Capture The Flag

An Introduction

Image © http://www.flickr.com/photos/janramroth/2264184078/

Me

- Jordan Wiens

jordan@psifertex.com
@psifertex

- Day: Work for The Man
- Night: Hack for The Fun

Outline

- What's CTF?
- Why CTF?
- Playing CTF?
- Running CTF?

What's CTF?

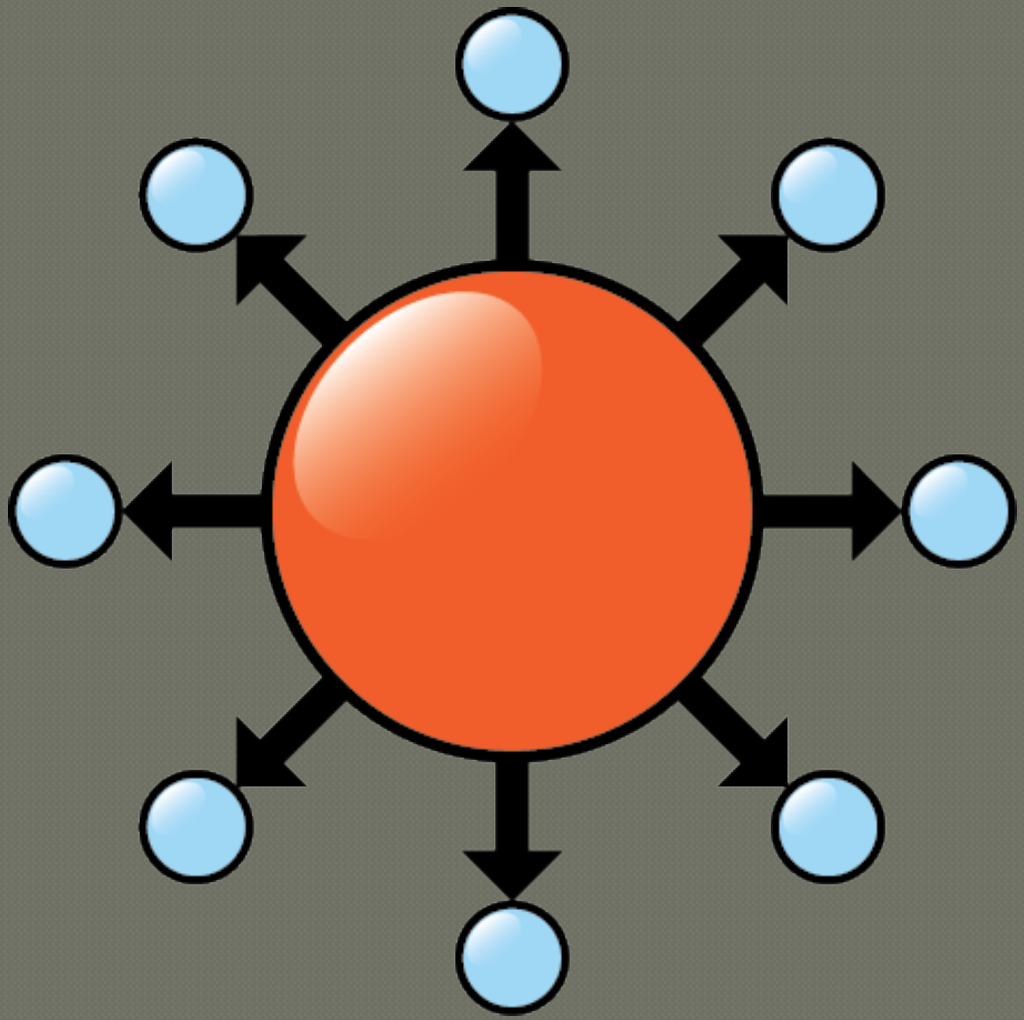
Capture the _ _ _ _

Jargon File

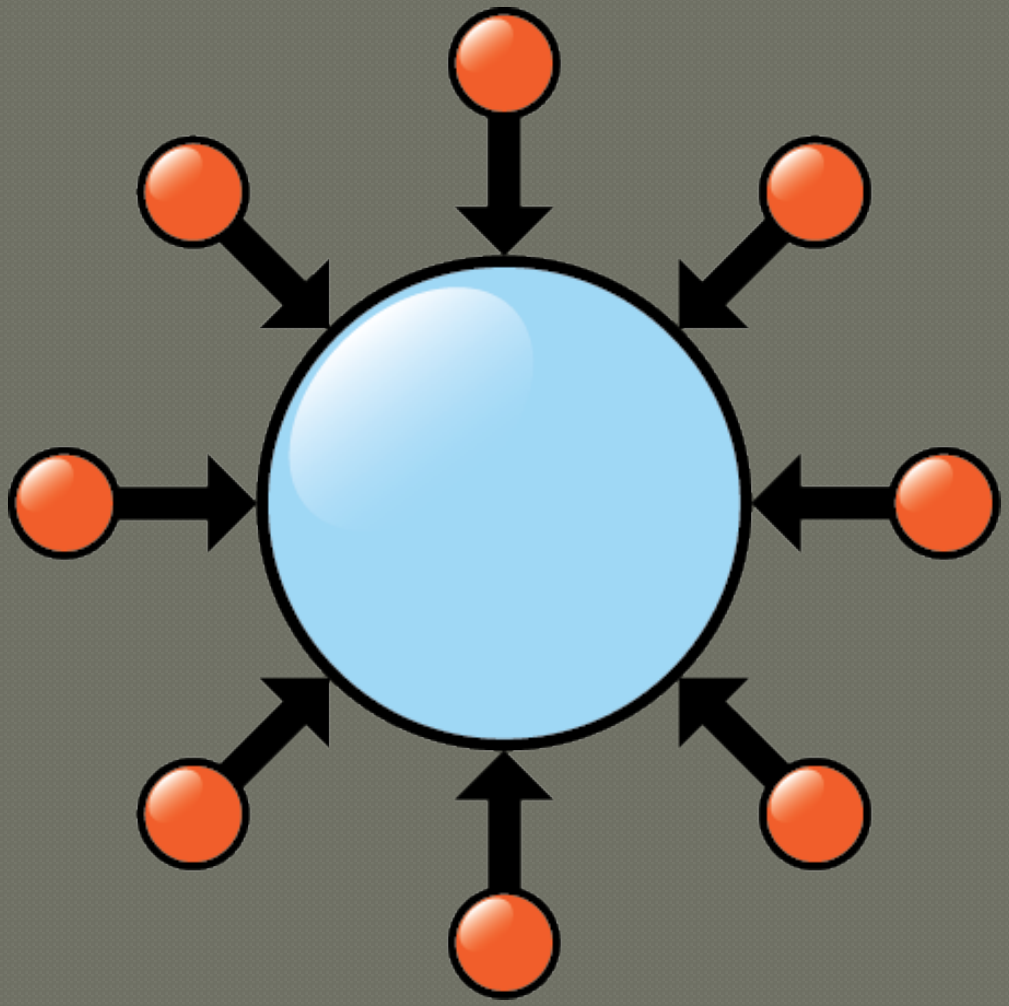
flag
key
SLA
service
binary
quals
prequals

