1.	Name of Course/Module	Computer Virus and Intrusion Detection
2.	Course Code	TCV2521
3.	Status of Subject	Major for B.IT Security Technology
4.	MQF Level/Stage	Bachelor Degree – MQF Level 6
5.	Version (state the date of the last Senate approval)	June 2012
6.	Requirement for Registration	TSC2211 Computer Security
7.	Name(s) of academic/teaching staff	Ooi Shih Yin Ho Yean Li
8.	Semester and Year offered	Trimester 2 (Delta Level)

9. Objective of the course/module in the programme :

This course addresses the concepts of the computer viruses and intrusion detection system. Students will learn on how to reverse-engineer malware by assessing the event's scope, severity, and repercussions.

10. Learning Outcomes :

At the completion of the subject, students should be able to:

LO1: Demonstrate an understanding of various computer malware and intrusion detection methods (Cognitive, Level 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, Level 4)
LO3: Revise the vulnerability that was exploited to allow the malware to get there in the first place (Cognitive, Level 5)
LO4: Evaluate the security of the system and the network (Cognitive, Level 6)

11. Synopsis:

This course provides a rounded approach to reverse-engineering by covering both behavioral and code phases of the analysis process. As a result, the course makes malware analysis accessible even to individuals with a limited exposure to programming concepts.

Kursus ini menyediakan satu pendekatan tentang sebalik-kejuruteraan melalui fasa-fasa tingkah laku dan kod analisis. Hasilnya, kursus membuat analisis malware yang boleh diakses walaupun individu yang mempunyai pendedahan yang terhad kepada konsep pengaturcaraan.

12. Mapping of Subject to Programme Outcomes :

Programme Outcomes	**% of Contribution**
PO1: Apply soft skills in work and career related activities	30.77
PO7: Demonstrate knowledge and understanding of essential facts, concepts, principles, and theories relating to security technology	30.77
PO8: Apply principles and knowledge of security technology in relevant areas	23.08

	PO9: Design, integrate, implement and manage information technology solutions and resources, and recognise the impact of technology on individuals, organisations and society	15.38

13. Assessment Methods and Types :

Method and Type	Description/Details	Percentage
Mid Test	Written Test	15%
Laboratory	Practical Work and Report	15%
Quiz	Written Quiz	10%
Final Exam	Written Exam	60%

14. Details of Subject

Topics	Mode of Delivery	
	Lecture	Lab
1. Introduction Introduction to Computer Viruses. 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.	1	1
2. Introduction to Malware Overview of Malware. Terminology.	1	1
3. Introduction to Reverse Engineering Overview of Reverse Engineering. Compilation Process. Why Do Reverse Engineering. Legal and Ethical Aspects. Illegal Uses of Reverse Engineering. Decompilation Process.	1	1
4. The Basics of Reverse Engineering Binary Numbers. Byte Order a.k.a. Endianness. Endianness Matters. System Endianness. ASCII Code. Unicode Strings. String Storage. Intel x86 Architecture. Data Register Layout. Data, Address, Segment, EFLAGS Registers. Mnemonics. Reversing C Code.	3	3
5. Malware Analysis and Antivirus Technologies: Windows Operating System Applications on Windows. Processes and Threads. Windows Architecture. System Mechanisms. Management Mechanisms. Memory Mechanisms. File Systems. Security Mechanisms. Driver Basics.	2	2
6. Kernel Malware Brain. Overview of Kernel Malware. Key Techniques. Kernel-Mode Support Routines. Rootkit Techniques. Evolution. Detection and Removal.	3	3

	7. Mobile Malware Mobile Security. Mobile Malware Overview. Trojanised Applications. Prevention. Exploits in Apps. Spytools. Way to Mitigate Possible Malware Incidents.	3	3
	8. AV Engines Detecting Malware. Strategies. Scanning Methods. Subcomponents of an Antivirus Engine. Design Principles. Virus-Specific Detections. Emulation.	3	3
	9. Intrusion Detection Intrusion Detection Architecture, Intrusion Detection Concepts, Intruder Types, Intrusion Methods, Intrusion Process, Detection Methods, IDES.	3	3
	10. Network Intrusion Detection Network Attack Characteristics, NSM, DIDS, NADIR, etc.	2	2
	11. Damage Control and Assessment Damage Control Techniques, Damage Assessment: Attack Recovery, Damage Prevention, Incident Recovery.	3	3
	12. Security of the Internet Overview of Internet Security, Security Concepts, Network Security Incidents, Internet Vulnerabilities, Security Technology, The Future.	3	3
	Total	**28**	**28**

15.	Laboratory		
	Students will learn on how to use/ configure the following tools: • Several types of anti-virus engine • Snort (IDS)		
16.	Total Student Learning Time (SLT)	Face to Face (Hour)	Total Guided and Independent Learning
	Lecture	28	28
	Tutorials	-	-
	Laboratory/Practical	28	14
	Presentation	-	-
	Assignment	-	-
	Mid Term Test	1	5
	Lab Test	-	-
	Final Exam	2	20
	Quiz	6	6
	Sub Total	65	73
	Total SLT	138/40 = 3.45 => 3	
17.	Credit Value	3	
18.	Reading Materials :		

	Textbook	Reference Materials
	1. Peter Szor, "The Art of Computer Virus Research and Defense", Addison-Wesley, 2005. ISBN-13: 978-0321304544	1. Chris Eagle, "The IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler", 2nd Ed. No Starch Press, 2011. ISBN-13: 978-1593272890 2. Cameron H.Malin, Eoghan Casey, James M. Aguilina, "Malware Forensics: Investigating and Analyzing Malicious Code", Syngress, 2008. ISBN-13: 978-1597492683
19.	Appendix (to be compiled when submitting the complete syllabus for the programme) : 1. Mission and Vision of the University and Faculty 2. Mapping of Programme Objectives to Vision and Mission of Faculty and University 3. Mapping of Programme Outcome to Programme Objectives 4. Programme Objective and Outcomes (Measurement and Descriptions)	