

Maximum CTF

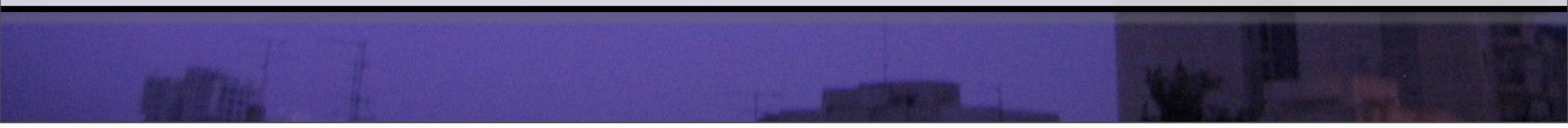
Get the most from capture the flag

Friday, July 31, 2009

capture the flag
(Two Toy Soldiers)
http://www.flickr.com/photos/janramroth/2264184078/
http://creativecommons.org/licenses/by/2.0/deed.en
jot.punkt

lightning round

"Hack the _____"



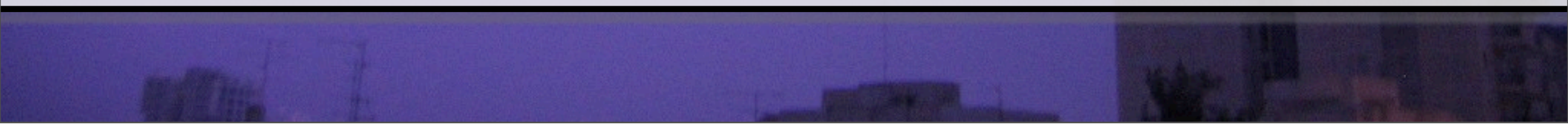
Friday, July 31, 2009

Trivia 100 from 2006 qualifier. And yeah this should be insanely obvious. The funny part though is that the next year, the 100 point question was

The thunder and lightning
RonAlmog
http://www.flickr.com/photos/ronalmog/2053473900/
http://creativecommons.org/licenses/by/2.0/deed.en

lightning round

"Hack the planet"



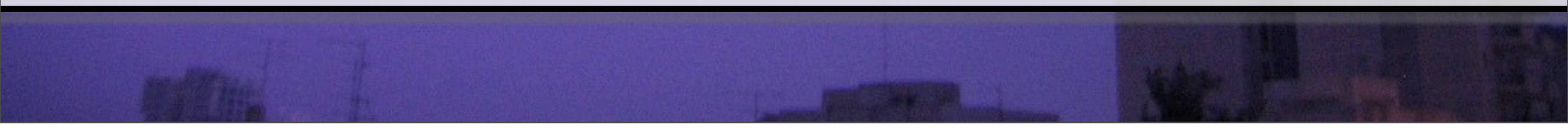
Friday, July 31, 2009

Trivia 100 from 2006 qualifier. And yeah this should be insanely obvious. The funny part though is that the next year, the 100 point question was

The thunder and lightning
RonAlmog
http://www.flickr.com/photos/ronalmog/2053473900/
http://creativecommons.org/licenses/by/2.0/deed.en

lightning round

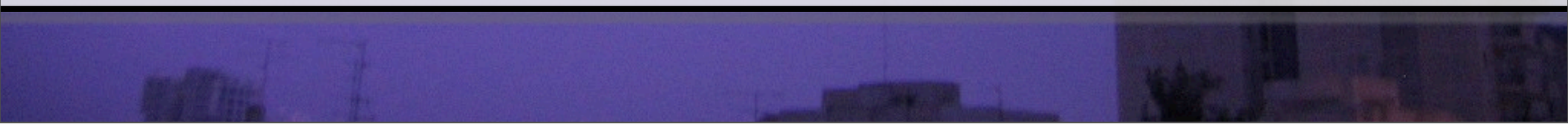
"_____ the planet"



And likewise, the year after that:

lightning round

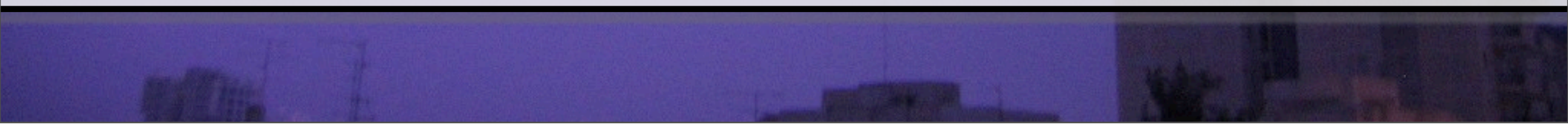
"Hack the planet"



And likewise, the year after that:

lightning round

"Hack ___ planet"

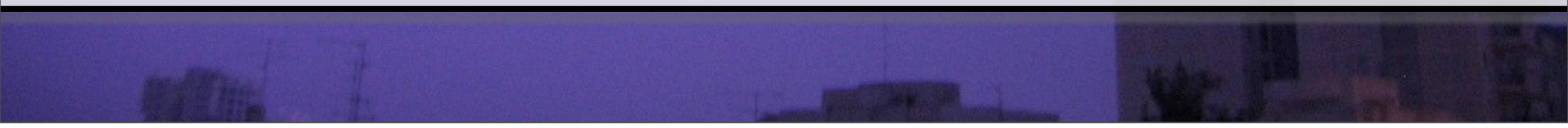


Friday, July 31, 2009

A fair amount of CTF has been inside jokes and homages to years past. If you plan on participating, check out and practice on previous years answers and writeups as they will make your life much easier.

lightning round

"Hack the planet"



Friday, July 31, 2009

A fair amount of CTF has been inside jokes and homages to years past. If you plan on participating, check out and practice on previous years answers and writeups as they will make your life much easier.



psifertex

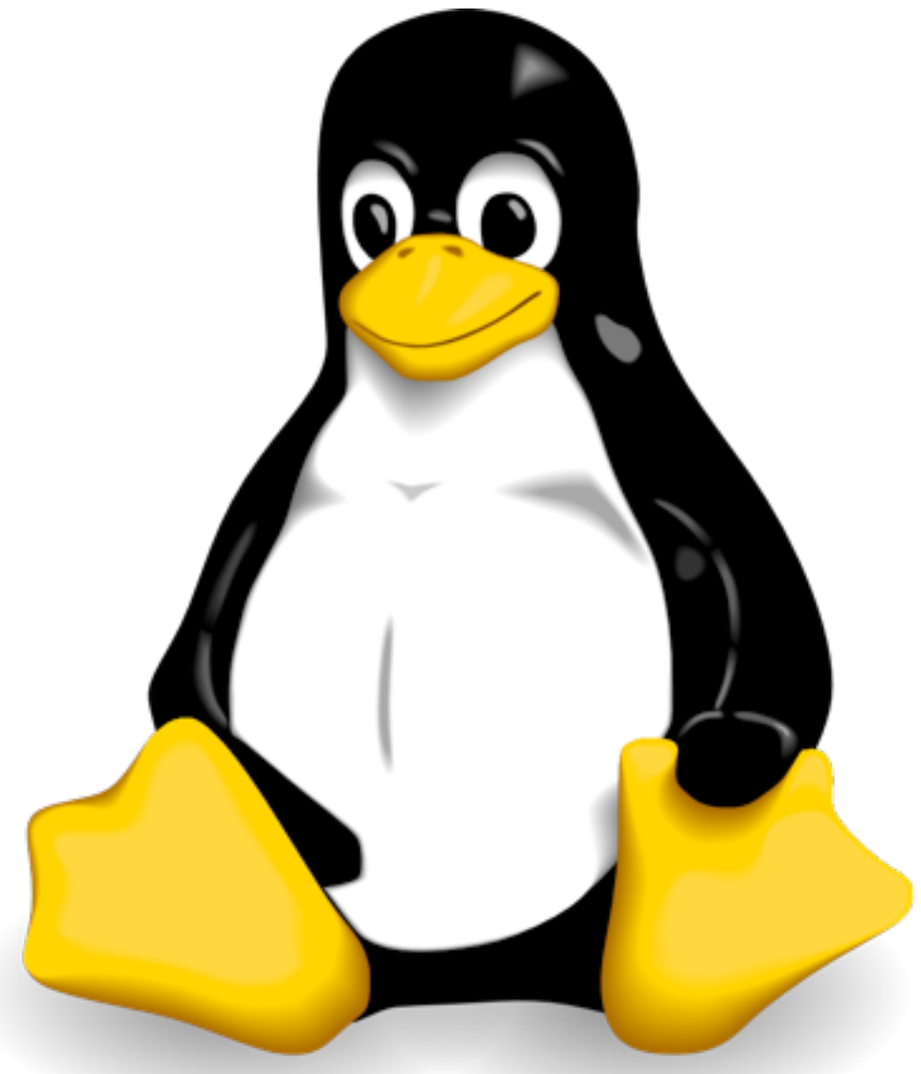
Friday, July 31, 2009

Hi, I’m psifertex, this is my bio. The parts that matter, anyway.

Photo copyright my dad -- used with permission, licensed the same as the presentation..



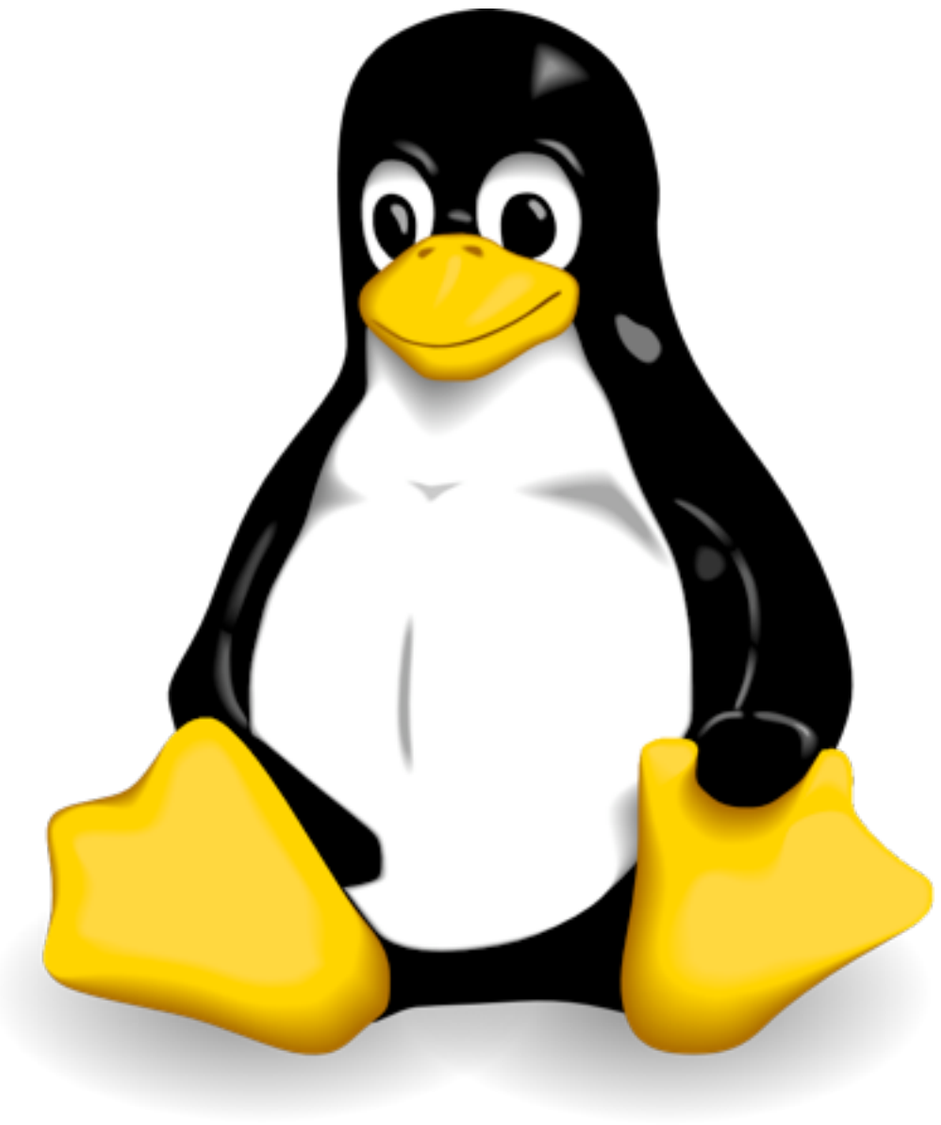
TM



Friday, July 31, 2009

It’s probably not surprising that I prefer Linux over Windows, though the older and lazier I get, the more Steve Jobs takes my money.