Hacker Games

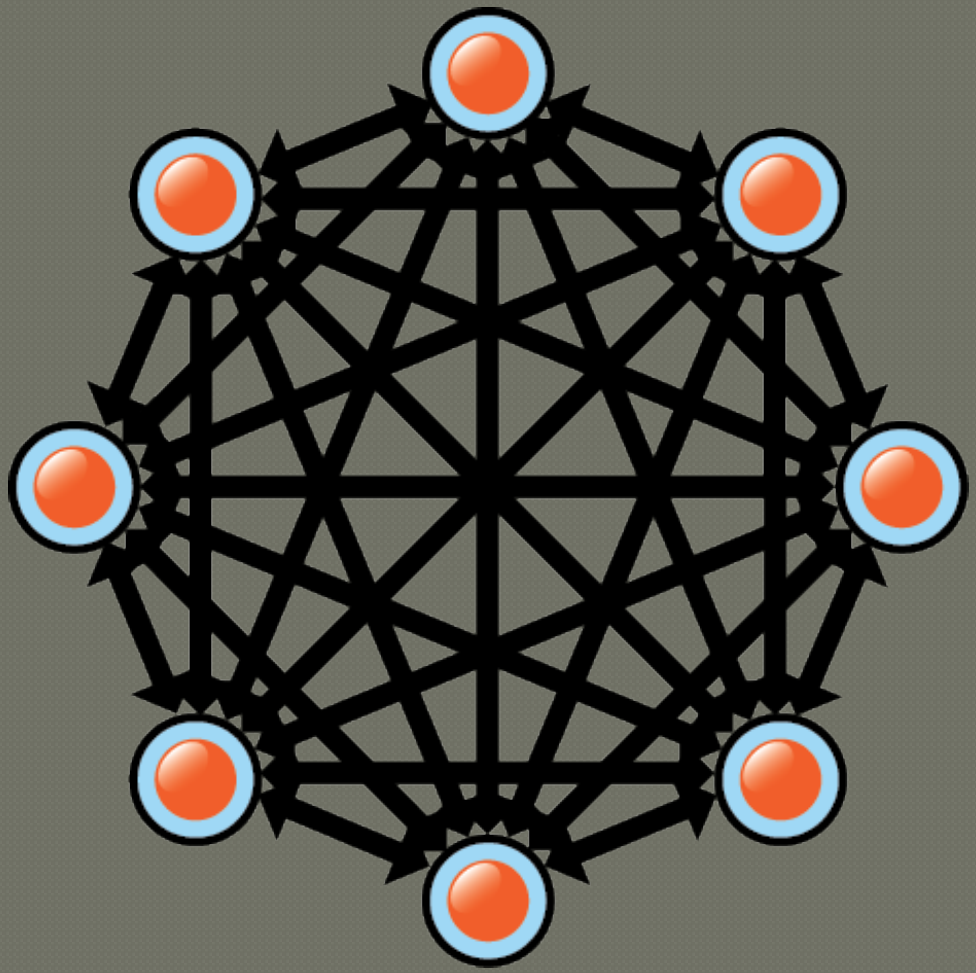
BLUE TEAM



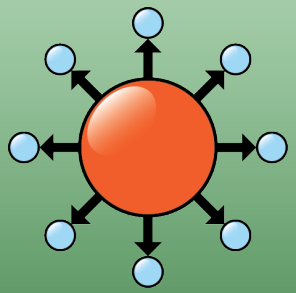
RED TEAM



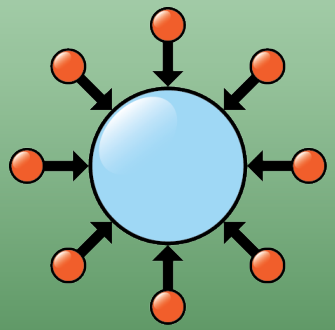
FULL SPECTRUM



CTFs

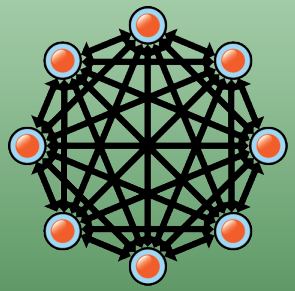


Collegiate Cyber Defense Competition (CCDC)
Cyber Defense Exercise (CDX)



