Session: 2022/23
Last modified: 21/07/2022 16:48:16

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:	Zeeshan Pervez		

Summary of Module

Security of computer networks has been a primary issue for the management of information systems used by organizations 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. Details to these attributes is available at UWS Graduate Attributes webpage.

Module Delivery Method

Face-To-Face	Blended	Fully Online	HybridC	HybridO	Work-based Learning
			✓		

Face-To-Face
Term used to describe the traditional classroom environment where the students and the lecturer meet synchronously in the same room for the whole provision.
Blended
A mode of delivery of a module or a programme that involves online and face-to-face delivery of learning, teaching and assessment activities, student support and feedback. A programme may be considered “blended” if it includes a combination of face-to-face, online and blended modules. If an online programme has any compulsory face-to-face and campus elements it must be described as blended with clearly articulated delivery information to manage student expectations
Fully Online
Instruction that is solely delivered by web-based or internet-based technologies. This term is used to describe the previously used terms distance learning and e learning.
HybridC
Online with mandatory face-to-face learning on Campus
HybridO
Online with optional face-to-face learning on Campus
Work-based Learning
Learning activities where the main location for the learning experience is in the workplace.

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)

Paisley:	Ayr:	Dumfries:	Lanarkshire:	London:	Distance/Online Learning:	Other:
			✓			

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

Learning Outcomes: (maximum of 5 statements)
On successful completion 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
This module comprises of interactive lectures and labs sessions, delivered through problem-based learning activities and associated practical sessions. The rationale beyond lectures is to deliver knowledge related to issues of management of the computer network, transmission of data, and securing network services. Through lectures, students will be able to learn different algorithms, protocols and methodologies to secure computer network of varied sizes and configurations. Furthermore, students will be introduced to selected topics on cybersecurity to enable them to understand vulnerabilities related to the next generation of computer networks. Labs sessions will help in developing in-depth understanding of the knowledge delivered in the lectures, and critical evaluation of algorithms and methodologies when applying for a specific problem. The contents of this module will be delivered according to the following list of indicative topics: • Common threats and vulnerabilities of networked systems. • Network perimeter methodologies. • Network monitoring techniques. • Cryptographic methodologies. • Network authentication protocols and systems. • Secure data transmission over the network. • Secure network architecture.

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 with Red 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
(**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)

Engagement Requirements

In line with the Academic Engagement Procedure, Students are defined as academically engaged if they are regularly engaged with timetabled teaching sessions, course-related learning resources including those in the Library and on the relevant learning platform, and complete assessments and submit these on time. Please refer to the Academic Engagement Procedure at the following link: Academic engagement procedure

Supplemental Information

Programme Board	Computing
Assessment Results (Pass/Fail)	No
Subject Panel	Business &amp; Applied Computing
Moderator	Steve Eager
External Examiner	N Coull
Accreditation Details	
Version Number	1.04

Assessment: (also refer to Assessment Outcomes Grids below)
During the laboratory sessions, each student will be required to successfully complete the task(s) mentioned in the lab manual (weighted 40%), consequently assessing the achievement of L1.
A formal written report (weighted 60%) will be required from each student summarizing their finding of a given topic – agreed by the module coordinator, to evaluate L2. This assignment will require the students to do some literature review, identify possible solutions and justify / critics them accordingly.
(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 Handbook.)

Assessment Outcome Grids (Footnote A.)

Component 1					
Assessment Type (Footnote B.)	**Learning Outcome (1)**	**Learning Outcome (2)**	**Weighting (%) of Assessment Element**	**Timetabled Contact Hours**	
Report of practical/ field/ clinical work	✓		40	0	
Component 2					
Assessment Type (Footnote B.)	**Learning Outcome (1)**	**Learning Outcome (2)**	**Weighting (%) of**	**Timetabled Contact Hours**	

			Assessment Element		
Dissertation/ Project report/ Thesis		✓	60	0	
Combined Total For All Components			100%	0 hours	

Footnotes

A. Referred to within Assessment Section above

B. Identified in the Learning Outcome Section above

Note(s):

1. More than one assessment method can be used to assess individual learning outcomes.
2. Schools are responsible for determining student contact hours. Please refer to University Policy on contact hours (extract contained within section 10 of the Module Descriptor guidance note).
   This will normally be variable across Schools, dependent on Programmes &/or Professional requirements.

Equality and Diversity

This module is suitable for any student. The assessment regime will be applied flexibly so that a student who can attain the practical outcomes of the module will not be disadvantaged. When a student discloses a disability, or if a tutor is concerned about a student, the tutor in consultation with the School Enabling Support co-ordinator will agree the appropriate adjustments to be made.

UWS Equality and Diversity Policy

(N.B. Every effort will be made by the University to accommodate any equality and diversity issues brought to the attention of the School)