

# Kayvon Karimi

Folsom, CA 95630 | Portfolio: [cyberbykayvon.com](https://cyberbykayvon.com) | Email: [cyberbykayvon@gmail.com](mailto:cyberbykayvon@gmail.com) | [LinkedIn](#) | [GitHub](#)

## Professional Statement

---

Detail-oriented Cybersecurity professional completing a Master's in Cybersecurity Engineering with a foundation in penetration testing, network defense, and digital forensics. Skilled in network security, vulnerability assessment, security operations, and risk management. Completed a Cyber Security Pre-Apprenticeship program, further strengthening expertise in SIEM tools, cloud security, and governance frameworks. Passionate about securing systems, protecting sensitive data, and contributing to resilient cybersecurity teams.

## Skills

---

- **Core Technical Skills:** Network & Web App Exploitation, Vulnerability & Penetration Testing, Server Hardening, Digital Forensics, Incident Response, Packet Analysis, Traffic Decryption, Bash/Python Scripting, Linux & Windows Administration, Cloud Security, Firewall/VPN Management, Log & Threat Analysis, Proxy Interception & Redirection
- **Offensive Security & Exploitation Tools:** Wireshark, Burp Suite, Nmap, Metasploit, SQLmap, FFUF, Gobuster, Hydra, Aircrack-ng, Airmo-ng, Hashcat, John the Ripper, Reaver, WebGoat, Selenium, OpenVAS, Nessus
- **Defensive Security & Monitoring Tools:** Wazuh, Splunk, Security Onion, Snort, tcpdump, PowerShell, CMD, ELK Stack (Elasticsearch, Logstash, Kibana), Autopsy, Volatility, Regripper, FTK Imager
- **Cloud, Containerization, and Virtualization:** AWS (EC2, S3, IAM, Security Groups), Azure Basics, Docker, Kubernetes, VirtualBox, Pi-hole, WireGuard, Tailscale
- **Web & Application Security:** Burp Suite, OWASP ZAP, OpenSSL, Apache2 HTTPS, PKI, TLS/SSL, X.509, Diffie-Hellman, Puttygen, Certificate Authority (CA) Configuration, WordPress Hardening
- **Systems Administration:** Linux (Debian/Ubuntu), Windows Server, Active Directory, Group Policy, RDP, Local Security Policy, iptables, Cpanel, Pycharm
- **Frameworks, Standards & Compliance:** NIST 800-53, MITRE ATT&CK, OWASP Top 10, CVE/CVSS, CIS Benchmarks, DISA STIGs, ISO 27001, SOC 2

## Education

---

### University of San Diego

**Dec 2025**

*Master of Science, Cybersecurity Engineering (GPA: 4.00)*

*San Diego, CA*

- **Achievements:** Advanced research and applied engineering

### Texas A&M University

**May 2012**

*Bachelor of Arts, Psychology, Minor in Business Administration (GPA: 3.4)*

*College Station, TX*

- **Achievements:** Men's D1 tennis team

## Certifications & Training

---

- **Cyber Proud: Cybersecurity Pre-Apprenticeship Program:** May 2025
  - \*Completed cybersecurity training in computer fundamentals, cryptography, cloud security, focused on security operations and vulnerability management.
  - \*Gained hands-on experience with Windows/Linux, Active Directory, PowerShell, AWS, Docker, and Kubernetes.
  - \*Developed practical skills in penetration testing, vulnerability assessments, network exploitation, SIEM tools, and IDS/IPS.
  - \*Proficient in securing sensitive data, configuring proxy servers, and managing firewalls and VPNs.
- **CompTIA Security+:** December 2025
- **Google: Foundations of Cybersecurity:** August 2023
- **Harvard: VPAL Cybersecurity - Managing Risk in the Information Age:** July 2023

## Cyber Security Projects

---

## Internal Penetration Test | Active Directory & Network Exploitation | [Report](#)

Sep 2025 - Oct 2025

### *Design World*

- Simulated full-scope internal penetration test targeting AD and segmented enterprise hosts.
- Exploited SMBv1 vulnerabilities (MS17-010/EternalBlue) to demonstrate remote code execution and lateral movement.
- Detected weak SSL/TLS cipher suites (SWEET32, RC4) and advised cryptographic hardening.

