CTF @ KIT 🏳

Hackers wanted!

team@kitctf.de

CTF in a nutshell

- Online contest
  - up to 1000 participating teams (!)
- Applied IT Security
- Team oriented
- Very diverse
- Legal hacking
- Usually on-line
  - Everyone with internet access can play
- Not very beginner friendly :(

How does it work?

- Teams register on website
- Contest starts
- Challenges accessible through website
- Flags (= character strings) are obtained by solving a challenge
  - `EKO{1337_x86_64_xplo1t}`
- Can be submitted on the website to get points
- The harder the challenge the more points it is worth
  - Well...
  - Timeframe per challenge: between just a few minutes and >8 hours
- Afterwards participants publish write-ups explaining their solutions
  - https://github.com/ctfs/write-ups-2015
  - Great way to learn!

Who plays CTFs?

Mostly student + industry professional teams

- Plaid Parliament of Pwning
  - Students and Alumni from CMU
- Dragon Sector
  - All polish team
  - Some Google (security) engineers
- Samurai
  - International, big team
  - Many Google (security) engineers
- FluxFingers
  - Students from RUB

RANK	AVATAR	TEAMNAME
1		Dragon Sector
2		PPP
3		Samurai
4		Shellphish
5		More Smoked Leet Chicken
6		!SpamAndHex
7		217
8		0ops
9		Tasteless
10		pollypocket
11		KITCTF
12		blue-lotus
13		c00kies@venice
14		dcua
15		0daysober
16		StratumAuhuur

Who organizes CTFs?

- Usually organized by other CTF teams
  - PlaidCTF ➜ PPP
  - CCC CTF ➜ Stratum Auhuur
  - Confidence CTF ➜ Dragon Sector
  - hack.lu CTF ➜ Fluxfingers
  - GPN CTF 2015 ➜ Squareroots + KITCTF
- Often take place during IT security conferences
- Usually on-line (jeopardy style)
- Sometimes on-site as well (attack-defense)
- “World-Championship”: DEFCON CTF
- Central hub: https://ctftime.org

Team rating

2015 | 2014 | 2013 | 2012 | 2011

Place	Team	Country	Rating
1	Plaid Parliament of Pwning		1474.545
2	Dragon Sector		917.240
3	0ops		891.525
4	!SpamAndHex		847.400
5	dcua		687.001
6	Shellphish		685.876
7	Gallopsled		646.089
8	Samurai		645.222
9	blue-lotus		625.695
10	217		579.824

Full rating | Rating formula

Upcoming events

Format	Name	Date	Duration
	WhiteHat Grand Prix – Qualification Round 2015 On-line	Oct. 24, 2015 02:00 — Oct. 25, 02:00 UTC 73 teams	1d 0h
	TUM CTF Teaser On-line	Oct. 24, 2015 12:00 — Oct. 25, 12:00 UTC 65 teams	1d 0h

Now running

WhiteHat Grand Prix – Qualification Round 2015 73 teams
On-line | Oct. 24, 2015 02:00 — Oct. 25, 02:00 UTC (6h more)

TUM CTF Teaser 65 teams
On-line | Oct. 24, 2015 12:00 — Oct. 25, 12:00 UTC (16h more)

Past events

EKOPARTY CTF 2015
Oct. 23, 20:00 UTC | On-line

Place	Team	Country	Points
1	More Smoked Leet Chicken		80.000
2	!SpamAndHex		55.072
3	Samurai		42.880

794 teams total | Tasks and writeups

Hack.lu CTF 2015
Oct. 22, 08:00 UTC | On-line

Place	Team	Country	Points
1	Dragon Sector		140.000
2	Plaid Parliament of Pwning		104.991
3	Samurai		93.269

248 teams total | Tasks and writeups

Team rating

2015 | 2014 | 2013 | 2012 | 2011

Place	Team	Country	Rating
1	Plaid Parliament of Pwning		1474.545
2	Dragon Sector		917.240
3	0ops		891.525
4	!SpamAndHex		847.400
5	dcua		
6	Shellphish		
7	Gallopsled		
8	Samurai		
9	blue-lotus		625.695
10	217		579.824

