MODULE DESCRIPTOR

Module Title

Securing Networks

Reference	CM4102	Version	5
Created	April 2023	SCQF Level	SCQF 10
Approved	July 2016	SCQF Points	15
Amended	August 2023	ECTS Points	7.5

Aims of Module

The module curriculum emphasises core security technologies, the installation, troubleshooting and monitoring of network devices to maintain integrity, confidentiality and availability of data and devices, and competency in the technologies that are used to secure network infrastructure.

Learning Outcomes for Module

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

1	Critique methodologies that can be used to evaluate the security of computer networks.
2	Illustrate the use of appropriate tools and techniques to protect networks against security threats.
3	Examine social and ethical issues arising through the operation of network security technologies.
4	Operate security solutions to effectively protect against network-based attacks.

Indicative Module Content

Risk Assessment, Incident analysis and threat modelling. Network Security Monitoring: SIEM, traffic monitoring. Attacks and Mitigation at Layer 2 (MAC/ARP spoofing, overflow attacks, VLAN storms and STP attacks). Intrusion Detection and Prevention Systems (IDS/IPS): IDS/IPS signatures and alarms, signature and anomaly-based detection, honeypots. Firewall Technologies: DMZ, Access Control Lists (ACLs), Zone-Based Policies. TCP/IP protocol stack: Security at the Application, Transport, Internet and Link layers.

Module Delivery

The module is based on a series of lectures supplemented by lab work on both simulated and real network equipment.

Module Ref:	CM4102 v5

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:	A coursework task incorporating a substantive practical component and a written report in which students must showcase their proficiency in secure network management for a given scenario.				

MODULE PERFORMANCE DESCRIPTOR

Explanatory Text

The calculation of the overall grade for this module is based on 100% weighting of component 1 (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 an B in C1.
C	The student needs to achieve an C in C1.
D	The student needs to achieve an 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	CM1103 Computer Systems and Networking, or equivalent. CM2103 Routing and Switching, or equivalent.
Corequisites for module	None.
Precluded Modules	None.

INDICATIVE BIBLIOGRAPHY

1	BARKER and MORRIS, 2012. CCNA Security Official Exam Certification Guide (Exam 640-554), Cisco Press.
2	KIZZA, 2015. Guide to Computer Network Security (Computer Communications and Networks). Springer.
3	STALLINGS, 2013. Network Security Essentials: Applications and Standards, Stallings. Pearson.
4	Chris McNab, 2016. Network Security Assessment: Know Your Network. 3 Edition. O'Reilly Media.
5	This module uses some of the material from CISCO CCNA (Cisco Certified Networking Associate) Security Curriculum. The material for the course is provided in the form of adapted lectures, web?based learning and assessment mechanisms, as well as practical lab activities.