Module specification

When printed this becomes an uncontrolled document. Please access the Module Directory for the most up to date version by clicking on the following link: Module directory

Module Code	COM756
Module Title	Networking and Defensive Security
Level	7
Credit value	20
Faculty	FACE
HECoS Code	100376
Cost Code	GACP

Programmes in which module to be offered

Programme title	Is the module core or option for this programme
MSc (Hons) Cyber Security	Core
MSc (Hons) Cyber Security with Advanced Practice	Core

Pre-requisites

N/A

Breakdown of module hours

Learning and teaching hours	10 hrs
Placement tutor support	0 hrs
Supervised learning e.g. practical classes, workshops	11 hrs
Project supervision (level 6 projects and dissertation modules only)	0 hrs
Total active learning and teaching hours	**21** hrs
Placement / work based learning	0 hrs
Guided independent study	179 hrs
Module duration (total hours)	**200** hrs

For office use only	
Initial approval date	08/11/2023

For office use only	
With effect from date	Sept 2024
Date and details of revision	
Version number	1

Module aims

This module aims to provide students with a comprehensive understanding of networking principles and the implementation of defensive security measures. Students will learn how to design, implement, and maintain secure network architectures while protecting systems, data, and networks from potential threats and attacks. A range of topics will be covered, including networking concepts, network topologies, security threats and attacks, defensive security measures, secure network configuration and management, data and system protection, and network security policies and compliance.

The module emphasizes the importance of a layered defence strategy, incorporating network security controls such as firewalls, intrusion detection systems, and encryption techniques. Additionally, students will learn about network monitoring, incident response, access controls, authentication mechanisms, and compliance with regulatory standards.

Module Learning Outcomes - at the end of this module, students will be able to:

1	Apply advanced networking concepts and protocols.
2	Critically analyse and evaluate potential network security risks and vulnerabilities.
3	Implement defensive security measures to protect and monitor networks and systems.
4	Facilitate the implementation of secure network architectures and access controls.

Assessment

Indicative Assessment Tasks:
This section outlines the type of assessment task the student will be expected to complete as part of the module. More details will be made available in the relevant academic year module handbook.

The assessment strategy for this module is based on a portfolio approach. The portfolio assessment allows students to demonstrate their understanding, skills, and application of knowledge related to networking and defensive security in a comprehensive and holistic manner.
The following are possible portfolio tasks:

- Conduct a comprehensive network security analysis, evaluating risks and vulnerabilities, and proposing defensive measures.
- Design and implement secure network architectures, considering scalability and access controls.
- Perform penetration testing, prioritize vulnerabilities, and propose remediation strategies.
- Evaluate the effectiveness of implemented security measures and suggest improvements.

- Create network security policies aligned with industry standards and regulatory requirements.
- Analyse case studies of network security breaches and propose preventive measures.
- Research and assess emerging networking concepts and their security implications.
- Participate in team-based network security simulations to practice defensive measures and incident response.

Assessment number	Learning Outcomes to be met	Type of assessment	Weighting (%)
1	1,2,3,4	Portfolio	100%

Derogations

None

Learning and Teaching Strategies

Aligned with the principles of the Active Learning Framework (ALF), the module will incorporate a blended digital approach utilising a Virtual Learning Environment (VLE). These resources may include a range of content such as first and third-party tutorials, instructional videos, supplementary files, online activities, and other relevant materials to enhance their learning experience.

Indicative Syllabus Outline

Indicative syllabus includes topic areas that may include:

- Network Security best practices
- Common network threats and vulnerabilities
- Network Defence Strategies
- Secure Network Protocols and Services
- Wireless Network Security
- Cloud Network Security concepts
- Network Security Best Practices

Indicative Bibliography:

Please note the essential reads and other indicative reading are subject to annual review and update.

Essential Reads

W. Stallings, *Network Security Essentials: Applications and Standards* (6th ed.). Harlow, UK: Pearson, 2017.

Other indicative reading

W.R Cheswick & S.M Bellovin, *Firewalls and Internet Security: Repelling the Wily Hacker* (2nd ed.). Reading, MA: Addison-Wesley, 2003.

C. Sanders, *Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems* (3rd ed.). San Francisco, CA: No Starch Press, 2017.

T. Mather, S. Kumaraswamy, & S. Latif, *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance.* Sebastopol, CA: O'Reilly Media, 2009.