

CTF \$EVENT

In introduction to Capture the Flag events

@hanemile - 2022-02-05 - @chaosdorf

What?

Capture The Flag



Break into a real bank



Illegal

CTF



Legal

Build your own bank
Break into it

Realistic

Novel

Challenging

Boring

Exciting

Not "real world"

Unrealistic

Kinds

- Jeopardy
- Attack and Defence
- Wargames



Jeopardy

“Just solve challenges”

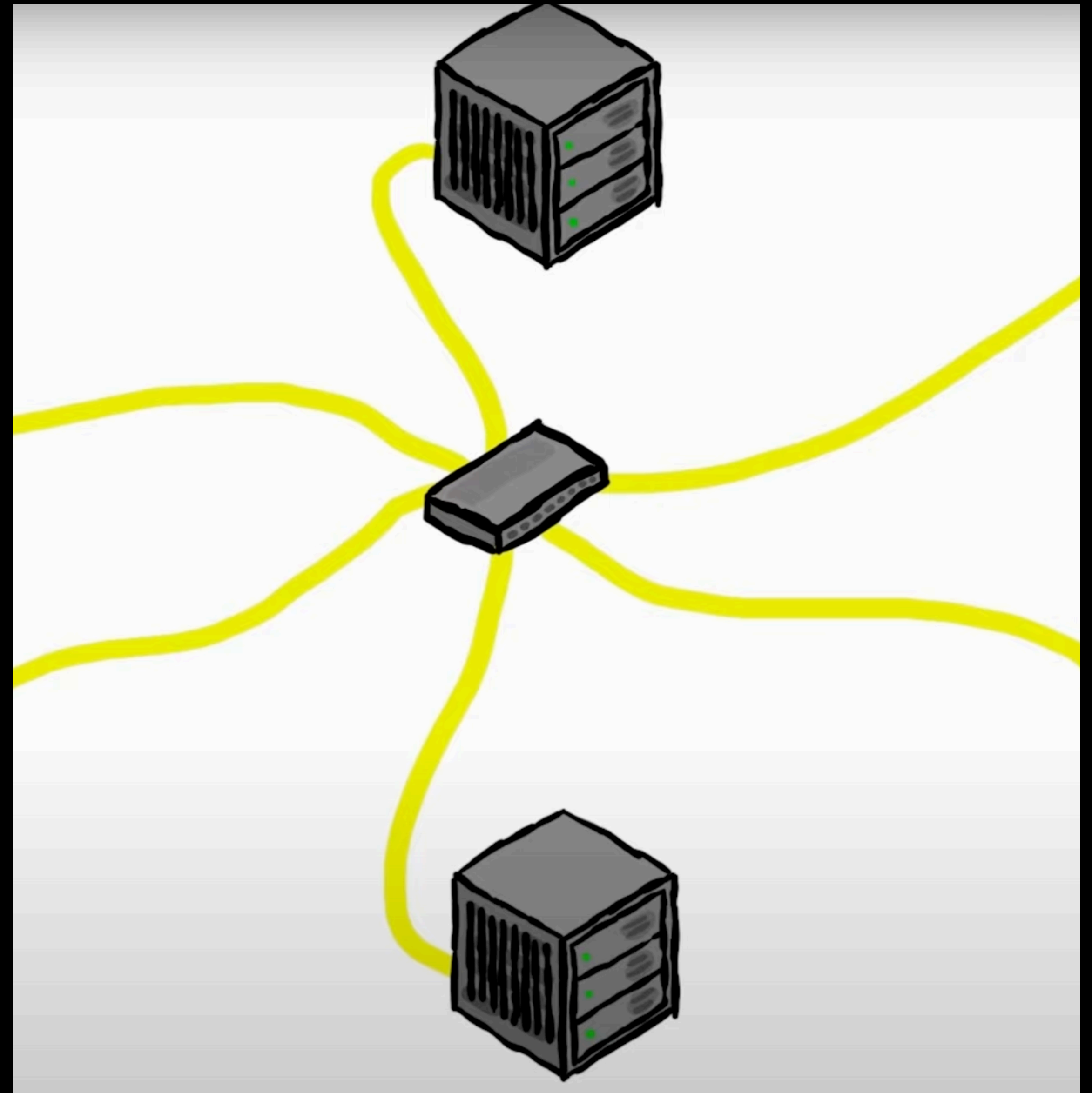
- Name
- Description
- Files
- Remote
- Points
- Hints

萌新1~baseblu ✓ 1	萌新2~凯撒大帝 ✓ 1
萌新5~word文件本质 ✓ 92	萌新6~excel也疯狂 ✓ 97
萌新8~破译密码 100	萌新10~莫斯 100
萌新14~二维码 100	萌新15~zip伪加密 ✓ 100
萌新18~Spamcarver 100	萌新19~暴力破解 100

