University of the West of Scotland

Module Descriptor

Session: 2022/23

Last modified: 10/01/2023 10:39:43

Title of Module: Ethical Hacking: Tools & Techniques

Code: COMP08094	**SCQF Level: 8** (Scottish Credit and Qualifications Framework)	**Credit Points: 20**	**ECTS: 10** (European Credit Transfer Scheme)
School:	School of Computing, Engineering and Physical Sciences		
Module Co-ordinator:	Althaff Mohideen		

Summary of Module

The aim of the module is to provide students with an introduction to both ethical hacking techniques and penetration testing practice in order to discover weaknesses with the goal of strengthening defences.

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 the methodologies of penetration testing methods; L2. effectively use a variety of tools to undertake penetration testing; L3. understand the fundamentals of system security in relation with weaknesses and vulnerability; L4. apply hacking methods to collect system information; L5. use web and databases as case studies to demonstrate the skills in penetration testing.

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 8. A detailed understanding of methodologies of penetration testing, legal and ethical issues of hacking.
Practice: Applied Knowledge and Understanding	SCQF Level 8. Use a variety of tools to undertake testing.
Generic Cognitive skills	SCQF Level 8. Systematic planning and undertaking of system design and testing.
Communication, ICT and Numeracy Skills	SCQF Level 8. Effective use of variety of tools. Analytic skills in identifying the weaknesses and vulnerability of systems. Report writing and presentation skills.
Autonomy, Accountability and Working with others	SCQF Level 8. Teamwork skills.

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	
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	12
Tutorial/Synchronous Support Activity	12
Laboratory/Practical Demonstration/Workshop	24
Independent Study	152
	200 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:

Kim, P. (2015) Hackers Playbook (2nd edition). CreateSpace Independent Publishing Platform.

Alcorn, W., Frichot, C., and Orru, M. (2014) The Browser Hacker's Handbook. John Wiley & Sons.

McClure, S., Scambray, J., and Kurtz, G. (2012) Hacking Exposed 7: Network Security Secrets and Solutions. McGraw-Hill.

(**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	Sean Sturley
External Examiner	M Davis
Accreditation Details	
Version Number	1.08

Assessment: (also refer to Assessment Outcomes Grids below)
Coursework (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)	Learning Outcome (4)	Learning Outcome (5)	Weighting (%) of Assessment Element	Timetabled Contact Hours
Report of practical/ field/ clinical work	✓	✓	✓	✓	✓	60	8

Component 2

Assessment Type (Footnote B.)	Learning Outcome (1)	Learning Outcome (2)	Learning Outcome (3)	Learning Outcome (4)	Learning Outcome (5)	Weighting (%) of Assessment Element	Timetabled Contact Hours
Report of practical/ field/ clinical work	✓			✓	✓	40	2
					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)