INTERNET SECURITY AND TRUSTWORTHINESS

Number of ECTS: 3
Synchronous workload: 35
Asynchronous workload: 55
Dates: 26.09.2022. – 31.01.2023.
Language: English
Number of participants: 24

Goal of JCC:

The program will guide students toward the safe use of web resources through an in-depth understanding of core technologies and security issues from three key perspectives - human, computer networks, and web technologies.

Learning outcomes:

- summarize concepts, theories and research within the domain of trust in technology
- explain the types of data used in network security monitoring, the alert assessment process and the classification of intrusion events with a diamond model
- use the knowledge gained to solve the Capture-The-Flag (CTF) challenge
- apply NIST incident management procedures in response to an incident
- analyze common vulnerabilities in network and web technologies, attacks, and data for the purpose of identifying warning sources
- assess vulnerability assessment tools
- create a virtual laboratory environment for conducting simulated penetration testing

Learning outcomes assessment:

Self-assessments, automated checks, monitoring through CTF activities.

Teachers:

University of Zagreb:
Igor Tomičić, igor.tomicic@foi.hr
Tallinn University:
Sonia Sousa, sonia.sousa@tlu.ee
University of L'Aquila:
Dajana Cassioli, dajana.cassioli@univaq.it
University of Žilina:
Jana Uramova, Jana.Uramova@fri.uniza.sk

Prerequisites for the JCC:

Basics of computer networks

Number and type of assesment:

Self-assessments, automated checks, monitoring through CTF activities

foi
TALLINN UNIVERSITY
UNIVERSITÀ DEGLI STUDI DELL'AQUILA
ŽILINSKÁ UNIVERZITA V ŽILINE UNIVERSITAS SOLNENSIS
Co-funded by the Erasmus+ Programme of the European Union