

Module:	Ethical Hacking and Security Testing
Lecturer:	Prof. Dr. Thomas Kemmerich
Language:	English
Teaching Method:	Lecture and practical exercise
Credit Points:	1 ECTS
Attendance requirements:	Knowledge of Linux OS, file systems, computer hardware and networks
Goals / Skill:	<p>In this lecture students learn the basics of 'hacking' and 'penetration testing'. They will become familiar with Kali Linux. The basics of 'hacking' mechanism will be introduced and strategies of penetration testing are discussed. During the lecture the students will learn using some tools like nmap, kismet and others testing the learned lessons and do practical exercises.</p> <p>During the Tutorial the basics of the hacker tools are introduced and the students shall penetrate a local IT-System. A WLAN access point will be setup for penetration and the network behind the access point shall be accessed. At the end of the course, attack strategies and according defense strategies will be discussed along the practical exercises.</p>
Detailed Content:	<ol style="list-style-type: none"> 1. Ethics of 'hacking' and 'penetration testing'. 2. Strategies of penetrating IT-Systems 3. Technical and organizational measures securing systems 4. Penetration testing According to the lecture the practical laboratory is introduced where the students will penetrate a prepared IT-System with some common hacker tools 5. Discussion and evaluation of the practical hacking exercises
Media Used:	Electronic Presentation, Blackboard Illustrations, Practical Demonstrations, practical network and device access, Kali Linx
Literature:	<ul style="list-style-type: none"> • Security Engineering: A Guide to Building Dependable Distributed Systems, Ross Anderson • Corporate Computer and Network Security [Hardcover] Raymond Pankow, Prentice Hall, 2010 • ISO/IEC 27001 Standards • Computer Networks, Andrew S. Tanenbaum, Prentice Hall 2003 • http://www.metasploit.com • http://nmap.org • http://www.wireshark.org
Assigned Tutorial:	<p>Hacking</p> <ul style="list-style-type: none"> • The students will learn the possibilities with penetration test tools, like nmap, wireshark or a composition of tools like metasploit, to gather security relevant information of a dedicated server system.
Suggested Reading before the start of the summer school:	<ul style="list-style-type: none"> • http://www.kali.org • http://www.metasploit.com • Kali Linux Cookbook, 2013, Packet Publishing Ltd.