The Hashemite University

الجامعـــــة الهاشميـــــة

Deanship of Academic Development and International Outreach

عمادة التطوير الأكاديمي والتواصل الدولي

Syllabus: Hacking Techniques (2010021732)

Second Semester 2021/2022

COURSE INFORMATION

Course Name: Hacking Techniques **Semester:** Second Semester 2021 /2022 **Department:** Department of CIS **Faculty:** Prince Al-Hussein bin Abdullah II Faculty for Information Technology	**Course Code:** 2010021732 **Section:** 3 **Core Curriculum**:
Day(s) and Time(s): Sunday: 9-10 Tuesday: 9-10 **Classroom:** IT: 210	**Credit Hours:** 3 **Prerequisites**: None

COURSE DESCRIPTION

This course introduces the principles of security, privacy, authentication, and attack recovery. It describes the changes that must be made to the architecture of system in order to achieve end-to-end secure environments. A detailed examination of the security challenges and sources of threat .in applications is provided

After discussing the security issues, various emerging and existing technologies focused on achieving a high degree of trust in the applications are discussed. Four different technologies, blockchain, fog computing, edge computing, and machine learning, to increase the level of security are discussed.

DELIVERY METHODS

The course will be delivered through a combination of active learning strategies. These will include:

- PowerPoint lectures and active classroom-based discussion
- Course Project
- E-learning resources: e-reading assignments through Model and Microsoft Team

FACULTY INFORMATION

Name	**Ayoub Alsarhan**
Academic Title:	**Professor**
Office Location:	**IT 232**
Telephone Number:	**5063**
Email Address:	**ayoubm@hu.edu.jo**
Office Hours:	**Sunday** 9.00-10.00 / **Tuesday** 9.00-10.00 *Please send an e-mail (ayoubm@hu.edu.jo) to meet at any other time.*

REFERENCES AND LEARNING RESOURCES

Required Textbook:

- Hands-On Ethical Hacking and Network Defense, 2th Edition , Michael T. Simpson, Kent Backman, James Corley ; Published: 2021 - ISBN-10: 978-1435486096 | ISBN-13: 1435486099.

Suggested Additional Resources:

- Josh Pauli, "The Basics of Web Hacking: Tools and Techniques to Attack the Web", Syngress; 1st editio, ISBN: 0124166008, (2013).
- Christopher C. C. Elisan, " Advanced Malware Analysis", McGraw Hill, ISBN−13: 978−0071819749, 1st Edition,2015.

COURSE OBJECTIVES

- To learn about the hacking techniques and identify security critical applications areas of hacking
- To learn about the sources of security threats in applications and improvement and enhancement required for upcoming applications.
- To learn about the password cracking techniques.
- To Evaluate web applications.
- To Evaluate the security schemes in wireless computing.
- To learn about the penetration Testing techniques.
- Identify the Information Security Threats and Vulnerability Assessment.
- Be able to identify several research challenges of security in cloud computing.
- Be able to work effectively in teams, collaborate with other cyber and information security specialists, and take the initiative in solving complex technical problems

ACADEMIC SUPPORT

It is The Hashemite University policy to provide educational opportunities that ensure fair, appropriate and reasonable accommodation to students who have disabilities that may affect

their ability to participate in course activities or meet course requirements. Students with disabilities are encouraged to contact their Instructor to ensure that their individual needs are met. The University through its Special Need section will exert all efforts to accommodate for individual's needs.

Special Needs Section:

Tel: 053903333 EXT 5023/4583

Location: (https://hu.edu.jo/facnew/index.aspx?typ=68&unitid=70000000)

Email: (huniv@hu.edu.jo)

COURSE REGULATIONS

Participation

Class participation and attendance are important elements of every student's learning experience at The Hashemite University, and the student is expected to attend all classes. A student should not miss more than 15% of the classes during a semester. *Those exceeding this limit of 15% will receive a failing grade regardless of their performance*. It is a student's responsibility to monitor the frequency of their own absences. **Attendance record begins on the first day of class irrespective of the period allotted to drop/add and late registration. It is a student's responsibility to sign-in; failure to do so will result in a non-attendance being recorded.**

In exceptional cases, the student, with the instructor's prior permission, could be exempted from attending a class provided that the number of such occasions does not exceed the limit allowed by the University. The instructor will determine the acceptability of an absence for being absent. A student who misses more than 25% of classes and has a valid excuse for being absent will be allowed to withdraw from the course.

Plagiarism

Plagiarism is considered a serious academic offence and can result in your work losing marks or being failed. HU expects its students to adopt and abide by the highest standards of conduct in their interaction with their professors, peers, and the wider University community. As such, a student is expected not to engage in behaviours that compromise his/her own integrity as well as that of the Hashemite University.

Plagiarism includes the following examples and it applies to all student assignments or submitted work:

- **Use of the work, ideas, images or words of someone else without his/her permission or reference to them.**
- **Use of someone else's wording, name, phrase, sentence, paragraph or essay without using quotation marks.**
- **Misrepresentation of the sources that were used.**

The instructor has the right to fail the coursework or deduct marks where plagiarism is detected

Late or Missed Assignments

In all cases of assessment, students who fails to attend an exam, class project or deliver a presentation on the scheduled date without prior permission, and/or are unable to provide a medical note, will automatically receive a fail grade for this part of the assessment.

