Course Specifications

Course Title:	Vulnerability Analysis and Testing
Course Code:	CSEC 422
Program:	Information and Computer Sciences
Department:	Computer Science and Information
College:	College of Science AzZulfi
Institution:	Majmaah University

T4

December 2018

Table of Contents

A. Course Identification

1. Credit hours:3				
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)**:** Cyber Security Essentials – CSEC 323 **Software Security**				
5. Co-requisites for this course (if any)**:** **None**				

6. Mode of Instruction (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	Traditional classroom	48	80%
2	Blended	6	10%
3	E-learning	0	0%
4	Correspondence	0	0%
5	Other	6	10%

7. Actual Learning Hours (based on academic semester)

No	Activity	Learning Hours
Contact Hours		
1	**Lecture**	30
2	**Laboratory/Studio**	15
3	**Tutorial**	15
4	**Others** (specify)	-
	Total	60
Other Learning Hours*		
1	**Study**	30
2	**Assignments**	30
3	**Library**	15
4	**Projects/Research Essays/Theses**	15
5	**Others** (specify)	10
	Total	100

* 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 the set of techniques for the penetration testing that are using to penetrate in a network as an ethical hacker. The starts with the ways the vulnerability analysis can be performed. It starts with finding live hosts and open ports to break into by exploiting the vulnerability and then to clear the break in tracks. It provides techniques and tool to ensure the security of computer network and applications. The student performs hands on in the virtual environment using Windows and Linux guest operating system.

2. Course Main Objective

The main objective of this course:

study concept of techniques for the penetration testing & the vulnerability analysis , also exploiting the vulnerability also student learn about techniques and tools to security of computer network and applications. using virtual environment by Windows and Linux guest operating system.

3. Course Learning Outcomes

CLOs		Aligned PLOs
1	**Knowledge:**	
1.1	Analyze trends of cyber-attacks, evolving security threats, the mechanisms for monitoring and detecting them, protection controls for mitigating their risks and approaches for holistic cyber defence	K3-CSEC
1.2	Explain the techniques and tools to ensure the security of a computer networks and applications.	
1.3	Apply best practices for security management within an enterprise abiding by legal obligations, regulatory requirements, international standards, ethical considerations, good governance, incident response and business continuity plans	
1...		
2	**Skills :**	
2.1	Analyze issues for creating security policy for a large organization.	S3-CSEC
2.2	Defend the need for protection and security, and the role of ethical considerations in computer networks use.	
2.3	Apply skills in research, independent study, career planning, self-management, including time management and prioritisation of tasks when tackling complex problems.	
2...	Analyze different kind of threats	
3	**Competence:**	
3.1	Function effectively on teams to accomplish a common goal	C3-CSEC
3.2	Keep your computer safe from different threats.	
3.3		
3...		

C. Course Content

No	List of Topics	Contact Hours
1	**review** Principles of cyber**security**	8
2	concept of techniques for the penetration testing	8

3	Explain the concept of ethical hackers.	8
4	the vulnerability analysis	8
5	exploiting the vulnerability	8
6	Describe the techniques and tools to security of computer network and applications.	8
8	the virtual environment using Windows and Linux guest operating system.	12
		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	Analyze trends of cyber-attacks, evolving security threats, the mechanisms for monitoring and detecting them, protection controls for mitigating their risks and approaches for holistic cyber defence	Lectures Lab demonstrations Case studies Individual presentations	Written Exam Homework assignments Class & Lab Activities Quizzes
1.2	Explain the techniques and tools to ensure the security of a computer networks and applications.		
…	Apply best practices for security management within an enterprise abiding by legal obligations, regulatory requirements, international standards, ethical considerations, good governance, incident response and business continuity plans		
2.0	**Skills**		
2.1	Analyze issues for creating security policy for a large organization.	Lectures Lab demonstrations Case studies Individual presentations Brainstorming	Written Exam assignments Lab Activities Quizzes
2.2	Defend the need for protection and security, and the role of ethical considerations in computer networks use.		
2.3	Apply skills in research, independent study, career planning, self-management, including time management and prioritisation of tasks when tackling complex problems.		
2.4	Analyze different kind of threats		
3.0	**Competence**		
3.1	Function effectively on teams to accomplish a common goal	Small group discussion Whole group discussion Brainstorming Presentation	Written Exam Homework assignments Lab assignments Class Activities Quizzes
3.2	Keep your computer safe from different threats.		
…			

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, Presentation	Every 2 weeks	5%
4	Homework + Assignments	After Every chapter	5%
5	Electronic exam	14	5%
6	Lab activities	15	5%
7	Final written exam	16	40%
8			

***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 :

Arrangements for availability of faculty and teaching staff for individual student consultations and academic advice. (include amount of time teaching staff are expected to be available each week)

- 6-office hours per week in the lecturer schedule.
- The contact with students by e-mail, mobile, office telephone, website and Black Board

F. Learning Resources and Facilities

1.Learning Resources

Required Textbooks	Gerben Kleijn & Terence Nicholls, Vulnerability Assessment and Penetration Testing Tools,2013
Essential References Materials	https://computing.uj.edu.sa/Pages-BScInCybersecurity.aspx
Electronic Materials	
Other Learning Materials	

2. Facilities Required

Item	Resources
Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.)	Classroom and Labe available at College of science in Zulfi.
Technology Resources (AV, data show, Smart Board, software, etc.)	All resource are available in the halls
Other Resources (Specify, e.g. if specific laboratory equipment is required, list requirements or attach a list)	N\A

G. Course Quality Evaluation

Evaluation Areas/Issues	Evaluators	Evaluation Methods
Effectiveness of teaching and assessment	Students Reviewers	Questionnaires (course evaluation) filled by the students and electronically organized by the university. Student-faculty and management meetings.
Quality of learning resources	Program Leaders	Direct/indirect

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	