Full rating | Rating formula

Upcoming events

Format	Name	Date	Duration
	WhiteHat Grand Prix – Qualification Round 2015 On-line	Oct. 24, 2015 02:00 — Oct. 25, 02:00 UTC 73 teams	1d 0h
	TUM CTF Teaser On-line	Oct. 24, 2015 12:00 — Oct. 25, 12:00 UTC 65 teams	1d 0h

Now running

WhiteHat Grand Prix – Qualification Round 2015 73 teams
On-line | Oct. 24, 2015 02:00 — Oct. 25, 02:00 UTC (6h more)

TUM CTF Teaser 65 teams
On-line | Oct. 24, 2015 12:00 — Oct. 25, 12:00 UTC (16h more)

Past events

EKOPARTY CTF 2015
Oct. 23, 20:00 UTC | On-line

	Country	Points
		80.000
		55.072
		42.880

794 teams total | Tasks and writeups

Hack.lu CTF 2015
Oct. 22, 08:00 UTC | On-line

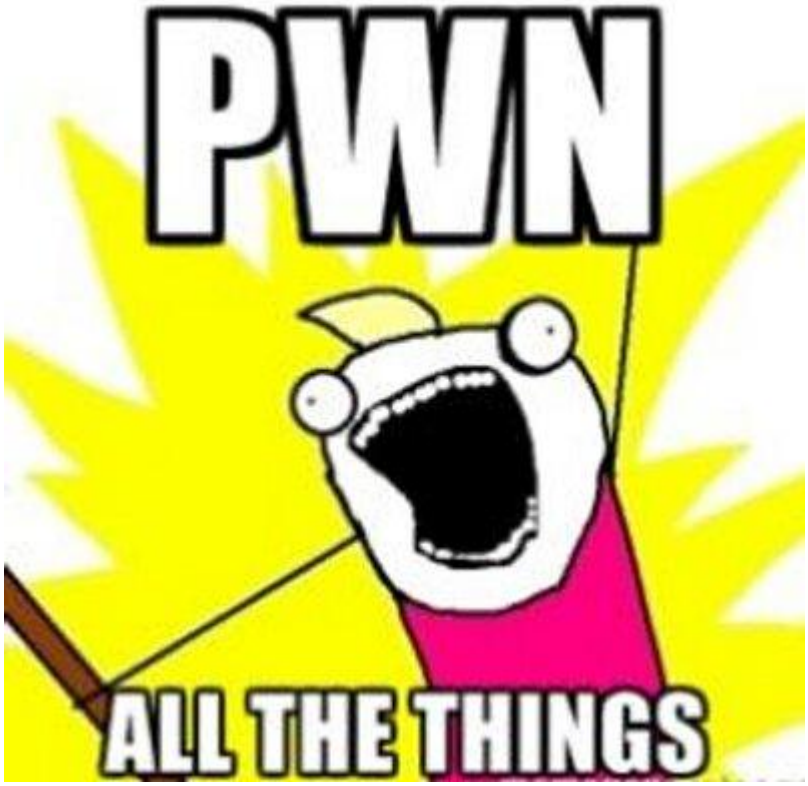
Place	Team	Country	Points
1	Dragon Sector		140.000
2	Plaid Parliament of Pwning		104.991
3	Samurai		93.269

248 teams total | Tasks and writeups

KITCTF #21 Currently!

CTF “Disciplines”

- Binary Exploitation
- Cryptography
- Web Security
- Reverse Engineering
- Forensics
- Sandboxing
- Kernel Exploitation
- Coding
- ...



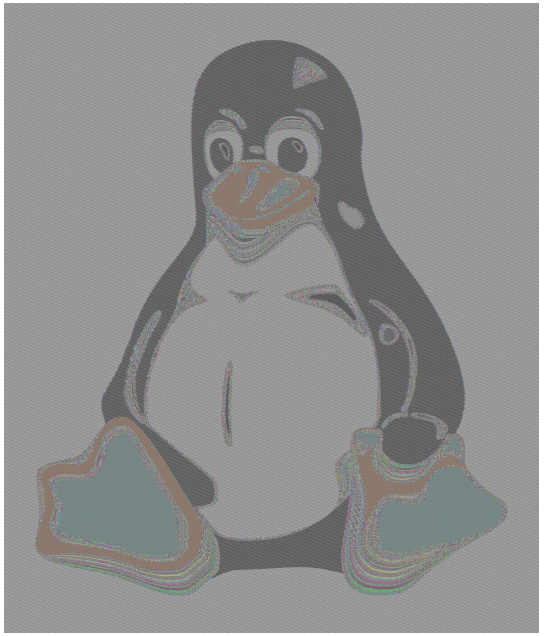
Binary Exploitation (“pwnables”)

