King Fahd University of Petroleum & Minerals

Continuing Education Programs

Short Course

Proposed course title in English: Advanced Malware Analysis

Proposed course title in Arabic: تحليل البرمجيات الخبيثة

Brief description in English	Brief description in Arabic
Malwares (Trojans, Rootkits, etc.) are impressively evolving to become undoubtedly the threat of the future. Recent sophisticated malwares, in particular Flame which has been used in cyber-espionage activities in the Middle-East, are confirming this trend. This course aims to provide a comprehensive coverage of advanced malware analysis techniques to combat against sophisticated techniques used by hacker to defeat anti-viruses and security software. The course is on the cutting edge technology in the field of computer and network security.	البرمجيات الخبيثة آخذة في التطور لتصبح من أكبر الأخطار التي تهدد أمن أنظمة الكمبيوتر و الشبكات. من أبرز الأمثلة هو البرنامج الخبيث فلايم (Flame) الذي نك استعماله مؤخرا لمهاجمة البرنامج النووي الإيراني. يهدف هذا المقرر إلى دراسة فن تشريح البرمجيات الخبيثة و المتمثل في فهم كيفية عملها، كيفية التعرف عليها، وكيفية القضاء عليها.
Date and Time – Gregorian	**Date and Time – Hijri**
4 – 8 May, 2013	**٢٤ – ٣٠ جمادى الآخرة ١٤٣٤هـ**
Department	**Language**
Information and Computer Science Department	English

Course fee	Course duration	Course location
5000 SAR	5 days	Building 23

Who should attend?

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

Detailed course description:

This course is about a cutting-edge technology in information security which is Malware analysis. A Malware is software created by hackers to gather sensitive information or gain access to private computer systems. Malwares are becoming the number one threat of computer and network systems around the world. The recent Flame malware (May 2012) is an example of the destruction potential of Malwares. Experts openly suspect that Flame was jointly developed by government agencies for cyber-espionage in the Middle-East.

This course is about malware analysis which is the art of dissecting a malware to understand how it works, how to identify it, and how to defeat or eliminate it. With millions of malwares in the wild, and more encountered every day, malware analysis is critical for anyone who responds to computer security incidents. And, with a shortage of malware analysis professionals, the skilled malware analyst is in serious demand.

Course outline/topics:

1. Overview of Windows Internals:
    - Windows Kernel
    - Windows Registry
    - Windows DLLs
    - x86 disassembly
2. Malware Classification
    - Backdoors
    - Reverse Shells
    - RATs
    - Botnets
    - Rootkits
3. Malware Obfuscation techniques:
    - Malware Encoding
    - Malware Packing
    - Malware Encrypting
4. Malware Dissection
    - Debugging Malware
    - Attaching to Processes
    - Analyzing PDF Malwares
    - Analyzing Office Malwares
5. Malware Basic Analysis:
    - Malware Static Analysis
    - Malware Dynamic Analysis
6. Malware Forensics
    - Hunting Suspicious loaded DLLs
    - Identifying injected Code
    - Detecting API hooks
    - Detecting Driver hooks
    - Detecting attempts to hide TCP/IP activity
    - Detecting raw sockets
7. Defeating anti-reverse engineering techniques:
    - Defeating anti-debugging
    - Defeating anti-disassembly
    - Defeating anti-virtualization

Name and designation of instructors:

Name	Designation
Dr. Sami Zhioua	Assistant Professor, Information and Computer Science Department, KFUPM

Coordinator Information

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