Intro to CTF / Setup

OSDC : Open Source Developers' Community of JIIT Noida , 62

WTF is CTF ?

CTF

{ Capture The Flag }

kind of information security competition ,

in which players put their skills to solve variety of

tasks ranging from solving

problems or to break into an opponent's system.

s4m71ng_s4m71ng_l1k3_7h15

Gamified hacking

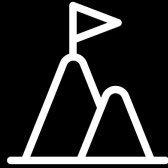Today's meet will focus on CTF contests

We learn to:

- Reverse engineer programs
- Find bugs and hack things
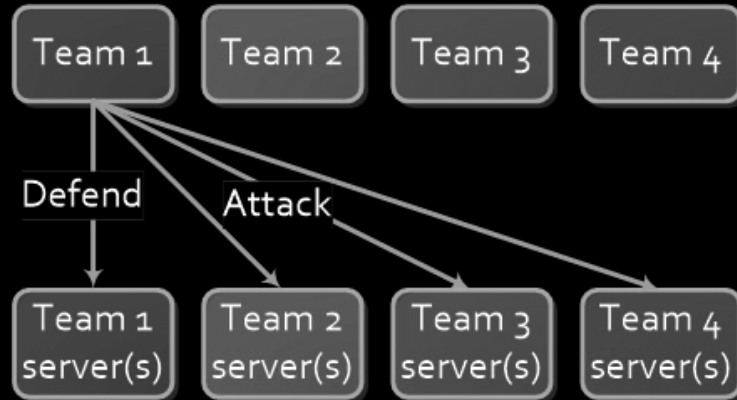- Break insecure cryptosystems

Playing CTF for fun
Playing CTF to learn
Solving challenges yourself
Taking solution from past writeup
Meeting new friends
Playing CTF to win
adjusting sleep schedule for 48hr CTF
CTF-specific tooling and scripts
coffee; energy drinks
clearing time for CTF
canned solutions for stereotyped problems
TABOO CTF TACTICS
begging for hints
flag hoarding
guessing/cheesing flags
abusing university clusters to brute force
trading hints with other teams
renting vps in same colo to brute
FORBIDDEN CTF TACTICS
nmapping IG to find chals early
straight-up flag sharing
attacking competition infrastructure (DoS)
adderall abuse
CURSED CTF TACTICS
ctftime weight manipulation
ctftime multiaccounting
attacking organizers
collusion, bribery of organizers; nepotism
hosting bogus ctfs
rooting competition infrastructure
ctfd backdoor
flag stealing and espionage
manufacturing drama so other teams disband
attacking other competitors
blackmailing organizers
blackmailing teammates

TYPES of CTFs :

1 . Jeopardy Style

2. Attack / Defense Style

| Team 1 | Team 2 | Team 3 | Team 4 |

Defend   Attack

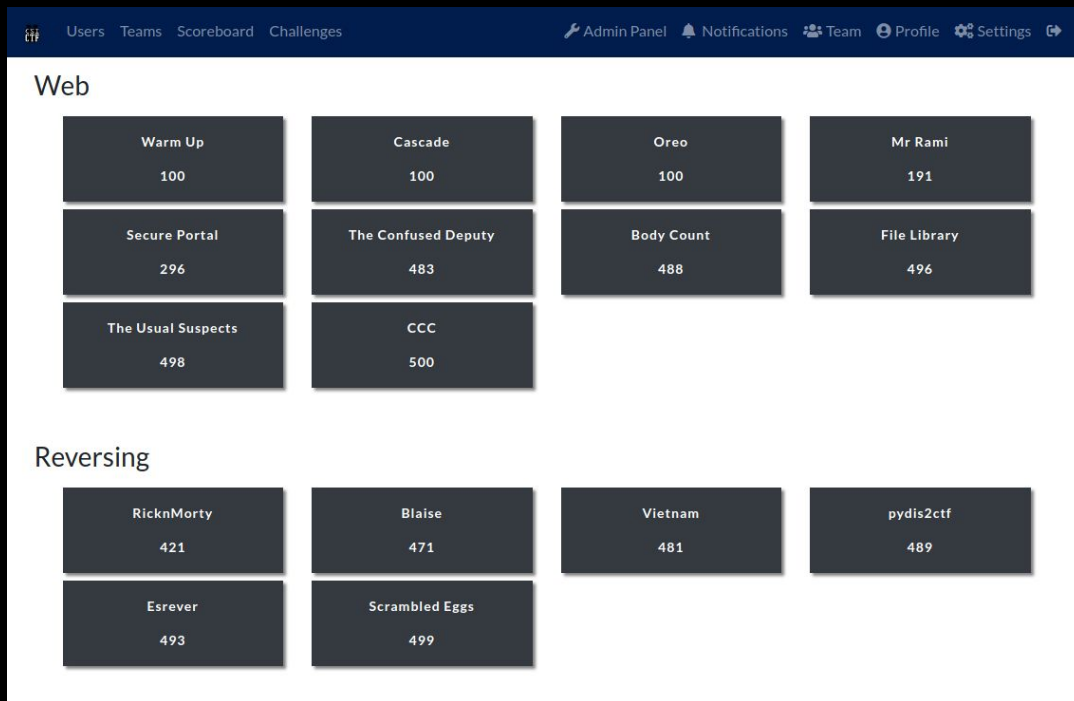| Team 1 server(s) | Team 2 server(s) | Team 3 server(s) | Team 4 server(s) |

Jeopardy style CTFs challenges are typically divided into categories

- **Cryptography - Typically involves decrypting or encrypting a piece of data**

- **Steganography - Tasked with finding information hidden in files or images**

- **Binary - Reverse engineering or exploiting a binary file**

- **Web - Exploiting web pages to find the flag**

- **Pwn - Exploit a binary typically running on a remote server**

What might a typical CTF look like?

