جامعة الإسراء
ISRA UNIVERSITY

Course Syllabus

According to JORDAN National Qualification Framework (JNQF)

Course Name: Intrusion Detection System

Course Number: 6043257

General Course Information:

Course title	Intrusion Detection System
Course number	6043257
Credit hours	3
Education type	Face-to-Face
Prerequisites/corequisites	Introduction to Cyber Security (06043150)
Academic Program	Department of Cyber Security
Program code	0604
Faculty	Isra University
Department	Cyber Security
Level of course	3
Academic year /semester	1st semester, 4rd year
Awarded qualification	Bachelor (Bsc)
Other department(s) involved in teaching the course	None
Language of instruction	English
Date of production/revision	18/10/2021

Course Coordinator:

Coordinator's name	Dr. Hasan Kanaker
Office No	4225
Office Phone extension number	2612
Office Hours	[11-12] Sun, [12-1] Tues, Thur.; [11:00-12:30] Mon, [9:30-11] Wed
Email	hasan.kanaker@iu.edu.jo

Other Instructors:

Instructor name	
Office No	
Office Phone extension number	
Office Hours	
Email	

Course Description *(English/Arabic)*:

English	*Introduction to the data and methodologies of computer intrusion detection, Statistical and machine learning approaches to detection of attacks on computers, Network monitoring, and analysis, Estimating the number and severity of attacks; network-based attacks: probes and denial of service attacks; host-based attacks: buffer overflows and race conditions; and malicious code: viruses and worms, Statistical pattern recognition for detection and classification of attacks. Visualization of network data..*
Arabic	مقدمة إلى بيانات ومنهجيات كشف التسلل الحاسوبي ، وأساليب التعلم الإحصائي والتعلم الآلي للكشف عن الهجمات على أجهزة الكمبيوتر، ومراقبة الشبكة وتحليلها ، وتقدير عدد الهجمات وشدتها ؛ الهجمات القائمة على الشبكة: تحقيقات وهجمات رفض الخدمة ؛ الهجمات المستندة إلى المضيف: تجاوزات العازلة وظروف السباق ؛ والشفرات الضارة: الفيروسات والديدان، التعرف على الأنماط الإحصائية للكشف عن الهجمات وتصنيفها. تصور بيانات الشبكة.

Textbook: *Author(s), Title, Publisher, Edition, Year, Book website.*

1. Intrusion Detection Systems, Di Pietro, Roberto, Mancini, Luigi V, 2008.

References: *Author(s), Title, Publisher, Edition, Year, Book website.*

1. McClure S., Scambray J., "Hacking Exposed Network Security, Secrets and Solutions", 6th Edition, McGraw Hill, 2009, ISBN 9780071613743.

Course Educational Objectives (CEOs):

1.	Gain Understanding of Basic Issues, Concepts, Principles, and Techniques in Intrusion Detection.
2.	Be Able to Evaluate Intrusion Detection Systems for Particular Security Requirements
3.	Discover which operating system software is used on a network, which patches have not been updated
4.	Identify which TCP and UDP services are running, listening, or established on the network (port scan)
5.	Detect, identify, resolve and document network intrusions
6.	Learn what are the Intruders and types of malicious Software

Intended Learning Outcomes (ILO's):

1.	Subject Intended learning outcomes (ILOs) describe what students are expected to know and be able to do at the end of the course. These outcomes are related to the knowledge, skill and competence that students acquire:	**Relationship to CEOs**	**Contribution to PLOs**	**Bloom Taxonomy Levels***	**Descriptors****
1. A	Knowledge and Understanding:				
2. A1	Identify intrusion detection systems and their signatures.	1,2,6	a,b,d,f	1	K,S,C
3. A2	Explain the fundamental concepts of Network Protocol Analysis and demonstrate the skill to capture and analyze network packets**.**	2,4,5	b,c,d	1	S,C
4. A3	List the concepts Security Prevention, Detection and Recovery.	2,3,5	c,f	1	S,C
5. B	Intellectual skills:				
6. B1	Use various protocol analyzers and Network Intrusion Detection Systems as security tools to detect network attacks and troubleshoot network problems.	1,4,5,6	a,b,f	4	S,C
7. C	Subject specific skills:				
8. C1	State the basic requirements and policies to design, implement and evaluate a security system	1,2,5,6	a,b	2	K,S
9. D	Transferable skills:				
10. D1	Design and implement a fully secured network design between client and server.	2,3,4,5	a,b,c,d,e,f	2	K,S,C

***Bloom Taxonomy Levels**

Level #	1	2	3	4	5	6
Level Name	Knowledge	Comprehension	Application	Analysis	Evaluation	Synthesis

**** Descriptor (National Qualification Framework Descriptors): K : Knowledge, S: Skill, C: Competency.**

Program Learning Outcome (PLOs):

