What is a CTF?

ggu

slides by balex

What is a CTF?

A CTF (Capture the Flag) is a security-focused competition in which teams solve various challenges from different fields of security.

When you solve each challenge, you get a flag (string of text) that you then can turn in for points.

The team with the most points wins!

How do they work?

- You have the main CTF website, where you will get challenge prompts and turn in flags. There's also usually a leaderboard, some rules, and the challenges page.
- Usually the CTF challenges are divided into categories based on topic, and the problems worth more points are typically more difficult.
    - Some CTFs use dynamic scoring, which means that all the problems start out with the same point value, and they decrease over time as they get more solves (since they're easier). The points go down even for people who have already solved it.
    - A few CTFs give out bonus points for being the first team to solve a challenge

How do they work?

- To start a challenge, click on it and read whatever prompt there is. You should also be given any files or links necessary to solve the challenge.
- Complete the challenge. The way to do that is up to you, and you can use any sort of resource you want (internet, friends, class notes, etc.)
- Get the flag. You should be given a flag format so you know what they look like (e.g. `utflag{example_flag}`). Copy the flag and paste it into the challenge page to get your points!

Categories

These are the main categories that you will see on different CTFs, although not all CTFs will have all of them:

- Binary Exploitation
- Cryptography
- Forensics
- Miscellaneous
- Networking
- Reverse Engineering
- Web

Binary Exploitation (or Binary, PWN, BinExp)

- You are given computer programs that purposefully have flaws in them that you must exploit
- Require knowledge about computer architecture, operating systems, Linux, etc.
- These are typically on the more difficult side
- Tools: Terminal, GNU Debugger (`gdb`), `gef`

Cryptography (or Crypto)

- Deals with codes, ciphers, encryption, etc.
- You might have to implement a cryptosystem (specific crypto algorithm), exploit a weakness in a cryptosystem, undo a cipher or encryption, or even figure out how a custom cryptosystem works
- Can range from very easy to very hard, typically the harder problems have lots of math involved
- Tools: CyberChef, SageMath

Forensics

- Deals with files and hiding information
- You may have to fix broken files, crack passwords, find hidden messages inside of files, and do reconnaissance on a fake person (find out info about them).
- This category is very vague, so you might see lots of different things. Typically forensics problems are on the easier side and may require special tools.
- Tools: `xxd`, `binwalk`, `file`

Miscellaneous (or Misc)

- As the name implies, this could be pretty much anything. Creators put any problem that doesn't quite fit into the other categories in Misc.
- A few things that are pretty common
- Esoteric languages: very specific programming languages you've probably never heard of. Like one that reads like Shakespeare plays. Or one where you can only use dog commands (fetch, sit stay).
- Map-related challenges: a lot of challenges have to do with map locations, lat/long coordinates, etc.
- Tools: Esolangs.org, What Three Words, Google :)

Networking

- Deals with information sent across networks between computers
- You may have to look at some captured packets (information that was sent over a network) to see what was being sent, or you may have to figure out a custom protocol (specific formats that computers use to communicate).
- Are usually on the more medium to hard side difficulty-wise
- Tools: Wireshark, `netcat`/`nc`

Reverse Engineering (or RevEng, Rev)

- Given a computer program, figure out what it does.
- You might have to look into the program to see what inputs it needs to give out the flag, or try to figure out how to trick or break the program to give up secrets.
- Usually medium to hard difficulty
- Tools: Ghidra, IDA, Cutter

Web

- Everything related to websites and web applications.
- May have to exploit a vulnerable website to give you secret information or trick a website into thinking you're an administrator.
- Can range from easy to very hard.
- Tools: Developer Tools on your browser, BurpSuite

It's CTF Time

- Connect to ctf.isss.io to try your hand at a CTF!