COURSE CODE	COURSE TITLE	L	T	P	C
1152CS170	INTRUSION DETECTION AND PREVENTION	3	0	0	3

Course Category: Program Elective

A. Preamble :

1. To provide a solid foundation to the students in network security and intrusion detection and prevention.
2. To enable the students to master the knowledge about intrusion detection and prevention in the context of real-life applications.
3. To prepare the students for understanding, evaluating critically, and assimilating new knowledge and emerging technology in network security

B. Prerequisite Courses:

Sl. No	Course Code	Course Name
1	1151CS111	Computer Networks

C. Related Courses:

Sl. No	Course Code	Course Name
1	1156CS701	Major Project

D. Course Outcomes :

Upon the successful completion of the course, students will be able to:

CO Nos.	Course Outcomes	Knowledge Level (Based on revised Bloom's Taxonomy)
CO1	Understand the physical location, the operational characteristics and the various functions performed by the intrusion detection and prevention system.	K2
CO2	Describe how components in different layers inter-operate in the intrusion detection and prevention system.	K2
CO3	Learn new techniques and to align new security technologies to existing network infrastructure.	K2
CO4	Understand the current and effective architecture to deal with network security threats.	K2
CO5	Apply intrusion detection alerts and logs to distinguish attack by using SNORT tool.	K3

E. Correlation of COs with POs :

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	H							L							M
CO2		H	M	M				L					L		
CO3	H	M			H	M		M					M	M	
CO4			H	L		M		M						H	L
CO5		H	H	H	H			M				M			H

H- High; M-Medium; L-Low

F. Course Content :

UNIT I INTRODUCTION 9

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 DETECTION AND NETWORK TRAFFIC SIGNATURE 9

Components of IDS, Steps of implementation and monitoring, Host- and network-based IDS, Implementing and evaluating IDS, intrusion detection versus intrusion prevention, Signature analysis, Detecting traffic signatures, Identifying suspicious events, Creating custom traffic signatures, Common Vulnerability and Exposures (CVE) standards

UNIT III INTRUSION DETECTION AND PREVENTION TECHNIQUES 9

Host-based intrusion detection system (IDS) / intrusion prevention system (IPS), network-based IDS/IPS. Data collection for IDS/IPS. Intrusion detection techniques, misuse detection: pattern matching, rule-based and state-based; anomaly detection: statistical based, machine learning based, data mining based; hybrid detection.

UNIT IV IDS and IPS ARCHITECTURE 9

Tiered architectures, single-tiered, multi-tiered, peer-to-peer. