Session: 2022/23
Last modified: 09/02/2021 14:41:52

Title of Module: Intrusion Analysis			
Code: COMP11102	**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:	Sean Sturley		

Summary of Module

The module allows students to develop the specialised technical knowledge and expertise needed to analyse the complex and varied data sources that exsist within todays modern enterprise networks in order to identify potential network intrusions.

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 intrusion analysis by investigating current theories and concepts. L2. Apply knowledge, skills and understanding to identify evidence of malicious behaviour in network traffic in real-time or previously captured format. L3. Collect, document and present evidence of compromise within a given scenario.

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 systematic and comprehensive knowledge of Intrusion Analysis. 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, comprehensive understanding and critical awareness of knowledge of Intrusion Analysis, and apply this in planning, implementing, capture and analysis of network traffic. They will also develop capability to apply a range of standard and specialised research skills, tools/software, development kit and related techniques in response to application requirements 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 report summarising his/her finding for a given scenario.
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	7
Tutorial/Synchronous Support Activity	7
Laboratory/Practical Demonstration/Workshop	14
Independent Study	72
	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: EC-Council (2016) 2nd Ed. Computer Forensics: Investigating Network Intrusions and Cybercrime. Cengage Learning Davdoff, S. (2013) NETWORK FORENSICS : TRACKING HACKERS THROUGH CYBERSPACE. Pearson India Fichera, J and Bolt, S. (2012) Network Intrusion Analysis: Methodologies, Tools, and Techniques for Incident Analysis and Response. Syngress Sanders, C and Smith , J. (2013) Applied Network Security Monitoring: Collection, Detection, and Analysis. Syngress	
(**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	Jose Alcaraz Calero
External Examiner	H Al-Khateeb
Accreditation Details	
Version Number	1.03

Assessment: (also refer to Assessment Outcomes Grids below)
Practical Examination (40%)
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**
Class test (practical)		✓	✓	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)