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_1298379817231293812837918273

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

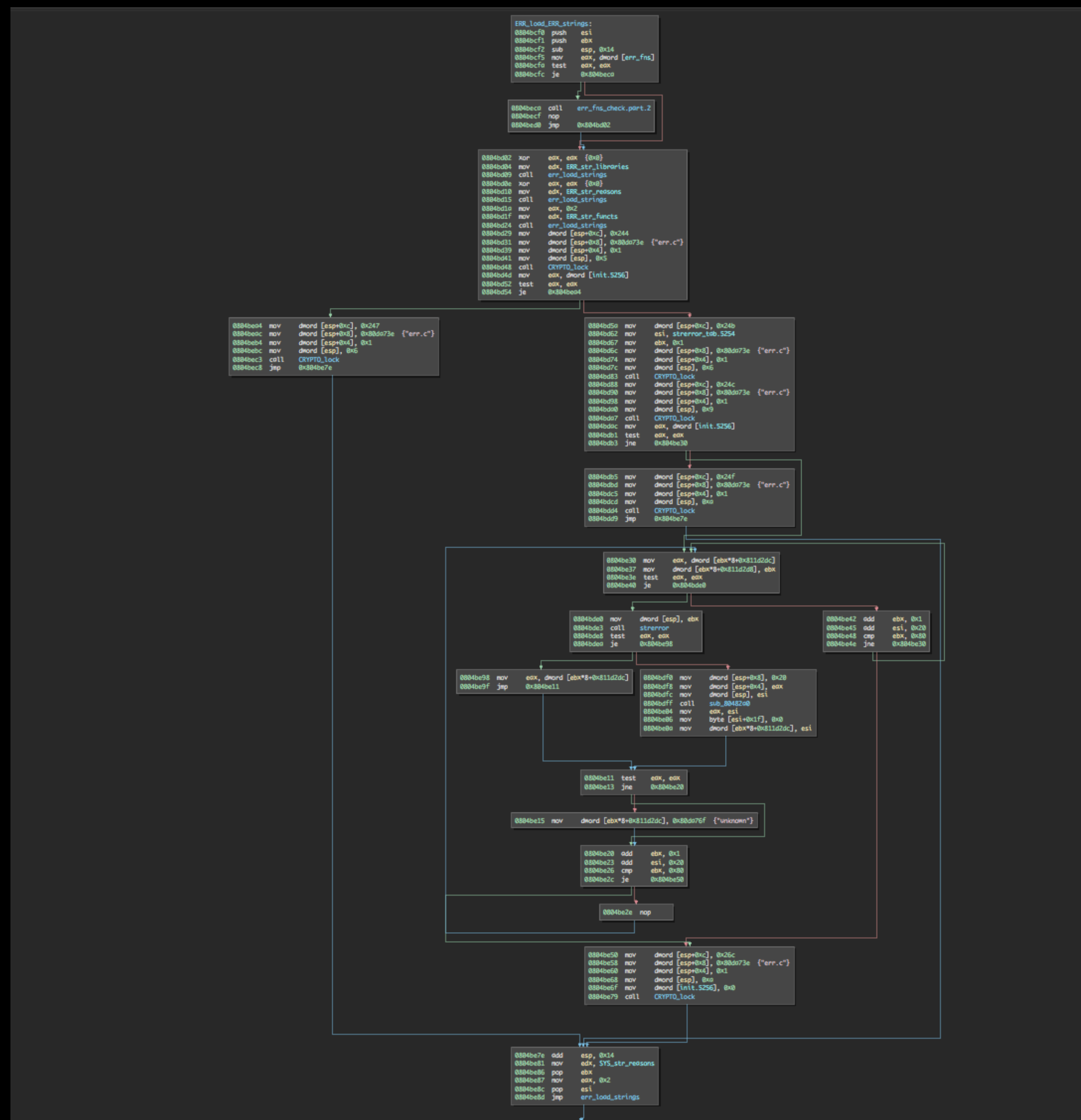
Pwn

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

```
0xffffcd50      8b3424      mov esi, dword [esp]
0xffffcd53      31c0        xor eax, eax
- offset -    0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
0xffffcd14    7061 796c 6f61 642e 7478 7400 6a01 5f68 payload.txt.j._h
0xffffcd24    0101 0101 8134 2475 7975 0168 6f61 642e .....4$uyu.hoad.
0xffffcd34    6870 6179 6c6a 0558 89e3 31c9 cd80 89c5 hpaylj.X..1.....
0xffffcd44    89c3 6a6c 5889 e1cd 8083 c414 8b34 2431 ..jlx.....4$1
0xffffcd54    c0b0 bb89 fb89 e999 cd80 0000 0000 0000 .....
0xffffcd64    0000 0000 0100 0000 0088 0408 0000 0000 .....
0xffffcd74    10e0 fef7 8088 fef7 00d0 fff7 0100 0000 .....
0xffffcd84    0088 0408 0000 0000 2188 0408 8f89 0408 .....!.....
0xffffcd94    0100 0000 b4cd ffff f08a 0408 608b 0408 .....`...
0xffffcda4    8088 fef7 accd ffff 18d9 fff7 0100 0000 .....
0xffffcdb4    fbcf ffff 0000 0000 0ad0 ffff 15d0 ffff .....
0xffffcdc4    2ad0 ffff 41d0 ffff 53d0 ffff 86d0 ffff *...A...S.....
0xffffcdd4    9ed0 ffff b4d0 ffff c3d0 ffff f7d0 ffff .....
0xffffcde4    0bd1 ffff 1cd1 ffff 33d1 ffff 43d1 ffff .....3...C...
0xffffcdf4    66d1 ffff 78d1 ffff 8fd1 ffff d3d1 ffff f...x.....
0xffffce04    ead1 ffff 17d2 ffff 24d2 ffff acd7 ffff .....$.
[0xffffcd20]> dso ; pd 5 @ eip; px @ esp
;-- eip:
0xffffcd4b      0900      or dword [eax], eax
0xffffcd4d      0000      add byte [eax], al
0xffffcd4f      0000      add byte [eax], al
0xffffcd51      0000      add byte [eax], al
0xffffcd53      00c0      add al, al
- offset -    0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
