CTF $EVENT

In introduction to Capture the Flag events

@hanemile - 2022-02-05 - @chaosdorf

What?

Capture The Flag

Break into a real bank

Illegal

Novel

Exciting

CTF

Realistic

Challenging

Build your own bank
Break into it

Legal

Boring

Not “real world”

Unrealistic

Kinds

- Jeopardy
- Attack and Defence
- Wargames

Jeopardy

“Just solve challenges”

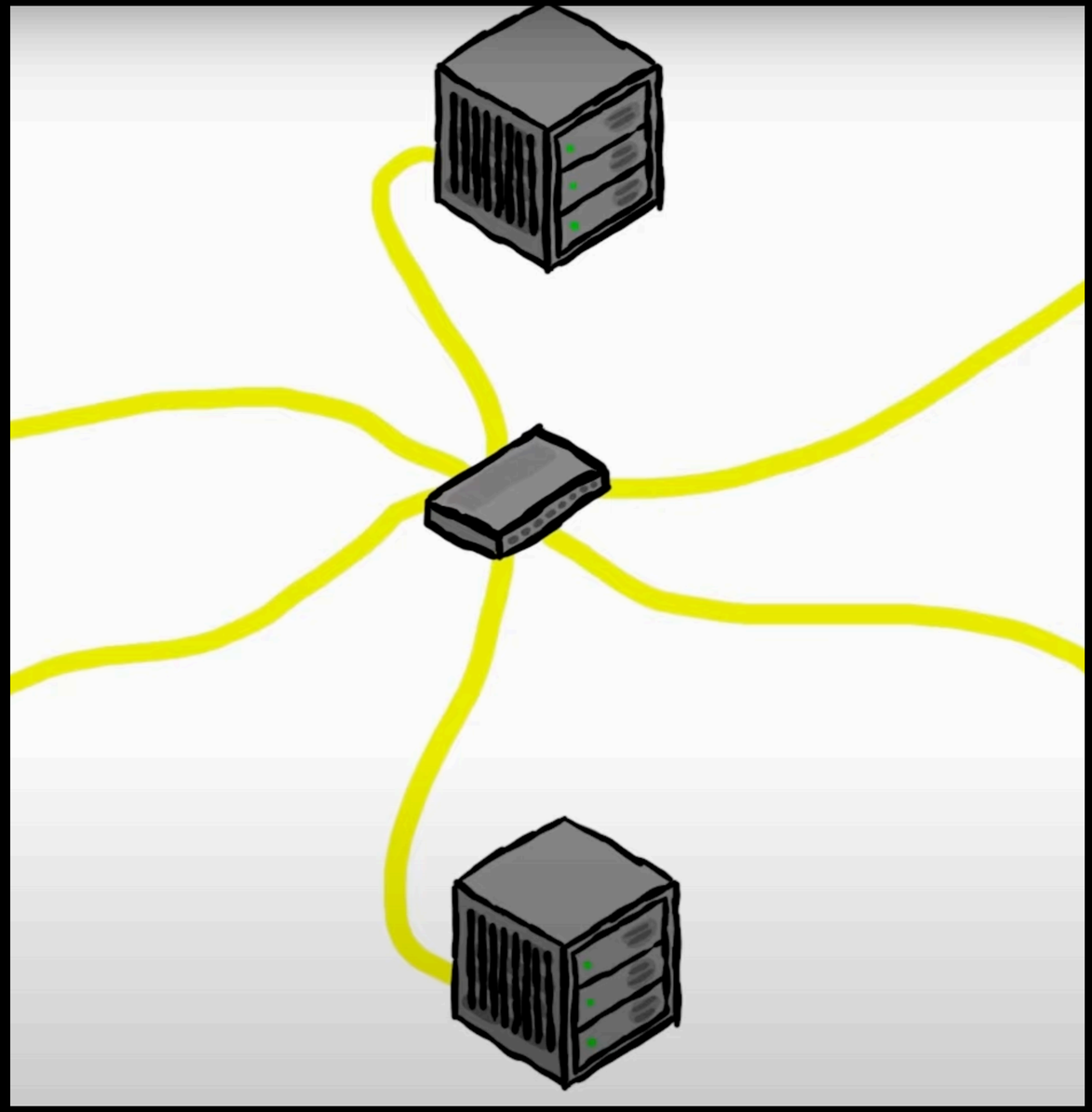
- Name
- Description
- Files
- Remote
- Points
- Hints

Attack and Defence

“PVP”

