Designing and Executing the World’s First All-Computer Hacking Competition

A panel with the development team

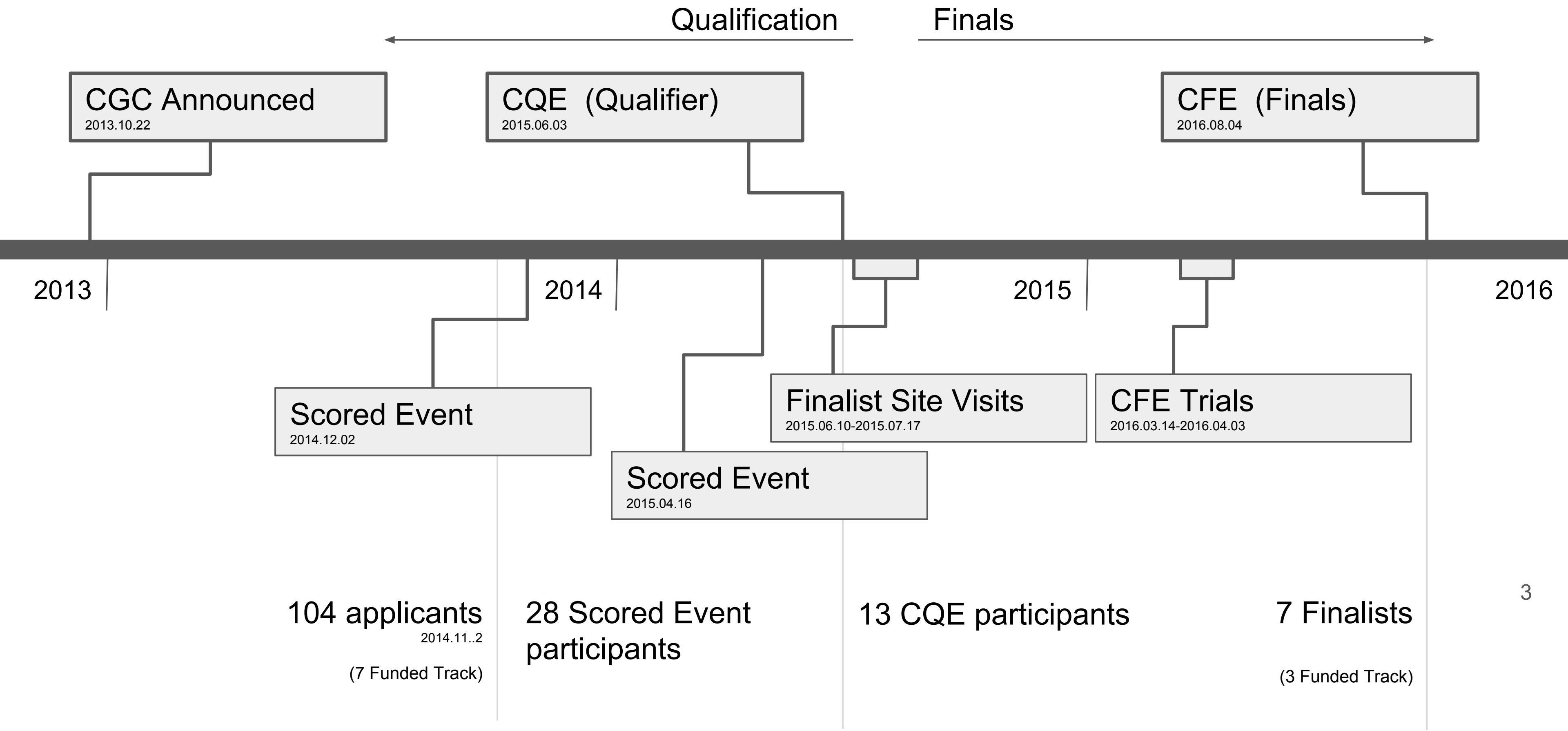
Timothy Vidas, Chris Eagle, Brian Caswell, Jason Wright, Holt Sorenson, Mike Thompson

Could a purpose-built super computer play in DEF CON’s Capture-the-flag (CTF)?

Autonomous...

