Title	Malware Behaviour Analysis
Long Title	Malware Behaviour Analysis
Credits	**5**
NFQ Level	Expert
Module Author	Prof Donna O'Shea

Module Description:

Malware analysis is used as part of a forensic investigation to understand the behavior and purpose of malware which is designed to cause harm or exploit any programmable device, service or network. In this module students will learn how to analyse static and dynamic malware samples and investigate malware using memory forensics.

Learning Outcomes

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

LO1	Critically analyse and differentiate between the main categories of malware and its obfuscation techniques.
LO2	Analyse malware using static techniques gleaning information about its behaviour.
LO3	Observe and interact with a malware sample observing its dynamic behaviour.
LO4	Conduct forensic analysis in multiple operating systems and environments.
LO5	Conduct a deep analysis of captured malicious code using memory forensics.

Indicative Content

Malware Fundamentals

Types of Malicious software. Virus / Worm / Trojan horse / Backdoors / Adware / Keystroke loggers / Botnets / Rootkits. How does malware spread. How can malware affect you. Infection Vectors, Blended Attacks, Botnets, Command & Control setups, AV Engines, YARA, Cuckoo, Botnet Takedowns. Malware obfuscation techniques – encryption, encoding, malware unpacking.

Malware Analysis

Malware analysis types - Behavioral malware analysis– types and stages; Reverse Engineering malware. Malware analysis as a tool for incident responders. Signatures versus behaviors. Case studies of high-profile malware attacks – HSE ransomware attack.

Malware Prevention & Detection

Vulnerability assessment and detection. Software patches and management. Anti-malware/anti-virus software. Case studies of vulnerability and patch management as a defence i.e. WannaCry. Should you pay the ransom. Defence in depth strategy. What to do if you are infected. Reporting a cyber incident.

Malware Static Analysis

Fingerprinting the malware, extracting strings, file obfuscation, file dependencies, classifying malware. Blackboxing. Rootkits

Malware Behavioural Analysis

Create a sandbox using virtual machines. Monitoring malware tools and techniques. Viewing normal and malware processes. Windows registry and comparing registry snapshots. Faking a network. Packet sniffing.

Analysing Malicious Malware Executable

Windows registry. Programs that run. Common registry function. Networking APIs. DLLs, processes, threads, services, kernel versus user mode.

Hunting Malware - Memory forensics

Memory acquisition. Volatility. Enumerating processes. Listing and dumping DDLs, process handles. Listing network connections and sockets. Inspecting windows registry and services. Extracting command history.

Course Work

Assessment Type	*Assessment Description*	*Outcome Addressed*	*% of Total*	*Assessment Date*
Project	Analyse malware using static analysis techniques without running the malware.	1,2,5	40.0	Week 6
Project	Analyse malware using dynamic methods with the malware running in a secure system. Write a report detailing the output of a memory forensics investigation.	1,2,4,5	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 the theoretical concepts underpinning the learning outcomes	2.0	Every Week	3.0
Lab	Lab to support the learning outcomes.	2.0	Every Week	2.0
Independent & Directed Learning (Non-contact)	Independent learning by the student.	3.0	Every Week	3.0

		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 the theoretical concepts underpinning the learning outcomes.	2.0	Every Week	2.0
Lab	Lab to support the learning outcomes.	2.0	Every Week	2.0
Independent & Directed Learning (Non-contact)	Independent learning by the student.	3.0	Every Week	3.0
		Total Hours		7
		Total Weekly Learner Workload		7
		Total Weekly Contact Hours		4

Recommended Book Resources

- **Monnappa K A 2018, Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware, Packt [ISBN: 9781788392501]**