MODULE DESCRIPTOR FORM

Module Information			
Module Title	Cryptosecurity Principles	**Module Delivery**	
Module Type	**CORE**	☒ **Lecture** ☒ **Practical**	
Module Code	**IT3202**		
ECTS Credits	**6**		
SWL (hr/sem)	**150**		
Module Level	UGIII	**Semester of Delivery**	2
Administering Department	Information Technology	**College**	College of Sciences
Module Leader	**Ahsan Ahmed Mohammed Lahmood**	**e-mail**	ahssan.ahsan@gmail.com
Module Leader's Acad. Title	Asst. Prof	**Module Leader's Qualification**	Ph.D
Module Tutor	**Ahsan Ahmed Mohammed Lahmood**	**e-mail**	ahssan.ahsan@gmail.com
Peer Reviewer name	Dr. Ali karem	**e-mail**	alialmujab@uowa.edu.iq
Review Committee Approval	2025-2026	**Version Number**	

Relation With Other Modules			
Prerequisite module	-	**Semester**	-
Co-requisites module	-	**Semester**	-

جامعة وارث الانبياء
كلية العلوم
قسم تكنولوجيا المعلومات

Department Head Approval

جامعة وارث الانبياء
عمادة كلية العلوم

Dean of the College Approval

Module Aims, Learning Outcomes and Indicative Contents

Module Aims	1. To establish rules and measure to use against attacks over the internet through understanding the 9 cybersecurity principles. 2. To designed the technologies and processes to protect computers, networks and data from unauthorized access and attacks delivered via the internet by cyber criminals. Though, cyber security is important for the network, data and application security. 3. To prevent Cybercrime to steal a person's identity or illegal imports or malicious programs using computers and the internet. 4. Building a penetration lab to train in discovering vulnerabilities in servers and web applications. The practical aspect of this course is directed to network and information security engineers and students in the field of information technology 5. Using Virtual box to simulate different operating system on one machine system. Also, using the Wireshark program to analysis the data and network traffic to discover the errors on the networks or programs. 6. Finally, use the Kali Linux in a virtual machine or box for the purpose to achieve cybersecurity labs.
Module Learning Outcomes	On successful completion of this course, students should be able to: 1. understanding the 9 cybersecurity principles and understanding problems of cyberspace try to planning for security to increase the effectiveness of management processes through the development implementation and evaluation of a security policy and programs; 2. provide solutions to real-world problems by applying security management models and practices to security programs; 3. demonstrate an understanding of change on organizations in the global environment and the impact of these on organizational systems by developing risk management strategies that incorporate appropriate controls; 4. demonstrate an understanding of the impact of interpersonal communication on specific management processes and outcomes using relevant theories and concepts by understanding the relationships between security and personnel, between security and law, between security and ethics; 5. communicate professionally and effectively in written communication to various audiences to achieve targeted outcomes demonstrating and collating concepts of Cyber Security. 6. implement specialist knowledge and skills to deal with cyber incident and examine sources of cyber security incident use cases, and how these can be applied towards improving organizational response and recovery; 7. examine and then apply specialist knowledge and skills in managing human factors and behavior to counter cyber threats; research and review sources using knowledge relating to cyber security knowledge, and how these can be applied towards improved cyber security controls;
Indicative Contents	**Topics** **Description** **Weighting (65%)** 1. Cybersecurity Perspectives and impact 5.00 5

	2.	Cybersecurity Policy goals and mechanisms	5.00	5
	3.	Security services, mechanisms and countermeasures	10.00	5
	4.	Vulnerabilities, threats and risk	10.00	10
	5.	Personal information	5.00	10
	6.	Social Engineering	5.00	
	7.	Cyberattacks and detection	5.00	15
	8.	Cyberattacks and security tools	10.00	
	9.	Phishing and related attack vectors and exploits	5.00	
	10.	The nine cybersecurity principles	5.00	

Learning and Teaching Strategies	
Strategies	Overview Strategies Cyber security is not just a technology problem, it is also a people problem as people are central to both the risk relating to many cyber threats, and also to mitigating this risk. This course provides insights, strategies and skills in mitigating control weaknesses relating to human behaviour in the organisation that exposes business to cyber security threats. - It is also important to have a good appreciation of importance of people, law and ethics in the management of Cyber Security programs in organisations. - In order to effectively manage and protect the information assets of organisations students need to develop the knowledge and skills required for security planning, development, implementation and evaluation of security policy and programs. - This course provides students with the knowledge, skills and processes to enact an appropriate response and recovery when a cyber-security incident is detected through many lectures. - Give to students' cybersecurity Principles instructions about how planning, detection, response and recovery to current and emerging cyber security threats are explored. - introduces students to how finding and fixing vulnerabilities, encryption, intrusion detection and managing cyber risks. - The application of appropriate work practices that support good cyber security posture in software applications development, systems administration and information system professional areas are reviewed through giving lectures, practical exercises within the laboratories, assignments about some specific topics, and small projects.

