SEAD KU Intro

How to build a CTF challenge

Intro lecture Content

1. Organizational stuff
2. What is a CTF?
3. Tips for your practical

Organization

~~5~~ 3 Phases of ~~Grief~~ SEAD

Phase 1: *Lay of the land*

On your own:

- Solve 2 SEAD challenges from last year
- Short intro to CTF challenges
- Just to get you started
- Maximum 10 points
- https://sead-ctf.student.iaik.tugraz.at

~~5~~ 3 Phases of ~~Grief~~ SEAD

Phase 2: *Build your own challenge*

As a group of 3:

- Design a CTF challenge together!
- Think about a cool vulnerability
- Build a **secure application** around it
- Create an automated solvescript
- Maximum 30 points

~~5~~ 3 Phases of ~~Grief~~ SEAD

Phase 3: *Hack all systems!*

On your own:

- Solve the challenges of other teams
- Harder challenge -> more points
- 60 points + bonus
- Some amount of bonus points possible
  Amount depends on number and difficulty of challenges

Grading

Phase 1: max. 10 points, 5 required

Phase 2: max. 30 points, 15 required

Phase 3: 60+ points, 30 required

Points	Grade
$\geq 87\frac{1}{2}$ points:	Sehr Gut (1)
≥ 75 points:	Gut (2)
$\geq 62\frac{1}{2}$ points:	Befriedigend (3)
≥ 50 points:	Genügend (4)

Timeline

- 01.03.2024:
  - Intro lecture (**today**)
  - Start of Phase 1
- 14.03.2024:
  - End of Phase 1
- 15.03.2024:
  - Phase 2 Kickoff lecture

Timeline

- 22.03.2024:
  - Group registration deadline
- 12.04.2024:
  - Hand in challenge idea
- **Afterwards:** Feedback by tutors
- 26.04.2024:
  - Challenge deadline
  - End of Phase 2

Timeline

- 03.05.2024: Start of Phase 3
- 21.06.2024:
    - Deadline for writeups
    - End of Phase 3
    - **Freedom!**

What is a CTF?

Capture The Flag

Capture The Flag

(Information Security)

Capture The Flag

- Infosec Competitions
- *"Competitive Hacking"*
- Deliberately vulnerable services
- Solve the challenge to get the flag
  - `LosCTF{this_is_how_a_flag_looks_like}`
  - `glacierctf{Ju57_P0s1X_th1ng5}`
  - `dvCTF{Br4v0K4sP4r0V}`
  - `"$CTFNAME{$some_funny_message}"`

Capture The Flag

Styles

Attack-Defense

- Teams get their own Server/VM with services
- Attack other teams, patch own services
- Usually short timeframe (e.g. 8 hours)
- Get attack points for stealing flags every tick
- Get defense points for defending flags and uptime
- Traffic analysis, rev, pwn, web, DevOps, binary patching

Capture The Flag

Styles

Jeopardy

- All teams get the same challenges
- Usually around 24-48 hours
- Get points by solving different challenges *once*
- Points scale based on difficulty
- rev, pwn, crypto, web, misc
- **This is what we create in this course**

Challenge Types

rev

- Reverse engineering
- Get a binary that compares input to the flag
- Get a binary that prints the flag, but very slowly
- Get a binary and some data that the binary created from the flag
- …
- usually offline

Challenge Types

pwn

- Binary exploitation
- Get a binary, find the bug, exploit it to print flag
- Often involves reverse engineering
- Usually has a local binary, and a remote with the **real** flag
- Buffer overflows, shellcode, ROP-chains, ...
- **Covered in SSD**

Challenge Types

crypto

- Cryptography
- Usually provide sourcecode
- Examples:
    - **Local:** Decrypt the flag, it was encrypted by *this algorithm*
    - **Remote:** Create a valid signature/token/etc to get the flag
    - **Remote:** You get *n* encryption oracle calls to guess the key
- Weird RSA math, insecure AES based ciphers, custom hashes...

Challenge Types

web

- You get a website, you exploit it
  - **XSS, CSRF, ...**: Send the admin something, he will look at it
  - **SQL injections**: Find the exploitable part, poke around the database
  - **Authentication**: Forge/modify JWTs, cookies, etc
- Usually with source code

Challenge Types

misc

- Everything that doesn't fit with other categories
- Can include hardware, RF, signal processing, stego, forensics, ...
- Very diverse category

Phase 1

Phase 1

- Available now at https://sead-ctf.student.iaik.tugraz.at/
- Login through https://git.teaching.iaik.tugraz.at/
  - If you already have an account there: Great!
  - If not: Save the flags for now
  - Accounts will be created after signups are done
- 2 Challenges, 5 points each
- Note: Solve both stages so the challenge counts

Tips for Phase 1

Tips for Phase 1

- **Google**
- Discuss challenges with your friends
  - No flag/solution sharing
- Poke around!
- Where is the flag?
- How can you get to it?
- Pro tip: "{Keywords} CTF Writeup"

Useful tools for solving CTF challenges

- **Python** - powerful builtins for quick and dirty scripts
- **pwntools** - Python library to connect to backends, analyze ELF binaries, interact with programs...
- **requestbin** - accepts and logs all kinds of HTTP requests
- **Cyberchef** - quickly translate between encodings and formats
- **Burpsuite** - intercept and modify web requests by your browser

Questions?