- Services
- SLA
- Ticks

- https://www.youtube.com/watch?v=RkaLyji9pNs



Basics

Agenda

- Find Team

CTF announced

- Register Team

CTF start

- Solve challenges

CTF end

- Write write-ups

Flag
Proving the hack

- Unique string only obtainable by solving challenge

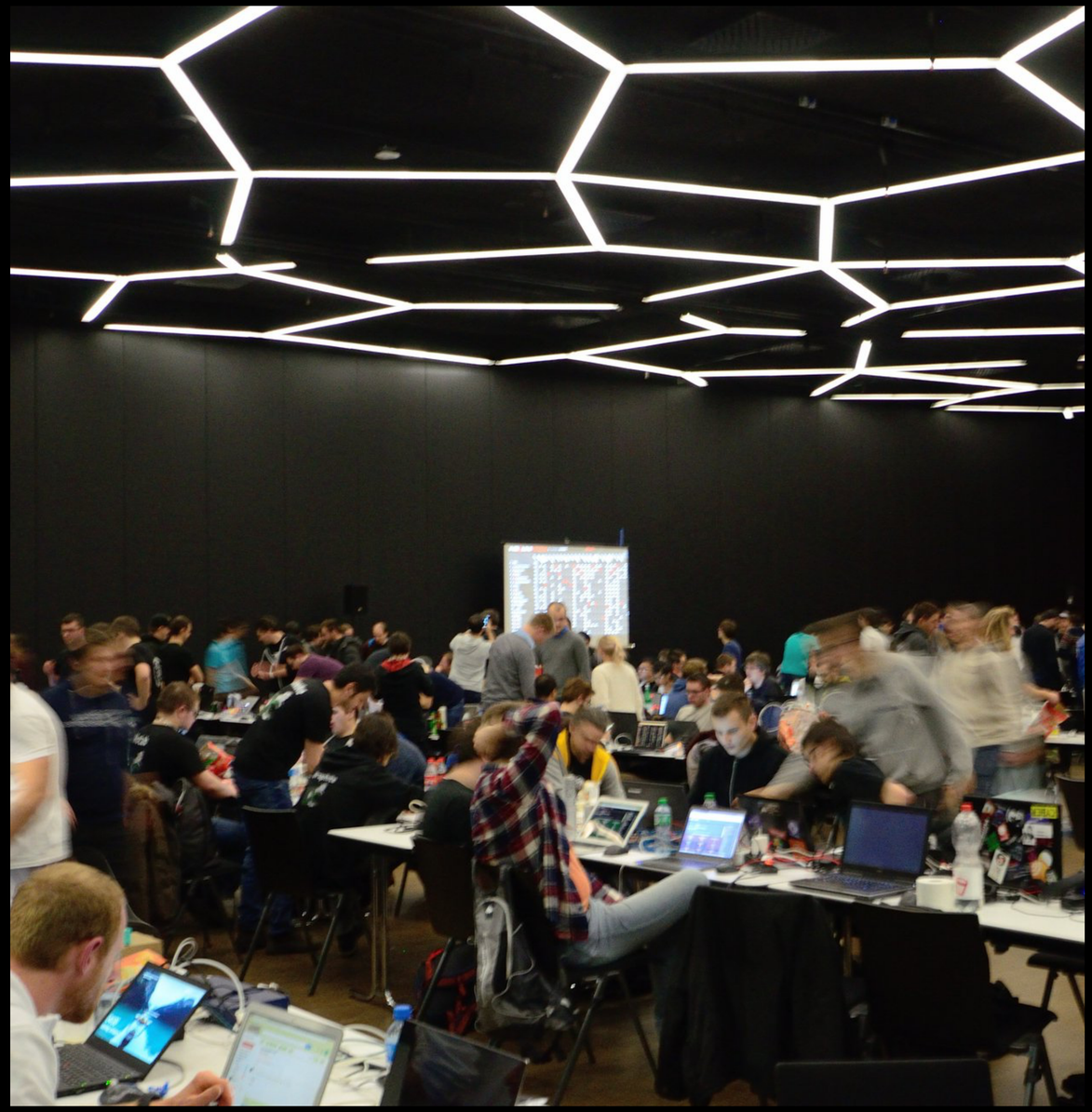
- Flag{…}
- SomeCTF{…}
- attctf_12983798172312938128379182 73

Challenge categories

pwn	Binary Exploitation	Remote
rev	Reversing	Local
crypto	Cryptography	Mathe
web	Web	Browser
forensics	Forensics	Archäologie
misc	Miscellaneous	Sandbox

Who?