DEF CON Quals
Ghost in the Shellcode
PlaidCTF
CSAW

Kommand && Kontroll
RuCTF Quals
Nuit du Hack Quals
Hack.lu

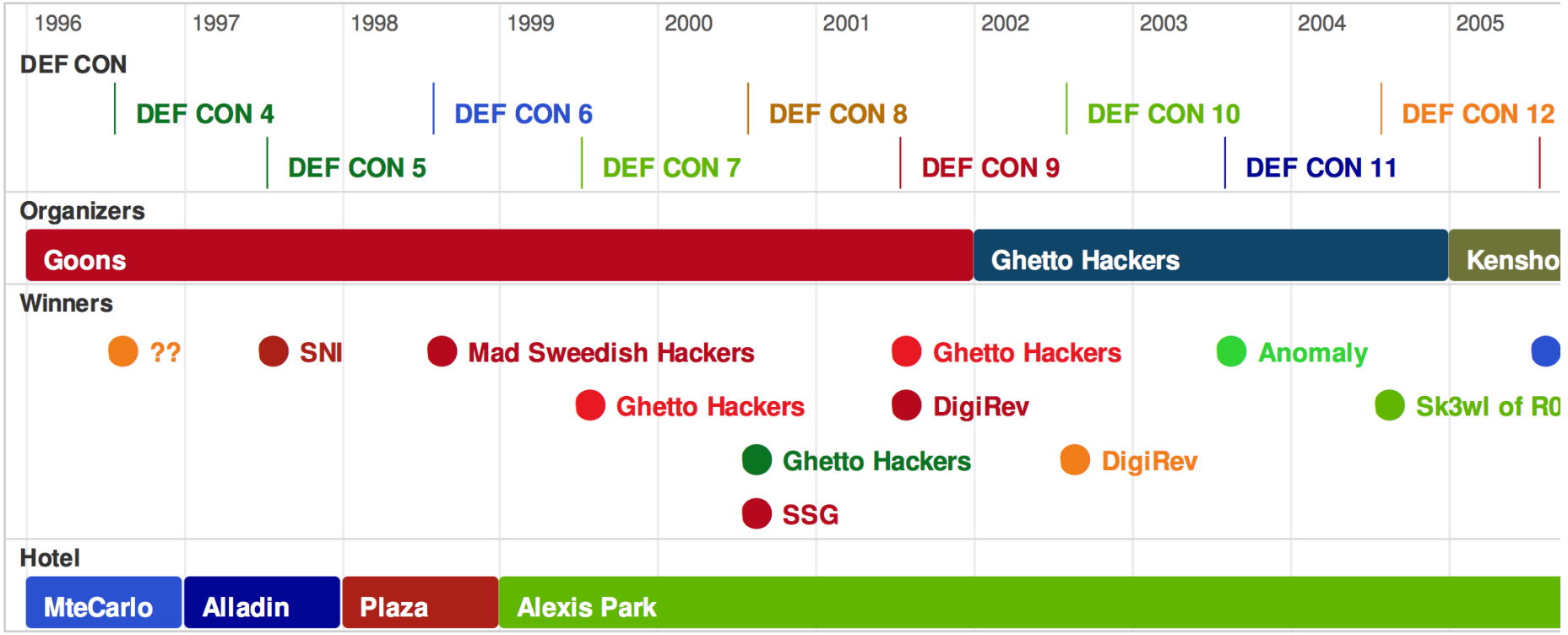


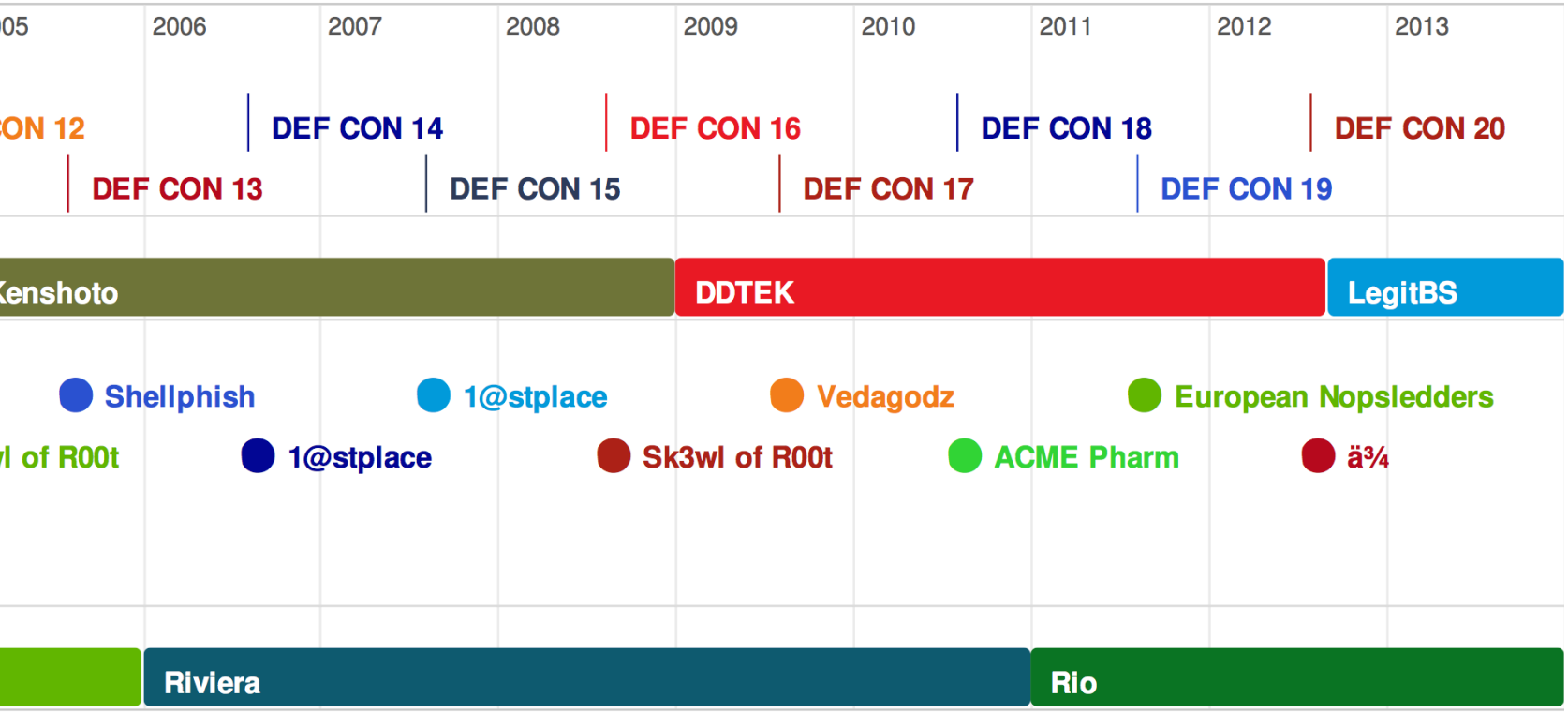
DEF CON Finals
CODEGATE YUT
RuCTF Finals

Nuit du Hack Finals
rwthCTF
iCTF

DEF CON CTF History

- http://preceden.com/timelines/62839


1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
DEF CON
DEF CON 4
DEF CON 5
DEF CON 6
DEF CON 7
DEF CON 8
DEF CON 9
DEF CON 10
DEF CON 11
DEF CON 12
Organizers
Goons
Ghetto Hackers
Kensho
Winners
??
SNI
Mad Sweedish Hackers
Ghetto Hackers
Ghetto Hackers
DigiRev
Ghetto Hackers
DigiRev
SSG
Anomaly
Sk3wl of R0
Hotel
MteCarlo
Alladin
Plaza
Alexis Park


005
2006
2007
2008
2009
2010
2011
2012
2013
CON 12
DEF CON 13
DEF CON 14
DEF CON 15
DEF CON 16
DEF CON 17
DEF CON 18
DEF CON 19
DEF CON 20
Kenshoto
DDTEK
LegitBS
Shellphish
1@stplace
Vedagodz
European Nopsledders
l of R00t
1@stplace
Sk3wl of R00t
ACME Pharm
ä¾
Riviera
Rio

“Jeopardy” (Defcon Quals)

Why CTF?

