MODULE DESCRIPTOR

Module Title

Securing Networks

Reference	CM4102	Version	2
Created	April 2017	SCQF Level	SCQF 10
Approved	July 2016	SCQF Points	15
Amended	August 2017	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	Demonstrate an understanding of the current technologies and tools (ASA, VPN, AAA & Firewalls etc.) available to a Network Security Professional when protecting routed and switched networks.
2	Critically appraise the choice of methodologies that can be used to securely interconnect and protect network systems. Analyse the choice of technology, its application and success.
3	Recognise and discuss the legal and ethical issues arising through the operation of network security technologies.
4	Configure, deploy, secure, monitor and troubleshoot computer networks to meet business goals.

Indicative Module Content

Securing Administrative Access: SSH, AAA, RADIUS, TACACS+ Security Technologies: Zone Based Firewalls, Demilitarised Zones. Threat Detection: Intrusion Detection System (IDS), Intrusion Prevention Systems (IPS) Securing Communications: Remote Access and Site to Site VPNs. Switch Security: Secure Trunks, Port Security, PortFast, BPDU Guard. Security Appliances: Configuration, Operation, Troubleshooting.

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 v2

Indicative Student Workload	Full Time	Part Time
Contact Hours	33	N/A
Non-Contact Hours	117	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:	Examination	Weighting:	50%	Outcomes Assessed:	1, 3
Description:	Exam worth 50% of total module assessment.				

Component 2

Type:	Practical Exam	Weighting:	50%	Outcomes Assessed:	2, 4
Description:	Practical Exam worth 50% of total module assessment.				

MODULE PERFORMANCE DESCRIPTOR

Explanatory Text

The calculation of the overall grade for this module is based on 50% weighting of C1 and 50% weighting of C2. An overall minimum grade D is required to pass the module.

Examination:

	Practical Exam: A	B	C	D	E	F	NS
A	A	A	B	B	C	E	
B	A	B	B	C	C	E	
C	B	B	C	C	D	E	
D	B	C	C	D	D	E	
E	C	C	D	D	E	E	
F	E	E	E	E	E	F	

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.

Module Ref:	CM4102 v2

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.