TM



Friday, July 31, 2009

It’s probably not surprising that I prefer Linux over Windows, though the older and lazier I get, the more Steve Jobs takes my money.



Friday, July 31, 2009

It’s probably not surprising that I prefer Linux over Windows, though the older and lazier I get, the more Steve Jobs takes my money.





Friday, July 31, 2009

For editor, my choice is Vim over Emacs



Friday, July 31, 2009

For editor, my choice is Vim over Emacs

over

under

Also important, I prefer over, over under.

TP
Dano
http://www.flickr.com/photos/mukluk/249464276/
http://creativecommons.org/licenses/by/2.0/deed.en

over



under

Friday, July 31, 2009

Also important, I prefer over, over under.

TP
Dano
http://www.flickr.com/photos/mukluk/249464276/
http://creativecommons.org/licenses/by/2.0/deed.en





Friday, July 31, 2009

Python over Ruby



Friday, July 31, 2009

Python over Ruby





Friday, July 31, 2009

Pepsi over Coke, but bawls over both.

Probably more relevant to this talk though, I’m a member of



Friday, July 31, 2009

Pepsi over Coke, but bawls over both.

Probably more relevant to this talk though, I'm a member of

1@stplace

this capture the flag team.

It’s pronounced “last place”, and we’ve been very lucky to have won the Defcon CTF a couple times.



Friday, July 31, 2009

this capture the flag team.

It's pronounced "last place", and we've been very lucky to have won the Defcon CTF a couple times.



1@stplace

Friday, July 31, 2009

Here's a decent shot of everybody on the team except for two members.

I'm partially visible here in the back, and the rest of the team is:

Plato -- likely the only lawyer who ever has or ever will win CTF
@tlas -- team captain and individual CTF winner in 2005
Mezzendo -- dual network sniffer in addition to defending
Shiruken -- sysadmin extraordinaire (and always the life of IRC during quals whether we're competing or not)
Fury -- or his twin, you gotta watch out for twins, defender
Doc Brown -- reverser/exploiter par excellence and maintainer of nopsr.us
Wrffr -- a secret weapon who gets very little recognition outside the group, but is an incredible reverser/exploiter with a long CTF history.

I mentioned Apu was missing in this photo, he has the distinction of acting not only as a network monitor and defender, but also as our physical security coordinator, utilizing his ex-marine skills.

Jrod, also missing from this picture, is another strong contributer to the exploitation side of things, and a frequent Defcon and BlackHat presenter/trainer.

As for me, I must not be too good at anything yet since I've bounced from defense to offense and everything in between over the years. Fortunately, they keep letting me hang around anyway.

photo used with permission from Dave Bullock, eecue.com



1@stplace

Friday, July 31, 2009

Here's a decent shot of everybody on the team except for two members.

I'm partially visible here in the back, and the rest of the team is:

Plato -- likely the only lawyer who ever has or ever will win CTF
@tlas -- team captain and individual CTF winner in 2005
Mezzendo -- dual network sniffer in addition to defending
Shiruken -- sysadmin extraordinaire (and always the life of IRC during quals whether we're competing or not)
Fury -- or his twin, you gotta watch out for twins, defender
Doc Brown -- reverser/exploiter par excellence and maintainer of nopsr.us
Wrffr -- a secret weapon who gets very little recognition outside the group, but is an incredible reverser/exploiter with a long CTF history.

I mentioned Apu was missing in this photo, he has the distinction of acting not only as a network monitor and defender, but also as our physical security coordinator, utilizing his ex-marine skills.

Jrod, also missing from this picture, is another strong contributer to the exploitation side of things, and a frequent Defcon and BlackHat presenter/trainer.

As for me, I must not be too good at anything yet since I've bounced from defense to offense and everything in between over the years. Fortunately, they keep letting me hang around anyway.

photo used with permission from Dave Bullock, eecue.com



1@stplace

Friday, July 31, 2009

Here's a decent shot of everybody on the team except for two members.

I'm partially visible here in the back, and the rest of the team is:

Plato -- likely the only lawyer who ever has or ever will win CTF
@tlas -- team captain and individual CTF winner in 2005
Mezzendo -- dual network sniffer in addition to defending
Shiruken -- sysadmin extraordinaire (and always the life of IRC during quals whether we're competing or not)
Fury -- or his twin, you gotta watch out for twins, defender
Doc Brown -- reverser/exploiter par excellence and maintainer of nopsr.us
Wrffr -- a secret weapon who gets very little recognition outside the group, but is an incredible reverser/exploiter with a long CTF history.

I mentioned Apu was missing in this photo, he has the distinction of acting not only as a network monitor and defender, but also as our physical security coordinator, utilizing his ex-marine skills.

Jrod, also missing from this picture, is another strong contributer to the exploitation side of things, and a frequent Defcon and BlackHat presenter/trainer.

As for me, I must not be too good at anything yet since I've bounced from defense to offense and everything in between over the years. Fortunately, they keep letting me hang around anyway.

photo used with permission from Dave Bullock, eecue.com



1@stplace

Friday, July 31, 2009

Here's a decent shot of everybody on the team except for two members.

I'm partially visible here in the back, and the rest of the team is:

Plato -- likely the only lawyer who ever has or ever will win CTF
@tlas -- team captain and individual CTF winner in 2005
Mezzendo -- dual network sniffer in addition to defending
Shiruken -- sysadmin extraordinaire (and always the life of IRC during quals whether we're competing or not)
Fury -- or his twin, you gotta watch out for twins, defender
Doc Brown -- reverser/exploiter par excellence and maintainer of nopsr.us
Wrffr -- a secret weapon who gets very little recognition outside the group, but is an incredible reverser/exploiter with a long CTF history.

I mentioned Apu was missing in this photo, he has the distinction of acting not only as a network monitor and defender, but also as our physical security coordinator, utilizing his ex-marine skills.

Jrod, also missing from this picture, is another strong contributer to the exploitation side of things, and a frequent Defcon and BlackHat presenter/trainer.

As for me, I must not be too good at anything yet since I've bounced from defense to offense and everything in between over the years. Fortunately, they keep letting me hang around anyway.

photo used with permission from Dave Bullock, eecue.com



1@stplace

Friday, July 31, 2009

Here's a decent shot of everybody on the team except for two members.

I'm partially visible here in the back, and the rest of the team is:

Plato -- likely the only lawyer who ever has or ever will win CTF
@tlas -- team captain and individual CTF winner in 2005
Mezzendo -- dual network sniffer in addition to defending
Shiruken -- sysadmin extraordinaire (and always the life of IRC during quals whether we're competing or not)
Fury -- or his twin, you gotta watch out for twins, defender
Doc Brown -- reverser/exploiter par excellence and maintainer of nopsr.us
Wrffr -- a secret weapon who gets very little recognition outside the group, but is an incredible reverser/exploiter with a long CTF history.

I mentioned Apu was missing in this photo, he has the distinction of acting not only as a network monitor and defender, but also as our physical security coordinator, utilizing his ex-marine skills.

Jrod, also missing from this picture, is another strong contributer to the exploitation side of things, and a frequent Defcon and BlackHat presenter/trainer.

As for me, I must not be too good at anything yet since I've bounced from defense to offense and everything in between over the years. Fortunately, they keep letting me hang around anyway.

photo used with permission from Dave Bullock, eecue.com



1@stplace

Friday, July 31, 2009

Here's a decent shot of everybody on the team except for two members.

I'm partially visible here in the back, and the rest of the team is:

Plato -- likely the only lawyer who ever has or ever will win CTF
@tlas -- team captain and individual CTF winner in 2005
Mezzendo -- dual network sniffer in addition to defending
Shiruken -- sysadmin extraordinaire (and always the life of IRC during quals whether we're competing or not)
Fury -- or his twin, you gotta watch out for twins, defender
Doc Brown -- reverser/exploiter par excellence and maintainer of nopsr.us
Wrffr -- a secret weapon who gets very little recognition outside the group, but is an incredible reverser/exploiter with a long CTF history.

I mentioned Apu was missing in this photo, he has the distinction of acting not only as a network monitor and defender, but also as our physical security coordinator, utilizing his ex-marine skills.

Jrod, also missing from this picture, is another strong contributer to the exploitation side of things, and a frequent Defcon and BlackHat presenter/trainer.

As for me, I must not be too good at anything yet since I've bounced from defense to offense and everything in between over the years. Fortunately, they keep letting me hang around anyway.

photo used with permission from Dave Bullock, eecue.com



1@stplace

Friday, July 31, 2009

Here's a decent shot of everybody on the team except for two members.

I'm partially visible here in the back, and the rest of the team is:

Plato -- likely the only lawyer who ever has or ever will win CTF
@tlas -- team captain and individual CTF winner in 2005
Mezzendo -- dual network sniffer in addition to defending
Shiruken -- sysadmin extraordinaire (and always the life of IRC during quals whether we're competing or not)
Fury -- or his twin, you gotta watch out for twins, defender
Doc Brown -- reverser/exploiter par excellence and maintainer of nopsr.us
Wrffr -- a secret weapon who gets very little recognition outside the group, but is an incredible reverser/exploiter with a long CTF history.

I mentioned Apu was missing in this photo, he has the distinction of acting not only as a network monitor and defender, but also as our physical security coordinator, utilizing his ex-marine skills.

Jrod, also missing from this picture, is another strong contributer to the exploitation side of things, and a frequent Defcon and BlackHat presenter/trainer.

As for me, I must not be too good at anything yet since I've bounced from defense to offense and everything in between over the years. Fortunately, they keep letting me hang around anyway.

photo used with permission from Dave Bullock, eecue.com



1@stplace

Friday, July 31, 2009

Here's a decent shot of everybody on the team except for two members.

I'm partially visible here in the back, and the rest of the team is:

Plato -- likely the only lawyer who ever has or ever will win CTF
@tlas -- team captain and individual CTF winner in 2005
Mezzendo -- dual network sniffer in addition to defending
Shiruken -- sysadmin extraordinaire (and always the life of IRC during quals whether we're competing or not)
Fury -- or his twin, you gotta watch out for twins, defender
Doc Brown -- reverser/exploiter par excellence and maintainer of nopsr.us
Wrffr -- a secret weapon who gets very little recognition outside the group, but is an incredible reverser/exploiter with a long CTF history.

I mentioned Apu was missing in this photo, he has the distinction of acting not only as a network monitor and defender, but also as our physical security coordinator, utilizing his ex-marine skills.

Jrod, also missing from this picture, is another strong contributer to the exploitation side of things, and a frequent Defcon and BlackHat presenter/trainer.

As for me, I must not be too good at anything yet since I've bounced from defense to offense and everything in between over the years. Fortunately, they keep letting me hang around anyway.

photo used with permission from Dave Bullock, eecue.com



1@stplace

Friday, July 31, 2009

Here's a decent shot of everybody on the team except for two members.

