Module Descriptor

Title	Malware Analysis & Reverse Engineering		
Session	2025/26	**Status**	Published
Code	COMP11090	**SCQF Level**	11
Credit Points	20	**ECTS (European Credit Transfer Scheme)**	10
School	**Computing, Engineering and Physical Sciences**		
Module Co-ordinator	TBC		

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,

Anti-disassembling, anti-debugging and de-obfuscation 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:

!!niversal

- Critical Thinker
- Ethically-minded
- Research-minded

Work Ready

- Problem-Solver
- Effective Communicator
- Ambitious

.S,uccessful

- Autonomous
- Resilient
- Driven

Module Delivery Method	On-Campus[1] ☒	Hybrid[2] ☐	Online[3] ☐	Work -Based Learning[4] ☐
Campuses for Module Delivery	☐ Ayr ☐ Dumfries	☒ Lanarkshire ☐ London ☐ Paisley	☐ Online / Distance Learning ☐ Other (specify)	

Terms for Module Delivery	Term 1	☒	Term 2	☐	Term 3	☐
Long-thin Delivery over more than one Term	Term 1 – Term 2	☐	Term 2 – Term 3	☐	Term 3 – Term 1	☐

Learning Outcomes	
L1	Comprehensively understand the key attributes and behaviour of malware, malicious code implementation and the methods of malware analysis.
L2	Critically evaluate the design, code and implementation of a malicious components and the steps required to reverse engineer the process.
L3	Employ low level techniques and system-monitoring to examine and assess how malware interacts with the file system, registry, network and other processes, and utilise memory techniques to examine, predict and compare capabilities.
L4	Identify, select and critically evaluate techniques at the forefront of the discipline used in detection strategies and the defence of systems against malicious software and software based attacks.
L5	Demonstrate critical awareness of the techniques to isolate an infected system and perform malicious code analysis and reverse engineering in line with advanced professional practice.

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 11** Critical and systematic knowledge and understanding of low level techniques and tools (such as assembly language programming and machine-level instruction sets) in the context of malicious code implementation.

[1] Where contact hours are synchronous/ live and take place fully on campus. Campus-based learning is focused on providing an interactive learning experience supported by a range of digitally-enabled asynchronous learning opportunities including learning materials, resources, and opportunities provided via the virtual learning environment. On-campus contact hours will be clearly articulated to students.

[2] The module includes a combination of synchronous/ live on-campus and online learning events. These will be supported by a range of digitally-enabled asynchronous learning opportunities including learning materials, resources, and opportunities provided via the virtual learning environment. On-campus and online contact hours will be clearly articulated to students.

[3] Where all learning is solely delivered by web-based or internet-based technologies and the participants can engage in all learning activities through these means. All required contact hours will be clearly articulated to students.

[4] Learning activities where the main location for the learning experience is in the workplace. All required contact hours, whether online or on campus, will be clearly articulated to students

Practice: Applied Knowledge and Understanding	**SCQF 11** Use specialised and advanced skills, techniques and practices.
Generic Cognitive skills	**SCQF 11** Critically identify, define, conceptualise and analyse complex problems; Demonstrate some originality and creativity; Critically review and consolidate knowledge, skills, practices and thinking in the discipline; Make judgements where data/information is limited or comes from a range of sources.
Communication, ICT and Numeracy Skills	**SCQF 11** Use a wide range of advanced and specialised skills in support of established practices. Interpret, use and evaluate a wide range of data.
Autonomy, Accountability and Working with Others	**SCQF 11** Exercise autonomy and initiative in activities. Manage complex ethical and professional issues.

Prerequisites	**Module Code**	**Module Title**
	Other	
Co-requisites	**Module Code**	**Module Title**

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 and teaching will take place through a variety of mechanisms, including lectures, seminars, with a collection of associated practical sessions, research into current developments and issues, and case studies. This module places an emphasis on active "hands-on" and an independent approach to learning, where students experience and develop capabilities through practical activities. Case studies will be used formatively in tutorials in order to promote application of knowledge to specific problems and encourage discussion. Topics will be introduced in lectures and discussed through guided inquiry learning activities. Additionally directed learning will reinforce essential theory and place understanding into context.	
Learning Activities During completion of this module, the learning activities undertaken to achieve the module learning outcomes are stated below:	**Student Learning Hours** (Note: Learning hours include both contact hours and hours spent on other learning activities)
Lecture / Core Content Delivery	24
Tutorial / Synchronous Support Activity	12
Laboratory / Practical Demonstration / Workshop	24
Independent Study	140
Please select	
Please select	

TOTAL	200

Indicative Resources

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

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:

The School of Computing, Engineering and Physical Sciences considers attendance and engagement to mean a commitment to attending, and engaging in, timetabled sessions. You will scan your attendance via the scanners each time you are on-campus and you will login to the VLE several times per week. Where you are unable to attend a timetabled learning session due to illness or other circumstance, you should notify the Programme Leader that you cannot attend. Across the School an 80% attendance threshold is set. If you fall below this, you will be referred to the Student Success Team to see how we can best support your studies.

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.

Aligned with the University's commitment to equality and diversity, this module supports equality of opportunity for students from all backgrounds and learning needs. Using the VLE, material will be presented electronically in formats that allow flexible access and manipulation of content. This module complies with University regulations and guidance on inclusive learning and teaching practice. This module has lab-based teaching and as such you are advised to speak to the Module Co-ordinator to ensure that specialist assistive equipment, support provision and adjustment to assessment practice can be put in place, in accordance with the University's policies and regulations.

(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**
Overall Assessment Results	☐ **Pass / Fail** ☒ **Graded**
Module Eligible for Compensation	☐ **Yes** ☒ **No** **If this module is eligible for compensation, there may be cases where compensation is not permitted due to programme accreditation requirements. Please check the associated programme specification for details.**
School Assessment Board	Business & Applied Computing
Moderator	Paul Keir
External Examiner	M Davis
Accreditation Details	
Module Appears in CPD catalogue	☐ **Yes** ☒ **No**
Changes / Version Number	1.06

Assessment (also refer to Assessment Outcomes Grids below)
Assessment 1
Examination (50%) - The examination evaluates the students' learning in all of the theoretical learning outcomes; students can expect to utilise low level analysis tools, and be presented with malware/malicious documents or network flow traces similar to those introduced in the lessons.
Assessment 2
Assignment: Report of practical work (50%) - The assignment will typically require either the analysis and/or reverse engineering of a malicious code sample; analysis/and or reverse engineering of malicious documents including memory analysis and reconstruction of artefacts.
Assessment 3
(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.)

Component 1							
Assessment Type	**LO1**	**LO2**	**LO3**	**LO4**	**LO5**	**Weighting of Assessment Element (%)**	**Timetabled Contact Hours**
Unseen closed book (standard)	☒	☒	☐	☒	☒	50	0

Component 2							
Assessment Type	**LO1**	**LO2**	**LO3**	**LO4**	**LO5**	**Weighting of Assessment Element (%)**	**Timetabled Contact Hours**
Report of practical/ field/ clinical work	☐	☒	☒	☒	☒	50	0

Component 3							
Assessment Type	**LO1**	**LO2**	**LO3**	**LO4**	**LO5**	**Weighting of Assessment Element (%)**	**Timetabled Contact Hours**
	☐	☐	☐	☐	☐		
Combined total for all components						100%	hours

Change Control

What	**When**	**Who**
Attendance and Engagement, EDI sand External Examiners updated	22/01/2025	A Adamson