- Binary analysis
- Binary patching
- Vulnerability discovery
- Service Resiliency (availability)
- Network Defense (IDS)

Competition Overview



Qualification

Finals

CGC Announced
2013.10.22

CQE (Qualifier)
2015.06.03

CFE (Finals)
2016.08.04

2013

2014

2015

2016

Scored Event
2014.12.02

Scored Event
2015.04.16

Finalist Site Visits
2015.06.10-2015.07.17

CFE Trials
2016.03.14-2016.04.03

104 applicants
2014.11..2

(7 Funded Track)

28 Scored Event participants

13 CQE participants

7 Finalists

(3 Funded Track)

CGC Qualification Event (CQE)

590 Explicit Flaws
131 Challenge Sets
24 hours
28 Participants
>=**5** CRSes on Twitter
$**750K** to prize to each unfunded qualifier

CRS Requirements:

- Demonstrate rudimentary capability
- Crashing inputs
- Mitigations
- Consensus evaluation

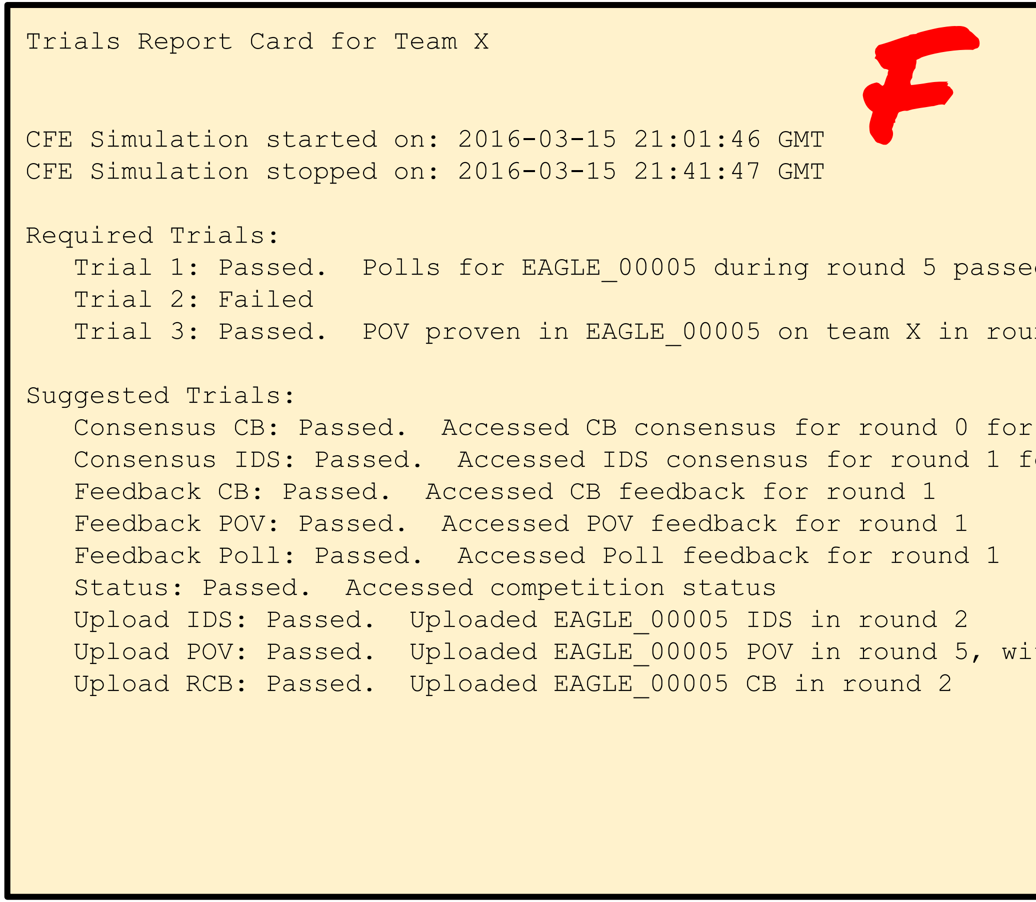
CFE Sparring/Trials

Conducted from 2016-02 to 2016-08

Opponents simulated by “sparring partner” software

CRS Requirements:

