The Last CTF Talk You'll Ever Need:

AMA with 20 years of DEF CON Capture-the-Flag organizers

Tim Vidas, Hawaii John, Chris Eagle, Invisigoth, Caezar, and Myles
@tvidas, @lbs_hj, @sk3wl, @invisig0th, @rileycaezar

Tim Vidas @tvidas

- I'll be laying the foundation for and then moderating the panel

- I'll make every effort to be objective
  - DDTEK organizer
  - Sk3wl of r00t player
  - PPP player (though, never at DEF CON)

What is CTF in this context?

- A cyber security based Capture-the-Flag contest (aka exercise, event, game)
- Typically these contests involve demonstrating proficiency or excellence in one or more areas of computer and network security
- There are different models for architecting these contests, which can stress different skills, lend to particular objectives
- Increasingly popular, common

It is not:

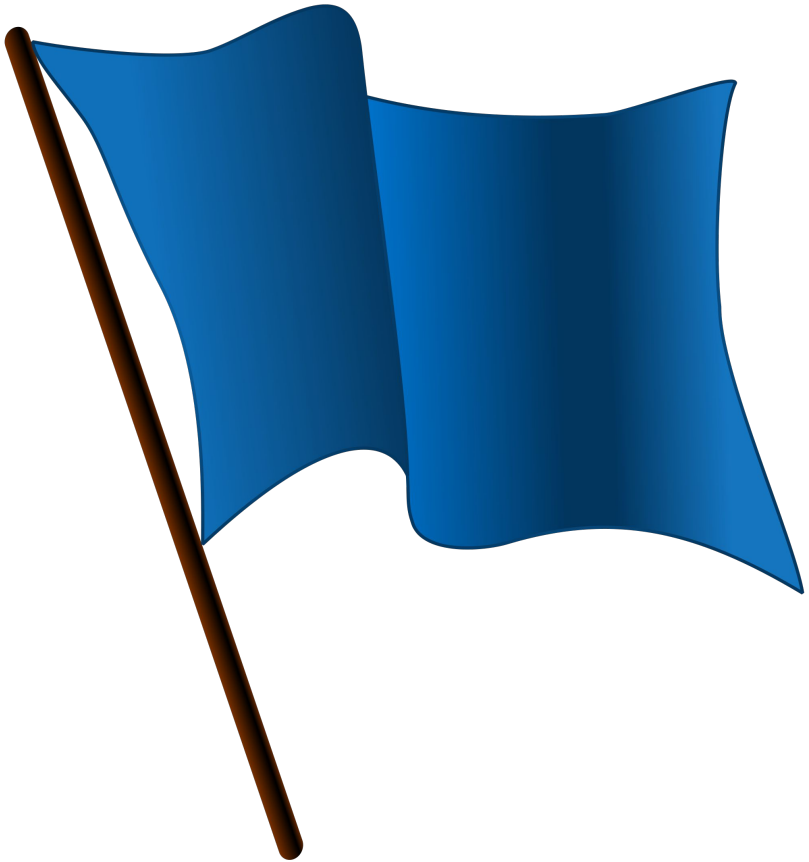
- A game kids play with physical flags on hills
- A first-person shooter video game CTF (usually)
- Focused in the field of Social Engineering
- A hackathon

Though there are certainly similarities to these other games.

Today, the characters “CTF” are appended to many contests, in most cases this simply means “contest,” sometimes there are flags involved

What is a flag?

The thing to be captured



What is a flag?

The thing to be captured

- **Random data/text**
  - May be difficult to know when a challenge is “solved” (e.g. forensics, stegonagraphy, etc)
  - May result in many, many “guesses” by participants
- **Structured**
  - Many options, all give more confidence in submission to a participant
  - May limit the search space for brute force guessing
  - May facilitate certain types of defense
    - IDS rule, filesystem monitor, fakes,etc
- **AKA “key” or “token”**

0x346ada9593d62a722af11cdbf9c0aa

avaweghawofimhawebfui

bTNyYyBsaWtlbSBzaGVlcHM=

notthesemaphoresiwaslookingfor

FLAG{avaweghawofimhawebfui}

What is a flag?

The thing to be captured

- Flags are typically presented to organizers as proof that a challenge has been completed
  - Via paper, email, writeup, web API / scoreboard server

- Flags might be shared (collusion)
- Flags might have a constant, preset value
- Flags might have variable value
  - How many participants have captured that particular flag
  - Elapsed time
  - Some flags might be more valuable than others
- Flags might expire
  - Can teams hoard flags until near the end of the event?
    - Is the visible scoreboard an accurate depiction of the current state of the game (potential)
    - Odds of collusion “deals” made near the end of the game

What is DEF CON CTF?

DEF CON's is one of highest regarded cyber security CTFs in the world.

Typically, the phrase "DEF CON CTF" refers to the on-premise attack-defend competition that more-or-less spans the duration of the con.

Coders from around the globe battle through a series of qualifying rounds to make it to the CTF. "These hackers here are the top of the world,"

~ CNN [4]

DEFCON CTF – one of the most prestigious and challenging CTF ever

~ infosec institute [2]

known among hacker circles as the "World Series of hacking."

~ CNBC [3]

"Historically this is a first type of CTFs, everybody knows about DEF CON CTF - something like a World Cup of all other competitions."

~ ctftime.org [1]

considered a legal talent show for hackers

~ FOXNEWS [5]

[1] https://ctftime.org/ctf-wtf/
[2] http://resources.infosecinstitute.com/tools-of-trade-and-resources-to-prepare-in-a-hacker-ctf-competition-or-challenge/#gref
[3]http://www.cnbc.com/2013/11/08/defcon-capture-the-flag-competition-is-only-for-top-hackers.html
[4] http://money.cnn.com/2012/07/27/technology/defcon-nsa/index.htm
[5] http://www.foxnews.com/printer_friendly_wires/2006Aug06/0,4675,HackerGames,00.html

In the beginning, there were the Goons...

DEF CON's CTF is one of the oldest and longest running CTFs.

CTF is one of DEF CON's oldest and longest running contests.

The first recognized DEF CON Capture-the-Flag took place at DEF CON 4, in 1996.

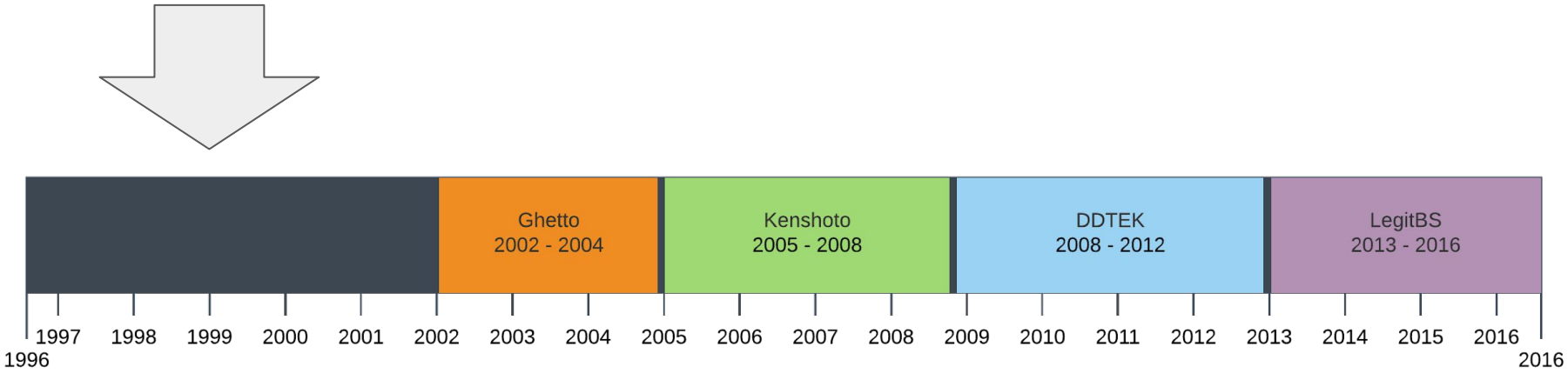
It was known only as CTF and took place entirely on-site (just as many of DEF CON's diverse CTFs do today).

$$For\ any\ CTF\ x,\ x \in \mathbf{N}$$

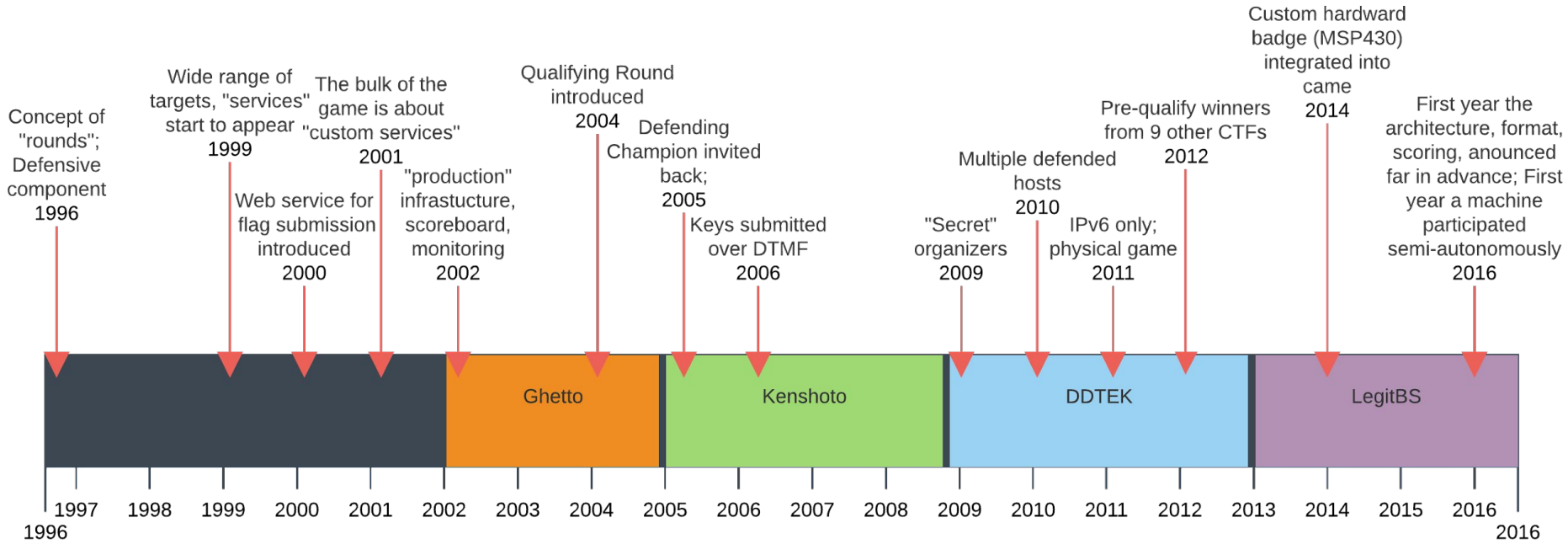
$$defcon(x) = x + 3, x \geq 1$$

$$year(x) = x + 1995, x \geq 1$$

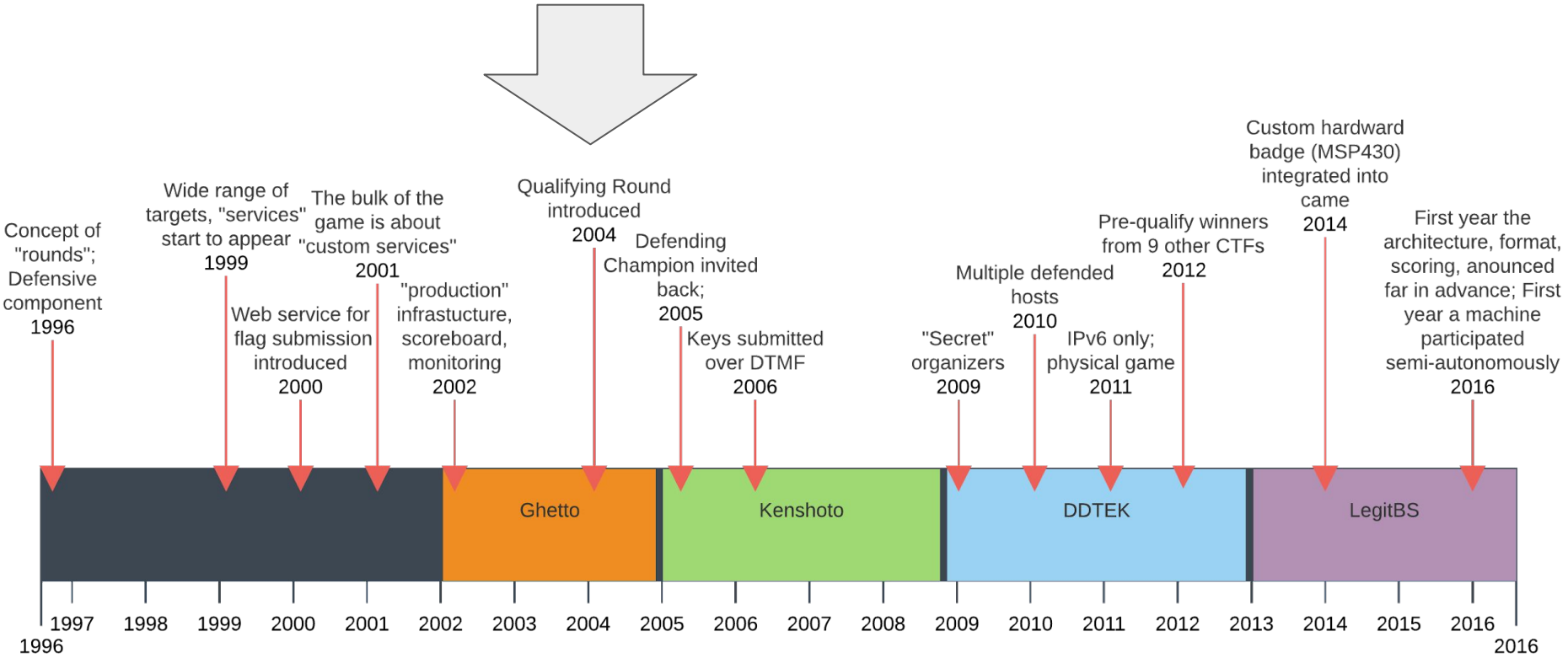
In the beginning, there were the Goons.



