Course Code: CSE3145	**Course Title: Intrusion Detection & Prevention System** **Type of Course: Theory Only Course**	**L-T- P-C**	3	0	0	3
Version No.	1					
Course Pre-requisites	Fundamental knowledge of the subject Network Security, TCP/IP, Network programming skills.					
Anti-requisites	NIL					
Course Description	Objective of this course is to understand when, where, how, and why to apply Intrusion Detection tools and techniques in order to improve the security posture of an enterprise. Apply knowledge of the fundamentals and history of Intrusion Detection in order to avoid common pitfalls in the creation and evaluation of new Intrusion Detection Systems and Analyze intrusion detection alerts and logs to distinguish attack types from false alarms.					
Course Objective	The objective of the course is to familiarize the learners with the concepts of **INTRUSION DETECTION AND PREVENTION SYSTEM** and attain **Skill Development** using **PARTICIPATIVE LEARNING** techniques.					
Course Out Comes	**On successful completion of the course the students shall be able to:** **CO1:** Identify the various attacks in the networks **[Understand]** **CO2:** Discuss intrusion detection and prevention policies **[Understand]** **CO3:** Apply the various tools for Intrusion Detection system. **[Apply]** **CO4:** Explain the procedures to do legal proceedings against intruders. **[Understand]**					

Course Content:

Module 1	**Introduction to IDPS**	Quiz	Assignment	**10 Sessions**

Topics:
Understanding Intrusion Detection – Intrusion detection and prevention basics – IDS and IPS analysis schemes, Attacks, Detection approaches –Misuse detection – Anomaly detection – specification based detection, hybrid detection. Internal and external threats to data, attacks, Need and types of IDS, Information sources, Host based information sources, Network based information sources.

.

Module 2	**Intrusion Response**	Quiz	Assignment	**10 Sessions**

Topics:
Intrusion Prevention Systems, Network IDs protocol based IDs, Hybrid IDs, Analysis schemes, thinking about intrusion. A model for intrusion analysis, techniques Responses requirement of responses, Types of responses mapping responses to policy Vulnerability analysis, credential analysis non credential analysis. Architecture models of IDs and IPs.

Module 3	**Implementation and**	Quiz	Assignment	**15 Sessions**

	Deployment			

Topics:
Tool Selection and Acquisition Process – Bro Intrusion Detection – Prelude Intrusion Detection – Cisco Security IDS – Snorts Intrusion Detection – NFR security. Introduction to Snort, Snort Installation Scenarios, Installing Snort, Running Snort on Multiple Network Interfaces, Snort Command Line Options. Step-By-Step Procedure to Compile and Install Snort Location of Snort Files, Snort Modes Snort Alert Modes.

Module 4	**Introduction to Snort**	Quiz	Assignment	**10 Sessions**

Topics:
Law Enforcement / Criminal Prosecutions – Standard of Due Care – Evidentiary Issues, Organizations and Standardizations.

Targeted Application & Tools that can be used:
NIL

Project work/Assignment:

Assignment:
Students should do case studies on the recent commercial and open source IDSs such as BRO IDPS, Prelude IDPS, SNORT IDS and other commercial IDS.

Text Book

T1. Radha B., Sakthivel Duraisamy and Arunraj Gopalsamy "Intrusion Detection and Prevention Concepts and Techniques: A Simple Guide to Beginners", Lambert Academic Publishing, 2021.
T2. Carl Endorf, Eugene Schultz and Jim Mellander " Intrusion Detection & Prevention", 1st Edition, Tata McGraw-Hill, 2004.
T3. Earl Carter, Jonathan Hogue, "Intrusion Prevention Fundamentals", Pearson Education, 2006.

References

R1. Rafeeq Rehman : " Intrusion Detection with SNORT, Apache, MySQL, PHP and ACID," 1st Edition, Prentice Hall, 2003.
R2. Christopher Kruegel, Fredrik Valeur, Giovanni Vigna, "Intrusion Detection and Correlation Challenges and Solutions", 1st Edition, Springer, 2005.
R3. Paul E. Proctor, "The Practical Intrusion Detection Handbook ", Prentice Hall , 2001.

Web resources:

W1. https://flylib.com/books/en/2.352.1/data_correlation.html

W2. Incident Response | Part IV - Security and IDS Management (flylib.com)

W3. Policy and Procedures | Part IV - Security and IDS Management (flylib.com)

W4. Laws, Standards, and Organizations | Part IV - Security and IDS Management (flylib.com)

W5. Security Business Issues | Part IV - Security and IDS Management (flylib.com)

W6. The Future of Intrusion Detection and Prevention | Part IV - Security and IDS Management (flylib.com)

Catalogue prepared by	Ms. Monisha Gupta

Recommended by the Board of Studies on	
Date of Approval by the Academic Council	