I'm partially visible here in the back, and the rest of the team is:

Plato -- likely the only lawyer who ever has or ever will win CTF
@tlas -- team captain and individual CTF winner in 2005
Mezzendo -- dual network sniffer in addition to defending
Shiruken -- sysadmin extraordinaire (and always the life of IRC during quals whether we're competing or not)
Fury -- or his twin, you gotta watch out for twins, defender
Doc Brown -- reverser/exploiter par excellence and maintainer of nopsr.us
Wrffr -- a secret weapon who gets very little recognition outside the group, but is an incredible reverser/exploiter with a long CTF history.

I mentioned Apu was missing in this photo, he has the distinction of acting not only as a network monitor and defender, but also as our physical security coordinator, utilizing his ex-marine skills.

Jrod, also missing from this picture, is another strong contributer to the exploitation side of things, and a frequent Defcon and BlackHat presenter/trainer.

As for me, I must not be too good at anything yet since I've bounced from defense to offense and everything in between over the years. Fortunately, they keep letting me hang around anyway.

photo used with permission from Dave Bullock, eecue.com

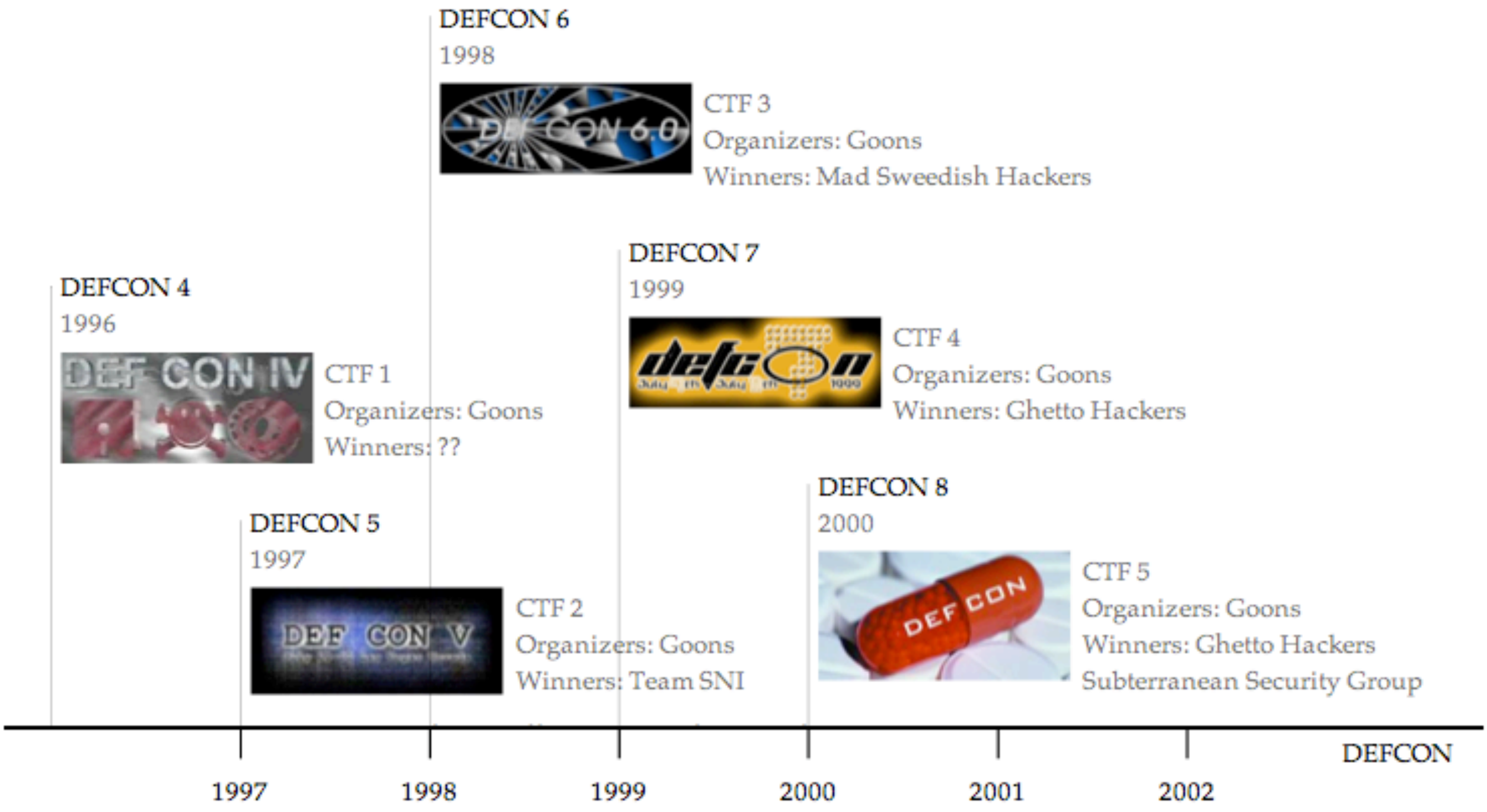


CTF

Friday, July 31, 2009

Capture the flag is the ultimate hacking game (legal one, anyway). It requires reverse engineering and exploiting dozens of never-before-seen network-services all while defending, monitoring, patching, and generally going crazy over the course of two and a half days.

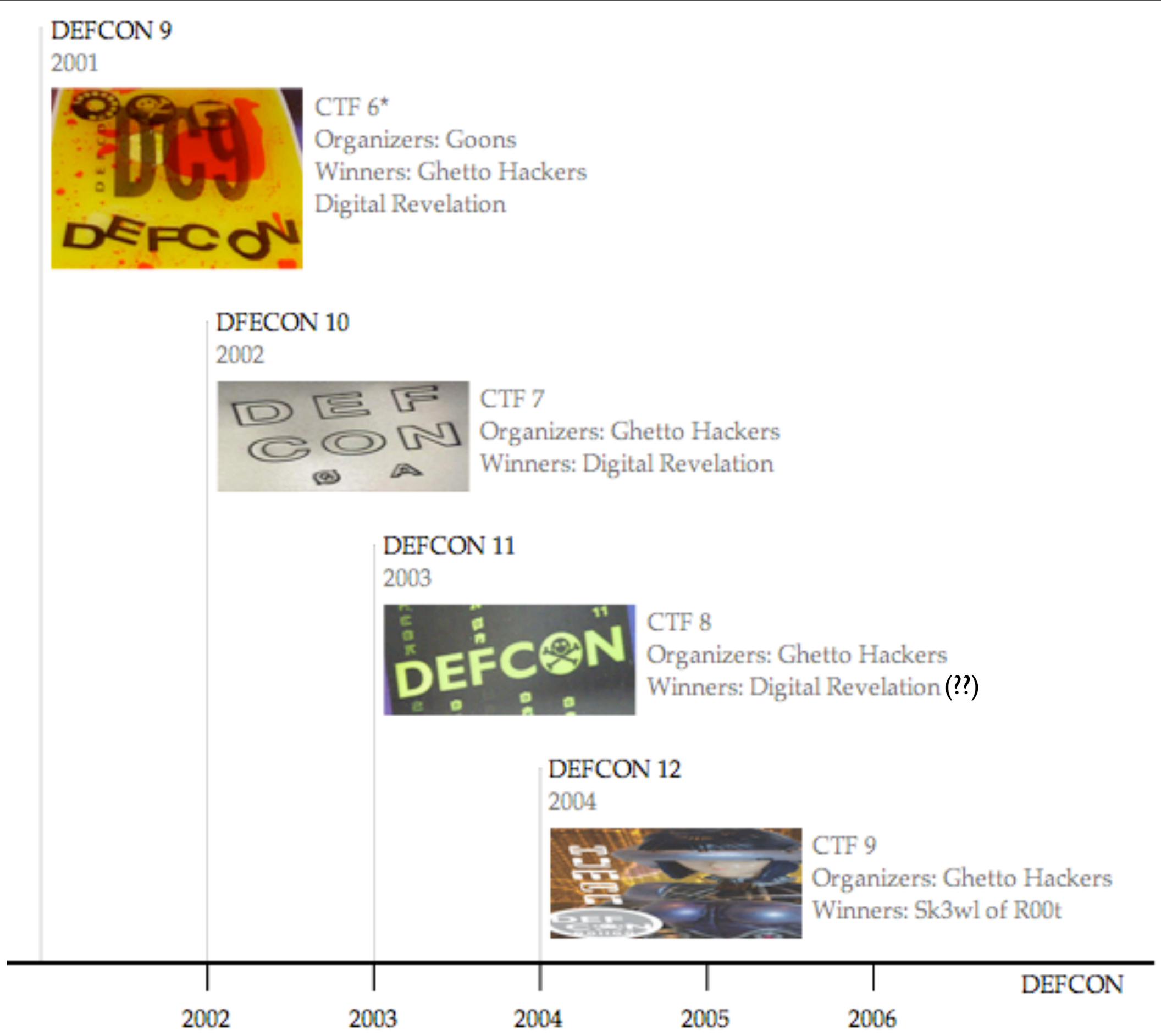
254 pirate flag
leadfoot
http://www.flickr.com/photos/mom320/2332456130/
http://creativecommons.org/licenses/by/2.0/deed.en



Friday, July 31, 2009

Hopefully you saw the previous presentation, with a bit more detail on the history of CTF. If not, grab the video when it gets put online.

There were essentially three different groups who ran CTF. From DEFCON 4 to DEFCON 8 BOFH (Defcon Goons) ran it, with a couple of different styles, but it was mostly free-for-all mayhem.



Friday, July 31, 2009

Then from DEFCON 9 to DEFCON 12, the Ghetto Hackers took over and eventually revamped the basic structure to the one we know today where a select group of teams maintain their own identical (at the start) virtual machine and attack everyone else's. Additionally, they added the concept of the now-common qualifier round in 2004.