Timeline


Concept of "rounds"; Defensive component 1996
Wide range of targets, "services" start to appear 1999
Web service for flag submission introduced 2000
The bulk of the game is about "custom services" 2001
"production" infrastucture, scoreboard, monitoring 2002
Qualifying Round introduced 2004
Defending Champion invited back; 2005
Keys submitted over DTMF 2006
"Secret" organizers 2009
Multiple defended hosts 2010
IPv6 only; physical game 2011
Pre-qualify winners from 9 other CTFs 2012
Custom hardward badge (MSP430) integrated into came 2014
First year the architecture, format, scoring, anounced far in advance; First year a machine participated semi-autonomously 2016
Ghetto
Kenshoto
DDTEK
LegitBS
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2016

Timeline


Concept of "rounds"; Defensive component 1996
Wide range of targets, "services" start to appear 1999
Web service for flag submission introduced 2000
The bulk of the game is about "custom services" 2001
"production" infrastucture, scoreboard, monitoring 2002
Qualifying Round introduced 2004
Defending Champion invited back; 2005
Keys submitted over DTMF 2006
"Secret" organizers 2009
Multiple defended hosts 2010
IPv6 only; physical game 2011
Pre-qualify winners from 9 other CTFs 2012
Custom hardward badge (MSP430) integrated into came 2014
First year the architecture, format, scoring, anounced far in advance; First year a machine participated semi-autonomously 2016
Ghetto
Kenshoto
DDTEK
LegitBS
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2016

What kind of Capture-the-Flag?

Attack-defend

- Participants are connected to each other in some way
- Fundamentally, active attack and defense
  - Concept of “service availability”
- Typically each participant is level-set with [near-]identical game configuration
  - Analyze your configuration to learn about opponents and defend your own flags
- Composed of a set of challenges (aka services)
  - Order might be controlled

Game board (aka Jeopardy style)

- You’ve seen the show
  - Might not literally, visually appear as a board
- Participants are NOT connected to each other
  - Defense is typically not incorporated
- Solve a series of challenges (aka questions)
  - Order might be controlled (e.g. leader)
  - Value might be pre-set (e.g. 100/200/400)
- “Categories” might be arbitrary or designed with objectives in mind

Jeopardy style

- Easily the most common world-wide
- Possibly more diversity within a single event, given that a “question” can be setup in infinite ways
- Arguably easier to organize / create
  - Divide-and-conquer approach to question creation
  - Less infrastructure to create, monitor
  - Lends to on-site and remote participation

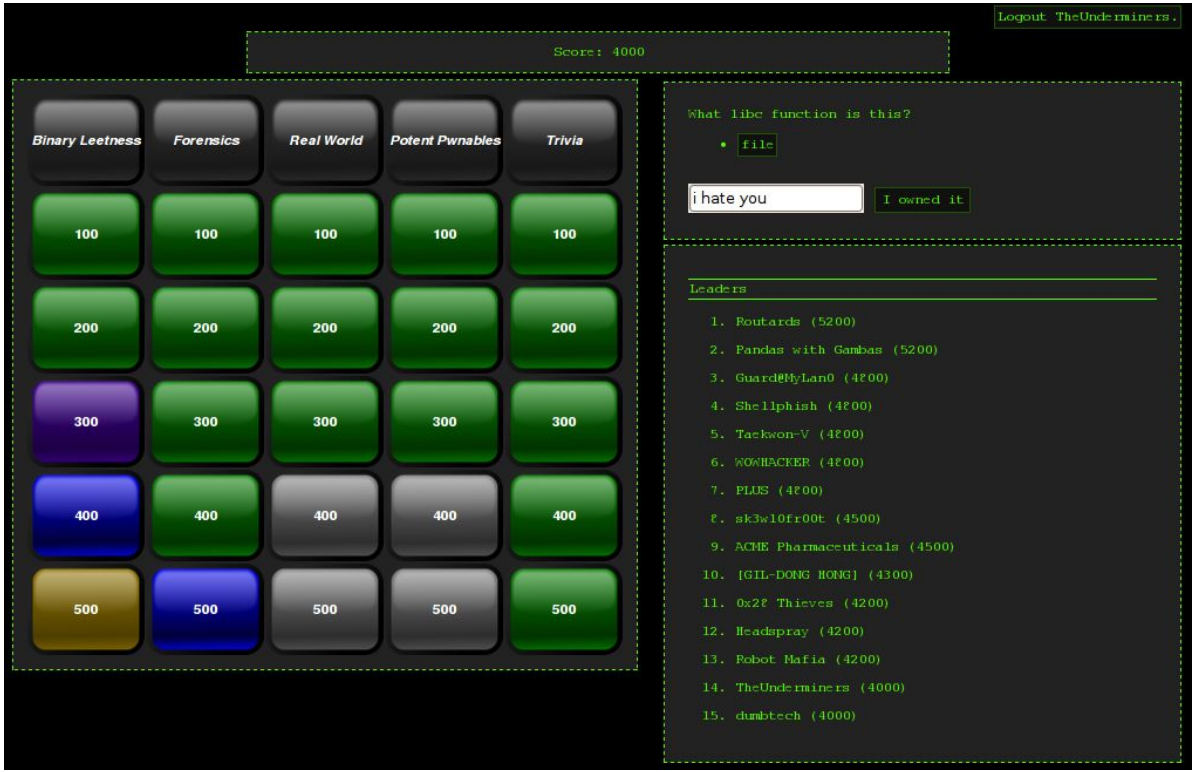
Today, DEF CON CTF is gated with a “qualifying round” which has been a Jeopardy style event.

Jeopardy style

- Questions are selected graphically revealing starter text (AKA a “hint”)
- Point values for answering a question are known a priori as well as the general category of the challenge
- A team answering the “lead” question correctly controls the board and may select the next question
  - If that takes too long, organizers open a new one
- Unlike Jeopardy, other players can continue to answer any previously “opened” question, accumulating points

Kenshoto 2006 Quals

Jeopardy style



What “areas of excellence” will be tested?

- Often there are some areas where newcomers can still garner some success
  - Lower point values
  - Trivia based questions

Kenshoto 2008 Quals (2007 was near identical)

Jeopardy style

What “areas of excellence” will be tested?

- Crypto
- SQLi
- XSS
- Buffer overflows
- Heap attacks
- Custom interpreters
- Etc
- Etc

Troll through CWE and CVEs?

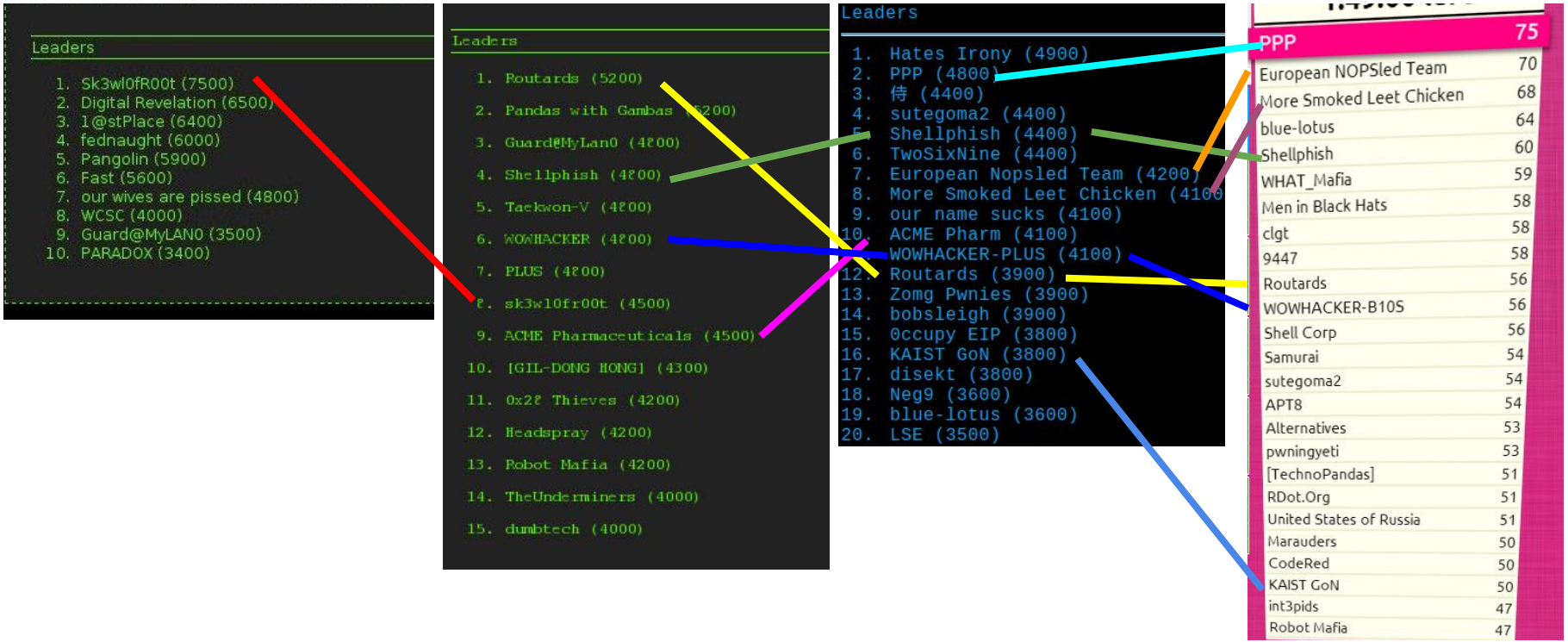
DDTEK 2012 Quals

Jeopardy style

- The concept of qualifying teams interactively based on achievement has persisted through the years.
- The basic organization and operation of the game board has remained similar through three organizers
  - Most other CTFs around the world have a similar appearance and operation
  - Some other CTFs have modified the semantics of the board

Legit BS 2013 Quals

Familiar Faces



Hacker Tracker

- Opt-in (mostly)
- Published formula
  - still subjective and/or crowdsourced components
- Cooperation, collusion, affiliation changes…
  - ?

Position	Name	Country	Points
1	Plaid Parliament of Pwning		1789.884
2	Dragon Sector		1184.774
3	0ops		1088.711
4	Shellphish		1019.307
5	!SpamAndHex		1015.489
6	dcua		917.887
7	Samurai		786.940

Rating is counted per-year

2017 formula

$$points\_coef = \frac{team\_points}{best\_points}$$

$$place\_coef = \frac{1}{team\_place}$$

$$if(points\_coef > 0) : E_{rating} = \frac{(points\_coef + place\_coef) * weight}{1/(1 + team\_place/total\_teams)}$$

$$total\_team\_rating = \sum_{i=1}^{10} E_{rating}$$

weight is an per-event value, depends on tasks and organization level, participated teams or public voting (pre
total_teams is a number of teams got >0 points in particular event
best_points is a number of points got by the winner of particular event
team_place is a final place got by the team in particular event
team_points is a number of points got by the team in particular event

No matter how many CTFs your team participate - only 10 best results count in yearly rating.

Pre-2017 formula

$$points\_coef = \frac{team\_points}{best\_points}$$

$$place\_coef = \frac{1}{team\_place}$$

$$if(points\_coef > 0) : E_{rating} = \frac{(points\_coef + place\_coef) * weight}{1/(1 + team\_place/total\_teams)}$$

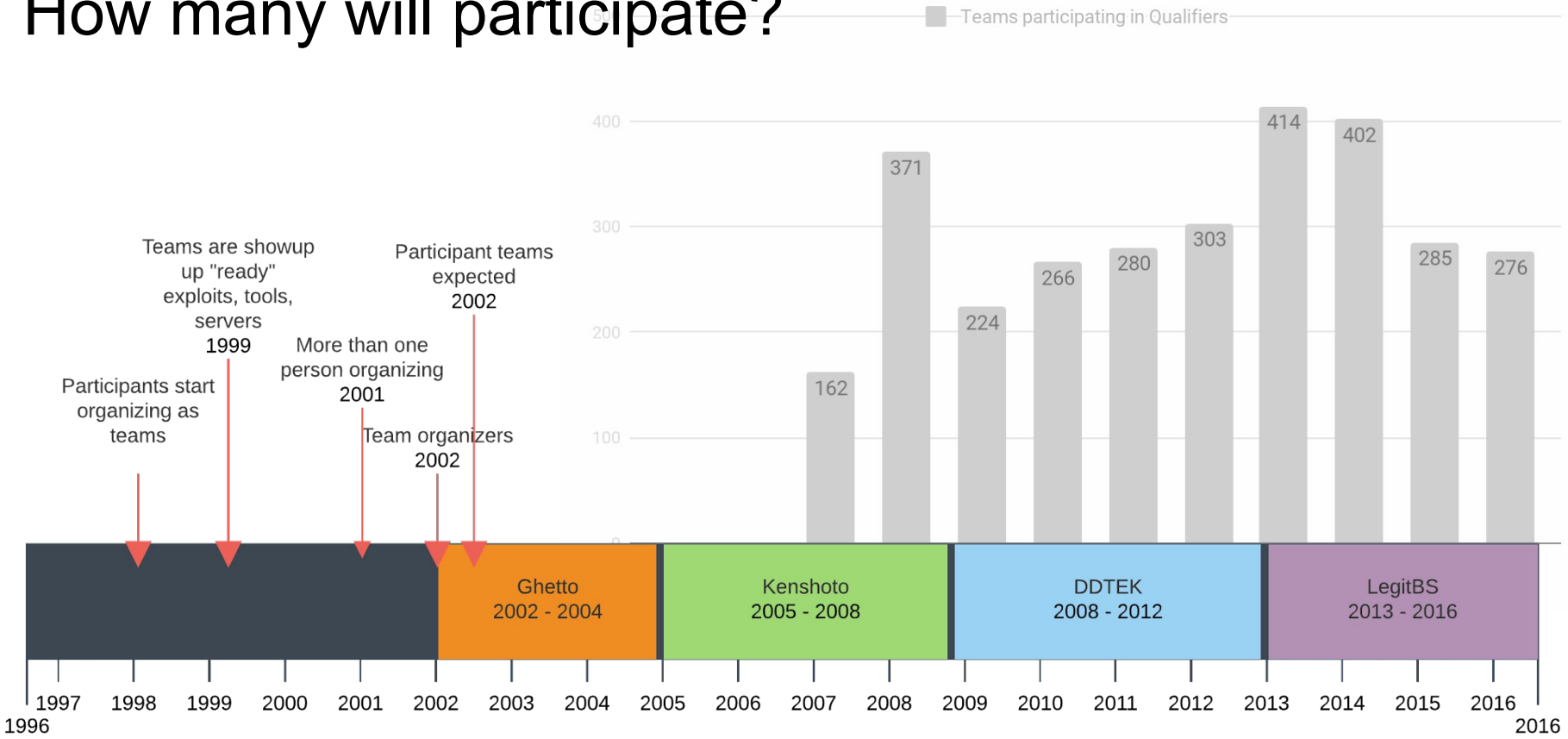
$$total\_team\_rating = \sum_{E \in participated\_year\_events} E_{rating}$$

weight is an per-event value, depends on tasks and organization level, participated teams or public voting
total_teams is a number of teams got >0 points in particular event
best_points is a number of points got by the winner of particular event
team_place is a final place got by the team in particular event
team_points is a number of points got by the team in particular event

