Capture the Flag

Acquiring practical security knowledge through enjoyable hacking challenges (Based on slides by Samuel Groß)

Liam Wachter | 28. April 2022

What are CTFs?

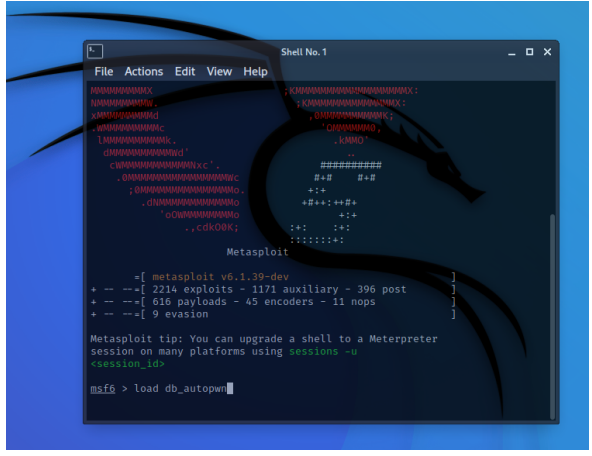
- Online or in-person contests
- Applied IT Security
- Team oriented

During CTFs, people...

- are hacking (in the positive sense of the word)
- do vulnerability discovery + exploit writing
- get in contact with all kinds of technology
- in general do computer science
- learn

What are CTFs NOT?

- Using existing exploits
- Illegal
- Step-by-step learning
- (Very beginner friendly)

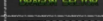
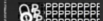
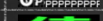
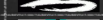


How does it work?

- Teams register on a website
- Contest starts
- Challenges accessible through website
- Flags are obtained by solving a challenge, e.g. `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 a few minutes and > 8 hours
- Afterwards participants publish write-ups explaining their solutions
  - https://kitctf.de/writeups/
  - Great way to learn!

Who plays CTFs

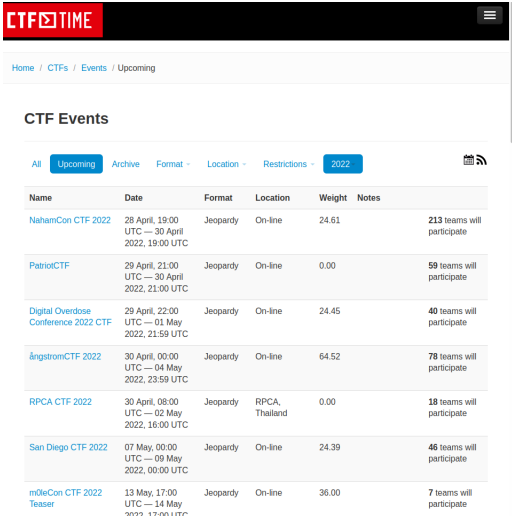
- Plaid Parliament of Pwning (PPP)
  - Students and Alumni from CMU
- FluxFingers
  - Students and Alumni from RUB
- Samurai
  - International, big team
  - Many Google (security) engineers
- Sauercloud
  - German team of teams
  - Participating in DEFCON and DEFCON-Qualifiers

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?

- Other CTF teams
  - PlaidCTF and PicoCTF → PPP
  - hack.lu → Fluxfingers
  - ALLES! CTF → ALLES!
- Companies
  - Google Capture The Flag
  - Real World CTF
- Usually online. Sometimes on-site, e.g., at conferences
- „World-Championship“: DEFCON CTF
- Central hub: `https://ctftime.org`

