CYBERSKILLS
BUILDING IRELAND'S CYBER SECURITY SKILLS

Title	Malware Investigations
Long Title	Malware Investigations
Credits	**5**
NFQ Level	**9**
Module Author	**Gillian O' Carroll**

Module Description:

This course will investigate modern malware types and techniques, and the tools used to analyze, defend and recover from malware attacks.

LO1	Identify and Contrast the different types of malware
LO2	Assess an Operating System as a target platform for malicious code
LO3	Analyze malware through behavioural analysis
LO4	Recommend defenses and develop solutions against malware attacks
LO5	Critically analyse and assess criminal network infrastructure and recommend remediations

Dependencies

Module Recommendations

This is prior learning (or a practical skill) that is strongly recommended before enrolment in this module. You may enrol in this module if you have not acquired the recommended learning but you will have considerable difficulty in passing (i.e. achieving the learning outcomes of) the module. While the prior learning is expressed as named MTU module(s) it also allows for learning (in another module or modules) which is equivalent to the learning specified in the named module(s).

Incompatible Modules

These are modules which have learning outcomes that are too similar to the learning outcomes of this module. You may not earn additional credit for the same learning and therefore you may not enrol in this module if you have successfully completed any modules in the incompatible list.

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. You may not enrol on this module if you have not acquired the learning specified in this section.

No requirements listed

Assessment Type	*Assessment Description*	*Outcome Addressed*	*% of Total*	*Assessment Date*
Written Report	Practical assignment based on blackboxing analysis of a given malware sample, and compiling a detailed report on its activities	1,2,3	50	Week 6
Written report	Project to carry out an internet investigation into the infrastructure of a piece of malware, as well as determining defences to protect against future attacks.	4,5	50	Sem End
No End Of Module Formal Examination				

Assessment Breakdown

Coursework	100%

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

Workload Type		*Hours*	*Frequency*	*Average Weekly Leaner Workload*
Lecture	Lecture	2	Every Week	2.00

Lab	Implementation of malware analysis tools	1	Every Week	1.00
Independent & Directed Learning (Non-contact)	Independent & Directed Learning	4	Every Week	4.00
		Total Hours		7.00
		Total Weekly Learner Workload		7.00
		Total Weekly Contact Hours		3.00

Workload Type		*Hours*	*Frequency*	*Average Weekly Leaner Workload*
Lecture	Lecture	2	Every Week	2.00
Lab	Implementation of malware analysis tools	1	Every Week	1.00
Independent & Directed Learning (Non-contact)	Independent & Directed Learning	4	Every Week	4.00
		Total Hours		7.00
		Total Weekly Learner Workload		7.00
		Total Weekly Contact Hours		3.00

Recommended Book Resources

Michael Ligh, Steven Adair, Blake Hartstein, Matthew Richard. (2011), Malware Analyst's Cookbook and DVD, John Wiley & Sons, Inc., [ISBN: 978-047061303].
Michael Sikorski, Andrew Honig. (2012), Practical Malware Analysis, No Starch Press, [ISBN: 978-159327290].
Peter Szor. (2005), The Art of Computer Virus Research and Defense, 1. Addison Wesley, [ISBN: 978-032130454].