Course Specification

(Postgraduate)

Course Title: Network security

Course Code: CYBS60203

Program: M.Sc. in Cybersecurity

Department: Department of Computer Science

College: Faculty of Computing and Information

Institution: Al-baha University

Version: 1

Last Revision Date: *Pick Revision Date.*

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: (3rd / 1st)

4. Course general Description:

This course imparts an understanding of methods and techniques essential for detecting and analyzing vulnerabilities and threats, while also equipping participants with the necessary skills to use these techniques effectively. It delves into various strategies to mitigate associated risks, ensuring that students can apply practical solutions in real-world scenarios. Additionally, the course emphasizes the development of critical thinking and problem-solving abilities, enabling learners to adapt and respond proactively to evolving cybersecurity challenges.

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

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

7. Course Main Objective(s):

The students completed this course will be able to:
- Explain what is meant by Network Security and how it works.
- Apply theoretical and practical knowledge to solve some selected real-world problems.
- Describe current threats and attacks and how to mitigate or defend against them.
Describe some of the standard tools to prevent attacks on networks environments.

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		

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**	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 the key concepts of network security.	**K1**	• Lectures • Assignments.	• Quizzes • Midterm Exams • Final Exam
2.0	**Skills**			
2.1	Utilize network defense tools to safeguard a network against vulnerabilities, threats, and attacks, and to manage incident response.	**S1**	• Lectures • Assignments	• Quizzes • Midterm Exams • Final Exam
2.2	Examine the implementation of security policies for network protection.	**S2**	• Lectures • Assignments	• Quizzes • Midterm Exams • Final Exam
2.3	Investigate network operations pertinent to defending a network.	**S3**	• Lectures • Assignments	• Quizzes • Midterm Exams • Final Exam
3.0	**Values, autonomy, and responsibility**			

Code	Course Learning Outcomes	Code of PLOs aligned with program	Teaching Strategies	Assessment Methods
3.1	Communicate concepts and techniques in discussions.	**V1**	• Assignments (Group) • Project (Group)	• Reports • Presentations • Class Discussions

C. Course Content:

No	List of Topics	Contact Hours
1	Network Threats, Attacks and Hardening	3
2	Minimizing Exposure, Attack Surface and Vectors, Threat Modeling	3
3	Defense in Depth and Implementing Firewalls	3
4	DMZs and Proxy Servers	3
5	Virtual Private Networks	3
6	Honeypots and Honeynets	3
7	Implementing IDS/IPS and Network Security Monitoring	3
8	Network Traffic Analysis	3
9	Threat Hunting	3
10	Attack Pattern Detection	2
11	Network Access Control	2
12	Network Policy Development and Enforcement	2
Total		**33**

D. Students Assessment Activities:

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1.	Assignments	Every two weeks	5%
2.	Report, presentation, and Class Discussions	Week 10	5%
3.	Midterm Exam	Within the 6th Week	20%
4.	Quizzes	Week 8	10%
5.	Project	Week 11	10%

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
6.	Final Exam	Week 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 E. Whitman and Herbert J. Mattord, Principle of Information Security, 2nd Edition –Thomson Course Technology • Bruce Schneier, Applied Cryptography, 2nd Edition, Wiley, 1996
Supportive References	• William Stallings, Cryptography and Network Security, 4th edition or later, Prentice Hall. • Communications of ACM (Association for Computer Machinery) - http://cacm.acm.org/ • Journal of the ACM - http://jacm.acm.org/
Electronic Materials	• Access to the Saudi Digital Library (SDL). • Using the learning management system of the university – Rafid System (https://lms.bu.edu.sa/). • IEEE/ACM Transactions on Networking https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=90
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 and assessment.	Students - Program Leaders	Indirect
Extent of achievement of course learning outcomes.	Peer reviewers	Direct
Quality of learning resources.	Students	Indirect
Reviewing course effectiveness and planning for improvement.	Program Leaders - Faculty	Direct
Verifying Standards of Student Achievement.	Faculty	Indirect

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

G. Specification Approval Data:

COUNCIL /COMMITTEE	
REFERENCE NO.	
DATE	