- Goal: Find and exploit (not only) memory corruption vulnerabilities in (usually) C or C++ applications
  - Find vulnerability/vulnerabilities
  - Write exploit
  - Run exploit against remote server
  - Gain access to the system
  - Read flag file (e.g. /flag.txt)
- Usually no source code access ⇒ need to reverse engineer
- Linux, sometimes other *Nix (e.g. FreeBSD) or Windows
- (Almost) never gets boring, so many ways to screw up :)

DEMO TIME!

Cryptography

- Break all kinds of self-made or incorrectly applied cryptography
- Caesar, Vigenère, XOR, ...
- Hash algorithms
- Block + Stream ciphers
- RSA, DH, EC-based systems: number theory!
- Unsafe use of random number generators



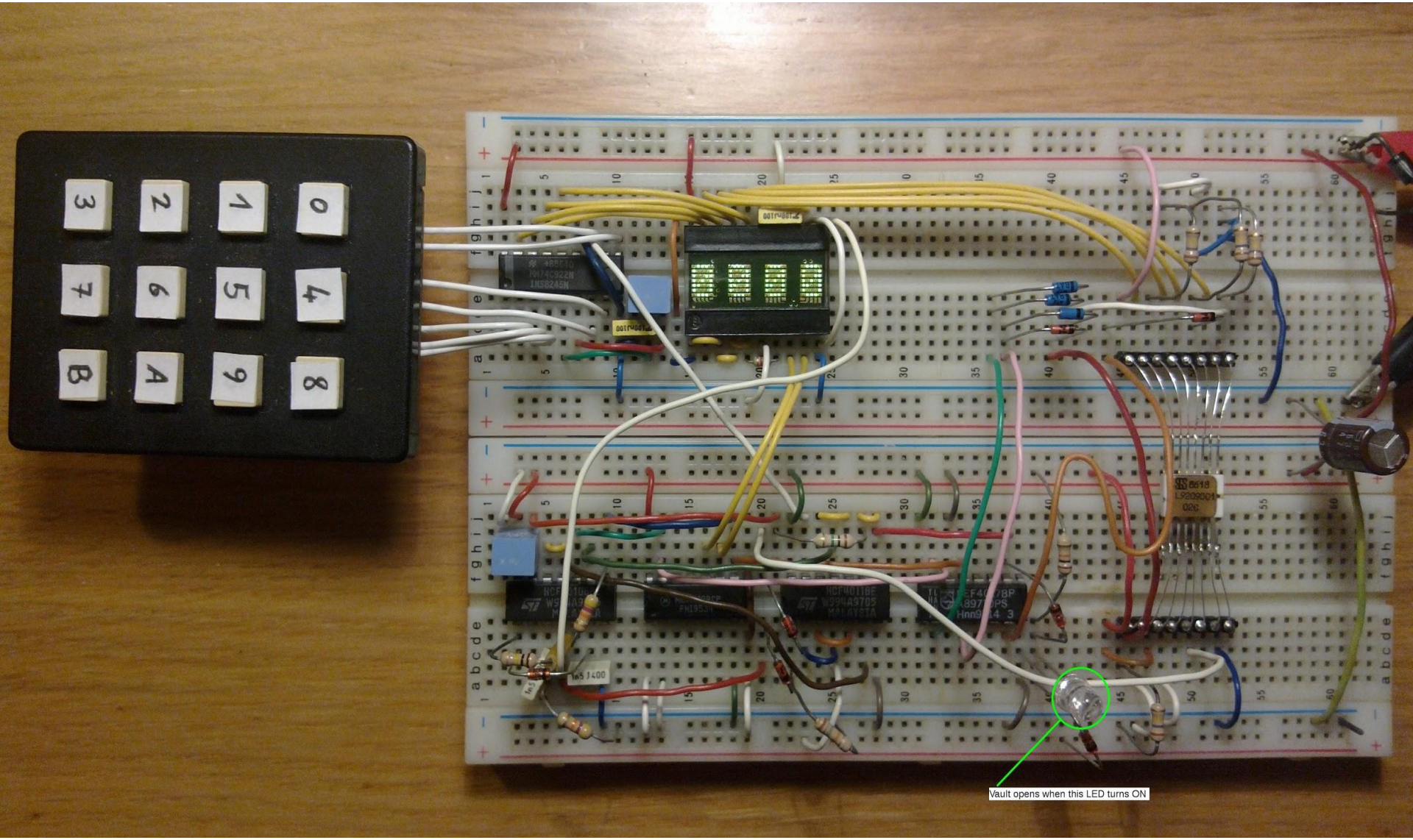
Web Security

