Jordan University of Science and Technology

Faculty of Computer & Information Technology

Network Engineering And Security Department

NES554 Computer Network Defence - JNQF Level: 7

Second Semester 2023-2024

Course Catalog
3 Credit Hours. This course provides a comprehensive overview of cybersecurity principles and practices essential for protecting organizational assets from evolving cyber threats. The course addresses various aspects of cybersecurity, including understanding the threat environment, developing effective planning and policy frameworks, implementing secure networks, network defense technologies, and responding to incidents and disasters. Hands-on exercises enable students to learn how to protect network/systems by using the tools and methods used by hackers to break into networks/systems.
Teaching Method: On Campus

Text Book	
Title	Corporate Computer Security, 5th edition
Author(s)	Randall J Boyle and Raymond R. Panko
Edition	5th Edition
Short Name	Ref#1
Other Information	

Course References

Short name	Book name	Author(s)	Edition	Other Information
Ref#2	Class handouts/ Research papers	----	1st Edition	

Instructor	
Name	**Prof. Basheer Al-Duwairi**
Office Location	C5L2
Office Hours	
Email	basheer@just.edu.jo

Class Schedule & Room
Section 1: Lecture Time: Mon, Wed : 10:00 - 11:30 Room: NES02-E1L3

Tentative List of Topics Covered		
Weeks	**Topic**	**References**
Week 1	The Threat Environment	From **Ref#1**
Weeks 2, 3	Planning and Policy	From **Ref#1**
Weeks 4, 5	Secure Networks	From **Ref#1**, From **Ref#2**
Week 6	Botnets	From **Ref#2**
Week 7	Firewalls	From **Ref#1**
Week 8	Intrusion Detection	From **Ref#1**, From **Ref#2**
Week 9	Host Hardening	From **Ref#1**
Week 10	Data Protection	From **Ref#1**
Weeks 11, 12	Incident and Disaster Response	From **Ref#1**
Weeks 13, 14	Contemporary Issues in Network Security	From **Ref#2**
Week 15	Review	

Mapping of Course Outcomes to Program Outcomes and NQF Outcomes	Course Outcome Weight (Out of 100%)	Assessment method
Use engineering judgment to draw conclusions about network security threats and current attack vectors [1SO6] [1L7S2]	15%	
Implement common cyber security attacks and conduct experiments to analyze and interpret their traffic traces. [1SO6] [1L7S1]	30%	
Demonstrate competency in using various hacking techniques. [1SO6] [1L7S1]	20%	
Implement different network defense technologies, analyze network traffic and interpret attack incidents [1SO6] [1L7S1]	25%	
Recognize ethical and professional responsibilities in cyber security taking into consideration the impact of engineering solutions in global, economic, environmental, and societal contexts [1SO4] [1L7S2]	10%	

Relationship to Program Student Outcomes (Out of 100%)						
SO1	SO2	SO3	SO4	SO5	SO6	SO7
			10		90	

Relationship to NQF Outcomes (Out of 100%)	
L7S1	L7S2
75	25

Evaluation	
Assessment Tool	**Weight**
Midterm Exam	30%
Second Exam (Labs + Quizzes)	30%
Final Exam	40%

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.
Makeups	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.
Workload	Average work-load student should expect to spend is 6 hours/week.
Graded Exams	Graded exam papers will be returned within a week.
Participation	1. Participation in the class will positively affect your performance.

Date Printed: 2024-02-25