Jair Ramirez

Irving, TX 75039
(512) 913-3021 | jairr0813@gmail.com

https://github.com/JairCodes | https://www.linkedin.com/in/jair-ramirez- | JR https://jairramirez.tech

Education & Certifications

Bachelor of Science in Computer Science (Minor: Mathematics) ***Aug. 2025***
Texas State University San Marcos, TX

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

Certifications:

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

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.
- **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*

- Built a four-zone SOC network in VirtualBox with pfSense, enforcing enterprise firewall policies, validating Active Directory/GPO configurations, and detecting lateral movement.
- Ingested Windows Security, Sysmon, and pfSense firewall logs into Splunk via a Debian collector for real-time detection and triage.
- Tuned detection rules and dashboards in Splunk to reduce incident triage time by 25% and validate AD hardening, enabling more effective root-cause analysis and risk visualization.

NetDefend Lab | Cisco 2960, Cisco 1841, Raspberry Pi, Rasploit, Splunk, Wireshark | *In Progress*

- Configured Cisco hardware to forward syslogs to Splunk and deployed a Splunk Universal Forwarder on an internal host to collect and consolidate system logs for full visibility.
- Deployed a Raspberry Pi with Rasploit on the guest network to generate attacking traffic against an internal VM, then analyzed Splunk alerts to develop and fine-tune detection rules for common network-based exploits.
- Performed endpoint hardening validation on the internal VM by enabling host-based firewalls and launching targeted scans/attacks from the Raspberry Pi to confirm blocked services.

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. 2025*

- Aggregated 2.8 M flow records from eight CICIDS2017 CSVs, removed 9.6% duplicates, handled edge cases (∞→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.

Technical Skills

Programming Languages: • Python • Java • C++ • SQL
Tools & Technologies: • Splunk • Wireshark • GitHub • PuTTY • MySQL • Excel • AWS • 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%.