University of the West of Scotland

Module Descriptor

Session: 2024/25

Title of Module: Advanced Network Security			
Code: COMP11076	**SCQF Level: 11 (Scottish Credit and Qualifications Framework)**	**Credit Points: 10**	**ECTS: 5 (European Credit Transfer Scheme)**
School:	School of Computing, Engineering and Physical Sciences		
Module Co-ordinator:	Althaff Mohideen		

Summary of Module

Security of computer networks has been a primary issue for the management of information systems used by organisations of all sizes ranging from start-ups to large enterprises. Often computer networks are compromised due to the use of inappropriate security and management measures to detect malicious access privilege escalation, monitor network traffic and services, ensure confidentiality and privacy of the network, prevent network attacks, and build resilience to modern day cyber attacks.

This module addresses the pivotal concepts of network security within the context of network and data management for trusted and untrusted computer networks. It is designed to cover core methodologies, algorithms and tools for network security, providing the essential hands-on experience for designing and managing secure, privacy-aware, and resilient computer networks.

This module has been specifically designed considering the UWS Graduate Attributes of Universal, Work ready, and Successful.

Module Delivery Method

Face-To-Face	Blended	Fully Online	HybridC	Hybrid 0	Work-Based Learning
☐	☒	☐	☐	☐	☐

See Guidance Note for details.

Campus(es) for Module Delivery

The module will **normally** be offered on the following campuses / or by Distance/Online Learning: (Provided viable student numbers permit) (tick as appropriate)

Paisley:	Ayr:	Dumfries:	Lanarkshire:	London:	Distance/Online Learning:	Other:
☐	☐	☐	☒	☒	☐	Add name

Term(s) for Module Delivery					
(Provided viable student numbers permit).					
Term 1	☐	Term 2	☒	Term 3	☐

Learning Outcomes: (maximum of 5 statements) **These should take cognisance of the SCQF level descriptors and be at the appropriate level for the module.** At the end of this module the student will be able to:	
L1	Demonstrate extensive knowledge of the core theories, concepts and principles of secure network design, network specific attacks and attack mechanisms.
L2	Develop skills to analyse and critically evaluate security of networked systems and recommend relevant technical and management improvements or solutions.

Employability Skills and Personal Development Planning (PDP) Skills	
SCQF Headings	During completion of this module, there will be an opportunity to achieve core skills in:
Knowledge and Understanding (K and U)	SCQF Level **11** Students will learn comprehensive knowledge of advanced network security. Students are expected to be familiar with the key technologies and techniques and their application in practice.
Practice: Applied Knowledge and Understanding	SCQF Level **11** Students will gain in-depth understanding and critical awareness of knowledge of advanced network security, and apply this in planning, implementing, configuration and testing of the security state of the test environment. They will also develop capability to apply a range of specialised research skills and relevant tools and software for their written assignment and lab tasks.
Generic Cognitive skills	SCQF Level **11** To complete their written reports and laboratory tasks, students will first build skills to integrate information and apply knowledge from various sources including technology advances informed by research and industry
Communication, ICT and Numeracy Skills	SCQF Level **11** Working in interacting groups, students will develop communication skills as well as the ability to write technical reports and documentation.

Autonomy, Accountability and Working with others	SCQF Level **11** Each student will generate a comprehensive technical report summarizing the finding for a given relevant topic on computer networks.	
Pre-requisites:	Before undertaking this module the student should have undertaken the following:	
	Module Code:	**Module Title:**
	Other:	
Co-requisites	**Module Code:**	**Module Title:**

*Indicates that module descriptor is not published.