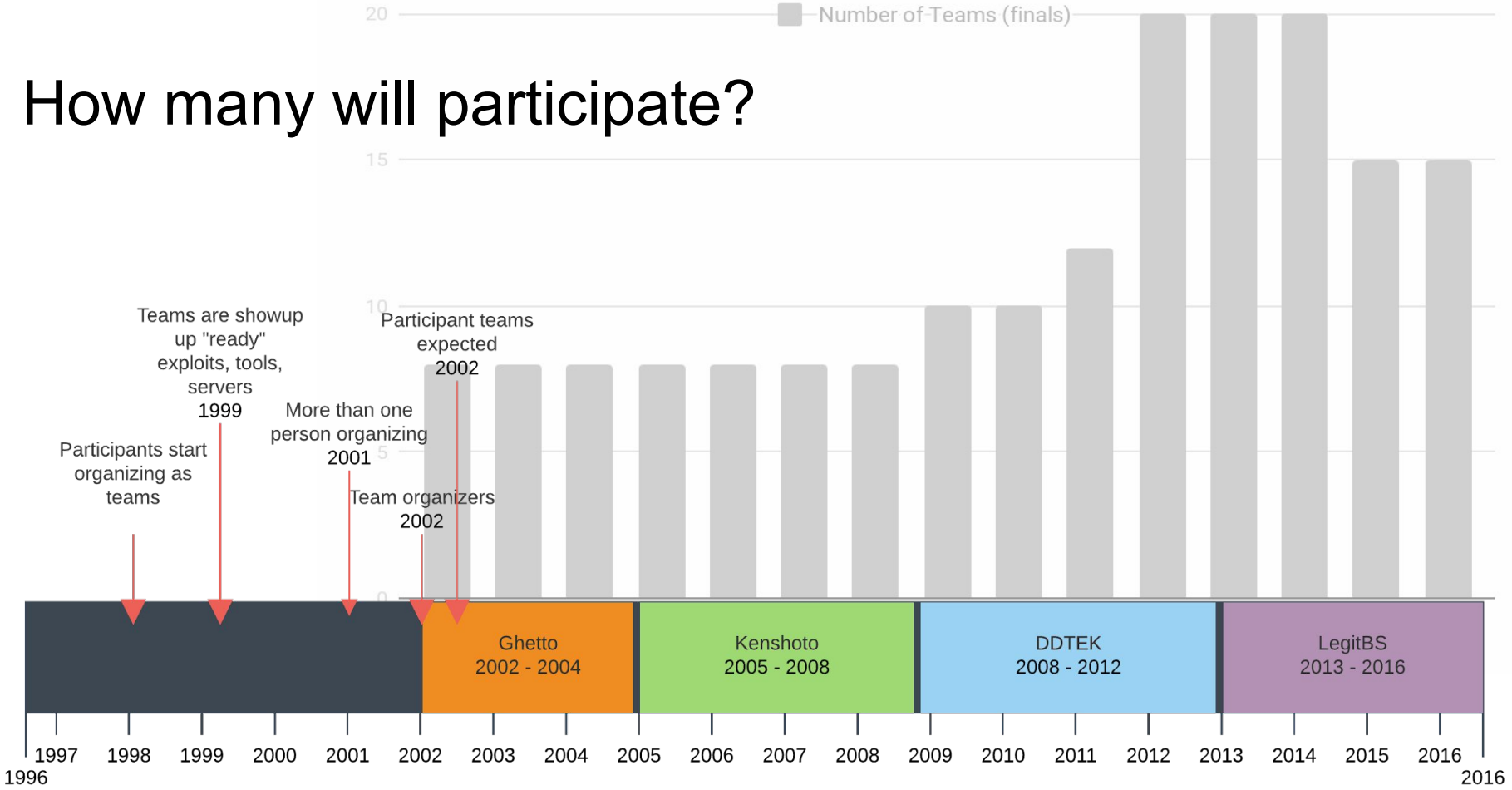
The more CTFs your team participate - the more rating points it gets.

https://ctftime.org/rating-formula/

How many will participate?



How many will participate?



How is attack-defend scoring implemented?

Offense

Stealing other teams' flags ("read")

Corrupting other teams' flags (aka deface, "write," overwrite")

Defense

Preventing other teams' offense ("block")

SLA

You have to keep your vulnerable services available to others

"Bonus Points"

First to gain some achievement ("breakthrough," "first blood")

Solve some out-of-game challenge

How is attack-defend scoring implemented?

Of course, these basic components need to be combined somehow….

Score = Offense * Defense * SLA

- If you have no Defense, you have no score...if you have no offense you have no score….

Score = Offense + Defense + SLA

- If a component is 0 it hurts, but doesn’t drive the score to zero

Score = (Offense + Defense) * SLA

- You must facilitate all teams’ ability to play the game in order to score

How is attack-defend scoring implemented?

These formulas need to work over time. The defense needs to be lasting, the attackers should demonstrate sustainable offense.

This is typically handled by “*rounds*” a fixed, or variable time segment. Many rounds pass during a CTF event.

Round score = ((Offense + Defense) * SLA)
Game score = sum(round scores)

Similarly, these formulas need to work across multiple services that might be present at any given time.

Service score = ((Offense + Defense) * SLA)
Round score = sum(service scores)
Game score = sum(round scores)

This is just a simple example, there are certainly many possibilities for formulas and implementations.

How is attack-defend scoring implemented?

On top of all this, the components need to be measured

Service availability (SLA)
This could be as simple as a port scan, but modern CTFs measure SLA more robustly many times per round by simulating non-malicious users via *polls*. A successful poll earns the tested team partial SLA points for that round. Polls are very service-specific and exercise various capabilities / code paths of a service.

Offense
If a flag is corrupted, how will the organizers know? Will the organizers prevent multiple opponents from continuously corrupting the same flag or is that the victim's responsibility?
Modern CTFs tend to employ custom kernels, hypervisors, etc to protect memory while still detecting the corruption. Manipulation of readable flags is similarly prevented.

Defense
Typically measured as the absence of other teams' offense against an opponent.

How is attack-defend scoring implemented?

None of this is set in stone.

Each year there is opportunity to devise new scoring methods to stress different goals.

Organizers will have to answer many questions:

- Is offense more important than defense?
- Is there desire to prevent “run away” scores and leave the possibility of dramatic “come from behind” victories?
- Should scores always increase over time?
- Should flag values be determined by the play of the game (e.g. commodity) or explicitly set by expert opinion (e.g. the service creators)?
- Will “bonus points” be a factor?

What should a “service” look like?

- Should there be a spec for services? [1]
- Is it “anything that listens on a socket?”
- Are local (non-networked) services permitted?
- How many services should there be in the entire event?
- How many active at any given time (concurrent)?
- What should the mix of ‘easy’ vs ‘difficult’ be?
- How to handle unintended vulnerabilities?
- Are services guaranteed to be vulnerable?

The more defined services are, the easier they are to:

- automate
- test
- deploy…
- ...and outsource!

Also...less flexible

[1] for instance https://github.com/CyberGrandChallenge/cgc-release-documentation/blob/master/walk-throughs/building-a-cb.md

How will teams interface with the infrastructure?

Will teams operate their own defended host?
-can teams entirely replace the OS?
-do they only have “root” access in BSD jail?

Does the game “route through” the table? (defended host on one cable, uplink on other)

Is a network tap / mirror cable provided?
-will this data be delayed?

Are inline network appliances (IDS) facilitated?

How are flags managed across rounds?
-rotated via the game network?
-rotated via hypervisor introspection (manipulation)

How to best protect the integrity of the game?

- Jails, chroots, VMs
  - layers?
- Solid infrastructure code
  - All the architecture and security that would be required in a hostile environment
  - Confidence in implementation; ability to verify
- Physical security
- Trustable people, secure Ops

Fair table positioning? (rotate tables, random assignment)

Fair addressing and naming? Shellcode considerations, nulls, \n, etc

- Ipv6 can contain an ‘a’
- Badge and team IDs might contain a 0
- Challenges that are only be vulnerable if they are executed on a Mac

Plan for failure

Shipping / sponsor issues

Failed hard discs on master server

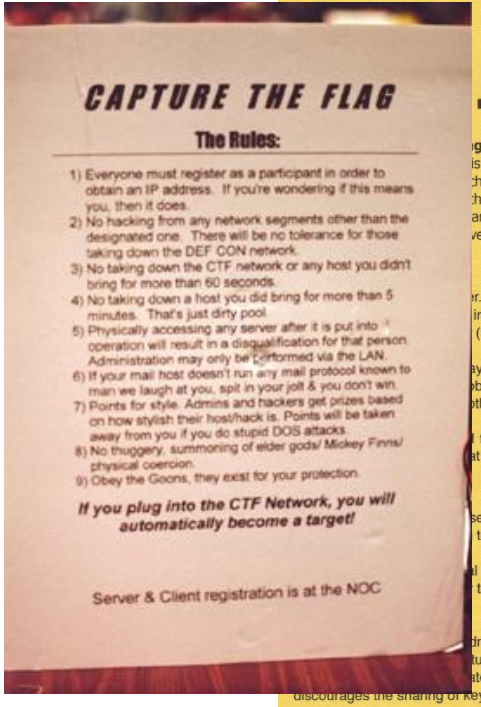
What will the rules and penalties be?

In the first years, rules were organically developed on-site

Typically, historically, the rules always include:

- **No physical attacks**

The intent is to literally prevent people from getting hurt.



CAPTURE THE FLAG

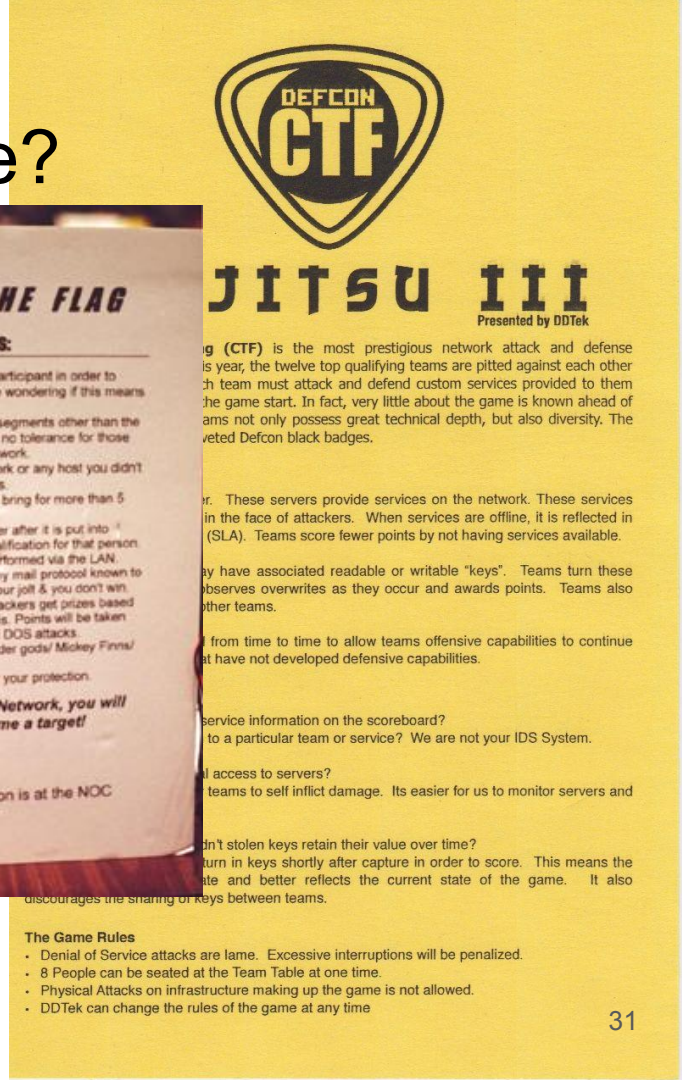
The Rules:

1) Everyone must register as a participant in order to obtain an IP address. If you're wondering if this means you, then it does.
2) No hacking from any network segments other than the designated one. There will be no tolerance for those taking down the DEF CON network.
3) No taking down the CTF network or any host you didn't bring for more than 60 seconds.
4) No taking down a host you did bring for more than 5 minutes. That's just dirty pool.
5) Physically accessing any server after it is put into operation will result in a disqualification for that person. Administration may only be performed via the LAN.
6) If your mail host doesn't run any mail protocol known to man we laugh at you, spit in your jolt & you don't win.
7) Points for style. Admins and hackers get prizes based on how stylish their host/hack is. Points will be taken away from you if you do stupid DOS attacks.
8) No thuggery, summoning of elder gods/ Mickey Finns/ physical coercion.
9) Obey the Goons, they exist for your protection.

If you plug into the CTF Network, you will automatically become a target!

Server & Client registration is at the NOC

DC 8



DEFCON CTF

JITSU III

Presented by DDTek

g (CTF) is the most prestigious network attack and defense
is year, the twelve top qualifying teams are pitted against each other
h team must attack and defend custom services provided to them
he game start. In fact, very little about the game is known ahead of
ams not only possess great technical depth, but also diversity. The
eted Defcon black badges.

r. These servers provide services on the network. These services
in the face of attackers. When services are offline, it is reflected in
(SLA). Teams score fewer points by not having services available.

y have associated readable or writable "keys". Teams turn these
bserves overwrites as they occur and awards points. Teams also
ther teams.

from time to time to allow teams offensive capabilities to continue
t have not developed defensive capabilities.

service information on the scoreboard?
to a particular team or service? We are not your IDS System.

l access to servers?
teams to self inflict damage. Its easier for us to monitor servers and

dn't stolen keys retain their value over time?
turn in keys shortly after capture in order to score. This means the
te and better reflects the current state of the game. It also
discourages the sharing of keys between teams.

