INTRUSION DETECTION SYSTEMS

Course Code: 15CS2211

L	P	C
3	0	3

Pre requisites: Fundamental knowledge in Operating Systems, and Networks

Course Outcomes:

CO1: Explain the fundamental concepts of Network Protocol Analysis and demonstrate the skill to capture and analyze network packets.

CO2: Use various protocol analyzers and Network Intrusion Detection Systems as security tools to detect network attacks and troubleshoot network problems.

UNIT-I (10-Lectures)

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 (10-Lectures)

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 (10-Lectures)

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 (10-Lectures)

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

UNIT-V (10-Lectures)

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," 1st Edition, Prentice Hall, 2003.

REFERENCES:

1. Christopher Kruegel, Fredrik Valeur, Giovanni Vigna, "Intrusion Detection and Correlation Challenges and Solutions", 1st Edition, Springer, 2005.
2. Carl Endorf, Eugene Schultz and Jim Mellander, "Intrusion Detection & Prevention",1st Edition, Tata McGraw-Hill, 2004.
3. Stephen Northcutt, Judy Novak, "Network Intrusion Detection", 3rd Edition, New Riders Publishing, 2002