University of the West of Scotland

Module Descriptor

Session: 2024/25

Title of Module: Malware Analysis			
Code: COMP11089	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

This module develops a deep understanding of low-level aspects of processors and code for analysing security vulnerabilities and malware. Through an initial examination of assembly language programming and machine- level instruction sets, the module will explore in detail reverse engineering methods to understand malware functionality, advanced static and dynamic analysis methods,

The ethical and professional issues/requirements of the professional practitioner are incorporated throughout the syllabus.

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	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	Develop a critical understanding of the best practices and mechanisms of malware design, implementation and analysis.
L2	Demonstrate an analytical awareness of the methods and techniques to examine a vulnerable system and identify malicious code using various malware analysis techniques.
L3	Critically evaluate the design, code and implementation of malicious software components and the steps required to identify/detect the anomalies in the process.

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 Malware 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 Malware Analysis, and apply this in planning, implementing, capture and analysis of malware. 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	
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.	
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
	Hours Total 100

**Indicative Resources: (eg. Core text, journals, internet access)

The following materials form essential underpinning for the module content and ultimately for the learning outcomes:

Monnappa, K. A. (2018) Learning Malware Analysis. Packt Publishing

Elisan, C. (2015) Advanced Malware Analysis. McGraw-Hill Education

Oktavianto, D and Muhardianto, I. (2013) Cuckoo Malware Analysis. Packt Publishing

Wong, R. (2018) Mastering Reverse Engineering: Your Practical guide to master the art of Malware Reversing. Packt Publishing

Dang, B and Gazet, A. (2014) Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation. 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.

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	Paul Keir
External Examiner	N Coull
Accreditation Details	e.g. ACCA Click or tap here to enter text.
Changes/Version Number	1.03

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 – Practical Examination (40%)
Assessment 2 – 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 Module Handbook.)

Assessment Outcome Grids (**See Guidance Note**)

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	1

Component 2					
Assessment Type (Footnote B.)	**Learning Outcome (1)**	**Learning Outcome (2)**	**Learning Outcome (3)**	**Weighting (%) of Assessment Element**	**Timetabled Contact Hours**
Clinical/ Fieldwork/ Practical skills assessment/ Debate/ Interview/ Viva voce/ Oral	✓	✓	✓	60	2

	Combined Total for All Components	**100%**	**3 hours**