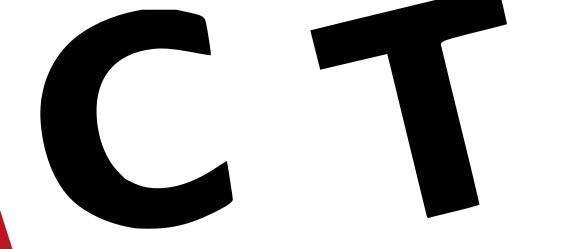
Capture the flag

Go waste your weekends

By Martin presented by ғипп



```
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".["
             9 - length) + 7 -1
               F+0x10)*b"<"
                 host", 1337) as conn:
                  (b"Brainf*ck code: ")
                  PROGRAM)
```

1mport pwn

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





5

The underdogs

- Blockchain, Al
- 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 / POlyglots ETH / EPFL
- Organizers Swiss merger team
- Kalmarunionen Nordic merger



CTFTime 💔

	CTFs Upcoming	Archive ▼ Calendar	Teams ▼ FAQ Cor	itact us ▼ At	pout		Sign in	
Team	rating			Past e	events a			
2024	2023 2022 2021 2020 2013 2012 2011	2019 2018 2017	2016 2015	With scor	reboard All			
Place 1	T eam	Country	Rating		Shift.Eclipse 2 Quals 24 12:00 UTC On-line Weight	t voting in progress		
业 1 k	kalmarunionen	=	1651.746	Place To	eam	Country	Points *	
2 t	hehackerscrew		1064.050	₩1 ut	foufo		0.000	
3 E	Blue Water		927.177	2 R	ledHazzarTeam	_	0.000	
4 r	3kapig	•0	906.231	3 N	1HC	_	0.000	
5	The Flat Network Society	ш	905.286		186 teams total Tasks and writ			
6 0	organizers	E .	838.907	⊞ Hacl	k The Vote 2024			
7 F	Project Sekai		764.308	Nov. 03, 20	24 23:00 UTC On-line Weight	t voting in progress		
8 (C4T BuT S4D	_	735.152	Place To	eam	Country	Points *	
9 i	f this doesn't work we'll get more for ne	xt year ◆■	728.438	业 1 №	laple Bacon	IH	0.000	
10 i	dek		694.559	2 to	bhru		0.000	
		Full	rating Rating formula	3 S	hellphish		0.000	
Upco	ming events ふ					559 teams	total Tasks and writeup	
Open	Finals			_	inor CTF 2024 24 19:00 UTC Norway, Oslo			
Format	Name	Date	Duration	Place To	eam	Country	Points	
	BlackAlps CTF 2024	Thu, Nov. 07, 19:15 — Th		≌ 1 R	lumbleInTheJungle	#=	50.000	
000	Switzerland, Yverdon-les-Bains	07, 23:30 UTC	15 teams	2 b	ootplug	#=	36.013	
0 0 0 0 0 0 0 0 0	HKCERT CTF 2024 (Qualifying Round) On-line	Fri, Nov. 08, 10:00 — Sur 10, 10:00 UTC	n, Nov. 2d 0h 90 teams	3 m	nneF00		31.146	
	Metared Argentina CERTUNLP	Fri, Nov. 08, 11:00 — Sat 09, 11:00 UTC	, Nov. 1d 0h 24 teams			78 teams	total Tasks and writeur	



What's next?

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

