Kayvon Karimi

Folsom, CA 95630 | Portfolio[: cyberbykayvon.com](https://cyberbykayvon.com/) | Email: cyberbykayvon@gmail.com [| LinkedIn](https://www.linkedin.com/in/kayvon-karimi-3b2334134/) [| GitHub](https://github.com/CyberbyKayvon)

# 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



* **Technical Skills:** Network Exploitation , Web Application Testing, Vulnerability Assessment, Penetration Testing, Digital Forensics,

Incident Detection & Response, Packet Analysis & Traffic Decryption, Malware Investigation, Cloud Security Configuration,

VPN & Firewall Management, Bash & Python Scripting, Linux & Windows Administration, Security Monitoring & Log Analysis,

Authentication & Cryptographic Protocols, CTF Problem Solving, TLS Key Logging, Security Automation & Scripting, Proxy Server Configuration, VPN Deployment, Privilege Escalaton

* **Offensive Security Tools:** Wireshark, Nessus, Nmap, OpenVAS, SQLmap, MySQL, Burp Suite, Metasploit, FFUF, Gobuster, Nikto, John the Ripper, Hashcat, aircrack-ng, airmon-ng, WebGoat, Selenium, Hydra
* **Defensive Security & Monitoring Tools:** Wazuh, Splunk, Snort, Security Onion, tcpdump, PowerShell, CMD, Autopsy, Volatility, Regripper, FTK Imager
* **Cloud & Virtualization Tools:** AWS (EC2, S3, IAM, Security Groups), Azure Basics, Docker on AWS, Kubernetes, VirtualBox, Pi-hole, WireGuard, Tailscale
* **Cryptographic & Web Security Tools:** OpenSSL, PuTTYgen, TLS Key Logging, Apache2 HTTPS, Certificate Authority, PKI, Diffie-Hellman, X.509 Chain Validation
* **Systems & Admin Tools:** Linux (Debian/Ubuntu), Windows Server, Active Directory, Group Policy Management, RDP, Local Security Policy, WordPress Hardening, C Panel, bash scripting, iptables
* **Frameworks & Compliance:** Frameworks & Compliance, NIST 800-53, MITRE ATT&CK, OWASP Top 10, CVE/CVSS Scoring, CIS Benchmarks, DISA STIFs, SOC 2, ISO 27001

# Education

|  |  |
| --- | --- |
| **University of San Diego** | **Dec 2025** |
| *Master of Science, Cybersecurity Engineering* (GPA: 4.00)  •**Achievements:** The Cybersecurity Student Club | *San Diego, CA* |
| **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](https://cyberbykayvon.com/designpentest.pdf) 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](https://cyberbykayvon.com/courtcratepdf.html)

*Court Crate*

## Jul 2024 - Aug 2025

* 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](https://cyberbykayvon.com/vpn_aws.pdf) 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](https://www.youtube.com/watch?v=EWGMDg7hSDQ&t=28s) Feb 2025 - Apr 2025

*Cyber Proud*

* Captured and decrypted 5,000+ WPA2-encrypted 802.11 frames using monitor mode, airmon-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](https://www.youtube.com/watch?v=0bu_kN53izE) 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](https://cyberbykayvon.com/autopsy.pdf) 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

* Mentor and coach players of all skill levels, building individualized development plans to foster growth, resilience, and strategic thinking.
* Cultivate strong communication skills by translating complex techniques into clear, actionable steps.

## Golden Gate Realty | *Real Estate Agent* Jan 2020 - Nov 2022

* Built trusted relationships with investors, utilizing strong analytical skills to identify high-value opportunities across the DFW metroplex.
* Delivered $10M in cumulative sales by leveraging strategic planning, attention to detail, and market analysis.

## Tri-Force Marketing | *Web Developer* Feb 2015 - May 2021

* Co-developed 100+ full-stack websites using HTML5, CSS3, JavaScript, PHP, and MySQL, with a focus on secure form handling, authentication logic, and server-side validation.
* Implemented input sanitization and parameterized queries to mitigate XSS, CSRF, and SQL Injection, aligning with early-stage OWASP Top 10 secure coding practices.
* Applied SSL/TLS configurations, basic access controls, and log analysis to identify anomalies, supporting more secure deployments and improved operational visibility.