ctftime.org: CTFs every weekend



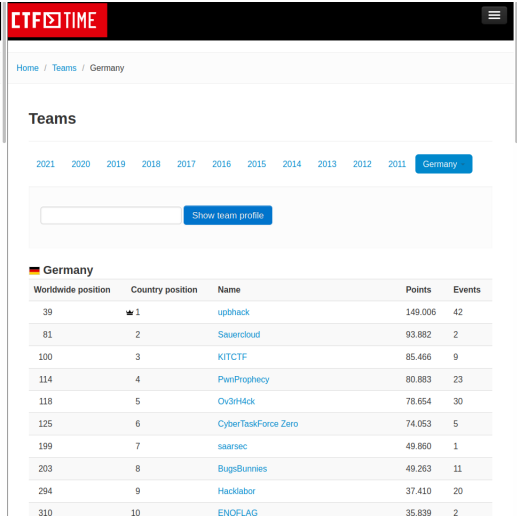
CTFTIME

Home / CTFs / Events / Upcoming

CTF Events

All | Upcoming | Archive | Format | Location | Restrictions | 2022

Name	Date	Format	Location	Weight	Notes	
NahamCon CTF 2022	28 April, 19:00 UTC — 30 April 2022, 19:00 UTC	Jeopardy	On-line	24.61		**213** teams will participate
PatriotCTF	29 April, 21:00 UTC — 30 April 2022, 21:00 UTC	Jeopardy	On-line	0.00		**59** teams will participate
Digital Overdose Conference 2022 CTF	29 April, 22:00 UTC — 01 May 2022, 21:59 UTC	Jeopardy	On-line	24.45		**40** teams will participate
ångstromCTF 2022	30 April, 00:00 UTC — 04 May 2022, 23:59 UTC	Jeopardy	On-line	64.52		**78** teams will participate
RPCA CTF 2022	30 April, 08:00 UTC — 02 May 2022, 16:00 UTC	Jeopardy	RPCA, Thailand	0.00		**18** teams will participate
San Diego CTF 2022	07 May, 00:00 UTC — 09 May 2022, 00:00 UTC	Jeopardy	On-line	24.39		**46** teams will participate
m0leCon CTF 2022 Teaser	13 May, 17:00 UTC — 14 May	Jeopardy	On-line	36.00		**7** teams will participate



CTFTIME

Home / Teams / Germany

Teams

2021 | 2020 | 2019 | 2018 | 2017 | 2016 | 2015 | 2014 | 2013 | 2012 | 2011 | Germany

Show team profile

Germany

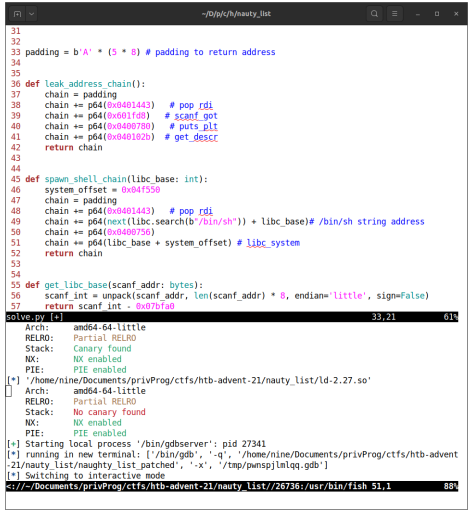
Worldwide position	Country position	Name	Points	Events
39	1	upbhack	149.006	42
81	2	Sauercloud	93.882	2
100	3	KITCTF	85.466	9
114	4	PwnProphecy	80.883	23
118	5	Ov3rH4ck	78.654	30
125	6	CyberTaskForce Zero	74.053	5
199	7	saarsec	49.860	1
203	8	BugsBunnies	49.263	11
294	9	Hacklabor	37.410	20
310	10	ENOFLAG	35.839	2

CTF „Disciplines“

- Binary/Kernel Exploitation
- Reverse Engineering
- Cryptography
- Web Hacking
- miscellaneous, e.g.,
  - Machine Learning
  - Cryptocurrency
  - Forensics
  - Sandboxing
  - Game Hacking

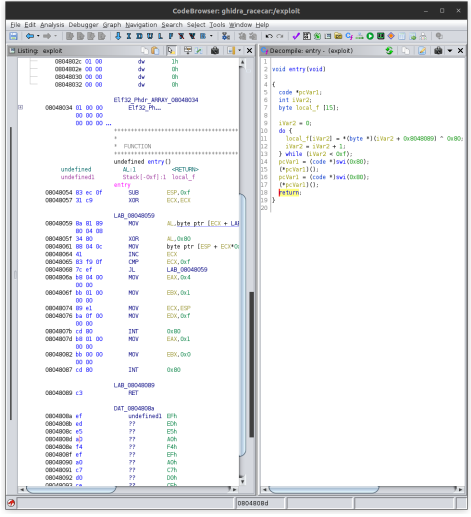
CTF „Disciplines“

- Binary/Kernel Exploitation
- Reverse Engineering
- Cryptography
- Web Hacking
- miscellaneous, e.g.,
  - Machine Learning
  - Cryptocurrency
  - Forensics
  - Sandboxing
  - Game Hacking