- Combinations of people from all places
- Universities
- Hackspaces
- Conferences
- Industry



Requirements

- Willpower
- Time
- Interest

CTF in 3… 2… 1…

Before

- VM / Docker / Tools
- Collab tools (pad, video conf, discord, …)
- Internet
- Power
- Eat + Sleep

Start

- Don’t Panic!
- Read the description / all the data given
- Experiment

During

- Select Challenge
- Deep dive
- Solve
- Eat + Sleep

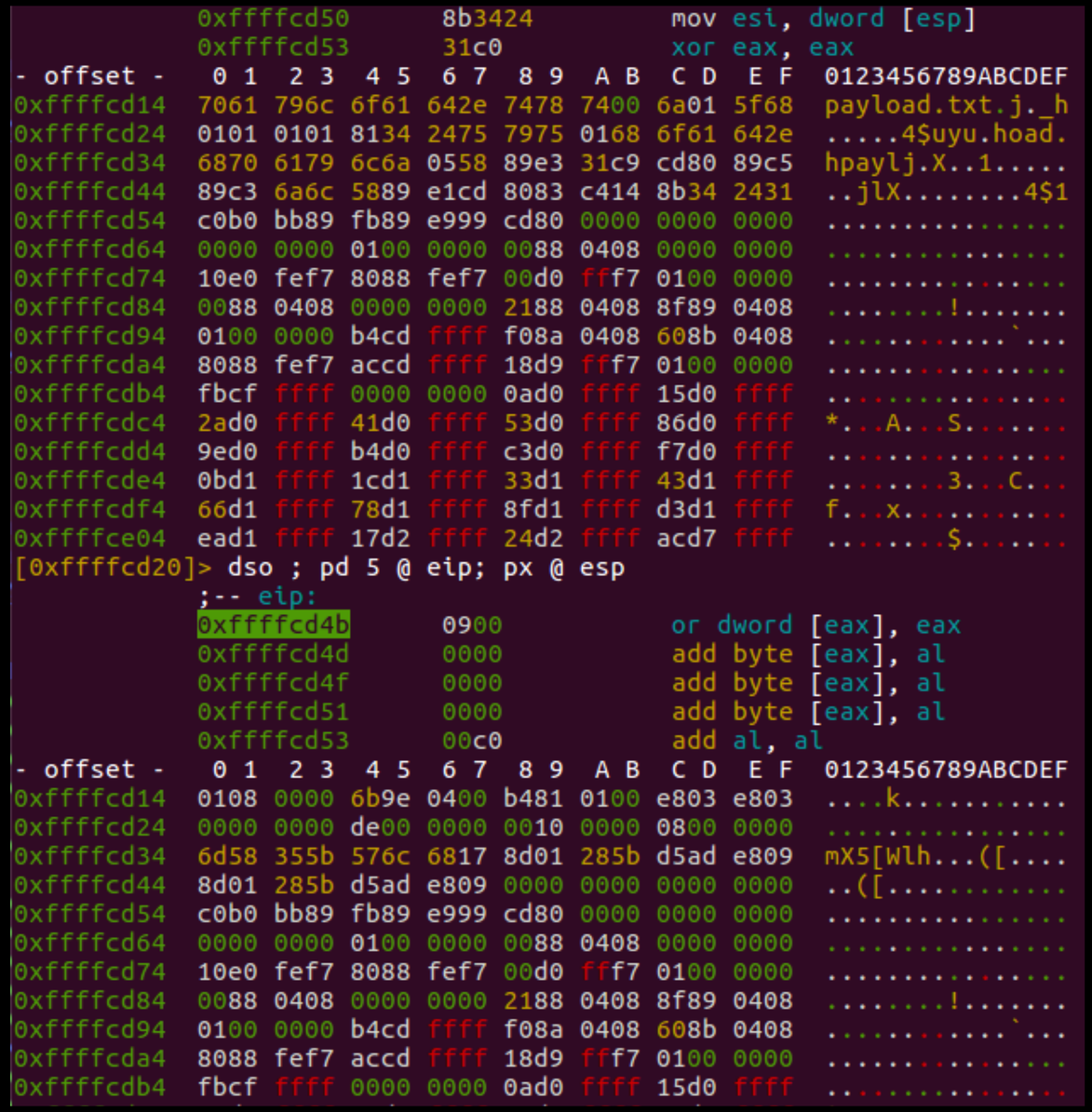
After

- Write Writeups
  - 1 sentence to n pages
  - Video
  - Talk
- Read Writeups
  - Challenge not solved?
- Solve unsolved challenges