- Interact with API
- Upload POV (POV must succeed)
- Upload patched binary (patched binary must prevent POV)
- Upload IDS rule (IDS rule must be valid)



F

```
Trials Report Card for Team X


CFE Simulation started on: 2016-03-15 21:01:46 GMT
CFE Simulation stopped on: 2016-03-15 21:41:47 GMT

Required Trials:
   Trial 1: Passed.  Polls for EAGLE_00005 during round 5 passe
   Trial 2: Failed
   Trial 3: Passed.  POV proven in EAGLE_00005 on team X in rou

Suggested Trials:
   Consensus CB: Passed.  Accessed CB consensus for round 0 for
   Consensus IDS: Passed.  Accessed IDS consensus for round 1 f
   Feedback CB: Passed.  Accessed CB feedback for round 1
   Feedback POV: Passed.  Accessed POV feedback for round 1
   Feedback Poll: Passed.  Accessed Poll feedback for round 1
   Status: Passed.  Accessed competition status
   Upload IDS: Passed.  Uploaded EAGLE_00005 IDS in round 2
   Upload POV: Passed.  Uploaded EAGLE_00005 POV in round 5, wi
   Upload RCB: Passed.  Uploaded EAGLE_00005 CB in round 2
```

96 Rounds
9h 13m 17s duration
82 Challenge Sets
410 unique RCBs fielded
1299 unique PoVs fielded
(total of **270772** throws)
7 Functioning CRSes
1 Failed water pump
$**3.75M** USD prizes awarded

CGC Final Event (CFE)

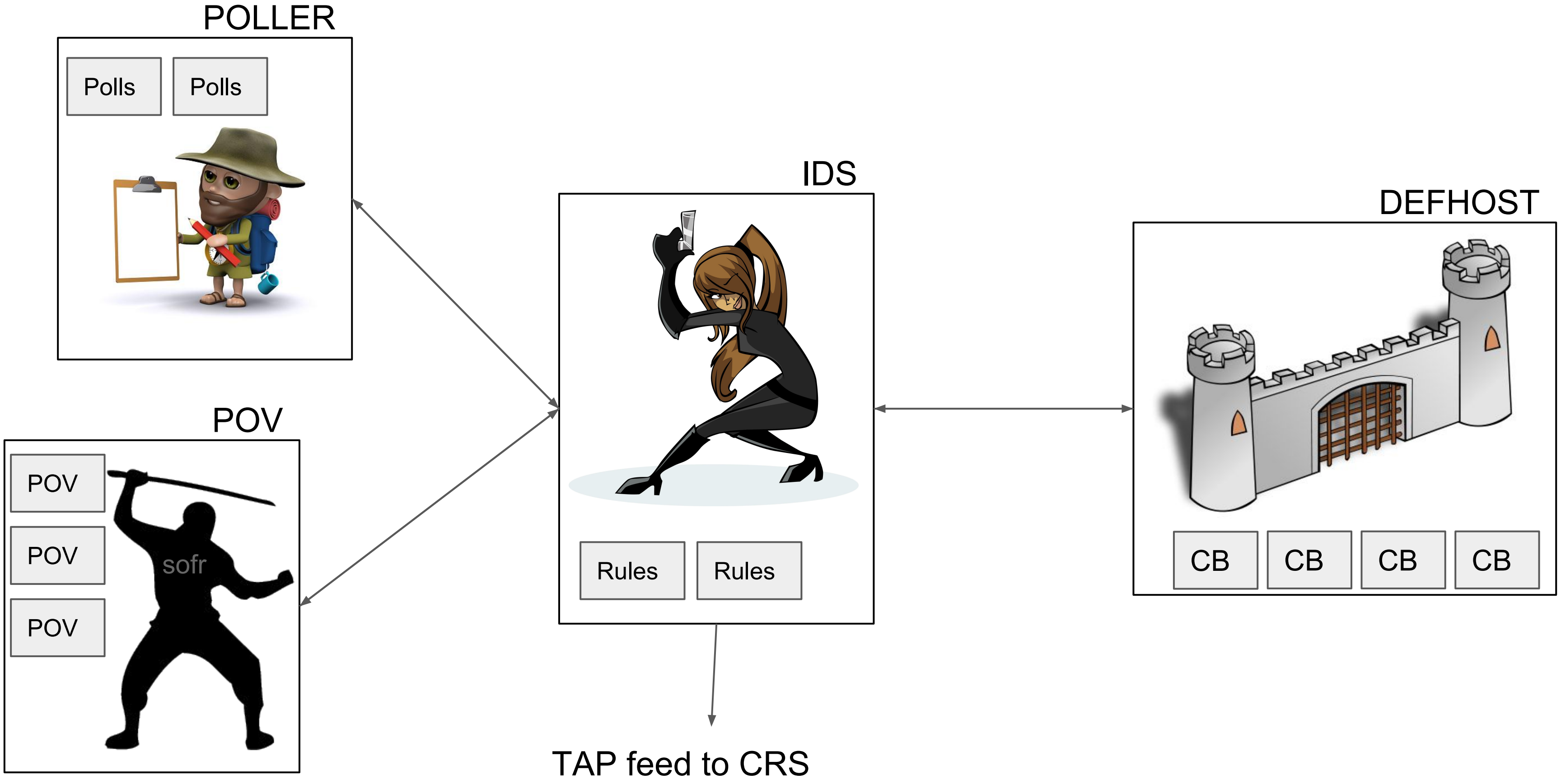
- Live event held at DEF CON in Aug 2016
- More expected of competitors than in CQE
    - IDS filters available
    - Full access to competitors mitigated binaries and IDS filter
    - Live network traffic feed available as tap on IDS
    - Stronger requirements for proof of vulnerability
- Infrastructure only evaluates performance and functionality
- Otherwise, infrastructure deploys mitigated binaries and launches POVs on behalf of competitors (a brokered competition)

