Course Specification

(Postgraduate)

Course Title:	**Cyber Threats (CTH)**
Course Code:	CYBSXXXX
Program:	M.Sc. in Cybersecurity
Department:	**Department of Computer Science**
College:	**Faculty of Computing and Information**
Institution:	Al-baha University
Version:	**1**
Last Revision Date:	**15 Des, 2023**

Table of Contents

A. General information about the course:

1. Course Identification:

1. Credit hours: (3)				
2. Course type				
A.	☐University	☐College	☐Department	☐Track
B.	☒ Required		☐Elective	
3. Level/year at which this course is offered: (1/1)				
4. Course general Description:				
This course includes the knowledge and skills of Cyber Threats Analysis and Defense. This knowledge-intensive program encompasses the critical understanding and proficiency in models, methodologies, and processes essential for evaluating, controlling, and mitigating cyber risks.				
5. Pre-requirements for this course (if any)**:**				
6. Pre-requirements for this course (if any)**:**				
7. Course Main Objective(s):				
The students who complete this course will: 1. **Comprehensive Understanding:** Cultivate a thorough grasp of cyber threats, enabling students to navigate adversary behaviors, understand various attack techniques, and comprehend the broader threat landscape. 2. **Analytical Proficiency:** Sharpen analytical skills to categorize adversary resources, capabilities, techniques, and motivations. Students will be equipped to effectively identify and respond to cybersecurity threats. 3. **Diverse Cyber Attack Exploration:** Investigate various cyber attack types, from traditional malware to advanced persistent threats (APTs). Students will compare and contrast the technical aspects of these attacks, gaining insights into their nuances. 4. **Practical Skills Development:** Gain hands-on experience in utilizing cyber threat modeling tools for vulnerability assessment and defense strategy formulation. Students will apply theoretical knowledge to practical scenarios, enhancing their proficiency. 5. **Specialized Challenge Addressing:** Tackle specialized challenges, including denial of service attacks, advanced persistent threats (APTs), MAC spoofing, web application security, and cloud computing security. This prepares students for real-world scenarios, enhancing their readiness to address complex cybersecurity issues.				

2. Teaching Mode: (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	Traditional classroom	26	80%

No	Mode of Instruction	Contact Hours	Percentage
2	E-learning	7	20%
3	Hybrid ☐ Traditional classroom ☐ E-learning		
4	Distance learning		

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

No	Activity	Contact Hours
1.	**Lectures**	33
2.	**Laboratory/Studio**	-
3.	**Field**	-
4.	**Tutorial**	-
5.	**Others (specify)……**	-
	Total	33

B. Course Learning Outcomes (CLOs), Teaching Strategies and Assessment Methods:

Code	Course Learning Outcomes	Code of PLOs aligned with program	Teaching Strategies	Assessment Methods
1.0	**Knowledge and understanding**			
1.1	**Categorize Adversary Resources, Capabilities, Techniques, and Motivations**	**K1**	• Lectures • Assignments	• Assignments • Quizzes • Midterm exams • Final Exam
1.2	**Demonstrating Proficiency in Various Risk Analysis Approaches**	**K2**	• Lectures • Assignments	• Assignments • Quizzes • Midterm exams • Final Exam
2.0	**Skills**			
2.1	**Distinguish and Identify Attack Indication Events**	**S1**	• Lectures • Assignments • Project (Group)	• Assignments • Quizzes • Midterm exams • Final Exam

Code	Course Learning Outcomes	Code of PLOs aligned with program	Teaching Strategies	Assessment Methods
2.2	**Selection of Appropriate Risk Mitigation Approaches, Considering Pros and Cons**	**S2**	• Lectures • Assignments (Group) Project (Group)	• Assignments • Quizzes • Midterm exams Final Exam
3.0	**Values, autonomy, and responsibility**			
3.1	**Work both independently and collaboratively**	**V1**	• Assignments (Group) Project (Group)	• Reports • Presentations • Class Discussions
3.2				

C. Course Content:

No	List of Topics	Contact Hours
1.	Models and Types of Cyber Threats	1.5
2.	Cyber Adversary Model: Resources, Capabilities, Intent, Motivation, Risk Aversion and Access	1.5
3.	Attack Techniques: Backdoors, Trojans, Viruses, Ransomware, Wireless Attacks, Social Engineering and Covert Channels	1.5
4.	Password Guessing and Cracking	1.5
5.	Data Interception, Spoofing, and Session Hijacking	1.5
6.	Data Disclosure, Alteration, and Sabotage Threats	1.5
7.	Repudiation Threats	1.5
8.	Denial of Service Attacks, Distributed Denial of Service Attacks and Bots	1.5
9.	MAC Spoofing, Web Application Attacks, Cloud Computing Attacks and Zero-Day Exploits	3
10.	Advanced Persistent Threats (APT)	3
11.	Attack Indication Events and Attack Timing, Attack Surfaces, Attack Vectors, and Attack Trees	3
12.	Insider Threats	1.5
13.	Threat Information Sources	1.5
14.	Strategies and Tools for Developing Cyber Threat Models	3
15.	Cryptographic Threats	3
16.	Legal Issues of Cyber Threats	3

Total	33

D. Students Assessment Activities:

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1.	Assignments	Every two weeks	5%
2.	Report, presentation, and Class Discussions	Week 10	5%
3.	Midterm Exam	Within the 6th Week	20%
4.	Quizzes	Week 8	10%
5.	Project	Week 11	10%
6.	Final Exam	Week 13	50%

*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	☐ "Hacking: The Art of Exploitation" by Jon Erickson. ☐ "Cybersecurity and Cyberwar: What Everyone Needs to Know" by P.W. Singer and Allan Friedman. ☐ Threat Modeling: Designing for Security" by Adam Shostack.
Supportive References	☐ Publishes research articles on various cybersecurity topics. https://academic.oup.com/cybersecurity ☐ IEEE Transactions on Dependable and Secure Computing. https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=8858
Electronic Materials	☐ Access to the Saudi Digital Library (SDL). ☐ Using the learning management system of the university – Rafid System (https://lms.bu.edu.sa/). ☐ IEEE/ACM Transactions on Networking https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=90
Other Learning Materials	

2. Educational and Research Facilities and Equipment Required:

Items	Resources
facilities (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)	• A classroom or lecture hall with whiteboard for 25 students. A laboratory with 25 computers.
Technology equipment (Projector, smart board, software)	All students shall have • A laptop or access to a desktop computer with access to a programming development tool

Items	Resources
	• High speed Internet connection • Power outlets for student's laptop plug-in Relevant programming software for use of students.
Other equipment (Depending on the nature of the specialty)	• The laboratory should have computers with programming development tools.

F. Assessment of Course Quality:

Assessment Areas/Issues	Assessor	Assessment Methods
Effectiveness of teaching	Students - Program Leaders	Indirect
Effectiveness of students assessment	Program Leaders	Indirect
Quality of learning resources	Students	Indirect
The extent to which CLOs have been achieved	Peer reviewers	Direct
Reviewing course effectiveness and planning for improvement.	Program Leaders - Faculty	Direct

Assessor (Students, Faculty, Program Leaders, Peer Reviewer, Others (specify)

Assessment Methods (Direct, Indirect)

G. Specification Approval Data:

COUNCIL /COMMITTEE	
REFERENCE NO.	
DATE	