

Module Title:	Penetration Testing
Language of Instruction:	English
Credits:	5
NFQ Level:	7
Module Delivered In	2 programme(s)
Teaching & Learning Strategies:	As well as traditional lectures learners will undertake various laboratory exercises. Learners will be expected to actively participate in class and work throughout each scheduled lab session to accomplish assigned tasks.
Module Aim:	To provide learners with a theoretical knowledge and the practical skills of security testing and documenting the security posture of software applications and underlying infrastructure, with particular emphases on web technologies.

Learning Outcomes	
<i>On successful completion of this module the learner should be able to:</i>	
LO1	Appraise and exploit the most prevalent software application security vulnerabilities.
LO2	Produce documentation of activities performed during testing such that vulnerability exploitation is repeatable.
LO3	Produce and justify actionable results with information about possible remediation measures for the successfully identified vulnerabilities.

Pre-requisite learning	
Module Recommendations <i>This is prior learning (or a practical skill) that is recommended before enrolment in this module.</i>	
No recommendations listed	
Incompatible Modules <i>These are modules which have learning outcomes that are too similar to the learning outcomes of this module.</i>	
No incompatible modules listed	
Co-requisite Modules	
No Co-requisite modules listed	
Requirements <i>This is prior learning (or a practical skill) that is mandatory before enrolment in this module is allowed.</i>	
No requirements listed	

Module Content & Assessment

Indicative Content

System Reconnaissance

Reconnaissance, footprinting, google Hacking, network and application scanning tools, enumeration techniques and tools.

System Hacking & Techniques

Hacking web-servers, hacking web applications, OWASP (Open Web Application Security Project) top ten vulnerability categories, hacking wireless networks, hacking mobile platforms, vulnerability exploitation, vulnerability scanning tools, social engineering, session hijacking.

Countermeasures and Evasion

Countermeasure bypass and Evasion techniques

Documentation

Produce documentation of vulnerability analysis. Promote and recommend appropriate protection/vulnerability mitigation measures.

Assessment Breakdown

	%
Continuous Assessment	20.00%
Project	40.00%
End of Module Formal Examination	40.00%

Continuous Assessment

Assessment Type	Assessment Description	Outcome addressed	% of total	Assessment Date
Examination	Examination on content up to week 10	1,3	10.00	Week 10
Examination	Examination on content up to week 4	1,3	10.00	Week 4

Project

Assessment Type	Assessment Description	Outcome addressed	% of total	Assessment Date
Project	Project based on content covered in practical's.	1,2,3	40.00	Week 12

No Practical

End of Module Formal Examination

Assessment Type	Assessment Description	Outcome addressed	% of total	Assessment Date
Formal Exam	The terminal exam will be a 3 hour written test.	1,2,3	40.00	End-of-Semester

SETU Carlow Campus reserves the right to alter the nature and timings of assessment

Module Workload

Workload: Full Time		
<i>Workload Type</i>	<i>Frequency</i>	<i>Average Weekly Learner Workload</i>
Lecture	12 Weeks per Stage	1.00
Laboratory	12 Weeks per Stage	2.00
Independent Learning Time	15 Weeks per Stage	5.93
Total Hours		125.00

Module Delivered In

Programme Code	Programme	Semester	Delivery
CW_KCCYB_B	Bachelor of Science (Honours) in Cyber Crime and IT Security	5	Mandatory
CW_KCCYB_D	Bachelor of Science in Cybercrime and IT Security	5	Mandatory