Capture The Flag

Overview

Capture The Flag (CTF) competition follows the tried and tested approach of hiding flags inside purposefully-vulnerable programs/web apps, which the participants are expected to retrieve by exploiting the vulnerabilities present in the program/web apps. The contest encompasses multiple challenges belonging to a wide array of cybersecurity categories.

Rounds

The competition consists of only one round:

Round 1: The participants will be given 3 hours to solve five challenges belonging to the following categories:

I. Web Security
II. Cryptography
III. Reverse Engineering & Binary Exploitation
IV. Forensics
V. Open-Source Intelligence (OSINT)

The winning team will be decided according to no. of challenges solved, with submission timestamp being the tiebreaker.

Team Formation

Each team can have a maximum of 3 members.

Rules

- Internet access will be allowed throughout the competition venue for the submission.
- The challenges will be hosted on an online platform i.e. CTFd, etc
- Teams are **required** to bring their own laptops with a native/VM Linux distro (preferably Kali or Parrot OS).
- Edibles are **strictly prohibited** in the competition venue
- Any team will **disqualify** due to any of the reasons mentioned below:
    - Plagiarism / Collaborating with other groups
    - Sharing credentials with outsiders
    - Sharing of captured flags
    - Disturbance or misconduct with any invigilator or fellow competitors
- Competition will be started on the stated time. All teams are expected to arrive on time or earlier to get a head start on instructions.

- The organizers reserve the right to modify the rules or competition parameters in the event of unforeseen challenges, technical difficulties, or circumstances beyond control.