

# CTF Contests: Hands-On Experience of the IT Security Culture – UE 04: Tools & Libraries

Clemens Hlauschek, Daniel Marth, Florian Fankhauser



**INSO – Industrial Software**

Institute of Information Systems Engineering | Faculty of Informatics | TU Wien

# PlaidCTF Debriefing



## Upcoming Event: RuCTF



- Postponed :(
- 22 May 2022
- We will keep you up to date, please have an eye on #announcements in Discord

## Tools & Libraries



- No silver bullet!
- But still helpful in many situations... if you know when and how to use them
- We have already seen a few:
  - `strace` / `ltrace`
  - CyberChef
  - Burp Suite
  - Cutter
  - Ghidra
  - RSACTFTool
  - ...

- Programming is a crucial skill during CTFs
- However, it is not reasonable to always start from scratch
- Lots of existing libraries can make our lives easier
- Know when it pays off to automate tasks!

- <https://nmap.org/>
- Network scanner
- Discovers hosts, ports, services
- Nmap Scripting Engine (NSE)
  - Extract specific service information
  - Brute force credentials
  - Vulnerability scanning
  - ...



- <https://sqlmap.org/>
- Automatically detects and exploits Structured Query Language (SQL) injections in web applications
- Very helpful on blind and time-based attacks
- Convenient features:
  - Dump the database content
  - Spawn a shell on the server
  - Read / write remote files
  - ...

- <https://scapy.readthedocs.io/>
- Network packet manipulation library
- Full control over data encoding / decoding
- Common use cases:
  - Send and receive network traffic interactively
  - Load and analyze traffic dumps

- <https://docs.pwntools.com/>
- “CTF framework and exploit development library”
- Convenient features:
  - Tubes: Communicate with processes, network hosts, etc. via a common interface
  - Integer encoding
  - Symbol resolution based on address leaks
  - Format string attacks
  - ...

- <https://github.com/ReFirmLabs/binwalk>
- Detects and extracts embedded files
  - E.g., a ZIP file within an image
- Based on file signatures

# Exercises



## Observe Closely

- <https://ctftime.org/task/10652>
- UTCTF 2020
- Forensics

# Table-tennis

- <https://ctftime.org/task/7744>
- BSidesSF 2019 CTF
- Forensics

**Thank you!**

<https://security.inso.tuwien.ac.at/ctf-2022s/>

