This Version is No Longer Current
The latest version of this module is available here

MODULE DESCRIPTOR

Module Title

Network Security

Reference	CMM528	Version	5
Created	April 2018	SCQF Level	SCQF 11
Approved	May 2013	SCQF Points	15
Amended	June 2018	ECTS Points	7.5

Aims of Module

To provide the student with the ability to identify and analyse network security threats. To provide students with the necessary skills to design and manage secure networks.

Learning Outcomes for Module

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

1	Understand and explain the principles and theory of Secure Network Design.
2	Analyse and critically appraise the technologies that can be used to protect LANs against modern security threats.
3	Evaluate the technologies that can be used to securely interconnect network systems.
4	Utilise appropriate methodologies to build a secure network topology incorporating remote access, authentication and protection to mitigate network attacks.

Indicative Module Content

Managing a Secure Network: Principles of Secure Network Design, Security Policy implementation. Securing Network Devices: Secure administrative access to devices, Secure management, monitoring and resiliency (syslog, SNMP, NTP), Security audit tools and auto secure mechanisms. Securing Local Area Networks: Endpoint vulnerabilities and protective measures, Layer 2 vulnerabilities (MAC spoofing and overflow attacks, VLAN storms and STP attacks), BPDU Guard and VLAN Trunk security. Firewall Technologies: Standard and Extended Access Control Lists (ACLs), Dynamic and reflexive ACLs, Zone-Base Policy Firewalls to mitigate network attacks. Intrusion Detection and Prevention Systems: Functions and operations of Intrusion Detection/Prevention Systems, IDS/IPS signatures and alarms. Intrusion analysis, monitoring and logging (e.g., syslog, wireshark) Virtual Private Networks: Remote access and site-to-site VPNs, VPN GRE Tunnels, IPSec VPNS (AH, ESP). Wireless Security.

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.

Module Ref:	CMM528 v5

Indicative Student Workload	Full Time	Part Time
Contact Hours	44	44
Non-Contact Hours	106	106
Placement/Work-Based Learning Experience [Notional] Hours	N/A	N/A
TOTAL	150	150
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:	50%	Outcomes Assessed:	1, 2, 3
Description:	Computer-based assessment				

Component 2

Type:	Practical Exam	Weighting:	50%	Outcomes Assessed:	4
Description:	Hands-on lab exercises				

MODULE PERFORMANCE DESCRIPTOR

Explanatory Text

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

		Practical Exam:						
		A	**B**	**C**	**D**	**E**	**F**	**NS**
Practical Exam:	**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	CMM516 or equivalent
Corequisites for module	None.
Precluded Modules	None.

Module Ref:	CMM528 v5

INDICATIVE BIBLIOGRAPHY

1	McNAB,C., 2016. Network Security Assessment. O'Reilly.3rd Ed.
2	BIJALWAN, A., 2022. Network forensics: privacy and security. Chapman & Hall/CRC Press.
3	MURDOCH, D., 2019. Blue Team Handbook: SOC, SIEM, and Threat Hunting (V1.02): A Condensed Guide for the Security Operations Team and Threat Hunter. Independently published.
4	KIZZA, 2017. Guide to Computer Network Security. Springer.
5	STALLINGS, 2017. Network Security Essentials: Applications and Standards. Pearson
6	BHUYAN, M., BHATTACHARYYA, D., and KALITA, J., 2017. Network traffic anomaly detection and prevention: concepts, techniques, and tools. Springer.