Capture the Flag
An Owner's Manual

Vito Genovese

USENIX Enigma, January 27, 2016

What is CTF?

FUN

OMG

Qualifiers

May 20 through May 22

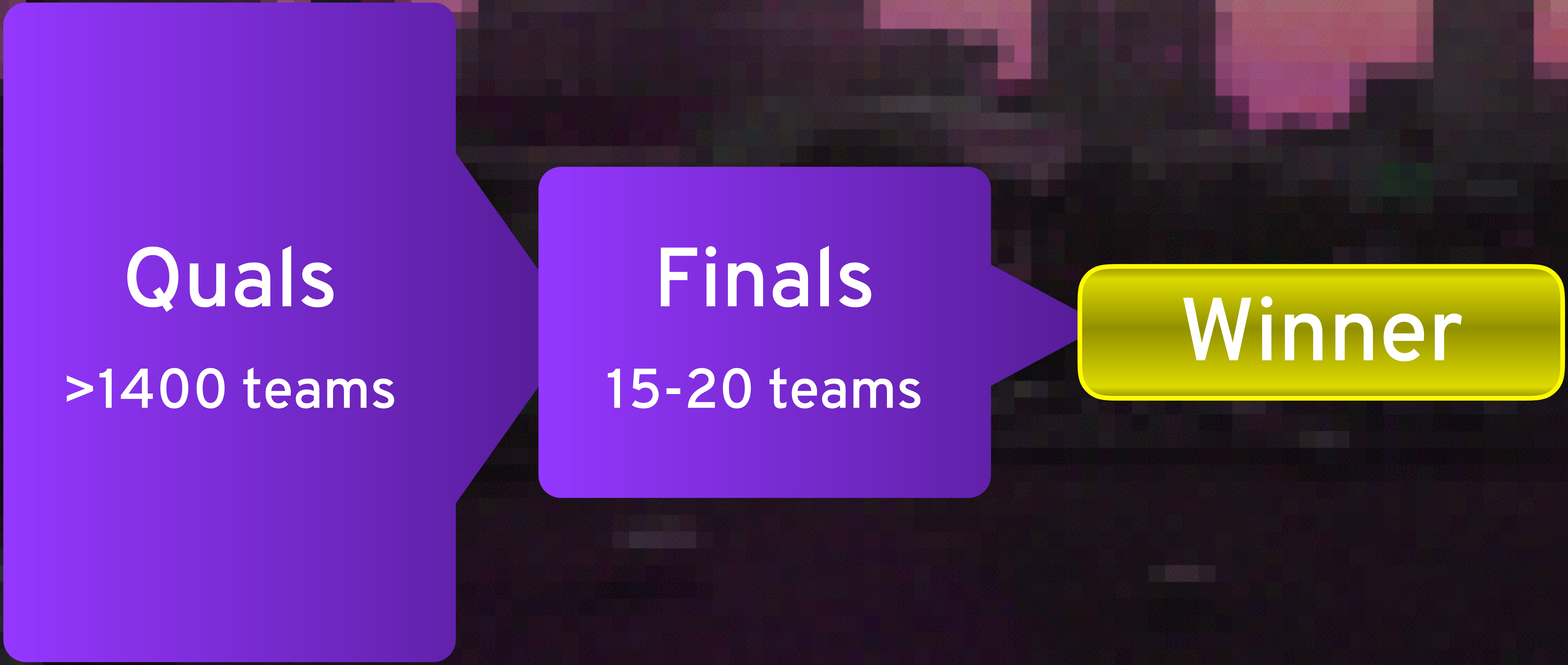
FREE

WOW

Finals

August 5 through August 7

Best of the Best



Quals

>1400 teams

Finals

15-20 teams

Winner

1	Plaid Parliament of Pwning
2	Dragon Sector
3	0ops
4	Shellphish
5	!SpamAndHex
6	dcua
7	Samurai
8	blue-lotus
9	217
10	Tasteless
11	StratumAuhuur
12	Gallopsled
13	HITCON
14	More Smoked Leet Chicken

Team Name	Final Score
DEFKOR	23949
Plaid Parliament of Pwning	19896
0daysober	17943
HITCON	13560
blue-lotus	12442
0ops	11306
Dragon Sector	11288
Samurai	10742
Shellphish	10591
LC↯BC	9941
!SpamAndHex	9461
Gallopsled	8608
9447	8410
CORNDUMP	7508
Bushwhackers	7447

Engineer a Non-Frustrating Game

Operate a Reliable Game

Have the Empathy to Make the Game Fun

Engineering

Engineering Process

1. Define problem
2. Research
3. Decide requirements
4. Brainstorm solutions
5. Pick the best solution
6. Build it
7. See if it's good enough
8. Redo what’s not

What kind of game?

Jeopardy

vs.

Attack-defense

Logout The Underminers.

Score: 5500

Binary Leetness	Forensics	Web Hacking	Potent Pwnables	Trivia
100	100	100	100	100
200	200	200	200	200
300	300	300	300	300
400	400	400	400	400
500	500	500	500	500

So, like, we wrote this admin app... The provided binary is running on quals07.allyourboxarebelongto.us:4455, Pwn it!

- binary

I owned it

Leaders

1. loller skaterz dropping from rofl copters! (6600)
2. sk3wl 0f r00t (6500)
3. Song of Freedom (6100)
4. Mighty Morf'n Power Haxor (6000)
5. FEDNAUGHTy (5900)
6. [0x28]Thieves (5900)
7. Routards (5800)
8. Osu, Tatakae, Sexy Pandas! (5800)
9. ReverseGhost (5700)
10. The Underminers (5500)
11. our wives are displeased
12. ShellPhish (5400)
13. Panicsecurity (5200)

Jeopardy is Easy

Scoreboard

Standalone challenges

Jeopardy is Easy

No complex networking

No complex admin work

(for players)

Attack-Defense is Hard

Complex network

Sensitive to connectivity

Teams host services?

