Princess Sumaya University for Technology

King Hussein School for Information Technology

Department of Cybersecurity

ABET Course Syllabus – Summer Semester 2022/2023
15233 Malicious Software Analysis

1. Course Information

Catalog Description	This course will introduce students to modern malware analysis techniques through readings and hands-on interactive analysis of real-world samples. After taking this course, the students will be equipped with the skills to analyze advanced contemporary malware using static and dynamic analysis. Students will learn to analyze malicious software using reverse engineering concepts safely and thoroughly. This analysis aims to understand malicious software's behavior and potential security impacts.
Credit Hours	3
Prerequisite	11335
Course Type	Lecture
Required/Elective	Required
Textbook	Michael Sikorski and Andrew Honig, "Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software"; ISBN-10: 1593272901.
References	Abhijit Mohanta and Anoop Saldanha, "Malware Analysis and Detection Engineering: A Comprehensive Approach to Detect and Analyze Modern Malware," ISBN: 1484261925.
Instructor/email	Dr. Qasem Abu Al-Haija/ q.abualhaija@psut.edu.jo
Class Schedule	Section 1: (10:50 AM - 12:05 PM)

Class Location(s) (Blended Course)	Synchronous on campus = Section 1: Room (201)
	Synchronous-Zoom = https://psut-edu-jo.zoom.us/my/qabualhaija
	Asynchronous = TBA by the instructor.

Office Hours	Sun-Mon-Tue 09:15 – 10:45 or By Appointment.
Teaching Assistant	No

2. Course Contents

Weeks	Topics	Chapter in Textbook
1 - 2	**Review of Cryptographic Principles** *Cryptography, Cryptanalysis, Codes, Types, Hashing.* ***Review of 16-bit Assembly programming*** *Instruction set, directives, functions, Branches, assembler, 8086 Emulation* **8086Addressing Modes & Machine Codes** *Addressing modes, Assembling ASM Code to Binary (Machine), Disassembling Binary (Machine) to ASM code.*	**Supporting Materials**
3-4	**Malware Analysis Primer** *Malware analysis goals, Malware signatures, Malware analysis techniques, and Types of Malware.* **Malware Analysis in Virtual Machines** *Virtualization, Virtual Machines, Why Virtual Machines, Oracle VM VirtualBox, Installing and Configuring Windows Environment in VM.*	**Ch. 00** **Ch. 02**
5-6	**Basic Static Analysis** *Using antivirus tools to confirm maliciousness, Using hashes to identify malware, and Gleaning information from a file's strings, functions, and headers.* **Basic Dynamic Analysis** *Advantages/Disadvantages of Dynamic Analysis, Malware Sandbox, Running and Monitoring Malware (ProcMon, ProcExp), and others.*	**Ch. 01** **Ch. 03**
First Exam		
7-8	**A Crash Course in X86 Disassembly (32-bit Microprocessors)** *Computer Abstraction Levels, Reverse Engineering, Why Is x86 So Popular? X86 Architecture, X86 Memory, X86 Instructions, Opcodes, Endianness, registers, Flags, Pointers, Stack, Calling Conventions, Disable Windows Security Features.*	**Ch. 04**
9-11	**Advanced Static Analysis:** • Disassemble using IDA Pro. • Recognizing C Code Constructs in Assembly. • Analyzing Malicious Windows Programs	**Ch. 05** **Ch. 06** **Ch. 07**
Second Exam		
12-13	**Advanced Adynamic Analysis:** • Debugging. • Debugging using IDA Pro/OllyDbg.	**Ch. 08** **Ch. 09**

14 -15	**Malware Behavior** *Downloaders, Launchers, Backdoors, Credential Stealers, Persistence Mechanisms, and others.* **Malware Encoding** *Understanding Encoding/decoding, using ciphers, using Base64 encoding, decoding.*	**Ch. 11** **Ch. 13**
Final Exam		

3. Course Objectives

The main objectives of the course are to:

1. Describe types of malware, including rootkits, Trojans, and viruses.
2. Perform basic static analysis with antivirus scanning and strings
3. Perform basic dynamic analysis with a sandbox
4. Perform advanced static analysis with IDA Pro
5. Perform advanced dynamic analysis with a debugger
6. Explain malware behavior, including launching and encoding.
7. Recognizing the disassembly process and recognizing C Code Constructs in Assembly.

4. Assessment Policy

Assessment Tool	Expected Due Date	Weight
First Exam	Topics to be decided by the instructor	25%
Second Exam		25%
Course Activities	Topics to be decided by the instructor	10%
Final Exam	Topics to be decided by the instructor	40%

5. Contribution of the Course to the Professional Component

Computer Science Topics	100%
General Education	20%
Mathematics & Basic Sciences	50%

6. Expected level of proficiency from students entering the course

Mathematics	Some
Physics	No
Technical writing	Some
Computer programming	Some

7. Material available to students, instructors, TAs, and department at the end of the course

	Students	Department	Instructors	TA(s)
Course objectives and outcomes form	X	X	X	
Lecture notes, homework assignments, and solutions	X	X	X	
Samples of homework solutions from 3 students		X		
Samples of lab reports of 3 students		X		
Samples of exam solutions from 3 students		X		
Course performance forms from student surveys		X	X	
End-of-course instructor survey		X	X	