

Jeremy Laratro

516-512-1463 | jeremylaratro@gmail.com | jeremylaratro.link | [jeremylaratro](https://www.youtube.com/channel/UCv33333333333333333333) | [jeremylaratro](https://www.linkedin.com/in/jeremylaratro)

Summary

Over the years, I've cultivated a rich background in diverse areas of technology from software to hardware. My projects serve both practical and educational purposes, and I always take a solution-focused approach to everything I do. By leveraging my skills, discipline, and passion, I'm excited to being a reliable, trustworthy, and proficient addition to any team.

Certifications

OSCP (Offsec), Security+ (CompTIA), Intro To Cyber Security (TryHackMe)

Work Experience

WeMeta LLC

Tampa, FL

ELECTRONIC HARDWARE REPAIR & IT SOLUTIONS

Nov. 2021 - Nov. 2022

- General IT troubleshooting, complex hardware/PCB troubleshooting (with multimeter, oscilloscope, signal generator, etc), fundamental security integration (software and hardware), soldering, and more (see LinkedIn).

Education

University of South Florida

Bachelor's of Science, Biology

- Calculus I, Physics I and II, Statistics, Trigonometry, Pre-Calculus
- My undergraduate degree provided a solid foundation in core STEM topics such as mathematics, physics, scientific writing/reporting, and analysis. These concepts are directly relevant to any STEM field, including cybersecurity, and this foundation has allowed me to succeed in my further computer science studies.

Projects and Accomplishments

Securicoder.com

Apr. 2023 - Present (WIP)

- Incorporated ML/LMMS into a security-oriented project using ChatGPT API to produce a comprehensive static code analysis report covering main vulnerabilities; built using Django framework and deployed with Linode cloud server. Future plans to implement locally-run and possibly locally-trained llama.cpp LMMS (open source).

Technology Blog / Portfolio Site

2020 - Present

- Built a portfolio website (jeremylaratro.link) with Github pages and Ruby/Rails to showcase my personal and academic projects, along with my cybersecurity, software development, hardware development projects.

Capture the Flag

Jul. 2021 - Present

- Experienced CTF participant in various online platforms including Proving Grounds, TryHackMe, HackTheBox, picoCTF, Microcorruption, and OWASP Juice Shop, and recently participated in an in-person CTF at BSIDES. Successfully rooted over 100 virtual lab machines.

Pentesting Automation Scripts - B-NEAS

Dec. 2022 - March. 2023

- Created an efficient script for OSCP lab penetration tests, including initial enumeration and discovery tools with multi-function capability and searchsploit functionality by grepping nmap results for known vulnerabilities.

PhotoSec - Python

Aug. 2022 - Nov. 2022

- Created a python program to minimize exposure of dangerous metadata in online photos by removing metadata and GPS data, bulk renaming, and image analysis. Also utilized project to learn about file encoding and python packaging.

Home Server with WIFI AP

Sep. 2022 - Present

- Created a Raspberry Pi home server with a wifi-dongle to learn system administration and wifi hacking, including real-world use like live-feed of security cameras and SSH access, and practiced wifi hacking with tools like aircrack-ng.

Hardware Hacking

Jul. 2022 - Dec. 2022

- Analyzed devices for UART, JTAG, or I2C ports and determined baud rate. Soldered leads and established communication via adapter and minicom/picocom on Linux.

Skills

- Strong ability to manually analyze networks and applications to find, prioritize, and exploit vulnerabilities.
- Proficiency in scripting languages such as Python, Bash, and PowerShell, and experience using tools like Metasploit, Nmap, Burp Suite, and Wireshark.
- In-depth knowledge of various types of vulnerabilities, including OWASP Top 10, CVEs, and emerging threats, as well as experience with different exploitation methods and techniques, including buffer overflows and SQL injection.
- Exceptional written/verbal communication skills with ability to articulate complex technical topics in concise and simple terms
- Strong understanding of security frameworks, including MITRE ATTACK, Lockheed Martin Cyber Kill Chain, and NIST Cybersecurity Framework, along with regulatory frameworks like PCI DSS, HIPAA, and GDPR.
- Experience with common operating systems such as Windows, Linux, and macOS, as well as cloud platforms like AWS, Azure, and Google Cloud.
- Python, bash, metasploit, burp suite, nmap, nessus, rustscan, mimikatz, impacket, active directory, docker, network, application security, web security, kali linux, cryptography, http, api, manual, mobile, c++, sliver, smb, ftp, searchsploit, owasp zap