MODULE SPECIFICATION PROFORMA

Module Code:	COM733

Module Title:	Advanced Ethical Hacking

Level:	7	**Credit Value:**	20

Cost Centre(s):	GACP	JACS3 **code**: HECoS code:	I190 100366

Faculty:	Arts, Science and Technology	**Module Leader:**	Nigel Houlden

Scheduled learning and teaching hours	21 hrs
Guided independent study	179 hrs
Placement	0 hrs
Module duration (total hours)	200 hrs

Programme(s) in which to be offered (not including exit awards)	Core	Option
MSc Cyber Security	✓	☐

Pre-requisites
None

Office use only
Initial approval: 28/11/2018 Version no:1
With effect from: 01/09/2019
Date and details of revision: Version no:

Module Aims

This module is designed to develop understanding, knowledge and skills associated with the various malicious hacking attacks targeting computer systems and the appropriate safeguards needed to minimise such attacks.

Intended Learning Outcomes

Key skills for employability

KS1	Written, oral and media communication skills
KS2	Leadership, team working and networking skills
KS3	Opportunity, creativity and problem solving skills
KS4	Information technology skills and digital literacy
KS5	Information management skills
KS6	Research skills
KS7	Intercultural and sustainability skills
KS8	Career management skills
KS9	Learning to learn (managing personal and professional development, self-management)
KS10	Numeracy

At the end of this module, students will be able to		Key Skills	
1	Provide students with knowledge and understanding of the various hacking methods used in attacking computer systems and networks.		
2	Enable students to use appropriate tools and techniques to identify, analyse, evaluate and test computer security vulnerabilities prone to hacking attacks, and develop appropriate procedures, solutions and countermeasures to defend and minimise such attacks.		
3	To develop students' awareness of ethical, professional and legal issues connected with hacking.		
4	Develop students' knowledge, transferable skills and confidence in the subject leading to further academic and professional progression in this area.		

Transferable skills and other attributes

Derogations

None

Assessment:

Indicative Assessment Tasks:

The coursework will involve identifying computing areas vulnerable to hacking and developing practical solutions to mitigate the problems using appropriate methods, techniques and tools. Students will produce a report detailing their work based on some case study, scenario or research investigation.

The practical test will further assess students' broader understanding of the practical concepts of the subject.

Students will be encouraged to complete weekly tutorial and workshop exercises as well as periodic formative diagnostic tests to enhance their learning. During tutorial and workshop sessions students will receive ongoing support and feedback on their work to promote engagement.

Assessment number	Learning Outcomes to be met	Type of assessment	Weighting (%)	Duration (if exam)	Word count (or equivalent if appropriate)
1	1-3	Coursework	60		3000
2	1,2,4	Practical	40	2 hours	

Learning and Teaching Strategies:

Students will develop theoretical understanding and practical skills in the subject area based on weekly lectures, tutorials and supervised workshops. The tutorials and workshops, in particular, are provided to support students in gaining practical experience in tackling a wide range of computer hacking related issues and problems.
Appropriate blended learning approaches and technologies, such as, the University's VLE and online tools, will be used to facilitate and support student learning, in particular, to:
• deliver content;
• encourage active learning;
• provide formative and summative assessments, and prompt feedback;
• enhance student engagement and learning experience.
Students will be expected and encouraged to produce reflective commentaries on the learning activities and tasks that they carry out to complete their work.

Syllabus outline:

1. Reconnaissance and Intelligence Gathering: Traditional and Current Hacking Methods.
2. Current Approaches to Hacking.
3. Software Tools and Practical Hacking Methods and Techniques.
4. Protocols, Network Communication, Internet & Web Based Hacking Attacks.
5. Blended Hacking Threats and Exploitations.
6. Cloud Insecurity: Hacking the Cloud.

7. Hacking Mobile Devices.
8. Phishing Ecosystem& Hacking.
9. Social Engineering Hacking Techniques: Influencing and Manipulating Victims.
10. Integrated Hacking Attacks Based on Complex Approaches, Processes & Systems.
11. Hacking: Ethical, Professional and Legal Issues.

Indicative Bibliography:

Essential reading

Harper, A. (2014), *Gray Hat Hacking: The Ethical Hacker's Handbook*. 4th ed. McGraw-Hill Education.

Kim, P. (2015), *The Hacker Playbook 2: Practical Guide to Penetration Testing*. CreateSpace.

Other indicative reading

McClure, S., Scambray, J., and Kurtz, G. (2012). *Hacking Exposed: Network Security Secrets and Solutions*. 7th ed. New York: McGraw-Hill/Osborne.

Engebretson, P. (2013), *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy*. 2nd ed. Syngress.