MULTIMEDIA UNIVERSITY®

SUMMARY OF INFORMATION ON EACH COURSE

1.	Name of Course	Ethical Hacking and Security Assessment
2.	Course Code	TEH 3221
3.	Status of Course [Applies to (cohort)]	Specialisation Core for B.IT (Hons) 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 Degree – 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	TDC1231 Data Communications and Networking
7.	Name(s) of academic/teaching staff	Ooi Shih Yin
8.	Semester and Year offered	Trimester 2, Year 3
9.	Objective of the course in the programme : To help the students master an ethical hacking methodology that can be used in a penetration testing or ethical hacking.	
10.	Justification for including the course in the programme : This course prepares the students with the knowledge on ethical hacking methodology, common practices and techniques used by computer hackers, and security assessment procedures. After learning this course, students shall be able to evaluate, select and design the best security systems for their computer and network.	

11.	Course Learning Outcomes :		Domain	Level
	LO1	Apply and discover the hacking techniques and prevention techniques.	Cognitive	3
	LO2	Analyse and identify the vulnerabilities of the system and the network.	Cognitive	4
	LO3	Plan and design the countermeasures.	Cognitive	5
	LO4	Evaluate the security of the system and the network.	Cognitive	6
12.	Mapping of Learning Outcomes to Programme Outcomes :			

MULTIMEDIA UNIVERSITY®

SUMMARY OF INFORMATION ON EACH COURSE

	Learning Outcomes	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9
	LO1	X						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	10%
Laboratory	Practical Work and Report	20%
Quiz	Written Quiz	10%
Final Exam	Written Exam	60%

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

Assessment Components	LO1	LO2	LO3	LO4
Mid Test		10	12.5	12.5
Laboratory	100	20		
Quiz		10	12.5	12.5
Final Exam		60	75	75

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. **Ethical Hacking Overview** Introduction to Ethical Hacking. The Role of Security and Penetration Tester. Penetration-Testing Methodologies. Certification Programs for Network Security Personnel. Laws of the Land. Recent Hacking Cases. Federal Laws. Anti-Spam Vigilantes.	2	2
2. **TCP/IP Concepts Review** Overview of TCP/IP. Four Different Layers of TCP/IP Protocol Stack. Basic Concepts of IP Addressing. Binary, Octal, and Hexadecimal Numbering System.	2	2
3. **Network and Computer Attacks** Different Types of Malicious Software. Methods of Protecting Against Malware Attacks. Types of Network Attacks. Physical Security Attacks and Vulnerabilities.	2	2

SUMMARY OF INFORMATION ON EACH COURSE

	4. **Footprinting and Social Engineering** Web Tools for Footprinting. Competitive Intelligence. DNS Zone Transfers. Types of Social Engineering.	2	2
	5. **Port Scanning** Port Scanning Overview. Different Types of Port Scans. Port-Scanning Tools. To Conduct Ping Sweeps. Shell Scripting.	2	2
	6. **Enumeration** Enumeration Step of Security Testing. Enumerate Microsoft OS Targets. Enumerate NetWare OS Targets. Enumerate *NIX OS Targets.	2	2
	7. **Programming for Security Professionals** Basic Programming Concepts. Simple C Program. Create Web Pages with HTML. Basic Perl Programs. Basic Object-Oriented Programming Concepts.	2	2
	8. **Desktop and Server OS Vulnerabilities** Describe the Vulnerabilities of Windows and Linux Operating Systems. Identify Specific Vulnerabilities and Explain Ways to Fix Them. Techniques to Harden Systems Against Windows and Linux Vulnerabilities.	2	2
	9. **Embedded Operating Systems: The Hidden Threat** Embedded Operating Systems Overview. Windows and Other Embedded Operating Systems. Vulnerabilities of Embedded Operating Systems and Best Practices for Protecting Them.	2	2
	10. **Hacking Web Servers** Web Applications. Web Application Vulnerabilities. The Tools Used to Attack Web Servers.	2	2
	11. **Hacking Wireless Networks** Wireless Technology. Wireless Networking Standards. Process of Authentication. Wardriving. Wireless Hacking and Tools Used by Hackers and Security Professionals.	2	2
	12. **Cryptography** Overview of Cryptography. Symmetric and Asymmetric Cryptography Algorithms. Public Key Infrastructure (PKI). Possible Attacks on Cryptosystems.	2	2
	13. **Network Protection Systems** Network Security Devices. Firewall Technology. Intrusion Detection Systems. Honeypots.	2	2
	Total	**26**	**26**

15.	Total Student Learning Time (SLT)	Face to Face / Guided Learning	Independent Learning
	Lecture	26	26

SUMMARY OF INFORMATION ON EACH COURSE

	Tutorials	0	0
	Laboratory/Practical	26	13
	Presentation	0	0
	Assignment	0	0
	Mid Term Test	1	5
	Final Exam	2	17
	Quizzes	4 times	4
	Sub Total	55	65
	Total SLT	**120**	
	Credit Value	**120/40 = 3**	

16. Reading Materials :

Textbooks

1. Michael T. Simpson, Kent Backman, James E.Corley, (2012). Hands-On Ethical Hacking and Network Defense, Cengage Learning. ISBN-13: 978-1-1339-3561-2

Reference Material (including 'Statutes' for Law)

1. Ed Skoudis with Tom Liston, (2007). Counter Hack Reloaded, 2nd Ed. Prentice Hall. ISBN: 0-13-148104-5

2. Jack Koziol, David Litchfield, Dave Aitel, Chris Anley, Sinan Eren, Neel Mehta, Riley Hassell, (2004). The Shellcoder's Handbook, Wiley Publishing. ISBN: 0-7645-4468-3

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