Jobs

Skillz

$$

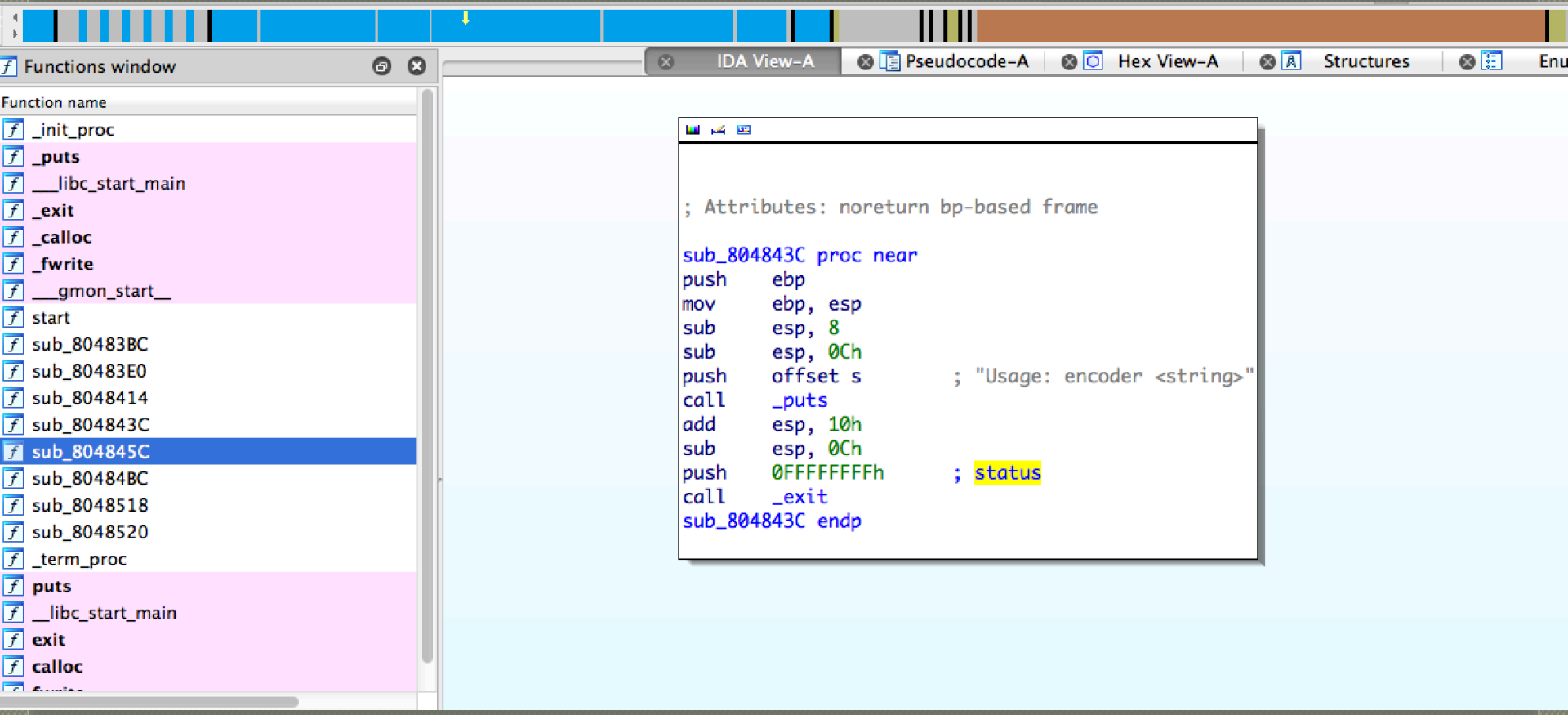
Cred

Sold for $3550.01 at auction

Image © http://www.greatestcollectibles.com/wp-content/uploads/2012/09/page-15.jpg

Fun!

2006 Quals – Reversing 400



2006 Quals – Reversing 400

```
1  void __cdecl sub_8049688(int a1)
2  {
3    size_t v1; // kr04_4@1
4    int v2; // [sp+20h] [bp-18h]@1
5    char v3; // [sp+24h] [bp-14h]@1
6    signed int i; // [sp+28h] [bp-10h]@1
7    void *ptr; // [sp+2Ch] [bp-Ch]@1
8
9    v2 = *(_DWORD *)(a1 + 4);
10   v3 = 0;
11   v1 = strlen(*(const char **)(a1 + 4)) + 1;
12   ptr = calloc(1u, v1 - 1 + 2);
13   for ( i = 0; i < (signed int)(v1 - 1); ++i )
14   {
15     *((_BYTE *)ptr + i) = 8 * *(_BYTE *)(v2 + i);
16     *((_BYTE *)ptr + i) |= v3;
17     if ( (unsigned int)(i % 8) <= 7 )
18       JUMPOUT(__CS__, dword_8048584[i % 8]);
19     v3 = *(_BYTE *)(v2 + i) >> 5;
20   }
21   *((_BYTE *)ptr + i) = v3;
22   fwrite(ptr, v1, 1u, stdout);
23   exit(0);
24 }
```