Tooling

Pwn

- IDA, Ghidra, Binary Ninja, Hopper, Radare2
- Python pwntools <3
- Debug: gdb + (get, peda, pwntools), radare2
- Nc
- …

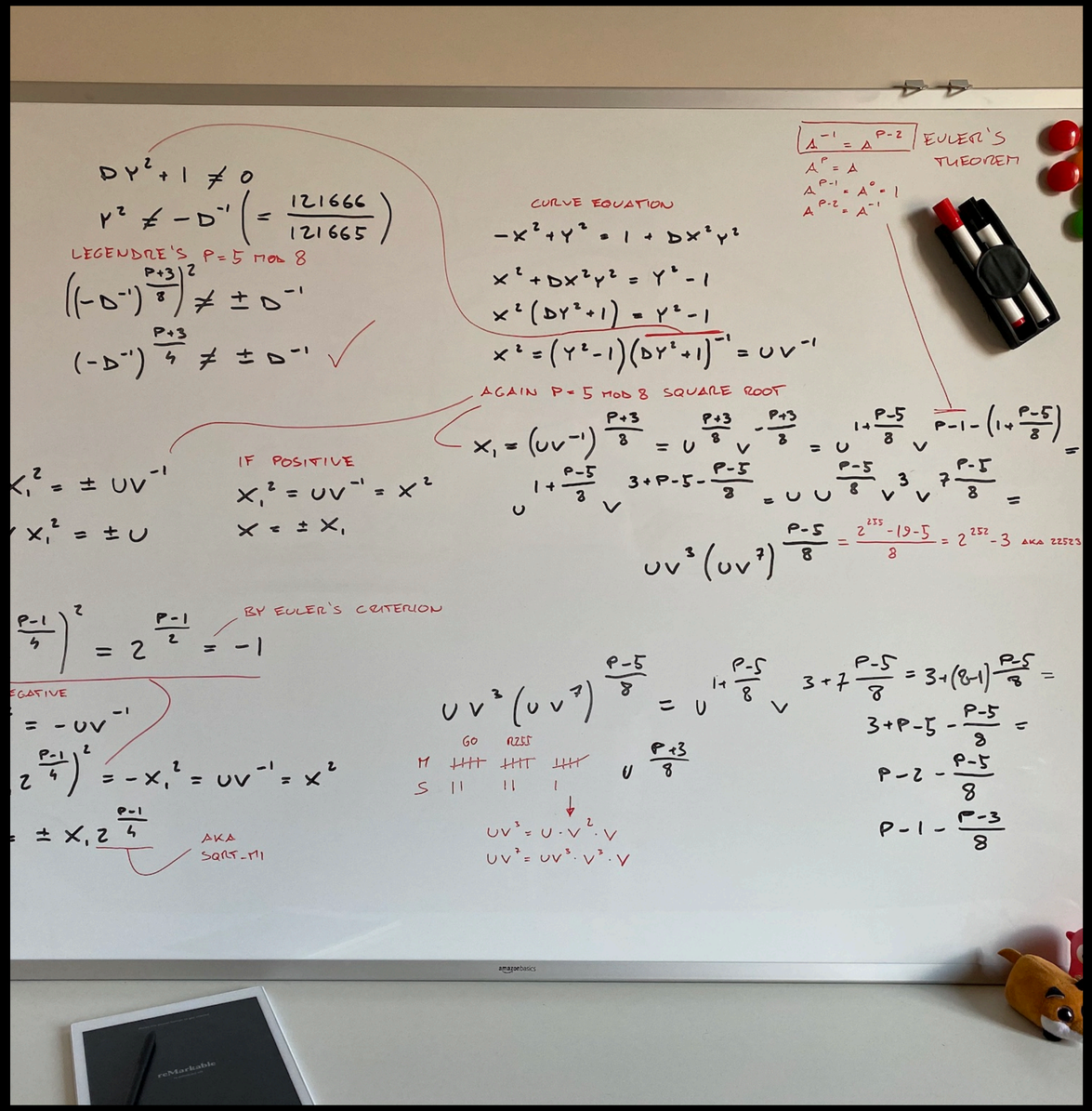


Rev

- IDA, Ghidra, Binary Ninja, Hopper, Radare2
- Python pwntools <3
- Debug: gdb + (get, peda, pwntools), radare2
- …

