



# Course Specification

## — (Bachelor)

Course Title: Fundamentals of Ethical Hacking

Course Code: APIS3213

Program: Information Security Diploma

Department: Diplomas

College: Applied College

Institution: Umm Al-Qura university

Version: 1.0

Last Revision Date: 15 December 2024



## Table of Contents

A. General information about the course: .....	3
B. Course Learning Outcomes (CLOs), Teaching Strategies and Assessment Methods .....	4
C. Course Content.....	5
D. Students Assessment Activities .....	6
E. Learning Resources and Facilities.....	6
F. Assessment of Course Quality .....	7
G. Specification Approval .....	7





## A. General information about the course:

### 1. Course Identification

1. Credit hours: ( 4 )

#### 2. Course type

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

3. Level/year at which this course is offered: ( Level 3, 2<sup>nd</sup> year )

#### 4. Course General Description:

This course introduces students to ethical hacking terminologies and methodologies. Students will learn what and who an ethical hacker is and its important role in protecting corporate, industrials, and government data from cyber-attacks. Students will apply attacker's techniques to compromise networks to learn how to protect them. Topics to be covered but not limited to the penetration testing methodologies and tools used by ethical hackers, hacker's tools and methodologies, and how to set up strong countermeasures to protect networks and systems thorough lab activities.

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

- Cyber Crimes and Threats
- Computer Networks
- Web Security

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

None

#### 7. Course Main Objective(s):

Upon completing this course, students will be able to:

1. Demonstrate the ability to report on the strengths and vulnerabilities of tested network
2. Express the ability to attack and defend a network
3. Demonstrate how to attack a system
4. Perform penetration testing using standard hacking tools in an ethical manner



## 2. Teaching mode (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	Traditional classroom	(3 lec + 2 Lab)/Week	100%
2	E-learning		
3	Hybrid <ul style="list-style-type: none"> <li>Traditional classroom</li> <li>E-learning</li> </ul>		
4	Distance learning		

## 3. Contact Hours (based on the academic semester)

No	Activity	Contact Hours
1.	Lectures	45
2.	Laboratory/Studio	30
3.	Field	
4.	Tutorial	
5.	Others (specify)	
Total		75

## 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 the ability to report on the strengths and vulnerabilities of tested network	K2	Lecture	Assignments/labs/Quizzes/Exams
2.0	Skills			
2.1	Express the ability to attack and defend a network	S1	Lecture/Labs	Assignments/labs/Quizzes/Exams
2.2	Perform penetration testing using standard hacking tools in an ethical manner	S3, S4, S6	Lecture/Labs	Assignments/labs/Quizzes/Exams





Code	Course Learning Outcomes	Code of PLOs aligned with the program	Teaching Strategies	Assessment Methods
3.0	Values, autonomy, and responsibility			
3.1	Working individually to empower students be responsible and motivated to complete tasks; therefore, it helps then to be more disciplined.	V1, V2, V4	Assignments/ Labs	labs/Quizzes

### C. Course Content

No	List of Topics	Contact Hours
1.	Introduction to Ethical Hacking	3
2.	Laws and Guidelines of Ethical Hacking	3
3.	Types of Ethical Hackers, Advantages and Disadvantages	3
4.	Overview of Cryptography and Encryption	4
5.	Ethical Hacking Methods	4
6.	Reconnaissance (defining legalities, social engineering, Internet footprinting, scanning and enumeration)	4
7.	Networks vulnerabilities (TCP/IP vulnerabilities: IP spoofing, connection hijacking, ICMP attacks, TCP SYN attacks, RIP attacks, IP Security Architecture (IPSec), Firewall and honeypots)	4
8.	Sniffing Tools and Techniques	4
9	System hacking (Windows and Linux)	4
10	Web-based hacking (attacking web servers and applications)	4
11	Wireless Network Hacking	4
12	Penetration testing (security assessments, information gathering and analysis)	4
Total		45





## Laboratory Content

No	List of Topics	Contact Hours
1.	Footprinting	4
2.	Scanning	4
3.	Enumeration	3
4.	Sniffing	4
5.	Denial of Service	3
6.	System Hacking	4
7.	Web Server Hacking	4
8.	Web Applications Vulnerabilities	4
Total		30

## D. Students Assessment Activities

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1.	Quizzes	Throughout Semester	10
2.	Midterm Exam	8	20
3.	Laboratory	14	30
4.	Final Exam	Final week	40

\*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

Walker, Matt. CEH Certified Ethical Hacker Boxed Set, 1 ed. McGraw-Hill USA, 2013

1. Learn Ethical Hacking from Scratch: Your stepping stone to penetration testing by Zaid Al-Quraishi, , ISBN : 978-1788622059

2. The Shellcoder's Handbook: Discovering and Exploiting Security Holes ", by Chris Anley, John Heasman, Felix Lindner, Gerardo Richarte; ASIN: B004P5O38Q



Supportive References	<ul style="list-style-type: none"> <li>Kim, Peter. The Hacker Playbook (Book 3), ed. Independently published, 2018</li> <li>Kim, P. (2014). The hacker playbook 3: Practical guide to penetration testing (pp. 328-362). South Carolina: Secure Planet LLC.</li> </ul>
Electronic Materials	
Other Learning Materials	

## 2. Required Facilities and equipment

Items	Resources
<b>facilities</b> (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)	Traditional Classroom, Laboratory
<b>Technology equipment</b> (projector, smart board, software)	Multimedia Projector, Internet access, Common digital hacking tools
<b>Other equipment</b> (depending on the nature of the specialty)	

## F. Assessment of Course Quality

Assessment Areas/Issues	Assessor	Assessment Methods
Effectiveness of teaching	Students	Survey at the end of the course
Effectiveness of Students assessment	Instructor	Course Report
Quality of learning resources	Instructor	Survey at the end of the course
The extent to which CLOs have been achieved	Instructor	Course Report
Other		

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





Assessment Methods (Direct, Indirect)

## G. Specification Approval

COUNCIL /COMMITTEE	Umm Al-Qura University Council
REFERENCE NO.	851141114462/190358
DATE	1446/11/22

