هيئة تقويم التعليم والتدريب
Education & Training Evaluation Commission

اعتماد
NCAAA

2024
TP-153

Course Specification

(Bachelor)

Course Title: Ethical hacking

Course Code: CYB 0211

Program: Computer Science(Cybersecurity)

Department: Applied Science

College: Applied Collage

Institution: Imam Muhammad Bin Islamic Universirty

Version: *Course Specification Version Number*

Last Revision Date: *Pick Revision Date.*

جامعة الإمام محمد بن سعود الإسلامية
١٤٠٥هـ ١٤٠٦هـ
الكلية التطبيقية

Table of Contents

A. General information about the course:

1. Course Identification

1. Credit hours: (4(3 Theory, 2 Lab))

2. Course type

A.	☐University	☐College	☒ Department	☐Track	☐Others
B.	☒ Required		☐Elective		

3. Level/year at which this course is offered: (First Semester)

4. Course General Description:

This course covers ethical hacking and penetration testing techniques using the latest software, techniques, and methodologies used by hackers and security professionals to lawfully hack an organization. Topics include session hijacking, hacking of web applications and servers, as well as social engineering and denial of services hacking techniques.

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

CYB 0202 (Cyber Threats)

6. Co-requisites for this course (if any)**:**

None

7. Course Main Objective(s):

- **Demonstrate an understanding of ethical hacking**
- **Identify possible ways to hack web applications**
- **Describe several techniques to attack wired and wireless networks**
- **Explain the concept of social engineering**

جامعة الإمام محمد بن سعود الإسلامية
١٤٠٥هـ ١٤٠٦هـ
الكلية التطبيقية

2. Teaching mode (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	Traditional classroom	4 hours\week	100%
2	E-learning		
3	Hybrid • Traditional classroom • E-learning		
4	Distance learning		

3. Contact Hours (based on the academic semester)

No	Activity	Contact Hours
1.	**Lectures**	36
2.	**Laboratory/Studio**	24
3.	**Field**	
4.	**Tutorial**	
5.	**Others (specify)**	
Total		60

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

Code	Course Learning Outcomes	Code of PLOs aligned with the program	Teaching Strategies	Assessment Methods
1.0	**Knowledge and understanding**			
1.1	Demonstrate an understanding of ethical hacking	**K1**	Class Discussion Questions/Answers sessions in class Case studies and analysis. Project and students	Quizzes, Exams, Project, Presentation
2.0	**Skills**			
2.1	Identify possible ways to hack web applications	**S1**	Class Discussion Questions/Answers sessions in class Case studies and analysis. Project and students	Quizzes, Exams, Project, Presentation
2.2	Describe several techniques to attack wired and wireless networks	**S2**	Class Discussion Questions/Answers sessions in class Case studies and analysis. Project and students	Quizzes, Exams, Project, Presentation
2.3	Explain the concept of social engineering	**S3**	Class Discussion Questions/Answers sessions in class Case studies and analysis. Project and students	Quizzes, Exams, Project, Presentation
3.0	**Values, autonomy, and responsibility**			

C. Course Content

No	List of Topics	Contact Hours
1.	Introduction to Ethical Hacking and Penetration Testing	6
2.	Planning and Scoping a Penetration Testing Assessment	8
3.	Information Gathering and Vulnerability Scanning	10
4.	Social Engineering Attacks	10
5.	Exploiting Wired and Wireless Networks	10
6.	Exploiting Application-Based Vulnerabilities	4
7.	Cloud, Mobile, and IoT Security	4
8.	Performing Post-Exploitation Techniques	4
9.	Reporting and Communication	4
Total		60

D. Students Assessment Activities

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1.	Quizes	3, 8	10%
3.	Midterm	7	20%
4.	Lab Assignments group or individual /Class Assignments group or individual	4,7,9	15%
4.	Lab Evaluations	All Semester	15%
5.	Project	10	10%
6.	Final	13, 14	30%

*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	Regalado, D. et al. , “Gray Hat Hacking: The Ethical Hacker's Handbook”, 2018, 5th Edition.
Supportive References	Wenliang Du, “Computer & Internet Security: A Hands-on Approach”, 2019, 2nd edition.
Electronic Materials	Online resources will be provided during class lectures.
Other Learning Materials	N/A

2. Required Facilities and equipment

Items	Resources
facilities (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)	Lecture room with Smart board Lab with 25 Pcs
Technology equipment (projector, smart board, software)	PC and WiFi Internet access within the classroom
Other equipment (depending on the nature of the specialty)	N\A

جامعة الإمام محمد بن سعود الإسلامية
١٤٠٥هـ ١٤٠٦هـ
الكلية التطبيقية

F. Assessment of Course Quality

Assessment Areas/Issues	Assessor	Assessment Methods
Effectiveness of teaching	Student	Indirect using course evaluation survey
Effectiveness of Students assessment	Student	Indirect using course evaluation survey
Quality of learning resources	Student and Faculty	Indirect using course evaluation and faculty survey
The extent to which CLOs have been achieved		
Other		

Assessors (Students, Faculty, Program Leaders, Peer Reviewers, Others (specify)

Assessment Methods (Direct, Indirect)

G. Specification Approval

COUNCIL /COMMITTEE	
REFERENCE NO.	
DATE	