

CTF Contests: Hands-On Experience of the IT Security Culture – UE 00: Preliminary Discussion

Clemens Hlauschek, Daniel Marth, Florian Fankhauser



ESSE



ESSE – Establishing Security

- Institute of Information Systems Engineering
- Research Group for Industrial Software (INSO)
- Working Group Establishing Security (ESSE)
- Lectures
 - Introduction to Security (*W, Bachelor*)
 - Security for Systems Engineering (CTF-Contest) (*S, Bachelor*)
 - Mobile Security (*S, Bachelor*)
 - Advanced Security for Systems Engineering (*W, Master*)
 - Selected Topics of Digital Forensics I (*S, Master*)
 - IT Security in Large IT Infrastructures (CTF-Contest) (*S, Master*)
 - Seminar on Security
 - CTF Contests: Hands-On Experience of the IT Security Culture (*S, Bachelor/Master*)
 - Projects, Bachelor Thesis, Master Thesis, PhD Thesis

Spheres of Action (Excerpts)

- eHealth, eGovernment
- Electronic Payments
- Secure and Anonymous Communication
- Embedded Security and Internet of Things
- Governance, Risk and Compliance
- Penetration Testing, Security Audits, Security Certification
- System Hardening
- Secure SDLC, Secure Architectures
- Identification, Authentication and Authorization, eID solutions
- IT Security Teaching Methods
- DevSecOps

Excerpt of Research Areas

- Malware and Internet Crime
- Physical Security of IT Systems
- Applied Cryptography
- Exploit Development, Offensive Computing, and Exploit Mitigation
- Rootkits and OS Security
- Honeypots, Honeynets, and Honeytokens
- Mobile Security
- Privacy-Protection in Cloud/Mobile Applications
- Security Usability for End-2-End Security
- Security Engineering in the Software Life-Cycle

- Questions regarding CTF Contests: Hands-On Experience of the IT Security Culture
 - See slide 15

- Other matters, e.g., bachelor/master theses, projects,... :
 - esse@inso.tuwien.ac.at
 - Office Hour on agreement: Wiedner Hauptstraße 76/2/2

CTF Contests: Hands-On Experience of the IT Security Culture UE 22S



Learning Outcomes

After successful completion of the course, students are able to fundamentally understand capture the flag (CTF) contests that are commonly used in the security community to train and upgrade skills. Students will be able to use their technical skills in a competitive environment effectively together in a team. Students will have exercised how to integrate their individual strengths in a CTF team while complementing their weaknesses. They will have exercised different ways to prepare themselves for various forms of contests, and will be trained in actively collaborating with each other during contests. Furthermore, students will have learned organisational aspects of CTF teams and CTF competitions.

Mode (1/2)

- Regular discussion and presentation meetings
- Content will be generated collaboratively as a group
- tuwel forum
- e-mail
- We will try to provide a stream of the meetings (but no recording!)
- If necessary because of the pandemic, we will switch to distance learning

Mode (2/2)

- Participation in 3 online CTFs
- Submit writeups for each of them
- Presentation of a single writeup
- You can reach a maximum of 100 points
- Starting with the first submission a certificate will be issued
- Register in TISS until 03.04.2022

Note on Attacks on the IT Security of Systems

- You will learn precise attacks on IT systems in the course
- This is only
 - to better understand IT security
 - secure your own IT systems
 - test your own IT systems in regard to the security level
 - and/or use in other legal ways
- Attacking TU Wien or conducting attacks based on systems of TU Wien may lead to the withdrawal of your eligibility to study
- Exception: Attacks within explicit lab or CTF environments are OK :-)

Planned Topics

- Characteristics of CTFs
- CTF platforms
- CTF writeups
- Tools and exploit scripting
- Infrastructure of attack/defense CTFs
- Automated analysis of network traffic
- Communication and collaboration strategies
- Organisation of a CTF team
- Organsiation of a CTF

Planned Events

08.04.2022 PlaidCTF

24.04.2022 RuCTFE

TBA

Planned Excercise Dates

Writeup CTF1 20 points, 10.04.2022–01.05.2022

Writeup CTF2 30 points, 24.04.2022–15.05.2022

Writeup CTF3 30 points, TBA

Presentation 20 points, TBA

Please note:

ESSE exercises traditionally begin at 11:55pm

Support for Questions Regarding the Lecture

- Questions that are interesting and should be visible for other students as well
 - Tuwel forum
 - *Please note: We do not monitor other forums*
- Specific questions
 - lva.security@inso.tuwien.ac.at – please state the lecture name as this e-mail address is used for multiple lectures; please state your team number, if available, as well
 - Office hour
- *Please do not use other ways, e.g., Tuwel submission comments*

Thank you!

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

