Courses in English
Course Description

Department	07 Computer Science and Mathematics
Course title	**Ethical Hacking**
Course number	
Hours per week (SWS)	4
Number of ECTS credits	5
Course objective	The domain of attacks on IT systems is very broad. Various technical and personal competencies can be derived from this Technical Competencies - Assess a vulnerability in the current system context - Reflect on the results and develop a solution strategy - Apply broad computer science knowledge to a specific problem - Analyze processes and identify vulnerabilities Personal competencies: - Focus on one topic - Work on a topic with persistence - Learn to deal with setbacks - Develop different approaches to the same problem - Take other people's point of view and evaluate their situations - Find arguments for own point of view problem - Take other people's point of view and evaluate their situations - Find arguments for own point of view
Prerequisites	
Recommended reading	Jon Erickson, Hacking - The Art of Exploitation, ISBN-13: 978-1593271442 Frank Neugebauer, Penetration Testing mit Metasploit, ISBN-13: 978-3898648202 Dominic Chell, The Mobile Application Hacker's Handbook, ISBN-13: 978-1118958506 Jayson E. Street, Dissecting the Hack: The F0rb1dd3n Network, ISBN-13: 978-1597495684
Teaching methods	
Assessment methods	oral exam, written exam or term paper
Language of instruction	English
Name of lecturer	Prof. Dr. Peter Trapp
Email	peter.trapp@hm.edu
Link	
Course content	Ethical hacking refers to legal attacks on IT systems in order to check and strengthen their security. This also includes red-teaming, reponsible disclosure or penetration tests. - Basic terminology, classification and structure of ethical hacking - Review of common defenses in a corporate context - Design of the legal basis for penetration testing - Design and structure of penetration tests - Penetration testing procedures - Attack types and vectors against systems - Evaluation of the attack strength as well as execution of the attacks in the selected strength - Social Engineering / Phishing-Attacks - Attacks against IT systems as a whole - Attacks against individual components of a system - Tool based attacks - Horizontal and vertical priviledge escalation - Command and control infrastructure for penetration of whole networks - Bypassing security barriers
Remarks	