QF01/0408-4.0E	Course Plan for Bachelor program - Study Plan Development and Updating Procedures/ Cyber Security Department

Study plan No.	**2024/2025**		**University Specialization**	**Cybersecurity**	
Course No.	**0133306**		**Course name**	Ethical Hacking in Cyber Security	
Credit Hours	**3**		**Prerequisite Co-requisite**	Infrastructure Security Using Linux Secure Communication Protocols	
Course type	☐ MANDATORY UNIVERSITY REQUIREMENT	☐ UNIVERSITY ELECTIVE REQUIREMENTS	☐ FACULTY MANDATORY REQUIREMENT	☐ Support course family requirements	☐ ✓ **Mandatory requirements** ☐ Elective requirements
Teaching style	☐ **Full online learning**		☐ Blended learning		☐ ✓ Traditional learning
Teaching model	☐ 2Synchronous: 1asynchronous		☐ 2 face to face : 1synchronous		☐ ✓ **3 Traditional**

Faculty member and study divisions information (to be filled in each semester by the subject instructor)

Name	Academic rank	Office No.	Phone No.	E-mail	
Dr Omran Salem	**assistant professor**	**316**		**o.salem@zuj.edu.jo**	
Division number	**Time**	**Place**	**Number of students**	**Teaching style**	**Approved model**

Brief description

This course equips students with essential knowledge to enhance their ability to detect hacking threats and employ techniques/tools to mitigate them. It covers foundational concepts of hacking, methods for gathering information, target enumeration, port scanning, vulnerability assessment, basics of Windows exploit development, and wireless/web hacking. Additionally, students will learn how to write official penetration testing reports, ensuring clear and professional documentation of findings and recommendations. The course also emphasizes ethical considerations in hacking, highlighting the importance of adhering to legal and moral standards, as well as the critical role of Non-Disclosure Agreements (NDAs) in maintaining confidentiality and trust. Students are strongly advised to avoid practicing any hacking exercises in open or public network environments.

Learning resources

Course book information (Title, author, date of issue, publisher ... etc.)	EC-Council Academia, Ethical Hacking and Countermeasures V13, Complete series (2023) (official)
Supportive learning resources (Books, databases, periodicals, software, applications, others)	1. Ric Messier - CEH V12 Certified Ethical Hacker Study Guide-Sybex (2023) 2. Glen D. Singh, The Ultimate Kali Linux Book: Harness Nmap, Metasploit, Aircrack-ng, and Empire for Cutting-Edge Pentesting in this 3rd Edition by Packt Publishing (2023) 3. William Chuck Easttom - Certified Ethical Hacker (Ceh) Exam Cram (Exam Cram (Pearson))-Pearson It Certification (2022
Supporting websites	https://hackersacademy.com/ , https://tryhackme.com/

QF01/0408-4.0E	Course Plan for Bachelor program - Study Plan Development and Updating Procedures/ Cyber Security Department

The physical environment for teaching	☐ **Class room**	☐ ✓labs	☐ **Virtual educational platform**	☐ Others
Necessary equipment and software				
Supporting people with special needs				
For technical support	**E-learning and Open Educational Center. Computer Center**			

Course learning outcomes (S= *Skills, C= Competences K= Knowledge,)*

No.	Course learning outcomes	The associated program learning output code
	Knowledge	
K1	knowledge of foundational cybersecurity concepts, including threats, vulnerabilities, and countermeasures.	**PLO1**
K2	Explain the main concepts of Ethical Hacking Methodology and framework.	**PLO2**
	Skills	
S1	Summarize the vulnerability analysis and assessment concept	**PLO7**
	Competences	
C1	Apply different techniques and tools for system hacking, gaining access, post exploitation and privilege escalation.	**PLO11**

Mechanisms for direct evaluation of learning outcomes

Type of assessment / learning style	Fully electronic learning	Blended learning	Traditional Learning (Theory Learning)	Traditional Learning (Practical Learning)
First exam	0	**0**	0	0
Second / midterm exam	%30	**%30**	%30	%30
Participation / practical applications	0	**0**	0	0
Asynchronous interactive activities	%30	**%30**	%30	%30
final exam	%40	**%40**	%40	%40

Note: Asynchronous interactive activities are activities, tasks, projects, assignments, research, studies, projects, work within student groups ... etc., which the student carries out on his own, through the virtual platform without a direct encounter with the subject teacher.

