MAURICIO MARTINEZ

Brownsville, TX | (956) 371-0886 | mauriciomartinezpersonal@gmail.com | LinkedIn | Portfolio

---

PROFESSIONAL SUMMARY

Security-focused cybersecurity student with experience in network defense, incident triage, and log/telemetry analysis. Proficient in vulnerability assessment using Tenable Nessus and finding the applicable CVEs and mitigation summaries, MITRE ATT&CK mapping with a focus on automation scripts for necessary threat hunting. Communicated findings to the designated professionals within IT for the required actions to remediate any issues. Learned foundational language within the cybersecurity world, such as CIA, AAA, HIPAA, PCI DSS, and PII

PROFESSIONAL EXPERIENCE

Student Information Security Analyst

UTRGV Regional Security Operations Center – Edinburg, TX | June 2025 – Present

- Proactively achieved Fortinet Certified Associate in Cybersecurity certification
- Proactively achieved Fortinet Certified Fundamentals in Cybersecurity certification

Information Security Intern

Cameron County – Brownsville, TX | December 2025 – February 2026

- Used Tenable Nessus to actively look for vulnerabilities and created scans based on suspicious endpoints found in DHCP scopes.
- Administered Security awareness training and phishing campaigns for staff in compliance with the Texas Government Code 2054.519. Enhancing employees' understanding of cybersecurity best practices and reducing human-related security risks.
- Worked with cross-functional teams to remediate CVEs found on servers by patching software or removing unnecessary software.
- Analyze and create an antivirus XQL script that would find any Remote Monitoring and Management (RMM) tools that are not authorized by the IT department or are not CJIS-compliant.
- Triaged XDR alerts by finding the severity of whether a server needed patching or the alert was endpoint-generated by behavior risk and would escalate to the appropriate cybersecurity specialist.
- Proactively used OSINT tools like Unit 42 GitHub IOCs, AlienVault, ThreatFox, Malware Bazaar, and Dark Reading to alert CISO to block certain specific hashes, IP addresses, and domain names.
- Learned the foundations of how Active Directory and Entra ID integrate together and how Group Policy is used to create rules based on user or computer configurations.

Student Academic Assistant

University of Texas Rio Grande Valley – Rio Grande Valley | September 2025 – December 2025

- Proactively created an inventory logging app
- Managed study room reservations
- Assisted with office work; printing, forwarding messages, equipment handling

Mentor

University of Texas Rio Grande Valley – Rio Grande Valley | March 2025 – September 2025

- Mentored 21 students and supported two summer camps as Resident Assistant, coordinating schedules, materials, and engagement tracking
- Managed communications and logistics using Microsoft Teams, Zoom, and Canva

---

EDUCATION

University of Texas Rio Grande Valley

- **Bachelor of Science, Cybersecurity** (2023-2027)

COURSES

- Intrusion Detection, Digital Forensics, Software Engineering & Project Management, Programming Cyber Systems & Reverse Engineering, Foundations of Systems I & II.

CORE COMPETENCIES

- **Vulnerability Management:** Identifying, prioritizing, and addressing security weaknesses using Arctic Wolf's Risk Management Platform and Tenable Nessus.
- **Incident Response & Threat Detection:** Wazuh configuration. Basic containment logic with evidence handling/preservation best practices and basics.
- **Frameworks and Standards:** Introduction to NIST SP 800-53, CIS Controls, MITRE ATT&CK, CJIS.
- **Network Security:** Learned public/private IP, NAT rules, NMAP scanning, port security, and DMZ infrastructure

ADDITIONAL TECHNICAL SKILLS

- **Email Security:** Used ANY.RUN to analyze malicious/suspicious links or attachments from inbound emails.
- **Endpoint & Patch Management:** Used Antivirus for building XQL queries that would find behavioral risks within an environment.
- **Next-Generation Firewalls:** Analyzed logs/telemetry to find inbound threats hitting DMZ infrastructure and any CVEs that correspond with the threats.
- **Programming & Data:** Experience with Python, JS/TS, Bash, PowerShell, HTML/CSS, NumPy, Pandas, ETL, API Ingestion, data cleaning, versioned environments, telemetry time-series

---

KEY ACHIEVEMENTS

- **Fortinet Certified Associate in Cybersecurity Certification**
- **Fortinet Certified Fundamentals in Cybersecurity Certification**
- **HomeLab –** Built a home lab environment for IT and cybersecurity practice. Implemented pfSense firewall with VLAN segmentation. Configured DHCP and DNS. Deployed Windows Server 2025 with Active Directory to manage users, groups, and authentication policies. Monitored user authentication activity and login attempts through Active Directory and Windows Event Viewer. Wazuh for centralized log collection and security monitoring. Practiced troubleshooting network connectivity, system issues, and access control problems across multiple systems. Simulated real-world SOC and IT support scenarios, including user authentication failures, network access issues, and system alerts.
- **Banadi – AI-Powered Pentesting & Vulnerability Triage Framework –** Built a modular offensive security framework integrating Claude Code orchestration, Dockerized Kali tooling, NVD CVE intelligence, and LLM-assisted analysis. Implemented slash commands (/banadi-recon, /banadi-cve, /banadi-patch) for nmap reconnaissance, port-service guidance via Hackviser, CVE identification against NVD REST API, and Windows installed-program triage with automated report.md generation.
- **Azure VSOC + self-hosted AI pentesting –** Learned fundamental Azure environment setup with Linux and Windows vulnerable VMs and Wazuh SIEM. Researching best LLM models for hardware to utilize self-hosted LLM for multi-agent penetration testing using PentAGI.
- **Lead @ Vaquero Information Security Initiative (VISI) –** Current lead and member. Working towards a cyber clinic, preparing students with technical practice through workshops and mentorship. https://vaqueroisi.org
- **Vulnerability Management Workshop (VISI) –** Demonstrated the use of port-scanning and vulnerability assessment tools such as Nmap, AngryIPScanner, and OpenVAS. Also explained CVE system, zero-day vulnerabilities, IP addresses and subnetting, SQL injection, path traversal, and distributed a VirtualBox Kali VM with OpenVAS installed.
- **OSINT Tools Workshop (VISI) –** Demonstrated open-source intelligence gathering techniques across identity, infrastructure, and incident response fields. Covered username enumeration, facial recognition search, metadata/geolocation extraction, domain email enumeration, Dorking, IP and port reconnaissance, data breach verification, people/property/vehicle lookup tools, surveillance awareness resources, malware hash analysis, browser-based sandboxing, phishing email analysis, and subdomain enumeration.
- **Developed an Inventory Scanner App –** A local React Native + Node.js system that scans 1D barcodes and writes entries in CSV format. Designed for offline-friendly use and simple deployment on Windows or Linux hardware. May be depreciated
- **Developed Gulf Water Quality Analysis –** A local web app that analyzes Gulf of Mexico water-quality data, with AI-assisted characteristic matching and simple charts. Created for an admission application, may be deprecated.