Course Specifications

Course Title:	**Reverse Engineering & Malware Analysis**
Course Code:	**CSEC 425**
Program:	**Information and Computer Sciences**
Department:	**Computer Science and Information**
College:	**College of Science at Az Zulfi**
Institution:	**Al- Majmaah University**

Table of Contents

A. Course Identification

1. **Credit hours:** **3 cr (2 Lec + 2 Lab)**

2. Course type

a. University □ College □ Department □ Others □

b. Required ■ Elective □

3. **Level/year at which this course is offered:**

4. **Pre-requisites for this course** (if any)**:**

Cybersecurity Principles – CSEC 313

5. **Co-requisites for this course** (if any)**:**

NIL

6. Mode of Instruction (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	**Traditional classroom**	✓	80 %
2	**Blended**	✓	5 %
3	**E-learning**	✓	5 %
4	**Correspondence**	✓	5 %
5	**Other**	✓	5 %

7. Actual Learning Hours (based on academic semester)

No	Activity	Learning Hours
Contact Hours		
1	**Lecture**	30
2	**Laboratory/Studio**	30
3	**Tutorial**	--
4	**Others** (specify)	--
	Total	60
Other Learning Hours*		
1	**Study**	45
2	**Assignments**	10
3	**Library**	05
4	**Projects/Research Essays/Theses**	15
5	**Others** (specify)	--
	Total	(60+75 = 135)

* The length of time that a learner takes to complete learning activities that lead to achievement of course learning outcomes, such as study time, homework assignments, projects, preparing presentations, library times

B. Course Objectives and Learning Outcomes

1. Course Description

This course provides students a foundational knowledge about reverse engineering and malware analysis, through the study of various cases and hand-on analysis of malware samples. It covers fundamental concepts in malware investigations so as to equip the students with enough background knowledge in handling malicious software attacks. Various malware incidents will be covered, such as cases in Ransomware, banking-trojan, state-sponsored and APT attacks, cases in Stuxnet and malicious software attacks on Industrial Control System and IoT devices. With the experience of studying these cases and analyzing selected samples, the students will be able to understand the global cyber security landscape and its future impact. Hands-on exercises and in-depth discussion will be provided to enable students to acquire the required knowledge and skill set for defending and protecting an enterprise network environment.

2. Course Main Objective

1. To be able to identify and reverse engineer malicious code and investigate activity stemming from malicious software infections, in order to forensically analyse and detect artefacts which remain on infected systems

2. To study the different methods for the identification, investigation and analysis of malicious code.

3 Identify key characteristics of malware and ways to mitigate the threat of malware.

4 To enable the student's knowledge, understanding, and reasoning by introducing them to alternative and developing environments (including, mobile devices). 5 To understand Reverse engineering of malware code (Static Analysis)

3. Course Learning Outcomes

	CLOs	Aligned PLOs
1	**Knowledge:**	
1.1	Understand knowledge of information security issues in relation to the design, development and use of information systems.	K3-CS
2	**Skills :**	
2.1	Analyze and implement user needs and consider them during the selection, integration, and administration of computer-based systems.	S2
2.2	Evaluate and analyze of computer networks, security policies, security controls and threats using a range of techniques.	S3- CS
3	**Competence:**	
3.1	Forensically analyze security problems from every angle to **solve** the scope of these problems for devising the most secure solutions.	C3-CS

C. Course Content

No	List of Topics	Contact Hours
1	**BASIC ANALYSIS**: Basic Static Techniques, Malware Analysis in Virtual, Machines, Basic Dynamic Analysis	12
2	**ADVANCED STATIC ANALYSIS:** A Crash Course in x86 Disassembly, IDA Pro, Recognizing C Code Constructs in Assembly Analyzing Malicious Windows Programs	12
3	**ADVANCED DYNAMIC ANALYSIS:** Debugging, vi Brief Contents, Olly Dbg, Kernel Debugging with WinDbg	12
4	**MALWARE FUNCTIONALITY:** Malware Behavior, Covert Malware Launching, Data Encoding, Malware-Focused Network Signatures	12
5	**ANTI-REVERSE-ENGINEERING:** Anti-Disassembly, Anti-Debugging, Anti-Virtual Machine Techniques, Packers and Unpacking	12
Total		60