CFE Game Flow

6 physical machines dedicated to “infrastructure side” for each competing CRS
Each CRS connected to the infrastructure via **2** ethernet cables

- Competitors interact with a “Team Interface” (**TI**)
  - Web server providing status updates and upload capability
- Defended host (**DEFHOST**)
  - Runs all Challenge Binaries or their CRS-supplied replacements (reformulated CB; RCB)
- Network Appliance (**IDS**)
  - Runs competitor supplied filter rules
  - Filters installed on a per-challenge set basis
  - ALL connections to Challenge Binaries run through IDS
- Poller (**POLLER**)
  - Runs DARPA generated functionality test interactions against active challenges
- POV (**POV**)
  - Runs CRS-provided POVs against active challenges

Game Flow



POLLER

Polls

Polls

POV

POV

POV

POV

sofr

IDS

Rules

Rules

DEFHOST

CB

CB

CB

CB

TAP feed to CRS

Evaluating a POV

2 types of POVs in CFE
During CFE, **118708** Type-1 and **152064** Type-2 were negotiated by CRSes (**7512** and **5975** successful, respectively)
Vulnerabilities were proven in **20** (of 82) Challenge Sets in CFE
All **7** CRS successfully proved at least one vulnerability

Two POV types specified for CFE

- Type 1
  - Competitor POV claims it can control EIP and one other register
  - Negotiation transaction dictates specific values to POV
  - POV interacts with challenge set to cause a crash in the dictated state
  - Crash state (if any) examined to confirm success or failure of POV
- Type 2
  - Competitor POV claims it can read from an arbitrary memory location
  - Negotiation transaction dictates a region of memory from which POV must obtain 4 bytes
  - POV interacts with challenge set to leak said 4 bytes and submits them to complete the negotiation
  - Submitted value is examined to confirm success or failure of POV

Building the Competition

- Design concerns from the outset
    - Repeatability
        - Anyone should be able to verify CFE results
    - Competition integrity
        - Concerns with running competitor-provided code (POV/RCB)
        - Concerns with parsing competitor-provided data (IDS filters)
    - Data collection
        - Desire to publish corpus to serve as a reference for program analysis going forward

5 instructions trapped by hypervisor modified the behavior of **11** additional instructions

