



# Course Specification

## (Bachelor)

Course Title: **Malware and Risk Analysis**

Course Code: **APIS3211**

Program: **Diploma in Information Security**

Department: **Diplomas**

College: **Applied College**

Institution: **Umm Al-Qura University**

Version: **1**

Last Revision Date: **14/12/2024**



## Table of Contents

A. General information about the course: .....	3
B. Course Learning Outcomes (CLOs), Teaching Strategies and Assessment Methods .....	4
C. Course Content.....	5
D. Students Assessment Activities .....	6
E. Learning Resources and Facilities.....	6
F. Assessment of Course Quality .....	7
G. Specification Approval .....	8





## A. General information about the course:

### 1. Course Identification

1. Credit hours: ( 3 )

#### 2. Course type

- A. ☐ University ☐ College ☒ Department ☐ Track ☐ Others
- B. ☒ Required ☐ Elective

3. Level/year at which this course is offered: ( level 2, 1<sup>st</sup> year)

#### 4. Course general Description:

This course exposes the student to various techniques and procedures employed in the practice of software analysis to detect and remove affected code. The areas explored will consist of trends in malicious code growth, common attack vectors, surface analysis of malware, run-time analysis of malware, system monitoring, debuggers, static reverse engineering of malware, and disassemblers to identify obfuscation techniques and Anti-reversing methods.

This course includes also the knowledge and skills of the models, methodologies and processes for assessing, managing and dealing with cyber risks.

5. Pre-requirements for this course (if any):

6. Pre-requirements for this course (if any):

#### 7. Course Main Objective(s):

1. Applying malware analysis methodology and technology
2. Identify known anti-reverse engineering techniques and some advanced malware functionality.
3. Discuss professional problems, analysis and conclusions in the field of malware analysis, both with professionals and with general audience.
4. To enable the student's knowledge, understanding, and reasoning by introducing them to alternative and developing environments (including, mobile devices).
- 5- To express knowledge of risk assessment models, methodologies and processes such that they can perform a risk assessment of a particular systems and recommend mitigations to identified risks.

### 2. Teaching mode (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	Traditional classroom	60	100%
2	E-learning		
3	Hybrid <ul style="list-style-type: none"> <li>• Traditional classroom</li> </ul>		





No	Mode of Instruction	Contact Hours	Percentage
	• E-learning		
4	Distance learning		

### 3. Contact Hours (based on the academic semester)

No	Activity	Contact Hours
1.	Lectures	30
2.	Laboratory/Studio	30
3.	Field	
4.	Tutorial	
5.	Others (specify)	
Total		60

## B. Course Learning Outcomes (CLOs), Teaching Strategies and Assessment Methods

Code	Course Learning Outcomes	Code of CLOs aligned with program	Teaching Strategies	Assessment Methods
1.0	Knowledge and understanding			
1.1	Be able to carry out independent analysis of modern malware samples using behavioral, code analysis and memory forensic techniques.	K1	Course lectures, lab exercises, project	Quizzes, Midterm Exam, Final Exam
1.2	Be able to apply the learned techniques to protect, reduce the security risks and avoid malicious software attacks on computer systems or networks.	K1	Course lectures, lab exercises, project	Quizzes, Midterm Exam, Final Exam
1.3	Be able to research independently and use learned skills and tools to investigate malicious software attacks and	K1	Course lectures, lab exercises, project	Quizzes, Midterm Exam, Final Exam





Code	Course Learning Outcomes	Code of CLOs aligned with program	Teaching Strategies	Assessment Methods
	implement or update a cyber protection plan.			
<b>2.0</b>	<b>Demonstrate the main risk management methodologies.</b>			
2.1	Define and functionally use low-level computer architecture terms, and employ malware analysis tools to analyze unknown artifacts.	S1	Lab coursework Project	Quizzes, Midterm Exam, Final Exam, project
2.2	Perform dynamic and static malware analysis to determine malware characteristics, and present findings in clear, concise reports.	S1, S5	Lab coursework Project	Quizzes, Midterm Exam, Final Exam, project
2.3	Develop automated analysis solutions and collaborate effectively to analyze large code bases.	S2	Lab coursework Project	Quizzes, Midterm Exam, Final Exam, project
<b>3.0</b>	<b>Values, autonomy, and responsibility</b>			
3.1	Work cooperatively and lead the teamwork to perform a range of tasks with moderate responsibility; and work towards achieving common goals effectively.	V4	Project	Project

