Jeremy **Laratro, OSCP**

Offensive Security · Electronic Hardware Technician

Port St Lucie, FL (open to relocation)

516-512-1463 | jeremylaratro@gmail.com | jeremylaratro.link | jeremylaratro | jeremylaratro | jeremylaratro

Hacking. Developing. Learning.

Summary

Throughout the years I have cultivated a rich background in various realms of technology, ranging from cyber security to electrical engineering. In this time I have developed numerous projects, which have served as both functional and educational. I believe in taking a solution-focused approach to everything I do and all of my projects are direct solutions to issues or inefficiencies I have come across, whether practical, educational, or in many cases, both. I look forward to applying this solution-seeking, practical mindset to my career in cyber security and leveraging my skills, discipline, and passion as a dependable, truthworthy, and skilled member of the team.

Certificates

2023 **Offensive Security Certified Professional,** OffSec (OSCP) *OS-101-41581*

2022 **Introduction To Cyber Security,** TryHackMe (THM) *THM-KZYADFWFA4*

Work Experience

WeMeta LLC

Tampa, FL

Electronic Hardware Repair & IT Solutions *Nov. 2021 - Nov. 2022*

- Started a sole propietorship to support myself during university, then transitioned to LLC and brought on a friend to expand scope/scale of work.
- Incorporate basic information security measures for local businesses.
- Repaired and refurbished surplus engineering equipment, laptops, and did general tech repair around the university.
- Hardware troubleshooting: used an oscilloscope to determine faulty behavior of MCUs, OpAmps, transistors/FETs, etc. Used DMM/ESR to discover missing/irregular voltage, faulty capacitors, etc
- Power troubleshooting: sent low voltage on the relevant power bus and then used IR camera to locate faulty part
- Parts and product integration: sourced cost-effective replacement components after discovering the faulty ones
- Soldering: desoldered faulty components, then soldered new components, many with complex footprints (SMT)
- Radio: Programmed amateur and professional radios including digital and trunked radio systems.

Education

USF(University of South Florida)

Tampa, FL

B.Sc. in Biology *Sep. 2019 - Aug. 2022*

- 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 self-studies of computer science and electrical engineering as well as in my studies for the OSCP.

Writing

Cybersecurity Blog

jeremylaratro.link/CS/cysec

Author and Website Creator *2021-2023*

- Built a portfolio website to showcase my personal and academic projects, cybersecurity studies, CTFs, along with technical notes on common cybersecurity tools.

System Weakness and Medium.com: Daily Bugle CTF Writeup

Medium.com, System Weakness Publication

Author *2022*

- Published a technical writeup or walkthrough of my methodology in hacking the CTF called 'Daily Bugle.'

Projects and Accomplishments

Securicoder.com

Port St Lucie

Developer

Apr. 2023 - Present

- Purpose: With the recent rush on AI and ChatGPT, I wanted to incorporate ML/LMMS into a security-oriented project and also learn about blue team methods.
- In creating a public-facing cloud server, security is essential and thus I have implemented a number of security features such as snort, reverse-proxy, SSL, and am working on implementing Security Onion for more IDS features.
- Overview: Leverage ChatGPT API on the backend with extra processing, take user-submitted code samples on the front-end, and learn about SOC/IDS in the process.
- The outcome will be a professional and in-depth static code analysis report which covers all of the main vulnerabilties including race conditions, buffer overflow/underflow, stack overflow, logic flaws, etc.
- Current State: Began development using the Django framework, purchased domain and configured DNS, and configured a cloud server using Debian on Linode for deployment once bugs are fixed and security is analyzed.

Pentesting Automation Scripts - B-NEAS

Port St Lucie

Developer

Dec. 2022 - March. 2023

- Purpose: Sought a solution to increase my efficiency when performing penetration tests on the OSCP lab targets and found that a large time sink was in initial enumeration and discovery, much of which involved similar commands and functions.
- Developed the script to include most of the tools used during initial enumeration and discovery stage.
- Added multi-function capability with input switches.
- Incorporated searchsploit functionality. This works by grepping the output of the nmap results and then searching service name and version number for known vulnerabilities.

PhotoSec - Python

Port St Lucie

Developer

Aug. 2022 - Nov. 2022, Present

- Purpose: Sought to create a solution to minimize the exposure of potentially dangerous metadata from photos posted online.
- Developed a python program which leverages other libraries and allows for metadata removal, GPS data removal, bulk file renaming, as well as image analysis.
- Also sought to learn more about file encoding and python packaging and used this project to learn.

Home Server with WIFI AP

Port St Lucie

Home Lab

Sep. 2022 - Present

- Purpose: To learn more about system administration and wifi hacking, I created a home server using a raspberry pi with a wifi-dongle to better emulate a real-world business or home.
- Implemented real-world use, including live-feed of my home's security cameras as well as ssh.
- Practiced wifi hacking with aircrack-ng and other wireless tools via my main machine.

Capture the Flag

Port St Lucie

Home Lab

Jul. 2021 - Present

- Throughout the past two years, I have participated in hundreds of online CTFs as well as my first in-person CTF recently at BSIDES.
- CTF platforms that I actively participate in: Proving Grounds by OffSec, TryHackMe, HackTheBox, picoCTF, Microcorruption, OWASP Juice Shop
- Over the past year, I have succesfully hacked (rooted) over 70 different virtual lab machines using a variety of different exploitation methods, including but not limited to SQLi, RCE, LFI, RFI, Buffer Overflow, Phishing, Bruteforcing, MS Word Macro injection, along with many popular exploits including Eternal Blue, Drupalgeddon, SambaCry, PwnKit, LovelyPotatoes, etc.

Hardware Hacking

Port St Lucie

Home Lab

Jul. 2022 - Dec. 2022

- Purpose: Desired to increase my understanding of hardware hacking.
- With a strong understanding of electronics already from my work, I acquired various old routers/modems/IP cameras.
- The devices were opened and analyzed for UART, JTAG, or I2C ports. Baud rate was discovered using a logic analyzer or oscilloscope. Then, I soldered leads onto the device and using an adapter (depending on protocol - FTDI,J-LINK Mini,UART, etc), I proceeded to establish communication with the device using minicom or picocom on linux. Depending on the security of the device, I attempted to obtain a shell, many of which, especially older devices, have minimal hardware or firmware security features.

Class-A Amplifier - PCB Design

Tampa

Home Lab

Dec. 2020 - Mar. 2021

- Purpose: Sought the skills and knowledge to design and create my own circuits in CAD.
- Using a variety of online sources, I learned the basics of KiCAD, an open-source CAD modeling software.
- Designed circuit for a simple class-A amplifier. I chose the class-A amplifier for multiple reasons, the main ones being that it is simple, and while not efficient, produces a clean signal.
- After designing the circuit in KiCAD, I converted the GRBR files into GCODE (via CAM). I then sent the GCODE to my mini-CNC machine which I built for milling PCBs at home. After completion, I soldered all of the necessary components and was able to use the device to boost my phones output volume.

Skills

Metasploit - Powershell Empire - Kali Linux - Enumeration - Web App Pentesting - Network Discovery - Burp Suite - Kill Chain - MITRE ATTACK - Code Analysis - Python - Bash - SOC - System Administration - Snort - Active Directory - Tunneling - Pivoting - Windows - Buffer Overflow - Reporting - Communication