ZTES H3201: Penetration Testing (Ethical Hacking)

Module Title:	Penetration Testing (Ethical Hacking)
Language of Instruction:	English

Credits:	5

NFQ Level:	7

Module Delivered In	No Programmes

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	
On successful completion of this module the learner should be able to:	
LO1	Apply a repeatable security testing methodology to penetration testing.
LO2	Appraise and exploit the most prevalent software application security vulnerabilities.
LO3	Perform both manual and automated vulnerability identification and analysis.
LO4	Produce documentation of activities performed during testing such that vulnerability exploitation is repeatable.
LO5	Produce and justify actionable results with information about possible remediation measures for the successfully identified vulnerabilities.

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

ZTES H3201: Penetration Testing (Ethical Hacking)

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 Firewalls, IDS, IPS, honeypot and evasion techniques
Documentation Produce documentation of vulnerability analysis. Promote and recommend protection/vulnerability mitigation measures.

Assessment Breakdown	%
Continuous Assessment	20.00%
Project	30.00%
End of Module Formal Examination	50.00%

Continuous Assessment

Assessment Type	*Assessment Description*	*Outcome addressed*	*% of total*	*Assessment Date*
Examination	Assessment on Semester 1 content.	2,5	10.00	Sem 1 End
Examination	Assessment on Semester 2 content.	2,5	10.00	Sem 2 End

Project

Assessment Type	*Assessment Description*	*Outcome addressed*	*% of total*	*Assessment Date*
Project	Project based on content covered in practical's.	1,2,3,4,5	15.00	Sem 1 End
Project	Project based on content covered in practical's	1,2,3,4,5	15.00	Sem 2 End

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.	1,2,3,4,5	50.00	End-of-Semester

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

ZTES H3201: Penetration Testing (Ethical Hacking)

Module Workload

Workload: Full Time		
Workload Type	*Frequency*	*Average Weekly Learner Workload*
Lecture	Every Week	1.00
Laboratory	Every Week	2.00
Independent Learning Time	Every Week	2.00
	Total Hours	5.00