Jair Ramirez

(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)   ***Aug. 2025***
Texas State University   San Marcos, TX

Relevant Coursework: ○ Data Structures & Algorithms ○ Object Oriented Programming ○ Database Systems ○ Technical Writing ○ Computer Architecture ○ Computer System Security ○ Computer Networks ○ Computer System Fundamentals ○ Machine Learning

Certifications:
- Security+ Certification (CompTIA)   *In Progress*
- Certified Defensive Security Analyst (Hack The Box)   *In Progress*

PROFESSIONAL EXPERIENCE

Software Engineer - AI Consultant   *Apr. 2024 - Present*
Outlier AI   Remote
- Accomplished **alignment of AI model outputs** with user expectations by evaluating results based on specific user criteria.
- Enhanced **AI model performance** by developing ideal responses that served as benchmarks for training data, aligning model behavior with user prompts.
- **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.

PROJECTS

Enterprise SOC & IT Lab | VirtualBox, pfsense, Debian, Splunk, Windows Server, Active Directory, Kali Linux | *In Progress*
- Simulated threat activity from an isolated attacker subnet (OPT1) targeting Windows systems to test AD authentication, GPO enforcement, and endpoint visibility in Splunk.
- Designed and segmented a virtual SOC network using pfSense with isolated LAN, WAN, and attacker zones, replicating enterprise firewall and access policies.
- Forwarded system and firewall logs to Splunk via Debian log collector, enabling SPL-based detection rules, dashboard insights, and alert triage workflows.

VM SandBox Project | 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 Project | Python, Pandas, scikit-learn, TensorFlow, Matplotlib, Seaborn | *Apr. 2024*
- Aggregated 2.8 M flow records from eight CICIDS2017 CSVs, removed 9.6% duplicates, handled edge cases ($\infty \rightarrow$ NaN), and standardized 78 flow features.
- Benchmarked Random Forest (78% accuracy), weighted SVM (75% WebAttack recall), and DNN (weighted F1 0.73), and presented findings that revealed trade-offs between overall accuracy and rare-attack detection.

Critical Threats in Modern Systems | MySQL, PostgreSQL, SQL, ER Modeling | *Apr. 2025*
- Built a CVE vulnerability tracking system for SecureTech Solutions using NIST data to classify and document major threats (XSS, SQLi, RCE, buffer overflows, and info disclosure).
- Developed SQL queries and views to reveal risk trends, map CVSS severity to mitigation strategies, and support evidence-based prioritization of remediation efforts.
- Deployed the system in both MySQL and PostgreSQL with enforced primary/foreign keys, validating schema integrity and ensuring consistent query results across platforms.

TECHNICAL SKILLS

Programming Languages: ○ Python ○ Java ○ C++ ○ C ○ SQL ○ MIPS32

Tools & Technologies: ○Splunk ○ Wireshark ○ VisualStudio Code ○ GitHub ○ PuTTY ○ MySQL ○ Excel ○ AWS EC2 ○ Oracle VM ○ Pfsense

Operating Systems: ○ Windows ○ Linux (Ubuntu, Kali, Debian)

Networking: ○ Network Protocols (e.g., TCP/IP, UDP, HTTP, DNS, DHCP) ○ Routing & Switching ○ VLAN Management ○ Subnetting ○ Firewall Configuration ○ Network Analysis & Troubleshooting

Security: ○ Security Monitoring ○ Threat Detection ○ Penetration Testing ○ Log Analysis ○ SIEM (Splunk) ○ IDS/IPS ○ Risk Management ○ OWASP Top 10, Incident Response (NIST, CIS)

LEADERSHIP EXPERIENCE

Peer Tutor – Database Systems & Calculus III
Texas State University
- Led peer tutoring sessions to help students better understand SQL, ER modeling, and multivariable calculus concepts.
- Reinforced technical communication and problem-solving through small-group guidance and exam preparation.