Student Workload (SWL)			
Structured SWL (h/sem)	60	**Structured SWL (h/w)**	4
Unstructured SWL (h/sem)	87	**Unstructured SWL (h/w)**	6
Student workload expectations (SWL &USWL) To do well in this subject, students are expected to commit approximately 10 hours per week including class contact hours, independent study, and all assessment tasks. If you are undertaking additional activities, the weekly workload hours may vary.			
Total SWL (h/sem)	147 + 3 final = 150		

Module Evaluation

		Time/Number	Weight (Marks)	Week Due	Relevant Learning Outcome
Formative assessment	**Quizzes**	4	8%(8)	3,6,10,13	
	Assignments	6	12%(12)	3,5,6,8,10,12	
	Project	1	10%(10)	Start from week 4 until week 14	
	Labs	5	10%(10)	7,13	
Summative assessment	**Midterm Exam**	2hr	10% (10)	7	
	Final Exam	3hr	50% (50)	16	
Total assessment			100% (100 Marks)		

Delivery Plan (Weekly Syllabus)		
	Material Covered	**Weighing (30+5=35%)**
Week 1	**Perspectives and impact** - Make sense of the hard problem areas in cybersecurity that continue to make cybersecurity a challenge to implement. - Describe how a significant cybersecurity event has led to increased organizational focus on cybersecurity. - Tell a story of a significant cybersecurity advance.	2
Week 2	**Perspectives and impact…cont'd** - Evaluate when the Confidentiality, Integrity and Availability (CIA) of information has been or could be violated with regards to providing trust of information. - Compare and evaluate different approaches/ implementations of digital currencies.	2
Week 3	**Policy goals and mechanisms** - Recognize when an organization focus is on compliance with standards vs. state of the practice vs. state of the art. - Be aware of multiple definitions for the word "policy" within a cybersecurity context. - Consider vulnerability notification and the issues associated with fixing or not fixing vulnerabilities and disclosing or not disclosing vulnerabilities.	2
Week 4	**Policy goals and mechanisms…cont'd** - Contrast the implications of relying on open design or the secrecy of design for security. Express why cybersecurity is a societal imperative.	2
Week 5	**Security services, mechanisms and countermeasures** - Analyze the tradeoffs of balancing key security properties (Confidentiality, Integrity, and Availability). - Make sense of the concepts of risk, threats, vulnerabilities and attack vectors (including the fact that there is no such thing as perfect security). - Document an example of "countermeasures" for specific threats. - Produce a list capabilities and tools that identify cybersecurity risks on an ongoing basis. - Show the concept of identity management and how it is important.	2

Week 6	**Security services, mechanisms and countermeasures…cont'd** - Make meaning of the concepts of authentication, authorization, and access control. - Argue for the benefit of multi-factor authentication. - Explain the concepts of authentication, authorization, and access control. - Explain the benefit of two-factor authentication, including the use of biometrics. - Define application 'whitelisting'. - Identify the costs and tradeoffs associated with security that a company implements into a product.	2
Week 7	**Mid Term Exam Revision**	2
Week 8	**Vulnerabilities, threats and risk** - Express the differences between vulnerabilities, threats, and risk. - Describe how security mechanisms can contain vulnerabilities. - Use a risk management framework. d. Use penetration-testing tools to identify a vulnerability. - Derive several benefits of defense in depth, e.g., having multiple layers of defenses. - Describe how security issues arise at boundaries between components.	2
Week 9	**Vulnerabilities, threats and risk…cont'd** - Use the National Vulnerability Database to determine if software installed on a server or network component has a known vulnerability. - Recognize vulnerabilities, threats and risks that are distinct to network infrastructure, cloud computing servers, desktop computers, and mobile devices. - Use a buffer-overflow attack against a server that reads an unbounded data into a fixed-size data structure. - Use a cross-site scripting attack against a server that does not properly - sanitize user input prior to displaying the results in a browser.	2
Week 10	**Personal information** - Make sense of the terms Personal Information, Personally Identifiable Information, De-Identification, Anonymization, Pseudonym, Masking, and Unmasking. - Describe how the Fair Information Practices apply to personal information and how online entities collect and use personal information. - Classify several categories of personal information according to privacy and disclosure risk.	2

