Network Defence

Module Information

2022.01, Approved

Summary Information

Module Code	6613YCOM
Formal Module Title	Network Defence
Owning School	Computer Science and Mathematics
Career	Undergraduate
Credits	20
Academic level	FHEQ Level 6
Grading Schema	40

Teaching Responsibility

LJMU Schools involved in Delivery
LJMU Partner Taught

Partner Teaching Institution

Institution Name
YPC International College (Kolej Antarabangsa YPC)

Learning Methods

Learning Method Type	Hours
Lecture	22
Practical	22
Tutorial	11

Module Offering(s)

Display Name	Location	Start Month	Duration Number Duration Unit
SEP-PAR	PAR	September	12 Weeks

Aims and Outcomes

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 intrusion detection and firewall techniques and tools for the protection of computer systems and applications.Develop practical skills in the use of security countermeasure technologies and associated tools.

After completing the module the student should be able to:

Learning Outcomes

Code	Number	Description
MLO1	1	Critically review use of security countermeasures in a networked environment.
MLO2	2	Plan and develop a solution using network defence techniques and tools.
MLO3	3	Compare and contrast methods of intrusion detection and firewall techniques to secure information systems.

Module Content

Outline Syllabus	Malware; viruses and worms, botnets, mobile code security, spyware. Other common attack types including Denial of Service, Phishing, XSS, SQL Injection.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.System security services: authentication, key management, access control models including Bell-LaPadula, Chinese Wall, Biba, RBA. Trusted Computing. Biometrics.
Module Overview	
Additional Information	Using network defence techniques are a core part of being an information security practitioner. Practical skills learnt in this module will be useful for employability.

Assessments

Assignment Category	Assessment Name	Weight	Exam/Test Length (hours)	Module Learning Outcome Mapping
Report	Network Security Scenario	40	0	MLO1, MLO2
Exam	Exam	60	2	MLO1, MLO3

Module Contacts

Module Leader

Contact Name	Applies to all offerings	Offerings
Aine Mac Dermott	Yes	N/A

Partner Module Team

Contact Name	Applies to all offerings	Offerings