What is CTF?
Qualifiers

May 20 through May 22

FREE

OMG

FUN

WOW

FREE
Finals
August 5 through August 7
Best of the Best

Quals
>1400 teams

Finals
15-20 teams

Winner
<table>
<thead>
<tr>
<th>Rank</th>
<th>Team Name</th>
<th>Final Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Plaid Parliament of Pwning</td>
<td>23949</td>
</tr>
<tr>
<td>2</td>
<td>DEFKOR</td>
<td>19896</td>
</tr>
<tr>
<td>3</td>
<td>Odaysober</td>
<td>17943</td>
</tr>
<tr>
<td>4</td>
<td>HITCON</td>
<td>13560</td>
</tr>
<tr>
<td>5</td>
<td>blue-lotus</td>
<td>12442</td>
</tr>
<tr>
<td>6</td>
<td>Oops</td>
<td>11306</td>
</tr>
<tr>
<td>7</td>
<td>Dragon Sector</td>
<td>11288</td>
</tr>
<tr>
<td>8</td>
<td>Samurai</td>
<td>10742</td>
</tr>
<tr>
<td>9</td>
<td>Shellphish</td>
<td>10591</td>
</tr>
<tr>
<td>10</td>
<td>LC4 BC</td>
<td>9941</td>
</tr>
<tr>
<td>11</td>
<td>!SpamAndHex</td>
<td>9461</td>
</tr>
<tr>
<td>12</td>
<td>Gallopsled</td>
<td>8608</td>
</tr>
<tr>
<td>13</td>
<td>More Smoked Less Chicken</td>
<td>8410</td>
</tr>
<tr>
<td>14</td>
<td>CORNDUMP</td>
<td>7508</td>
</tr>
<tr>
<td></td>
<td>Bushwhackers</td>
<td>7447</td>
</tr>
</tbody>
</table>
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
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, Tatake, Sexy Pandas! (5800)
9. ReverseGhost (5700)
10. The Underminers (5500)
11. our wives are displeased
12. ShellPhish (5400)
13. Panicsecurity (5200)
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
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

scorebot

deposit

PPP
atmail

Shellphish
Attack-Defense Game Flow

scorebot

PPP
atmail

steal

Shellphish
Attack-Defense Game Flow

scorebot

PPP
atmail

redeem

Shellphish
Attack-Defense Game Flow

- PPP atmail
  - availability check
  - availability okay

scorebot

Shellphish
Shellphish

Attack-Defense Game Flow

failed availability

scorebot

PPP

atmail

can’t steal

Shellphish

can’t steal
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
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
- Smaller
- and
- and
- Harder
- Smarter
## Final Scoreboard

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

<table>
<thead>
<tr>
<th>Team name</th>
<th>Score</th>
<th>Time of Last Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gallopsled</td>
<td>49</td>
<td>2014-05-18 23:38:00.116973</td>
</tr>
<tr>
<td>Dragon Sector</td>
<td>40</td>
<td>2014-05-18 19:32:09.304041</td>
</tr>
<tr>
<td>9447</td>
<td>39</td>
<td>2014-05-18 21:35:49.215453</td>
</tr>
<tr>
<td>Routards</td>
<td>35</td>
<td>2014-05-18 23:32:46.756685</td>
</tr>
<tr>
<td>raon_ASRT</td>
<td>34</td>
<td>2014-05-18 22:09:35.744464</td>
</tr>
<tr>
<td>KAIST GoN</td>
<td>32</td>
<td>2014-05-18 23:50:45.04053</td>
</tr>
</tbody>
</table>
Challenges and Operations

Engineering great, fun, reliable challenges is the best ops improvement you can make.
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
<table>
<thead>
<tr>
<th>Description</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boston Key Party Party Servers</td>
<td>$27</td>
</tr>
<tr>
<td>Quals 2013 Servers</td>
<td>$284</td>
</tr>
<tr>
<td>Quals 2013 Booze</td>
<td>$340</td>
</tr>
</tbody>
</table>
Attack-Defense Operations
Attack-Defense Operations

We bring hardware to Vegas
Bring Hardware

Weird architectures
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
Attack-Defense Dynamics

Player time is a limited resource

1 shower

2 meals

3 hours of sleep
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
Qualifiers

May 20 through May 22

https://legitbs.net/

FREE

FUN

OMG

wow

FREE
Thanks

Vito Genovese
vito@legitbs.net
@vito_lbs

GPG B07D616143CAA77B
https://legitbs.net
@legitbs_ctf