MODULE **DESCRIPTOR**

MODULE TITLE	Penetration Testing		
MODULE CODE	CO3517 (L6)	**CREDIT VALUE**	20 / 10 ECTS
SCHOOL	SCHOOL OF SCIENCE		

MODULE **AIMS**

1. To raise awareness of the need for penetration testing.
2. To provide students with the experience of testing a network's security both internally and externally.
3. To develop an understanding of the legal and ethical issues concerning penetration testing.
4. To encourage students to expand their knowledge about network security from published research materials and to conduct independent investigations into network security related areas.

MODULE **CONTENT**

In September 2016, Yahoo confirmed a massive security breach that saw hackers steal personal information for over 500 million accounts. This is an extreme and well publicised case of hacking but it is indicative of the potential problems faced by virtually every organisation that uses a computer network. In order to provide the best possible defence for their networks professionals need to know how to rigorously test their systems both internally and externally, using the methods and the tools that hackers employ.

Introduction to Ethical and Legal hacking

Building a Virtual Test Platform

Internal and External Threats

Network Vulnerabilities

Penetration Testing Methodology and Documentation

Relevant Standards and guidelines for Penetration Testing, e.g. OSSTMM, ISSAF etc.

Passive Information Gathering

Wireless Networks

Black Box versus Full Knowledge Testing

Evaluating and Deploying Appropriate Penetration and Hacking Tools

Emerging technologies and new threats.

INTENDED **LEARNING OUTCOMES**

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

1. Critically evaluate appropriate methodologies for testing networks in both a legal and an ethical manner.
2. Critically review the security of a computer system using an effective approach
3. Communicate solutions to identified security issues in a range of formats appropriate for different levels of organisation and management.

TEACHING METHODS

This module will provide students with the skills and knowledge. It will take the view point, put forward by Paul Midian of Insight Consulting Ltd, that the end point of any penetration test is a report containing details of tests carried out, vulnerabilities and exploits discovered plus recommendations for improving security.

Case studies will be used to develop students understanding and practical skills.

All the practical work involving active penetration testing will take place on isolated virtual networks. At no point will the students deploy penetration techniques on live networks within the university. All assessments will require the students to reflect on both the legal and ethical issues raised by the work they have completed.

Students are expected to be actively engaged in research activities into relevant topics by making full use of external learning resources, such as the Web, magazines, and other professionally published material

ASSESSMENT METHODS

This module is assessed through two Practical Test with write-up.