Form: Course Syllabus	Form Number	
	Issue Number and Date	2/3/24/2022/2963 5/12/2022
	Number and Date of Revision or Modification	
	Deans Council Approval Decision Number	
	The Date of the Deans Council Approval Decision	
	Number of Pages	11

1.	Course title	Penetration Testing and Ethical Hacking	
2.	Course number	1911381	
3.	Credit hours	4	
	Contact hours (theory, practical)	(theory :2 , practical : 2)	
4.	Prerequisites/corequisites	1901363 + 1911211	
5.	Program title	CYBER SECURITY	
6.	Program code	01	
7.	Awarding institution		
8.	School	King Abdullah II School of Information Technology	
9.	Department	Computer Science	
10.	Course level	3	
11.	Year of study and semester (s)	First year / First Semester	
12.	Other department (s) involved in teaching the course	-	
13.	Main teaching language	English	
14.	Delivery method	☒Face to face learning ☐Blended ☐Fully online	
15.	Online platforms(s)	☒Moodle ☐Microsoft Teams ☐Skype ☐Zoom ☐Others.....	
16.	Issuing/Revision Date	Oct/2025	

17. Course Coordinator:

Name: Dr. Ahmad Al Hwaitat	Contact hours: Wed (11:30 – 12:30)
Office number: 322	Sun (12:30-1:30)
Email: a.hwaitat@ju.edu.jo	hone number: 5355000

18. Other instructors:

19. Course Description:

This course on Penetration Testing and Ethical Hacking is designed to provide participants with comprehensive knowledge and practical skills essential for identifying and securing vulnerabilities within computer systems and networks. Students will delve into the world of ethical hacking, exploring techniques employed by cybersecurity professionals to assess and fortify the security posture of digital environments. The curriculum covers a range of topics, including reconnaissance, vulnerability analysis, exploitation, post-exploitation, and reporting. Participants will gain hands-on experience using industry-standard tools and methodologies, enabling them to simulate real-world cyber-attacks in a controlled environment. Emphasis will be placed on the ethical considerations surrounding hacking activities, ensuring that students understand the importance of responsible and lawful practices in the field. By the end of the course, participants will be equipped with the skills necessary to conduct penetration tests ethically, contributing to the enhancement of cybersecurity measures in today's dynamic and ever-evolving digital landscape

20. Course aims and outcomes:

A- Aims:

Goal:

The primary aim of the Penetration Testing and Ethical Hacking course is to equip participants with a comprehensive understanding of cybersecurity concepts and methodologies essential for ethical hacking practices. The course aims to provide a practical and hands-on learning experience, allowing students to develop the skills necessary for identifying, exploiting, and securing vulnerabilities in computer systems and networks..

Objectives:

- *Understand fundamental concepts of cybersecurity, including confidentiality, integrity, and availability.*
- *Explore the role of ethical hacking in identifying and mitigating security risks.*
- *Learn methods for information gathering and reconnaissance to assess potential vulnerabilities.*
- *Utilize open-source intelligence (OSINT) tools to gather information about target systems.*
- *Develop skills in identifying and assessing vulnerabilities in software, networks, and systems.*
- *Explore automated and manual vulnerability scanning techniques.*
- *Gain proficiency in exploiting identified vulnerabilities through hands-on exercises.*
- *Understand common exploitation techniques and tools used in ethical hacking.*
- *Explore techniques for maintaining access to compromised systems for further analysis.*
- *Understand the importance of covering tracks and maintaining stealth during post-exploitation.*
- *Emphasize ethical behavior and adherence to legal frameworks in conducting penetration tests.*
- *Understand the implications of unauthorized access and the importance of responsible disclosure.*
- *Familiarize yourself with industry-standard tools such as Metasploit, Wireshark, and Nmap.*
- *Gain practical experience using these tools to simulate various stages of an ethical hacking engagement.*
- *Develop the ability to document and report findings in a clear, structured manner.*
- *Understand the importance of tailored reports for technical and non-technical stakeholders.*
- *Engage in collaborative exercises to simulate real-world ethical hacking scenarios.*
- *Foster teamwork and communication skills essential for effective cybersecurity practices.*
- *Instill a commitment to continuous learning and staying updated on evolving cybersecurity threats.*
- *Provide resources and guidance for ongoing professional development in ethical hacking.*

B- **Intended Learning Outcomes (ILOs):** Upon successful completion of this course students will be able to …

A-Knowledge and understanding with the ability to …

A1) Understand basic concepts of Introduction to Cybersecurity.
A2) Understand basic concepts of Reconnaissance Techniques.
A3) Understand basic concepts of Vulnerability Analysis.
A4) Understand basic concepts of Exploitation Methods.
A5) Understand basic concepts of Post-Exploitation Activities.
A6) Understand basic concepts of Ethical and Legal Considerations.
A7) Understand basic concepts of Hands-On Experience with Tools.
A8) Understand basic concepts of Effective Reporting Skills.
A9) Understand basic concepts of Collaborative Team Exercises.