CTF „Disciplines“

- Binary/Kernel Exploitation
- Reverse Engineering
- Cryptography
- Web Hacking
- miscellaneous, e.g.,
  - Machine Learning
  - Cryptocurrency
  - Forensics
  - Sandboxing
  - Game Hacking

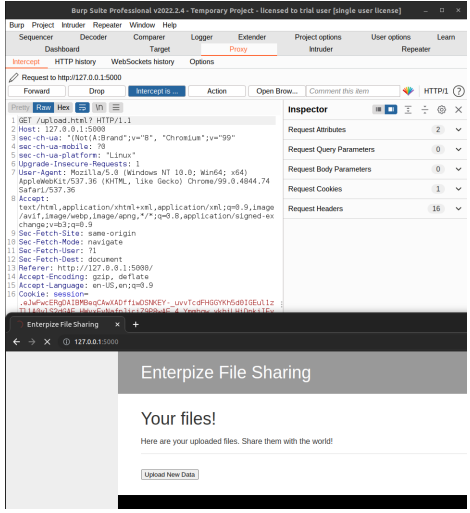


CTF „Disciplines“

- Binary/Kernel Exploitation
- Reverse Engineering
- Cryptography
- Web Hacking
- miscellaneous, e.g.,
  - Machine Learning
  - Cryptocurrency
  - Forensics
  - Sandboxing
  - Game Hacking

CTF „Disciplines“

- Binary/Kernel Exploitation
- Reverse Engineering
- Cryptography
- Web Hacking
- miscellaneous, e.g.,
  - Machine Learning
  - Cryptocurrency
  - Forensics
  - Sandboxing
  - Game Hacking



CTF „Disciplines“

- Binary/Kernel Exploitation
- Reverse Engineering
- Cryptography
- Web Hacking
- miscellaneous, e.g.,
  - Machine Learning
  - Cryptocurrency
  - Forensics
  - Sandboxing
  - Game Hacking

What you will learn on the side?

- Deep knowledge of operating system internals
- Good intuition for: „There is something wrong“
- Familiarity with various programming languages and frameworks
- Various useful tools
  - debuggers, (dis)assemblers, (de)compilers, networking tools, sandboxes, . . .
- Crypto libraries
- Stuff you (maybe) didn’t know even existed!
  - SMT solvers, weird protocols, various modern exploit mitigations, interesting mathematics

Requirements?

None*

Requirements?

*

- basic computer and programming knowledge
- a laptop is useful

motivation and some spare time

How to learn (non-exhaustive list)

- Playing CTFs
  - There are easier and harder CTFs: PicoCTF, CSCG, ...
  - Most CTFs have at least some easier challenges
  - **try and read writeups**
- Free courses with challenges
  - OverTheWire
  - pwn.college
  - ProtSwigger Web Security Academy
  - Open Security Training 2
- Videos
  - LiveOverflow, GynvaelEN, John Hammond
  - stacksmashing, gamozolabs, OALabs
  - IppSec, PinkDraconian, PwnFunction
  - Day0-Podcast
- Reading stuff
  - Magazines
    - phrack
    - pagedout
  - Blogs
    - r/netsec
  - Books
    - The Art of Software Security Assessment
    - Hacking: The Art of Exploitation
- Conferences
- KIT Courses :)

About us

- Started around June 2014
- Currently playing with 3-6 players per CTF
- Communication over Slack
- Weekly in-person meetings: Thursdays Room 252
- Intro talks on first four meetings
- Workshops from industry professionals and researches T.B.A.

Introduce yourself at team@kitctf.de