We host services?

Slow services

Unavailable services

Superman defenses

Metagaming

Theming

Banking

Stuxnet

Board Game

Marijuana culture

Money Laundering

Botnet

SCADA

Wizardterrorism

Generic hacker

Theming

- web
- crypto
- forensics
- reverse engineering
- programming
- shellcode

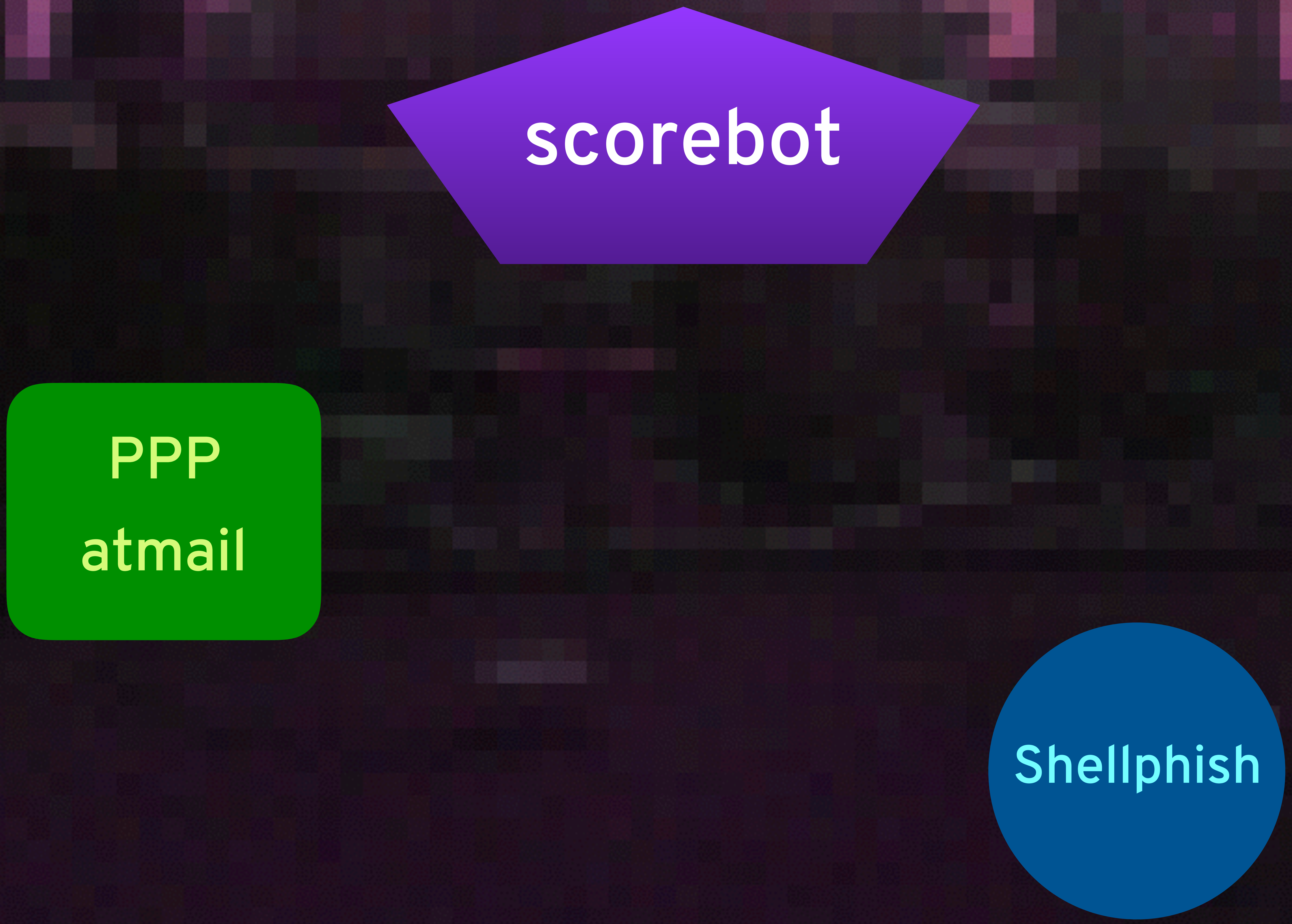
Jeopardy Scoring

```
SELECT
  t.id AS team_id, t.name AS team_name,
  SUM(c.points) AS score, MAX(s.created_at) AS last_solve
FROM
  teams AS t
  INNER JOIN solutions AS s ON s.team_id = t.id
  INNER JOIN challenges AS c ON s.challenge_id = c.id
WHERE team_id != 1
GROUP BY t.id
ORDER BY
  score DESC,
  MAX(s.created_at) ASC,
  MAX(s.id) ASC
```

