CSE3501	Information Security Analysis and Audit	L	T	P	J	C
		2	0	2	4	4
Pre-requisite	NIL	Syllabus version				
		1.0				

Objective of the course

1. To introduce system security related incidents and insight on potential defenses, counter measures against common threat/vulnerabilities.
2. To provide the knowledge of installation, configuration and troubleshooting of information security devices.
3. To make students familiarize on the tools and common processes in information security audits and analysis of compromised systems.

Expected Outcome

After successfully completing the course the student should be able to

1. Contribute to managing information security
2. Co-ordinate responses to information security incidents
3. Contribute to information security audits
4. Support teams to prepare for and undergo information security audits
5. Maintain a healthy, safe and secure working environment
6. Provide data/information in standard formats
7. Develop knowledge, skills and competence in information security

Student Learning Outcomes (SLO)	1,2,17

1. Having an ability to apply mathematics and science in engineering applications
2. Having a clear understanding of the subject related concepts and of contemporary issues
17. Having an ability to use techniques, skills and modern engineering tools necessary for engineering practice

1	**Information Security Fundamentals**	7 hours

Definitions & challenges of security, Attacks & services, Security policies, Security Controls, Access control structures, Cryptography, Deception, Ethical Hacking, Firewalls, Identify and Access Management (IdAM).

2	**System Security**	6 hours

System Vulnerabilities, Network Security Systems, System Security, System Security Tools, Web Security, Application Security, Intrusion Detection Systems,
.

3	**Information Security Management**	3 hours

Monitor systems and apply controls, security assessment using automated tools, backups of security devices, Performance Analysis, Root cause analysis and Resolution, Information Security Policies, Procedures, Standards and Guidelines

4	**Incident Management**	5 hours

Security requirements, Risk Management, Risk Assessment, Security incident management, third party security management, Incident Components, Roles.

5	**Incident Response**	4 hours

Incident Response Lifecycle, Record, classify and prioritize information security incidents using standard templates and tools, Responses to information security incidents, Vulnerability Assessment, Incident Analysis

6	**Conducting Security Audits**	3 hours
Common issues in audit tasks and how to deal with these, Different systems and structures that may need information security audits and how they operate, including: servers and storage devices, infrastructure and networks , application hosting and content management, communication routes such as messaging, Features, configuration and specifications of information security systems and devices and associated processes and architecture, Common audit techniques, Record and report audit tasks, Methods and techniques for testing compliance.		
7	**Information Security Audit Preparation**	2 hours
Establish the nature and scope of information security audits, Roles and responsibilities, Identify the procedures/guidelines/checklists, Identify the requirements of information security, audits and prepare for audits in advance, Liaise with appropriate people to gather data/information required for information security audits.		
8	**Self and Work Management**	2 hours
Establish and agree work requirements with appropriate people, Keep the immediate work area clean and tidy, utilize time effectively, Use resources correctly and efficiently, Treat confidential information correctly, Work in line with organization's policies and procedures, Work within the limits of their job role.		
	Total Lecture hours:	**30 hours**

Text Book(s)

1. William Stallings, Lawrie Brown, Computer Security: Principles and Practice, 3rd edition, 2014.
2. Nina Godbole, Information Systems Security: Security Management, Metrics, Frameworks and Best Practices, Wiley, 2017
3. Nina Godbole, Sunit Belapure, Cyber Security- Understanding cyber-crimes, computer forensics and legal perspectives, Wiley Publications, 2016
4. Andrew Vladimirov Michajlowski, Konstantin, Andrew A. Vladimirov, Konstantin V. Gavrilenko, Assessing Information Security: Strategies, Tactics, Logic and Framework, IT Governance Ltd, O'Reilly, 2010

Reference Books

1. Charles P. Pfleeger, Security in Computing, 4th Edition, Pearson, 2009.
2. Christopher J. Alberts, Audrey J. Dorofee , Managing Information Security Risks, Addison-Wesley Professional, 2004
3. Peter Zor, The Art of Computer Virus Research and Defense, Pearson Education Ltd, 2005
4. Lee Allen, Kevin Cardwell, Advanced Penetration Testing for Highly-Secured Environments - Second Edition, PACKT Publishers, 2016
5. Chuck Easttom , System Forensics Investigation and Response, Second Edition, Jones & Bartlett Learning, 2014
6. David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni, Metasploit The
7 Penetration Tester's Guide, No Starch Press, 2014
8. Practical Malware Analysis by Michael Sikorski and Andrew Honig, No Starch Press, 2015
9. Ref Links:
   https://www.iso.org/isoiec-27001-information-security.html
   https://csrc.nist.gov/publications/detail/sp/800-55/rev-1/final
   https://www.sans.org/reading-room/whitepapers/threats/paper/34180
   https://www.sscnasscom.com/qualification-pack/SSC/Q0901/

List of Experiments (Indicative)		SLO: 1,2,17
	• Install and configure information security devices • Security assessment of information security systems using automated tools. • Vulnerability Identification and Prioritization • Working with Exploits • Password Cracking • Web Application Security Configuration • Patch Management • Bypassing Antivirus Software • Static Malware Analysis • Dynamic Malware Analysis • Penetration Testing • MySQL SQL Injection • Risk Assessment • Information security incident Management • Exhibit Security Analyst Role	
	Total Laboratory Hours	**30 hours**

Recommended by Board of Studies	05.02.2020		
Approved by Academic Council	58	Date	26.02.2020