MODULE **DESCRIPTOR**

MODULE TITLE	ETHICAL HACKING		
MODULE CODE	CO4103 (L7)	**CREDIT VALUE**	20 UK CREDITS / 10 ECTS
SCHOOL	SCHOOL OF SCIENCES		

MODULE **AIMS**

The aims of this module are to:
•Introduce different topics related to computer security, including vulnerabilities and techniques for improving defences.
•Identify and discuss penetration testing methodologies and techniques as well as their importance to the security of a network.
•Explore the various ways for examining countermeasures to flaws found by penetration testing.

MODULE **CONTENT**

Indicative syllabus content:

•Basics of ethical hacking
Identifying basic elements of information security. Classification of hackers and definition of terms associated with hacking. Defining and profiling an ethical hacker. Phases of ethical hacking. Understanding EU and international legal acts related to cybercrime. Cover legal acts such as the terrorism act, the computer misuse act, and the data protection act.

•Footprinting
Definitions and steps for gathering information about computers and networks. Understanding the use of google search for information gathering. Methods to limit information exposure.

•Design of a Vulnerability Assessment and Analysis test
Developing the Project Scope. Goals of Vulnerability Assessment. Elements of a Good Vulnerability Assessment. Risk Analysis Procedure

•Penetration testing

- ✓ Network -The use of a penetration testing application to give a quick snapshot of security of the target network.
- ✓ External Devices - Penetration testing of Web Sites, Mail Servers, DNS Servers.
- ✓ Database security – Threats and security needs, exploit vulnerabilities, SQL injection hacking

•Security countermeasures
Understanding of the different security measures to address the vulnerabilities discovered by the penetration testing.

INTENDED **LEARNING OUTCOMES**

On successful completion of this module a student will be able to:

1.	Plan and design a penetration test in accordance with standards, legal and ethical issues.
2.	Critically discuss and assess the significance of penetration test results and appraise them in the context of issues for the client.
3.	Identify and assess the various methods used to exploit computer security.
4.	Derive and justify countermeasures to computer and network vulnerabilities found as a result of penetration tests.

TEACHING METHODS

The theoretical material will be delivered during the lectures. Speakers from leading security organisations will be invited to present and share their industry experiences with the students. The students are expected to actively participate and prepare for practicals, assessment briefs and other matters relating to the creation of penetration tests and evaluations.
During the practical sessions, students will be asked to carry out penetration tests as well as other practical work (i.e. setting up tools, etc). Synchronous (i.e. in class) and/or asynchronous (i.e. blogs) discussions will take place to further discuss practical findings. As a result of the discussions, additional directed reading may be required.

As this is a skills based course, the assessment is both focused on knowledge content and skills. The content component of the module is mainly assessed in the module examination, whereas the skills and practical understanding of the module content is assessed in the coursework component. Therefore, the coursework assessment component for this module requires that students do work in between taught classes and that this is reviewed before the examination component of the assessment – to that end the students can get feedback on the coursework assessment to contribute to their preparation for the examination assessment component.
Distance learning
The module tutor will deliver live online lectures through Adobe Connect. During the live lectures the participating students will have the opportunity to engage in discussions, present their views and ask questions. The lecture sessions will be recorded and made available to the students through Blackboard. Students who cannot participate in a live lecture will have the opportunity to answer and reflect on guided questions in the subsequent live lectures or participate asynchronously on discussion boards. Where appropriate, students will be also provided with relevant further reading, web links and resources for independent study. Speakers from leading security organizations will be invited, where possible, to deliver invited talks and enhance the students' experience.
Virtual laboratories will be utilized to give the opportunity to students to apply their practical skills. Students will be provided with access to virtual laboratories through which they will be able to complete the practical components of the module. The students will obtain the practical sheets from Blackboard and they are expected to follow the instructions included in the practical sheets to complete the lab work. If students have difficulties with a particular exercise, they are expected to contact the module tutor or post a question on the discussion forum, where the module tutor and/or their peers can provide feedback. Different means of communication will be utilized by the tutor to offer support to the students based on the reported issue, i.e. email, Skype, Adobe Connect, virtual laboratory, etc.
Through the virtual laboratories, the students are expected to apply their theoretical knowledge to solve security problems in a professional and legal way. Feedback to the students will be provided asynchronously through Blackboard. If the need arises, the module tutor will schedule live sessions to provide further feedback to the students.

ASSESSMENT METHODS

This module is assessed through an examination and a report.