Module Specification

Module Summary Information

1	**Module Title**	Ethical Hacking
2	**Module Credits**	20
3	**Module Level**	6
4	**Module Code**	CMP6176

5	**Module Overview**

The module provides you with an opportunity to learn and critically reflect on the skills of Ethical Hacking and information security within a global context. This module builds on the knowledge and underpinning theory from the networking modules and reviews the requirements for a secure network communication system.

The module consists of:

- Subject specific lectures/workshops to introduce knowledge and skills relevant to network and information security.
- Lectures/workshops to introduce principles and techniques for secure communication within a network and ensuring security of data in transit.
- Global view on information security and the changing requirements for information and data communication security.

Relationship to programme philosophy:

This module provides an opportunity for the student to develop knowledge and skills, which will contribute to the acquisition of key BCU graduate attributes; creative problem solvers, global outlook, enterprising, professional and work ready. In the context of the information and data communication industries and at this academic level, this means an ability to: respond to a critical brief to find practical solutions to problems; evaluate and respond to the opportunities and challenges of interdisciplinary approaches to the realisation of a task; respond flexibly and imaginatively to a set, or group-determined brief within a fixed timescale.

6	**Indicative Content**

It is expected that this module will develop the following areas:

- Ethical hacking methodology
- Pre-attach reconnaissance
- How to fingerprint and enumerate targets
- How to perform network scanning and sniffing
- How to perform system vulnerability assessments
- How to create attack vectors
- Web attacks such as XSS, directory traversals and SQL injection
- How to plan and initiate cyber-attacks in order to prevent them
- How to think like a criminal hacker in order to defeat them

7	Module Learning Outcomes On successful completion of the module, students will be able to:	
	1	Critically evaluate the requirements for penetration testing and ethical hacking.
	2	Design security assessment experiments to expose security vulnerabilities.
	3	Critically evaluate resulting data from security assessment experiments to recommend remedial actions.
	4	Critically appraise the role of security testing within the wider context of continuous security improvements to the information assurance processes within an organisation.

8	Module Assessment			
Learning Outcome				
	Coursework	Exam	In-Person	
1-4	X			

9	Breakdown Learning and Teaching Activities	
Learning Activities		Hours
Scheduled Learning (SL) includes lectures, practical classes and workshops, peer group learning, Graduate+, as specified in timetable		48
Directed Learning (DL) includes placements, work-based learning, external visits, on-line activity, Graduate+, peer learning, as directed on VLE		90
Private Study (PS) includes preparation for exams		62
Total Study Hours:		200