Liverpool John Moores University

Title:	ETHICAL HACKING
Status:	Definitive
Code:	**7141COMP** (126789)
Version Start Date:	01-08-2021
Owning School/Faculty:	Computer Science and Mathematics
Teaching School/Faculty:	Computer Science and Mathematics

Team	Leader
Alex Akinbi	Y
Nathan Shone	

Academic Level:	FHEQ7	**Credit Value:**	20	**Total Delivered Hours:**	33
Total Learning Hours:	200	**Private Study:**	167		

Delivery Options
Course typically offered: Semester 2

Component	Contact Hours
Lecture	11
Practical	22

Grading Basis: 50 %

Assessment Details

Category	Short Description	Description	Weighting (%)	Exam Duration
Artefacts	AS1	Report relating to hacking tools, penetration testing and exploit development	40	
Report	AS2	Report relating to threats, intrusion campaigns and techniques to develop threat hunting, network security monitoring and forensic investigation solutions.	60	

Aims

To gain a significant understanding of various security vulnerabilities and cyber

threats to computer systems/applications as well as the importance of cyber security.
To assess critically a variety of ethical hacking tools and penetration testing techniques for the protection and evaluation of computer systems and applications.
To promote the use of appropriate ethical security techniques to solve cyber security problems.
To understand practices of network forensics and intrusion analysis to aid cyber threat intelligence gathering.
To develop independent research skills in threat intelligence to detect, respond to, and defeat focused and targeted threats.

Learning Outcomes

After completing the module the student should be able to:

1	Deploy ethical hacking tools and techniques to complex computer systems
2	Demonstrate critical awareness of recent developments in ethical hacking techniques
3	Critically review developments in system defence, response and intelligence techniques.

Learning Outcomes of Assessments

The assessment item list is assessed via the learning outcomes listed:

Report on hacking tools	1	2
Report on defence tools	3	

Outline Syllabus

Ethical hacking fundamentals: Penetration testing lifecycle, vulnerability detection, vulnerability-scanning techniques.

Hacking methods and tools: system hacking methods exploit frameworks, network and device-hacking techniques, web application attacks, password attacks and exploit development.

Advanced techniques: malicious software code, network forensics, intrusion detection and prevention, cyber threat hunting, security monitoring and incident response techniques and procedures.

Learning Activities

Include attending lectures, practical sessions and tutorials, as well as reading online resources.

Notes

The spectacular growth of the Internet has spawned a great demand for secure computer systems. Ethical hacking can help to assess the cyber security defence of computer systems. Intrusion detection and firewalls provide additional layers of defence for the detection and prevention of cyber-attacks on computer systems. This module examines various cyber security issues and solutions within these areas.