Module Definition Form (MDF)

Module code: MOD003121	**Version:** 5 **Date Amended:** 16/Jul/2026

1. Module Title
Ethical Hacking and Countermeasures

2a. Module Leader
Segun Popoola

2b. School
School of Computing and Information Sciences

2c. Faculty
Faculty of Science and Engineering

3a. Level
6

3b. Module Type
Standard (fine graded)

4a. Credits
15

4b. Study Hours
150

5. Restrictions

Type	Module Code	Module Name	Condition
Pre-requisites:	None		
Co-requisites:	None		
Exclusions:	None		
Courses to which this module is restricted:	None		

LEARNING, TEACHING AND ASSESSMENT INFORMATION

6a. Module Description

This module introduces you to the key principles of ethical hacking, combining both theory and hands-on technical practice. You'll examine the issues surrounding systems security, cybercrime and the criminal justice system, including the Computer Misuse Act (1990). Through a combination of lectures, demonstrations and practical sessions, you'll learn how ethical hacking can be used to protect and strengthen computer systems and networks, including wireless networks. You'll gain experience using essential hacking tools and techniques, with a particular focus on penetration testing and systems security within a safe sandboxed environment. Alongside technical skills, you'll develop the ability to produce clear evidence-based reports and deliver professional presentations. Through research and practical application, you'll develop the skills to manage the legal, social, ethical and professional challenges facing Information Security practitioners, with particular reference to the criminal justice system in England and Wales. By the end of the module, you'll have the practical skills and critical understanding required to apply ethical hacking techniques responsibly and effectively in real-world scenarios.

6b. Outline Content

Compulsory elements of this module content will be : - Ethics and Legality i.e. Misuse of Computers Act, British Computer Society professional guidelines. - Develop an understanding of the fundamental principles of systems security, particularly in relation to weaknesses and vulnerabilities. - Security policy development - Define how ethical hacking relates to, and makes use of, the underpinning theories and principles of computing and engineering. Due to the dynamic nature of Computing further content will reflect the latest developments in security related topics. These will typically be, but not limited to: - Denial of Service, Firewalls, Honeypots, Web based attacks and prevention - Malware e.g. Trojans, Bots and prevention - Penetration Testing and network security

6c. Key Texts/Literature

The reading list to support this module is available at: https://readinglists.aru.ac.uk/

6d. Specialist Learning Resources

Secure laboratory environment i.e. isolated PCs and network, for investigation of threat methodologies and defensive strategy evaluation through the use of virtual machine sandboxes. This would be currently achievable using a combination of Netlab (through a networked Web browser) and an isolated lab such as our Cisco networking lab.

7. Learning Outcomes (threshold standards)		
No.	**Type**	**On successful completion of this module the student will be expected to be able to:**
1	Knowledge and Understanding	Evidence awareness of comprehensive knowledge of Computer Security and attack and countermeasure, and can incorporate these factors into a major piece of work.
2	Knowledge and Understanding	Analyse and exhibit comprehensive knowledge of 'professional' codes of conduct incorporated into a major piece of work.
3	Intellectual, practical, affective and transferrable skills	Critically evaluate evidence / research in order to support personal conclusions/recommendations while reviewing validity and significance.
4	Intellectual, practical, affective and transferrable skills	Demonstrate confidence and flexibility in identifying and defining complex problems and the application of appropriate knowledge, tools/methods to their resolution.

8a. Module Occurrence to which this MDF Refers				
Year	**Occurrence**	**Period**	**Location**	**Mode of Delivery**
2026/7	ZZF	Template For Face To Face Learning Delivery		Face to Face

8b. Learning Activities for the above Module Occurrence			
Learning Activities	**Hours**	**Learning Outcomes**	**Details of Duration, frequency and other comments**
Lectures	12	1,2,4	Logbook and Lab. work provide opportunities for Formative Feedback
Other teacher managed learning	24	1,2,3	Logbook and Lab. work provide opportunities for Formative Feedback
Student managed learning	114	1-4	Case Study plus logbook/lab. work support development in these elements.
TOTAL:	150		

9. Assessment for the above Module Occurrence

The assessment for some modules includes a presentation (see below for details on how this particular module is assessed). We recognise that presenting, especially to a large group, can cause significant anxiety or distress for some students. If this may affect you, please contact your Module Leader or the Disability and Neurodiversity Service as early as possible. We will work with you to consider appropriate reasonable adjustments. Depending on your individual needs, these might include, for example, presenting to a smaller group or presenting only to a member of academic staff.

Assessment No.	Assessment Method	Learning Outcomes	Weighting (%)	Fine Grade or Pass/Fail	Qualifying Mark (%)
010	Coursework	1-4	100 (%)	Fine Grade	30 (%)
Case Study and Analysis Report (2500 words equivalent)					

In order to pass this module, students are required to achieve an overall mark of 40% (for modules at levels 3, 4, 5 and 6) or 50% (for modules at level 7*).

In addition, students are required to:
(a) achieve the qualifying mark for each element of fine graded assessment as specified above
(b) pass any pass/fail elements

[* the pass mark of 50% applies for all module occurrences from the academic year 2024/25 – see Section 3a of this MDF to check the level of the module and Section 8a of this MDF to check the academic year]