DEFCON 14
2006



CTF 11
Organizers: Kenshoto
Winners: 1@stplace

DEFCON 15
2007



CTF 12
Organizers: Kenshoto
Winners: 1@stplace

DEFCON 13
2005



CTF 10
Organizers: Kenshoto
Winners: Shellphish

DEFCON 16
2008



CTF 13
Organizers: Kenshoto
Winners: sk3wl of r00t

2006 2007 2008 2009 DEFCON

Friday, July 31, 2009

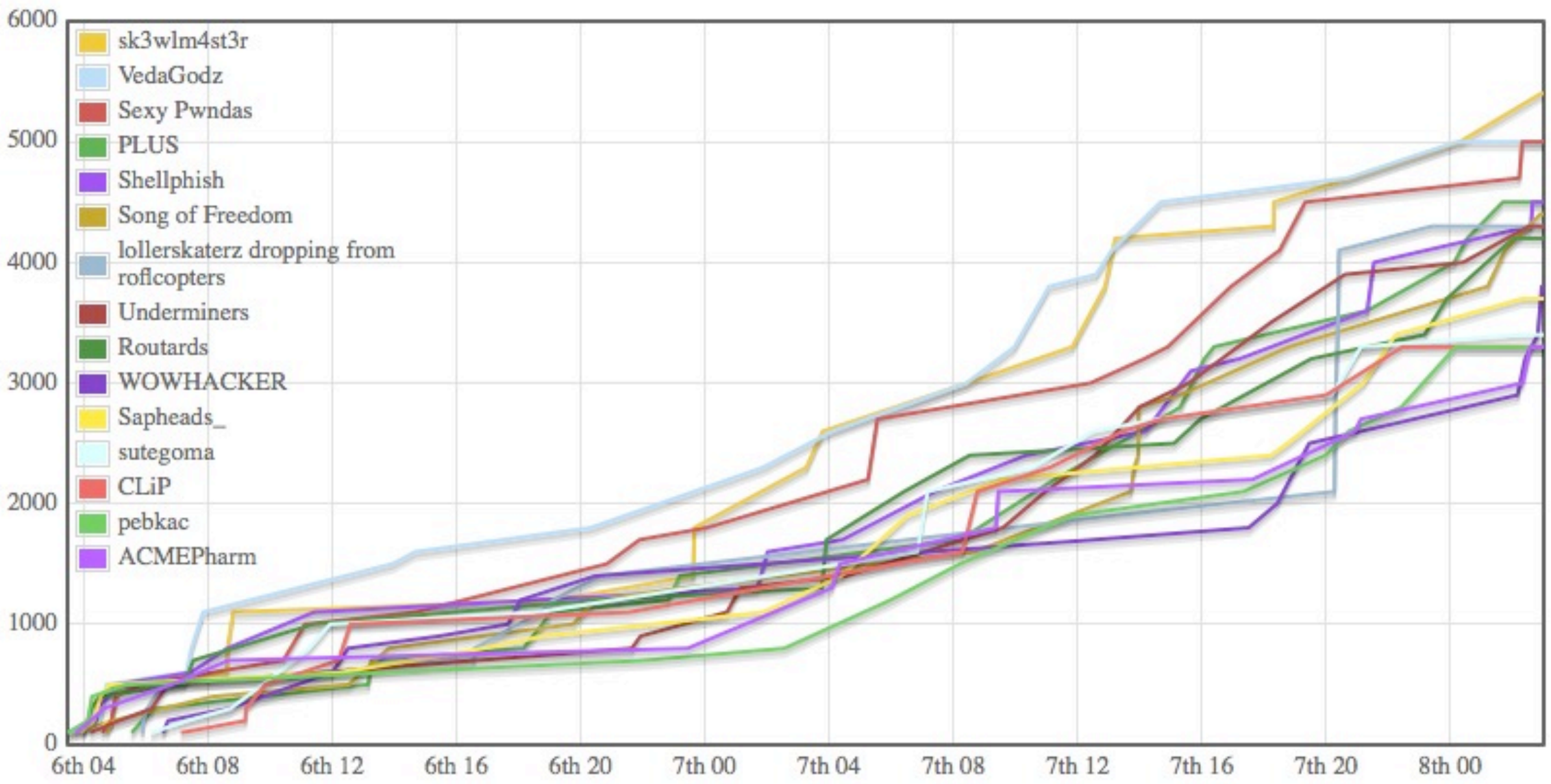
Finally, the illustrious Kenshoto assumed control from DEFCON 13 to DEFCON 16, refining and tweaking the game design with a splash of game theoretics and a bunch of very slick architectures. Not only did they have some impressive challenges, but they provided many other bits of fun as the annual tossing of the cookies (fortune cookies with custom hidden messages being tossed from their balcony).





Friday, July 31, 2009

And finally, this year we have DDTEK (Diutinus Defense Technologies Corp), whose qualifier round was indeed very similar to the Kenshoto qualifiers of years past and most likely a very similar CTF is underway as I speak.



Friday, July 31, 2009

This year and the previous five CTFs have included a qualifier round. Because the event itself is so popular, the qualifier round ensures that the playing field is narrowed before the event even starts.

Here's the final score board for DDTEK's 2009 qualifying round that ran for 48 straight hours starting June 5 at 2300 UTC.

知彼知己，

百戰不殆

-Sun Tzu

Friday, July 31, 2009

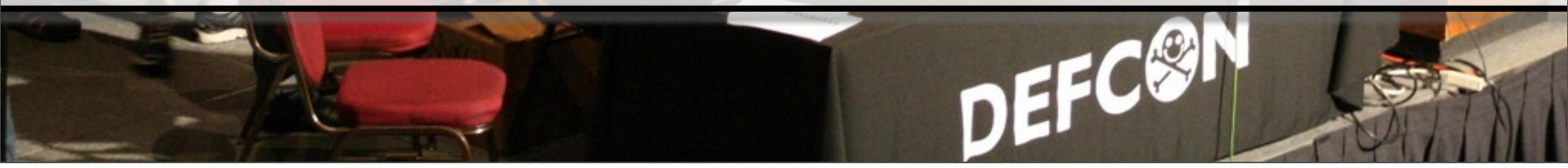
What's a good security presentation without a Sun Tzu quote?

I'm sure it says something very wise about winning.

If you want to compete at next year's CTF, ten of your most likely opponents are competing in the other room right now, so let's take a look at those teams now, presented in the order they qualified in.



sk3wl of r00t



Friday, July 31, 2009

Winners of the 2004 and 2008 Defcon CTF, sk3wl of r00t is primarily composed of students from the Naval Postgraduate School (http://www.nps.edu/). The team captains are Jon Boss (BossMan) who keeps things running smoothly and frees up the other captain, Chris Eagle (sk3wlm4st3r) who is an outright binary ninja and pirate rolled into one. Incredibly difficult challenges have been created solely to give him some entertainment.

They dominate early and often in both quals and finals, last year putting up a true beat-down on the rest of the competition when they were able to effectively make use of their large team. That may have been in no small part due to Eagle's Collabreate Tool (http://www.idabook.com/collabreate/), a collaborative plugin to the IDA Disassembler. Which he graciously released as open source... immediately after the competition ended. That was one of Eagle's many great hacks.

CTF Winners
Leduardo
http://www.flickr.com/photos/leduardo/2755245443/

http://creativecommons.org/licenses/by/2.0/deed.en



Friday, July 31, 2009

(aka VedaGodz) Composed of mostly first-timers to the CTF scene, they led for much of the qualifiers, but succumbed to sk3wl's might at the end. Sk3wl was likely being gracious as the previous winners because the previous years CTF winner typically has an automatic entry into the next final. It's very gentlemanly of them then to not take control of the board and influence the qualifiers, so no one knows exactly how much they were holding back.

Another big question mark will be how TeamA performs during the final. Being good at quals is often a very different thing from dealing with the environment and different challenges during the big dance.

I do have some friends on this team, so while 1@stplace is on a hiatus this year, you'll likely see me hanging out with these guys.

Domo photo used with permission, Team Awesome.



Friday, July 31, 2009

AKA Pandas with Gambas
AKA Osu, Tatakae, Sexy Pandas!
AKA, woobi woobi pandas
AKA, Sexy Pwndas
AKA, Ailuropoda Melanoleucas

http://sexy.pandas.es/blog/
These Spaniards have often been cursed with a great start and a poor finish during finals, but they definitely don't lack for solid reversing and exploitation skills. They've made strong showings in a number of other CTFs and are always a threat, especially if they can keep the tempo they usually start with. Their strong finish in this years quals is a good indicator of the quality of their team.

Team photo from Hanzo and used with Permission.



PLUS@postech

Friday, July 31, 2009

http://www.plus.or.kr/zbxe/
http://postech.ac.kr/

One of the many ROK (Republic of Korea) teams that have been storming the top 10 in recent years, PLUS is back this year after a one year hiatus. Plus is primarily made up of undergraduates from Postech (the Pohang University of Science and Technology).

ShellPhish

HEX on the beach

Menu

- Home
- Code

People



sicko



ViRus



weaver



beetal



irish



nullptr



void



balzaroth



zanardi

Friday, July 31, 2009

http://shellphish.net

Formed from a group out of the University of California Santa Barbara, and led by Giovanni Vigna, Shellphish is a permanant fixture of many CTFs (Defcon and otherwise). Additionally, the group runs the iCTF, the International Capture the Flag primarily for academic groups world-wide (http://ictf.cs.ucsb.edu/). Shellphish is a staple of the CTF scene, winning in 2005, and participating in many other finals as well.

Screenshot from http://shellphish.net/

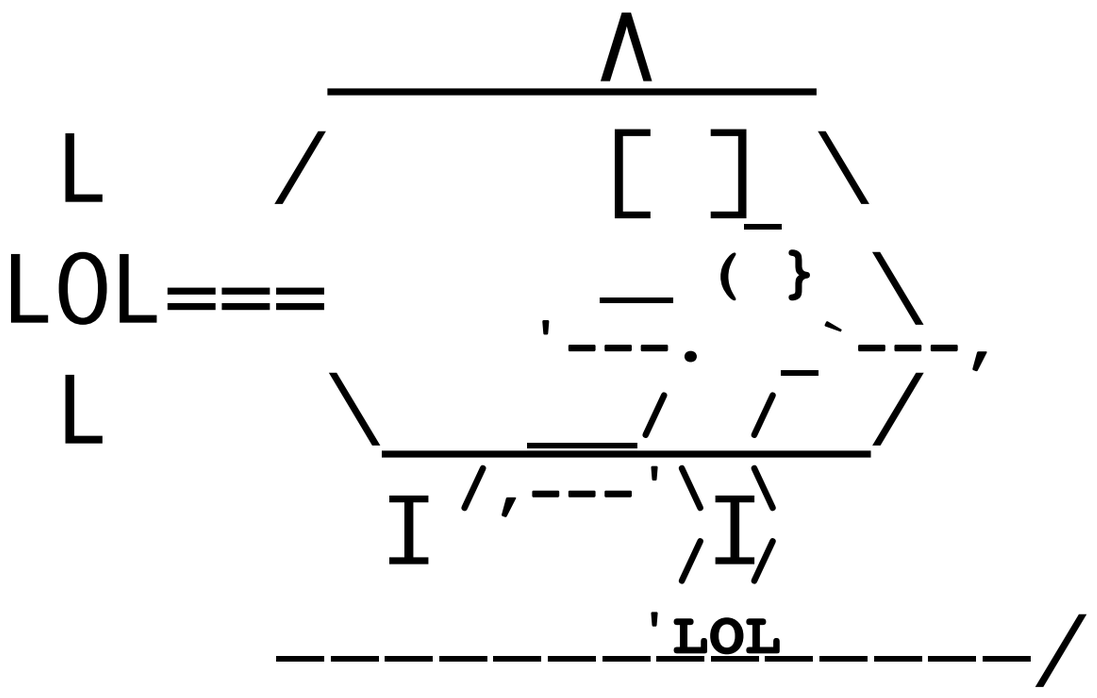
song of freedom

송오브프리덤

Friday, July 31, 2009

Song of Freedom
송오브프리덤
Yet another among the Korean Power houses

ROFL:ROFL:LOL:ROFL:ROFL



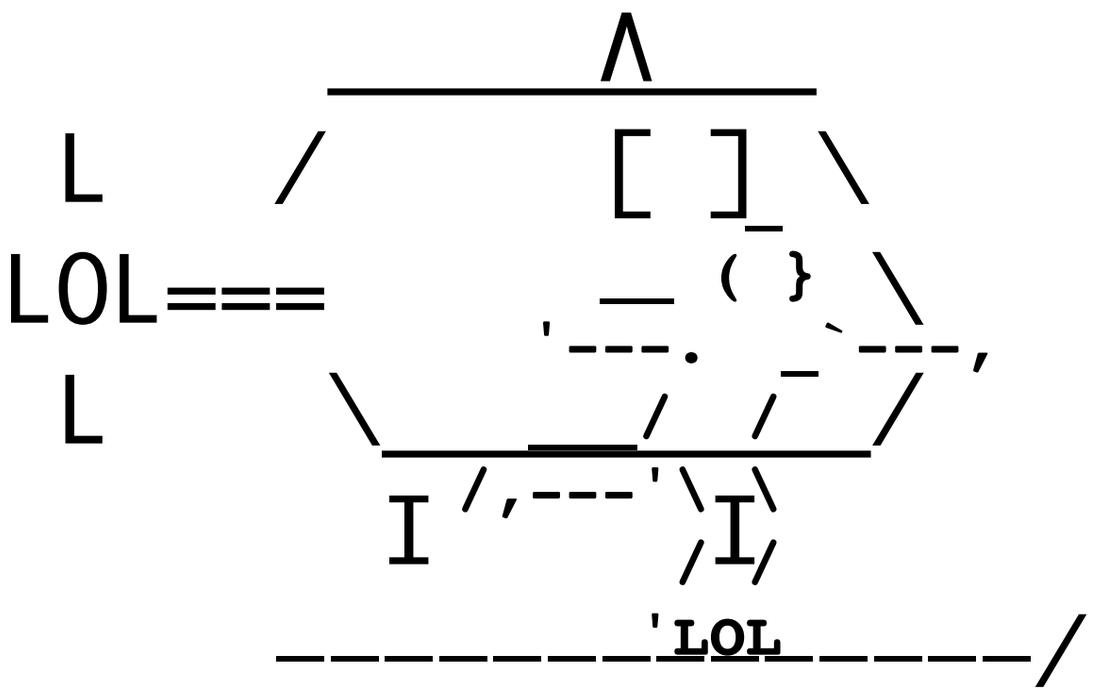
lollerskaterz dropping from roflcopters

Friday, July 31, 2009

Lollerskaterz is a diverse collection of international friends that has changed membership over the years, from the small 3-person team that stormed the 2007 Quals, to the current larger team (they expected to bring five here currently, and might add a few others while they're here)

