So you think you can break stuff?

...

Cyber@UCR

What's a CTF?

- Capture-the-Flag, simply put, you're just solving puzzles to get a flag that gives you points.
- The puzzles could be any of the following:
  - Pwning
  - Cryptography
  - Steganography
  - OSINT
  - Reversing
  - Log Analysis

Pwning

- There is something wrong with the program and you must figure out what is wrong and break it.
  - Example: Use-After-Free, Memory leak, race condition, heap/stack/buffer overflow
  - Little_tommy on HTB

Crypto

- Crack a crypto-system or algorithm or derive it to get the key/flg.
  - Example: crack a weak RSA program, this can be done with some Python and some math.

OSINT

- Open-Source-INTelligence
- GOOGLE!!!
  - How well can you google to find the answer, google accepts regex, there is a guide called “Hacking Google” or something and is about 100 pages and details how to use a lot of that google trickery to find things faster.

Steganography

- Hiding stuff in plain sight.
  - Could be hidden whitespace character, hex data in an image, hiding a zip in a picture, etc
  - Forest on HTB

Reversing

- Given an executable, figure out how it works and get the flag
- Usually using a debugger like gdb or a reversing tool like radare2 or IDA or Ghidra.
  - IOLI crackmes: https://github.com/Maijin/Workshop2015, intro workshop to r2
  - Cbm-hackers on crackmes.one, easy_reverse

Log Analysis

- Find stuff in a large log file
- Example: given a bunch of network logs from wireshark, find out what a specific user was trying to find and the flag is found in the logs.

Questions?

- What do I need to get started?
- What do I need to know?
- What are some good starting resources?
- Do I need to be able to read assembly? Do I need to be able to read C/C++?
- How much math do I need?
- Are there any classes at UCR that will cover this material?
- How can I prepare for doing CTF's?
- CPTC?
- ???

Let’s start!

- picoCTF
- crackmes.one
- HackTheBox.eu