

---

## INTRUSION DETECTION SYSTEMS (ELECTIVE – 2)

**Course Code:** 13CS2214

**L P C**  
**4 0 3**

**Pre requisites:** Fundamental knowledge in Operating Systems, and Networks

### **Course Educational Objectives:**

1. Understand when, where, how, and why to apply Intrusion Detection tools and techniques in order to improve the security posture of an enterprise.
2. 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
3. Analyze intrusion detection alerts and logs to distinguish attack types from false alarms

### **Course Outcomes:**

1. Explain the fundamental concepts of Network Protocol Analysis and demonstrate the skill to capture and analyze network packets.
2. Use various protocol analyzers and Network Intrusion Detection Systems as security tools to detect network attacks and troubleshoot network problems.

### **UNIT-I**

History of Intrusion detection, Audit, Concept and definition , Internal and external threats to data, attacks, Need and types of IDS, Information sources Host based information sources, Network based information sources.

### **UNIT-II**

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

**UNIT-III**

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

**UNIT-IV**

Working with Snort Rules, Rule Headers, Rule Options, The Snort Configuration File etc. Plugins, Preprocessors and Output Modules, Using Snort with MySQL

**UNIT-V**

Using ACID and Snort Snarf with Snort, Agent development for intrusion detection, Architecture models of IDs and IPs.

**TEXT BOOKS:**

1. Rafeeq Rehman : “ Intrusion Detection with SNORT, Apache, MySQL, PHP and ACID,” 1<sup>st</sup> Edition, Prentice Hall , 2003.

**REFERENCES:**

1. Christopher Kruegel, Fredrik Valeur, Giovanni Vigna: “Intrusion Detection and Correlation Challenges and Solutions”, 1<sup>st</sup> Edition, Springer, 2005.
2. Carl Endorf, Eugene Schultz and Jim Mellander “ Intrusion Detection & Prevention”, 1<sup>st</sup> Edition, Tata McGraw-Hill, 2004.
3. Stephen Northcutt, Judy Novak : “Network Intrusion Detection”, 3<sup>rd</sup> Edition, New Riders Publishing, 2002.
4. T. Fahringer, R. Prodan, “A Text book on Grid Application Development and Computing Environment”. 6<sup>th</sup> Edition, KhannaPublihsers, 2012.