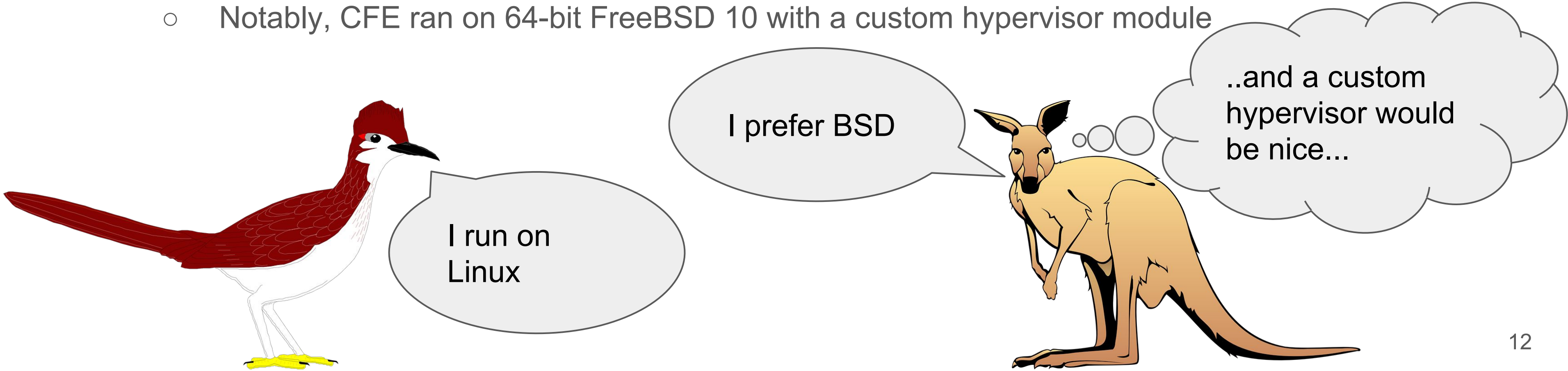
Repeatability

- Design goal was for every transaction to be as deterministic as possible
  - Modulo TCP
- Eliminated all sources of randomness that might be accessible to CGC binaries and made available the “random” system call
  - CGC hypervisor trapped all instructions that might be used to gather entropy
    - rdpmc, rdrand, rdtsc, rdtscp, rdseed
  - Some other instructions emulated or forbidden
    - cpuid, lgdt, lidt, sgdt, sidt, lldt, ltr, sldt, str, in, out
    - cpuid returned same values as developer’s MacBook Pro laptop
- Random pulled from a PRNG seeded by the CGC loader at process creation time
  - All seeds generated ahead of game time and recorded for later use

Competition Integrity

7 system calls

- Given the amount of prize money at stake, integrity of the competition was a grave concern and drove many design decisions
- Air Gap
- Committed to kernels versions released prior to announcement of CGC
- Designed DECREE syscall environment / file format to reduce attack surface
- All game infrastructure components released to the public had private internal implementations
  - Notably, CFE ran on 64-bit FreeBSD 10 with a custom hypervisor module



Forensics

- Real-time forensics harness to vet software
    - Monitor OS for execution & data integrity
    - Built upon a full system emulator (Simics)
    - High fidelity x86 model from Intel
- Evaluated non-trusted code (POV/RCB) for attempts to breakout of DECREE environment
- Analyst replay tool
    - Replay any CFE session via IDA Pro gdb client
    - Reverse execution & scoring event detection

Data Collection

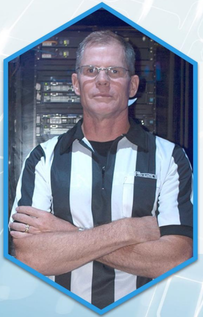
- From the outset we wanted to be able to be able to contribute a corpus of vulnerable challenge binaries of known provenance following CFE
  - Perhaps to serve as a reference for future program analysis research
- Additionally we wanted the game to be replayable and verifiable by any interested parties after the event.