B- Intellectual skills: with the ability to …

B1) Demonstrate the ability to critically analyze complex cybersecurity scenarios, identifying potential vulnerabilities and evaluating the effectiveness of security measures.
B2) Apply problem-solving skills to address and mitigate security challenges, devising effective solutions in ethical hacking scenarios.
B3) Exhibit strategic thinking in planning and executing ethical hacking activities, considering potential risks and formulating proactive security measures.
B4) Conduct thorough risk assessments, weighing the impact and likelihood of identified vulnerabilities to prioritize remediation efforts effectively.
B5) Demonstrate adaptability in responding to dynamic and evolving cybersecurity threats, adjusting ethical hacking strategies to address new challenges.
B6) Explore innovative approaches to ethical hacking, staying ahead of potential threats and devising creative solutions to secure digital environments.
B7) Apply intellectual skills to develop incident response strategies, demonstrating the ability to react promptly and effectively to security incidents.
B8) Exhibit sound decision-making skills in ethical hacking scenarios, considering ethical, legal, and technical factors to determine the appropriate course of action.
B9) Showcase research competence by staying updated on the latest cybersecurity trends, tools, and methodologies, integrating new knowledge into ethical hacking practices.
10) Conduct systematic evaluations of security postures, utilizing intellectual skills to identify weaknesses and recommend improvements in digital systems.

C- Subject specific skills – with ability to …

C1) Demonstrate a deep understanding of network architectures, protocols, and configurations relevant to ethical hacking scenarios.
C2) Exhibit proficiency in programming languages and scripting for developing custom tools and automating ethical hacking tasks
C3) Showcase expertise in various operating systems (Windows, Linux, Unix) to navigate, exploit, and secure systems encountered during ethical hacking engagements.

D- Transferable skills – with ability to

D1) Demonstrate effective communication skills through the ability to articulate complex technical concepts clearly and concisely to both technical and non-technical stakeholders. This includes the proficiency to create detailed yet accessible reports and documentation.
D2) Exhibit strong collaborative skills by actively participating in team-based ethical hacking exercises, fostering an environment of shared knowledge and expertise. This includes the ability to work seamlessly within diverse teams to achieve common cybersecurity goals.
D3) Showcase a commitment to continuous learning and adaptability by staying informed about evolving cybersecurity trends, tools, and methodologies.

Program SOs / ILOs of the course	SO (1)	SO (2)	SO (3)	SO (4)
A1 ... A10	√			
B1... B9	√			
C1... C3	√			
D1 ... D3	√			

21. Topic Outline and Schedule:

Week	Lecture	Topic	ILOs	Learning Methods (Face to Face/Blended / Fully Online)	Platform	Synchronous / Asynchronous Lecturing	Evaluation Methods	Resources
1	1.1	Information Security Overview	A1	Face to face lecturing	Moodle	Synchronous		
	1.2	HACKING &ETHICAL HACKING	A1&A6 &C1	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Textbook: CH01
	1.3	**Labs Introduction**	A1&A7 &C1-C3 &A9	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Hands-on
	2.1	FOOTPRINTING CONCEPTS	A1-A3&B3 &B4	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Textbook: CH02
2	2.2	Common Tools - FOOTPRINTING	A2&A7 &	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Textbook: CH02
	2.3	**Lab1**	A7&B1 &C3&D2&A9	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Hands-on
	3.1	SCANNING CONCEPTS	A2-A3&B4	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Textbook: CH03
3	3.2	Scan Types and Tools	A2&A7 &B3					
	3.3	**Lab2**	A3&A7 &A9&B1&B4& C3&D2 &	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Hands-on

	4.1	Enumeration Concepts	A2&A3	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Textbook: CH04
4	**4.2**	Enumeration Tools and Techniques	A7&B2	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Textbook: CH04
	4.3	**Lab3**	A9&B1 &B10& C3&D2	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Hands-on
	5.1	Vulnerability Scans	A4&B3	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Textbook: CH05
5	**5.2**	Vulnerability Scanning Penetration TestingTools	A4&A7 &A8&B 6&D1& D3	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Textbook: CH05
	5.3	**Lab4**	A9&B1 &B10& C3&D2	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Hands-on
	6.1	SYSTEM HACKING CONCEPTS	A4&B3	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Textbook: CH06
6	**6.2**	SYSTEM HACKING TOOLS AND FRAMEWORK S (Metasploit)	A4&A7 &B6&B 7&D3	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Textbook: CH06
	6.3	**Lab5**	A9&B1 &B10& C3&D2	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Hands-on
	7.1	INTRODUCTI ON TO MALWARE	A3&A4 &B2&B 5	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Textbook: CH07
7	**7.2**	How Malware Works	A4&B6 &C1	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Textbook: CH07
	7.3	**Lab6**	A9&B1 &B10& C3&D2	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Hands-on
	8.1	SNIFFING OVERVIEW and Types of Sniffing	A4&B1 &B10	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Textbook: CH08

