Course Specification

(Postgraduate)

Course Title:	**Malware Analysis and Engineering**
Course Code:	CYBS60308
Program:	M.Sc. in Cybersecurity
Department:	**Department of Computer Science**
College:	**Faculty of Computing and Information**
Institution:	Al-baha University
Version:	**2**
Last Revision Date:	**12 December 2023**

Table of Contents

A. General information about the course:

1. Course Identification:

1. Credit hours: (3)				
2. Course type				
A.	☐University	☐College	☐Department	☐Track
B.	☐ Required		☒ Elective	
3. Level/year at which this course is offered: (5/2)				
4. Course general Description:				
Introduction to the theory and practice of software reverse engineering applied to the analysis of malicious software (malware). Students will learn techniques of static and dynamic analysis to help identify the full spectrum of the behavior of code that is presented without documentation or source code and to identify possible remediation and avoidance techniques. The course will use a large number of software tools employed by malware and computer forensic analysts. Techniques to create malwares are also being discussed in this course.				
5. Pre-requirements for this course (if any)**:**				
Advanced Programming in Cybersecurity (CYBS60201)				
6. Co-requirements for this course (if any)**:**				
7. Course Main Objective(s):				
Upon successful completion of the course, the student will be able: 1. **Describe how to safely and thoroughly analyze malicious software.** 2. **Explain the behavior and potential security impacts of such malicious code. Students will learn a variety of static and dynamic analysis techniques that help them understand a program's structure and behavior.** 3. **Infer theoretical and practical knowledge with a large number of software tools will be employed during the class and students will become familiar with them through hands-on application during analysis of actual malware samples.** 4. **Preparing students to be able to analyze new malware artifacts, the course will provide a very good background for understanding, analyzing, and developing low-level code.** 5. **Students are able to apply techniques to create malware**				

2. Teaching Mode: (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	Traditional classroom	26	80%
2	E-learning	7	20%
3	Hybrid ☐ Traditional classroom ☐ E-learning		
4	Distance learning		

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

No	Activity	Contact Hours
1.	**Lectures**	33
2.	**Laboratory/Studio**	-
3.	**Field**	-
4.	**Tutorial**	-
5.	**Others (specify).....**	-
	Total	33

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

Code	Course Learning Outcomes	Code of PLOs aligned with program	Teaching Strategies	Assessment Methods
1.0	**Knowledge and understanding**			
1.1	Describe and possess knowledge of methodology, technology and application of malware analysis and reverse engineering	K.1	Lectures Assignments Group Discussion	☐ Homework ☐ Midterm exams ☐ Final Exam
1.2	Examine the malware through advanced static and dynamic techniques	K.1	Lectures Assignments Group Discussion	☐ Homework ☐ Midterm exams ☐ Final Exam
...				
2.0	**Skills**			
2.1	Demonstrate the capability of applying malware analysis	S.1	Lectures	☐ Quiz ☐ Midterm exam

Code	Course Learning Outcomes	Code of PLOs aligned with program	Teaching Strategies	Assessment Methods
	methodology and technology		Assignments Case study	☐ Final Exam
2.2	Experiment and gain an understanding of various malware analysis techniques, procedures and tools	S.2	Lectures Assignments Case study	☐ Quiz ☐ Midterm exam ☐ Final Exam
...				
3.0	**Values, autonomy, and responsibility**			
3.1	Work both independently and collaboratively	V1	Project	Project evaluation form (rubric)

C. Course Content:

No	List of Topics	Contact Hours
1	Introduction to malware analysis, reverse engineering, and Testing Methodologies	3
2	Malware Analysis Techniques: Static and Dynamic Analysis	6
3	Common Analysis Tools and Methods: Initial Infection Vectors and Malware Discovery tools	6
4	Sandboxing Malware and Gathering Information from Runtime Analysis	6
5	Source & Binary Code Analysis: Introduction to the IDA pro Disassembly	3
6	Malware Defensive/Obfuscate Techniques	6
7	Anti-Reverse Engineering Techniques	3
Total		**33**

D. Students Assessment Activities:

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1	Homework	Week 4 – Week 8	10%
3	Midterm exam	Week 6	20%
4	Quiz	Week 8	10%
5	Project	Week 11	10%
6	Final Exam	Week 12-13	50%

*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	Michael Sikorski, Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, No Starch Press, 2012, ISBN-10: 1593272901 M. Ligh, S Adair, B Hartstein and M.Richard, Malware Analysts Cookbook and DVD: Tools and Techniques for Fighting Malicious Code, John Wiley & Sons, 2010, ISBN-10: 9780470613030
Supportive References	- Computer Forensic Training Center Online http://www.cftco.com/ - Computer Forensics World http://www.computerforensicsworld.com/ Computer Forensic Services http://www.computer-forensic.com/ - Digital Forensic Magazine http://www.digitalforensicsmagazine.com/ - The Journal of Digital Forensics, Security and Law http://www.jdfsl.org/ - Journal of Digital Forensic Practice http://www.tandf.co.uk/15567281 - DOJ Computer Crime and Intellectual Property Section - http://www.usdoj.gov/criminal/cybercrime/searching.html - Electronic Crime Scene Investigation: A Guide for First Responders - http://www.ojp.usdoj.gov/nij/pubs-sum/187736.htm and related publications at http://nij.ncjrs.org/publications/pubs_db.asp - CERIAS Forensics Research (http://www.cerias.purdue.edu/research/forensics/) - Scientific Working Group on Digital Evidence (http://ncfs.org/swgde/index.html) - DoD Cybercrime Center (http://www.dc3.mil) - National Criminal Justice Reference Service - http://www.ncjrs.gov/app/publications/alphalist.aspx - Digital Forensics Research Workshop (http://www.dfrws.org/) - National White Collar Crime Center (http://www.nw3c.org/) Website relating to DOS commands, batch files, autoexec.bat/config.sys, and boot disks http://www.computerhope.com/
Electronic Materials	- Access to the Saudi Digital Library (SDL). - Using the learning management system of the university – Rafid System (https://lms.bu.edu.sa/). - https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=90

	- ACM Transactions on Computing Education (TOCE) – http://toce.acm.org/ - ACM (Association for Computer Machinery) Curricula Recommendations http://www.acm.org/education/curricula-recommendations
Other Learning Materials	

2. Educational and Research Facilities and Equipment Required:

Items	Resources
facilities (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)	• A classroom or lecture hall with whiteboard for 25 students. A laboratory with 25 computers.
Technology equipment (Projector, smart board, software)	All students shall have • A laptop or access to a desktop computer with access to a programming development tool • High speed Internet connection • Power outlets for student's laptop plug-in Relevant programming software for use of students.
Other equipment (Depending on the nature of the specialty)	• The laboratory should have computers with programming development tools.

F. Assessment of Course Quality:

Assessment Areas/Issues	Assessor	Assessment Methods
Effectiveness of teaching	Students - Program Leaders	Indirect
Effectiveness of students assessment	Program Leaders	Indirect
Quality of learning resources	**Students**	**Indirect**
The extent to which CLOs have been achieved	Peer reviewers	Direct
Reviewing course effectiveness and planning for improvement.	Program Leaders - Faculty	Direct

Assessor (Students, Faculty, Program Leaders, Peer Reviewer, Others (specify)
Assessment Methods (Direct, Indirect)

G. Specification Approval Data:

COUNCIL /COMMITTEE	
REFERENCE NO.	
DATE	