The Game Rules

- Denial of Service attacks are lame. Excessive interruptions will be penalized.
- 8 People can be seated at the Team Table at one time.
- Physical Attacks on infrastructure making up the game is not allowed.
- DDTek can change the rules of the game at any time

31

DC 19

What will the rules and penalties be?

https://blog.legitbs.net/2013/08/finals-2013-rules.htm

In the first years, rules were organically developed on-site

Typically, historically, the rules always include:

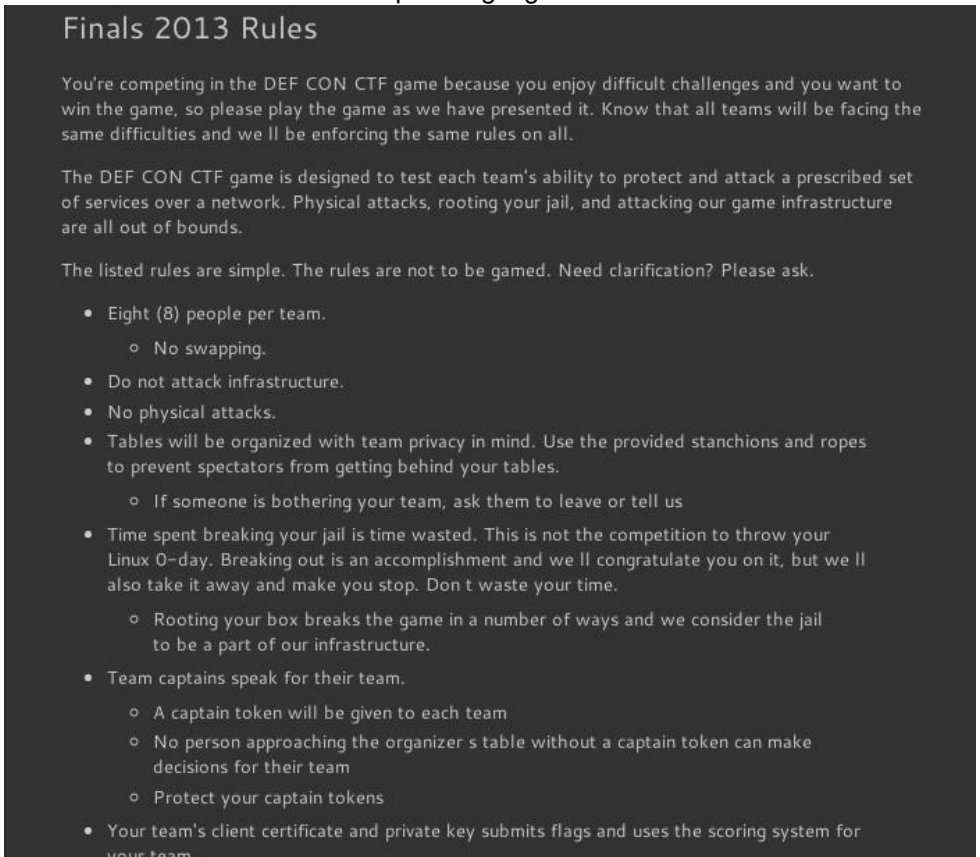
- **No physical attacks**

The intent is to literally prevent people from getting hurt.

Otherwise, common recurring rules include:

- Don’t mess with the infrastructure
- Don’t DOS teams

Violations are handled in various ways, typically to fit the crime



Finals 2013 Rules

You're competing in the DEF CON CTF game because you enjoy difficult challenges and you want to win the game, so please play the game as we have presented it. Know that all teams will be facing the same difficulties and we ll be enforcing the same rules on all.

The DEF CON CTF game is designed to test each team's ability to protect and attack a prescribed set of services over a network. Physical attacks, rooting your jail, and attacking our game infrastructure are all out of bounds.

The listed rules are simple. The rules are not to be gamed. Need clarification? Please ask.

- Eight (8) people per team.
  - No swapping.
- Do not attack infrastructure.
- No physical attacks.
- Tables will be organized with team privacy in mind. Use the provided stanchions and ropes to prevent spectators from getting behind your tables.
  - If someone is bothering your team, ask them to leave or tell us
- Time spent breaking your jail is time wasted. This is not the competition to throw your Linux 0-day. Breaking out is an accomplishment and we ll congratulate you on it, but we ll also take it away and make you stop. Don t waste your time.
  - Rooting your box breaks the game in a number of ways and we consider the jail to be a part of our infrastructure.
- Team captains speak for their team.
  - A captain token will be given to each team
  - No person approaching the organizer s table without a captain token can make decisions for their team
  - Protect your captain tokens
- Your team's client certificate and private key submits flags and uses the scoring system for

Cultural influences upon CTF

When designing challenges, it is easy to assume too much about localized culture

- Language barrier
- Popular culture (e.g. “hacker movies”)
- Time zones / holidays

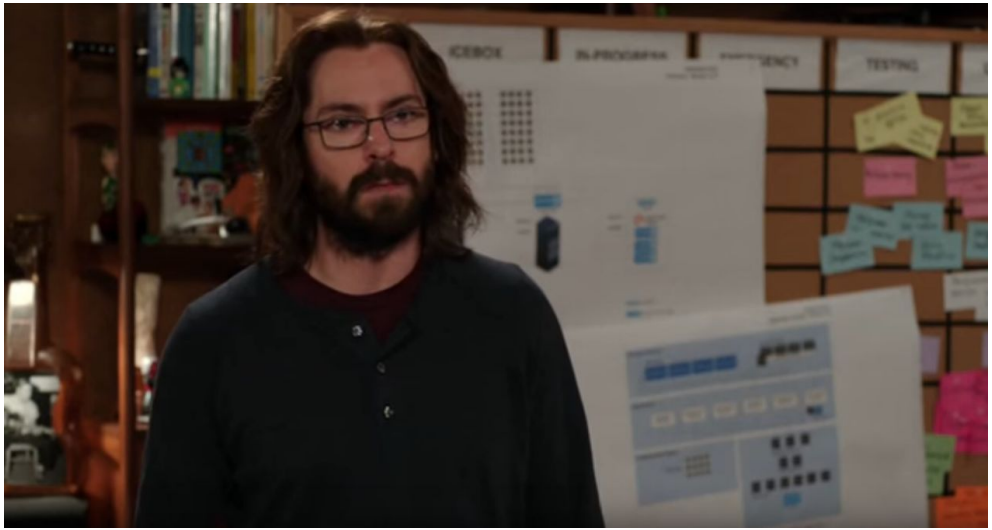
This can have impact throughout a CTF event, but tends to come up quickly in:

- Trivia category for Jeopardy style
- Question “starters” in Jeopardy style
- When giving hints, tutorials, clarifications
- generally interacting with teams/capitans
- User interface / ascii protocols in challenges

Cultural influence by CTF

The CTF community also leaves it’s mark on various cultures

Generals, producers, actors, etc visit the CTF room



“No one is cracking our transfer, not Seth, not some rogue nuclear state, not Sk3wl of f*&#% Root.”

HBO Silicon Valley, Season 2, Episode 8

How will the audience participate / Visualization

Should there be ambiance? Distraction? Attraction?

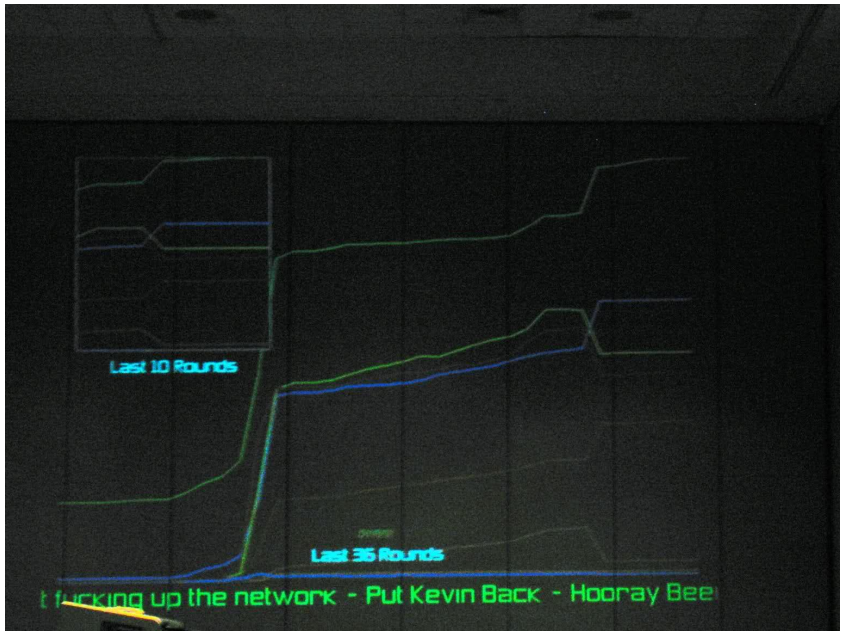
Music, videos, scoreboard, visual effects, etc

Otherwise, it's just a bunch of people staring at computers

Visualization

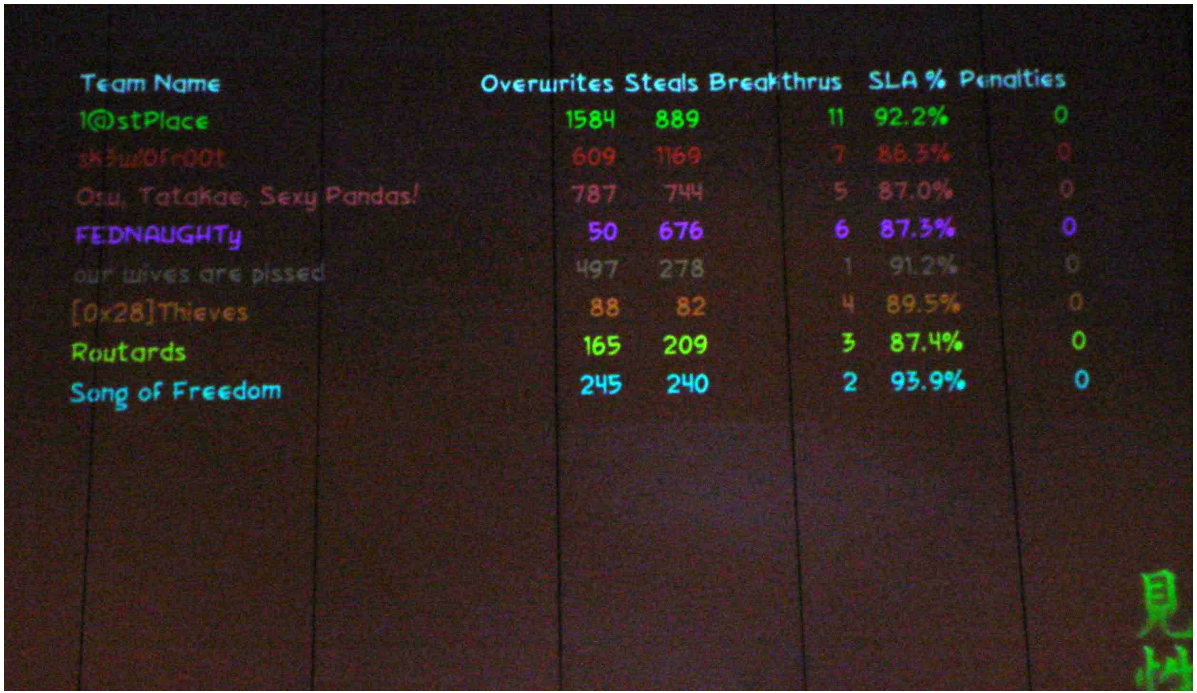
DEF CON CTF 2002?

