بسم الله الرحمن الرحيم

CY 411 Reverse Software Engineering

Course Overview

Dr. Qasem Abu Al-Haija

Department of Cybersecurity
Faculty of Computer & Information Technology
Jordan University of Science and Technology

Basic information about the course

❑ Course Name and Code:

- ✓CY 411 Reverse Software Engineering – **CY 411**

❑ Instructor Information:

- ✓Name: Dr. Qasem Abu Al-Haija. Email: q.abualhaija@psut.edu.jo
- ✓Department: Department of Cybersecurity.

Prerequisites and Grading

Prerequisite Course:

- CY101 + CY111 + CY211

Prerequisite Skills:

- Basic cryptographic knowledge.
- Basic knowledge of X86 architecture and organization.
- Skills in assembly coding.
- Skills in code analysis and investigation.
- Computer skills to prepare written reports and presentations.

Grading Policy:

First Exam	To be decided	25%
Second Exam	To be decided	25%
Class Activities	To be decided	10%
Final Exam	To be decided	40%

Student Responsibilities

❑ Attendance Policy

- ✓ In accordance with the University Regulations, it is the student’s responsibility to be punctual and to attend all classes.

❑ Cheating and Plagiarism

- ✓ Plagiarism: Using the words, thoughts, ideas, results, etc., of another person in a written assignment, without acknowledging the source, as if it were the student's own work.

Course Regulations

❑ A Student is completely prohibited from doing any of the following:

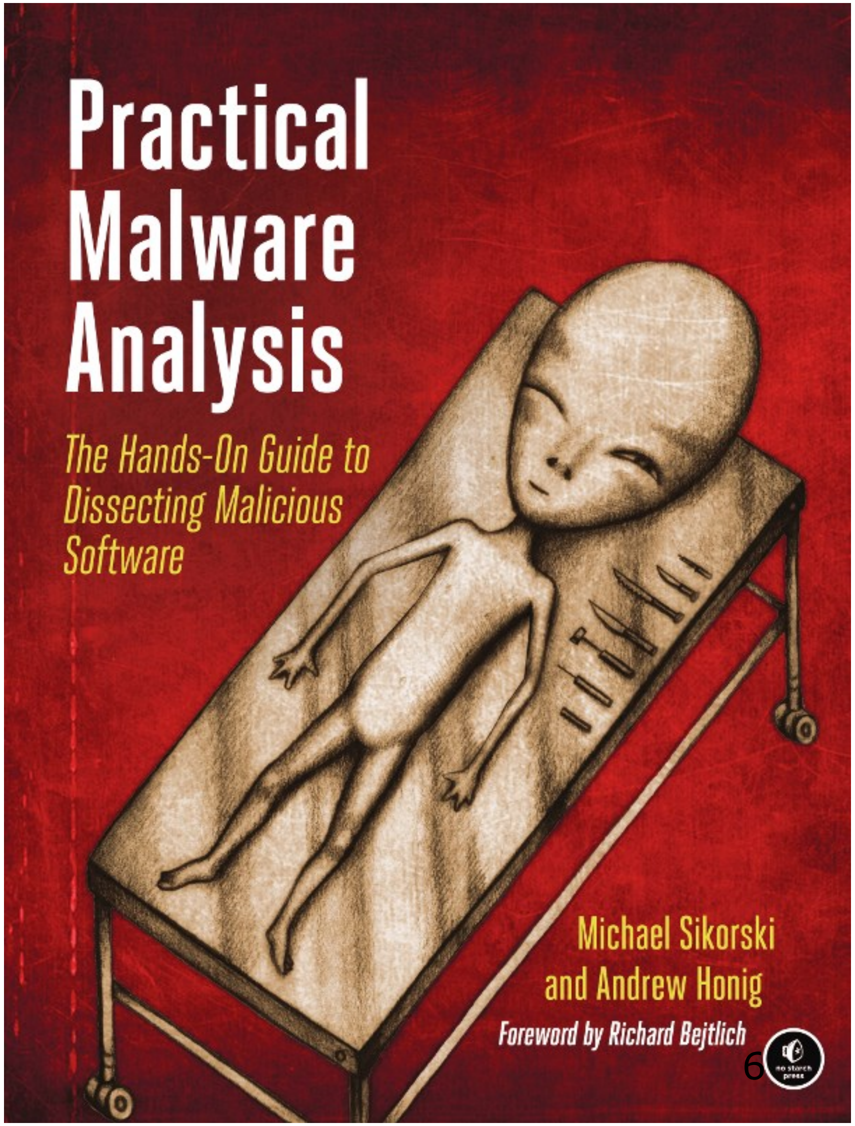
- ✓ Copying, attempting to copy, from another student's work (exams or others)
- ✓ Permitting another student to copy from your work.
- ✓ Using notes of whatever kind during closed book examinations.
- ✓ Disrupting the conduct of examinations by any illegal action.

❑ A Student is recommended of doing the following:

- ✓ Please use email whenever possible for your inquiries and appointments.
- ✓ Please read the assigned materials and lecture notes before each class.
- ✓ Class participation and interaction with instructor are very essential.
- ✓ You are responsible for downloading and printing lecture notes or other materials

Required textbook

- Michael Sikorski and Andrew Honig, *Practical Malware Analysis*, ISBN-13: 978-1-59327-290-6


Practical Malware Analysis
The Hands-On Guide to Dissecting Malicious Software
Michael Sikorski and Andrew Honig
Foreword by Richard Bejtlich
no starch press

Topics to be covered

- Review of Cryptographic Principles.
- Overview of Reverse Engineering.
- Malware Analysis Primer.
- Malware Analysis in Virtual Machines.
- Basic Static Malware Analysis.
- Basic Dynamic Malware Analysis.
- X86 Disassembly (32-bit Microprocessors).
- Advanced Static Malware Analysis.
- Advanced Adynamic Malware Analysis.
- Malware Behavior and Malware Encoding

Dr. Abu Al-Hajja, Q.

Malware over time

- 1988 – Morris Worm exploits use of gets() in finger daemon
- 1990 – Mark Washburn develops first polymorphic malware
- 2001 – Code Red worm exploits a MS web server vulnerability to hit hundreds of thousands of computers
- 2004 – Vundo trojan displays popups and advertising, distributed through spam email, peer-to-peer file sharing, drive-by downloads, and by other malware.
- 2005 – Sony infects CDs with a rootkit to prevent music piracy; the rootkit was is installed on a victim computer playing the CDs
- 2008 – Koobface RAT spreads via infected Facebook and Myspace profiles
- 2008-2010 – Stuxnet employs four Windows 0days to spread through Iranian nuclear refinery control system networks
- 2013 – Mandiant publishes evidence on APT1, a Chinese cyber espionage campaign dating as early as 2005
- 2015 – Duqu2 targets McAfee with advanced, modularized, in- memory only malware; Duqu2 is a variant of Duqu, and Duqu is a variant of Stuxnet.