

# DEREK MARTIN

Red Team Operator | Offensive Security Engineer

Berkeley, CA 510-981-9531 derekmartinsf@gmail.com [linkedin.com/in/derekmartinoscp](https://www.linkedin.com/in/derekmartinoscp)

## PROFILE

Offensive security professional with 3+ years of red team and penetration testing experience and 8+ years in software engineering. Specializing in adversary simulation, network/web application pentesting, and social engineering at a Tier 1 global investment bank. Builds custom offensive tooling in Python, PowerShell, Go, and JavaScript. OSCP+, CISSP, and CPTS certified.

## CERTIFICATIONS

OSCP+ | CISSP | CPTS (Certified Penetration Testing Specialist) | ISC2 Cybersecurity | CPA

## CORE COMPETENCIES

**OFFENSIVE** Red Team Engagements · Adversary Simulation (MITRE ATT&CK) · Network & Web App Pentesting · Social Engineering · AD Attacks · C2 Infrastructure · Privilege Escalation · Phishing Campaigns · Lateral Movement · EDR/AV Evasion  
**TECHNICAL** Python · PowerShell · Go · Node.js · Bash · Solidity · Cobalt Strike · Metasploit · Burp Suite · BloodHound · Ghidra · Nmap · Wireshark · SIEM · Terraform  
**FRAMEWORKS** OWASP Top 10 · PTES · NIST · ISO 27001 · CIS Controls · Smart Contract Auditing · Secure Code Review · Threat Modeling

## EXPERIENCE

**Red Team Analyst**, BNP Paribas CIB — Montreal, QC Nov 2023 – Present

- Design and execute full-scope red team engagements simulating APTs against enterprise infrastructure of a Tier 1 global investment bank
- Conduct network, web application, and Active Directory penetration tests; identify critical attack paths to domain compromise
- Develop custom offensive tooling in Python, PowerShell, and Go for payload delivery, C2 communication, and defense evasion
- Execute social engineering campaigns including phishing, vishing, and physical security assessments to test human-layer defenses
- Map adversary TTPs to MITRE ATT&CK framework; collaborate with blue team and SOC to improve detection and response capabilities
- Integrate LLM-assisted automation into reconnaissance and vulnerability triage workflows, reducing manual effort by ~30%
- Produce executive-level engagement reports translating complex attack chains into business risk and prioritized remediation roadmaps
- Assess and evade EDR, SIEM, and network monitoring controls to validate detection coverage gaps across the enterprise

**Red/Offensive Operations Analyst**, CyVault™ — Montreal, QC Jan – Oct 2023

- Performed external and internal penetration tests across client network infrastructure, web applications, and wireless networks
- Conducted secure code reviews using static and dynamic analysis tools to identify vulnerabilities in client software
- Authored detailed findings reports with CVSS-scored vulnerabilities and remediation guidance aligned to NIST and ISO 27001
- Supported SOC operations including incident response, threat hunting, and security event analysis during concurrent engagements
- Assessed firewall rules, IDS/IPS configurations, and network segmentation controls; recommended hardening measures to reduce attack surface
- Built Python-based recon and vulnerability scanning scripts targeting bug bounty programs, uncovering sensitive data exposures and misconfigurations

**Director, Ad Technology**, Metric Theory — San Francisco, CA Jan 2018 – May 2022

- Led 3-person engineering team building API integrations, ETL pipelines (BigQuery), and internal tooling serving 180+ clients and \$157MM+ in managed spend
- Authored JavaScript API integrations from scratch for 10+ advertising platforms (Google, Facebook, Amazon, LinkedIn, Bing, DV360)
- Implemented version control (Bitbucket) and secure development practices to protect agency intellectual property
- Developed automated Slack-integrated monitoring, budget alerting, and reporting tools using Python and Google Apps Script

## EARLIER CAREER

Software Engineer, Noteable (2022) · Sr. Account Manager, 3Q Digital (2017) · SEM Manager, CreativeLive (2016–2017) · SEM Manager, Ask.com (2015–2016) · PPC Account Manager, Wpromote (2014–2015) · Senior Accountant, SBE Entertainment (2013–2014) · Property Accountant, Macerich (2011–2013) · Audit Associate, PwC (2005–2007)

## EDUCATION & TRAINING

**Villanova University** — B.S. Accounting & B.S. Finance 2002 – 2006

Hack The Box: 25+ challenges completed (SQLi, XSS, CSRF, JWT forgery, MITM, reverse engineering) · HTB Academy Pentester Track · MLExpert Certificate · Cybrary.it Offensive Security Coursework