Program Learning Outcomes describe what students are expected to know and be able to do by the time of graduation. These relate to the knowledge, skills, and behaviours that students acquire as they progress through the program. A graduate of the () program will demonstrate:		Descriptors**		
		K	S	C
A.	Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions.	X		
B.	Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program's discipline.		X	
C.	Communicate effectively in a variety of professional contexts.			X
D.	Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles.			X
E.	Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline.			X
F.	Apply security principles and practices to maintain operations in the presence of risks and threats. [CY]		X	

**** Descriptors according to the national qualifications framework (K: knowledge, S: skill, C: Competency)**

Weekly Schedule *(please choose the type of teaching)*

☐ **Face to Face**

☐ **Hybrid** *(**2 Lectures** Face – To - Face **+1 Lecture** Asynchronous)*

☐ **Hybrid (*1 Lectures* Face – To - Face *+1 Lecture* Asynchronous)**

☐ **Online** *(**2 Lectures** Synchronous **+1 lecture Asynchronous**)*

Week	First Hour (F2F)	Second Hour (F2F)	Third Hour (F2F)	Ach. ILOs	Ach. PLOs	Descriptors*
1	Introduction to IDS	Introduction to IDS	Components of IDS	A1, A2	a	s
2	Value of IDS	Value of IDS	How IDS Works	A1, A3	b	s
3	Types of ID	Types of ID	Types of ID	A1, A2, A3	b	s
4	Intruders	Intruders	Intruders	A3, B1	c	c
5	IDS Techniques	IDS Techniques	Quiz#1	B1,C1,D1	d	c

6	Firewall-IDS	Firewall-IDS-Works	Firewall Architecture	A2, A3,B1,C1,D1	a	s
7	Firewall Architecture	Types of Firewall	Types of Firewall	A2, A3,B1,C1,D1	b	s
8	Firewall Technologies	Firewall Technologies	Firewall Technologies	A2, A3,B1,C1,D1	c	c
9	Firewall Technologies	Firewall-Limitations	Midterm Exam	B1, C1, D1	c	c
10	Honeypot-IDS	Types of Honeypots	Types of Honeypots	A2, A3,B1,C1,D1	b	s
11	Types of Honeypots	Types of Honeypots	Types of Honeypots	A2, A3,B1,C1,D1	b	s
12	Introducing Snort	Introducing Snort	Quiz#2	A2,A3,B1,C1,D1	e	k
13	Introduction to IPS	IPS & IDS - Differences	Types of IPS	A3, B1	f	k
14	IDS-Penetration Testing	IDS-Penetration Testing Stages	Firewall/IDS - Penetration Testing	A1,A2, A3,B1,C1,D1	f	k
15	Final Exam					
16						

* **K: Knowledge, S: Skills, C: Competency**

Teaching Methods and Assignments:

Development of ILOs is promoted through the following teaching and learning methods:

- Interactive videos
- Practice Labs
- Discussion Forums
- Quizzes
- Other Interactive online activities
- Reports

Course Policies:

A- Attendance policies:

The maximum allowed absences is 15% of the lectures.

B- Absences from exams and handing in assignments on time:

Midterm exam can be retaken based on approval of excuse by the instructor's discretion.

Not handing assignment on time will incur penalties.

C- Academic Health and safety procedures

D- Honesty policy regarding cheating, plagiarism, and misbehaviour:

Cheating, plagiarism, misbehaviour will result in zero grade and further disciplinary actions may be taken.

E- Grading policy:

- All homework is to be posted online through the e-learning system.
- Exams will be marked within 72 hours and the marked exam papers will be handed to the students.
- Online Activities (Course Videos, Practice labs, Discussion Forums, Quizzes) **30%**
- Midterm **20%**
- Final Exam **50%**

F- Available university services that support achievement in the course: **E-Learning Platform, Labs, Library.**

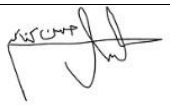
Required equipment:

- **PC / Laptop with webcam and mic**
- **Internet Connection**
- **Access to the IU E-Learning Platform at: https://elearn.iu.edu.jo/**
- **E-learning plan**
- Satisfaction questionnaires for online and face-to-face learning
- Software for e-learning
- Training

Assessment Tools implemented in the course:

- **Final Exam**
- **Midterm Exam**
- **Quizzes**
- **Homework**
- Practice Labs
- Discussion Forums
- Periodic reports for learning assessment
- Improvement plans for online or face-to-face teaching
- Others: Written Report

Responsible Persons and their Signatures:

Course Coordinator	**Dr.Hasan Kanaker**	**Completed Date**	**29/ 6 / 2022**
		Signature	

Received by (Department Head)	**Dr. Hasan Kanaker**	**Received Date**	**29/ 6 / 2022**
		Signature