Francis J. Kim

Fkim39@gmail.com • (443) 980-0847 • www.linkedin.com/in/franciskim-cybersecurity

KEY SKILLS

- Offensive Security Engineering (adversary emulation, OPSEC, payload development, C2: Cobalt Strike)
- Red Teaming (Kerberoasting, AS-REP roasting, constrained and resource-based delegation, AD CS abuse, DCSync, pass-the-ticket and pass-the-hash, lateral movement)
- Social Engineering (Evilginx2, GuardPhish, Gophish, MFA interception techniques, phishlets, landing pages, SPF and DKIM and DMARC readiness)
- Web and API Security (Burp Suite)
- Cloud and Container (AWS, Azure, GCP, IAM privilege escalation, metadata services, role assumption, Docker, Kubernetes RBAC and workload abuse)
- Network and Mobile (Wireshark, Responder, Impacket and CrackMapExec, NTLM relay, Frida)
- Programming and Scripting (Python, PowerShell, Bash, SQL, automation for data reduction and report-ready outputs)
- Vulnerability Management and SIEM (Tenable Nessus, Qualys VMDR and Policy Compliance, Splunk, CVSS scoring, POA&M tracking)

CERTIFICATIONS

OSCP, Security+

PROFESSIONAL EXPERIENCE

Schellman *11/2024 – Present*

Penetration Tester, Cybersecurity Consultant

- Performed internal and assumed breach, cloud across AWS and Azure and GCP, external network, mobile on iOS and Android, client-side, and web application testing; delivered FedRAMP and PCI tests for compliance.
- Applied exploit development, privilege escalation, lateral movement, and evasion techniques to simulate real-world attacks.
- Led threat modeling and attack surface analysis to identify weaknesses for FedRAMP compliance.
- Executed red team operations using social engineering, OSINT, and adversary emulation to assess resilience.

- Reviewed source code in Python, Java, JavaScript, and C# to identify security flaws.
- Produced detailed reports with remediation guidance and risk ratings for technical and executive stakeholders.

Deloitte *08/2022 – 11/2024*

Cybersecurity Engineering Consultant

Security Architecture and Engineering (SAE)

- Aligned IRS secure SDLC workflows with Zero Trust Maturity Model; embedded security in each GitLab CI/CD stage.
- Improved deployment efficiency by 250% by automating GitLab pipelines and deploying immutable workloads on OpenShift and Kubernetes.
- Authored a hardening playbook for DevSecOps integrating SAST, DAST, API security testing, adversarial testing, and data validation.

Stakeholder Enterprise Cybersecurity Enterprise Risk Evaluation (SECURE)

- Drove vulnerability management for IRS systems using Tenable Nessus, Qualys, Guardium, BigFix, and Splunk across 500+ web applications and 50,000+ weekly vulnerabilities.
- Coordinated with 100+ stakeholders weekly to communicate assessments and facilitate remediation of Filing Season vulnerabilities.
- Built Python scripts to transform vulnerability data into actionable and tracked outputs (POA&M and RBD and RAFT) and to compute risk using CVSS.

National Security Agency *12/2021–05/2022*

Security Researcher

- Contributed to OpenC2 cloud language specification on AWS and Azure using JSON and YAML to enable near real time response to security events.
- Integrated three OpenC2 actuators on AWS to automate attack detection such as cryptojacking and brute force with over 90% success; included in an NSA publication.

EDUCATION

University of Maryland, Honors College — B.S.; ACES (Advanced Cybersecurity Experience for Students)