Visualization



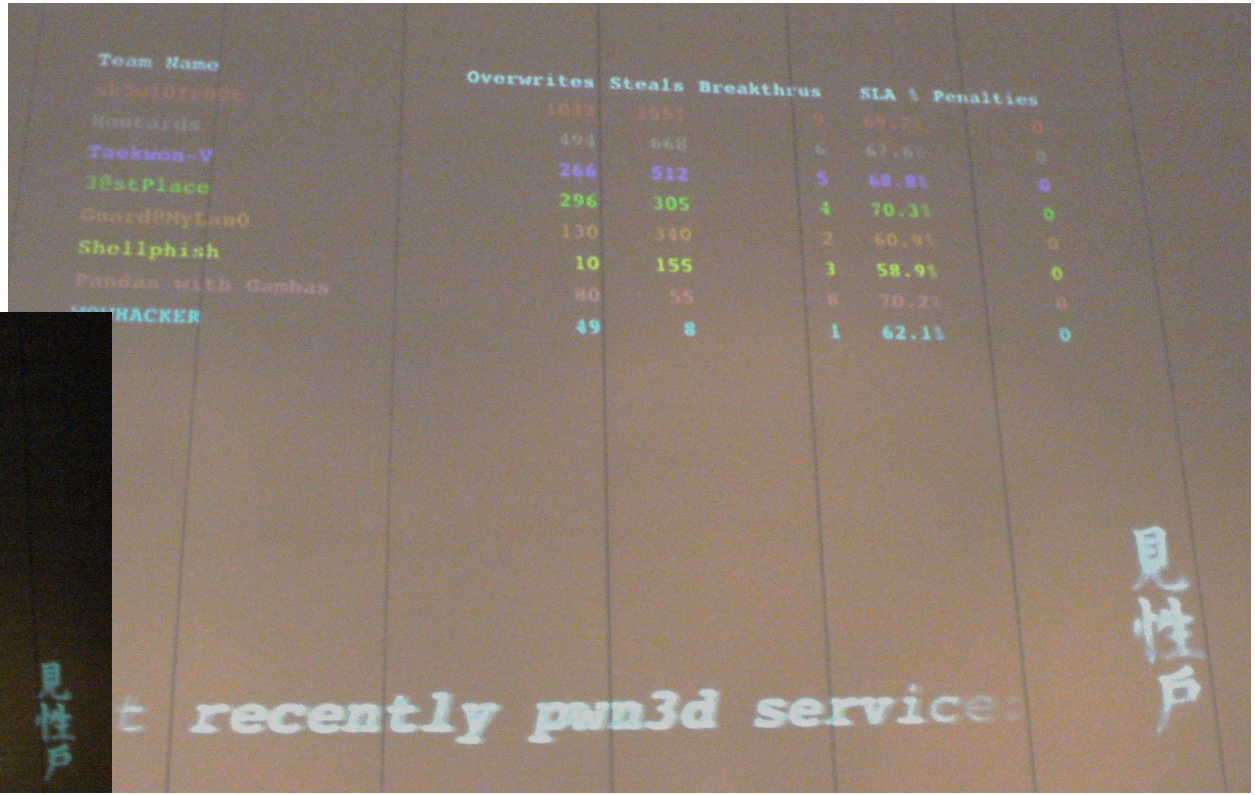
DEF CON CTF 2006

Visualization



DEF CON CTF 2007

Visualization



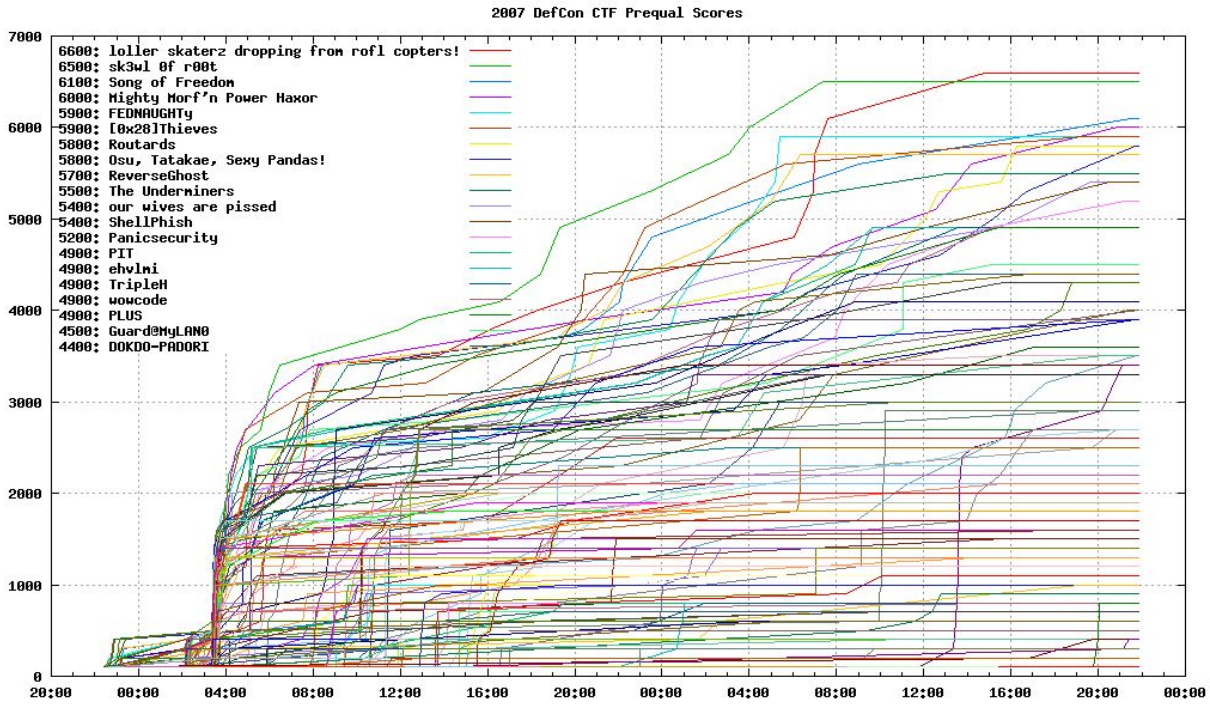
DEF CON CTF 2008

Visualization

Making data available allows others to use the data in unanticipated ways

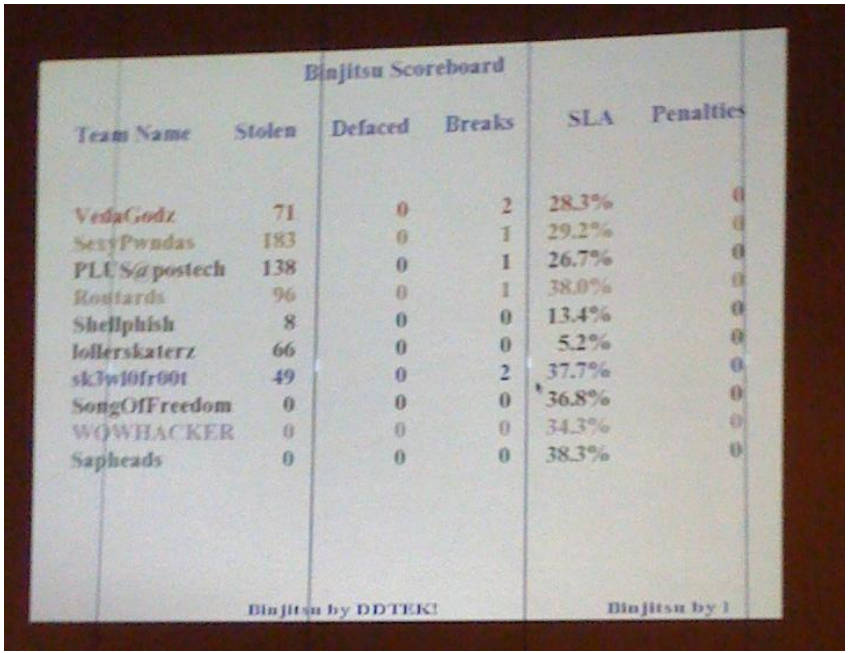
Here a team used Qualifier data to plot the relative positioning of teams through the weekend event.

Note how this visualization makes it easy to see teams pull ahead and come from behind



Quals 2007 score plot (http://nopsr.us/ctf2007prequal/)

Visualization



Binjitsu Scoreboard

Team Name	Stolen	Defaced	Breaks	SLA	Penalties
VedaGodz	71	0	2	28.3%	0
SexyPwndas	183	0	1	29.2%	0
PLUS@postech	138	0	1	26.7%	0
Routards	96	0	1	38.0%	0
Shellphish	8	0	0	13.4%	0
lollerskaterz	66	0	0	5.2%	0
sk3wl0fr00t	49	0	2	37.7%	0
SongOfFreedom	0	0	0	36.8%	0
WOWHACKER	0	0	0	34.3%	0
Sapheads	0	0	0	38.3%	0

Binjitsu by DDTEK! Binjitsu by 1

DEF CON CTF 2009

Visualization

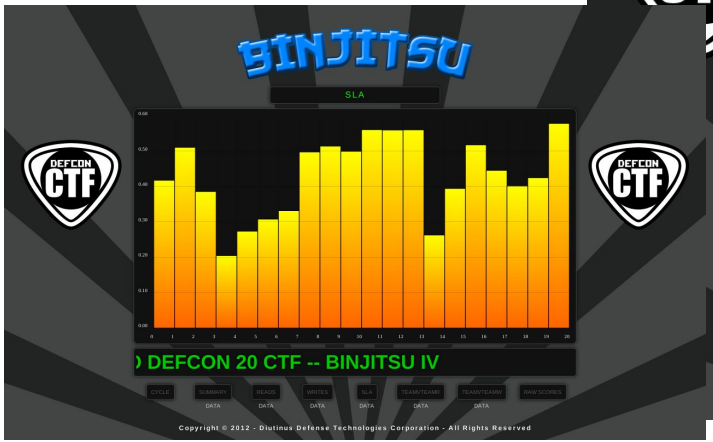
SCOREBOARD

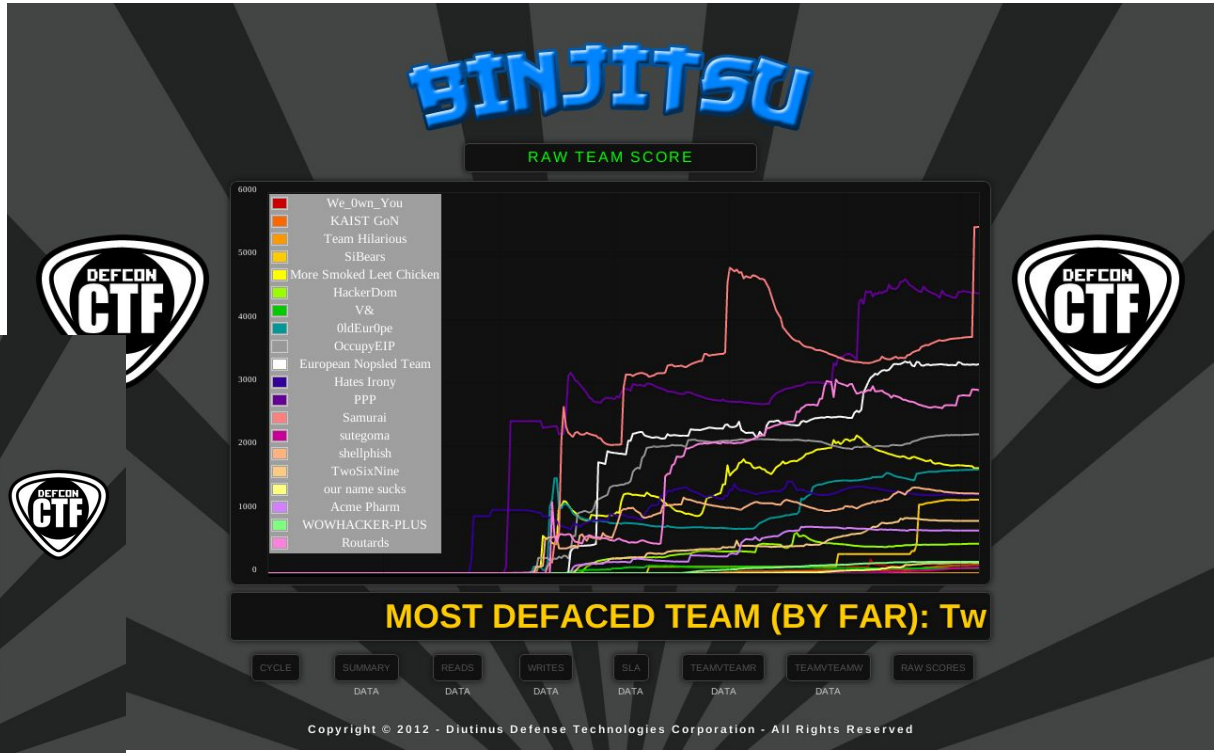
SUMMARY

Rank	Team	Steals	Defaces	First Blood
1	NOPSledTeam	1961	1404	0
2	Routards	2459	1350	6
3	HatesIrony	1460	710	0
4	Int3pid	759	180	0
5	IV	1059	329	0
6	PPP	984	565	1
7	Plus@Postech	980	418	1
8	Lollersk8ters	247	0	3
9	AcmePharm	26	122	0
10	Velociroptors	343	229	0
11	ShellPhish	37	28	0
12	Sutegoma2	195	0	0

