ANAL: Basic Malware Analysis

Module Title:	Basic Malware Analysis
Language of Instruction:	English

Credits:	5

NFQ Level:	8

Module Delivered In	1 programme(s)

Teaching & Learning Strategies:	Learners will be expected to actively participate in class and work through assigned laboratory assessments throughout the year.

Module Aim:	To provide learners with a theoretical knowledge of, and practical skills with, Reverse Engineering and Malware Analysis of Software Systems.

Learning Outcomes	
On successful completion of this module the learner should be able to:	
LO1	Identify and Analyse Malware
LO2	Use Industry Standard Tools for Malware Analysis and Reverse Engineering
LO3	Understand the Techniques used in the Development of Malware

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

ANAL: Basic Malware Analysis

Module Content & Assessment

Indicative Content
Fundamentals Overview of Malware, Techniques used in Malware, Approaches to Reverse Engineering, Ethics
Tools Disassemblers, Debuggers, Process System and Network Monitoring, Code Analysis
Techniques Data Encoding, Obfuscating and De-obfuscating, DLL Injection, Function Hooking, Keylogging, HTTP Communication, Memory Overflow
Reverse Engineering Unpacking Software, Behavioural Analysis, Code Analysis
Malware Analyzing Office and PDF documents, Analyzing Web based Malware, Rootkit Analysis

Assessment Breakdown	%
Continuous Assessment	10.00%
Project	15.00%
Practical	15.00%
End of Module Formal Examination	60.00%

Continuous Assessment

Assessment Type	*Assessment Description*	*Outcome addressed*	*% of total*	*Assessment Date*
Multiple Choice Questions	MCQ tests revising material covered in the lectures.	1,3	10.00	Ongoing

Project

Assessment Type	*Assessment Description*	*Outcome addressed*	*% of total*	*Assessment Date*
Project	Project Work involving larger scale analysis of malware	1,2,3	15.00	Week 11

Practical

Assessment Type	*Assessment Description*	*Outcome addressed*	*% of total*	*Assessment Date*
Practical/Skills Evaluation	Practical Laboratory Work based on lectures. Malware analysis in laboratory settings.	1,2,3	15.00	Every Week

End of Module Formal Examination

Assessment Type	*Assessment Description*	*Outcome addressed*	*% of total*	*Assessment Date*
Formal Exam	n/a	1,3	60.00	End-of-Semester

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

ANAL: Basic Malware Analysis

Module Workload

Workload: Full Time		
Workload Type	*Frequency*	*Average Weekly Learner Workload*
Lecture	12 Weeks per Stage	1.00
Independent Learning	15 Weeks per Stage	5.93
Laboratory	12 Weeks per Stage	2.00
	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	7	Mandatory