Title	Security Assurance
Long Title	Security Assurance
Credits	5
NFQ Level	Expert
Module Author	Jacqueline Kehoe

Module Description:

T systems inherently have security vulnerabilities both within the individual software applications or at various integration points throughout the system. In this module students will learn how to locate and identify system vulnerabilities along with methods to identify potential vulnerabilities in a system design. The student will also learn methods to validate a system's security meets the organizations security needs. This module was developed under the Cyber Skills HCI Pillar3 Project. Please refer to consortium agreement for ownership.

Learning Outcomes

On successful completion of this module the learner will be able to:

LO1	Critically evaluate the steps involved in defining a process to elicit and document organizational security requirements for a system design.
LO2	Use threat modelling techniques to assess a system architecture identifying exploitable vulnerabilities in the design.
LO3	Using appropriate tools perform a software security analysis, testing the security of a software system against an organizations requirements.
LO4	Appraise current and emerging offensive security techniques.
LO5	To present and prioritise security findings to potential stakeholders.

Indicative Content

Security Requirements Elicitation

Requirements elicitation process, specification, documentation verification, and validation

Security Assurance Strategy Design

Designing a strategy to create and manage a security team dedicated to system vulnerability identification and mitigation in an organization.

Threat Modelling

White box and black box Threat Modelling with a view to locating architecture and design related threats and vulnerabilities; ATASM (Architecture, Threats, Attack Surfaces, Mitigations)

Software Security Analysis

Systematic security testing of code and applications. Testing concepts such as Code Reviews, Static Application Security Testing (SAST), Software Composition Analysis (SCA), and Dynamic Application Security Testing (DAST).

Security Assessment Techniques

Tools and methods which can be employed to locate exploitable vulnerabilities in a system as Black Box testing, penetration testing concepts, root cause analysis methodologies. The introduction of tools such as IDAPro, discussing fuzzing techniques and tools and the use of real-time memory analysis with a view to determining exploitability. Web application security assessment tools: BurpSuite, OWASP ZAP.

Course Work

Assessment Type	*Assessment Description*	*Outcome Addressed*	*% of Total*	*Assessment Date*
Written Report	This report will assess the student's theoretical knowledge of security requirements gathering and evaluation against a system design. The student may be expected to write a report on the current state of the art of offensive security and how this is applicable to a particular industry. The report will prioritise the finding of the security requirements gathered and present those prioritised findings to a range of stakeholders.	1,3,5	40.0	Week 8
Project	The focus of this project will be to execute and document a system security analysis. This will involve both analysis of the architecture and the system. The student will be expected to employ both theoretical and practical knowledge learned in the module to perform this activity. The learner will present the results of their project through a written report on specified targeted areas of the system's security.	1,2,3,4	60.0	Sem End

No End of Module Formal Examination

Assessment Breakdown

	%
Coursework	100

Re-Assessment Requirement

Coursework

This module is reassessed solely on the basis of re-submitted coursework. There is no repeat written examination.

Workload – Full Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Leaner Workload*
Lecture	Lectures covering essential theory.	2.0	Every Week	2.00
Lab	Interactive labs leveraging sophisticated virtualised environment.	2.0	Every Week	2.00

Independent & Directed Learning (Non-contact)	Student independent learning.	3.0	Every Week	3.00
		Total Hours		7
		Total Weekly Learner Workload		7
		Total Weekly Contact Hours		4

Workload – Part Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Leaner Workload*
Lecture	Lectures covering essential theory.	2.0	Every Week	2.00
Lab	Interactive labs leveraging sophisticated virtualised environment.	2.0	Every Week	2.00
Independent & Directed Learning (Non-contact)	Student independent learning.	3.0	Every Week	3.00
		Total Hours		7
		Total Weekly Learner Workload		7
		Total Weekly Contact Hours		4

Recommended Book Resources

- **Brook S. E. Schoenfield 2015, *Securing Systems: Applied Security Architecture and Threat Models*, CRC Press [ISBN: 9781482233971]**