Schedule of simultaneous / face-to-face encounters and their topics

Week	Subject	learning style*	Reference **
1	• Introduction • Overview of important technologies	Face to Face	Ric Messier - CEH V12 Certified Ethical Hacker Study Guide

2	• Categories of penetration tests • Categories of Linux Systems, major Linux operating systems	Face to Face	Ric Messier - CEH V12 Certified Ethical Hacker Study Guide
3	• File structure inside of Linux, common applications of Linux • Information gathering methods	Face to Face at the lab	Ric Messier - CEH V12 Certified Ethical Hacker Study Guide
4	• Differences between active and passive information gathering, sources of information gathering • Copying websites locally and globally	Face to Face at the lab	Ric Messier - CEH V12 Certified Ethical Hacker Study Guide
5	• Intercepting a response, target enumeration and port scanning techniques • Scanning for open ports and services	Face to Face. Experiment	Ric Messier - CEH V12 Certified Ethical Hacker Study Guide
6	• Types of port scanning, port status types • Scanning for a vulnerable host	Face to Face at the lab	Ric Messier - CEH V12 Certified Ethical Hacker Study Guide
7	• Vulnerability assessment, pros and cons of a vulnerability scanner • Assessment with Nmap, Nessus vulnerability scanner	Face to Face at the lab	Glen D. Singh, The Ultimate Kali Linux Book: Harness Nmap, Metasploit, Aircrack-ng
8	**Midterm Exam**		
9	• Port range, Network sniffing, • types of sniffing	Face to Face at the lab	Glen D. Singh, The Ultimate Kali Linux Book: Harness Nmap, Metasploit, Aircrack-ng
10	• Networks sniffing (cont'd), MITM attacks • ARP protocol basics, ARP attacks	Face to Face at the lab	Glen D. Singh, The Ultimate Kali Linux Book: Harness Nmap, Metasploit, Aircrack-ng
11	• Remote Exploitation • Understanding network protocols, server protocols, Client-side exploitation	Face to Face at the lab	Glen D. Singh, The Ultimate Kali Linux Book: Harness Nmap, Metasploit, Aircrack-ng
12	• Client-side exploitation methods • PDF launch action, origami framework	Face to Face at the lab	Ric Messier - CEH V12 Certified Ethical Hacker Study Guide
13	• Browser exploitation & Web hacking, attacking the authentication, • Windows exploit development basics,	Face to Face at the lab	Ric Messier - CEH V12 Certified Ethical Hacker Study Guide
14	• Ethical Hacking Project • 2 or 3 students manage to conduct ethical hacking using new tools	Face to Face	
15	Project Discussion	Face to Face	
16	Final Exam		

*** Learning styles: Lecture, flipped learning, learning through projects, learning through problem solving, participatory learning ... etc.**

**** Reference: Pages in a book, database, recorded lecture, content on the e-learning platform, video, website ... etc.**

Schedule of asynchronous interactive activities (in the case of e-learning and blended learning)

QF01/0408-4.0E	Course Plan for Bachelor program - Study Plan Development and Updating Procedures/ Cyber Security Department

Week	Task / activity	Reference	Expected results
1	Footprinting and reconnaissance/gathering publicly accessible information about targeted system using required tools	Ethical Hacking and Countermeasures V13, Complete series (2023)/module 02	Generating blueprint file
2	Vulnerability identification and analysis/ run automated vulnerability analysis tool such as nessus	Ethical Hacking and Countermeasures V13, Complete series (2023)/module 05	Writing a report with exploitable identified vulnerabilities and classify them based on severity level
3	Post exploitation/escalating the privilege sand maintaining access on hacked system using the required techniques	Ethical Hacking and Countermeasures V13, Complete series (2023)/module 010	Remaining undetected and enhancing the ability of being existed on the hacked system
4			
5			
6			
7			
8			