CRYPTONITE JTP II

Congratulations for making it through TP-1.
You are now a part of Cryptonite's second task phase.

This will last from **October 22, 2025** to **December 7, 2025**.
A final *offline* interview will be held at the start of the next semester.

For the first stage, you're going to be completing a set of selected challenges on CMU's PicoCTF platform: PicoCTF

The deadline to finish **all** of the below PicoCTF challenges is **31 October, 2025**.

Reverse Engg.	**Forensics**	**Web Exp**	**Cryptograph**	**Binary Exp**	**Hardware**
GDB baby step 1	trivial flag transfer protocol	Web Gauntlet	RSA oracle	buffer overflow 0	IQ Test
ARMssembly 1	tunn3l v1s10n	SSTI1	Custom encryption	format string 0	I like Logic
Vault door 3	m00nwalk	Cookies	miniRSA	clutter overflow	Bare Metal Alchemist

You are also required to attach a final screenshot of your dashboard with your username and graph of all challenges solved in your repository's `README.md` file.

In addition to these mandatory challenges, you are also required to complete 5 custom challenges in any two domains of your interest. These will be provided after the completion of PicoCTF challenges.

You are expected to make detailed writeups for each and every one of the challenges. They must include:

- The flag you found after solving the challenge.
- Your thought process and approach to the challenge.
- Every single new concept and point of knowledge you learned or improved upon through solving the challenge.
- Any incorrect tangents you went on while solving, and why.

A few other pointers:

- Avoid using screenshots for terminal output; use triple backticks instead.
- Include textual outputs and screenshots for everything.
- Flags for Pico are unique, so don't copy others' flags or work.
- Your reasoning must be non GPTish and **usage of LLMs is barred**.

Writeups should go into a `picoctf/` directory in your task phase repos, and all domains should have a single file with all the writeups, e.g. `picoctf/Cryptography.md`.

RESOURCES

What is a CTF?

- What is a CTF?

Reverse Engineering

- Intro to Reverse Engineering
- Reverse Engineering Walkthrough
- Reverse Engg. Playlist

Forensics

- Forensics Intro
- Trail of Bits — CTF Forensics
- John Hammond — CTF Katana

Cryptography

- CTF101 — Cryptography Overview
- W3Schools — Python Tutorial
- Cryptography Playlist

Web Exploitation

- Web Exploitation Intro
- WebEx Walkthrough
- Web Exploitation Playlist A
- Web Exploitation Playlist B

Binary Exploitation

- CTF101 — Binary Exploitation
- Binary Exploitation Intro
- Binary Exploitation Playlist

Hardware

- Modulation
- Logic Gates
- Communication Protocols