

Jair Ramirez

Irving, TX 75039

(512) 913-3021 | jairr0813@gmail.com

 <https://github.com/JairCodes>

|  <https://www.linkedin.com/in/jair-ramirez->

|  <https://jairramirez.tech>

EDUCATION & CERTIFICATIONS

Bachelor of Science in Computer Science (Minor: Mathematics)

Texas State University

Aug 2025

San Marcos, TX

Relevant Coursework: • Computer System Security • Computer Networks • Database Systems • Computer Architecture

Certifications:

- Security+ Certification (CompTIA)
- Certified Defensive Security Analyst (Hack The Box)

In Progress

In Progress

SECURITY EXPERIENCE

Enterprise SOC & IT | VirtualBox, pfsense, Debian, Splunk, Windows Server, Active Directory, Kali Linux |

Jun 2025

- Built a four-zone SOC network in VirtualBox with pfSense, enforcing enterprise firewall policies, validating Active Directory/GPO configurations, and detecting lateral movement.
- Created, managed, and tuned over 30 Splunk alert rules to detect suspicious activity (lateral movement, failed logins).
- Monitored & triaged real-time security alerts from Splunk, reducing false positives by 25% through custom correlation searches and dashboards.

NetDefend | Cisco 2960, Cisco 1841, Raspberry Pi, Rasploit, Splunk, Wireshark |

In Progress

- Configured network devices to forward syslogs into Splunk and tuned forwarder settings for complete visibility.
- Tuned exploit-signature detection rules using Raspberry Pi-generated attack traffic, then investigated alerts.
- Conducted endpoint hardening validation and guided a peer through switch/router fundamentals, translating technical risk into clear mitigation strategies.

VM Sandbox | VirtualBox, pfsense, Ubuntu, Kali Linux, Win XP, Win 95, Wireshark |

Nov 2024

- Simulated real-world attacks by exploiting Windows vulnerabilities (MS08-067, MS17-010) and launching phishing campaigns using Metasploit and SET.
- Collaboratively built a multi-OS sandbox with segmented subnets, pfSense firewall rules, and custom access controls to simulate enterprise network defense.
- Performed Linux-based penetration tests (SQL injection, buffer overflow, password cracking), leveraging Wireshark and debugging tools to validate exploit impact.

Machine Learning NIDS | Python, Pandas, scikit-learn, TensorFlow, Matplotlib, Seaborn |

Apr 2025

- Aggregated 2.8 M flow records from eight CICIDS2017 CSVs, removed 9.6% duplicates, handled edge cases ($\infty \rightarrow \text{NaN}$), and standardized 78 flow features.
- Benchmarked Random Forest, weighted SVM, and DNN on CICIDS2017, and presented results alongside common attack analysis (DoS, brute-force, WebAttack) to explain detection strengths and gaps to a general audience.

PROFESSIONAL EXPERIENCE

Software Engineer - AI Consultant

Apr 2024 - Present

Outlier AI

Remote

- Aligned AI model outputs with end-user coding requirements by evaluating interaction logs and refining prompt-response mappings.
- Documented real-time troubleshooting processes to create comprehensive records of complex AI model challenges, resulting in optimized training data.
- Improved development efficiency by swiftly troubleshooting and resolving AI model issues.

TECHNICAL SKILLS

Programming Languages: • Python • Java • C++ • SQL

Tools & Technologies: • Splunk • Wireshark • GitHub • PuTTY • MySQL • Excel • AWS • Microsoft Azure • Oracle VirtualBox • Pfsense • Microsoft 365 • Active Directory • MFA • ServiceNow (ticketing) • Remote Desktop (RDP/VNC)

Operating Systems: • Windows • Windows Server • Linux (Ubuntu, Kali, Debian)

Networking: • Network Protocols (e.g., TCP/IP, UDP, HTTP, DNS, DHCP) • Routing & Switching • VLAN Management

• Subnetting • Firewall Configuration • Network Analysis • Network Troubleshooting

Security & Compliance: • SIEM • IDS/IPS • Security Monitoring • Log Analysis • Threat Detection • Risk Management

• OWASP Top 10 • Incident Response (NIST, CIS, PCI DSS) • GRC Concepts • Security Control Validation • MITRE ATT&CK

LEADERSHIP & COMMUNICATION EXPERIENCE

Cybersecurity Awareness Presenter - Round Rock, TX

2025

- Presented a phishing awareness session to educate family members on social engineering tactics and preventative practices.

Peer Tutor – Database Systems & Calculus III - Texas State University

2024

- Led peer support sessions to reinforce concepts in Database & Calculus, increasing exam grades by 10-15%.