H9MWAN: Malware Analysis

Module Code:	H9MWAN
Long Title	Malware Analysis APPROVED
Title	Malware Analysis
Module Level:	LEVEL 9
EQF Level:	7
EHEA Level:	Second Cycle
Credits:	5
Module Coordinator:	Arghir Moldovan
Module Author:	Margarete Silva
Departments:	School of Computing
Specifications of the qualifications and experience required of staff	PhD/Master's degree in a computing or cognate discipline. May have industry experience also.

Learning Outcomes	
On successful completion of this module the learner will be able to:	
#	**Learning Outcome Description**
LO1	Research, compare and contrast the different types of malware.
LO2	Evaluate the Windows Operating System as a target platform for malicious code.
LO3	Investigate and assess malware through behavourial analysis and sandboxing.
LO4	Design, evaluate and implement defence solutions to prevent against malware attack.
LO5	Analyse criminal infrastructure as part of an online malware investigation.

Dependencies
Module Recommendations
No recommendations listed
Co-requisite Modules
No Co-requisite modules listed

Entry requirements	Programme entry requirements must be satisfied.

H9MWAN: Malware Analysis

Module Content & Assessment

Indicative Content
Introduction / Cyber Landscape Cyber Threat Landscape, Cybercrime, Cost of Malware, Cyber Kill Chain, Future Trends
Malware Types and Lab Setup Trojan Horses, Backdoors, Worms, Downloaders and Droppers, Bots, Ransomware, Spyware, Adware, Rootkits, Viruses
Extracting / Handling / Discovering Malware The Anatomy of an Attack, Indications of an infection, Scanning with AV, Scanning for Rootkits, Examining memory Dumps
Static Analysis Hashes, Strings, PE file structure, Compression, Obfuscation, Unpacking
Dynamic Analysis Change Monitoring Tools, Memory Forensics, Realtime Monitoring – Process Changes, File system changes, Registry changes, Network Traffic
Rootkits and Memory Forensics x86 privilege rings, Windows modes, Unstructured and Structured analysis of memory dumps
Internet Forensics Malware Search, Indicators, Intelligence Analysis, People Search
PDFs and Office Documents Analysing PDF files, Understanding Office Macros
Underground Actors MaaS, Types of Actors, Tracking Underground Actors
Botnets and PCAP Analysis Architecture, Backdoors and RATs, C&C, Multi-headed, DGA, Fast flux, Multi-tier, P2P etc., Botnet Takedown approaches, Sinkholing
Reverse Engineering Assembly language concepts, Compilers and Decompilers
Android Malware Analysis Structure of APKs, Analysis tools, Permissions

Assessment Breakdown	%
Coursework	100.00%

Assessments

Full Time

Coursework

Assessment Type:	Formative Assessment	**% of total:**	Non-Marked
Assessment Date:	n/a	**Outcome addressed:**	1,2,3,4,5
Non-Marked:	Yes		

Assessment Description:
Formative assessment will be provided on the in-class individual or group activities. Feedback will be provided in written or oral format, or on-line through Moodle. In addition, in class discussions will be undertaken as part of the practical approach to learning.

Assessment Type:	Continuous Assessment	**% of total:**	50
Assessment Date:	n/a	**Outcome addressed:**	1,2,3
Non-Marked:	No		

Assessment Description:
Assignment to set up a Malware Lab and to carry out a research-based investigation into a given malware sample

Assessment Type:	Project	**% of total:**	50
Assessment Date:	n/a	**Outcome addressed:**	3,4,5
Non-Marked:	No		

Assessment Description:
Project to carry out an internet investigation into the infrastructure of a given botnet, as well as determining defences to protect against future attacks.

No End of Module Assessment

No Workplace Assessment

Reassessment Requirement

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

Reassessment Description
The reassessment strategy for this module will consist of a project that will assess all learning outcomes.

H9MWAN: Malware Analysis

Module Workload

Module Target Workload Hours 0 Hours

Workload: Full Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	Classroom and demonstrations	24	Per Semester	2.00
Tutorial	Mentoring and small-group tutoring	12	Per Semester	1.00
Independent Learning	Independent learning	89	Per Semester	7.42
			Total Weekly Contact Hours	3.00

Workload: Blended

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	Classroom and demonstrations	12	Per Semester	1.00
Tutorial	Mentoring and small-group tutoring	12	Per Semester	1.00
Directed Learning	Directed e-learning	12	Per Semester	1.00
Independent Learning	Independent learning	89	Per Semester	7.42
			Total Weekly Contact Hours	3.00

Workload: Part Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	Classroom and demonstrations	24	Per Semester	2.00
Tutorial	Mentoring and small-group tutoring	12	Per Semester	1.00
Independent Learning	Independent learning	89	Per Semester	7.42
			Total Weekly Contact Hours	3.00

Module Resources

Recommended Book Resources

Alexey Kleymenov,Amr Thabet. Mastering Malware Analysis: The complete malware analyst's guide to combating malicious software, APT, cybercrime, and IoT attacks, 2nd Edition. Packt Publishing, [ISBN: 978-1789610789].

Abhijit Mohanta,Anoop Saldanha. (2020), Malware Analysis and Detection Engineering: A Comprehensive Approach to Detect and Analyze Modern Malware, Apress, p.780, [ISBN: 978-1484261927].

Supplementary Book Resources

Michael Sikorski,Andrew Honig. (2012), Practical Malware Analysis, 3rd Edition. No Starch Press, p.802, [ISBN: 978-1593272906].

Michael Ligh,Steven Adair,Blake Hartstein,Matthew Richard. (2010), Malware Analyst's Cookbook and DVD, John Wiley & Sons, p.747, [ISBN: 978-0470613030].

This module does not have any article/paper resources

Other Resources

[Website], SysInternals, http://technet.microsoft.com/en-us/sysin ternals/default.aspx

[Website], PE Format, https://learn.microsoft.com/en-gb/window s/win32/debug/pe-format

Discussion Note:	