2006 Quals – Reversing 400

```
$ hexdump key.enc
0000000 f9ef 0942 1aa3 f743 8b8c 22bb c22a 14a3
0000010 0003
```

2006 Quals – Reversing 400

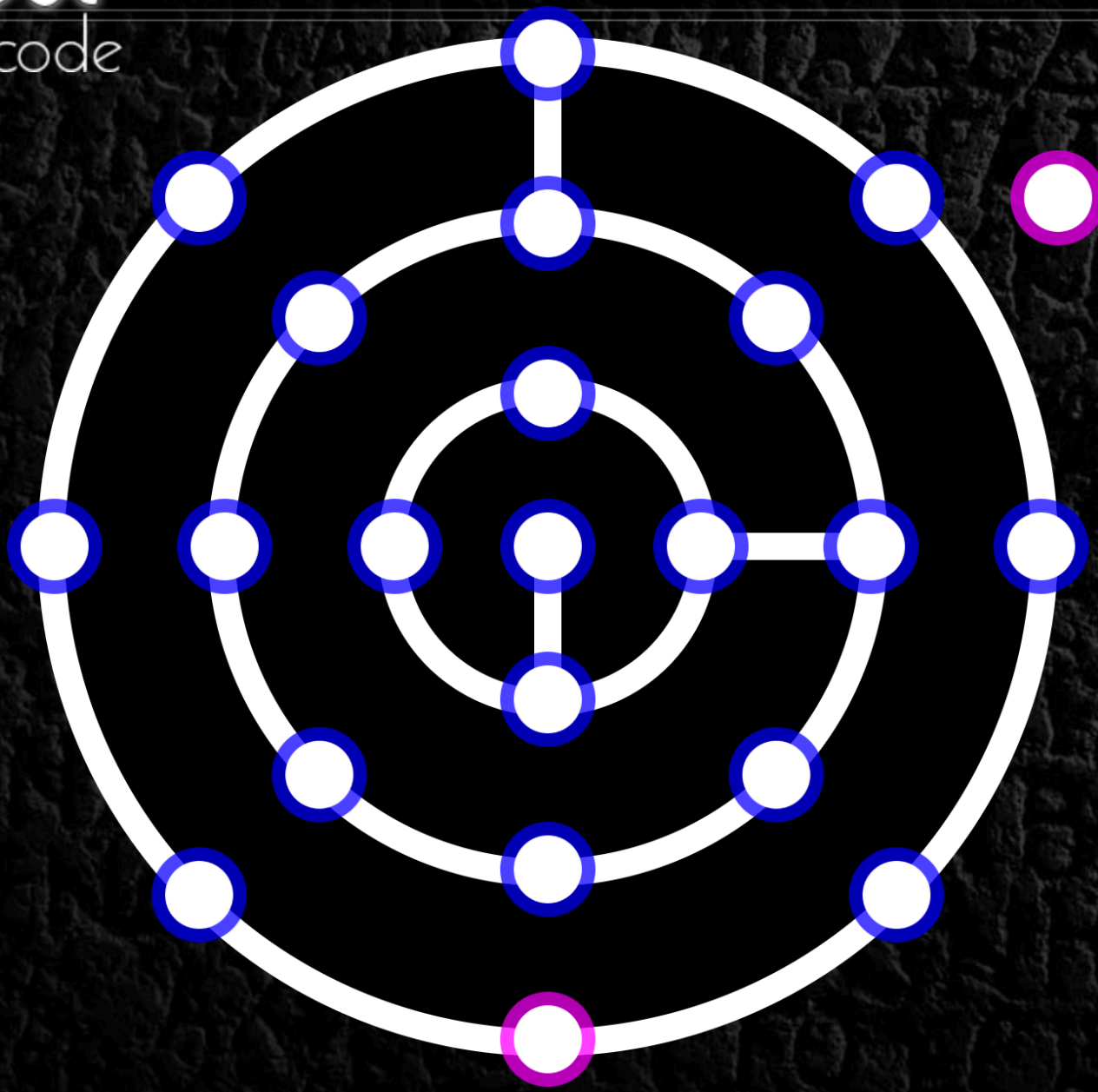
```
#!/bin/bash
for c1 in {a..z}; do
    for c2 in {a..z}; do
        echo -e "$c1$c2\t"`./encoder \
"$c1$c2"|hexdump|head -1`
    done
done
```

ghost in the shellcode

Top 10

#	Team Name	Score
1	PPP ‡	4550
2	More Smoked Leet Chicken	2750
3	Dragon Sector	2550
4	TheSamurai ‡	2500
5	pwnies	2450
6	TracerTea	2400
7	0x8f	2051
8	European Nopsled Team	2000
9	GoN	1950
10	Eindbazen	1950

