



MARRI LAXMAN REDDY INSTITUTE OF TECHNOLOGY AND MANAGEMENT

(AN AUTONOMOUS INSTITUTION)

(Approved by AICTE, New Delhi & Affiliated to JNTUH, Hyderabad)

Accredited by NAAC with 'A' Grade & Recognized Under Section 2(f) & 12(B) of the UGC act, 1956

COURSE CONTENT

INTRUSION DETECTION SYSTEMS								
III Semester: CSE								
Course Code	Category	Hours / Week			Credits	Maximum Marks		
		L	T	P		C	CIA	SEE
2235830	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:

This course provides an overview of computer and network security, covering common threats, vulnerabilities, and why security solutions like firewalls, VPNs, and intrusion detection systems sometimes fail. It explores different types of cyberattacks across network, application, and human layers, along with attacker classifications and automated threats.

Course Objectives:

1. To understand the fundamental concepts, architecture, and importance of Intrusion Detection Systems (IDS) in network and information security.
2. To study different types of attacks, vulnerabilities, and intrusion detection techniques used in secure computing environments.
3. To learn signature-based, anomaly-based, and hybrid intrusion detection approaches for identifying malicious activities.
4. To analyze network traffic, system logs, and security events using intrusion detection tools and methodologies.
5. To develop the ability to design, implement, and evaluate intrusion detection mechanisms for protecting computer networks and systems.

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

1. Possess a fundamental knowledge of Cyber Security.
2. Understand what vulnerability is and how to address most common vulnerabilities.
3. Know basic and fundamental risk management principles as it relates to Cyber Security and Mobile Computing.
4. Have the knowledge needed to practice safer computing and safeguard your information using Digital Forensics.
5. Understand basic technical controls in use today, such as firewalls and Intrusion Detection systems.

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- 30545-3.
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/>
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)