MODULE DESCRIPTOR

Module Title

Ethical Hacking

Reference	CM3146	Version	1
Created	November 2023	SCQF Level	SCQF 9
Approved	May 2019	SCQF Points	15
Amended	July 2022	ECTS Points	7.5

Aims of Module

This module aims to provide students with advanced ethical hacking skills, tools, and ethical frameworks, equipping them to safeguard digital landscapes and fortify systems against potential threats.

Learning Outcomes for Module

On completion of this module, students are expected to be able to:

1	Demonstrate a comprehensive understanding of ethical hacking methodologies.
2	Demonstrate proficiency in using advanced tools and techniques to identify vulnerabilities in diverse systems.
3	Design and implement countermeasures to protect systems, proactively addressing identified weaknesses.
4	Demonstrate proficiency in generating articulate and comprehensive reports for ethical hacking assessments.

Indicative Module Content

Ethical Hacking: hacking as a career, the CEH methodology: Reconnaissance, Scanning, Gaining access, Maintaining access, and Covering tracks; Assessing Network and wireless Security; Assessing Hosts and Applications security; Hardware Hacking; Social Engineering; System Security and Hardening; Red Team/Blue Team; Black/Grey/White Hats; Vulnerability Scanning with a variety of tools like Nmap, Metasploit Framework, Burp Suite, OWASP Zap, Aircrack-ng, Hping, SQLMap, and John the Ripper; Standards and Best Practice Guides: ISO 27001, ISO 27005, ISO 27014. Cyber Security Law and Ethics in the context of ethical hacking; Latest security threats and trends.

Module Delivery

Lectures introduce and illustrate key concepts, while practical skills are honed through a series of laboratory exercises.

Module Ref:	CM3146 v1

Indicative Student Workload	Full Time	Part Time
Contact Hours	30	N/A
Non-Contact Hours	120	N/A
Placement/Work-Based Learning Experience [Notional] Hours	N/A	N/A
TOTAL	150	N/A
Actual Placement hours for professional, statutory or regulatory body		

ASSESSMENT PLAN

If a major/minor model is used and box is ticked, % weightings below are indicative only.

Component 1

Type:	Coursework	Weighting:	100%	Outcomes Assessed:	1, 2, 3, 4
Description:	Coursework consisting of both practical and theoretical elements covering all learning outcomes of the module.				

MODULE PERFORMANCE DESCRIPTOR

Explanatory Text

The calculation of the overall grade for this module is based on 100% weighing of Component 1. An overall minimum grade D is required to pass the module.

Module Grade	Minimum Requirements to achieve Module Grade:
A	The student needs to achieve an A in Component 1.
B	The student needs to achieve a B in Component 1.
C	The student needs to achieve a C in Component 1.
D	The student needs to achieve a D in Component 1.
E	The student needs to achieve an E in Component 1.
F	The student needs to achieve an F in Component 1.
NS	Non-submission of work by published deadline or non-attendance for examination

Module Requirements

Prerequisites for Module	CM1131 Cyber Security Fundamentals CM1132 Computing Network Fundamentals
Corequisites for module	None.
Precluded Modules	None.

INDICATIVE BIBLIOGRAPHY

1	Wilson, R. (2022). Hands-on ethical hacking and network defense. Cengage Learning.
2	Walker, M. (2022). CEH Certified Ethical Hacker Bundle. McGraw-Hill Education.
3	Singh, G. D. (2022). The Ultimate Kali Linux Book: Perform Advanced Penetration Testing Using Nmap, Metasploit, Aircrack-ng, and Empire. Packt Publishing Ltd.
4	Graham, D. G. (2021). Ethical hacking: A hands-on introduction to breaking in. No Starch Press.
5	Follis, L., & Fish, A. (2020). Hacker states. MIT Press.
6	Maurushat, A. (2019). Ethical hacking. University of Ottawa Press.