Module specification

When printed this becomes an uncontrolled document. Please access the Module Directory for the most up to date version by clicking on the following link: Module directory

Module Code	CONL724
Module Title	Ethical Hacking
Level	7
Credit value	15
Faculty	FACE
HECoS Code	100366
Cost Code	GACP

Programmes in which module to be offered

Programme title	Is the module core or option for this programme
MSc Computer Science with Cyber Security	Core

Pre-requisites

None

Breakdown of module hours

Learning and teaching hours	15 hrs
Placement tutor support	0 hrs
Supervised learning e.g. practical classes, workshops	0 hrs
Project supervision (level 6 projects and dissertation modules only)	0 hrs
Total active learning and teaching hours	15 hrs
Placement / work based learning	0 hrs
Guided independent study	135 hrs
Module duration (total hours)	150 hrs

For office use only	
Initial approval date	17/06/21
With effect from date	28/06/21
Date and details of revision	27/06/2024 Programme revalidation
Version number	2

Module aims

The module aims to give students a solid and professional level of competence in the field of ethical hacking, which is predominantly led by the coverage of tools, techniques and systems that allow penetration testing to be carried out on computer systems and networks.

Much of the module material follows the footsteps of a would-be intruder and thus includes coverage of the communication and social side of computer attacks as well as the technological. Having been led to understand how systems, software and devices can be vulnerable to unwanted penetration, students will then investigate countermeasures and organisational strategies to mitigate these risks.

Module Learning Outcomes - at the end of this module, students will be able to:

1	Display a systematic understanding of an extensive range of hacking methods used to compromise computer systems and networks, incorporating current problems and new insights at the forefront of cybersecurity practice.
2	Demonstrate a comprehensive understanding and critical awareness of security vulnerabilities by using advanced tools and techniques to identify, analyse, and evaluate security risks.
3	Exhibit self-direction and originality in identifying, selecting, and planning sophisticated procedures and countermeasures to defend against and minimize computer security attacks.
4	Make and justify decisions on cybersecurity interventions, showing awareness of ethical, professional, and legal issues connected with hacking.
5	Continuously advance your knowledge and skills in cybersecurity, demonstrating the ability to learn independently and develop new competencies at a high level.

Assessment

This section outlines the type of assessment task the student will be expected to complete as part of the module. More details will be made available in the relevant academic year module handbook.

Indicative Assessment Tasks:

Assessment 1 will consist of an in-depth analysis of a cyber-attack from recent years. This will see students explore both the technical and non-technical elements of the attack along with the impacts of the attack in all societal areas. This assessment will have a word count of 2250 +/- 10%.
Further understanding on in-class techniques and concepts will be assessed using an in-class test.

Assessment number	Learning Outcomes to be met	Type of assessment	Weighting (%)
1	1,2,5	Coursework	70%
2	3,4	In-class test	30%

Derogations

None

Learning and Teaching Strategies

The overall learning and teaching strategy is one of guided independent study requiring ongoing student engagement. Online material will provide the foundation of the learning resources, requiring the students to log in and engage regularly throughout the eight weeks of the module. There will be a mix of suggested readings, discussions and interactive content containing embedded digital media and self-checks for students to complete as they work through the material and undertake the assessment tasks. A range of digital tools via the virtual learning environment and additional sources of reading will also be utilised to accommodate learning styles. There is access to a helpline for additional support and chat facilities through Canvas for messaging and responding.

Indicative Syllabus Outline

- Software tools and practical hacking methods and techniques.
- Protocols, network communication, Internet & web-based hacking attacks and Blended hacking threats and exploitations.
- Cloud insecurity: hacking the cloud and hacking mobile devices.
- Phishing ecosystem & hacking.
- Social engineering hacking techniques: influencing and manipulating victims.
- Integrated hacking attacks based on complex approaches, processes & systems.
- Hacking: Ethical, professional and legal issues.

Indicative Bibliography:

Please note the essential reads and other indicative reading are subject to annual review and update.

Essential Reads

License to access SudoCyber online platform.

Other indicative reading

C. Easttom, *Computer Security Fundamentals*, 3rd ed. London, U.K.: Pearson Education, 2016.

P. Engebretson, *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy*, 2nd ed. Waltham, MA: Syngress, 2013.

S. McClure, J. Scambray, and G. Kurtz, *Hacking Exposed: Network Security Secrets and Solutions*, 7th ed. New York, NY: McGraw-Hill/Osborne, 2012.

.