Attack-Defense Scoring

aww jeez

Attack-Defense Game Flow

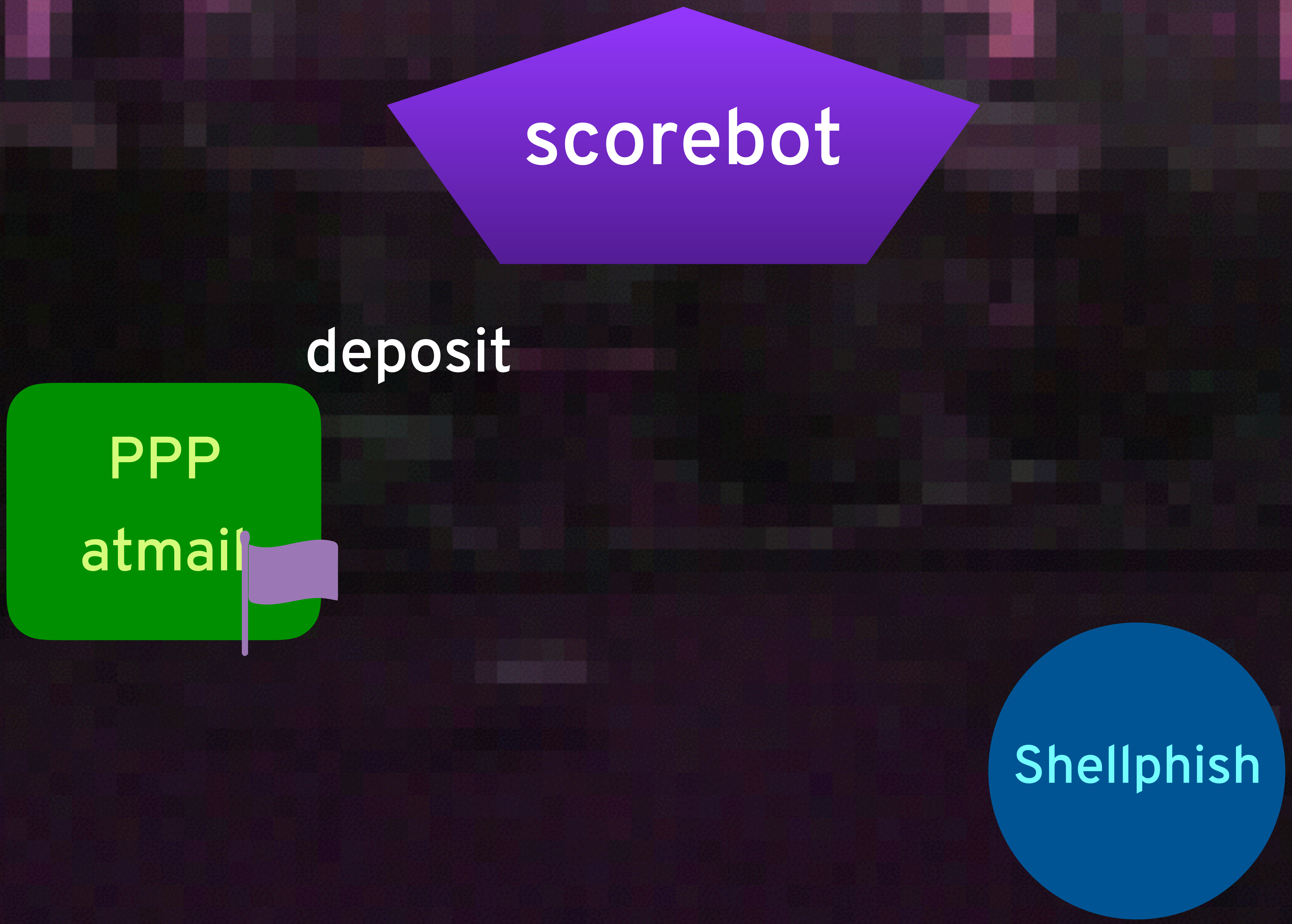


scorebot

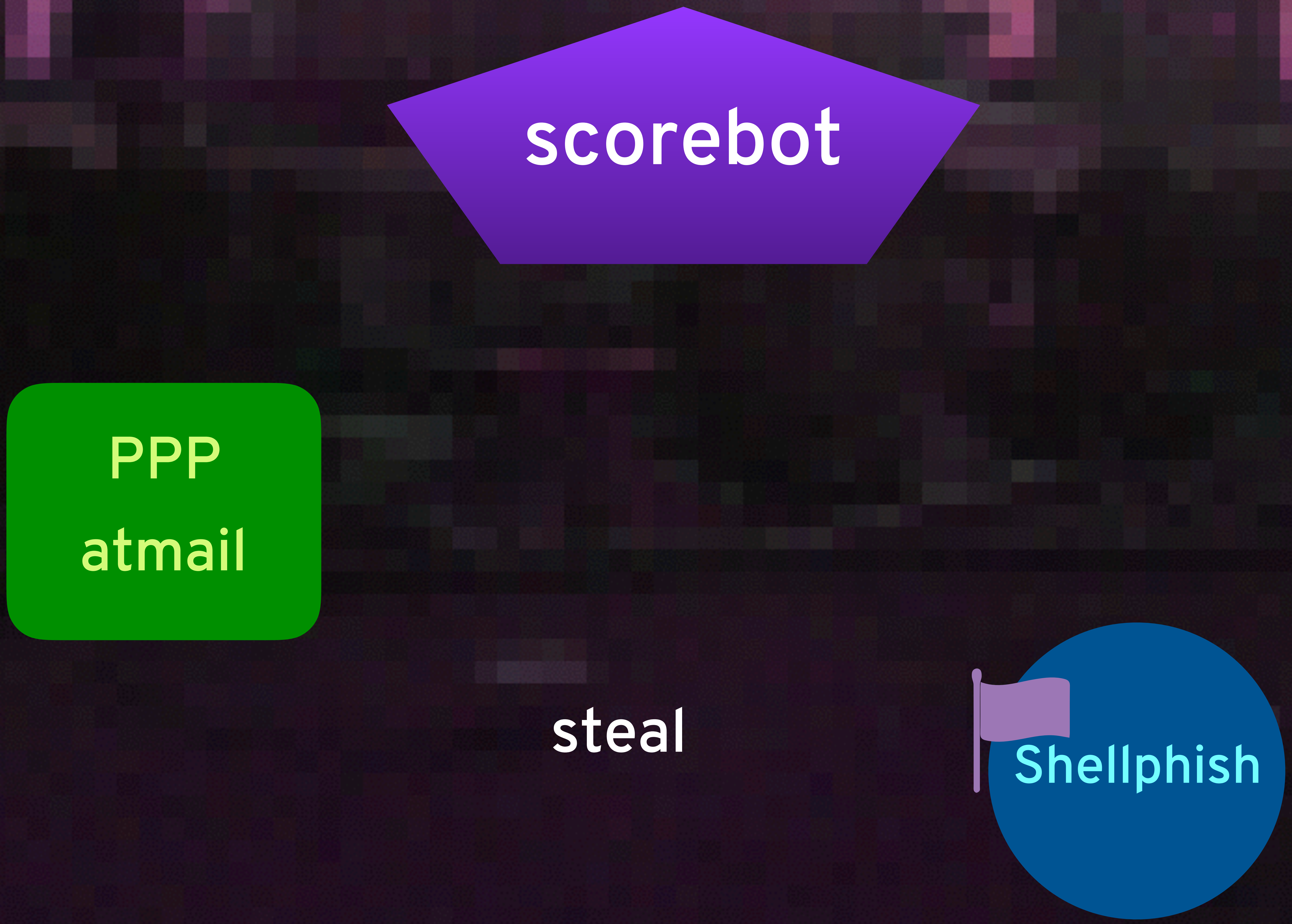
PPP
atmail

Shellphish

Attack-Defense Game Flow



Attack-Defense Game Flow



scorebot

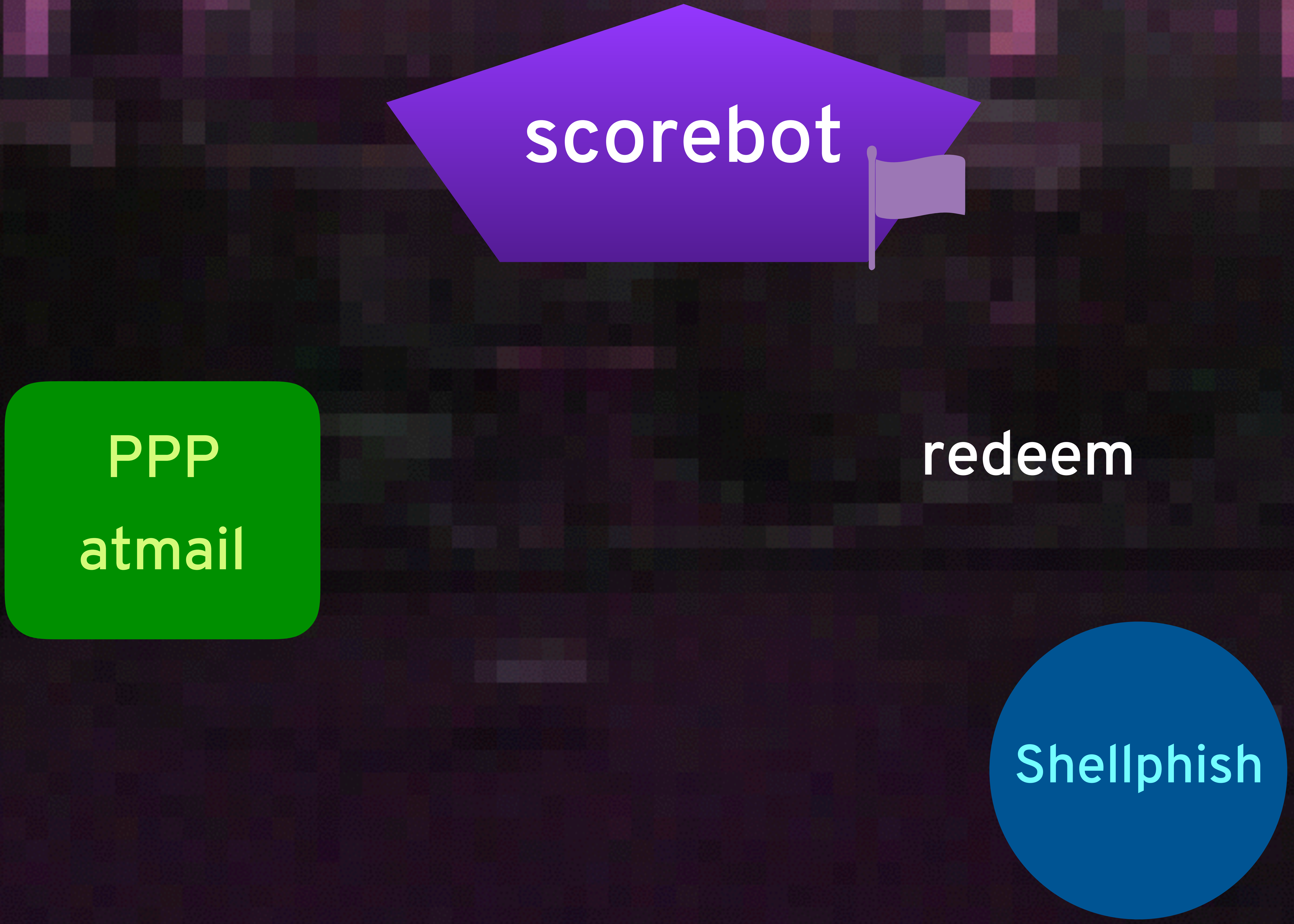
PPP

atmail

steal

Shellphish

Attack-Defense Game Flow



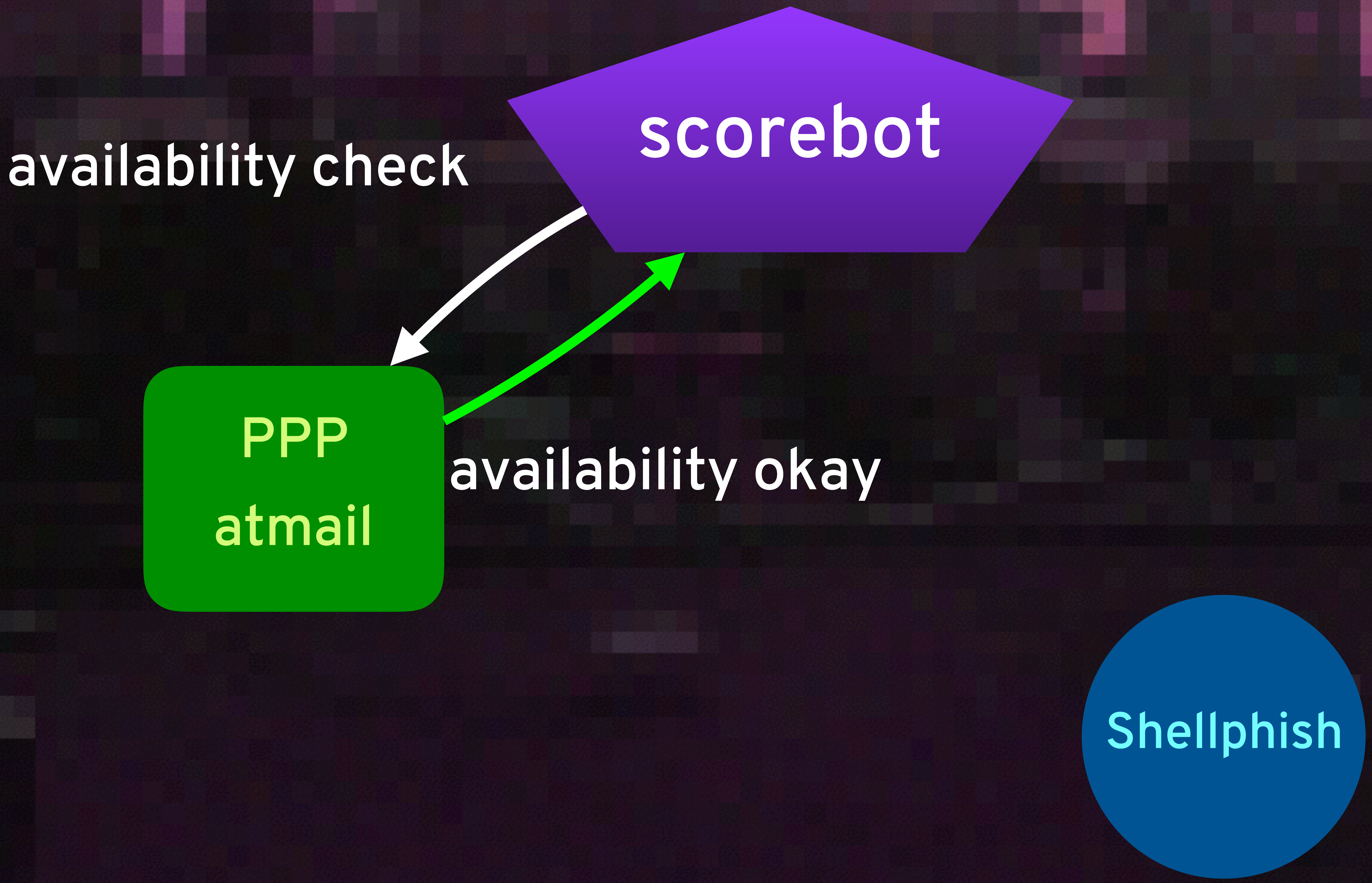
