MULTIMEDIA UNIVERSITY®

SUMMARY OF INFORMATION ON EACH COURSE

1.	Name of Course	Malware and Intrusion Detection
2.	Course Code	TMI 3231
3.	Status of Course [Applies to (cohort)]	Specialisation Core for B.IT Security Technology
4.	MQF Level/Stage Note : *Certificate – MQF Level 3* *Diploma – MQF Level 4* *Bachelor – MQF Level 6* *Masters – MQF Level 7* *Doctoral – MQF Level 8*	Bachelor – MQF Level 6
5.	Version (State the date of the Senate approval – history of previous and current approval date)	Date of previous version: June 2012 Date of current version: June 2014
6.	Pre-Requisite	TCS2251 Computer Security
7.	Name(s) of academic/teaching staff	Teo Chuan Chin Jaya Kumar Krishnan Rouzbeh Behnia
8.	Semester and Year offered	Trimester 2, Year 3
9.	Objective of the course in the programme : This course addresses the concepts of the computer viruses and intrusion detection system. Students will learn on how to prevent, detect and remove malware by assessing the event's scope, severity, and repercussions.	
10.	Justification for including the course in the programme : Malware and Intrusion Detection is one of the major domains of security studies. The course will cover techniques for detection of security violations in computer systems. Such techniques allow a swift response to security incidents and complement traditional preventive security mechanisms.	

11.

Course Learning Outcomes :	Domain	Level
LO1 Demonstrate an understanding of various computer malware and intrusion detection methods.	Cognitive	3
LO2 Identify damage from an intrusion, and analyse the indicators of compromise that will reveal other machines that have been affected by the same malware or intruders.	Cognitive	4
LO3 Revise the vulnerability that was exploited to allow the malware to get there in the first place.	Cognitive	5
LO4 Evaluate the security of the system and the network.	Cognitive	6

12. Mapping of Learning Outcomes to Programme Outcomes :

Learning Outcomes	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9

SUMMARY OF INFORMATION ON EACH COURSE

	LO1	X						X		
	LO2	X						X	X	
	LO3	X						X	X	X
	LO4	X						X	X	X

13. Assessment Methods and Types :

Method and Type	Description/Details	Percentage
Mid Test	Written test	15%
Laboratory	Practical work and report	15%
Quizzes	Written quizzes	10%
Final Examination	Written examination	60%

14. Mapping of assessment components to learning outcomes (LOs)

Assessment Components	LO1	LO2	LO3	LO4
Mid Test	17.6	15		15
Laboratory		15	100	15
Quizzes	11.8	10		10
Final Examination	70.6	60		60

15. Details of Course

Topics	Mode of Delivery (eg : Lecture, Tutorial, Workshop, Seminar, etc.) Indicate allocation of SLT (lecture, tutorial, lab) for each subtopic	
	Lecture	Lab
1 Introduction Introduction to Information Security. Component Parts of Information Security in General and Network Security. Critical Concepts Of Information and Network Security. Business Need for Information and Network Security. Introduction to Computer Viruses and Vulnerabilities. General Information About Computer Viruses. How to Deal with Viruses. How to Protect from Viruses. Computer Viruses in Malaysia. How Computer Viruses Have Spread Out Around The World. Computer Viruses and Network Security.	4	4
2 Malware and Social Engineering Malicious Software. Different Types of Malware. File Infection Techniques of Viruses. Countermeasure.	4	4

SUMMARY OF INFORMATION ON EACH COURSE

	Generations of Antivirus. Recognizing Social Engineering Tactics.		
	3 Firewalls Introduction to Firewalls. Common Misconceptions about Firewalls. Types of Firewall Protection. Limitations of Firewalls.	2	2
	4 Packet Filtering Packets and Packet Filtering. Approaches to Packet Filtering. Filtering Rules based on Business Needs.	2	2
	5 Firewall Configuration and Administration Different Firewall Configuration Strategies. Remote Management Interface. Tracking Firewall Log Files.	2	2
	6 Proxy Servers and Application-Level Firewalls Proxy Servers. Critical Issues in Proxy Server Configurations. Evaluation on Proxy-Based Firewall Products. Deploy and Use Reverse Proxy.	2	2
	7 Bastion Host Security Requirements. Different Options for Positioning the Bastion Host. Bastion Host Configuration.	4	4
	8 Securing Network Intrusion Detection System. Intrusion Prevention System. Securing Wireless Networks. Exploring Remote Access.	2	2
	9 Encryption – Foundation for the Virtual Private Network Encryption in Firewall and VPN Architectures. Digital Certificates. SSL, PGP. IPSec.	2	2
	10 Virtual Private Network Components and Essential Operations of VPN. Types of VPNs. VPN Tunneling Protocol.	2	2
	Total	**26**	**26**

Total Student Learning Time (SLT)	Face to Face / Guided Learning	Independent Learning
Lecture	26	26
Tutorials	0	0
Laboratory/Practical	26	13
Presentation	0	0
Assignment	0	0
Mid Term Test	1	5
Final Exam	2	15

SUMMARY OF INFORMATION ON EACH COURSE

	Quizzes	6 times	6
	Sub Total	55	65
	Total SLT	**120**	
16.	Credit Value	**120/40 = 3**	
17.	Reading Materials :		
	Textbooks		
	Michael E. Whitman, Herbert J. Mattord, Andrew Green, (2011). Guide to Firewalls & VPNs, Cengage Learning, ISBN-13: 978-1-111-13539-3. Christopher C. Elisan, (2012). Malware, Rootkits & Botnets: A Beginner's Guide, McGraw Hill, ISBN-13: 978-0071792066.		
	Reference Material (including 'Statutes' for Law)		
	Chris Eagle, (2011). The IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler, 2nd Ed. No Starch Press, ISBN-13: 978-1593272890. Cameron H.Malin, Eoghan Casey, James M. Aguilina, (2008). Malware Forensics: Investigating and Analyzing Malicious Code, Syngress, ISBN-13: 978-1597492683. Peter Szor, (2005). The Art of Computer Virus Research and Defense, Addison-Wesley, ISBN-13: 978-0321304544.		

Appendix (to be compiled when submitting the complete syllabus for the programme) :

1. Mission and Vision of the University and Faculty
2. Programme Objectives or Programme Educational Objectives
3. Programme Outcomes (POs)
4. Mapping of POs to the 8 MQF domain
5. Summary of the Bloom's Taxonomy's Domain Coverage in all the Los in the format below :

Subject	Learning Outcomes (please state the learning 0utcomes)	Bloom's Taxonomy Domain		
		Affective	Cognitive	Psychomotor
ABC1234	Learning Outcome 1			
	Learning Outcome 2			
	Learning Outcome 3			
	Learning Outcome 4			
DEF5678	Learning Outcome 1			
	Learning Outcome 2			
	Learning Outcome 3			
	Learning Outcome 4			

6. Summary of LO to PO measurement
7. Measurement and Tabulation of result for LO achievement
8. Measurement Tabulation of result for PO achievement

MULTIMEDIA UNIVERSITY®

SUMMARY OF INFORMATION ON EACH COURSE