0xffffcd14    0108 0000 6b9e 0400 b481 0100 e803 e803 .....k.....
0xffffcd24    0000 0000 de00 0000 0010 0000 0800 0000 .....
0xffffcd34    6d58 355b 576c 6817 8d01 285b d5ad e809 mX5[wlh...([....
0xffffcd44    8d01 285b d5ad e809 0000 0000 0000 0000 ..([.....
0xffffcd54    c0b0 bb89 fb89 e999 cd80 0000 0000 0000 .....
0xffffcd64    0000 0000 0100 0000 0088 0408 0000 0000 .....
0xffffcd74    10e0 fef7 8088 fef7 00d0 fff7 0100 0000 .....
0xffffcd84    0088 0408 0000 0000 2188 0408 8f89 0408 .....!.....
0xffffcd94    0100 0000 b4cd ffff f08a 0408 608b 0408 .....`...
0xffffcda4    8088 fef7 accd ffff 18d9 fff7 0100 0000 .....
0xffffcdb4    fbcf ffff 0000 0000 0ad0 ffff 15d0 ffff .....
```

Rev

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



Crypto

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

$DY^2 + 1 \neq 0$
 $Y^2 \neq -D^{-1} \left(= \frac{121666}{121665} \right)$

LEGENDRE'S $P=5 \pmod 8$
 $\left((-D^{-1})^{\frac{P+3}{8}} \right) \neq \pm D^{-1}$
 $(-D^{-1})^{\frac{P+3}{4}} \neq \pm D^{-1} \checkmark$

CURVE EQUATION
 $-X^2 + Y^2 = 1 + DX^2Y^2$
 $X^2 + DX^2Y^2 = Y^2 - 1$
 $X^2(DY^2 + 1) = Y^2 - 1$
 $X^2 = (Y^2 - 1)(DY^2 + 1)^{-1} = UV^{-1}$

AGAIN $P=5 \pmod 8$ SQUARE ROOT
 $X_1 = (UV^{-1})^{\frac{P+3}{8}} = U^{\frac{P+3}{8}} V^{-\frac{P+3}{8}} = U^{1+\frac{P-5}{8}} V^{-\frac{P-5}{8}} = U^{2+\frac{P-5}{4}} V^{-\frac{P-5}{8}}$
 $U^{1+\frac{P-5}{8}} V^{3+P-5-\frac{P-5}{2}} = U U^{\frac{P-5}{8}} V^3 V^{\frac{P-5}{2}}$
 $UV^3 (UV^{\frac{P-5}{2}})^{\frac{P-5}{8}} = \frac{2^{255} - 19 - 5}{8} = 2^{252} - 3 \text{ AKA } 22523$

IF POSITIVE
 $X_1^2 = UV^{-1} = X^2$
 $X = \pm X_1$

BY EULER'S CRITERION
 $\left(\frac{P-1}{4} \right)^2 = 2^{\frac{P-1}{2}} = -1$

NEGATIVE
 $= -UV^{-1}$
 $2^{\frac{P-1}{4}} = -X_1^2 = UV^{-1} = X^2$
 $= \pm X_1 2^{\frac{P-1}{4}}$ AKA SQR(-1)