scorebot

PPP
atmail

redeem

Shellphish

Attack-Defense Game Flow



scorebot

availability check

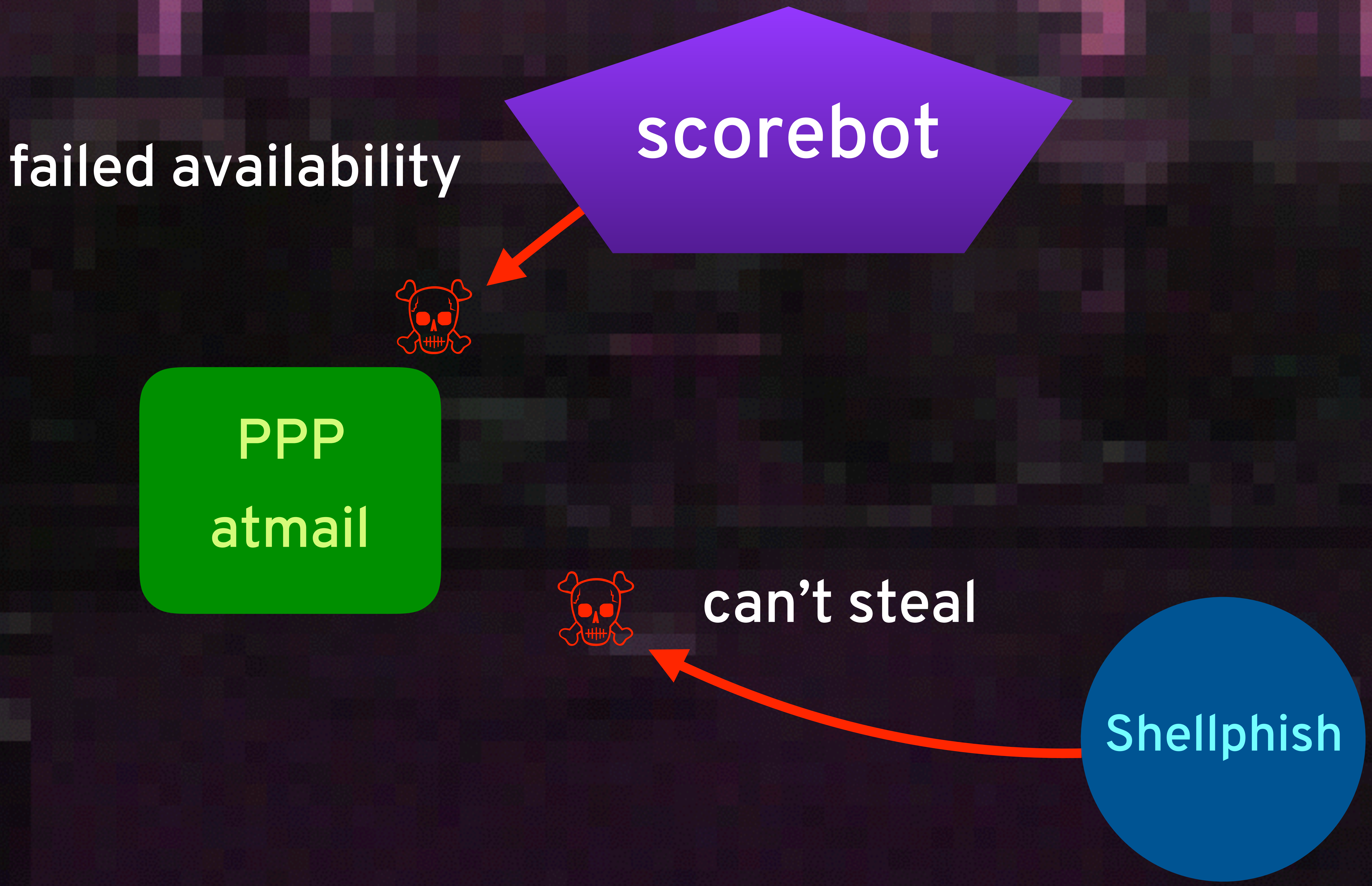
PPP

atmail

availability okay

Shellphish

Attack-Defense Game Flow



Attack-Defense Metagaming

Any sufficiently complex game is metagameable

Downtime

vs.

Being Hacked

Reflection

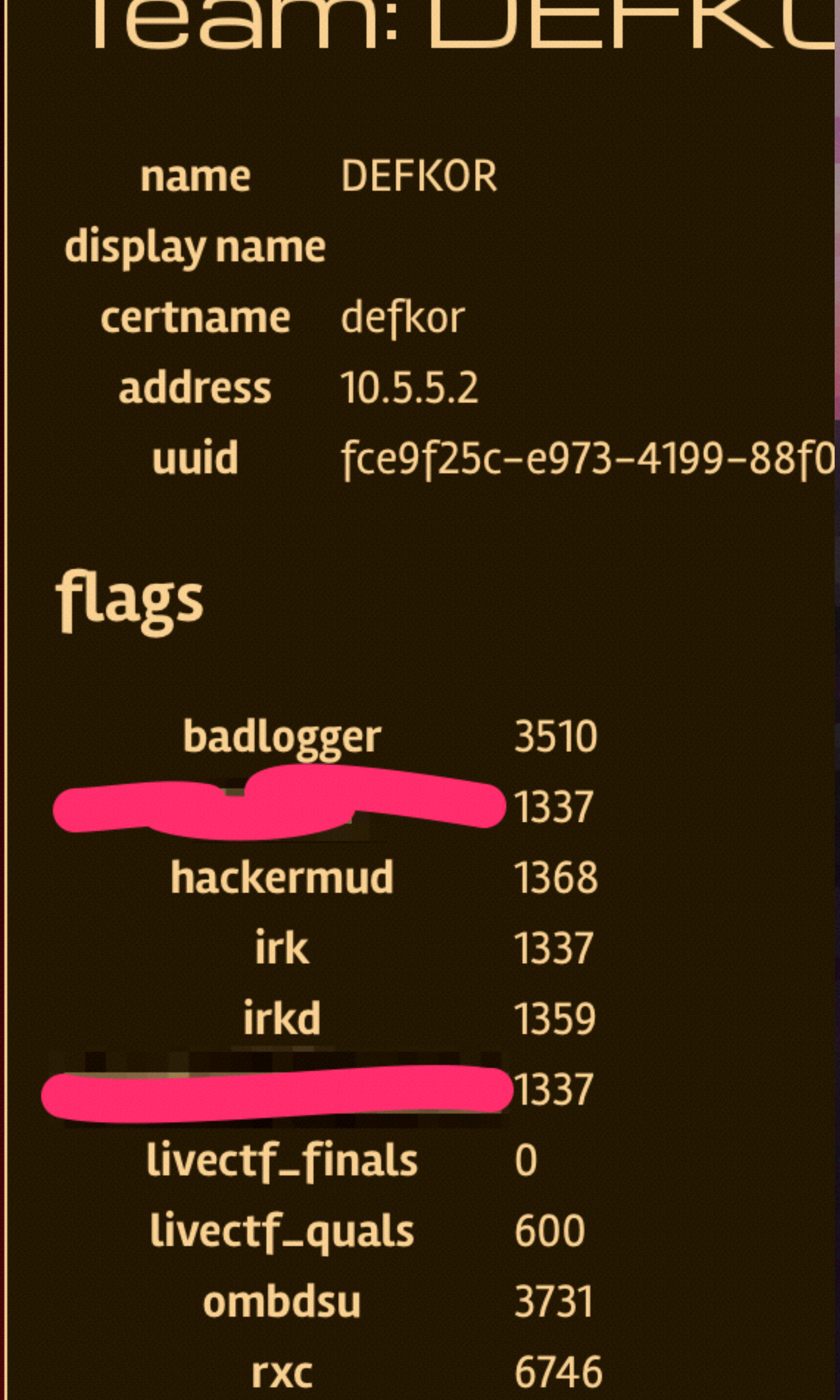
First Blood

Attack-Defense Scoring

Zero Sum

Finite number of flags

Flags per-service



Team: DEFK

name	DEFKOR
display name	
certname	defkor
address	10.5.5.2
uuid	fce9f25c-e973-4199-88f0

flags

badlogger	3510
[redacted]	1337
hackermud	1368
irk	1337
irkd	1359
[redacted]	1337
livectf_finals	0
livectf_quals	600
ombdsu	3731
rxc	6746

Attack-Defense Scoring

Can lose N-1 flags to steals per round

Stolen flags split among stealers

Remainders redistributed fairly

Attack-Defense Scoring

Downtime means lost steal opportunity

Teams lose 2(N-1) flags to downtime

Attack-Defense Scoring

Remainder and downtime flags are the flags of the people

Science of Challenges

- Think of cool bugs
- Write bugs, tool to check vulnerability
- Wrap ‘em in analysis surface
- Write smoke test and health checks

