CSCS 505: INTRUSION DETECTION SYSTEM

Course Objective:

The objective of the courses to

1) Basic concepts of intrusion detection system
2) Understanding and application of threat detection and prevention.

UNIT - I

Chapter 2: History of Intrusion detection, Audit, Concept and 2.1- definition, Internal and external threats to data, attacks, 2.3 - need and types of IDS, 2.3.7 - Information sources, 2.3.7.2 - Host based information sources, 2.3.7.1- Network based information sources.
Intrusion Prevention Systems, Network IDs protocol-based IDs, Hybrid IDs, Analysis schemes, thinking about intrusion, A model for intrusion analysis, techniques. **12 Hours**

UNIT - II

[1st Reference book]

Chapter 1: Introduction to Snort, Chapter 2: 2.1 - Snort Installation Scenarios, 2.2- Installing Snort, 2.3 - Running Snort on Multiple Network Interfaces, 2.4 - Snort Command Line Options, 2.5- Step-By-Step Procedure to Compile and Install Snort, 2.6 - Location of Snort Files, 2.7 - Snort Modes, 2.8 - Snort Alert Modes.
Chapter 3: Working with Snort Rules, 3.5 - Rule Headers, 3.6 - Rule Options, 3.7 - The Snort Configuration File etc. Chapter 4: Plugins, Preprocessors and Output Modules, Chapter 5: Using Snort with MySQL Chapter 6: Using ACID and SnortSnarf with Snort. **12 Hours**

UNIT - III

[2nd Reference book]

Chapter 8 : Securing database-to-database communications : 8.1 - Monitor and limit outbound communications , 8.2 - Secure database links and watch for link-based elevated privileges, 8.3 - Protect link usernames and passwords, 8.4 - Monitor usage of database links, 8.5 - Secure replication mechanisms, 8.6 - Map and secure all data sources and sinks, Chapter 9: Trojans : 9.1 - The four types of database Trojans, 9.2 - Baseline calls to stored procedures and take action on Divergence, 9.3 - Control creation of and changes to procedures and triggers, 9.4 - Watch for changes to run-as privileges, 9.5 - Closely monitor developer activity on production environments, 9.6 - Monitor creation of traces and event monitors, 9.7 - Monitor and audit job creation and scheduling, 9.8 - Be wary of SQL attachments in e-mails.
12 Hours

Course Outcome:

At the end of the course student will be able to

1) Obtain comprehensive knowledge in the subject of Intrusion Detection System.
2) Gets random exposure to principles and techniques used in Intrusion Detection System.

TEXTBOOK:

1. Rebecca Gurley Base “Intrusion Detection” MacMillan Technology Series (MTP Series) ISBN 1578701856, 9781578701858

REFERENCE BOOKS:

1. RafeeqRehman “Intrusion Detection with SNORT, Apache, MySQL, PHP and ACID”, Prentice Hall PTR, 2003 ISBN 0-13-140733-3.
2. RonBenNatan, Implementing Database Security and Auditing, Elsevier, Indian reprint, ISBN: 9781555583347.