Liverpool John Moores University

Title:	NETWORK DEFENCE
Status:	Definitive
Code:	**6613YCOM** (125490)
Version Start Date:	01-08-2021
Owning School/Faculty:	Computer Science and Mathematics
Teaching School/Faculty:	YPC International College (Kolej Antarabangsa YPC)

Team	Leader
Aine MacDermott	Y

Academic Level:	FHEQ6	**Credit Value:**	20	**Total Delivered Hours:**	57
Total Learning Hours:	200	**Private Study:**	143		

Delivery Options
Course typically offered: Semester 1

Component	Contact Hours
Lecture	22
Practical	22
Tutorial	11

Grading Basis: 40 %

Assessment Details

Category	Short Description	Description	Weighting (%)	Exam Duration
Report	AS1	Network Security Scenario	40	
Exam	AS2	Examination	60	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 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.

Learning Outcomes

After completing the module the student should be able to:

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

Learning Outcomes of Assessments

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

Network Security Scenario	1	2
Exam	1	3

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.

Learning Activities

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

Notes

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.