Session: 2022/23

Last modified: 21/07/2022 08:05:15

Title of Module: Cyber Security Principles			
Code: COMP11080	**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

This module provides a complete overview of all the essential aspects of Cyber Security within and outside various national and international domains of interest.

The module covers a discreet introduction about information and cyber security, cyber security risk process, national cyber security structure, management of security and relevant measures. This module also discusses various vectors of security attacks, and threats. This module further discusses various policies, standards and procedures governed nationally and internationally. This module also covers a theme of cyber warfare management in the context of critical system like Command and Control (C2) and C4 critical defence applications. This module also covers research-based assignments and study to acquire relevant and up-to date trends, challenges and scope in the domain of information and cyber security.

This module will work to develop a number of the key '**I am UWS' Graduate Attributes** to make those who complete this module:

Universal

- Critical Thinker
- Ethically-minded
- Research-minded

Work Ready

- Problem-Solver
- Effective Communicator
- Ambitious

Successful

- Autonomous
- Resilient
- Driven

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 a critical understanding of cybersecurity principles, platforms, protocols, management and architecture.

L2. Apply knowledge, understanding and skills to different case studies/vendors by evaluating security risks, vulnerabilities and attacks.

L3. Analyse and validate critical frameworks and perform various Forensics techniques to identify critical risks, threats and attacks to these systems.

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 about cybersecurity principles, platforms, protocols, management and architecture.

Practice: Applied Knowledge and Understanding	SCQF Level 11. Students will gain in-depth, comprehensive understanding and critical awareness of knowledge of cybersecurity and use forensics techniques to identify risks, threats and attacks.
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 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. Exercise a substantial ability to work autonomously, demonstrating critical inquiry in producing quality work underpinned by rigorous investigation. Learn effectively for the purpose of continuing personal development planning through interacting with others in academic and professional bodies and organisations relevant to m-business. Demonstrate an ability to manage and work autonomously with a range of self-directed m-business related learning resources.

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	
The module will be delivered by means of lectures and supervised hands-on lab work. Lectures will cover the theoretical background and practical applicability in real life problems. Concepts will be introduced by posing a practical problem and working out the needed theoretical knowledge to solve them. The delivery will encourage student participation to ensure an active learning experience. Group discussions will be held to promote critical thinking and boost informed decisions on the suitability of different state-of-the-art methods. Lab exercises will help student develop their knowledge in incremental fashion using a learning-by-doing approach. This will support the development of knowledge and understanding of the topics.	
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	6
Tutorial/Synchronous Support Activity	6
Laboratory/Practical Demonstration/Workshop	12
Independent Study	76
	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:

Tevault, D.A. (2018) Mastering Linux Security and Hardening: Secure your Linux server and protect it from intruders, malware attacks, and other external threats. Packt Publishing.

Brotherston, L. And Berlin, A. (2017) Defensive Security Handbook Paperback. O'Reilly.

Chris Chapman (2016) Network Performance and Security: Testing and Analyzing Using Open Source and Low-Cost Tools. Syngress.

Yuri Diogenes, Erdal Ozkaya (2018) Cybersecurity – Attack and Defense Strategies. Packt Publishing.

Corey P. Schultz, Bob Perciaccante (2018) Kali Linux Cookbook, Pack Publishing.

Brotherston, L. And Berlin, A. (2017) Defensive Security Handbook Paperback. O'Reilly.

(**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 & Applied Computing
Moderator	Steve Eager
External Examiner	N Coull
Accreditation Details	
Version Number	1.06

Assessment: (also refer to Assessment Outcomes Grids below)

Project Report (40%)

Practical Coursework (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 Handbook.)

Assessment Outcome Grids (Footnote A.)

Component 1

Assessment Type (Footnote B.)	Learning Outcome (1)	Learning Outcome (2)	Learning Outcome (3)	Weighting (%) of Assessment Element	Timetabled Contact Hours
Dissertation/ Project report/ Thesis	✓	✓	✓	40	2

Component 2

Assessment Type (Footnote B.)	Learning Outcome (1)	Learning Outcome (2)	Learning Outcome (3)	Weighting (%) of Assessment Element	Timetabled Contact Hours
Report of practical/ field/ clinical work	✓	✓	✓	60	8
Combined Total For All Components				100%	10 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)