While most teams have their compositions fixed, there are occasionally smaller teams interested in picking up some ronin, so if you have a strong interest in playing but aren't on a qualified team, be patient, polite and ask around, and you might be able to join a team with open seats, but be warned that for many teams, it's unlikely if you don't know someone on it.

ROFL:ROFL:LOL:ROFL:ROFL



lollerskaterz dropping from roflcopters

Friday, July 31, 2009

Lollerskaterz is a diverse collection of international friends that has changed membership over the years, from the small 3-person team that stormed the 2007 Quals, to the current larger team (they expected to bring five here currently, and might add a few others while they're here)

While most teams have their compositions fixed, there are occasionally smaller teams interested in picking up some ronin, so if you have a strong interest in playing but aren't on a qualified team, be patient, polite and ask around, and you might be able to join a team with open seats, but be warned that for many teams, it's unlikely if you don't know someone on it.

routards

hanzo
fetard
vicelard
grincheux
rebel
prof
joyeux
poueteur
dormeur
sorcier

Friday, July 31, 2009

Started two years ago with a core group from France, the Routards have expanded their membership in recent years to include members from Switzerland and Belgium as well. Now it's easiest to simply describe them as a French-speaking team.

Mostly made up of InfoSec professionals doing CTF for fun, the team is led by hanzo, and I'll spare you my mangled pronunciation of the rest of the team member's handles!

One interesting bit of trivia; the routards are only one of three teams to have made it to all three of the last three years worth of finals along with the sexy pandas and sk3wl of r00t).



WOWHACKER

와우해커

Friday, July 31, 2009

http://wowhacker.org/

Another of the Korean teams -- I dunno what's in the water over there, but I hear that Starcraft is considered a real sport there. Any place where that's the case I imagine you'd have to get a bunch of awesome hackers.



graz
hex
jvprat
KOrUPt
mongii
Philkill
Razed
seoman
singi
t1g3r
whats

Friday, July 31, 2009

http://www.sapheads.org/ (t1g3r)
http://korupt.co.uk/ (korupt)

Sapheads are another recent entry to the lineup of usual suspects, and are a meta-team composed of three other smaller groups that came together:
AIAFNFASG (AIAFNFASG Is Another Fucking Name For A Security Group)
WiseguyS@Hackerschool
Binary Devils

They're also behind an incredibly cool comic-book style writeup for one of this years challenges, definitely make sure to check that out.

lightning round

\xEB\xFE is to x86

as

_____ is to PPC

Friday, July 31, 2009

If you saw this one during previous CTF quals, let someone else answer it...

\xEB\xFE is an infinite loop, a jmp back to itself.

PPC has no jumps, but an unconditional branch is
\x48\x00\x00\x00

lightning round

\xEB\xFE is to x86 as \x48\x00\x00\x00 is to PPC

Friday, July 31, 2009

If you saw this one during previous CTF quals, let someone else answer it...

\xEB\xFE is an infinite loop, a jmp back to itself.

PPC has no jumps, but an unconditional branch is
\x48\x00\x00\x00



mechanics

Friday, July 31, 2009

As far as the game mechanics go, here's the rundown:

First, the difference between Quals and the Finals, which I've mentioned briefly, but haven't explained yet.

They are two very different events. While there is definitely some skill overlap, it doesn't always transfer.

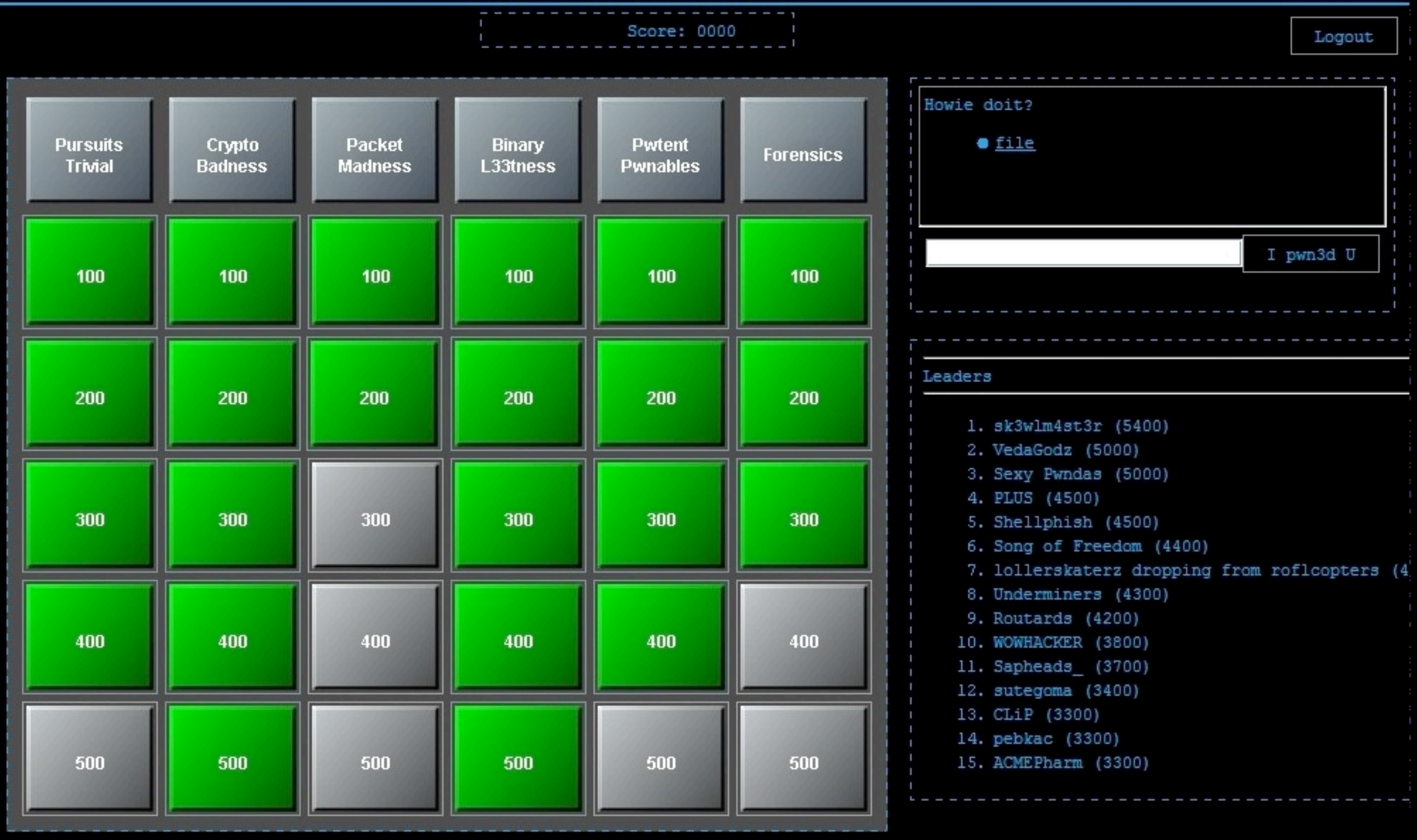
Quals are more linear, they're non-stop, and there's a lot more variety to the type of problems. There's no defense, and a wider variety of esoteric topics and skills are usually covered.

Mechanics at Charles Street Shops, 1956
Seattle Municipal Archives
http://www.flickr.com/photos/seattlemunicipalarchives/3576509006/
http://creativecommons.org/licenses/by/2.0/deed.en

	Qualifier	CTF
Style	Q&A with attack of shared services	Defend from and attack against other teams
Timing	48 hours straight (Fri-Sun before DC)	10 + 10 + 6 hours (Fri-Sun at Defcon)
Location	Remote	Riviera // Las Vegas (aka, next-door)
Teams	200+	8-10
Spoils	Entry to CTF	Black badge, leather jacket, dates, prestige

Friday, July 31, 2009

Here's a better breakdown -- of course, the exact details change each time. This is the first year with 10 teams participating in the finals, and the exact hours per day in the finals fluxuates somewhat. Some years it's even been non-stop at defcon itself too



Friday, July 31, 2009

Here's a screenshot of this year's qualifier board. DDTEK definitely up'ed the ante, providing a whopping 30 challenges in the categories pursuits trivial, crypto badness, packet madness, binary l33tness, pwtent pwnables, and forensics.

While there's a lot of overlap between the qualifier game and the final game, they're really fairly different. It's possible to be very good at one, but not as good at the other.



big show

The top 7 or 9 teams (along with the previous year's winning team that gets an automatic berth) from the qualifiers make it to the main event.

At the finals, every team gets their own identical server, and they must not only defend their server, but attack all of their opponents as well. While there are some general preparation that can occur, most of the time it's all on-the-fly patching and exploitation against custom, never-before-seen services.

A general framework for automated exploitation and key-submission is nice, but don't put too much work into it in case you get a curve-ball like DTMF key submission process like the one from 2006.

Be prepared to possibly serve as the network infrastructure between your VM and the rest of the world. This allows you to do some neat tricks with inline firewalls and packet filtering, but also allows you to easily shoot yourself in the foot by dropping your server entirely offline.

A score bot is constantly monitoring the services you are running on your server, ensuring that services are up and running. A final tally of all successful services checks divided by the total number of service checks produces an SLA percentage that is multiplied by all other points.

Of course, to actually score points, you need to go out and capture some

Shrine Circus 2006 - 2
D'Arcy Norman
http://www.flickr.com/photos/dnorman/142386154/
http://creativecommons.org/licenses/by/2.0/deed.en



Friday, July 31, 2009

flags.

First, there are lots and lots of flags--they're generated over time so that a team that is able to steal earlier and more often will be able to gather more flags than their opponents.

Second, each flag must be tracked as to who it came from (I shouldn't be able to submit a flag that came from my own server, for example), and there's also flag used to overwrite existing flags in vulnerabilities that have write access to a flag.

Of course, the ability to detect flag overwrites is also one of the most important reasons that jail or zone type of technology is usually used. The score server must be able to monitor an overwritten key, and instantly replace it. Otherwise, when the score server works on a polling interval, only one team will be able to get points during a given time interval. That's a bad thing since it incentivizes teams to blast out their overwrites as fast as possible to ensure their flag is king of the hill. An automated transparent overwrite detection with its own built-in interval during which only one overwrite may be had by each team keeps that from happening.

