هيئة تقويم التعليم والتدريب
Education & Training Evaluation Commission

T-104
2022

Course Specification

Course Title:	**Operating System Security**
Course Code:	CYBS60202
Program:	M.Sc. in Cybersecurity
Department:	**Computer Science**
College:	Faculty of Computing and Information
Institution:	Albaha University
Version:	*Course Specification Version Number*
Last Revision Date:	*Pick Revision Date.*

Table of Contents:

A. General information about the course:

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: 2nd / 1st					
4. Course general Description This course covers both the fundamentals and advanced topics in operating system (OS) security. Access control mechanisms (e.g., SACL/DACL), memory protections, and inter-process communications mechanisms will be studied. Students will learn the current state-of-the-art OS-level mechanisms and policies designed to help protect systems against sophisticated attacks. In addition, advanced persistent threats, including rootkits and malware, as well as various protection mechanisms designed to thwart these types of malicious activities, will be studied. Advanced kernel debugging techniques will be applied to understand the underlying protection mechanisms and analyze the malicious software. Students will learn both hardware and software mechanisms designed to protect the OS (e.g., NX/ASLR/SMEP/SMAP). The course will use virtual machines to study traditional OS environments on modern 64-bit systems (e.g., Windows, Linux,), as well as modern mobile operating systems (Android).					
5. Pre-requirements for this course (if any): None					
6. Co- requirements for this course (if any): None					
7. Course Main Objective(s) Upon successful completion of the course, the student will be able: - to develop fundamental understanding and competency of Operating systems concepts and structure (Operating Systems: Windows, Linux and Android) - to understand the thread and attacks models in Operating System level as well as hardware security - to master techniques for achieving O/S security.					

1. 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		-

2. 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 CLOs aligned with program	Teaching Strategies	Assessment Methods
1.0	Knowledge and understanding			
1.1	Develop fundamental understanding and competency of Operating Systems concepts and structure (Operating Systems: Windows, Linux and Android)	**K1**	• Lectures • Assignments	• Homework • Midterm exams • Final Exam
1.2	Explain the thread and attacks models in Operating System level as well as hardware security	**K2**	• Lectures • Assignments	• Homework • Midterm exams • Final Exam
1.3	Demonstrate hardening steps for a given OS according to given applications.	**K3**	• Lectures • Assignments	• Homework • Midterm exams • Final Exam
2.0	Skills			
2.1	Perform secure OS installation and disable unneeded components, services, and ports.	**S1**	• Lectures • Assignments	• Homework • Midterm exams • Final Exam
2.2	Perform OS patching and updating periodically.	**S2**	• Lectures • Assignments	• Homework • Midterm exams • Final Exam
3.0	Values, autonomy, and responsibility			
3.1	Communicate effectively through oral presentations, computer presentations and written reports.	**V1**	• Small groups • Oral presentation	Course project presentation and report
3.2	Develop ability to work as a team.	**V2**	• Small groups Oral presentation	Course project presentation and report

C. Course Content

No	List of Topics	Contact Hours
1.	Introduction to OS Security & Overview of O/S (Windows, Linux, and Android)	3
2.	Secure Installation, Removing Unnecessary Components	3
3.	File system Maintenance: Isolation of Sensitive Data	3
4.	Authentication/Authorization Mechanisms, Interposes Communication, Privilege Separation.	3
5.	User Restrictions: Access and Authorizations	3
6.	User, Group and File Management	3
7.	Password Standards and Requirements	3
8.	Patch Management and Software Updates	3
9.	Operating System Security Internals, User Mode Security, Kernel Mode Security, Kernel Debugging	3
10.	Hardware Mechanisms, Virtualization	3
11.	Vulnerability Scanning	3
Total		33

D. Students Assessment Activities

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1.	Midterm exam	6	20%
2.	Quiz	9	20%
3.	Project	11	10%
4	Final exam	12	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	Trent Jaeger, Operating System Security Synthesis Lectures on Information Security, Privacy, and Trust, Morgan & Claypool publisher, 2008
Supportive References	Michael Palmer, Guide to Operating Systems Security, 3rd ed. ISBN-13: 978-0619160401, ISBN-10: 0619160403
Electronic Materials	- ACM (Association for Computer Machinery) web site - http://www.acm.org/ - IEEE Computer Society web site - http://www.computer.org/portal/web/guest/home - Access to the Saudi Digital Library (SDL). - Using the learning management system of the university – Rafid System (https://lms.bu.edu.sa/).
Other Learning Materials	-

2. Required Facilities and equipment

Items	Resources
facilities (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)	□ A classroom or lecture hall with whiteboard. □ A instructor computer station with ○ High speed Internet connection; ○ A desktop computer; ○ Appropriate software access; ○ Power outlets for instructor's laptop plug-in; ○ A DVD/Blu Ray player; ○ A digital image projection system with connection and switches to desktop computer, laptop computer and DVD/Blu Ray player. ○ Audio-visual recording capability so students can review lectures offline.
Technology equipment (projector, smart board, software)	□ High speed Internet connection □ A digital image projection system that ○ Is connected to instructor desktop computer ○ Has connection for laptop plug-in
Other equipment (depending on the nature of the specialty)	-

F. Assessment of Course Quality

Assessment Areas/Issues	Assessor	Assessment Methods
Effectiveness of teaching	Faculty, Program Leaders	Direct
Effectiveness of students assessment	Students, Program Leaders, Peer Reviewer	Direct
Quality of learning resources	Students, Program Leaders, Peer Reviewer	Direct
The extent to which CLOs have been achieved	Faculty, Program Leaders, Peer Reviewer	Indirect
Other		

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

G. Specification Approval Data

COUNCIL /COMMITTEE	
REFERENCE NO.	
DATE	