Capital University of Science and Technology

Department of Computer Science

CS3713 - Introduction to Information Security and Forensics

Course Title:	Introduction to Information Security and Forensics (CS3713)
Pre-requisite(s):	None
Credit Hours:	3
Instructor(s):	
Text Book(s):	Principles of Information Security and Forensics, Michael Whiteman, 6th Edition
Reference Book(s):	• Security+ Guide to Network Security Fundamentals, Mark Ciampa, 6th Edition, CENGAGE Learning • Guide to Computer Forensics and Investigations: Processing Digital Evidence, Bill Nelson, 6th Edition, CENGAGE Learning
Web Reference:	• www.kali.org

Course Introduction:

With the ever-increasing dependence of organizations on information technology for managing their day-to-day businesses, the importance of information security has multiplied manifold. Information security is concerned with keeping the information and information systems of an organization safe from any threat that can adversely impact their business objectives. Information security has, therefore, become an important subject in academia, research, and development fields. Be it the managers, IT professionals or end users, the basic understanding of information security concepts is a key requirement for everyone concerned directly or indirectly with information systems. Inclusion of this course in undergraduate curriculum for Computer Science/Software Engineering degree is aimed at serving this very purpose.

Course Objectives:

This course will be providing abstract level knowledge of all the domains linked with Information Security and its relation with IT security. The course will start from basics and will end up by Risk

management and audit techniques as being used in Industry. Also, this course will be linking with digital forensics techniques which will be covered throughout with every topic discussed. The course will be having one project in which students will be using tools to work on different domains i.e., Firewalls configuration, IDS, Risk Management, Caine OS, OS Forensics, FTK etc.

Course Learning Outcomes (CLOs):

At the end of this course, the students should be able to:

CLO1: Define the fundamental concepts of information security and digital forensics (C1-Remember)

CLO2: Explain and understand concepts of information security, security threats and the role of digital forensics in incident response and investigatory process (C2-Understand)

CLO3: Select and Use security tools for data and information system protection, evidence collection and evidentiary (C3-Apply)

CLO4: Analyze and illustrate information system protection, digital evidence collection, handling, and storage approaches in common scenarios (C4-Analyze)

CLOs – PLOs Mapping:

	CLO:1	**CLO:2**	**CLO:3**	**CLO:4**
PLO:1 (Academic Education)				
PLO:2 (Knowledge for Solving Computing Problems)	√	√		
PLO:3 (Problem Analysis)				√
PLO:4 (Design/ Development of Solutions)				
PLO:5 (Modern Tool Usage)			√	

Course Contents:

Week	Contents
1	Introduction about the course and the agenda, Introduction about Information Security. Need of security in IT systems. Introduction to basic terminologies, Security Principles, security goals
2	Black hat and white hat hacking procedures and techniques Vulnerability Assessment, Malware, its types, and attacks
3	Introduction to virus total, introduction to cryptography (symmetric and asymmetric) and its use for security (https, ssl), secure coding practices, introduction to owasp, octave, coso, itil)
4	Introduction to virtualization, setting up kali linux, hands-on practice on kali linux and concept of network attack and vulnerability assessment using nessus, nmap
5	Introduction to risk management, definition, and importance of asset, five steps of risk management • identify the risk • analyze the risk • evaluate or rank the risk • treat the risk • monitor and review the risk, risk management steps: risk assessment, risk analysis, risk mitigation
6	How does risk management work? Risk mitigation techniques, risk management process, risk analysis method (qualitative + quantitative)
7	Business continuity and disaster recovery, incident handling (case scenario), risk transfer + revision
8	Risk mitigation & techniques, security controls
Mid-Term Exam	
9	Intrusion detection and prevention system, snort
10	Introduction to firewall, generation of firewalls

11	Introduction to digital forensics, digital forensic investigation process
12	Hands-on practice on digital forensic tools, discussion on overall course contents
13	Server configuration, access controls, introduction to domains, importance of logs, extracting evidence from server
14	Isms, iso-27001
15	Offensive security
16	Project demos course revision

Grading Policy:

S.No	Grading	% of Total Marks
1	Assignments	15
2	Quizzes	15
3	Project	10
4	Mid-term Exam	20
5	Final Exam	40
	Total	**100**