‡ is at ShmooCon.



What the hell is keming?

1. **Run “file”**

```
$ file 35e25782a7b3b88409e58756e63c40c2.bin
35e25782a7b3b88409e58756e63c40c2.bin: XZ compressed data
```

What the hell is keming?

1. Run “file”
2. **Read spec (RFC-1952)**

> “A gzip file consists of a series of ‘members’ (compressed data sets). The format of each member is specified in the following section. The members simply appear one after another in the file, with no additional information before, between, or after them.”

What the hell is keming?

1. Run “file”
2. Read spec (RFC-1952)
3. **Extract / re-arrange**

```
Exercise for the reader. (python, binwalk, shell script)
```

What the hell is keming?

1. **Run “file”**
2. Read spec (RFC-1952)
3. **Extract / re-arrange**
4. GOTO 1

```
$ file output
output: POSIX tar archive (GNU)
$ tar –xvf output
keming/
keming/index.html
keming/pronoun.woff
keming/preposition.woff
keming/adjective.woff
keming/interjection.woff
```

What the hell is keming?

1. Run “file”
2. **Read spec (http://w3.org/TR/WOFF)**
3. Extract / re-arrange
4. GOTO 1

```
Exercise for the reader.
```

Playing

Skills…

- x86/MIPS/ARM/PPC/ Atmel
- Reverse Engineering
- Binary Exploitation
- File System Forensics
- File Format Forensics
- Cryptography
- Web App Sec
- Hacker Trivia
- Emulation/Virtualization
- Custom compression
- Programming (scripting and the real deal)
- PHP "Phun"
- Binary Protection Mechanisms
- Formal Methods
- Network Protocol Analysis
- Shellcode Tricks
- Number Systems
- Bizarre Encodings

The one true secret to success:

TRYING

Resources

- Calendars
  - http://captf.com/calendar
  - http://ctf.forgottensec.com/wiki
  - http://ctftime.org/ctfs/

Resources

- Archives
  - http://captf.com/
  - http://shell-storm.org/repo/CTF/
  - http://ctftime.org/event/list/past/

Resources

- Practices
  - http://captf.com/practice-ctf/
  - http://www.wechall.net/
  - http://ctf.forgottensec.com/wiki

Resources

- Videos
  - Hacker Joe (http://youtu.be/6e4kJB4cthA)
  - Psifertex(http://youtu.be/okPWY0FeUoU)
  - Chris Eagle (http://vimeo.com/29689138)
  - Arpaia (http://vimeo.com/30141771)
  - ShmooCon (http://youtu.be/c9Rc6DjYJr8)

Running

http://schlockmercenary.com/

The Many Maxims of a Maximally Effective CTF

http://captf.com/maxims.html

Maxims

1. We hack for fun, not for frustration.
2. The scoring mechanism should always be the easiest challenge.
3. Solutions might be a surprise, but recognizing when you have one shouldn't be.
4. When the next step requires a leap of faith, be sure to include a bridge.
5. An homage honors, but duplication doesn't.

Maxims

6. Learners always win even when winners don't learn.
7. Your point estimates are exactly that until calibrated.
8. Never rely on the survival of a vulnerable server.
9. Competitors are more clever than you, they also have more time.
10. Learning starts where prior knowledge ends.

Questions?

THANKS:
family, friends, CTF mates past and present, HackUCF, b-sides organizers!

SLIDES:
http://captf.com/intro

Bonus content!

Other things

- Team Organization
- Culture of the game
  - Good / bad
- Strategy
  - Sleep
  - Play the organizers
  - “scrum”