MODULE DESCRIPTOR

Module Title

Cyber Security Fundamentals

Reference	CM1131	Version	1
Created	November 2023	SCQF Level	SCQF 7
Approved	April 2024	SCQF Points	15
Amended		ECTS Points	7.5

Aims of Module

This module aims to provide students with a strong foundation in key concepts, enabling them to identify attack patterns, apply attack modelling techniques, and develop practical skills in the ethical use of adversary tools, preparing them for advanced studies and empowering them to address Cyber Security challenges responsibly and effectively.

Learning Outcomes for Module

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

1 Acquire foundational knowledge of key cyber security concepts.

2 Recognise different stages and patterns of common cyber attacks.

3 Describe various cyber-attack modelling methods, encompassing attack graphs, attack trees, fault trees, MITRE ATT&CK, and the Cyber Kill Chain

4 Apply tools, techniques, and adversary procedures in practical cyber security scenarios.

5 Recognise the importance of legal, ethical, and methodical conduct in applying cybersecurity measures.

Indicative Module Content

Security principles and practices, CIA, risks, threats, vulnerabilities, human factors and security usability, system security, software security, application security, data security, network security, and platform security, fundamentals of security operations and incident management, fundamentals of digital forensics, cyber-attacks, and defense methods, common cyber-attack modelling methods (attack graphs, trees, fault trees, MITRE ATT&CK, and the Cyber Kill Chain), fundamentals of security testing and validation. Cyber Landscape and Automation: Understanding the cyber landscape, Linux command line, Bash scripting, and automation (e.g. Python). Legal and ethical considerations.

Module Delivery

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

Indicative Student Workload	Full Time	Part Time
Contact Hours	40	N/A
Non-Contact Hours	110	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:	The coursework assesses students' proficiency in foundational cybersecurity concepts, practical skills, ethics, and the application of security principles across diverse contexts, demonstrating their understanding and adaptability in the dynamic digital security landscape.				

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 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 Diogenes, Y., & Ozkaya, E. (2022). Cybersecurity?Attack and Defense Strategies: Improve your security posture to mitigate risks and prevent attackers from infiltrating your system. Packt Publishing Ltd.

2 Brooks, C. J., Grow, C., Craig Jr, P. A., & Short, D. (2018). Cybersecurity essentials. John Wiley & Sons.

3 Stallings, W. (2021). Network Security Essentials. Pearson.

4 Rush, G. (2023). Introduction to Cyber Security Operations and the Incident Management Lifecycle. Wiley.

5 Erickson, J. (2020). Hacking: The Art of Exploitation. No Starch Press.

6 Ransome, J., & Misra, A. (2018). Core software security: Security at the source. CRC Press.