team15/BUILDS2:

how to go from -3 to 30,000 points
in just two days

defense strategy

- focus on defense.
  - only put up one plugin at a time to monitor what was breaking
  - monitor *EVERYTHING.*
    - htop, apachetop, error logs, netstat, mysql users/queries
  - chroot everything
    - no binary runs with access to main filesystem
    - each binary has its own user
  - minimize open ports
    - proxy other http servers through apache

defense strategy (cont'd)

- get plugins up as quickly as possible
  - sanitize all input
  - enforce typing
  - make sure there are no sketchy exec commands

defense strategy (cont'd)

- chroot
  - copy minimum necessary files for a working linux box
    - libc, /etc/passwd, bash, etc
  - add any other files that the program needs to run
  - run as a limited user
- proxying
  - web services don't need to be open to the world
  - apache sends request through
  - adjusts headers on response

attack strategy

- woot
  - injected parameter into post request
- ticket
  - misconfigured apache happily serves data.txt
- monocle
  - open mysql without password

memorable moments

- Five minutes into day one we removed the symlinks to wordpress. This resulted in us getting no points because, obviously, our site didn't work
  - it worked for us, so it took about an hour to fix
  - then as soon as we went up we got pwned
  - yeah -3 points

memorable moments

- gettin' ddos'd all day long?
  - at one point we had 160-something tcp keepalives stacked up
  - we limited the amount of memory apache could use
  - limited the number of tcp connections
  - turned off keepalive

- got fork-bombed by a reverse shell
  - panicked killing things in htop