1.	Name of Course/Module	Ethical Hacking and Security Assessment
2.	Course Code	THT2531
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	TCE2311 Data Communications and Networking
7.	Name(s) of academic/teaching staff	Ooi Shih Yin Asrul Hadi b Yaacob Ong Thian Song
8.	Semester and Year offered	Trimester 2 (Delta Level)

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

To help the students master an ethical hacking methodology that can be used in a penetration testing or ethical hacking.

10. Learning Outcomes :

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

LO1: Apply and discover the hacking techniques and prevention techniques (Cognitive, Level 3)
LO2: Analyse and identify the vulnerabilities of the system and the network (Cognitive, Level 4)
LO3: Plan and design the countermeasures (Cognitive, Level 5)
LO4: Evaluate the security of the system and the network (Cognitive, Level 6)

11. Synopsis:

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.

Kursus ini akan memberi pengetahuan tentang cara-cara 'ethical hacking', teknik yang digunakan untuk 'hacking', dan langkah-langkah peninjauan keselamatan. Pelajar-pelajar akan dapat menilai, memilih dan merangka sistem keselamatan yang paling sesuai untuk sistem komputer mereka.

12. Mapping of Subject to Programme Outcomes :

Programme Outcomes	**% of Contribution**
PO1: Apply soft skills in work and career related activities	28.57
PO7: Demonstrate knowledge and understanding of essential facts, concepts, principles, and theories relating to security technology	28.57
PO8: Apply principles and knowledge of security technology in relevant areas	28.57
PO9: Design, integrate, implement and manage information technology solutions and resources, and recognise the impact of technology on individuals, organisations and society	14.29

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. Details of Subject

Topics	Mode of Delivery	
	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
4. Footprinting and Social Engineering Web Tools for Footprinting. Competitive Intelligence. DNS Zone Transfers. Types of Social Engineering.	3	3
5. Port Scanning Port Scanning Overview. Different Types of Port Scans. Port-Scanning Tools. To Conduct Ping Sweeps. Shell Scripting.	3	3
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	**28**	**28**

15. Laboratory

- Implementation using Metasploit
- Stealing passwords with a packet sniffer, e.g.: Wireshark
- Using whois in a Terminal Windows
- Conduct a scanning session by using the Nmap tool
- NetBIOS enumeration, enumeration using SuperScan
- C programming on Ubuntu
- Demonstrate the HTML concept
- Explore the password auditing tool to crack the encrypted password, e.g.: John the Ripper, Cain and Abel.
- Using a software keylogger
- Performing a denial of service attack with Nmap
- Performing wireless hacking within a control environment
- Implementation using simulated honeypots

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	3
Lab Test	-	-

	Final Exam	2	16
	Quiz	9	9
	Sub Total	68	70
	Total SLT	138/40 = 3.45 => 3	
17.	Credit Value	3	
18.	Reading Materials :		
	Textbook	Reference Materials	
	1. Michael T. Simpson, Kent Backman, James E.Corley, "Hands-On Ethical Hacking and Networking Defense", 2nd Ed. Cengage Learning, 2011. ISBN-13: 978-1-4354-9665-1	1. Ed Skoudis with Tom Liston, "Counter Hack Reloaded", 2nd Ed. Prentice Hall, 2007. ISBN: 0-13-148104-5 2. Jack Koziol, David Litchfield, Dave Aitel, Chris Anley, Sinan Eren, Neel Mehta, Riley Hassell, "The Shellcoder's Handbook", Wiley Publishing, 2004. ISBN: 0-7645-4468-3	
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)		