Course Title	Ethical Hacking and Penetration Testing				
Course Code	CYS655				
Course Type	Compulsory				
Level	Master (2nd cycle)				
Year / Semester	1st Year / 2nd Semester				
Teacher's Name	TBA				
ECTS	10	Lectures / week	None	Laboratories / week	None
Course Purpose and Objectives	The objective of this course is to provide a detailed introduction into the world of ethical hacking and to understand its usefulness to organizations in practical terms. Hacking concepts, tools and techniques, and countermeasures are covered, along with how penetration testing fits into a comprehensive cybersecurity regime. Beyond the confines of ethical hacking, this course covers aggressive hacking techniques that are essential knowledge for professionals who need to be able to defend against such advanced attacks.				
Learning Outcomes	Upon succesful completion of this course students should be able to: • Define the different types of hacking and its legal and illegal uses in the cybersecurity world • Identify and evaluate the different type of hacking attacks and how these attacks proceed • Explain the principles of vulnerability research • Describe the different phases of ethical hacking and select appropriate techniques depending on the assignment. • Define, describe and perform the different kinds of penetration testing – black box, grey box, white box. • Make effective use of penetration testing related tools • Define which tool is more effective at each step of a penetration testing project				
Prerequisites	None	Co-requisites	CYS600		

Course Content	Introduction: Definition of ethical hacking and penetration testing, position within a comprehensive cybersecurity posture, applicable national and international laws, difference between ethical (white hat), non-ethical (black hat) and grey hat hackers, vulnerability research and zero-day vulnerabilities. Hacking phases: The five phases of hacking – reconnaissance, scanning, gaining access, maintaining access, covering tracks. Reconaissance: Discovery of target information, footprinting, competitive intelligence, social engineering, Google hacking, website footprinting, email tracking Scanning: TCP flags, ping sweeps, connect scans, TCP flag manipulation, SYN scans, IDLE scans, scanning tools, banner grabbing, vulnerability scanning, ip spoofing, enumeration techniques and tools Gaining and maintaining access: password cracking, dictionary attacks, brute force attacks, hashing attacks, privilege escalation, executing applications, malware (viruses, worms, trojans, rootkits, spyware, botnets), lalware detection and anti-malware software, DoS/DDoS, network sniffing, MAC, ARP and DNS attacks, session hijacking, web application attacks, SQL injection, wireless network and mobile device attacks, cryptanalysis and related attacks. Covering tracks: Rootkits, disabling auditing, clearing logs, anonymisers, proxies, hiding files, track covering tools Practical penetration testing: Penetration testing methodology, ethical considerations, assignments and contracts, reporting, relationship to audits and audit techniques. Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on the practicalities and challenges of penetration testing.
Teaching Methodology	E-Learning As this course has a major practical component, a major part of the student workload is based on participating and completing online lab exercises.
Bibliography	*Kim, P. The Hacker Playbook 3: Practical Guide to Penetration Testing.* *Harper, A., Harris, S., Ness, J., Eagle, C., Lenkey, G. and Williams, T. Gray hat hacking: the ethical hacker's handbook. McGraw-Hill Education.* *"Hacking: The Art of Exploitation, 2nd Edition", by Jon Erickson*

	"Social Engineering: The Science of Human Hacking", by Christopher Hadnagy and Paul Wilson
Assessment	Examinations 50% Assignments/On-going evaluation 50% 100%
Language	English