Mauricio Spadoni

Atlanta, GA | (404) 4**-**** | mspadonitech@gmail.com

LinkedIn Profile | Website Portfolio

Education

University of North Georgia, Mike *Cottrell College of Business* Dahlonega, GA

Bachelor of Science in Cybersecurity ***May 2025***

Relevant Coursework: Information Technologies; Computer Science I; Script Programming; Applied Cybersecurity; Web Programming; Computer Security; Network Security; Database Security; Data Networks; Reverse Engineering

Technical Skills

Languages: SQL, TSQL, Python, CSS, HTML, Powershell, Bash

Frameworks & Platforms: React.js, Salesforce (Admin + Platform Dev I), .NET (C#), Flask

Tools: VS Code, Visual Studio, Postman, JIRA, ServiceNow, FTK Imager, Kibana, OpenAI APIs

Data & Analytics: Tableau, Power BI, Excel (advanced), PostgreSQL, SSMS

Security & Networking: Active Directory, Networking (LAN/WAN, TCP/IP, DNS, DHCP, VPN, VLANs, Wireless), Wireshark, nmap, OpenVAS, Linux (Debian, CentOS), Windows Server, VMware

Experience

Scholastic Projects ***August 2021 – Present***

A selection of hands-on labs, capstone work, and course projects demonstrating applied cybersecurity, full-stack development, reverse engineering, and defensive techniques.

- ***Active Directory Home Lab*** — Hands-on AD exploration including OU design, user & group management, replication, group policy implementation, and both logical & physical AD architecture. Implemented OU structure, RBAC policies, and tested replication/topology scenarios.

- ***T-Pot Honeypot (Capstone / T-Pot Honey Project)*** — Deployed a T-Pot honeypot environment with centralized logging and Kibana dashboards to capture real-world attack telemetry. Implemented monitoring, log ingestion, and produced analytical findings on attack vectors and IOCs.

- ***SQL Injection Web App in Flask*** — Built a Flask-based sample web app to demonstrate SQL injection vulnerabilities and implemented mitigations (parameterized queries, input validation, ORM usage, prepared statements). Documented test cases and remediation steps.

- ***Python Scripting Assignment*** — Collection of scripting tasks including file handling, cryptographic hashing, randomized data generation, brute-force utilities, and system automation scripts (tooling for data extraction and basic forensic collection).

- ***Reverse Engineering & Debugging Labs*** — Series of reverse-engineering exercises using IDA, Ghidra, OllyDbg, Cutter and Linux debugging utilities. Performed anti-debugging bypasses, binary patching, and flag recovery. Documented methodology and remediation recommendations.

Aarons Tech ***Oct 2021 – August 2023***

IT Analyst

- Delivered enterprise technical support for over 3,600 cases across Windows/macOS systems, Active Directory, and VoIP platforms.
- Provided LAN/WAN troubleshooting and support for VPN connectivity, network wiring, and remote hardware.
- Used ServiceNow ticketing system to record, document, and resolve issues with a 95%+ user satisfaction rate.
- Worked closely with internal and third-party teams to coordinate hardware replacements, cabling installs, and site upgrades.
- Created knowledge base articles and site-specific documentation to assist future field service operations.
- Supported security compliance efforts and maintained adherence to technical standards and documentation protocols.