1. Title of subject	Ethical Hacking and Security Assessment
2. Subject code	THT 2531
3. Status of subject	Major
4. Credit Hours	3 28 Hours of Lecture 28 Hours of Lab LAN Credit Hours Equivalence: 3.00
5. Pre-Requisite	TCE2311 Data Communication & Telecommunications Systems
6. Assessment	Course Work Assessment 40% Final Exam 60% **Total 100%**
7. Methods of teaching	28 Hours of Lecture 28 Hours of Lab
8. Teaching staff (Proposed)	Mr. Asrul Hadi
9. Semester	Trimester 3 (Gamma Level)
10. Objective of subject	By the end of the course, students will learn about different techniques and methods applied by hackers. Students will also learn the prevention methods for these hacking and how to minimize the risks of such attacks.
11. Synopsis of subject	The course aims to impart knowledge on assessment of computer security and hacking prevention so that students are able to provide and design the best solutions for their computer and network systems. Students will learn about the common practices and techniques used by computer hackers so that they are able to evaluate, select and design the best security systems for their computers.
	Kursus ini akan memberi pengetahuan tentang cara-cara 'hacking' dan cara-cara pencegahannya supaya pelajar-pelajar akan dapat merangka penyelesaian terbaik untuk system rangkaian keselamatan merekea. Pelajar-pelajar juga akan mempelajari teknik yang digunakan untuk 'hacking' dan menilai, memilih dan merangka sistem keselamatan yang paling sesuai untuk sistem komputer.
12.Learning Outcomes	At the completion of the subject, students should be able to: • To impart knowledge on hacking techniques and prevention • Able to provide and design the best solutions for their

	computer and network systems. 1. Learn about the common practices and techniques used by computer hackers	
	Programmes Outcomes	**Degree of Contribution (%)**
	• Ability to apply soft skills in work and career related activities	5
	• Good understanding of fundamental concepts	15
	• Acquisition and mastery of knowledge in specialized area	30
	• Acquisition of analytical capabilities and problem solving skills	20
	• Adaptability and passion for learning	5
	• Cultivation of innovative mind and development of entrepreneurial skills	5
	• Understanding of the responsibility with moral and professional ethics	20
13. Details of subject	**Tajuk Pengajaran**	**Hours**
	1. Introduction to Ethical Hacking Essential Terminologies. The Security, Functionality, and Ease of Use Triangle • **What Does a Malicious Hacker Do?** • **Types of Hacker Attacks** • **Hacktivism** Hacker Classes and Ethical Hacking Can Hacking be Ethical? How to Become an Ethical Hacker? Skill Profile of an Ethical Hacker • **What is Vulnerability Research?** Why Hackers Need Vulnerability Research? Vulnerability Research Tools Vulnerability Research Websites • **Computer Crimes and Implications** Legal Perspective Computer Crime Act 1997	4
	2. Casing the Establishment • **Footprinting** Footprinting, Scope of Activities, Network Enumeration, DNS Interrogation, Network Reconnaisance	4

• **Scanning** Determining if system is alive, Determining which services are running and listening: Scan types, Identifying TCP and UDP Services Running, Windows based port scanners, port scanning breakdown Detecting Operating Systems: Active and Passive Stack Fingerprinting, Automated Discovery Tools • **Enumerations**	
3. Systems Vulnerabilities & Solutions • **Windows System** • Windows systems vulnerabilities Footprinting, Scanning, Enumerating, Penetration, DoS, Privilege Escalation, Pilfering, Covering Tracks, Back Doors, General Countermeasures • **Hacking UNIX** • UNIX systems vulnerabilities Quest for Root, Remote Access vs Local Access, Post Root Hacking • **Remote Connectivity and VOIP Hacking** • War dialing, brute-force scripting, PBX Hacking, VPN Hacking, VoIP Attacks	8
4. Network Vulnerabilities & Solutions • **Network Devices** • Discovery, AS Lookup, Services Detection, network vulnerabilities • **Wireless** • Footprinting, scanning and enumerations, SSID, Gaining Access, WEP weakness, DoS • **Firewall and Dos** • Firewall landscape, identification, scanning through firewall, packet filtering • Common DoS, DoS countermeasures: resisting, detecting and responding	6
5. Software Vulnerabilities & Solutions • **Code** • Common Exploit Techniques, Buffer overflow attacks, input validation attacks • Common Countermeasures: changing the culture, technology, SDL • **Web** • Web server hacking: sample file, source code disclosure, server extensions • Web Application hacking: finding	6

	vulnerable web application, web crawling, web application assessment • **Internet Users** • Malicious Mobile Code, SSL Fraud, Email Hacking, XSS, SQL Injection, Global Countermeasures to Internet User Hacking	
Laboratory	1. Casing the Establishment 2. Systems Security Assessment 3. Network Security Assessment 4. Software Security Assessment	
	Total Contact Hours (Equivalent to lecture hours)	**28**
14. Text	**Text Book**	1.McClure Stuart, Scambray, Joel, Kurtz, George, Hacking Exposed: Network Security Secrets and Solutions 5th Ed. McGraw Hill, 2005, New York
	Reference Books	1. Scambray, Joel, Mike Shema, Hacking Exposed: Web Applications. McGraw Hill, 2002, New York 2. Ed Skoudis, Tom Liston, Counter Hack Reloaded: A step-by-step Guide to Computer Attacks and effective defenses, Prentice Hall, 2006, USA