One interesting twist is that this year the scoring system will be based on a zero-sum game. The available points for any given service will be divided up proportionally amongst the teams who exploit it. It will be interesting to see what impact this has on the games score.

This also does away with one of the other main features of previous Defcon scoring -- breakthrough points. Breakthrough points were awarded for the first team or two to succeed at any given exploit. Harder services earned more breakthrough points.

While there's certainly a fair amount of strategy in producing gameplay optimized toward the scoring system (for example -- if you are in second place, do you throw an exploit against the lead team that you know they haven't landed yet, or do you hold on to it to try to keep



A successful CTF team has a variety of specialized roles. It's not enough to simply be good at binary reverse engineering or exploitation.

Obviously, many of these roles may overlap, and some teams will operate differently, but generally speaking, a successful team will have something similar.

Cinnamon Rolls!
bcmom
http://www.flickr.com/photos/bcmom/66951454/
http://creativecommons.org/licenses/by/2.0/deed.en

leader



Friday, July 31, 2009

The leader holds the team together. This should be the person best able to direct, coordinate, communicate, and make sure everyone is on task and working together. Try not to make this the best technical person in any other skillset if possible -- those folks should be spent doing what they do best, not herding cats.

Herding Cats
DrBacchus
http://www.flickr.com/photos/rbowen/1148435913/
http://creativecommons.org/licenses/by/2.0/deed.en



The NetAdmin not only must maintain the network and configure appropriate firewall rules, but most importantly is responsible for monitoring all network traffic. Using sniffers, IDS or other signature matching systems, a good NetAdmin is crucial. A successful CTF team is one that is able to very quickly recognize, adapt, and re-use exploits or other attacks sent against them. The nose must work closely with both the exploiters and reversers, as well as the sysadmin/defenders to make sure they're abreast of what others are attempting.

Sniffing around
Leonid Mamchenkov's
http://www.flickr.com/photos/mamchenkov/278157281/
http://creativecommons.org/licenses/by/2.0/deed.en

reversing

exploitation

No image on this slide. I decided against an image search for “exploitation”.

The reverser/exploiter roles are often the same person, but not necessarily. Sometimes the person who finds the vulnerability is not the best person to be writing the exploit code. Make sure you maximize your time each doing what you do best.

While all of the roles truly are important to a winning team, if you don’t have people skilled in this area, you don’t stand a chance. There’s simply no way to score points without being good at exploitation. The qualifier rounds ensure that any team that makes it to the finals can pull their weight in exploitation and reversing.



The sysadmin is responsible for keeping your SLA up. Remember, SLA is a multiplier of /all other points/. Never forget that. Never make a change to a service if it will impact your SLA without carefully checking it out. It's better to let your opponents score on you and keep the server up than to take it down and take off a percentage of all your points.

Keep your SLA up at all times, and a good sysadmin is critical to that process.

Time Management for System Administrators
mightyohm
http://www.flickr.com/photos/mightyohm/2942621738/
http://creativecommons.org/licenses/by/2.0/deed.en

defender



Friday, July 31, 2009

The defender is the guy whose job is not only to help the sysadmin in maintaining the server, but actively making life difficult for those intruding on the box. While lots of shenanigans can (and should) be prepared in advance (find ways to cripple libraries, move standard binaries, trojanize certain tools to better monitor attacks who get shells -- all in ways that allow legitimate services to keep running), much of it must be done on the fly. You never know if you'll be getting the same setup as previous years, so putting too much work into work beforehand is risky.

Catch Me
powerbooktrance
http://www.flickr.com/photos/powerbooktrance/276488800/
http://creativecommons.org/licenses/by/2.0/deed.en

gopher



Friday, July 31, 2009

Man does not live on bread alone, and neither do hackers live on caffeine alone. At some point you need some food. Or help carrying things, or watching to make sure no one's peeking on your screens. Having friends to help you with the little tasks makes life much easier!

We Gopher You
Mykl Roventine
http://www.flickr.com/photos/myklroventine/2562860881/
http://creativecommons.org/licenses/by/2.0/deed.en



teamwork

Friday, July 31, 2009

Let me emphasize this again. Teamwork is absolutely crucial.

I don't care how good you are at the individual skills, a team of individual superstars will not win. There are so many things going on and so much depends on being able to effectively communicate and work together in a high-pressure environment.

1@stplace won two years in a row. Neither time were we the sneakinest (ok, maybe we were close). Neither time we were the best at getting the breakthrough exploits, neither time were we the best at defending our server from the attacks of others. However, we were /good/ at all of those things, each person had a role, stuck to it will, and we coordinated extremely well between each functional group.

toy soldiers 2
http://www.flickr.com/photos/janramroth/1302905330/
http://creativecommons.org/licenses/by/2.0/deed.en
jot.punkt



team size

Friday, July 31, 2009

There are advantages and disadvantages to both large and small teams. Most likely, your team size will be determined by your friends, co-workers, affiliations, etc. Still, you might consider limiting yourself if you decide you want to make a small team and have lots of potential candidates.

The danger with a large team is that it will struggle under its own weight. Clearly defining roles and responsibilities, making sure the right groups are communicating with the right other groups, these are big issues. Some people complained last year when sk3wl of r00t won that they only did so because they had so many people. That's an entirely unfair accusation -- having a big team can be a liability if you don't manage it right, and congrats to sk3wl for putting together the right mixture to be able to pull it off and pull it off big last year.

Of course, CTF has so many components that a team with five or less members would have an extremely difficult time being competitive, no matter how good each individual was. There's simply too many binaries, too many tasks. Consider merging with another team to form a larger team if that's your situation, but make sure you carefully delineate tasks and responsibilities if you do so.

Photo copyright me -- same license as the presentation.



Let's talk about one important piece of CTFiquette. Many teams take the competition very seriously. Unless you personally know someone on a team, be very careful about going up and trying to watch their screen, or even sitting behind or to the side of a team. Spying on other teams is a perfectly acceptable strategy (both inside the game room, and elsewhere), so most take their physical security seriously.

High voltage warning sign
NIOSH - Nat Inst for Occupational Safety & Health
http://www.flickr.com/photos/niosh/2492839488/
http://creativecommons.org/licenses/by/2.0/deed.en

lightning round

Implement the following
in one x86 instruction:

```
for (ecx = 0; ecx < 32; ecx++)
{
    if ((1 << ecx) & eax)
    {
        ebx = ecx;
    }
}
```


The original answer required the actual bytes, but I'll assume everyone who can find the answer is capable of running an assembler -- I'll take the mnemonic here.

lightning round

BSR ebx, eax

Also accepted: BSR $eax, $ebx
Or for those showing off (if done in their head): \0x0f\xbd\xd8

Answer: BSR ebx, eax (also accepted: BSR $eax, $ebx)



dirty tricks

Friday, July 31, 2009

Of course, CTF is primarily about hacking, and what isn't hacking without some dirty tricks?

free candy
http://www.flickr.com/photos/endora57/49474343/
http://creativecommons.org/licenses/by-nc/2.0/deed.en
endora57

Photoshopped by me, new image likewise released to the public domain.



security is only as strong as...



Friday, July 31, 2009

Everyone say it with me: “security is only as strong as...” “the weakest link”

What’s usually the weakest link in security... Passwords, of course!

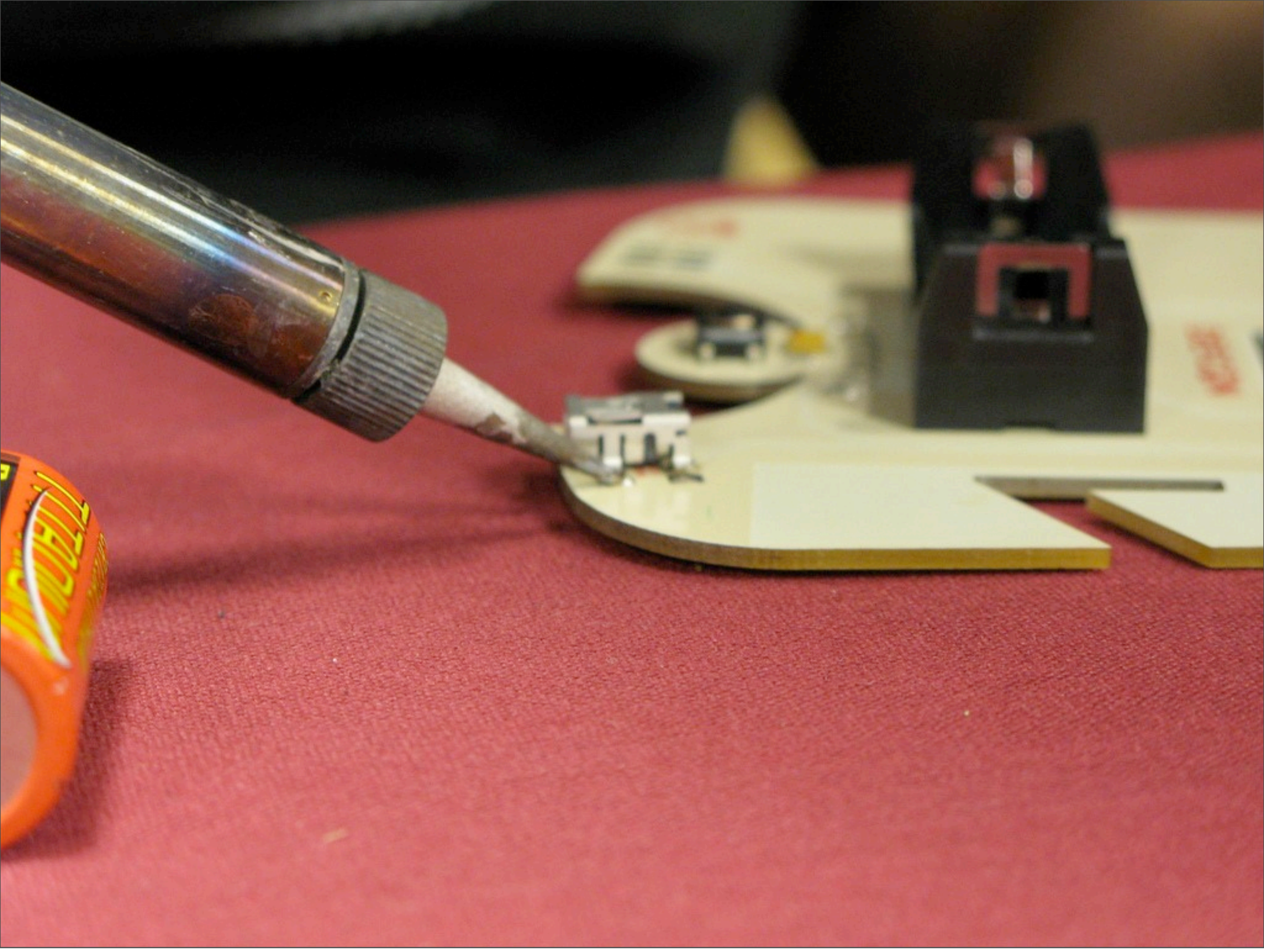
Story about using the score server to reset the overwrite token on Sk3wlofr00t for a good chunk of Saturday at DC15.

Only as strong as the weakest link. Part 2
David
http://www.flickr.com/photos/afferent/461165947/
http://creativecommons.org/licenses/by/2.0/deed.en



Our attack on the overwrite-reset wasn't the only one that year. While the Kenshoto CTF didn't have much of a web-app security focus, that didn't mean it was entirely non-existent. For example, the score server was potentially vulnerable to a CSRF attack against the same overwrite-key change we abused with a stolen credential. One team embedded an attack against that into all their web services. It was too bad the legitimate web services weren't working that year, or more folks might have been bit by that clever attack as well.