Week 11	**Personal information…cont'd** - Contrast policies for collecting, processing, storing, sharing, and disposing of personal information. - Illustrate the role and limitations of encryption for protecting personal information. - Make sense of policies and technologies for isolating personal data from enterprise data. - Analyze approaches for controlling access to personal information.	2
Week 12	**Cyberattacks and detection** - Define the roles of prevention, deterrence, and detection mechanisms. - Identify password guessing, port scanning, SQL injection probes, and other cyberattacks in log files. - Discuss the role and limitations of signature-based and behavioral- based anti-virus technology.	2
Week 13	**Cyberattacks and detection…cont'd** - Explain two differences between host-based and network-based intrusion detection systems. - Create three rules for a network-based intrusion detection system that will protect against specific known attacks. - Discuss the use of deception by malware to evade security mechanisms.	2
Week 14	**Cyberattack and Security Tools** - Explain the hacking and phishing concepts - Learn about Denial of Service and Spam Email - Types of security tools and Safety Tips to Cybercrime - Follow the instructions of Cybersecurity Principle	2
Week 15	- Students course workload evaluation.	2
Week 16	**Prepare to the final Exam**	3

Delivery Plan (Weekly Lab. Syllabus)		
	Material Covered	**Weighing 30%**
Week 1 - Lab 1	- Prepare cybersecurity lab environment, - Introduction to the cybersecurity concept - Explain the privacy/copyrights and the difference between security concept. - Install virtual machines and some security tools for penetration lab.	2
Week 2 - Lab 2	**(Confidentiality)** - learn how hackers gather sensitive information from a target such as credit card details or passwords, without them knowing that this information is being captured using Credential harvesting process	2
Week 3 - Lab 3	**(Availability)** - Learn how Denial of Service (Dos) works and Discover the Vulnerability on the injection machines	2
Week 4 – Lab 4	**(Availability…cont'd)** - Install security tools to complete lab 3 - Install some injection machines	2
Week 5 – Lab 5	**(Integrity)** - Install SQL injection machine - Learn how hackers tamper information. - What are the countermeasures?	2
Week 6 – Lab 6	**(Integrity…cont'd)** - Install virtual infection machine Metasploitable2	2
Week 7 – Lab 7	- Labs exam1 with evaluation	2
Week 8 – Lab 8	**(Privilege Elevation or Escalation)** - Learn how to perform privilege escalation. - How hackers exploit SQL injection to privilege escalation attacks. - Install Kali Linux - Prepare Pentastar Lab: From SQL Injection To Shell	2
Week 9 – Lab 9	**(Pre-Broken Access Control)** - Install xampp on kali - Install OWASP Mutillidae II - How hackers can exploit injection machine by broken access information.	2
Week 10 – Lab 10	**(Pre-Broken Access Control with Burp Suite)** - Learn how to use Burp Suite tool to intercept client-side requests. - Burp Suite is an especially useful tool when testing web applications.	2

Week 11 – Lab 11	**(OWASP A5 Broken Access Control)** - Learn how to take advantage of a broken access control vulnerability to log in as another user. - Broken Access control is what happens when restrictions on what authenticated users can do are not properly enforced This vulnerability can be exploited by attackers to access unauthorized functionality and or data such as other users' accounts, modify other users' data, change access rights, view sensitive files etc. **Phishing Pages Attack** - Learn how hackers use original website pages to harm the victim - How to create Phishing Page using Hidden Eye tool - How to Gaining Facebook credentials of the victim	2
Week 12 – Lab 12	**A Man-In-The-Middle Attack** - Sniffing victim's FTP login credentials - Tool: Ettercap and run your kali Linux virtual machine in a bridge mode	2
Week 13 – Lab 13	- Labs exam2 with evaluation	2
Week 14 – Lab 14	**Password Cracking Attack** - Learn how the hackers Make a custom password cracking wordlist using Crunch tool	2
Week 15 – Lab 15	- Cybersecurity project Implementation with discussion for each student	2

Learning and Teaching Resources

	Text	Available in the Library?
Required Texts	1. Whitman, ME & Mattord, HJ 2014, *Hands-on information security lab manual*, 4th edn, Thomson Course Technology, Boston, Massachusetts. 2. Whitman, ME & Mattord, HJ 2018, *Management of information security*, 6th edn, Thomson Course Technology, Boston, Massachusetts. 3. ITE-CSP Cybersecurity Principles: Curriculum Guidelines for Undergraduate Degree Programs in Information Technology	No
Recommended Texts	Whitman, ME & Mattord, HJ 2018, *Management of information security*, 6th edn, Thomson Course Technology, Boston, Massachusetts.	No
Websites	https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-cyber-security https://www.coursehero.com/file/18066467/ip5/ https://www.101labs.net	

APPENDIX:

GRADING SCHEME				
Group	**Grade**	**Mark**	**Marks (%)**	**Definition**
Success Group (50 - 100)	**A -** Excellent	Excellent	90 - 100	Outstanding Performance
	B - Very Good	Very Good	80 - 89	Above average with some errors
	C - Good	Good	70 - 79	Sound work with notable errors
	D - Satisfactory	Fair / Average	60 - 69	Fair but with major shortcomings
	E - Sufficient	Pass / Acceptable	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX –** Fail	Fail (Pending)	(45-49)	More work required but credit awarded
	F – Fail	Fail	(0-44)	Considerable amount of work required
Note:				

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.