8	**9.1-9.2**	Social Engineering Concepts	A3&B3	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Textbook: CH09
	10.1	DOS-DDOS CONCEPTS	A3&B7	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Textbook: CH10
	10.2	VOLUMETRIC ATTACKS and Tools	A7&B4	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Textbook: CH10
	10.3	**Lab7**	A9&B1 &B10& C3&D2	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Hands-on
9	**11.1**	SESSION HIJACKING CONCEPTS	A3&B7	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Textbook: CH11
	11.2	SESSION HIJACKING TOOLS	A7&B4	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Textbook: CH11
		Midterm Exam		Face to face lecturing	Moodle	Synchronous	Midterm	
10	**12.1**	Web Server Security	A3&A4 &B7	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Textbook: CH13
	12.2	Testing Web Servers	A3&A4 &A8&B 7	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Textbook: CH13

	13.1	WEB APPLICATION CONCEPTS	A3&A4 &B7	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Textbook: CH14
	13.2	**Lab8**	A9&B1 &B10& C3&D2	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Hands-on
11	14.1	SQL INJECTION OVERVIEW	A3&B3 &B5	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Textbook: CH15
	14.2	FINDING VULNERABLE WEBSITES and tools	A7&B4 &B10	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Textbook: CH15
	14.3	**Lab9**	A9&B1 &B10& C3&D2 &D3	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Hands-on
12	15.1	WIRELESS CONCEPTS	A3&B3 &B5	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Textbook: CH16
	15.2	WI-FI DISCOVERY TOOLS	A3&B3 &B5	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Textbook: CH16
	15.3	**Lab10**	A7&B4 &B10	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Hands-on
13		Revision						
		Final Exam		Face to face lecturing	Moodle	Synchronous	Final	

22. Evaluation Methods:

Opportunities to demonstrate achievement of the ILOs are provided through the following assessment methods and requirements:

Evaluation Activity	Mark	Topic(s)	ILOs	Period (Week)	Platform
MID exam	30	1 … 11	A4,A5,B7,B8,B10, D1	50 minutes 5h week	JUExams
Quiz exam Practical	10	1 … 15	A1,A2,B1-B10	30 minutes 5th week	JUExams
Home works	10	1..15	All ILOs		
Final exam	50	1 … 15	All ILOs	60 minutes 9th week	JUExams

23. Course Requirements

(e.g: students should have a computer, internet connection, webcam, account on a specific software/platform…etc):

- Computer + security tools
- Internet connection
- Account on Moodl

24. Course Policies:

A- Attendance policies:

Deliberate abstention from attending **1911381** *classes and any other similar acts will lead to student deprivation from the course according to the UJ regulations.*

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

If you miss the midterm, then a makeup exam will not be provided unless you submit a valid absence excuse, within three days from the midterm to your lecturer. This excuse must be signed and stamped from the UJ hospital to be valid. If your lecturer accepts the excuse, then you will be able to take the makeup. You need

to follow up the departmental announcements regarding the makeup date and time. Please note that the lecturer may either accept or reject your excuse based on UJ regulations.

C- Health and safety procedures:

N/A

D- Honesty policy regarding cheating, plagiarism, misbehavior:

All students in this course must read the University policies on plagiarism and academic honesty.

http://registration.ju.edu.jo/RegRegulations/Forms/All_Regulations.aspx

E- Grading policy:

- *Midterm Exam:*	*30%*
-Homework	*10%*
- Short Quiz (practical)	*10%*
- Final Exam:	*50%*

F- Available university services that support achievement in the course:

N/A

G- Statement on Students with disabilities

Students with Disabilities: Students with disabilities who need special accommodations for this class are encouraged to meet with the instructor and/or their academic advisor as soon as possible. In order to receive accommodations for academic work in this course, students must inform the course instructor and/or their academic advisor, preferably in a written format, about their needs no later than the 4th week of classes.

25. References:

A- Required book (s), assigned reading and audio-visuals:

Ethical Hacking and Countermeasures Version 12 , 2022 by EC-Council.

B- Recommended books, materials, and media:

Hacking: The Art of Exploitation, 2nd Edition Book by Jon Erickson

26. Additional information:

ملاحظة 1 : في حالة التغيب عن امتحان ال Mid Term لن يكون هناك امتحان تعويضي إلا في حالة وجود عذر وحالة طارئة من المستشفى. على الطالب إبراز العذر لمدرس المادة في فتره لا تتجاوز الثلاثة أيام من تاريخ الامتحان, وللمدرس الحق في قبول أو رفض العذر , وحسب التعليمات.
ملاحظة 2 : لتفادي المشاكل والأخطاء التي تنتج, لا يجوز إجراء النقل الداخلي بأي حال من الأحوال.

For more details on University regulations please visit http://www.ju.edu.jo/rules/index.htm

Moodle:
http://elearning.ju.edu.jo/

Name of Course Coordinator: --Dr.Ahmad AL Hwaitat-- Signature:
Date: Feb 18 , 2024

Head of Curriculum Committee/Department: ----------Signature: ----------

Head of Department: ----------Signature: ----------

Head of Curriculum Committee/Faculty: ----------Signature: ----------

Dean: ----------Signature: ----------