Technology
Arts Sciences
TH Köln

Course
IS - IT Security

Version: 3 | Last Change: 05.04.2022 17:30 | Draft: 0 | Status: vom verantwortlichen Dozent freigegeben

General information

Long name	IT Security
Approving CModule	IS_MaCSN, IS_MaTIN
Responsible	Prof. Dr. Heiko Knospe Professor Fakultät IME
Level	Master
Semester in the year	winter semester
Duration	Semester
Hours in self-study	78
ECTS	5
Professors	Prof. Dr. Heiko Knospe Professor Fakultät IME
Requirements	Rquirements, objectives and application of cryptographic mechanisms: symmetric encryption, hashes, message authentication codes, random number generation, asymmetric encryption, signatures, key establishment
Language	English
Separate final exam	Yes

Final exam

Details

Written exam

Minimum standard

Passing the exam

Exam Type

Written exam

Lecture / Exercises

Learning goals

Knowledge

Introduction to IT Security
- Standards and Guidelines
- Taxonomy
- Security Objectives, Vulnerabilities, Threats, Risk, Attacks, Security Controls

Authentication and Key Establishment
- Authentication Protocols
- Key Exchange
- Kerberos
- Public Key Infrastructures
- Passwords and their Vulnerabilities
- Security Token

Access Control
- Authentication, Authorization, Auditing
- Discretionary and Mandatory Access Control
- Access Matrix, Unix ACL
- Role-Based Access Control
- Multi-Level Security, Bell-LaPadula Model

Network Security
- Threat Model
- LAN and WLAN Security
- IP Security, IPsec
- TCP Security, TLS, SSH
- Virtual Private Networks
- IDS and IPS
- Firewalls and UTM
- DNS Security

Software Security
- Safety and Security
- Software Vulnerabilities
- Web Security

Security Management
- Information Security Management System

- Security Standards ISO 27001, ISO 27002, BSI Grundschutz
- Privacy Regulations

Expenditure classroom teaching

Type	Attendance (h/Wk.)
Lecture	2
Exercises (whole course)	1
Exercises (shared course)	0
Tutorial (voluntary)	0

Separate exam

none

Practical training

Learning goals

Skills

- Generation of key pairs, certificates and setting up a public-key infrastructure (PKI).
- Implementation of a secure socket connection and analysis of a TLS handshake.
- Implementation and analysis of a VPN.
- Penetration testing of web applications using open source tools.
- Perform SQL injection, XSS and CSRF attacks against test systems.
- Reconnaissance, exploitation and infiltration in a lab environment.
- Interpret DNS and HTTP data to analyze an attack.

Expenditure classroom teaching

Type	Attendance (h/Wk.)
Practical training	1
Tutorial (voluntary)	0

Separate exam

Exam Type

working on practical scenarion (e.g. in a lab)

Details

-

Minimum standard

-