DEF CON CTF 2011

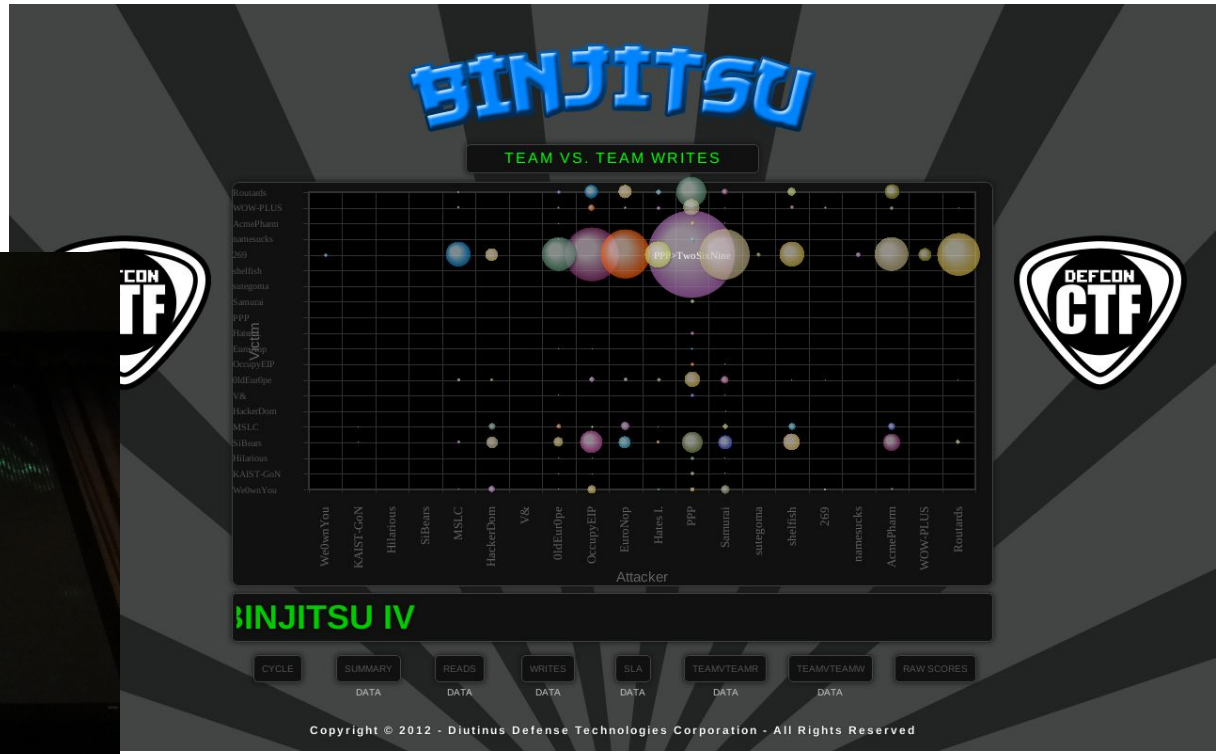
Visualization





DEF CON CTF 2012

Visualization

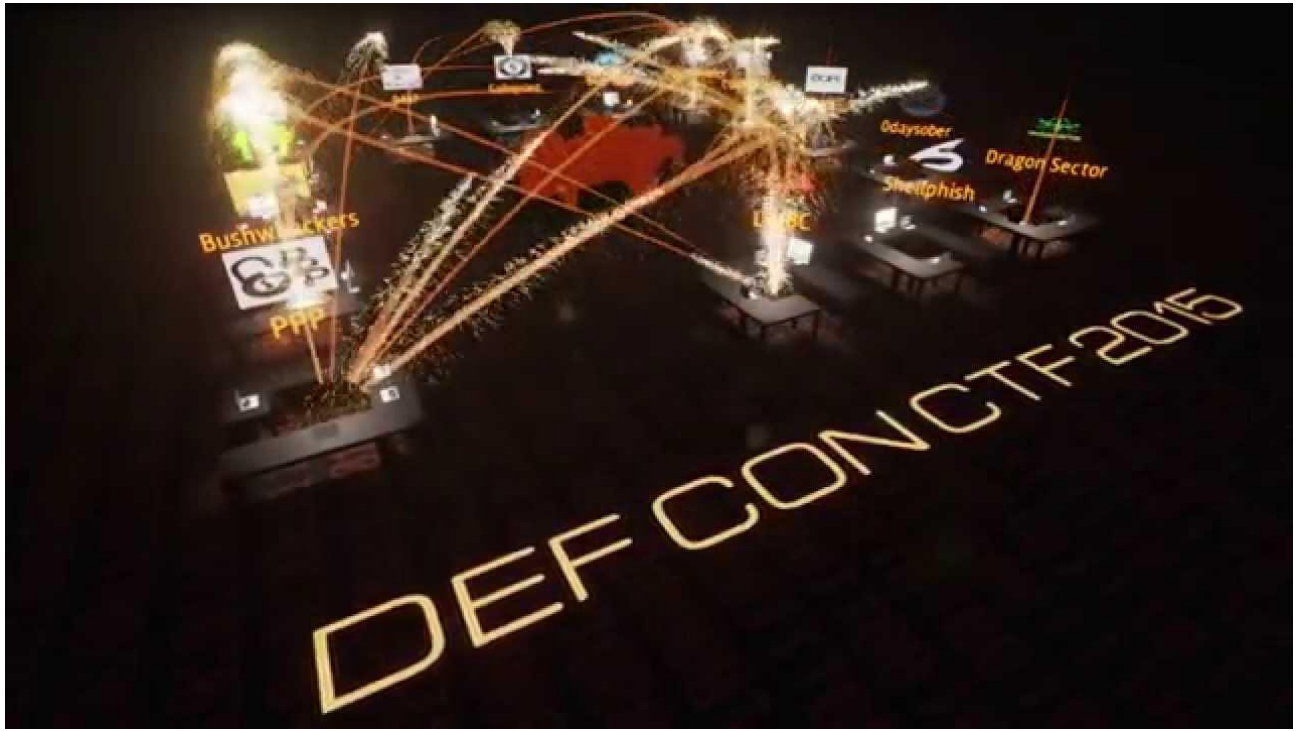


DEF CON CTF 2012

Visualization

DEF CON CTF 2014

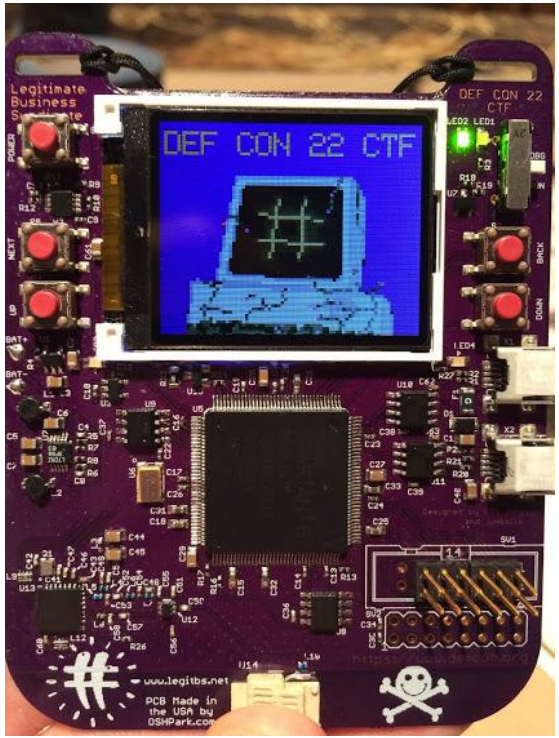
Visualization



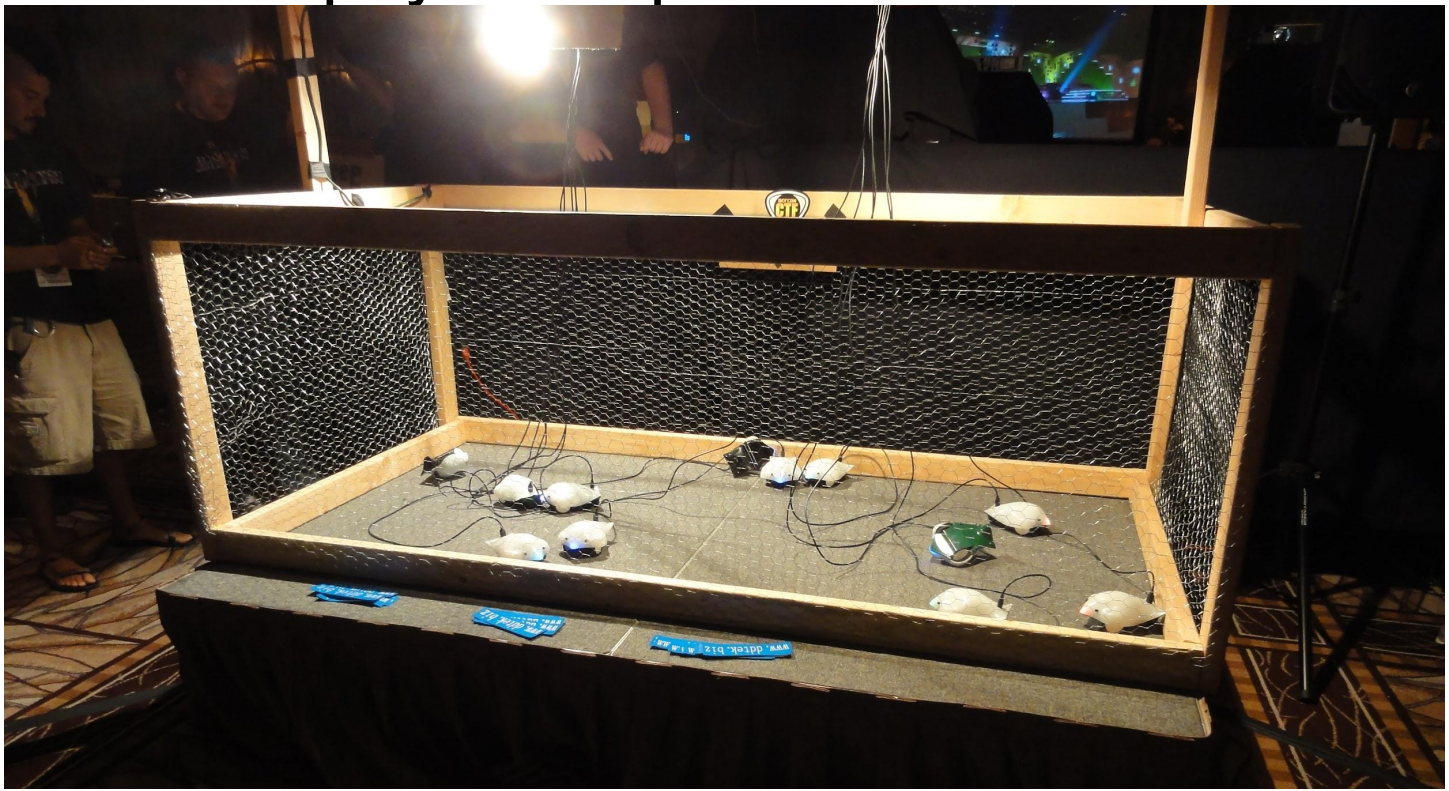
DEF CON CTF 2015

Expansion into physical space

- “Game outside the game” / meta game
- can be engaging for the audience
- Can bring unusual/unexpected challenge to the participants
- Lock picking is common in many CTFs
- Examples:
  - Distribution of initial password via floppy disc + RFID tag
  - Physical printers on each table
  - Custom badge that is actually part of a scorable CTF service (DC22)
  - Embedding challenge info (CTF scorable) into all the DEF CON badge firmware (DC18)
  - “Robot chicken cage match”



Expansion into physical space



2011

Tradition

- Keeping DEF CON CTF
  - best in the world
  - fair
  - fun
- Innovate
- Attempt to engage the audience
  - Visualization
  - Handouts
  - Other enticements

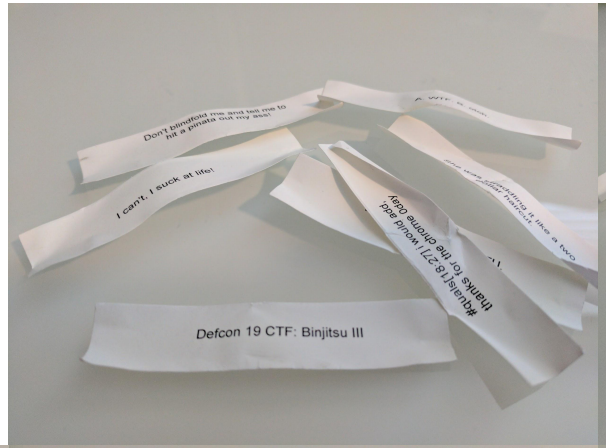
DEF CON 16 Banner

- Logistics
  - Game banner (given to winning team)
  - Team banners
- Swag
  - T-shirts
  - Fortune cookies (Tossing of the cookies)
  - Stickers
  - Stress sheep
  - Patches
  - Other
- Announcements happen on April 1
-

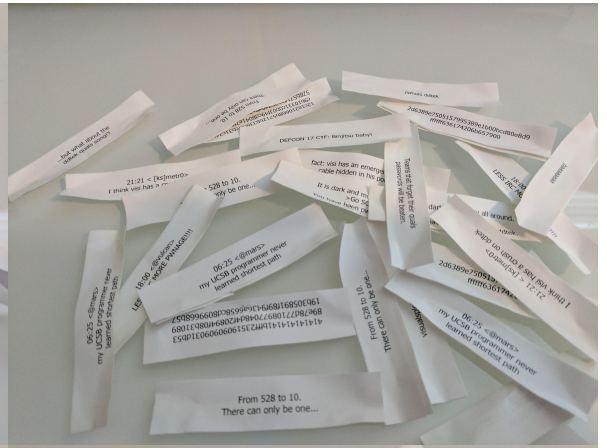
Fortunes

Tossing of the cookies

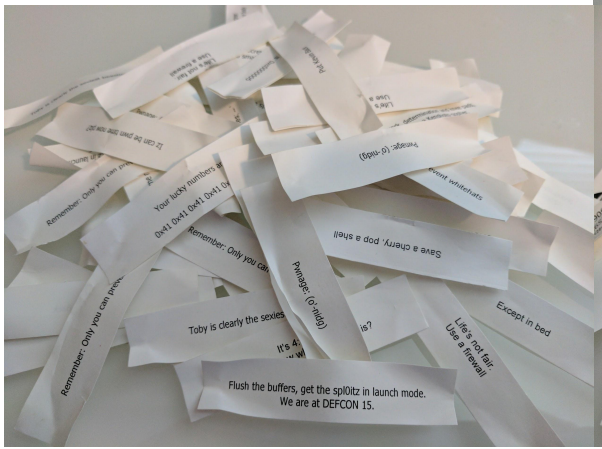
DEF CON 19



DEF CON 17



DEF CON 15



DEF CON 18

DEF CON 20

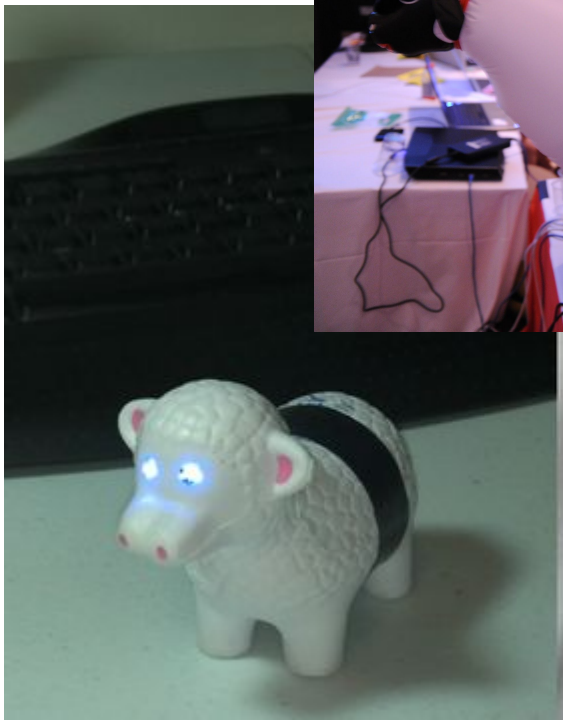
Will there be stickers?

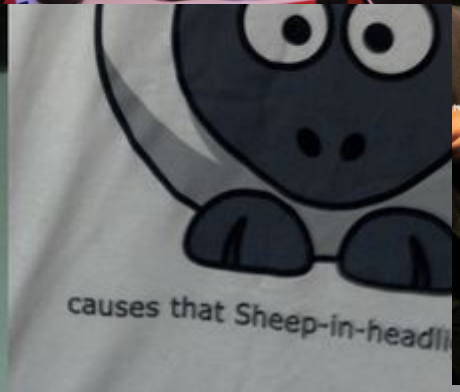
Will there be coins?

