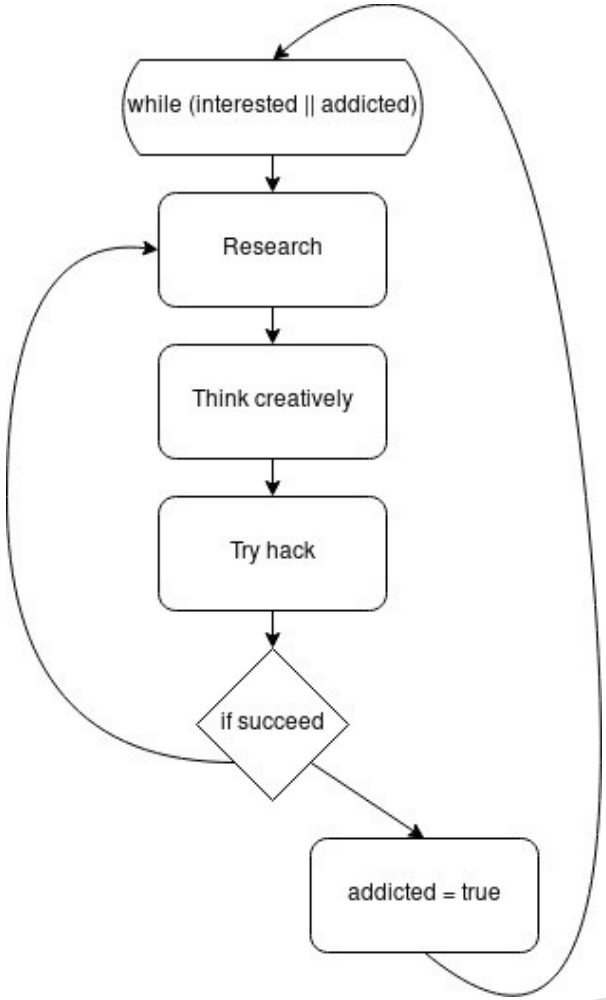
How to HAX this CTF

Hacking Mindset

(yes I'm keeping these titles)

- Think creatively
- Find a way in
  - Unlike a normal CTF there is not just one way
- Do research



Linux/terminal

- Powerful tool for scripting and exploits
- <command> <file>
- Directory tree/path traversal
- linux.wpi.edu example:

- How can I practice/work on this?
  - Get a VM – VirtualBox + OSboxes.org
  - Read the man pages/search engine/CSC Slack if lost

Reverse Engineering

- Take CS-2011
- Code we write → executable
- SEE JUSTIN

Reversing

Whirlwind tour

- If the source code for a software is unavailable, we generally reverse engineer the binary
- Common that you'll have the executable but not the source
- If it's on your computer you're golden

Whirlwind tour

- (Free) Tools
- GDB, Radare2
- There are also paid tools…. Not worth.

Quick and painless demo

Using R2

Code/Web Injections

- Stuffing code into input fields
  - Frequently seen in SQL injections
- Useful in many different exploits
- Lazy Python code example:

Encryption

- (see Nicole’s computer/USB – the slides are here but LibreOffice cannot handle them)

Port Scanning

- Do NOT do while on WPI’s network
- Port is network communication endpoint
  - 65535
- Many applications/ports tied
- Nmap

CTF Practice/resources

- Read about some fun pen-testing stories
  - Rapid7
- PicoCTF – beginner, available year-round
- RootMe – fun CTF challenges
- Bomblab – available on Github and CS-2011
- **Bandit Overthewire**