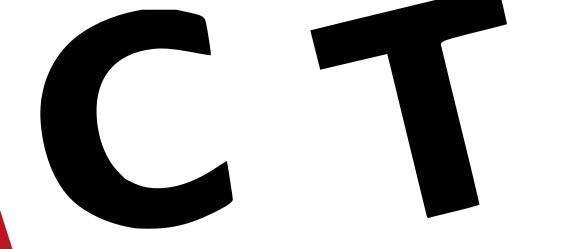# Capture the flag

Go waste your weekends

By Martin presented by Finn

```python
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
    ngth+= 13


    0x8000 - length) > 0x40:
    RAM += b"<>"
    h += 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**

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

CTFTime 💔

What's next?

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