IT-SicherheitsAG

/* University of Passau */

Organizational Stuff

- 5829AG IT-Sicherheit (Arbeitsgemeinschaft / eng: IT-Security Working-group)
- Tuesday & Thursday 18:30 - 20:00
- Meetings are currently held on our Discord server https://discord.gg/sNckMdy (switch to physical meetings in our Security Lab (ITZ) when the corona stuff is over)
- No exam, no ECTs but a lot of valuable knowledge (certificate of participation can be granted)
- Topic this semester: Capture the Flag (CTF) & Wargames
- Preparation for other security courses (especially for the Security Insider Lab I + II (5822UE), 12 ECTS each)

CTF Team

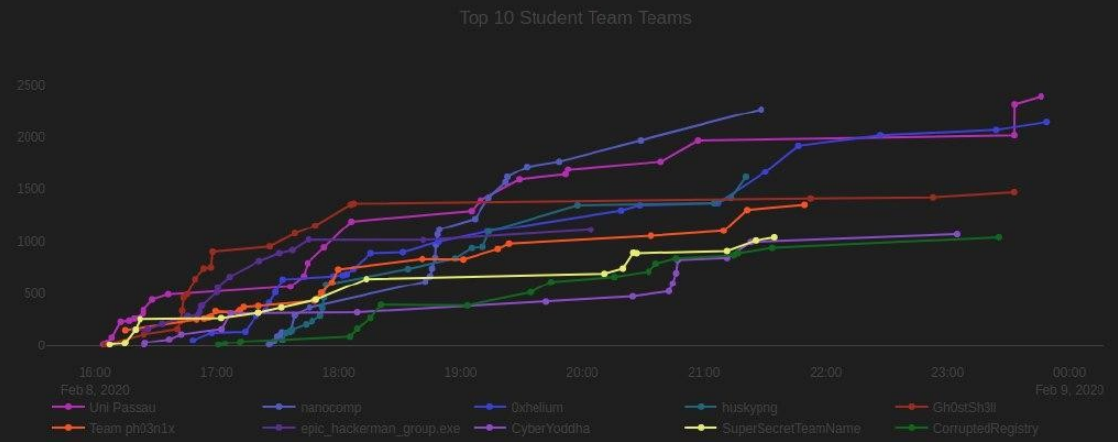
/* University of Passau */

Who are we?

The Team

@un1x, @babbadeckl

Who are we?



Place	Team	Score
1	Uni Passau	2390
2	nanocomp	2265
3	0xhelium	2140
4	huskypng	1615
5	Gh0stSh3ll	1470

What is CTF?

What is CTF?

CTF: Capture the Flag

What is CTF?

CTF: Capture the Flag

Flag: A string of text hidden on a server, or an answer to a question or riddle.

What is CTF?

CTF: Capture the Flag

Flag: A string of text hidden on a server, or an answer to a question or riddle.

flag{N3v3r_g0nna_g1v3_y0u_up}

What is CTF?

CTF: Capture the Flag

Flag: A string of text hidden on a server, or an answer to a question or riddle.

The Goal: Find and capture all of the flags for your team… and to do it the fastest

flag{N3v3r_g0nna_g1v3_y0u_up}

What is CTF?

CTF: Capture the Flag

Flag: A string of text hidden on a server, or an answer to a question or riddle.

The Goal: Find and capture all of the flags for your team… and to do it the fastest

Each flag is worth points to the team's total score, and at the end of the game the team that has the highest score will WIN.

flag{N3v3r_g0nna_g1v3_y0u_up}

Types of CTFs

/* Attack - Defense */

- Network of vulnerable systems
- Each team gets 1 system
- Goal: Fix as many vulnerabilities of your system while “hacking” as many systems of the other teams.
- Each successful attack gives points

/* Jeopardy */

- Tasks in different categories
  - Reverse Engineering
  - Pwn
  - Web
  - Crypto
  - Misc

Jeopardy Categories

Reverse Engineering (RE)

You are given a file/executable (often some sort of malware).

Find out what it does and how to stop it.

The flag is either hidden in the code or part of the prevention technique.

Jeopardy Categories

Pwn

You are given a file/executable.

Find a vulnerability and exploit it to gain root access / trigger functions

Flag is mostly hidden in the root directory / output is given

Jeopardy Categories

Web

You are given a web application

Find the vulnerability and exploit it

Flag is mostly a hidden text/file

Jeopardy Categories

Crypto

Advanced mathematical problems…

Most of the time only solvable if you are up-to-date with current research topics in this area …

Jeopardy Categories

Misc

Everything else that’s not RE, Pwn, Web or Crypto

Mostly some programming tasks (efficient implementation)

What is CTF?

Youtube: LiveOverflow - What is CTF?

How is it organized?

/* Beginners */

- Learn the basics
- Weekly meetings to discuss new tasks/solutions
- presentations
- subgroups for e.g. programming or specific areas in CTF

/* No Beginners */

- fast repetition of the basics
- active participation in existing CTFs

Who are you?

Groups

THX <3

How to reach us:

Korbinian Spielvogel: ks2@sec.uni-passau.de
Felix Klement: fk@sec.uni-passau.de

...or via Telegram/Discord

Slides: https://github.com/CTF-UP/talk_introductory_event