COURSE CONTENT

INTRUSION DETECTION SYSTEMS								
III Semester: CSE								
Course Code	**Category**	**Hours / Week**			**Credits**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CIA**	**SEE**	**Total**
25X5825	**Foundation**	3	0	0	3	40	60	100
Contact Classes: 45	**Tutorial Classes: Nil**	**Practical Classes: Nil**				**Total Classes: 45**		
Prerequisites: Computer Networks, Computer Programming								

Course Overview:

The Digital Forensics course provides students with the knowledge and practical skills required to investigate digital crimes, collect and preserve digital evidence, analyze computer systems and network traffic, and support legal proceedings. The emphasis is on understanding forensic methodologies, legal and ethical considerations, and using forensic tools to extract and interpret evidence from digital devices and environments.

Course Objectives:

1. To understand the fundamentals of intrusion detection and prevention systems.
2. To study network, host-based, and anomaly-based IDS techniques and architectures.
3. To analyze various cyber attacks, malware, and security threats in computer networks.
4. To evaluate IDS tools, signature-based methods, and anomaly detection algorithms.
5. To develop effective security solutions for threat detection, alert correlation, and cyber defense.

Course Outcomes: After Completion of the Course, Students should be able to

1. Apply fundamental security concepts including firewalls, VPNs, and vulnerability assessment to mitigate threats against computers and networked systems.
2. Demonstrate classes of attacks across network, application, and human layers, and relate them to corresponding attacker profiles and automated threats.
3. Analyze intrusion detection models using signature-based solutions and assess cost-sensitive in IDS performance.
4. Examine anomaly detection algorithms based on software vulnerabilities and payload analysis.
5. Evaluate malware detection strategies, alert correlation, insider threats, and evolving techniques to recommend future collaborative security approaches.

UNIT – I

The state of threats against computers, and networked systems-Overview of computer security solutions and why they fail-Vulnerability assessment, firewalls, VPN's -Overview of Intrusion Detection and Intrusion Prevention, Network and Host-based IDS

UNIT - II

Classes of attacks - Network layer: scans, denial of service, penetration Application layer: software exploits, code injection-Human layer: identity theft, root access-Classes of attackers-Kids/hackers/sop Hesitated Groups-Automated: Drones, Worms, Viruses

UNIT - III

A General IDS model and taxonomy, Signature-based Solutions, Snort, Snort rules, Evaluation of IDS, Cost sensitive IDS

UNIT - IV

Anomaly Detection Systems and Algorithms-Network Behavior Based Anomaly Detectors (rate based) Host-based Anomaly Detectors-Software Vulnerabilities-State transition, Immunology, Payload Anomaly Detection

UNIT - V

Attack trees and Correlation of alerts- Autopsy of Worms and Botnets-Malware detection - Obfuscation, polymorphism- Document vectors. Email/IM security issues-Viruses/Spam-From signatures to thumbprints to zero day detection-Insider Threat issues-Taxonomy-Masquerade and Impersonation Traitors, Decoys and Deception-Future: Collaborative Security

TEXT BOOKS:

1. Peter Szor, The Art of Computer Virus Research and Defense, Symantec Press ISBN 0-321-30545
2. Markus Jakobsson and Zulfikar Ramzan, Crimeware, Understanding New Attacks and Defenses.

REFERENCE BOOKS:

1. Saiful Hasan, Intrusion Detection System, Kindle Edition.
2. Ankit Fadia, Intrusion Alert: An Ethical Hacking Guide to Intrusion Detection.

ELECTRONIC RESOURCES:

1. https://www.intechopen.com/books/intrusion-detection systems/ Online Courses:
2. https://www.sans.org/course/intrusion-detection-in-depth
3. https://www.cybrary.it/skill-certification-course/ids-ips-certification-training-course

MATERIALS ONLINE:

1. Course template
2. Tutorial question bank
3. Tech talk and Concept Video topics
4. Open-ended experiments
5. Definitions and terminology
6. Assignments
7. Model question paper – I
8. Model question paper – II
9. Lecture notes
10. E-Learning Readiness Videos (ELRV)