Frosty Morning Web
foxpar4
http://www.flickr.com/photos/foxypar4/2124673642/
http://creativecommons.org/licenses/by/2.0/deed.en



Friday, July 31, 2009

While the badge hacking contest winner from last year was neat, the second place entry was much more entertaining to me. A whole slew of badges were programmed to transmit the IR codes for the hibernate command on HP laptops and with the activate-front-row codes for OS X laptops.

The range on these suckers was phenomenal. It was great watching people try to figure out why their laptops were constantly hibernating or going in and out of Front Row.

Normally that would be entertaining enough as it is, but when one of the recipient of the IR signal of doom is on one of the CTF teams and trying to actually get work done, well, then I count this as an excellent dirty trick for CTF too.

Be warned! Disable /all/ your external interfaces before you bring a machine to Defcon, and especially expect the CTF room to be home to some real shenanigans!

Soldering USB Interface to Badge
Kankie
http://www.flickr.com/photos/kankie/2762312562/
http://creativecommons.org/licenses/by/2.0/deed.en



Friday, July 31, 2009

School’s patched binary used against them, also DC15.

judo - ga≈°per med padcem 2
MelkiaD
http://www.flickr.com/photos/melkiad/2329190548/
http://creativecommons.org/licenses/by/2.0/deed.en



Friday, July 31, 2009

In 2006, one team came tantalizingly close to the hole grail of a CTF win -- hacking the score system itself. While often technically against the rules, and it's easy to screw up and make the game no fun, a clever hack is a clever hack, and taking advantage of a default admin interface in one of the VOIP adapters accepting key submissions would have been very clever if the attack had actually been pulled off successfully. Instead, the device's IP was changed, just causing a temporary outage while Kenshoto fixed it. So close... The team that did it was awarded some breakthrough points by Kenshoto for their cleverness even if they didn't quite pull it off.



Friday, July 31, 2009

It’s a little known fact that there were /two/ challenges solved by use of a vim swap file in this year’s qualifiers.

First was the intentional one, Forensics200 -- read the writeups linked to at the end of this presentation for more information.

Then there was the other one... Pwn200 -- a service that had some trouble and was being fixed live during the qualifiers. Fixed by editing the service live with vim on the service. And exposing the source, making the challenge much simpler. I wonder if anybody from DDTEK is actually here, I don’t know if Team Awesome officially told you guys about that one yet. ;-)



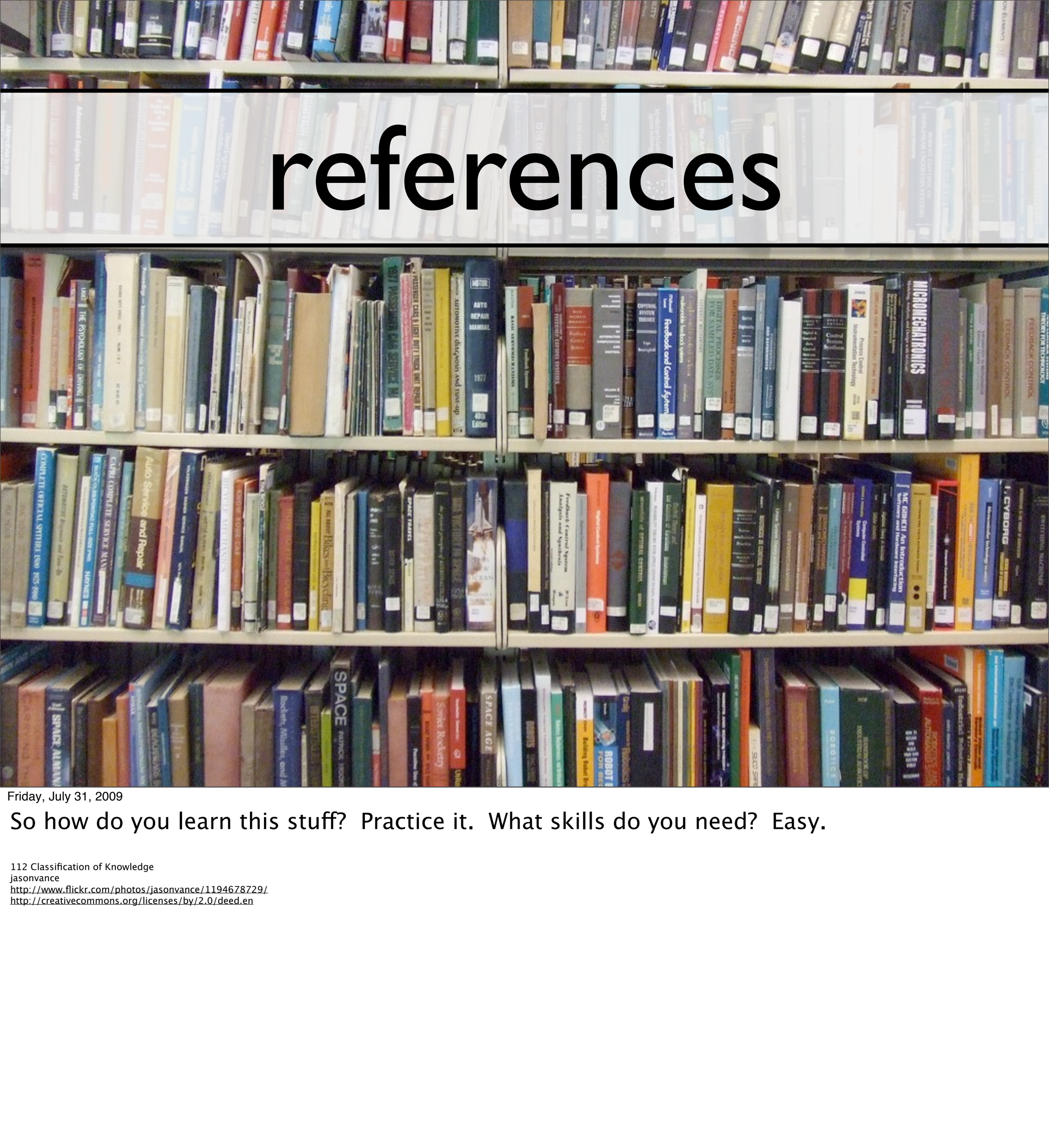
Don’t ruin the game for everyone. There are some dirty tricks that are best not played:

Collusion, Denial Service, Physical Attacks

The moral is to always check if unsure. Ask the conference organizers if in doubt. You do not want to be the team banned from CTF because you didn’t think something through, and if it’s actually a good hack, most likely the organizers will be cool with you doing it!

STOP ALL WAY
Peter Kaminski
http://www.flickr.com/photos/peterkaminski/1510724/
http://creativecommons.org/licenses/by/2.0/deed.en

references



Friday, July 31, 2009

So how do you learn this stuff? Practice it. What skills do you need? Easy.

112 Classification of Knowledge
jasonvance
http://www.flickr.com/photos/jasonvance/1194678729/
http://creativecommons.org/licenses/by/2.0/deed.en



Friday, July 31, 2009

Start with this small list.

The best skills are the ones mentioned previously under roles. Get really good at one of those and practice it. There are literally dozens of online challenge sites out there with starter problems to get you going. Just start breaking stuff and playing with it. No better way to learn.

Go back through the Defcon video archives and check out the presentation my team captain Atlas did a few years back on his radical transformation during the 2005 Qualifiers to CTF. If you apply yourself, you really can go from just knowing the basics to being truly l33t.

tools and techniques



Ok, those are the skills, but what about the tools?

You want to come prepared with a framework for managing flags, and exploiting other servers. Any defensive techniques need to be scripted in packages easy to install no matter what the platform you end up defending.

Wrench Red
Kyle May
http://www.flickr.com/photos/kylemay/2078979917/
http://creativecommons.org/licenses/by/2.0/deed.en





Friday, July 31, 2009

Get good at a scripting language. Quick and dirty perl, python, ruby, it doesn't matter. Unless you're very good and very fast with C, it's worth your time to invest effort into a language that enables quick solutions, tools, and techniques.

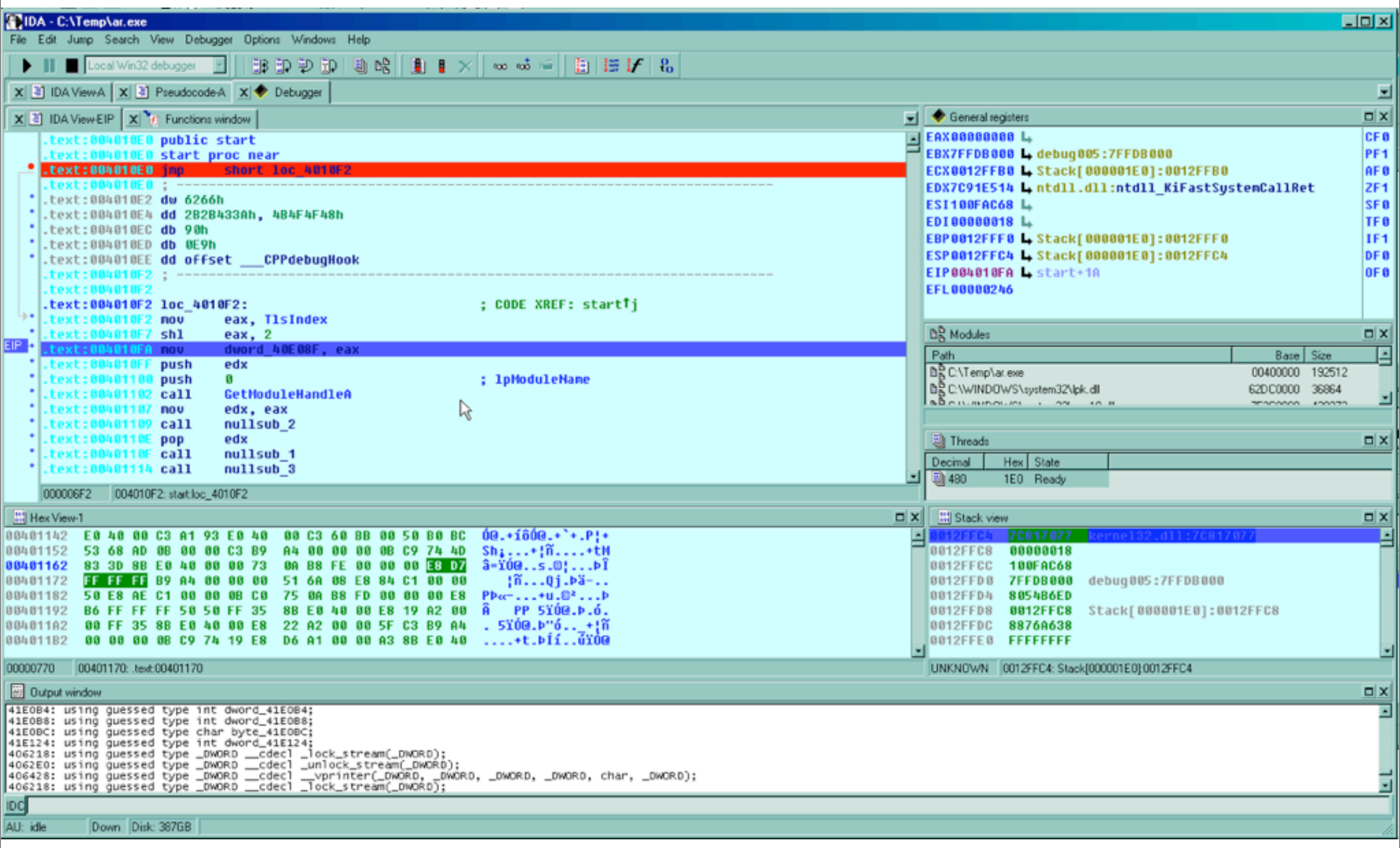
Focus on attacks, scoreboard submissions, website scraping, custom service monitoring, etc. The key here is rapid development.

gnisrever reversing

Friday, July 31, 2009

There's a lot of different tools you could use for your reversing and exploitation. Most important is to have a few you are comfortable with. Practice lots with GDB, or another portable debugger. Those skills will last no matter what the platform.