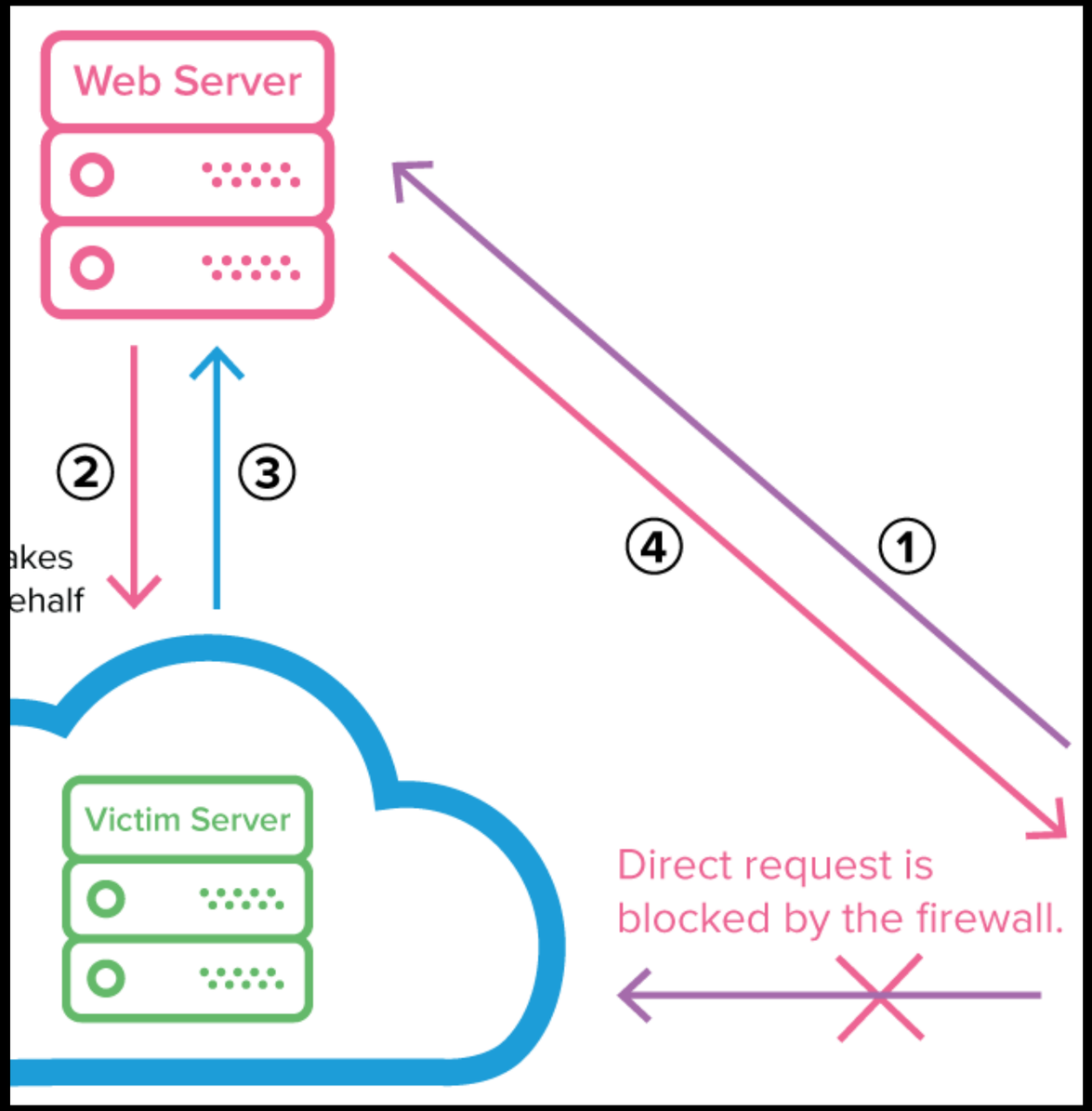
Crypto

- Python
- Sage
- Pen + Paper
- PDF Viewer
- …



Web

- Proxy: Burp Suite, OWASP Zap, MitmProxy
- Discovery
  - Fuzz: dirb, dirbuster, gobuster, wfuzz, ffuf
  - Spider: gospider
- …



Forensics

- volatility
- binwalk
- $(HEX)EDITOR

Misc

- …

Help!

Help

- man …
- $SEARCHENGINE (google, duck duck go, wolfram alpha)
- Read ALL the documents (3 times)
- Other people

Training

- Pwn: pwn.college
- Crypto: cryptohack.org
- Web: portswigger academy

- https://emile.space/ctf/

Hack The Planet!

ctf.emile.space