

# Aira Nicole Natividad

Cainta, Rizal | 0960-471-7131 | [annatividad@up.edu.ph](mailto:annatividad@up.edu.ph) | [github.com/airanatividad](https://github.com/airanatividad)

## OBJECTIVE

Eager to start a career in cybersecurity, applying analytical skills and a strong technical foundation to protect systems and mitigate emerging threats.

## EDUCATION

### University of the Philippines - Los Baños

*Bachelor of Science in Computer Science*

Los Baños, Laguna

*Sept. 2021 – Present*

### Cainta Catholic College

*Senior High School – STEM Strand*

Cainta, Rizal

*June 2019 – June 2021*

## EXPERIENCE

### Tech Intern

*Razza Consulting Group Inc.*

June 2024 – July 2024

*Quezon, City*

- Gained hands-on experience with Agile workflows, daily stand-ups, and project management tools like Jira
- Developed frontend features using React and JavaScript, collaborating with developers and tech leads
- Implemented and optimized web scraping modules using Cheerio to extract and process data
- Enhanced debugging and problem-solving skills by tackling real-world development challenges

## PROJECTS

### Capture The Flag (CTF) Challenges | *GDB, Python, Wireshark, Ghidra*

Dec. 2024

- Exploited buffer overflows by using GDB to analyze memory, find offsets, and overwrite return addresses
- Extracted hidden flags from PCAP files in Wireshark by reconstructing base64-encoded network data
- Reverse-engineered executables in Ghidra, analyzing functions and obfuscated strings to uncover flags
- Decrypted XOR-encoded messages and cracked MD5 hashes using Python for cryptographic challenges

### Penetration Testing on Virtual Machines | *Kali Linux, Metasploit, Nmap*

Dec. 2024

- Scanned for open ports using Nmap, identifying vulnerabilities in ProFTPD and SMB services
- Exploited ProFTPD backdoor with Metasploit, gaining root access and executing system commands
- Extracted password hashes from /etc/shadow and attempted cracking using John the Ripper
- Maintained persistence by injecting an SSH public key into authorized\_keys for remote access

### Malware Analysis | *VirusTotal, Strings, Wireshark, Ghidra*

Dec. 2024

- Detected keylogging and persistence techniques by analyzing malware in VirusTotal
- Reverse-engineered executables using Ghidra, extracting obfuscated API calls for data exfiltration
- Investigated network traffic with Wireshark, identifying C2 communication and suspicious connections
- Examined registry modifications and startup persistence, confirming malware's stealth mechanisms

## CO-CURRICULAR ACTIVITY

### UPLB Computer Science Society (UPLB COSS)

Oct. 2023 – Present

*Backend Team Lead*

- Leading the backend development for the organization's website using the MERN stack.
- Collaborating with the team on system design and feature implementation to ensure secure coding practices and mitigate web vulnerabilities.

## TECHNICAL SKILLS

**Languages:** Python, C/C++, Bash Scripting, Assembly (NASM), Javascript, PHP, SQL (PostgreSQL, MariaDB)

**Cybersecurity Tools:** Metasploit, Nmap, Wireshark, Ghidra

**Security Techniques:** Penetration Testing, Binary Exploitation, Malware Analysis, Reverse Engineering, Web Exploitation, Digital Forensics, Cryptography

## REFERENCES

**Asst. Prof. Rodolfo Camaclang**

*Special Project Adviser*

*UPLB Institute of Computer Science*

[rccamaclang1@up.edu.ph](mailto:rccamaclang1@up.edu.ph)

**Francesca Cruz**

*Tech Lead*

*Razza Consulting Group Inc.*

[cesca.cruz@razzaconsulting.com](mailto:cesca.cruz@razzaconsulting.com)

**Asst. Prof. Joseph Hermocilla**

*Assistant Professor*

*UPLB Institute of Computer Science*

[jhermocilla@up.edu.ph](mailto:jhermocilla@up.edu.ph)