## Internal Web Application Vulnerability Assessment | eCommerce Platform | [Report](#)

Jul 2024 - Aug 2025

### *Court Crate*

- Performed network reconnaissance and service enumeration using Nmap (SYN stealth scans, service version detection) and Tenable Nessus Essentials, identifying 26 distinct vulnerabilities across 4 severity tiers (0 critical, 2 medium).
- Mapped discovered vulnerabilities to OWASP Top 10 categories and provided risk ratings based on CVSS, supporting executive and developer-friendly remediation reporting.

## VPN Client Monitoring with Wazuh SIEM | AWS Cloud Deployment | [Report](#)

Jun 2024 - Jul 2025

### *University of San Diego*

- Provisioned and configured AWS EC2 instance to deploy a secure, cloud-based VPN infrastructure using Pi-hole for DNS-level ad/tracker blocking and PiVPN (WireGuard) for encrypted remote access.
- Integrated Wazuh SIEM/XDR to enable centralized log aggregation, correlation rules, and alerting mechanisms for VPN client activity.

## Wireless Traffic Capture & WPA2 Cracking | Capstone Project | [YouTube](#)

Feb 2025 - Apr 2025

### *Cyber Proud*

- Captured and decrypted 5,000+ WPA2-encrypted 802.11 frames using monitor mode, airmmon-ng, and aircrack-ng to crack weak passwords.
- Analyzed decrypted traffic in Wireshark, exposing DNS, TLS, ARP, SSDP, LLMNR metadata and endpoint behavior.

## Kali Linux GRUB Menu Login Bypass | Cracking a Kali Linux User | [YouTube](#)

Jan 2025 - Feb 2025

### *Independent Project*

- Demonstrated local privilege escalation via bypassing GRUB authentication and modifying kernel boot parameters to gain root shell access.
- Analyzed the boot process, GRUB configuration, and Linux runlevels to enable unauthorized access without credentials.

## Forensic Investigation | System Artifact Analysis with Autopsy | [Report](#)

Nov 2024 - Dec 2024

### *Independent Project*

- Processed and parsed 300+ Windows registry artifacts (NTUSER.DAT, OpenSaveMRU, MUICache, UserAssist) to reconstruct user activity timelines and detect anomalous behavior.
- Employed Autopsy, RegRipper, and manual registry inspection to perform layered forensic analysis, event correlation, and artifact extraction.

## Work Experience

---

### **Court Crate** | *Project Manager - (Present)*

Oct 2019 - Present

- Built and managed a secure e-commerce platform with WordPress hardening, user authentication, HTTPS/TLS, and uptime SLAs exceeding 99.9%.
- Implemented robust web application security controls, including SSL/TLS enforcement, plugin audits, and regular vulnerability patching to protect user data and maintain platform resilience.
- Oversaw end-to-end platform development lifecycle, coordinating with developers, content teams, and hosting providers to ensure system scalability, secure deployment, and continuous uptime.

### **Broadstone Sports Club** | *Tennis Professional - (Part-Time)*

May 2023 - Present

- Mentored and coached players across all skill levels, developing individualized improvement plans while translating complex techniques into clear, actionable guidance that strengthened communication and leadership skills.

### **Golden Gate Realty** | *Real Estate Agent*

Jan 2020 - Nov 2022

- Built trusted client relationships and closed over \$10M in sales. Leveraged analytical and interpersonal skills transferable to high-stakes cybersecurity environments.

### **Tri-Force Marketing** | *Web Developer*

Feb 2015 - May 2021

- Developed 100+ full-stack websites (HTML5, CSS3, JavaScript, PHP, MySQL) with secure form handling, authentication, and server-side validation.
- Implemented input sanitization and parameterized queries to prevent XSS, CSRF, and SQL injection per OWASP Top 10.
- Configured SSL/TLS, access controls, and log analysis to strengthen deployment security and operational monitoring.