- Usually server side, sometimes client side
- Goal: Either RCE (Remote Code Execution), file disclosure (e.g. read flag.txt) or database access (flag is stored in the database)
- Various languages
- Various frameworks
- Various vulnerabilities :)

DEMO TIME!

Reverse Engineering

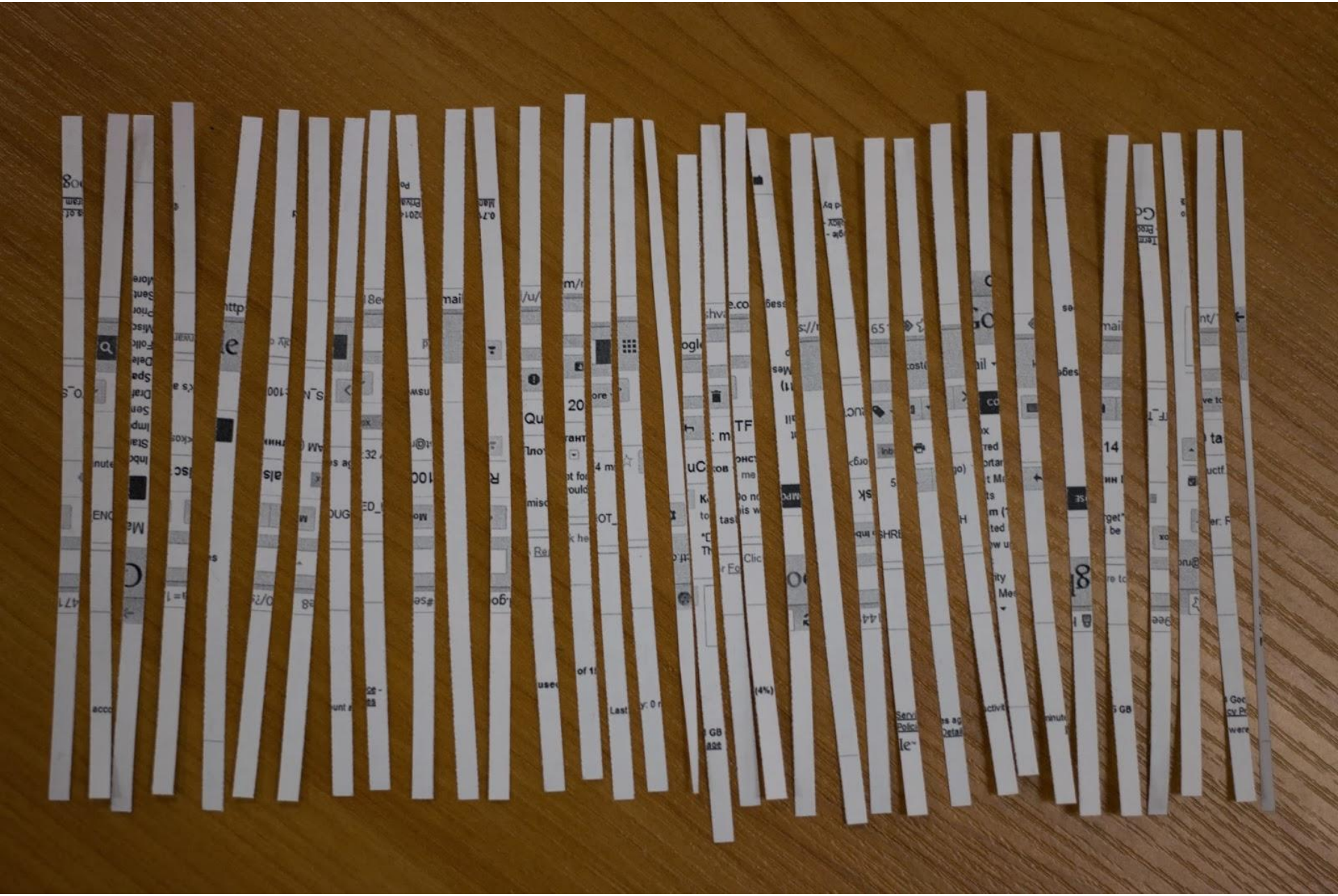
- Often crack-me style challenges: Given a binary that accepts some input string, find that string (== the flag)
- Not only native code:
  - “Compiled” Python, Ruby, PHP, Perl, ...
  - .NET, JVM, Android APKs, ...
- Or something completely different
  - Given a file compressed with an self-made compression algorithm, reverse engineer the algorithm and reconstruct the original file
  - Reverse engineer the function of a digital circuit from a photography...


