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

Module Description:

This module teaches students the skills required for indepth investigations of modern malware, and the tools used to analyze, defend and recover from malware attacks. Particular emphasis will be put on more advanced topics like Reverse Engineering, and Debugging – as well as low level descriptions of the Windows OS and file formats used by malware. These approaches are key to move from the knowledge of what a malware is doing to the system (from blackboxing), to a deeper level of understanding of the purpose of the code itself.

LO1	Evaluate techniques at the forefront of the discipline used in detection strategies and the defence of systems against malicious attacks.
LO2	Assess complex evidence and communicate subject knowledge clearly to specialist and non-specialist audiences.
LO3	Examine a commercial Operating System as an attack platform for malicious code.
LO4	Analyze common non-operating system executable malware, such as PDF or Android
LO5	Appraise malware through reverse engineering and debugging

Windows as an attack surface
System Load Points, Windows Registry, Windows Kernel, Code Injection, System call hooking, Layered Service Providers, Windows Services, Browser Helper Objects, Malware removal from infected systems, Malware defenses, Rootkits

Reverse Engineering & Debugging
Microsoft Windows PE File format, x86 assembly language, Disassembly and debugging with IDA, Packer analysis, Malware anti-debugging techniques, Windows API

Non-Windows Executable Malware
PDF File Format, Analysing PDF files, Android Malware, Document Malware

Core Tools and Techniques
Interactive Dissassembler for Reverse Engineering of malware samples. Ollydby to debug and live analyse running malware code. Dependancy Walker, PE Builder and PeiD to examine in-depth files that make use of the Windows PE file format (used by exe, scr, dll and sys files among others). Different techniques for File Infector malware, and how to disinfect files affected by it. Analysis of packed malware through the use of unpacker tools, but also via dumping memory contents and patching the resulting binaries using Volatilty and other tools. Analysing Android malware with tools such as Dex2Jar. Analysis of PDF files using the Didier Stevens suite of tools. Analysis of Malicious DOC Files.

Assessment Type	*Assessment Description*	*Outcome Addressed*	*% of Total*	*Assessment Date*
Project	Assignment based on reverse engineering of a given malware sample, and compiling a detailed report on its activities	1,2,3	40	Week 7
Project	Assignment based on the reverse engineering and debugging of a given sophisticated malware sample designed to defeat several anti-analysis countermeasures, and compiling a detailed report on its activities	1,4,5	60	Sem End
No End Of Module Formal Examination				

Assessment Breakdown

Coursework

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
Directed Learning	Implementation of Malware Analysis Tools	2	Every Week	2.00
Independent & Directed Learning (Non-contact)	Independent & Directed Learning	3	Every Week	3.00
		Total Hours		7.00
		Total Weekly Learner Workload		7.00
		Total Weekly Contact Hours		2.00

Workload Type		*Hours*	*Frequency*	*Average Weekly Leaner Workload*
Lecture	Lecture	2	Every Week	2.00
Lab	Implementation of Malware Analysis Tools	2	Every Week	2.00
Independent & Directed Learning (Non-contact)	Independent & Directed Learning	3	Every Week	3.00
		Total Hours		7.00
		Total Weekly Learner Workload		7.00
		Total Weekly Contact Hours		4.00

Recommended Book Resources

Eldam Eilam. (2005), Reversing : Secrets of Reverse Engineering, 1. Wiley Publishing inc., [ISBN: 9780764574818].
Richard C Detmer. (2009), Introduction to 80x86 Assembly Language and Computer Architecture, Jones & Bartlett Publishers, [ISBN: 9780763772239].
Kris Kaspersky. (2007), Hacker Disassembling Uncovered, 2. [ISBN: 9781931769648].