Art of Challenges

The machine is your canvas and the only limit is *~your imagination~*

Art of Challenges

Historic interest

Uniqueness

Inherent humor

Challenges and Team Size

Smaller teams don’t solve challenges slower

Bigger teams can solve more challenges at once

Challenges and Team Size

Fewer

and

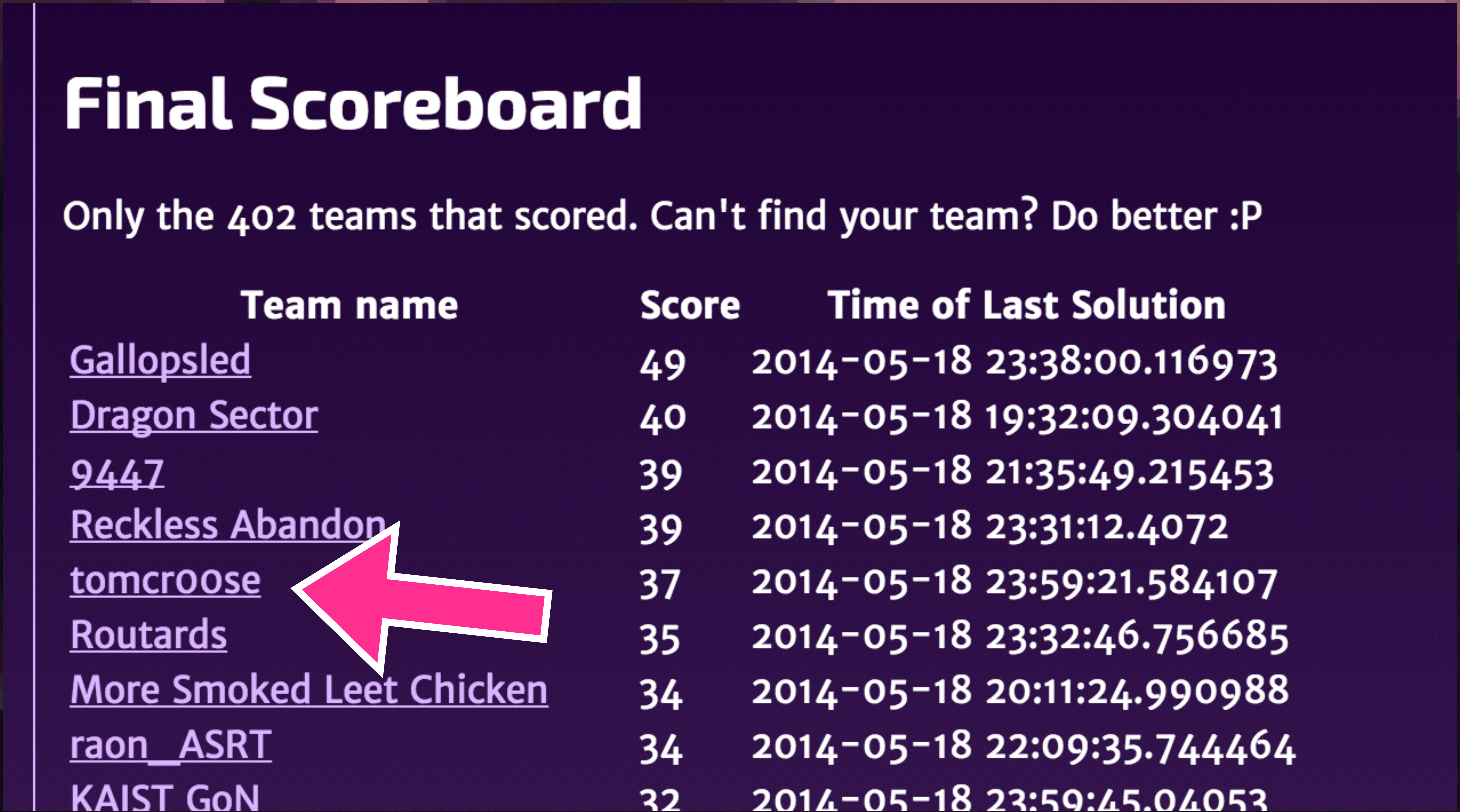
Harder

Smaller

and

Smarter

Challenges and Team Size



Final Scoreboard

Only the 402 teams that scored. Can't find your team? Do better :P

Team name	Score	Time of Last Solution
Gallopsled	49	2014-05-18 23:38:00.116973
Dragon Sector	40	2014-05-18 19:32:09.304041
9447	39	2014-05-18 21:35:49.215453
Reckless Abandon	39	2014-05-18 23:31:12.4072
tomcroose	37	2014-05-18 23:59:21.584107
Routards	35	2014-05-18 23:32:46.756685
More Smoked Leet Chicken	34	2014-05-18 20:11:24.990988
raon_ASRT	34	2014-05-18 22:09:35.744464
KAIST GoN	32	2014-05-18 23:59:45.04053

Challenges and Operations

Engineering great, fun, reliable challenges is the best ops improvement you can make.

Operations

CTF Operations

The dream is for the organizing team to just party ~~and be jerks to teams~~ during the game

CTF Operations

“Is this down or broken?”

“Is this actually exploitable?”