$UV^3 (UV^{\frac{P-5}{2}})^{\frac{P-5}{8}} = U^{1+\frac{P-5}{8}} V^{3+7\frac{P-5}{8}} = 3+7\frac{P-5}{8} = 3+(8-1)\frac{P-5}{8} =$
 $3+P-5-\frac{P-5}{2} =$
 $P-2-\frac{P-5}{8}$
 $P-1-\frac{P-3}{8}$

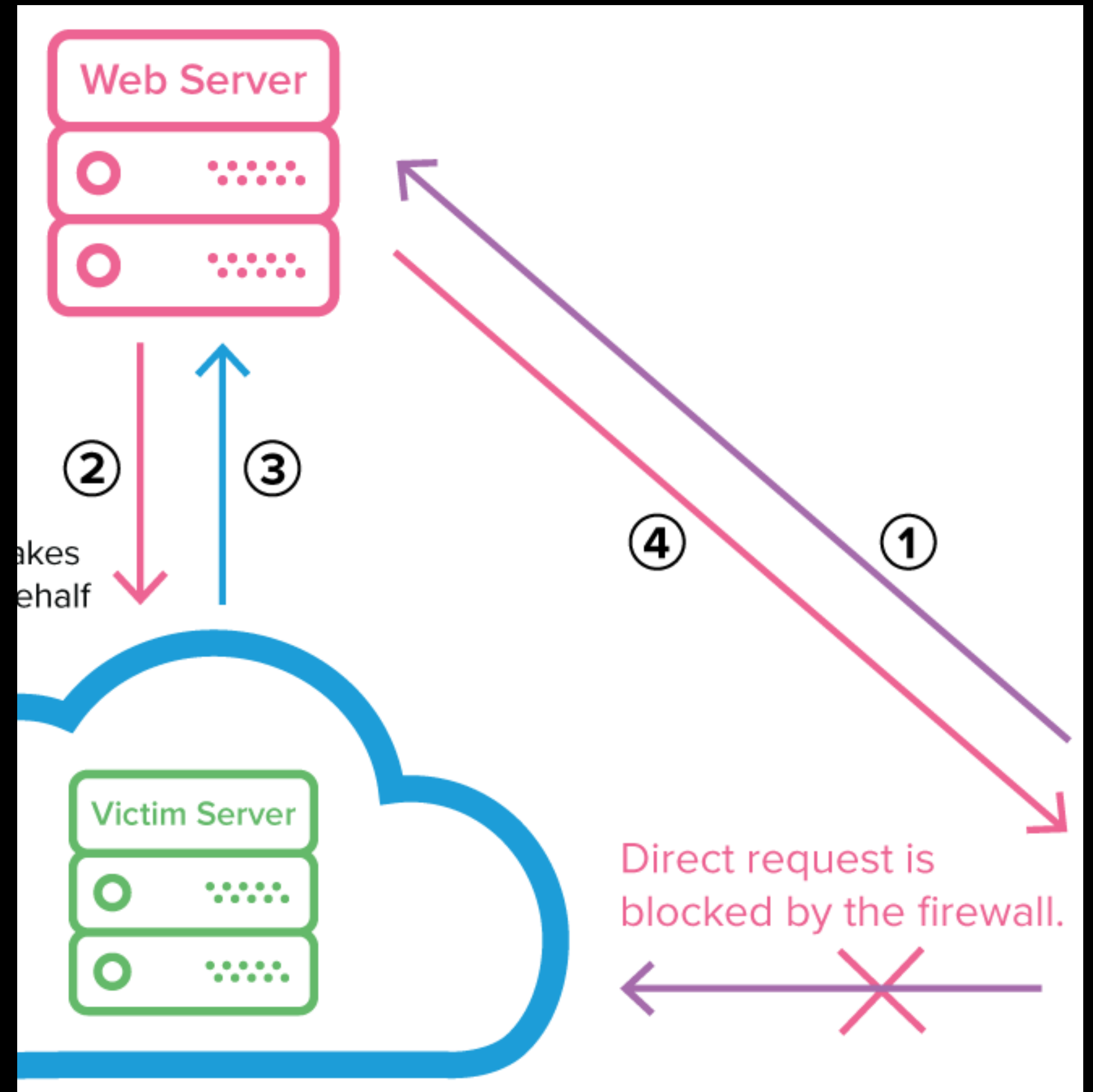
	60	125					
M							
S							

 $UV^3 = U \cdot V^2 \cdot V$
 $UV^2 = UV^3 \cdot V^2 \cdot V$

EULER'S THEOREM
 $A^{-1} = A^{P-2}$
 $A^P = A$
 $A^{P-1} = A^0 = 1$
 $A^{P-2} = A^{-1}$

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](http://portswigger.academy)

- <https://emile.space/ctf/>

Hack The Planet!

ctf.emile.space