

Capture the flag

Go waste your weekends

By **Martin** presented by **חחח**

```
import pwn
```

```
pwn.context.arch = "amd64"  
pwn.context.os = "linux"
```

```
SHELLCODE = pwn.shellcraft.amd64.linux.echo('Test') + pwn.shellcraft.  
EXPLOIT = 0x45*b"\x90" + pwn.asm(SHELLCODE, arch="amd64", os="linux")
```

```
PROGRAM = b""  
length = 20 + 16  
for i in EXPLOIT:  
    PROGRAM += i*b'+' + b'>'
```

```
    if i == 1:  
        length += 5  
    elif i > 1:  
        length += 6  
    length += 13
```

```
    (0x8000 - length) > 0x40:  
        PROGRAM += b"<>"  
        length += 2*13
```

```
    b"["
```

```
    (0 - length) + 7 - 1
```

```
    (F+0x10)*b"<"
```

```
host", 1337) as conn:  
    (b"Brainf*ck code: ")  
    PROGRAM)  
    e()
```

What the **flag**?

- Competitions about finding and exploit security vulnerabilities
- A way to develop vulnerability research & exploitation skills
- Team based, mostly running for one weekend
- A fun way into the infosec community

What CTF is **NOT**

- Illegal
- A way to quickly learn "hacking"
- Using ready-made exploits and automated tools
- Straight forward and super beginner-friendly

What are the challenges?

- No fixed rules, but common categories
- Really wide range of difficulty levels
- Always new stuff – that's why we are here

The big 4

Web.

REV

CRYPTO

pwn

The underdogs

- Blockchain, AI
- OSINT, Forensic
- Game hacking
- Scripting, competitive programming

A CTF events lifecycle

- Some CTF team host an event
- **KITCTF** decides to participate
- During the event we collaborate to solve as many challenges as possible and become **first place**
- At the next meeting solutions and interesting challenges get discussed

How do I get started

- Play CTF
- Read writeups !!!
- Be curious, there is no guide to CTF. Learning is part of the game
- Join the meetings, connect with others

How do I get good?

- Just start playing & read writeups
- Play for a team (hopefully us)
- Don't get intimidated
- Follow kitctf.de/learning/howto








What is KITCTF?

- CTF team at KIT, founded in 2014
 - Currently **#5 in Germany** and **#42 globally**
- Weekly meetings every **thursday**
 - General exchange about security & non-IT banter
- Irregular competitions during weekends
 - The occasional international competition
- Hosting our own CTF once a year. Last year with over 650 teams

Other teams

- ENOFLAG - TU Berlin
- FAUST - FAU Erlangen
- Platypwnies - Hasso-Plattner-Institut
- Sauercloud - German merger team
- Flagbot / P0lyglots - ETH / EPFL
- Organizers - Swiss merger team
- Kalmarunionen - Nordic merger

Team rating







2024	2023	2022	2021	2020	2019	2018	2017	2016	2015
2014	2013	2012	2011						
Place	Team	Country	Rating						
1	kalmarunionen		1651.746						
2	thehackerscrew		1064.050						
3	Blue Water		927.177						
4	r3kapig		906.231						
5	The Flat Network Society		905.286						
6	organizers		838.907						
7	Project Sekai		764.308						
8	C4T BuT S4D		735.152						
9	if this doesn't work we'll get more for next year		728.438						
10	idek		694.559						

[Full rating](#) | [Rating formula](#)

Upcoming events

Open

Finals

Format	Name	Date	Duration
	BlackAlps CTF 2024  Switzerland, Yverdon-les-Bains	Thu, Nov. 07, 19:15 — Thu, Nov. 07, 23:30 UTC 15 teams	4h
	HKCERT CTF 2024 (Qualifying Round)  On-line	Fri, Nov. 08, 10:00 — Sun, Nov. 10, 10:00 UTC 90 teams	2d 0h
	Metared Argentina CERTUNLP  On-line	Fri, Nov. 08, 11:00 — Sat, Nov. 09, 11:00 UTC 24 teams	1d 0h



Past events

With scoreboard

All

RedShift.Eclipse 2 Quals



Nov. 04, 2024 12:00 UTC | On-line | [Weight voting in progress](#)

Place	Team	Country	Points [*]
👑 1	ufoufo		0.000
2	RedHazzarTeam		0.000
3	MHC		0.000

[186 teams total](#) | [Tasks and writeups](#)

Hack The Vote 2024



Nov. 03, 2024 23:00 UTC | On-line | [Weight voting in progress](#)

Place	Team	Country	Points [*]
👑 1	Maple Bacon		0.000
2	tohru		0.000
3	Shellphish		0.000

[559 teams total](#) | [Tasks and writeups](#)

Equinor CTF 2024

Nov. 02, 2024 19:00 UTC | Norway, Oslo

Place	Team	Country	Points
👑 1	RumbleInTheJungle		50.000
2	bootplug		36.013
3	mneF00		31.146

[78 teams total](#) | [Tasks and writeups](#)

What's next?

- Intro Talks
 - Web security (8.5.)
 - Reverse engineering (15.5.)
 - Binary exploitation (22.5.)
 - Cryptography (05.6.)