It matters more that you have something you're comfortable with than you have something that other people are using to solve problems.



Friday, July 31, 2009

If you're doing any binary analysis at all, one required tool is IDA Pro. The second major requirement is a scriptable debugger you're comfortable with. Whether it's Immunity Debugger, IDA with the appropriate plugins and debug modules, or some other solution, you need to be able to quickly script up tasks in the debugger. Of course, for most CTF challenges, you're going to be spending some quality time with GDB, so don't neglect it.

http://capture.thefl.ag/

http://ddtek.biz/
http://nopsr.us/
http://shallweplayaga.me/
http://hackerschool.org/DefconCTF/17/B300.html
http://ha.ckers.org/blog/20090406/hacking-without-all-the-jailtime/

Websites

Capture.TheFl.Ag -- Updated copy of these slides, mirror/links to specific CTF content, many more links, links to other writeups, etc. At some point in the near future when I get more trustworthy Internet access.

Nopsrus -- 2006-2008 Qualifiers and many Finals Binaries from Doc Brown and 1@stplace
shallweplayaga.me -- Writeups for 2009 qualifiers from Team Awesome
RSnake's blog entry has a huge list of online CTF type sites, many different formats, but some great resources among there.

books

Friday, July 31, 2009

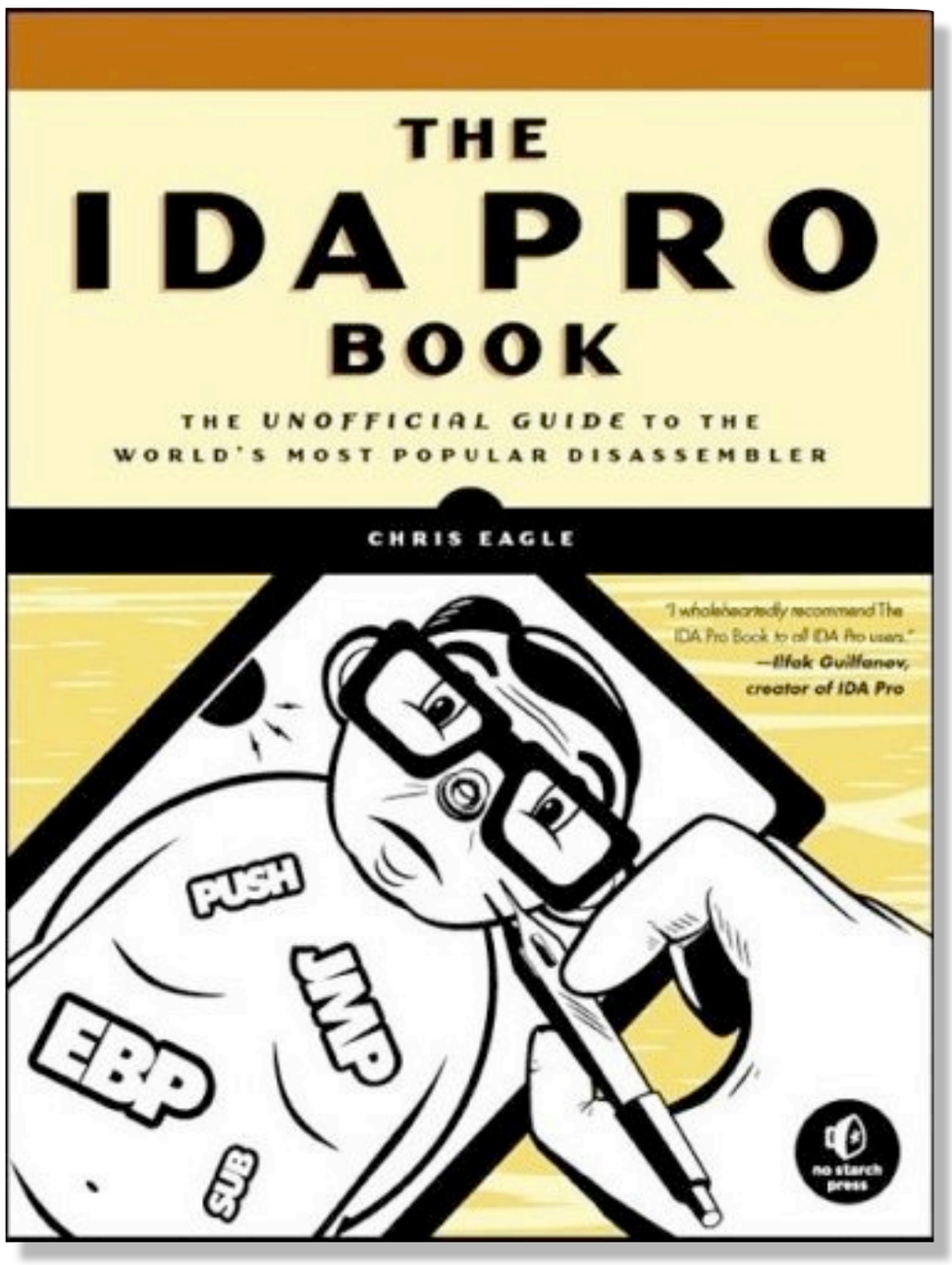
IDA Pro Book -- Notice the author on that is none other than the sk3wlm4st3r, Chris Eagle himself. This book is the IDA bible. The book was at least partially responsible for the release of the Collabreate tool mentioned earlier.

Hacking: TAOE is a good solid overview to all sorts of good security techniques.

Shellcoders Handbook: covers many relevant topics

There are many other good books to get you started, but practice the online resources and use the books as needed.

books



Friday, July 31, 2009

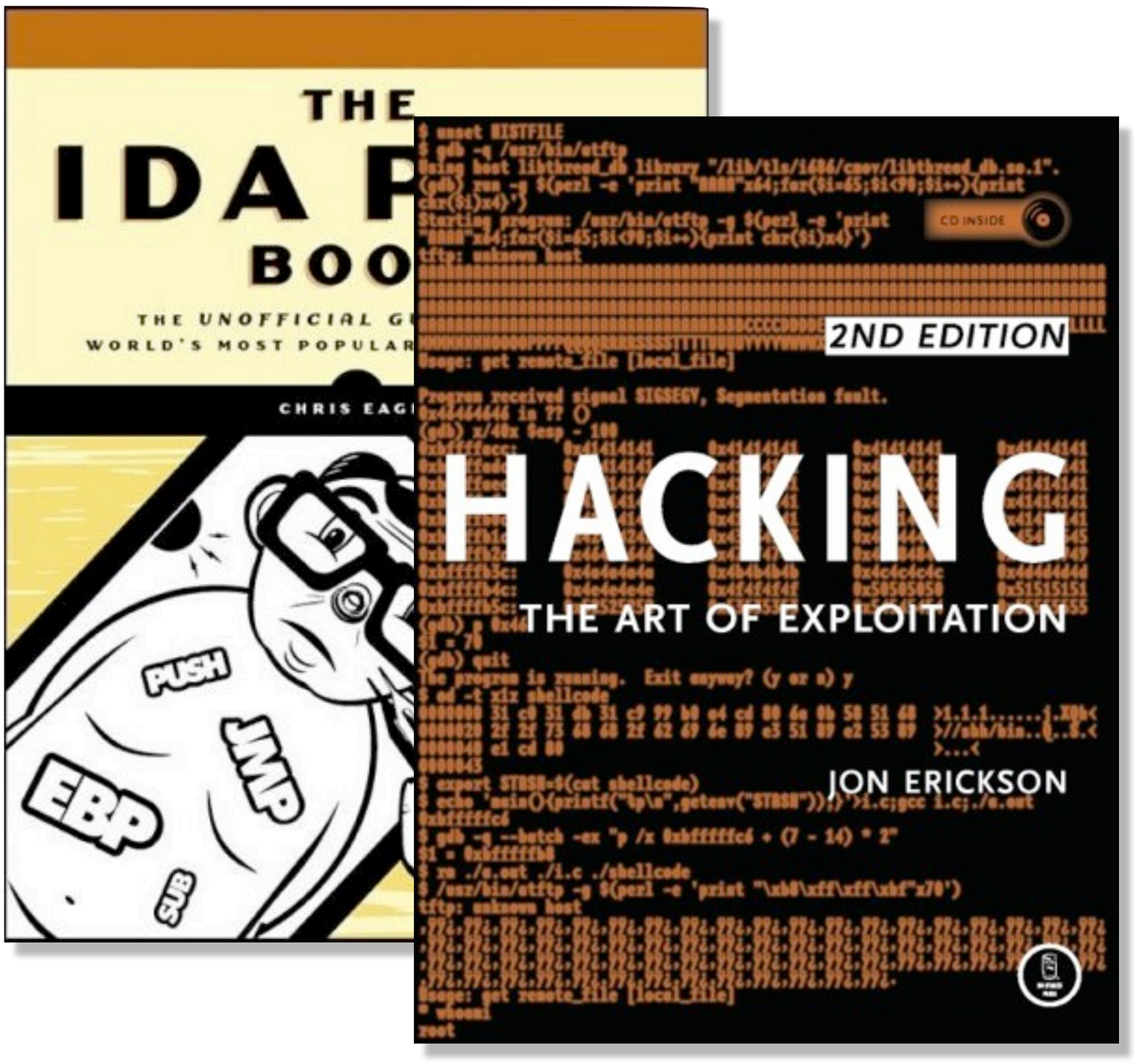
IDA Pro Book -- Notice the author on that is none other than the sk3wlm4st3r, Chris Eagle himself. This book is the IDA bible. The book was at least partially responsible for the release of the Collabreate tool mentioned earlier.

Hacking: TAOE is a good solid overview to all sorts of good security techniques.

Shellcoders Handbook: covers many relevant topics

There are many other good books to get you started, but practice the online resources and use the books as needed.

books



Friday, July 31, 2009

IDA Pro Book -- Notice the author on that is none other than the sk3wlm4st3r, Chris Eagle himself. This book is the IDA bible. The book was at least partially responsible for the release of the Collabreate tool mentioned earlier.

Hacking: TAOE is a good solid overview to all sorts of good security techniques.

Shellcoders Handbook: covers many relevant topics

There are many other good books to get you started, but practice the online resources and use the books as needed.

books



Friday, July 31, 2009

IDA Pro Book -- Notice the author on that is none other than the sk3wlm4st3r, Chris Eagle himself. This book is the IDA bible. The book was at least partially responsible for the release of the Collabreate tool mentioned earlier.

Hacking: TAOE is a good solid overview to all sorts of good security techniques.

Shellcoders Handbook: covers many relevant topics

There are many other good books to get you started, but practice the online resources and use the books as needed.

The Fine Print

This presentation:
(Some Rights Reserved)
Creative Commons Attribution 3.0 United States License
http://creativecommons.org/licenses/by/3.0/us

Company/product logos:
All photos of companies or products trademarked/copyright their respective companies.

Background images:
Most photos releasd under a Free license. See the slide notes for each slide for more information on image source and license.

Friday, July 31, 2009

Links to each image's original Flickr page and author credits in the slide notes on each slide.