Why play CTFs?

CTFs are a great opportunity to:

- Have fun
- Meet an awesome community
- Learn a lot about tons of topics
- Win prize money and free trips

How do I start playing?

- Introductory
  - picoCTF (CMU)
  - TJCTF (TJHSST)
  - HSCTF (WW-P HSN)
- Intermediate
  - CSAW CTF (NYU Tandon)
  - UIUCTF (UIUC)
- Professional
  - DEF CON CTF
  - PlaidCTF (CMU)
  - DiceCTF

ctftime.org

CTF>TIME

CTFs   Upcoming   Archive ▾   Calendar   Teams ▾   FAQ   Contact us ▾   About

Sign in

3   ECSC TeamNL   55.795
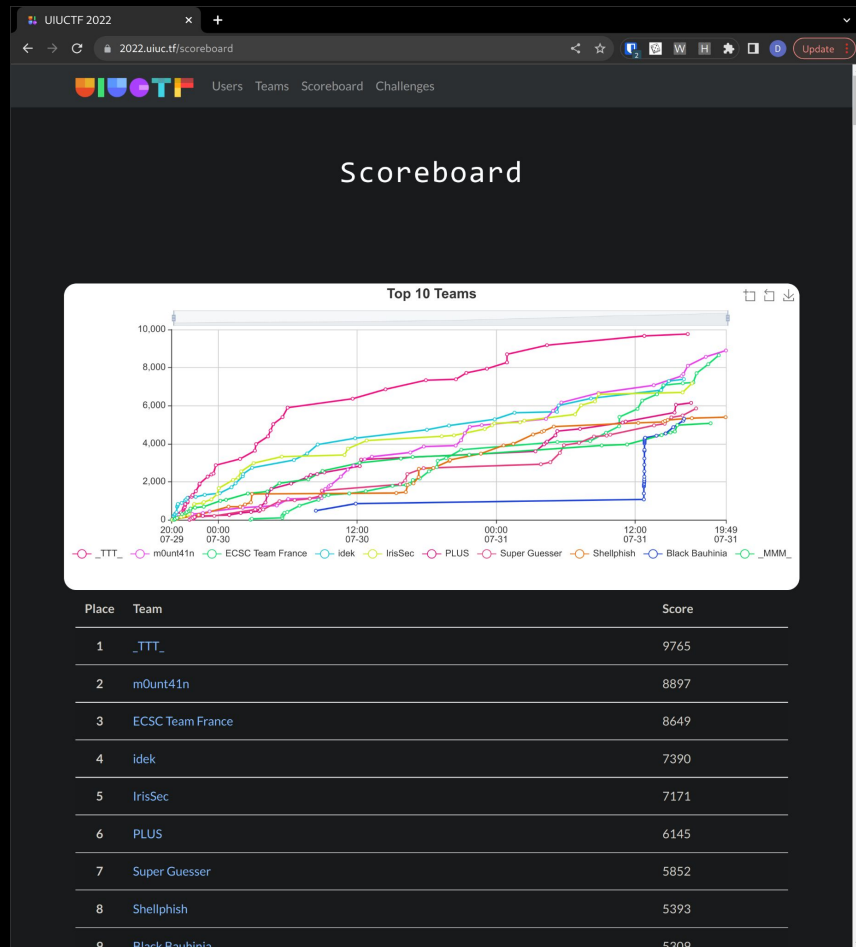
Full rating | Rating formula

1423 teams total | Tasks and writeups

Upcoming events 📅 📶

| Open | Finals |

WACON 2023 Prequal

Sept. 03, 2023 00:00 UTC | Online | Weight voting in progress

Place	Team	Country	Points *
👑 1	ARESxSekai		0.000
2	perfect blue	🇺🇸	0.000
3	0ops	🇨🇳	0.000

110 teams total | Tasks and writeups

Format	Name	Date	Duration
▦	HITCON CTF 2023 Quals 🌐 On-line	Fri, Sept. 08, 14:00 — Sun, Sept. 10, 14:00 UTC 120 teams	2d 0h
▦	PatriotCTF 2023 🌐 On-line	Fri, Sept. 08, 21:00 — Sun, Sept. 10, 21:00 UTC 89 teams	2d 0h
▦	Cyber Heroines CTF 🌐 On-line	Fri, Sept. 08, 21:00 — Sun, Sept. 10, 21:00 UTC 44 teams	2d 0h
▦	Information and Technology Festival 2023 🌐 On-line	Sat, Sept. 09, 08:00 — Sun, Sept. 10, 08:00 UTC 20 teams	1d 0h
▦	COMPFEST CTF 2023 🌐 On-line	Sun, Sept. 10, 00:00 — Mon, Sept. 11	1d 0h

Prerequisites

You would think that doing CTFs would require a lot of prior knowledge, but that is not actually true. In reality, it only requires:
- Willingness to learn
- That's about it :)

No but really, in reality you just need to be willing to Google search and ready to explore!

HANDS ON!!

flag{thanks_for_coming!}

Further practice

https://overthewire.org/wargames/bandit/

Resources

- **CTF teams:** https://ctftime.org/stats/
- **Upcoming CTFs:** https://ctftime.org/event/list/upcoming
- **Learn more about CTF:**
    - https://trailofbits.github.io/ctf/
    - https://ctf101.org/
    - https://pwning.net/2014/04/01/why-ctf/
- **Get started:** https://picoctf.org/