Other things

Teams also bring things

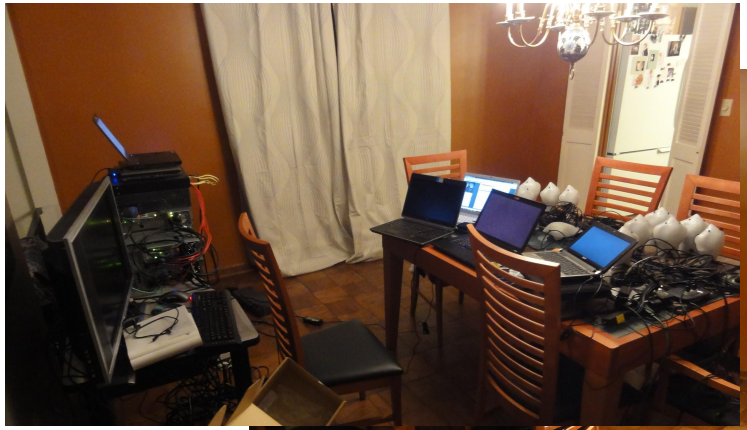
And do things





Preparation

Pre-Programming and configuring special purpose laptops, servers



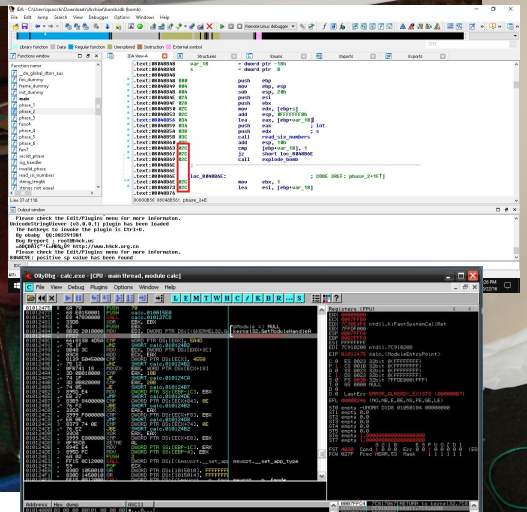
Preparation

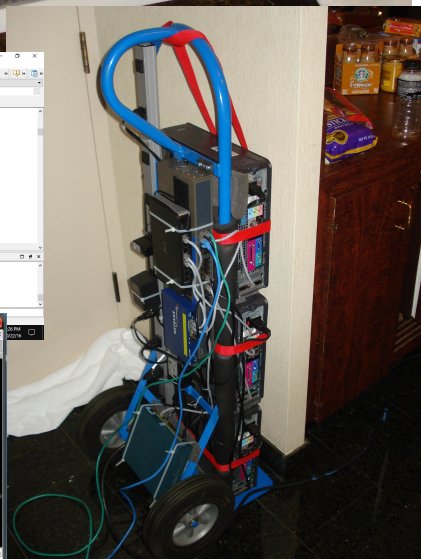
- Credential / information distribution

- SWAG

What an organizer sees (proportionally)

What a participant sees (proportionally)

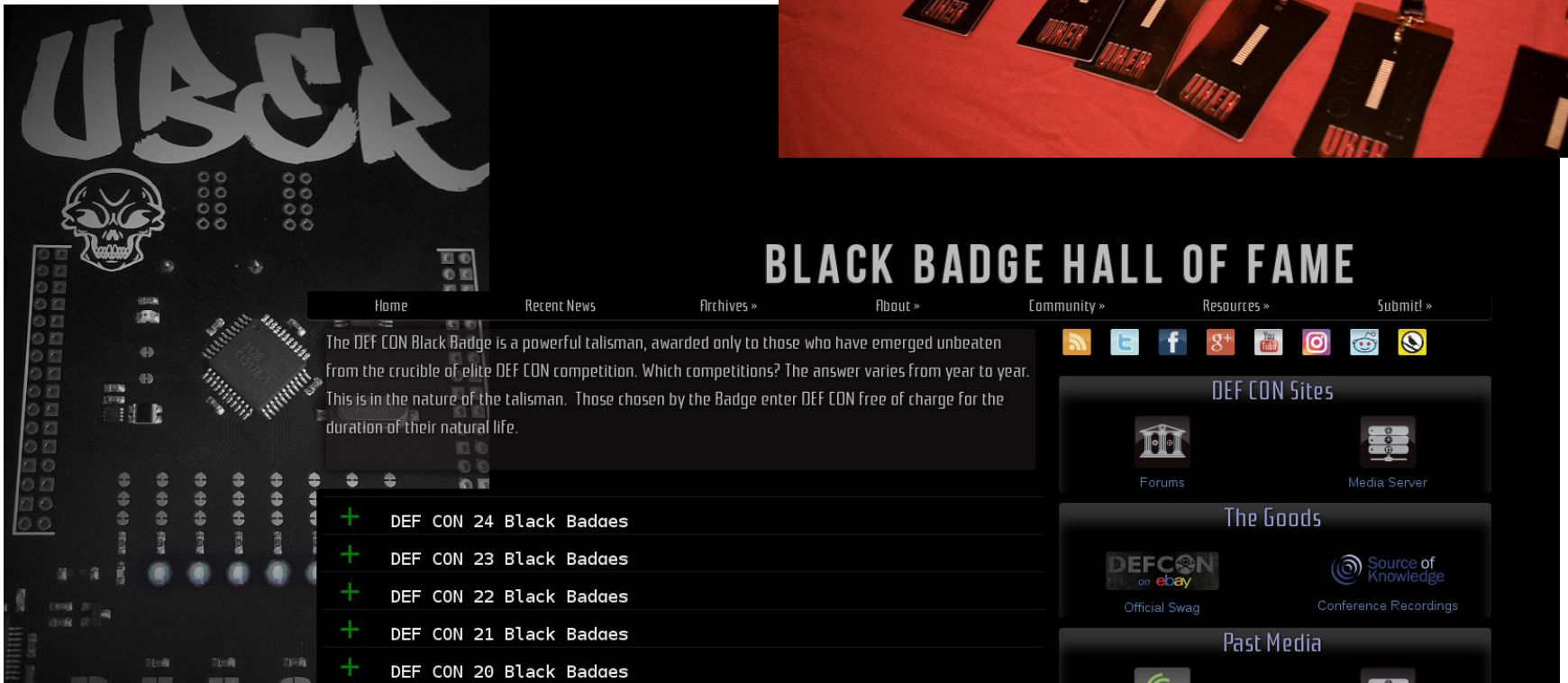




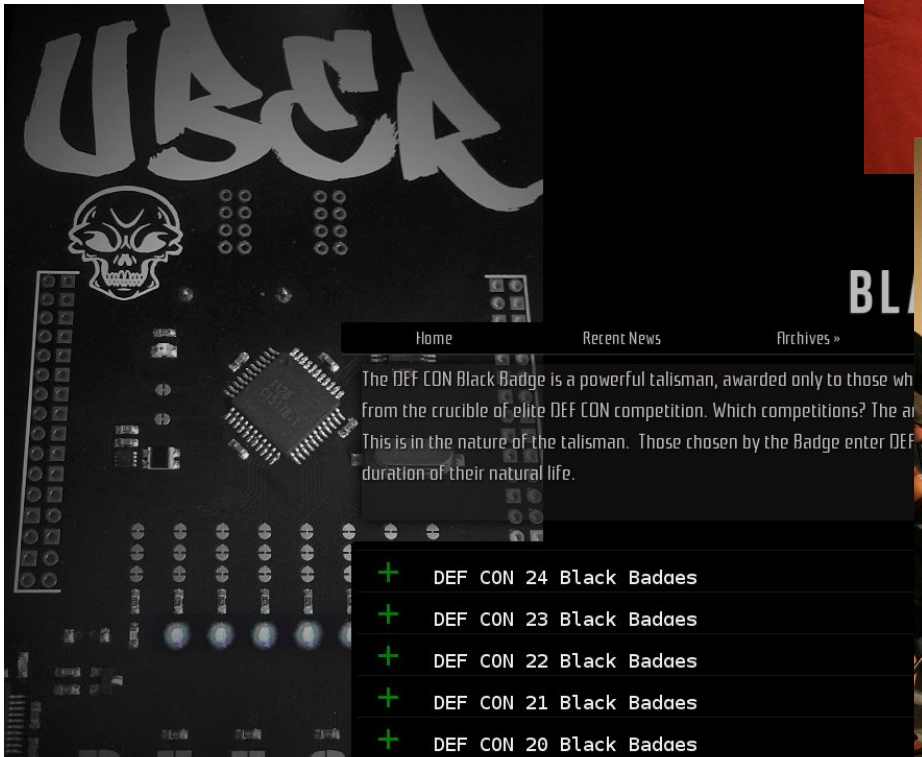
Why do people play?

- Challenge
- Prizes
- Can’t get into talks
- Pathological disorder
- Accomplishment / prestige

Why do people play?



Why do people play?



Why do organizers organize?

?

Panelists

DEF CON CTF Organizer 2005-2008 (Kenshoto)
Vivisect creator
Crowdsources bios

Invisigoth @invisig0th

@femmeshoto:	Founder and Chief Wine Taster of the Vertex Project. Will only toast to pwning.
@tvidas:	...known to hide spare Ethernet cables in his ponytail...
@1o57:	Was invited to tea, drank all of it... with no sugar.
@s7ephen:	Principal Knickerbocker at the PantsFactory
@zakklol:	Famous whitehat hacker
@tobyhush:	Purchaser of the most expensive glass of scotch i've had the pleasure of tasting
@cybercrimetech:	조금 미쳤어
@grimmcyber:	[Redacted]
@KyleHanslovan:	Defender of dance moves. Emperor of exploitation. Master of the Manchu hairstyle.
@snowchyld:	hoopiest of froods
@xabean:	' DELETE FROM BIO; --
@zakklol:	once tamed a rabid hedgehog
@aris_ada:	Wrote some random code for reasons.
@cocaman:	STATUS 418
@bertjwregeer:	Rabbit? Flu shot? Someone talk to me!
@brysonbort:	Taught me, like many others, a lot in this space
@sckain:	Likes those freakin' toe shoes.
@soylentGrn:	Former CTO of Prestige Worldwide. Boats and...

DEF CON CTF Organizer 2008-2012 (DDTEK)
DEF CON CTF Champion (2x) (Sk3wl of r00t)
The Ida Pro Book author

Chris Eagle @sk3wl

Chris Eagle is a registered hex offender. He has been taking software apart since he first learned to put it together over 36 years ago. His research interests include computer network operations, malware analysis and reverse/anti-reverse engineering techniques. He is the author of The IDA Pro Book and co-author of Gray Hat Hacking.

Chris organized and led the Sk3wl of r00t to two DEF CON Capture the Flag championships and produced that competition for four years as part of the DDTEK organization.

Caezar @rileycaezar

DEF CON CTF Organizer 2002-2004 (Ghetto)
DEF CON CTF Champion (3x) (Ghettohackers)
Known for “Caezer’s Challenge

Riley Eller began his career at the age of fourteen when he taught himself to program and explored the “hacking community.” A product of canyon life in Nevada, he felt that hacking allowed him a new and novel way to explore the world - allowing him to liberate ideas and connect people. In the late 90's, Eller joined a group of professional hackers to compete in DEFCON, the most prestigious hacking event in the world. In 2000, he and his team of hackers won the DEFCON 7 competition and subsequently DEFCON 8 and 9. This allowed Riley to expand new skills and dive further into the world of security.

Eller has spoken at many established security venues, is a listed inventor on numerous patents, and is known for hosting “the most interesting party to get into in the world” - Caezar’s Challenge (a yearly party for the smartest and weirdest people in the world who discuss the world’s pressing security concerns). In his free time, Eller continues to mentor and counsel young hackers and to address the mental health issues in the hacking community.

DEF CON CTF Organizer 2013 - ??? (LegitBS)
DEF CON CTF Champion (2x) (Samurai, TA)

Hawaii John

hj@cromulence.com

Hawaii John started hacking a long time ago and still at it. He is currently the CTO of Cromulence, is a two-time winner of DEF CON CTF, and runs DEF CON CTF as part of the Legitimate Business Syndicate.

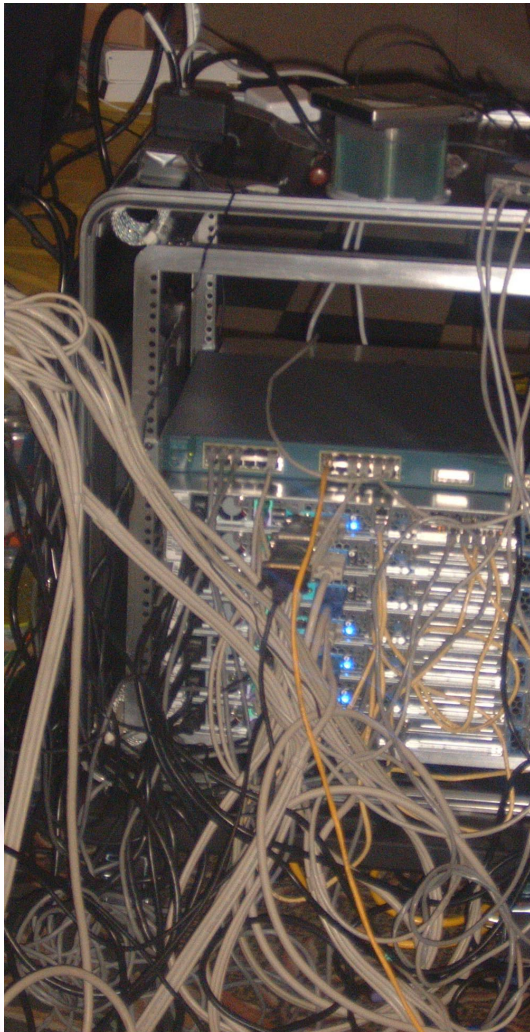
Myles

Myles attended DEF CON 3 and realized it was missing a contest. the next year he started CTF and ran it through DC 10.

Miles now hacks on keyboard micro controllers and global cloud extranets.