3 2 1 0
7 6 5 4
B A 9 8
Vault opens when this LED turns ON

Forensics

Find or recover pieces of information from various sources:

- Analyze disk image of compromised system
- Extract the flag from a PCAP file (network traffic)
  - Not only network protocols though, USB, SCSI, etc. can be captured as well
- Recover encryption keys or other data from system memory dumps
- Deal with corrupted data
  - E.g. recover a corrupted git repository
    - Afterwards you'll know pretty well how Git works ;)
- Or even...



Sandboxing

- Break out of some kind of sandbox
- At the OS level or language interpreter level (or even hypervisor level)
  - Python is almost impossible to sandbox, JavaScript pretty easy
  - Combine with pwnable: first exploit sandboxed process, than break out of the sandbox

Kernel Exploitation

- Goal: Attack the operating system kernel to escalate privileges (to root)
  - Usually memory corruption bugs
  - Unique attack surface and environment
- Can be considered a form of sandbox escape

Coding

- Various algorithmic challenges, sometimes even artificial intelligence
  - Ever wanted to write a snake AI?

Oh, and...

... did you ever want to hack an online game? ;)

http://pwnadventure.com/

What can/will you learn on the side?

- Deep knowledge of operating system internals and low-level computing (assembly)
- Good C (and C++) skills
- Scripting language (Python, Ruby, ...)
- Various useful tools
  - debuggers, (dis)assemblers, (de)compilers, networking tools, shell tools
- Web application frameworks
- Crypto libraries
- Stuff you (maybe) didn't know even existed!
  - SMT solvers, weird networking protocols and of course the various exploit mitigation technologies at work in modern operating system
- In general: **To break a system you need to understand how it works first!**

Bonus Motivation

[–] **DeadStarMan** 9 points 10 months ago

What do you look for in a intern, experience wise? Any advice for a CS major looking to break into the field?

permalink save give gold

> [–] **IncludeSec** [S] 24 points 10 months ago*
>
> CTFs....DO.EVERY.CTF! ctftime.org
>
> that's it, as a student this is what you should be spending all your waking hours on. It will make you a self-starter, you'll learn technical skills ahead of your peers and it's a huge green "This guy knows what he's doing" flag for potential employers who really know security.
>
> You can also use it as a reverse red-flag, if nobody on the technical security team you're interviewing with knows what CTFs are then you've got to wonder how good they are :-|
>
> permalink save parent give gold
>
> > [–] **valsmithar** 9 points 10 months ago
> >
> > I'd agree with this. Spend all of your free time building VM's with vulnerabilities, attacking them, recreating exploits. Everything is theoretically easy until you physically try to recreate it. You'll learn a lot by building applications and systems which will make you better when attacking them because you will understand the thought process of a sysadmin or dev.
> >
> > permalink save parent give gold
>
> > [–] **OfFireAndFlame** 9 points 10 months ago
> >
> > To add to that, here's an archive of older CTF challenges you can go through.
> >
> > permalink save parent give gold
>
> > [–] **DeadStarMan** 3 points 10 months ago
> >
> > Thanks for the tip! I am on spring break right now, so I will start this today.
> >
> > permalink save parent give gold
>
> > [–] **aaronhigbee** 4 points 10 months ago
> >
> > Yup. CTF puzzle solving is a good trait for services that don't have known methodologies.
> >
> > permalink save parent give gold

Requirements?

Requirements?

None *

Requirements?

