MODULE DESCRIPTOR

Module Title

Security Testing

Reference	CMM518	Version	3
Created	April 2022	SCQF Level	SCQF 11
Approved	August 2017	SCQF Points	15
Amended	July 2022	ECTS Points	7.5

Aims of Module

To enable students to apply strategies for identifying security vulnerabilities in systems and networks.

Learning Outcomes for Module

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

1	Analyse, evaluate and discuss the threats to computer systems.
2	Explore and analyse the technical as well as non-technical vulnerabilities of computer systems.
3	Apply relevant penetration testing tools and methods to exploit, document and report on the vulnerabilities.
4	Evaluate and discuss the standards and the ethical issues pertaining to performing security testing.

Indicative Module Content

Ethics and hacking. Methodologies and Frameworks (e.g. 27000 series and Common Criteria, Ethical hacking framework and offensive security). Information gathering, Footprinting, Scanning, Enumeration, System Hacking. Vulnerability identification and exploitation. Pre vs Post gain attacks. Evasion Techniques. Social Engineering. Physical Security. MITRE ATT&CK Framework. System and network penetration testing with Kali Linux Reporting results. Audit methodologies, processes and techniques.

Module Delivery

Key concepts are introduced and illustrated through lectures and directed reading. The understanding of students is tested and further enhanced through lab sessions.

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

Module Ref:	CMM518 v3

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:	Students will prepare a security test report after applying security test methods to a given scenario.				

MODULE PERFORMANCE DESCRIPTOR

Explanatory Text

The calculation of the overall grade for this module is based on 100% weighting of C1. An overall minimum grade of D is required to pass this 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	Allsopp, W. (2017). Advanced Penetration Testing: Hacking the World's Most Secure Networks. John Wiley & Sons.
2	Nastase, R. (2018). Hacking with Kali Linux: A step by step guide for you to learn the basics of cybersecurity and hacking. Elsevier.
3	Peter, K. (2018). The Hacker Playbook 3: Practical Guide To Penetration Testing. Security planet LLC.
4	Anderson, R. (2020). Security engineering: a guide to building dependable distributed systems. John Wiley & Sons.
5	Messier, R. (2021). CEH v11 Certified Ethical Hacker Study Guide. John Wiley & Sons.