Jeffrey DeOcampo

(206)-475-8683 | jjdeocampo20@gmail.com | San Diego, California | https://github.com/CLANMOKBACK

EDUCATION

San Diego State University **Graduation: May 2025**

B.S. in Computer Science, Minor in Mathematics **GPA: 3.21/4.0**

Relevant Coursework: Computer Security, Machine Learning, Data Structures & Algorithms, Operating Systems

OBJECTIVE

Software engineer with a strong foundation in mathematics seeking an internship to leverage technical skills in linux, computer security, and machine learning. Proven ability to lead successful projects and collaborate effectively.

TECHNICAL SKILLS

Programming Languages: C# & C++, Java, Python, Bash, MATLAB, MIPS/Assembly

Frameworks & Tools: Linux, Vim, GitHub, Google Cloud Platform, Unity Engine, Twilio, Docker Compose

PROJECT EXPERIENCE

Buffer Overflow Attack | Linux OS, Google Cloud VM, Python, Vim, Bash Mar 2025 - Apr 2025

- Developed and executed buffer overflow attacks across multiple vulnerable servers using custom 32-bit and 64-bit shellcode, achieving **reverse** and **root shells** through precise return address manipulation and payload injection.
- Engineered a **multi-VM lab environment** using **Docker Compose**, with separate containers for listening, attacking, and hosting vulnerable services; coordinated attacks by sending crafted payloads from one VM to a victim server, which triggered a reverse shell to a listener.
- Tested and evaluated memory protection mechanisms such as **ASLR, StackGuard,** and **non-executable stacks**, utilizing **GDB** for offset discovery and brute-force methods to assess the effectiveness of modern exploit countermeasures.

Set-UID Program | Linux OS, Google Cloud VM, C, Vim, Bash Feb 2025 - Mar 2025

- Explored environment variable behaviors and propagation in Unix-like systems, demonstrating how variables like **PATH** and **LD_PRELOAD** can influence program execution across **parent/child processes** and privileged contexts.
- Analyzed and exploited vulnerabilities in Set-UID programs, including **PATH hijacking**, **LD_PRELOAD injection**, and command injection via system(), demonstrating **privilege escalation** and **secure alternatives** using execve().
- Demonstrated capability leaking and privilege manipulation by exploiting unclosed file descriptors and understanding real vs. effective UID handling in Set-UID binaries, achieving unauthorized file access in a controlled lab environment.

2D Unity Game Project | C#, Unity Engine, GitHub Aug 2024 - Nov 2024

- Built a 3-level 2D maze game in Unity using object-oriented **C# scripts**, implementing custom obstacle movement (linear and circular) with increasing gameplay difficulty.
- Programmed player controls and collision detection using Rigidbody2D, Collider2D, and OnCollisionEnter2D, and managed scene transitions with Unity's SceneManager API.
- Designed an interactive UI using the Canvas system and EventSystem, and integrated AudioSource components for real-time sound effects triggered by button presses, collisions, and level completions.

CERTIFICATIONS

Oracle Cloud Infrastructure 2023 AI Foundations (1Z0-1122-23)

WORK EXPERIENCE

Rosemary Trattoria | Server Aug 2023 - Present

P.F. Changs | Server June 2022 - Aug 2023

McDonald's | Line Cook Oct 2020 - May 2021