

King Fahd University of Petroleum & Minerals

Continuing Education Programs

Short Course

Proposed course title in English: Ethical Hacking

Proposed course title in Arabic: القرصنة الأخلاقية

Brief description in English		Brief description in Arabic	
This course aims at providing a comprehensive coverage of the various techniques used by hackers to penetrate computer and network systems. It is a highly technical course where the emphasis will be on inviting the participants to carry out all presented attacks themselves.		تهدف هذه المادة إلى توفير تغطية شاملة لمختلف التقنيات المستخدمة من قبل المتسللين لاختراق أنظمة الكمبيوتر والشبكات. هذه المادة هي تطبيقية بدرجة عالية حيث سيكون التركيز على دعوة المشاركين لتنفيذ جميع الهجمات المقدمة بأنفسهم.	
Date and Time – Gregorian		Date and Time – Hijri	
1 – 5 December, 2012		١٧-٢١ محرم ١٤٣٤ هـ	
Department		Language	
Information and Computer Science Department		English	
Course fee	Course duration	Course location	
5000 SAR	5 days	KFUPM / Building 23	

Who should attend?

This course is of particular interest to professionals in charge of ensuring network and system security in their companies. The course is also interesting for Software engineers, System administrators, Programmers, and anyone interested in the field of Security and Hacking.

Detailed course description:

Ethical hacking is an original approach to secure systems by trying to attack and hack them in order to find their weaknesses and vulnerabilities. In this course, students will learn how to scan computer systems and networks for vulnerabilities, how to exploit them to get access to the target's system/network, how to escalate privilege, how to bypass security measures like firewalls and antiviruses, how to crack passwords, how to sniff and modify traffic in the network, how to steal sessions, how to develop viruses and trojans, how to hack websites, etc.

This course focuses on two main aspects: (1) a deep understanding of the basics and principles of hacking techniques and (2) a practical hands-on experience of those hacking techniques. Every class/session will start by describing the background and principles of a security/hacking technique which will be followed by a set of live demos of the attacks.

Course outline/topics:

1. Initial Hacking steps
 - Scanning
 - Enumeration
 - Google Hacking
2. Hacking and infiltrating Operating Systems
 - Creating back-doors
 - Transferring and executing files in the victim
 - Opening sessions
3. Detecting Vulnerabilities
 - Vulnerability Scanners
 - Vulnerability databases
4. Using Exploitation tools
 - Writing exploits
 - Meta-Exploitation Tools
5. Password Cracking
 - Password cracking tools
 - Using dictionaries
6. Network Hacking
 - Network Sniffing to observe traffic
 - ARP Poisoning attacks
 - Man-In-The-Middle attacks
 - Session Hijacking
7. Web Application Hacking
 - Top 10 Web Application Attacks
 - SQL Injection Attacks
 - XSS Scripting Attacks
 - Etc.
8. Hacking with Malwares and Rootkits
 - Different Types of malwares
 - Malware coding
 - Malware binders and packers
 - Bypassing Antivirus Tools
 - Social Engineering Toolkits
9. Other Topics
 - Software Cracking
 - Anonymous Group Denial of Service Attacks
 - Etc.

Coordinator Information

Name	Contact Tel. Nos.: & Fax No.	E-mail Address
Dr. Sami Zhioua	Tel. 038601251, Fax. 038602174	zhioua@kfupm.edu.sa