राष्ट्रीय प्रौद्योगिकी संस्थान पटना / NATIONAL INSTITUE OF TECHNOLOGY PATNA
संगणक विज्ञान एंव अभियांत्रिकी विभाग / DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
अशोक राजपथ, पटना-८००००५, बिहार / ASHOK RAJPATH, PATNA-800005, BIHAR
Phone No.: 0612-2372715, 2370419, 2370843, 2371929 Ext- 200, 202 Fax-0612-2670631 Website: www.nitp.ac.in

No:- **Date:**

CSX4185 Intrusion Detection

L-T-P-Cr: 2-0-2-3

Pre-requisites: Brief knowledge of the subject Network Security, TCP/IP, Network programming skills.

Objectives/Overview:

- To build further on the grounding of principles in the earlier security courses.
- To apply those principles to currently popular technologies such as firewalls and intrusion detection systems, widely sold as commercial solutions.
- To evaluate performance of any security solutions using several metrics.
- Students will construct and adapt firewalls and intrusion detectors and analyze their architectures through this course.
- Students will be aware of architecture and implementation of several available IDS in market.

Course Outcomes:

At the end of the course, a student should:

Sl. No	Outcome	Mapping to PO
1.	Analyze several security threats and the significance of security needs.	PO4, PO5
2.	Describe various foundations on which detection approaches can be built.	PO2, PO3
3.	Explain several types of IDS and IPS, their use and implementation, and also how to evaluate their performance.	PO4, PO5
4.	Detail implementation of Snort and its working principle.	PO3, PO4, PO5

UNIT I **Lectures: 9**

Network Attacks, Understanding Intrusion Detection and Intrusion Prevention System, Detection Approaches (Misuse Detection, Anomaly Detection, etc.), Uses of IDPS Technologies, Key Functions of IDPS Technologies, Stateful Protocol Analysis.

UNIT II **Lectures: 10**

Data Collection (Host-Based, Network-Based, Application-Based, Application-Integrated and Hybrid), Theoretical Foundations of Detection - Taxonomy of anomaly detection system, fuzzy

logic, Bayes theory, Artificial Neural networks, Support vector machine, Evolutionary computation, Association rules, Clustering, Architecture and Implementation.

UNIT III **Lectures: 8**

IDS Challenges, Alert Management & Correlation (Data Fusion, Alert Correlation, Cooperative Intrusion Detection), Evaluation Criteria- Accuracy, Performance, Completeness, Timely Response, Adaptation and Cost-Sensitivity, Intrusion Tolerance and Attack Resistance, Test. Intrusion Response.

UNIT IV **Lectures: 6**

Security and IDS Management (Data Correlation, Incident Response, Policy and Procedures, Law, Standards and organizations, Security Business issues, Future of Intrusion Detection and Prevention).

UNIT V **Lectures: 5**

Implementation and Deployment: Internet Security System's Real Source, Snort, NFR Security, IDS Tools. Detail case study of IDS in different networks like Ethernet Networks, 802.11 Networks, Mobile Networks, Ad-hoc Networks, and Wireless Sensor Networks.

UNIT VI **Lectures: 4**

Introduction to Snort, Different modes of Snort, Snort IDS Components, Snort Rules, Snort Filters, Snort output, Alert modes.

Text/ Reference Book:

1. Network Intrusion Detection and Prevention by Ali A. Ghorbani, Wei Lu Mahbod Tavallaee, Springer.
2. Intrusion Detection & Prevention by Carl Endorf, Eugene Schultz, and Jim Mellander, TMH.
3. Implementing Intrusion Detection Systems by Tim Crothers, Wiley.