PIS216: INTRUSION DETECTION AND ANALYSIS

L	T	P	Cr
3	0	2	4.0

Course Objectives: To describe appropriate situations and scenarios where intrusion detection may be applied to achieve an increased level of situational awareness and information assurance, then apply the knowledge of architecture, configuration, and analysis of specific intrusion detection systems.

Introduction of Intrusion Detection systems

Purpose and Scope, Need and applications of intrusion detection systems, Firewalls and intrusion detection systems, Challenges, Sample IDS Deployment examples.

Intrusion Detection Systems and Associated Methodologies

Uses of Intrusion detection technologies, Key Functions of Intrusion detection systems, Common Detection Methodologies, Signature-Based Detection, Anomaly-Based Detection, stateful protocol analysis, Types of Intrusion detection technologies

Intrusion detection Technologies and components

Components and Architecture, Typical Components Network Architectures, Security capabilities, Information Gathering Capabilities, Logging Capabilities, Detection Capabilities Prevention Capabilities and its implementation, Deploying IDS.

Network-Based Intrusion Detection Systems

Networking Overview, Application Layer, Transport Layer, Network Layer, Hardware Layer, Components and Architecture, Typical Components, Network Architectures and Sensor Locations, Security Capabilities, Information Gathering Capabilities, Logging Capabilities

Wireless Network based Intrusion Detection Systems

Wireless Networking Overview, WLAN Standards, WLAN Components, Threats against WLANs Components and Architecture, Typical Components, Network Architectures, Security Capabilities, Information Gathering Capabilities, Logging Capabilities, Detection Capabilities, Prevention Capabilities, Handling Alerts

Using and Integrating Multiple Intrusion Detection Systems Technologies

Need for Multiple IDS technologies, Integrating Different IDS Technologies, Direct IDS Integration Indirect IDS Integration, Other Technologies with IDS Capabilities, Network Forensic Analysis Anti-Malware Technologies, Honeypots

Host-Based IDS and Network Behavior analysis

Components and Architecture, Typical Components and Network Architectures, Host Architectures, Security Capabilities, Logging Capabilities, Detection Capabilities, Prevention Capabilities, Components and Architecture of network behavior in presence of IDS, Components in presence of IDS, Network Architectures and Sensor Locations, Security Capabilities in presence of IDS, Information Gathering Capabilities, Logging Capabilities, Detection Capabilities, Prevention Capabilities

Laboratory Work: Configuring different Intrusion detection tools for analysing various attacks.

Recommended Books

1. Implementing Intrusion Detection Systems: A Hands-On Guide for Securing the Network, Tim Crothers,

Wiley,1st Edition,2002

2. Intrusion Detection and Correlation: Challenges and Solutions, Christopher Kruegel, FedrickValeur,Springer, 1st Edition **,** 2005

3. Practical Intrusion Analysis: Prevention and Detection for the Twenty-First Century: Prevention and Detection, Ryan Trost, Addison Wesley, 1st Edition , 2009