2023
TP-153

Course Specification

Master of Science in Cybersecurity

Course Title:	Network Forensics
Course Code:	CYBS60306
Program:	M.Sc. in Cybersecurity
Department:	Computer Science
College:	Computing and Information
Institution:	AlBaha University
Version:	2023
Last Revision Date:	16 December 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	☐Others
B.	☐Required		☒ Elective		

3. Level/year at which this course is offered: (4/2)

4. Course general Description:

This course helps students gain a valuable skill set in computer and networking. The course enables students to understand the importance of forensics in a digital age. Students will explore techniques used by hackers to compromise network resources, how to detect the activity and gather evidence for the incident. Students will also explore digital forensics concepts, procedures, and the extraction of evidence from hard drives and other digital media. The course also provides a project on the use of open source and commercial based tools with industry best practices to emulate real world hacking and forensics scenarios and equip the student to competently enter the world of network forensics.

5. Pre-requirements for this course (if any):

None

6. Pre-requirements for this course (if any):

None

7. Course Main Objective(s):

Upon successful completion of the course, the student will be able:

- □ **Demonstrate network forensic methodologies.**
- □ **Describe the importance and benefits of network forensics.**
- □ **Describe ethical guidelines and industry best practices for performing network forensics.**
- □ **Describe how network forensics protocols and procedures.**
- □ **Analyze network traffic.**
- □ **Demonstrate familiarity with both open source and commercial based tools used to perform network forensics.**
- □ **Detect malicious and anomalous activities and their effects.**
- □ **Demonstrate the knowledge to perform network forensics.**
- □ **Identify evidence found in network and system breaches.**
- □ **Show the knowledge to prepare a forensics report for senior management.**

2. Teaching mode (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	Traditional classroom	26	80%
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 CLOs aligned with program	Teaching Strategies	Assessment Methods
1.0	Knowledge and understanding			
1.1	Describe the importance and benefits of network forensics, ethical guidelines and industry best practices for performing network forensics.	K.2	□ Lectures □ Assignments Group Discussions	□ Home work □ Presentations □ Midterm exam □ Quiz Final Exam
1.2	Identify evidence found in network and system breaches.	K.3	□ Lectures □ Assignments □ Group Discussions	□ Home work □ Presentations □Midterm exam □ Quiz Final Exam

Code	Course Learning Outcomes	Code of CLOs aligned with program	Teaching Strategies	Assessment Methods
2.0	**Skills**			
2.1	Demonstrate network forensic methodologies.	S.1	□ Lectures Assignments	□ Midterm exam □ Quiz Final Exam
2.2	Analyze network traffic.	S.2	□ Lectures Assignments	□ Midterm exam □ Quiz Final Exam
2.3	Detect malicious and anomalous activities and their effects.	S.3	□ Lectures Assignments	□ Midterm exam □ Quiz Final Exam
3.0	**Values, autonomy, and responsibility**			
3.1	Show the knowledge to prepare a forensics report for senior management.	C.3	□ Project (Group) □ Presentations Group Discussions	□ Report Presentations

C. Course Content

No	List of Topics	Contact Hours
1.	**Introduction to Network Forensics:**	**3**
2.	**Network Principles and Layer 2 Protocol**	**3**
3	**Packet Capture and Analysis**	**3**
4	**Intrusion Detection and Prevention**	**3**
5	**Interlacing of Device and Network Forensics**	**3**
6	**Log-File Analysis**	**3**
7	**Network Tunneling**	**3**
8	**Mobile Device Forensics**	**3**
9	**Network Forensics Investigative Theory**	**3**
10	**Network Incident Handling**	**3**
11	**Web Proxies and Encryption**	**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 5th Week	20%
4	Quizzes	Week 8	10%
5	Project	Week 9	10%
6	Final Exam	Week 12	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	1. Davidoff at el, Network forensics: tracking hackers through cyberspace2012, Prentice hall). ISBN: 0132564718.
Supportive References	Introduction to Security and Network Forensics, William J. Buchanan, 2011, Auerbach Publications. ISBN-13: 978-0849335686, ISBN-10: 084933568X.
Electronic Materials	- ACM (Association for Computer Machinery) web site - http://www.acm.org/ - IEEE Computer Society web site - http://www.computer.org/portal/web/guest/home - Access to the Saudi Digital Library (SDL). - Using the learning management system of the university – Rafid System (https://lms.bu.edu.sa/).
Other Learning Materials	None -

2. Required Facilities and equipment

Items	Resources
facilities (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)	□ A classroom or lecture hall with whiteboard for 25 students.
Technology equipment (projector, smart board, software)	□ A digital image projection system with connection to desktop computer and laptop computer. High speed Internet connection.

Items	Resources
Other equipment (depending on the nature of the specialty)	□ A classroom or lecture hall with whiteboard for 25 students.

F. Assessment of Course Quality

Assessment Areas/Issues	Assessor	Assessment Methods
Effectiveness of teaching	Students - Program Leaders	Indirect
Effectiveness of Students assessment	Peer reviewers	Direct
Quality of learning resources	Students	Indirect
The extent to which CLOs have been achieved	Program Leaders - Faculty	Direct
Other		

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

Assessment Methods (Direct, Indirect)

G. Specification Approval

COUNCIL /COMMITTEE	
REFERENCE NO.	
DATE	**16-12-2023**