2002

DC 12



DEF CON 12


MEGA
ROOT FU
[EAST VS. WEST]
A 3000 PARTICIPANT BI-COASTAL CYBERWAR SHOWDOWN
HTTP://MEGA.ROOTFU.ORG
INFO@ROOTFU.ORG
POWERED BY GHI


友万每
万名友
北

DEFCON CTF HISTORY

CTF	DC	Year	winner	host - title / image (number of teams)
1	4	1996	AJ Reznor	goons - ctf
2	5	1997	AJ Reznor	goons - ctf
3	6	1998	SNI	goons - ctf
4	7	1999	ghettohackers	goons - ctf / up to team
5	8	2000	ghettohackers	goons - ctf / up to team
6	9	2001	ghetto+digirev	goons - ctf / up to team
7	10	2002	digirev	ghettohackers - root fu / redhat 6.2 (8)
8	11	2003	Anomaly	ghettohackers - root fu / openbsd (4)
9	12	2004	sk3wl0fr00t	ghettohackers - root fu / windows (8)
10	13	2005	shellphish	kenshoto - war gamez / freebsd 5.4 (8)
11	14	2006	l@stplace	kenshoto - war gamez / solaris 10 (8)
12	15	2007	l@stplace	kenshoto - war gamez / freebsd (8)
13	16	2008	Sk3wl0fr00t	kenshoto - war gamez / freebsd (8)
14	17	2009	vedagodz	ddtek - binjitsu / freebsd (10*)
15	18	2010	ACME Pharm	ddtek - binjitsu / freebsd+debian (10)
16	19	2011	TBD	ddtek - binjitsu / ????? (12)

*well actually 9, as the team "sk3wl0fr00t" was actually ddtek running the game from a team table

Capture the Flag is one of the oldest contests at Defcon dating back to Defcon 4. In the past few years, "capturing the flag" has become a popular moniker for all kinds of contests, and the sheer quantity of CTFs has been increasing steadily. Defcon CTF is one of the (if not the) oldest CTF that continues to run today. Here you can find a brief history of the contest and its evolution.

Defcon 4 was the first time CTF was really formalized into a contest - judges now decided when a points should be awarded. In Defcon 5 and 6, participants could either provide a target or attack provided targets for points, as you might imagine this amount of flexibility led to chaos on the game floor. Over the years, the game has matured and events such as point scoring have largely been automated (heavily in many cases), this maturity is largely a result of having dedicated, non-defcon organizers. Naming the organizer early allows the organizer to dedicate time to game structure and infrastructure.

After a display of dominance in DC7-9, the ghettohackers became contest organizers for three years, before giving the reigns up to Kenshoto. After winning twice (and coming very close to winning several other times) ddtek took over contest organization for DC17 (ddtek is a subgroup of Sk3wl0fr00t). During DC7-9 the contest seemed to be about equally as much about hacking the contest as hacking the game servers

Since DC10, CTF has been about custom services, pwn others', patch and protect your own. Each organizer has built on this model with technology aimed at preserving a fair game, additional twists such as scoring methods, and ever increasing difficulty. Recent organizers have chosen to keep the game layout secret until the game starts, participants do not necessarily know the scoring algorithm, network structure, or operating systems involved. At its core CTF is meant to test computer and network security. To some, that seems to be a fairly narrow focus area, but most Defcon attendees realize that "cyber security" is actually a very large and diverse field. Services range from poorly implemented or configured crypto, SQL-injection, cross-site-scripting, buffer overflows, timing attacks, heap exploits, malformed network constructs, custom interpreters, the list is truly endless. What will the contest bring this year?

As the contest matured, teams started participating regularly and more desired to play. A method of "qualifying" was implemented similar to the Olympics and other sporting events. For the past several years a qualification weekend has pitted teams against a set of challenges and the clock. Teams with the most points at the end are invited to participate in person at Defcon. There is really no excuse to not participate in quals, if you're reading this, you should register and participate next year. Phrases like "placing 132nd feels like quite an accomplishment" tend to appear on social networks.

In 2009 ddtek, an unknown name in the community, was announced as the CTF organizer. From the time of organizer announcement, through qualification round, a lot of google-translated IRC, and even through the entire contest during Defcon, nobody suspected that the folks sitting at the sk3wl0fr00t contest table were actually running the game! "Hacking the top hacker contest" seemed like a fun way to introduce ourselves to CTF organization. The yells of "bullshit" from CTF teams during the Defcon 17 awards ceremony were very gratifying.

more info at https://www.defcon.org/html/links/dc-ctf.html

more info at http://www.ddtek.biz

Swing by the CTF Room and see what's going on. You'll never really know what it's about until you dive in.

~vulc@n

TOP SECRET

Handouts

DEFCON CTF

BINJITSU III

Presented by DDTek

Defcon Capture the Flag (CTF) is the most prestigious network attack and defense competition in the world. This year, the twelve top qualifying teams are pitted against each other in an all out digital war. Each team must attack and defend custom services provided to them that are not known prior to the game start. In fact, very little about the game is known ahead of time. As such, successful teams not only possess great technical depth, but also diversity. The winning team will receive coveted Defcon black badges.

The Game Explained

Teams are provided a server. These servers provide services on the network. These services must remain available even in the face of attackers. When services are offline, it is reflected in the Service Level Availability (SLA). Teams score fewer points by not having services available.

Each exploitable service may have associated readable or writable "keys". Teams turn these keys in for credit. DDTek observes overwrites as they occur and awards points. Teams also submit keys they read from other teams.

Readable keys are changed from time to time to allow teams offensive capabilities to continue pwning services of teams that have not developed defensive capabilities.

CTF Q&A

Why doesn't DDTek display service information on the scoreboard?
Why should we call attention to a particular team or service? We are not your IDS System.

Why don't teams get physical access to servers?
Many reasons, it's harder for teams to self inflict damage. Its easier for us to monitor servers and ensure the game is running.

Why do keys expire? Shouldn't stolen keys retain their value over time?
Expiring keys forces teams turn in keys shortly after capture in order to score. This means the scoreboard is more accurate and better reflects the current state of the game. It also discourages the sharing of keys between teams.

The Game Rules

- Denial of Service attacks are lame. Excessive interruptions will be penalized.
- 8 People can be seated at the Team Table at one time.
- Physical Attacks on infrastructure making up the game is not allowed.
- DDTek can change the rules of the game at any time

DEFCON CTF SCORING

Scoring a CTF is a challenging proposition. In order to become a master of binjitsu, it is essential to understand how you will be measured.

True binjitsu masters understand that the path to enlightenment may only be achieved by maintaining the delicate balance between the offensive and the defensive arts. This year CTF scoring follows the approach introduced last year for measuring what is happening in the game and is designed to reward offensive as well as defensive excellence. Services constitute the heart of the CTF game. Each team must attack and defend identically configured servers, each running some number of custom services. The idea is to analyze the custom services for vulnerabilities and to develop both an attack and a defense strategy for each service. By exploiting a service an attacker gains access to privileged information which is generally referred to as a key (aka flag, aka token). Keys may be readable (steal information), writable (corrupt information), or both. Teams demonstrate that they have stolen information by turning stolen keys into a key submission server. Teams demonstrate that they can deface a service by overwriting keys with a replacement key unique to the attacker. For both of these activities, teams are awarded points. In order to keep things interesting, keys are periodically updated by the contest organizers, allowing teams to demonstrate that they can maintain continued access to their victim's data through submission or corruption of the new key values. Additionally the period during which teams may submit stolen keys is finite (for example within 30 minutes following the steal) in order to reduce the effects of key hoarding (displayed score not representative of actual score) and key sharing (where teams obtain keys by trading with other teams rather than via attacking other teams).

Rather than simply awarding a point per stolen or overwritten key, the scoring system treats keys as commodities (such as diamonds). The following factors are taken into account when deriving a team's overall score:

1. The more keys that are stolen/overwritten for a particular service, the less each key is worth.

2. Teams earn more points for demonstrating diversity of attack across a given service. In other words, teams can score points for attacking the weakest defender, but they can earn far more points by demonstrating that they can attack across all other teams as well. 3. The longer a team's attacks go unnoticed, the longer that a team remains the sole possessor of an 0-day, the more points a team can accrue for a given service (effectively cornering the market on that commodity)

Teams are awarded points as follows:

1. For a given service up to 1800 points are available for distribution to the teams. 900 points for reading keys from their 9 opponents and 900 points for overwriting keys of their 9 opponents.

2. For a given attacker, a given victim V, and a given service S, the attacker's partial score for the stealing keys from the service is their percentage (0-100) of all keys stolen from V via service S.

3. For a given service S, an attacker's score for service S is the sum of the their partial scores (across all of the other teams) for that service.

4. A team's overall raw score is the sum of its scores across all services in the game.

5. A team's raw score is then multiplied by a measure of the availability of the team's services for the duration of the game. Note that availability does not imply the service is unexploitable, so the team may not in fact be defending the service.

One example of a partial score awards a team 100 points if they are the only team to steal keys for service S from victim V, even if the attacker steals only one key. Thus this is a very valuable key. In another example team 1 may have stolen 400 keys, team 2 300 keys, team 3 200 keys, and team 4 100 keys from service S on victim V. In this second case, the teams are awarded 40, 30, 20, and 10 points respectively. In this case, individual keys are worth less because keys for this service are common.

Item 5 above is meant to ensure that a team does not simply shut down all of its services in order to achieve a perfect defense (and make a boring game for everyone else).

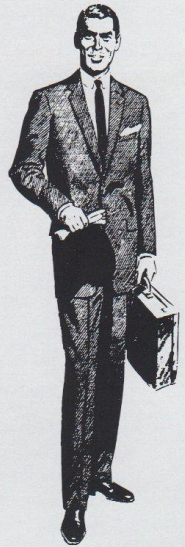
An interesting effect that may be observed under this scoring system is that a team's score may actually decrease from time to time. For example, the first team to submit a key for a service/victim will have the one and only key submitted and therefore a partial score of 100 (percent) for that service. If a second team submits a key for the same service/victim each team's partial score will now be 50 points and the first team will see a decrease in their score owing to the fact that their 0-day is no longer as valuable as it once was. On the other hand if the first team manages to capture 99 keys before the second team submits their first key, the first team will see their score drop almost imperceptibly from 100 to 99 while the second team's score will be only 1. This situation reflects the first team's early entry into the market for these keys and their near monopoly on these keys.

Those familiar with the "breakthrough" system of past CTFs, may note that there is no mention of breakthroughs in the description above. We feel that this scoring system rewards 0-day when 0-day is used effectively to build one's hoard of keys ahead of any other team developing their own version of the same exploit. Further this system allows teams to delay the use of their 0-day in order to keep the number of keys in play to a minimum with the associated risk that another team will beat them to the punch. Thus, in addition to testing a team's offensive and defensive skills, this scoring system attempts to make teams consider the strategy of how, when, and where to make use of their 0-day. Additionally it places increased emphasis on keeping exploits stealthy.

In the CTF room each team is assigned a unique color which is reflected by their team banner, tablecloth and on the scoring displays. The contest allows each team to have at most eight players at the table at any time (though some teams likely have additional resources beyond what is visible at the table). Teams are allowed to bring in whatever tools they prefer.

Stop by the CTF room and talk to a DDTEK representative for more details on the scoring system and displays you will see during the contest.

~ur CTF cr3w



Handout

DEFCON CTF

BINJITSU III

Presented by DDTek

GAME SCORING

Scoring a CTF is a challenging proposition. Ideally a scoring system will reward offensive as well as defensive excellence. This year CTF scoring continues with the same approach of years past to measure what is happening in the game.

Services constitute the heart of the CTF game. Each team must attack and defend identically configured servers, each running some number of custom services. The idea is to analyze the custom services for vulnerabilities and to develop both an attack and a defense strategy for each service.

By exploiting a service an attacker gains access to privileged information which is generally referred to as a key, a flag, or a token. Keys may be readable (steal information), writable (corrupt information), or both. Teams demonstrate that they have stolen information by turning stolen keys into a key submission server. Teams demonstrate that they can deface a service by overwriting keys with a replacement key unique to the attacker. For both of these activities, teams are awarded points.

In order to keep things interesting, keys are periodically updated by the contest organizers, allowing teams to demonstrate that maintain continued access to their victim's data through submission or corruption of the new key values. Additionally the period during which teams may submit stolen keys is finite (for example within 30 minutes following the steal) in order to reduce the effects of key hoarding (displayed score not representative of actual score) and key sharing.

Rather than simply awarding a point per stolen or overwritten key, the scoring system this year will treat keys as commodities (such as diamonds). The following factors are taken into account when deriving a team's overall score:

1. The more keys that are stolen/overwritten for a particular service, the less each key is worth.
2. Teams earn more points for demonstrating diversity of attack across a given service. In other words, teams can score points for attacking the weakest defender, but they can earn far more points by demonstrating that they can attack the stronger teams as well.
3. The longer a team's attacks go unnoticed, the longer that a team remains the sole possessor of an 0-day, the more points a team can accrue for a given service.

Teams are awarded points as follows:

1. For a given service 900 points are available to each team.
2. For a given attacker, a given victim V, and a given service S, the attacker's partial score for the service is their percentage (0-100) of all keys stolen from V via service S.
3. For a given service S, an attacker's score for service S is the sum of the their partial scores (across all of the other teams) for that service.
4. A team's overall raw score is the sum of its scores across all services in the game.
5. A team's raw score is then multiplied by a measure of the availability of the team's services for the duration of the game. Note that availability does not imply the service is unexploitable, so the team may not in fact be defending the service.

One example of a partial score awards a team 100 points if they are the only team to steal keys for service S from victim V, even if the attacker steals only one key. Thus this is a very valuable key. In another example team 1 may have stolen 400 keys, team 2 300 keys, team 3 200 keys, and team 4 100 keys from service S on victim V. In this second case, the teams are awarded 40, 30, 20, and 10 points respectively. In this case, individual keys are worth less because keys for this service are common.

Item 5 above is meant to ensure that a team does not simply shut down all of its services in order to achieve a perfect defense.

An interesting effect that may be observed under this scoring system is that a team's score may actually decrease from time to time. For example, the first team to submit a key for a service/victim will have the one and only key submitted and therefore a partial score of 100 (percent) for that service. If a second team submits a key for the same service/victim each team's partial score will now be 50 points and the first team will see a decrease in their score owing to the fact that their 0-day is no longer as valuable as it once was. On the other hand if the first team manages to capture 99 keys before the second team submits their first key, the first team will see their score drop almost imperceptibly from 100 to 99 while the second team's score will be only 1. This situation reflects the first team's near monopoly on the given key type.

Those familiar with the "breakthrough" system of past CTFs, may note that there is no mention of breakthroughs in the description above. We feel that this scoring system rewards 0-day when 0-day is used effectively to build one's hoard of keys ahead of any other team developing their own version of the same exploit. Further this system allows teams to delay the use of their 0-day in order to keep the number of keys in play to a minimum with the associated risk that another team will beat them to the punch. Thus, in addition to testing a team's offensive and defensive skills, this scoring system attempts to make teams consider the strategy of how, when, and where to make use of their 0-day.

Stop by the CTF room and talk to a DDTEK representative for more details on the scoring system and displays you will see during the contest.

DEFCON CTF