MODULE DESCRIPTOR

Module Title

Ethical Hacking

Reference	CM3109	Version	3
Created	June 2022	SCQF Level	SCQF 9
Approved	May 2019	SCQF Points	15
Amended	July 2022	ECTS Points	7.5

Aims of Module

To provide students with the knowledge and skills to identify network security threats and implement countermeasures within an IT infrastructure.

Learning Outcomes for Module

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

1	Demonstrate understanding of network protocol vulnerabilities and the security of an IT infrastructure.
2	Design and implement countermeasures to protect a network from unauthorised network access.
3	Demonstrate understanding of the ethical and legal policies of network security testing.
4	Implement appropriate ethical hacking techniques to carry out a network security test.
5	Demonstrate an awareness and ability to analyse and perform network security testing procedures on an IT infrastructure to identify vulnerabilities.

Indicative Module Content

Ethical Hacking: hacking as a career, the CEH methodology: Reconnaissance, Scanning, Gaining access, Maintaining access, and Covering tracks. Firewalls, IDS/IPS & Honeypots: screening filters, application-layer and proxy firewalls. Stateful and stateless firewalls. Network & Wireless Security: review of some TCP/IP stack protocols and their known vulnerabilities. Wired Equivalent Privacy (WEP)vulnerabilities, Wireless Protected Access (WPA/WPA2) and IEEE802.11i Cyber Security law and Ethics. Network scanning techniques. Hardware Hacking. Vulnerability Scanning. Footprinting & Social Engineering. Red Team/Blue Team. Black/Grey/White Hats. Standards and Best Practice Guides: ISO 27001, ISO 27005, ISO 27014.

Module Delivery

This module is taught using a structured programme of lectures, lab sessions and student centred learning.

Module Ref:	CM3109 v3

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, 5
Description:	A practical coursework assessment that involves identifying security threats and implementing countermeasures on a test host.				

MODULE PERFORMANCE DESCRIPTOR

Explanatory Text

The calculation of the overall grade for this module is based on 100% weighing of C1. 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 C1.
B	The student needs to achieve a B in C1.
C	The student needs to achieve a C in C1.
D	The student needs to achieve a D in C1.
E	The student needs to achieve an E in C1.
F	The student needs to achieve an F in C1.
NS	Non-submission of work by published deadline or non-attendance for examination

Module Requirements

Prerequisites for Module	None.
Corequisites for module	None.
Precluded Modules	None.

INDICATIVE BIBLIOGRAPHY

1. McNAB, C., 2016. Network Security Assessment. 3rd ed. O'Reilly.
2. WILHELM, T., 2013. Professional Penetration Testing. 2nd ed. Syngress.
3. COLEMAN, D.D. et al., 2016. CWSP Certified Wireless Security Professional Official Study Guide: Exam PWO-204(CWNP Official Study Guides). 2nd ed. John Wiley & Sons.
4. KIM, P., 2015. The Hacker Playbook 2: Practical Guide To Penetration Testing. CreateSpace Independent Publishing Platform.
5. WEIDMAN, G., 2014. Penetration Testing: A Hands-On Introduction to Hacking. No Starch Press.
6. KOLOKITHAS, A., 2015. Hacking Wireless Networks - The ultimate hands-on guide. CreateSpace Independent Publishing Platform.
7. SEITZ, J., 2014. Black Hat Python: Python Programming for Hackers and Pentesters. No Starch Press.
8. REGALADO, D. et al., 2015. Gray Hat Hacking The Ethical Hacker's Handbook. 4th ed. McGraw-Hill Osborne.