Liverpool John Moores University

Title:	CYBER HACKING AND DEFENCE
Status:	Definitive
Code:	**6064COMP** (117508)
Version Start Date:	01-08-2019
Owning School/Faculty:	Computer Science
Teaching School/Faculty:	Computer Science

Team	Leader
Nathan Shone	Y
Alex Akinbi	
Qi Shi	

Academic Level:	FHEQ6	**Credit Value:**	24	**Total Delivered Hours:**	74
Total Learning Hours:	240	**Private Study:**	166		

Delivery Options

Course typically offered: Standard Year Long

Component	Contact Hours
Lecture	24
Practical	24
Tutorial	24

Grading Basis: 40 %

Assessment Details

Category	Short Description	Description	Weighting (%)	Exam Duration
Report	AS1	Design of cyber security solutions for given hacking/defence scenario.	50	
Exam	AS2	Examination.	50	2

Aims

To gain a significant understanding of various security vulnerabilities in and cyber threats to computer systems/applications as well as the importance of cyber security.

To assess critically a variety of hacking, intrusion detection and firewall techniques and tools for the protection and evaluation of computer systems and applications. To promote the use of appropriate security techniques to solve cyber security problems.

Learning Outcomes

After completing the module the student should be able to:

1 Apply creative skills in relation to security techniques and tools to solve cyber security problems.

2 Critically review cyber security threats and vulnerabilities, and identify appropriate security techniques to protect organisational computer systems.

3 Critically evaluate methods of ethical hacking, intrusion detection and firewall techniques for the provision of security services needed for secure computer applications.

Learning Outcomes of Assessments

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

Cyber security solutions	1	2
Examination	3	

Outline Syllabus

Ethical hacking: Ethical hacking fundamentals; security vulnerabilities; attack foot printing; attack scanning techniques; system hacking methods; network and device hacking techniques; application and data hacking methods; ethical hacking planning; and ethical hacking reporting and responding.

Intrusion detection: Overview of intrusion detection systems; host-based intrusion detection; network-based intrusion detection; intrusion detection tool selection and analysis; deployment issues of intrusion detection, effective use of intrusion detection technologies; organisational issues and operational planning; and recent advances in intrusion detection.

Firewalls: Network security threats; firewall purposes and types; firewall requirements; firewall techniques; firewall deployment issues, and firewall interoperations with other security measures such as IPSec.

Lab: The practical laboratory exercises will develop skills in the use of relevant security tools, e.g. for intrusion detection, and an understanding of cyber attacks.

Learning Activities

Lectures and practical work. The practical work builds on the module contents covered in the lectures. This involves laboratory and user demonstrations of relevant security tools.

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.