Panelists

REFEREE

DR. TIM VIDAS DEV TEAM LEAD

- Member sk3wl 0f r00t CTF team
  Two time winner of DEF CON CTF
- Co-Founder of DDTEK
  Four time organizers of DEF CON CTF
- DC3 Forensics Challenge Grand Champion
- Member of The Shmoo Group
- Technical Editor of the IDA Pro book



REFEREE

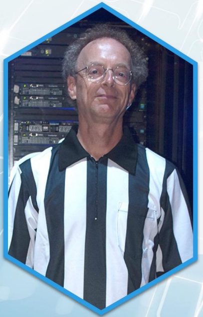
CHRIS EAGLE CGC ARCHITECT

- Founder of the sk3wl 0f r00t CTF team
  Two time winner of DEF CON CTF
- Founder of DDTEK
  Four time organizers of DEF CON CTF
- Author of the IDA Pro book
- Senior Lecturer at the Naval Postgraduate School

REFEREE

BRIAN CASWELL CODER OF EVERYTHING

- Member sk3wl 0f r00t CTF team
  Two time winner of DEF CON CTF
- Core member of DDTek
  Four time organizer of DEF CON CTF
- Former author of the most widely used IDS ruleset
- Past presenter at DEFCON, Blackhat, ShmooCon, CanSecWest, et al



REFEREE

MIKE THOMPSON COMPETITION INTEGRITY

- On dev-team for world's only Class A1 trusted computer system
- Lead developer of the CyberCIEGE video game
- 20+ experience developing trusted computing systems
- Research Associate at the Naval Postgraduate School

REFEREE

HOLT SORENSON DEV OPS

- Member of Sk3wlOfR00t
  Two time winner of DEF CON CTF
- Co-Founder of DDTek
  Four time organizer of DEF CON CTF
- Member of The Shmoo Group
- Author for Security Focus

REFEREE

JASON WRIGHT KERNEL HACKER

- Member of ACME Pharm CTF team
  Won DEF CON 18 CTF
- Former OpenBSD developer
  Co-creator of SPARC64 port
- SCADA/ICS vulnerability research at Idaho National Lab
- MS Computer Science, University of Idaho 2014

akhir

cuối

vég

τέλος

結束

einde

uç

끝

Ende

fine

fin

చివర

конец

pää

koniec

終わり

अंत

ปลาย

ände

סוף

End

Further reading

Rules https://cgc.darpa.mil/CGC_Rules_18_Nov_14_Version_3.pdf
Master Schedule https://cgc.darpa.mil/CGC_Master_Schedule_15_Apr_15.pdf
CQE news http://www.darpa.mil/news-events/2015-07-08
CRS Twitter feeds https://twitter.com/tvidas/lists/cgc-crses/

CGC Competitor Portal https://cgc.darpa.mil/
CGC Website https://www.cybergrandchallenge.com/
CGC Release Repo http://repo.cybergrandchallenge.com/
CGC GitHub Repo https://github.com/CyberGrandChallenge

CFE commentary

- CFE officially started at 16:00:45 UTC
- 40 rounds had completed by 19:41:09 UTC
- Power failure outside of airgap resulted in momentary failure in receiving data to feed visualization (Round 43 utilized our contingency data export protocol)
- CFE ended at max rounds (96) at 01:13:17 UTC
- Not counting original CBs, there were 512 unique RCBs uploaded, 410 of which were fielded
- Of 3570 unique POVs uploaded, 1299 were fielded, totalling 284823 throw opportunities, 270772 completed negotiations, and 13487 successful proofs

Some POV Related Numbers

Team	Type 1	Type2
CodeJitsu	2438	1202
CSDS	3	145
DeepRed	235	630
Disekt	89	1936
ForAllSecure	218	583
Shellphish	2398	1479
TECHx	2131	0

CSET	Type 1	Type 2
CROMU_00046	220	
CROMU_00051	83	70
CROMU_00055	68	2068
CROMU_00058		5
CROMU_00064		187
CROMU_00065	786	
CROMU_00073	95	7
CROMU_00088		6
CROMU_00094	779	400
CROMU_00095	25	

CSET	Type 1	Type 2
CROMU_00096		127
CROMU_00097		80
CROMU_00098	72	
KPRCA_00065	542	443
KPRCA_00094	148	
NRFIN_00052	1405	10
NRFIN_00059		620
NRFIN_00062	346	120
YAN01_00015	1652	730
YAN01_00016	1291	1102