Liverpool John Moores University

Title:	System Penetration Testing
Status:	Definitive
Code:	**5216COMP** (127992)
Version Start Date:	01-08-2021
Owning School/Faculty:	Computer Science and Mathematics
Teaching School/Faculty:	Computer Science and Mathematics

Team	Leader
Nathan Shone	Y

Academic Level:	FHEQ5	**Credit Value:**	20	**Total Delivered Hours:**	44
Total Learning Hours:	200	**Private Study:**	156		

Delivery Options
Course typically offered: Semester 2

Component	Contact Hours
Lecture	22
Practical	22

Grading Basis: 40 %

Assessment Details

Category	Short Description	Description	Weighting (%)	Exam Duration
Report	AS1	Research Report	50	
Artefacts	AS2	Software analysis task	50	

Aims

To familiarize students with common penetration testing techniques, security issues and software vulnerabilities as well as the methods, tools and techniques that can be used during penetration testing to detect such vulnerabilities.
To provide students with an understanding of techniques that should be applied through a penetration testing methodology in order to test for system insecurity.

Learning Outcomes

After completing the module the student should be able to:

1 Analyse software for vulnerabilities.
2 Apply a range of techniques to detect software insecurity.
3 Demonstrate awareness of the technical issues and complexity surrounding software security assessment.
4 Investigate software vulnerabilities through performing penetration tests

Learning Outcomes of Assessments

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

Research Report	1	3
Technical Analysis Task	2	4

Outline Syllabus

Software vulnerability analysis
Low level programming language analysis in a security context
Analysis and exploitation of data structures
Practical penetration and software testing
Operating system security
Use of exploitation tools
Bug and exploitation hunting

Learning Activities

Students will participate in lectures and practical tutorial/lab sessions.

Notes

Students will produce a report discussing aspects of penetration testing and vulnerability analysis. They will consider the various stages of a penetration testing lifecycle and the necessary technologies available in performing software tests. This module follows on from skills developed in the Operating System module and prepares students for a boarder discussion of ethical hacking topics covered in the final year.