Responder • ntlmrelayx • BloodHound • Go
Nmap • Nuclei • ffuf • Amass • Gobuster • OSINT frameworks
AWS CLI • PACU • MicroBurst • ScoutSuite • AzureHound • PowerZure
Python • Bash • PowerShell • Git • Dradis • AttackForge • Plextrac

Projects & Research

- Building an extended-range antenna for RFID badge cloning for the Proxmark3
- Writing a long-form research series on psychological principles of phishing
- Active in local San Antonio and Austin hacker meetups (AHA, SAHA, B-Sides)
- Co-presented at B-Sides Toronto on Business Process Compromise methodologies.

Education

University of Texas at San Antonio | Bachelor of Arts in Psychology – Minor in Cyber Security - Dec 2018