CTF Operations

It only has to work for a weekend

CTF Operations

Start on time by being ready early

Jeopardy Operations

Boston Key Party Servers	$27
Quals 2013 Servers	$284
Quals 2013 Booze	$340

L
ci20 t04
K
ci20 t06
ci20 t08
J
Imagination
creator
Model: CI20
micro SD ADAPTER
QC PASS

rpi 187
rpi 185
rpi 184
rpi 183
rpi 182
rpi 181

Attack-Defense Operations

We bring hardware to Vegas

Bring Hardware

Weird architectures

Bring Hardware

Teams don't want to bring hardware

Bring Hardware

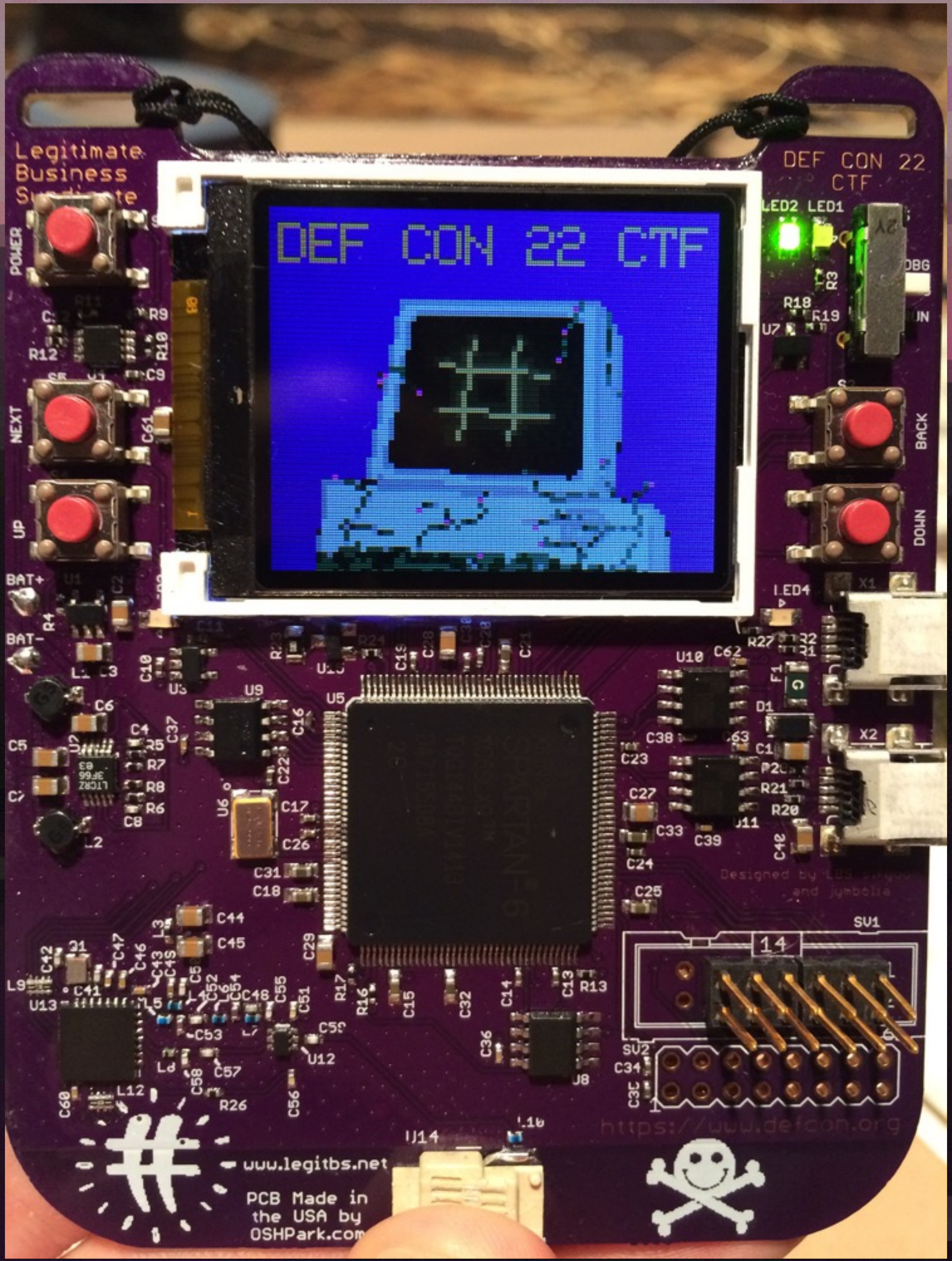
Don’t trust the uplink

Exceptions

- Stratum Auhuur who trusted the uplink at cccamp
- Also shout out to Shellfish for bringing a server rack to compete at DEF CON

TEAM5
TEAM3
TEAM1
TEAM12
TEAM10
TEAM8
TEAM11
TEAM9
TEAM7
TEAM18
TEAM16
TEAM14
TEAM17
TEAM15
TEAM13
TEAM22
TEAM20
TEAM19

Attack-Defense Dynamics



Attack-Defense Dynamics

Player time is a limited resource

1 shower

2 meals

3 hours of sleep

Attack-Defense Dynamics

1. Player 1 solves Service A
2. Player 1 starts Service B
3. Service A’ is released
4. Player 1 has a choice

Defecators & Ventilators

Sometimes challenges break

Defecators & Ventilators

10 hours / 1 Tester = 10 Hours

10 hours / 20 Teams = 30 Minutes

10 hours / 1000 Teams = 36 Seconds

Defecators & Ventilators

Perverse incentives

Empathy

Challenges and Empathy

The game is for the players

Players want good, fun, working challenges

Empathy

- We do it for the users/players/audience
- picture of CLU goes here

Empathy

Run the game you want to play

Empathy

Don’t lie to players

Deceive the players iff it makes the game more fun

Frustration

Trivia & Memes are hit or miss

Think of non-US and non-English teams

Guessing and Large Solution Spaces

Writing a solver for a 2^8 solution space is fun

Writing and paying for a 2^{16} space isn't

Preserve Player Agency

No hints once a challenge has been solved

Think carefully about force-unlocking

Jeopardy challenges

Preserve Player Enjoyment

Force-unlock easy challenges for teams to learn from

Force-unlock hard challenges early enough they'll be solvable

Hacking Computers is Fun!

Engineer a Non-Frustrating Game

Operate a Reliable Game

Have the Empathy to Make the Game Fun

FUN

OMG

Qualifiers

May 20 through May 22

https://legitbs.net/

FREE

WOW

Thanks

Vito Genovese

vito@legitbs.net

@vito_lbs

GPG B07D616143CAA77B

https://legitbs.net

@legitbs_ctf