

Angel Garcia J.

(702) 960-9278 ● angel.garciaj@owasp.org ● [linkedin.com/in/angelgarciaj/](https://www.linkedin.com/in/angelgarciaj/) ● vanglez.us/

Professional Development

Certifications: [Security+](#), [A+](#), [LPI Linux Essentials](#)

Homelab: [Proxmox](#) | [Windows Server 2022](#) | [Ubuntu Server](#) with [Docker](#) | [pfSense](#) | [Cloudflare](#)

Involvement: [DEFCON\(29-31\)](#), [BSides Las Vegas\(22-23\)](#), [Pro Vs Joes CTF: 2022/23 1st Place Winner](#)
[NCL CTF 2022 Teams\(71/1068 \)/ Individuals\(242/3487 \)](#), [TryHackMe - Top 3% of 2226572 players](#)

Beginner Level Languages: C#, Javascript, KQL, x86 Assembly

Intermediate Level Languages: C++, Python, SQL

Speaking Languages: English, Spanish, & Japanese(Learning)

EXPERIENCE

Druvstar, Cybersecurity Intern

May 2023 - October 2023

- Responded to tickets by analyzing log data from security tool portals (Microsoft Defender for 365 & Azure) to report & communicate to clients on how to proceed on a monthly basis
- Monitored SIEM alerts and conducted investigations to improve true positive detections by an average of 26.7% and up to 100% resulting in over \$200,000 in savings for the MSSP in a year
- Provided proactive "threat hunting" to detect incidents & accelerate the enhancement of the SOC

Contract Work, Systems Administrator

May 2022 - Present

- Administer virtual machines & services provided to 100+ users to accomplish 99.999% uptime
 - Proxmox, pfSense, Cloudflare, Wazuh, Ubuntu, Wordpress, Docker, & Windows
- Create and revise internal documentation for networks, infrastructure & assets to minimize costs
- Manage and collaborate on projects through Jira & [Asana](#) to keep business operating
- Clients: [Free Cyber Clinic](#), [Layer Zero](#) & Personal Homelab

Free Cyber Clinic, Co-Founder

October 2021 - Present

- Non-profit that assesses threat actor Tactics, Techniques & Procedures (TTPs) focused on 100s of small businesses under the [SBDC](#) to help prevent [\\$100,000+ of damages](#) from hacks & breaches.
- Create virtual labs to be assessed with open-source & system tools to train for vulnerabilities or weaknesses found in small businesses.
- Design & create additional training for tools or certifications like Security+ in order to lead our 60+ students to learn, perform and lessen that [workforce gap of millions of people](#).

UNLV, Co-Instructor

July 2021 - Present

- Teach a class of about 30 university students about design and implementation of computer communication networks, their protocols and applications down to the header level and bits.
- Create labs under the NSA/NSF GenCyber with tools such as Wireshark to analyze network traffic, ESP8266 microcontrollers to simulate ICS devices, & Kali Linux tools to show vulnerabilities with IOT devices (nmap), web applications (BurpSuite) & wireless networks (aircrack-ng).
- Provide lab documentation through Github to students in order to maintain a smooth learning experience through teaching and walk-throughs.

NNSA MSIPP, Security Researcher

September 2022 - January 2023

- Create datasets with tools like Havoc - C2 Framework, Wireshark / TCPDump, VMware Workstation Pro & self-made tools/programs to recreate attacks from Advanced Persistent Threats(APTs).
- Implement machine learning on Python with network data (assumed breach) from IOT & ICS devices to discover threats & new trends leading to a continuous production of threat intelligence

EDUCATION

Western Governors University - Network Engineering & Security, Bachelor of Science