### C. Course Content

No	List of Topics	Contact Hours
1.	Malware analysis fundamental	2
2.	BASIC ANALYSIS: Basic Static Techniques, Malware Analysis in Virtual, Machines, Basic Dynamic Analysis	4
3.	Reversing malicious code using static and dynamic techniques	4
4.	Analyzing malicious documents	2
5.	MALWARE FUNCTIONALITY: Malware Behaviour, Covert Malware Launching, Data Encoding, Malware Focused Network Signatures	4



6.	ANTI-REVERSE-ENGINEERING: Anti-Disassembly, Anti-Debugging, Anti-Virtual Machine Techniques, Packers and Unpacking	2
7.	Incident response	2
8.	Principles and Concepts of Cybersecurity Risk Analysis and Management Risk Management Lifecycle and Steps Cyber Risk Assessment and Analysis Methodologies Methodologies for Measuring and Evaluating Cyber Risks Cyber Risk Management Standards and Frameworks Cyber Risk Management Processes Across Levels in the Organization Cyber Risks Mitigation Economics Transference, Acceptance and Mitigation of Cyber Risks Cyber Risks Policies for Technologies, Individuals and Entities Characteristics of Organizations that Influence Cyber Risk Analysis and Management Communication of Cyber Risks	4
Total		30

#### D. Students Assessment Activities

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1.	Quizzes	1 - 15	10%
2.	Labs	1 - 15	15%
3.	Project	1 - 15	20%
4.	Midterm	1 - 15	20%
5.	Final Exam	Finals Week	35%

\*Assessment Activities (i.e., Written test, oral test, oral presentation, group project, essay, etc.).

#### E. Learning Resources and Facilities

##### 1. References and Learning Resources





Essential References	<p><b>Cybersecurity Risk Management: Mastering the Fundamentals Using the NIST Cybersecurity Framework”</b> Cynthia Brumfield, Brian Haugli, ISBN: 978-1-119-81628-7, March 2022</p> <ul style="list-style-type: none"> <li>Michael Sikorski and Andrew Honig, Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, No Starch Press, 1 st edition, ISBN-13: 978-1593272906</li> </ul>
Supportive References	<ul style="list-style-type: none"> <li>The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory by Michael Hale Ligh, Andrew Case, Jamie Levy, Aaron Walters, 1st Edition, 2014.</li> </ul>
Electronic Materials	<a href="https://www.sans.org/cyber-security-courses/reverse-engineering-malware-malware-analysis-tools-techniques/">https://www.sans.org/cyber-security-courses/reverse-engineering-malware-malware-analysis-tools-techniques/</a>
Other Learning Materials	N/A

## 2. Required Facilities and equipment

Items	Resources
<p><b>facilities</b> (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)</p>	<p>Lecture room with:</p> <ul style="list-style-type: none"> <li>* at least 30 seats</li> <li>* A data show projector connected to a PC preferably with Internet connection</li> <li>* sliding board</li> <li>* PC Lab (at least 30 seats)</li> </ul>
<p><b>Technology equipment</b> (projector, smart board, software)</p>	<p>30 Linux/Windows PCs</p>
<p><b>Other equipment</b> (depending on the nature of the specialty)</p>	<p>A maintenance lab + A PC lab with various operating systems such as Linux windows etc.</p>

## F. Assessment of Course Quality

Assessment Areas/Issues	Assessor	Assessment Methods
Effectiveness of teaching	Students	Indirect
Effectiveness of Students' assessment	Peers	Direct





Assessment Areas/Issues	Assessor	Assessment Methods
Quality of learning resources	Quality Assurance Committee/ Curriculum Committee	Direct
The extent to which CLOs have been achieved	Instructor	Direct
Other		

**Assessors** (Students, Faculty, Program Leaders, Peer Reviewer, Others (specify))

**Assessment Methods** (Direct, Indirect)

### G. Specification Approval

<b>COUNCIL /COMMITTEE</b>	Umm Al-Qura University Council
<b>REFERENCE NO.</b>	851141114462/190358
<b>DATE</b>	1446/11/22