D. Teaching and Assessment

1. Alignment of Course Learning Outcomes with Teaching Strategies and Assessment Methods

Code	Course Learning Outcomes	Teaching Strategies	Assessment Methods
1.0	**Knowledge**		
1.1	Understand knowledge of information security issues in relation to the design, development and use of information systems	Lectures Lab demonstrations Case studies Individual presentations	Written Exam Homework assignments Class & lab Activities Quizzes
2.0	**Skills**		
2.1	Analyze and implement user needs and consider them during the selection, integration, and administration of computer-based systems.	Group discussions, Brainstorming Presentations	HomeWorks and assignments
2.2	Evaluate and analyze of computer networks, security policies, security controls and threats using a range of techniques.		
3.0	**Competence**		

Code	Course Learning Outcomes	Teaching Strategies	Assessment Methods
3.1	Forensically analyze security problems from every angle to **solve** the scope of these problems for devising the most secure solutions..	Group discussions Case Studies Brainstorming Presentations	Lab Activities, Project report evaluation

2. Assessment Tasks for Students

#	Assessment task*	Week Due	Percentage of Total Assessment Score
1	First written mid-term exam	6	20%
2	Second written mid-term exam	12	20%
3	Class activities, group discussions, Seminars, Project Presentations.	Every week	10%
4	Homework + Assignments	After every chapter	10%
5	Final written exam	16	40%

***Assessment task** (i.e., written test, oral test, oral presentation, group project, essay, etc.)

E. Student Academic Counseling and Support

Arrangements for availability of faculty and teaching staff for individual student consultations and academic advice :
Office hours:
Email: @mu.edu.sa

F. Learning Resources and Facilities

1.Learning Resources

Required Textbooks	**Michael Sikorski and Andrew Honig, Practical Malware Analysis : The Hands-On Guide to Dissecting Malicious Software, No Starch Press, 1st edition, ISBN-13: 978-1593272906**
Essential References Materials	. Jon Erickson ,Hacking: The Art of Exploitation, No Starch Press; 2nd edition, ISBN-13 : 978-1593271442
Electronic Materials	1.https://www.sans.org/cyber-security-courses/reverse-engineering-malware-malware-analysis-tools-techniques/
Other Learning Materials	**Course material includes handouts, ppt, questionnaires as distributed among the students**

2. Facilities Required

Item	Resources
Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.)	1. Classrooms with required digital aids and to support traditional method of teaching using blackboard. 2. Classrooms with proper lighting and air conditioning system integrated with the sound System /audio system.

Item	Resources
	3. Classroom with smart board interface, display screen and a computer to aid the sessions
Technology Resources (AV, data show, Smart Board, software, etc.)	Smart Board with supporting software / computers with updated versions of software as required to understand the subject concepts with quality headphones.
Other Resources (Specify, e.g. if specific laboratory equipment is required, list requirements or attach a list)	NIL

G. Course Quality Evaluation

Evaluation Areas/Issues	Evaluators	Evaluation Methods
Effectiveness of Teaching	Students Classroom Observation Committee Professional Development Unit External Reviewers – accreditation committee	Formal Classroom Observation - Direct Student Surveys - Indirect
Effectiveness of Assessment	Curriculum and Test Development Unit Curriculum Committee Assessment Committee External Reviewers	Faculty Feedback - indirect Student Feedback – indirect Course Reports
Extent of Achievement of Course Learning Outcomes	Quality Assurance Unit Curriculum and Test Development Unit	Course Reports Annual Program Review

Evaluation areas (e.g., Effectiveness of teaching and assessment, Extent of achievement of course learning outcomes, Quality of learning resources, etc.)

Evaluators (Students, Faculty, Program Leaders, Peer Reviewer, Others (specify)

Assessment Methods (Direct, Indirect)

H. Specification Approval Data

Council / Committee	
Reference No.	
Date	