Module specification

When printed this becomes an uncontrolled document. Please access the Module Directory for the most up to date version by clicking on the following link: Module directory

Module code	CONL724
Module title	Ethical Hacking
Level	7
Credit value	15
Faculty	FAST
Module Leader	Leanne Davies
HECoS Code	100366
Cost Code	GACP

Programmes in which module to be offered

Programme title	Is the module core or option for this programme
MSc Computer Science with Cyber Security	Core
MSc Computer Science with Networking	Core

Pre-requisites

Studied CONL701 Critical Research for Postgraduate Study

Breakdown of module hours

Learning and teaching hours	15 hrs
Placement tutor support	0 hrs
Supervised learning e.g. practical classes, workshops	0 hrs
Project supervision (level 6 projects and dissertation modules only)	0 hrs
Total active learning and teaching hours	**0** hrs
Placement / work based learning	0 hrs
Guided independent study	135 hrs
Module duration (total hours)	150 hrs

For office use only	
Initial approval date	17/06/21
With effect from date	28/06/21
Date and details of revision	
Version number	1

Module aims

The module aims to give students a solid and professional level of competence in the field of ethical hacking, which is predominantly led by the coverage of tools, techniques and systems that allow penetration testing to be carried out on computer systems and networks.

Much of the module material follows the footsteps of a would-be intruder and thus includes coverage of the communication and social side of computer attacks as well as the technological.

Having been led to understand how systems, software and devices can be vulnerable to unwanted penetration, students will then investigate countermeasures and organisational strategies to mitigate these risks.

Module Learning Outcomes - at the end of this module, students will be able to:

1	Select and explain an appropriate range of hacking methods used in attacking computer systems and networks.
2	Identify, analyse, evaluate and test computer security vulnerabilities using suitable tools and techniques.
3	Identify, select and plan appropriate procedures, solutions and countermeasures to defend and minimise computer security attacks.
4	Make and justify decisions requiring an awareness of ethical, professional and legal issues connected with hacking.
5	Extend and improve knowledge in the subject leading to further academic and professional progression in this area

Assessment

Indicative Assessment Tasks:

This section outlines the type of assessment task the student will be expected to complete as part of the module. More details will be made available in the relevant academic year module handbook.

Students will complete a portfolio of work identifying computing areas vulnerable to hacking and developing practical solutions to mitigate the problems using appropriate methods, techniques and tools.

The portfolio may include written submissions, quizzes, discussions and practical based activities which will assess students' broader understanding of the practical concepts through simulation requiring the identification, evaluation and resolution using the hacking tools and techniques learned during the module.

Word count equivalent: 3000 words

Assessment number	Learning Outcomes to be met	Type of assessment	Weighting (%)
1	1-5	Portfolio	100%

Derogations

None

Learning and Teaching Strategies

The overall learning and teaching strategy is one of guided independent study requiring ongoing student engagement. Online material will provide the foundation of the learning resources, requiring the students to login and engage on a regular basis throughout the eight-week period of the module. There will be a mix of suggested readings, discussions and interactive content containing embedded digital media and self-checks for students to complete as they work through the material and undertake the assessment tasks. The use of a range digital tools via the virtual learning environment together with additional sources of reading will also be utilised to accommodate learning styles. There is access to a helpline for additional support and chat facilities through Canvas for messaging and responding.

Indicative Syllabus Outline

1. Introduction to ethical hacking.
2. Software tools and practical hacking methods and techniques.
3. Protocols, network communication, Internet & web-based hacking attacks.
4. Blended hacking threats and exploitations.
5. Cloud insecurity: hacking the cloud.
6. Hacking mobile devices.
7. Phishing ecosystem & hacking.
8. Social engineering hacking techniques: influencing and manipulating victims.
9. Integrated hacking attacks based on complex approaches, processes & systems.
10. Hacking: Ethical, professional and legal issues.

Indicative Bibliography:

Please note the essential reads and other indicative reading are subject to annual review and update.

Essential Reads

Easttom, C. (2016). *Computer Security Fundamentals*. 3rd ed. Pearson Education.

Other indicative reading

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

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

Employability skills – the Glyndŵr Graduate

Each module and programme is designed to cover core Glyndŵr Graduate Attributes with the aim that each Graduate will leave Glyndŵr having achieved key employability skills as part of their study. The following attributes will be covered within this module either through the content or as part of the assessment. The programme is designed to cover all attributes and each module may cover different areas.

Core Attributes
Engaged
Ethical

Key Attitudes
Commitment
Curiosity
Confidence
Adaptability

Practical Skillsets
Digital Fluency
Organisation
Critical Thinking
Emotional Intelligence
Communication