राष्ट्रीय प्रौद्योगिकी संस्थान पटना / NATIONAL INSTITUTE 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:**

CSXX2013: ***Intrusion Detection*** **L-T-P-Cr: 3-0-0-3**

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**	**Level of Attainment**
1.	Analyze several security threats and the significance of security needs.	PO4, PO5	Familiarity
2.	Explain several types of IDS and IPS, their use and implementation, and also how to evaluate their performance.	PO4, PO5	Familiarity
3.	Describe various foundations on which detection approaches can be built.	PO2, PO3	Assessment
4.	Design of IDS using machine learning based approach	PO2, PO3	Assessment
5.	Detail implementation of Snort and its working principle.	PO3, PO4, PO5	Assessment
6.	Performance of different types of cyber-attacks and their detection using IDS	PO2, PO3, PO5	Assessment

UNIT I Lectures: 5

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: 7

Manual Malware Infection Analysis, Signature Based Malware Detection and Classification – pros and cons, Types of IDS: Network-Based IDS, Host-Based IDS, Hybrid IDS, Intrusion Prevention Systems (IPS): Network-Based IPS, Host-Based IPS, Intrusion Detection Tools, the limitations and open problems of intrusion detection systems, advanced persistent threats.

UNIT III Lectures: 8

Need for machine learning based techniques, Case studies of intrusion detection systems against real-world threats and malware. Statistical and machine approaches to detection of attacks on computers - Techniques for studying the Internet and estimating the number and severity of attacks, network based attacks, host based attacks. Statistical pattern recognition for detection and classification of attacks and techniques for visualizing network data, etc.

UNIT IV Lectures: 8

Intrusion into network – Firewalls, Rule Based Techniques, Signature Based Techniques, Simple Machine Learning Models on Network Data

UNIT V Lectures: 7

About Snort, Snort Modes, Snort's IDS Components, Snort Rules, Snort Output, Special Requirements, More about Snort 2.0, Additional Tools, SNORT- A case study

UNIT VI Lectures: 7

Unauthorized access – buffer overflow, packet fragmentation, out-of-spec packets Review of Network protocol – TCP/IP, Intrusion detection through tcpdump, Malicious and non-malicious traffic, IP headers, TCP, UDP and ICMP protocols and header formats, Header information to detect intrusion, logs and their analysis, IDS through reaction and response Intrusion analysis – data correlation.

Text/Reference Books

1. Carl Endorf, Gene Schultz, Jim Mellander, Intrusion Detection and Prevention, McGraw Hill.

2. Paul E. Proctor. The Practical Intrusion Detection Handbook, Prentice Hall.
3. Roberto Di Pietro, Luigi V. Mancini, Intrusion Detection System, Springer, 2008.
4. Fadia, A., Zacharia, M., (2009). *Intrusion alert: An ethical hacking guide to intrusion detection*. Vikas Publishing House Pvt Ltd.