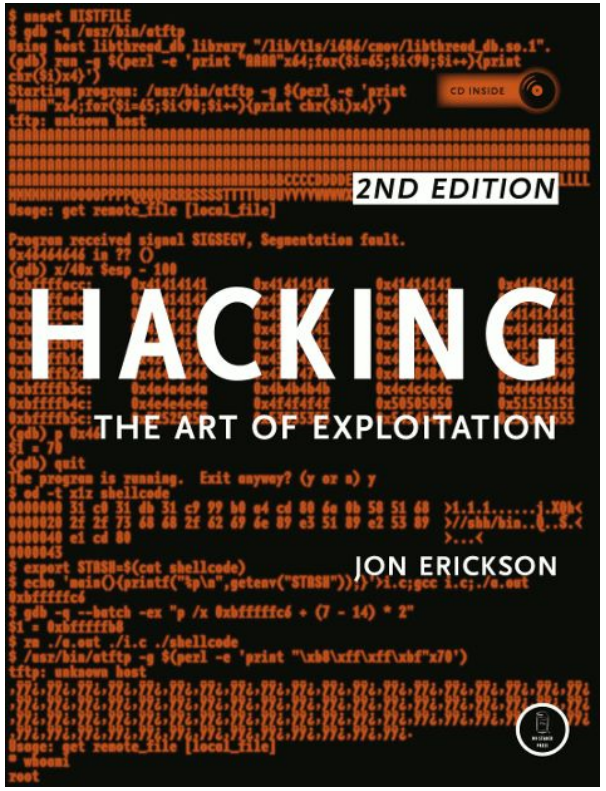
*

- a laptop ;)
- basic computer and programming skills
- maybe some Linux knowledge
- but most importantly:

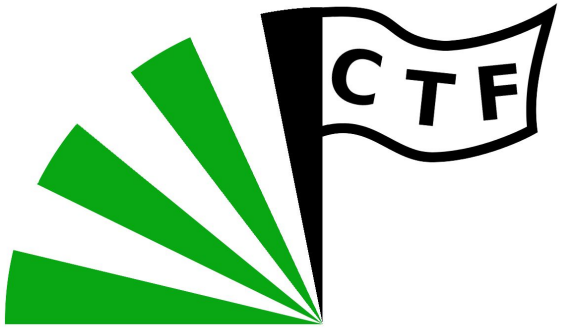
motivation and some spare time

How to learn how to CTF? (non-exclusive list)

- Playing CTFs: https://ctftime.org/event/list/upcoming
  - There are easier and harder CTFs
  - Also most CTFs have at least some easier challenges
  - **!! read writeups !!**
- Online wargames and similar challenges
  - http://smashthestack.org
  - http://overthewire.org/wargames/
  - https://microcorruption.com/
  - http://cryptopals.com
- Reading stuff
  - http://phrack.org
  - https://reddit.com/r/netsec
  - Books
    - Hacking: The Art of Exploitation
    - Reversing: Secrets of Reverse Engineering
  - Many more, just ask us for suggestions
- Shameless plug: https://kitctf.de/learning



About Us



- Started around June 2014
- Currently around 5 core members
- Travel to conferences and play CTF
  - “Insomi’Hack”
  - “Confidence” - We won travel + accommodation by making #1 in the teaser CTF :)
  - 32C3 (upcoming)
- Communication via IRC (deprecated) and Slack: https://kitctf.slack.com
  - Slack has clients for Mac, Windows, Linux, Android, iOS and Web
  - If you want to join (you should! :)) send your email address to team@kitctf.de
- Sometimes team up with “Stratum Auhuur” for bigger CTFs
  - DEFCON, PlaidCTF, ...
  - Won 15 RPI 2 in one CTF and 1024$ in another :)
- https://kitctf.de

Meetings

- Once a week, currently Wednesday starting at around 4PM, R250 - Infobau
- Present solutions for previous CTF challenges (or solve them together)
- Do small workshops:
  - Kernel Exploitation
  - Mobile Exploitation, e.g. Stagefright
  - Browser Exploitation, e.g. v8, Firefox
  - Network Security, e.g. Scapy
  - ...
- Idea: 1 hour of newcomer training at beginning of meeting
  - Introduction to binary exploitation and tool setup, starting *next week* (11.11)
- Don’t worry if you can’t make it, there’s enough material out there

One last thing...

One last thing...

CTFs are hard. Stay motivated, it will pay off :)

Questions?