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	COM576
Module Title	Ethical Hacking
Level	5
Credit value	20
Faculty	FACE
HECoS Code	100376
Cost Code	GACP

Programmes in which module to be offered

Programme title	Is the module core or option for this programme
BSc (Hons) Cyber Security	Core
BSc (Hons) Cyber Security with Industrial Placement	Core
Stand-alone module aligned to BSc (Hons) Cyber Security for QA and assessment	Option

Pre-requisites

N/A

Breakdown of module hours

Learning and teaching hours	15 hrs
Placement tutor support	0 hrs
Supervised learning e.g. practical classes, workshops	15 hrs
Project supervision (level 6 projects and dissertation modules only)	0 hrs
Total active learning and teaching hours	**30** hrs
Placement / work based learning	0 hrs
Guided independent study	170 hrs
Module duration (total hours)	**200** hrs

For office use only	
Initial approval date	08/11/2023
With effect from date	Sept 2025

For office use only	
Date and details of revision	
Version number	1

Module aims

This module aims to provide students with an understanding of the principles, techniques and tools used in the field of Ethical Hacking allowing them to develop a proactive approach to securing digital assets. The primary aim of such a module is to equip students with the necessary knowledge and skills to identify and address vulnerabilities in computer systems and networks. By adopting the perspective of an ethical hacker, students are exposed to numerous relevant methodologies, tools and techniques employed by potential attackers, students are better prepared to identify vulnerabilities, exploit them responsibly, and propose effective security measures.

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

1	Characterise the principles, concepts, and legal frameworks that govern ethical hacking practices.
2	Evaluate and interpret different hacking techniques, tools, and methodologies used in penetration testing.
3	Critically evaluate the effectiveness of different security measures, countermeasures, and ethical hacking methodologies.
4	Adhere to the suitable standards of ethics and professionalism within the field.

Assessment

Indicative Assessment Tasks:

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.

The assessment strategy for this module encompasses both theoretical understanding and practical skill development. The coursework assignments aim to reinforce the acquired knowledge and showcase the students' comprehension of ethical hacking principles, concepts, and legal frameworks, as well as their ability to evaluate ethical hacking tools, techniques, and methodologies. These assignments may include tasks such as preparing reports, maintaining journals, or conducting simulated analyses.

Students will have a two-hour in-class test. This test will assess students' theoretical knowledge of ethical hacking, requiring them to demonstrate their understanding of key concepts, terminology, and principles within a specified timeframe. The test will provide an opportunity for students to showcase their theoretical knowledge and comprehension of the subject matter. In-Class test to align to industry-level certification.

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

Derogations

None

Learning and Teaching Strategies

Aligned with the principles of the Active Learning Framework (ALF), the module will incorporate a blended digital approach utilising a Virtual Learning Environment (VLE). These resources may include a range of content such as first and third-party tutorials, instructional videos, supplementary files, online activities, and other relevant materials to enhance their learning experience

The learning methodology for this module adopts a blended approach, integrating both theoretical and practical components. Students will engage in a series of workshops and practical sessions, which combine theory-based lectures with hands-on activities. These activities will involve students working on simulated problems and developing solutions.

Indicative Syllabus Outline

Indicative syllabus includes topic areas that may include:

- Ethical Hacking Fundamentals
- Information Security Threats
- Password Cracking Techniques
- Social Engineering Techniques
- Network Level Attacks
- Web Application Attacks
- Wireless Attacks
- Mobile, IoT & OT Attacks
- Cloud Computing Threats
- Penetration Testing

Indicative Bibliography:

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

Essential Reads

N/A.

Other indicative reading

D. Graham, *Ethical Hacking: A Hands-On Introduction to Breaking in.* Daniel Graham., No Starch Press, 2021

Z. Sabih, *Learn Ethical Hacking from Scratch,* Packt Publishing, 2018.