- Submitting a term paper on time is a key part of the assessment process. Students who fail to submit their work by the deadline specified will automatically receive a 10% penalty. Assignments handed in more than 24 hours late will receive a further 10% penalty. Each subsequent 24 hours will result in a further 10% penalty.
- In cases where a student misses an assessment on account of a medical reason or with prior permission; in line with University regulations an incomplete grade for the specific assessment will be awarded and an alternative assessment or extension can be arranged.

Student Complaints Policy

Students at Hashemite University have the right to pursue complaints related to faculty, staff, and other students. The nature of the complaints may be either academic or non-academic. For more information about the policy and processes related to this policy, you may refer to the students' handbook.

COURSE ASSESSMENT

Course Calendar and Assessment

Students will be graded through the following means of assessment and their final grade will be calculated from the forms of assessment as listed below with their grade weighting taken into account.

Assessment	Grade Weighting	Deadline Assessment
Midterm exam	30%	To be announced
Project	20%	To be announced
Presentations and Assignments	10%	Monthly
Final Exam	40%	To be announced

Description of Exams:

Test questions will predominately come from the material presented in the lectures. Semester exams will be conducted during the regularly scheduled lecture period. Exam will consist of a combination of multiple-choice, short answer, match, true and false and/or descriptive questions.

Homework:
Will be given for each chapter, while the chapter in progress you are supposed to work on them continuously and submit in next lecture when I finish the chapter.
You are also expected to work on in-chapter examples, self-tests and representative number of end of chapter problems. The answers of self-tests and end of chapter exercises are given at the end of the book.

Quizzes: Unannounced quizzes will be given during or/and at the end of each chapter based upon the previous lectures. It will enforce that you come prepared to the class.
No make-up exams, homework, or quizzes will be given. Only documented absences will be considered as per HU guidelines.

Grades are not negotiable and are awarded according to the following criteria*:

Letter Grade	Description	Grade Points
A+	Excellent	4.00
A		3.75
A–		3.50
B+	Very Good	3.25
B		3.00
B–		2.75
C+	Good	2.50
C	Fail	2.25

WEEKLY LECTURE SCHEDULE AND CONTENT DISTRIBUTION

Course Plan

Week no.	Topic	chapters
1	**Introduction:** The Need for Security The Elements of Information Security the Elements of Information Security Motives, Goals, and Objectives of Information Security Attacks Overview of Classification of Attacks Overview of Information Security Attack Vectors Overview of Various Information Security Laws and Regulations	
2	**Ethical Hacking Fundamentals** Understanding the Cyber Kill Chain Methodology Understanding Tactics, Techniques, and Procedures Overview of Indicators of Compromise (IoCs) Overview of Hacking Concepts and Hacker Classes Understanding Different Phases of Hacking Cycle Understanding Ethical Hacking Concepts and Its Scope	
3	**Information Security Threats and Vulnerability Assessment** Understanding the Threat and Threat Sources. Understanding Malware and Components of Malware. Common Techniques Attackers use to Distribute Malware on the Web. Different Types of Malware and Malware Countermeasures.	
4	**Password Cracking Techniques and Countermeasures** Understanding the Password Cracking and Password Complexity Understanding Microsoft Authentication Understanding Various Types of Password Attacks Overview of Password Cracking Tools	

Week no.	Topic	chapters
5	**Social Engineering Techniques and Countermeasures** Understanding Social Engineering Concepts Understanding Various Social Engineering Techniques Understanding Insider Threats	
6	**Network Level Attacks and Countermeasures** Understanding Packet Sniffing and Types of Sniffing Understanding Various Sniffing Techniques and Tools Understanding Different Sniffing Countermeasures	
7	**Web Application Attacks and Countermeasures** Understanding Web Server Concepts and Attacks Understanding Different Web Server Attack Tools and Countermeasures Overview of Web Application Architecture and Vulnerability Stack.	
8	**Wireless Attacks and Countermeasures** Overview of Wireless Encryption Algorithms Understanding Wireless Network-Specific Attack Techniques. Overview of Different Wireless Attack Tools.	
9	**Mobile Attacks and Countermeasures** Understanding Anatomy of a Mobile Attack Understanding Mobile Platform Attack Vectors	
10	**IoT and OT Attacks and Countermeasures** Understanding IoT Concepts Understanding IoT attacks and IoT attack Tools	
11+12	**Cloud Computing Threats and Countermeasures** Understanding Cloud Computing Concepts Overview of Container Technology Understanding Cloud Computing Threats Overview of Cloud Attacks and Tools Understanding Cloud Attack Countermeasures	
13	**Penetration Testing Fundamentals** Understanding Penetration Testing and its Benefits	

Week no.	Topic	chapters
	Understanding Types of Penetration Testing Understanding Phases of Penetration Testing Overview of Penetration Testing Methodologies	
14+15	**Student Presentations**	