Learning and Teaching	
In line with current learning and teaching principles, a 20-credit module includes 200 learning hours, normally including a minimum of 36 contact hours and maximum of 48 contact hours.	
Learning Activities During completion of this module, the learning activities undertaken to achieve the module learning outcomes are stated below:	**Student Learning Hours** (Normally totalling 200 hours): (Note: Learning hours include both contact hours and hours spent on other learning activities)
Lecture/Core Content Delivery	10
Laboratory/Practical Demonstration/Workshop	10
Independent Study	80
	100 Hours Total
****Indicative Resources: (eg. Core text, journals, internet access)**	

The following materials form essential underpinning for the module content and ultimately for the learning outcomes: Diogenes, Y and Ozkaya, E. (2018) Cybersecurity – Attack and Defense Strategies: Infrastructure security withRed Team and Blue Team tactics. Packt Publishing McNab, C. (2016) 3rd Ed. Network Security Assessment: Know Your Network. O'Reilly Media Allsopp, W. (2017) Advanced Penetration Testing: Hacking the World's Most Secure Networks. John Wiley &Sons Please ensure the list is kept short and current. Essential resources should be included, broader resources should be kept for module handbooks / Aula VLE. Resources should be listed in Right Harvard referencing style or agreed professional body deviation and in alphabetical order.
(**N.B. Although reading lists should include current publications, students are advised (particularly for material marked with an asterisk*) to wait until the start of session for confirmation of the most up-to-date material)
Attendance and Engagement Requirements
In line with the Student Attendance and Engagement Procedure: Students are academically engaged if they are regularly attending and participating in timetabled on-campus and online teaching sessions, asynchronous online learning activities, course-related learning resources, and complete assessments and submit these on time. For the purposes of this module, academic engagement equates to the following:

Equality and Diversity
The University's Equality, Diversity and Human Rights Procedure can be accessed at the following link: UWS Equality, Diversity and Human Rights Code. Please ensure any specific requirements are detailed in this section. Module Co-ordinators should consider the accessibility of their module for groups with protected characteristics..
(N.B. Every effort will be made by the University to accommodate any equality and diversity issues brought to the attention of the School)

Supplemental Information

Divisional Programme Board	Computing

Assessment Results (Pass/Fail)	Yes ☐No ☒
School Assessment Board	Business and Applied Computing
Moderator	Steve Eager
External Examiner	N Coull
Accreditation Details	e.g. ACCA Click or tap here to enter text.
Changes/Version Number	2.0

Assessment: (also refer to Assessment Outcomes Grids below)
This section should make transparent what assessment categories form part of this module (stating what % contributes to the final mark). Maximum of 3 main assessment categories can be identified (which may comprise smaller elements of assessment). **NB: The 30% aggregate regulation (Reg. 3.9) (40% for PG) for each main category must be taken into account. When using PSMD, if all assessments are recorded in the one box, only one assessment grid will show and the 30% (40% at PG) aggregate regulation will not stand. For the aggregate regulation to stand, each component of assessment must be captured in a separate box.** Please provide brief information about the overall approach to assessment that is taken within the module. In order to be flexible with assessment delivery, be brief, but do state assessment type (e.g. written assignment rather than "essay" / presentation, etc) and keep the detail for the module handbook. Click or tap here to enter text.
Assessment 1 - Coursework 1 (40%)
Assessment 2 – Coursework 2 (60%)
(N.B. (i) **Assessment Outcomes Grids** for the module (one for each component) can be found below which clearly demonstrate how the learning outcomes of the module will be assessed. (ii) An **indicative schedule** listing approximate times within the academic calendar when assessment is likely to feature will be provided within the Student Module Handbook.)

Assessment Outcome Grids (See Guidance Note)

Component 1							
Assessment Type (Footnote B.)	**Learning Outcome (1)**	**Learning Outcome (2)**	**Learning Outcome (3)**	**Learning Outcome (4)**	**Learning Outcome (5)**	**Weighting (%) of Assessment Element**	**Timetabled Contact Hours**
Report of practical/ field/clinical work	√					40	4

Component 2							
Assessment Type (Footnote B.)	**Learning Outcome (1)**	**Learning Outcome (2)**	**Learning Outcome (3)**	**Learning Outcome (4)**	**Learning Outcome (5)**	**Weighting (%) of Assessment Element**	**Timetabled Contact Hours**
Dissertation/ Project report/Thesis		√				60	8

Combined Total for All Components	**100%**	**12 hours**