Jordan University of Science and Technology

Faculty of Computer & Information Technology

Network Engineering And Security Department

NES752 Intrusion Analysis And Incident Management - JNQF Level: 9
Second Semester 2023-2024

Course Catalog
3 Credit Hours. This course focuses on Intrusion Detection, Intrusion Prevention, and Incident Handling. Topics include an analysis of the principles and practices of intrusion detection, intrusion prevention, and incident handling, identifying attack patterns; deployment of resources and responses to handle the incident, surveillance, damage assessment, risk assessment, datamining, attack tracing, system recovery, and continuity of operation.
Teaching Method: On Campus

Text Book	
Title	Practical intrusion analysis: prevention and detection for the twenty-first century
Author(s)	Ryan Trost
Edition	1st Edition
Short Name	Ref #1
Other Information	

Course References

Short name	Book name	Author(s)	Edition	Other Information
Ref #2	Corporate Computer Security	Randall Boyle , Raymond Panko	4th Edition	
Ref # 3	Research papers covering Intrusion Detection and Incident Response	research scientists	1st Edition	

Instructor	
Name	**Prof. Basheer Al-Duwairi**
Office Location	C5L2

Office Hours	Sun : 12:00 - 13:30 Mon : 11:30 - 13:00 Tue : 11:00 - 13:00 Wed : 09:00 - 10:00
Email	basheer@just.edu.jo

Class Schedule & Room
Section 1: Lecture Time: Wed : 11:30 - 14:30 Room: NES01-E1L3

Tentative List of Topics Covered		
Weeks	**Topic**	**References**
Week 1	Threat Landscape and Cybersecurity Challenges	From **Ref #1**
Week 2	Infrastructure Monitoring	From **Ref #1**
Week 3	Network traffic analysis using Wireshark	From **Ref # 3**
Weeks 4, 5	Intrusion Detection Systems	From **Ref #1**, From **Ref # 3**
Weeks 6, 7, 8	Network Traffic Analysis using Zeek/Bro	From **Ref #1**
Week 9	Life Cycle of a Vulnerability	From **Ref #1**
Week 10	Network Flows and Anomaly Detection	From **Ref #1**
Weeks 11, 12	Incident Response fundamentals	From **Ref #2**, From **Ref # 3**
Week 13	Security Operations Center	From **Ref #2**, From **Ref # 3**
Week 14	Contemporary issues in intrusion analysis and incident response	From **Ref # 3**
Week 15	Project presentations	

Mapping of Course Outcomes to Program Outcomes and NQF Outcomes	Course Outcome Weight (Out of 100%)	Assessment method
Understand the fundamental principles and methodologies of intrusion detection, intrusion prevention to effectively recognize and protect networks from cyberattacks. [1MSO5] [1L9S1]	25%	
Demonstrate proficiency in analyzing network traffic utilizing tools such as Wireshark and Zeek/Bro, to effectively detect and identify suspicious activity within network environments. [1MSO5] [1L9S1]	25%	
Understand the fundamental principles and methodologies of incident handling to effectively respond to various attack patterns and security threats. [1MSO5] [1L9S1]	25%	

Gain a comprehensive understanding of contemporary issues in intrusion analysis and incident response, encompassing the latest developments and challenges in the field [1MSO5] [1L9S1]	25%	

Relationship to Program Student Outcomes (Out of 100%)													
SO1	SO2	SO3	SO4	SO5	SO6	SO7	MSO1	MSO2	MSO3	MSO4	MSO5	MSO6	MSO7
											100		

Relationship to NQF Outcomes (Out of 100%)
L9S1
100

Evaluation	
Assessment Tool	**Weight**
Labs/Assignments	25%
Paper presentation	10%
Midterm	15%
Final Exam + Project	50%

Policy	
Exams	1. May include: Definitions, True/False, Multiple-Choice, Analysis and Descriptive formats. 2. Use only your own tools: calculator, pens and ruler 3. Instructions on the first page of the exam are quite important. 4. Not abiding by the rules is a reason for dismissal from the exam.
Makeup	Makeup exam should not be given unless there is a valid excuse.
Drop Date	Last day to drop the course is before the 12th week of the current semester.
Cheating	Standard JUST policy will be applied.
Course workload	Average work-load student should expect to spend is 6 hours/week.
Exam papers	Graded exam papers will be returned within a week.

Date Printed: 2024-03-15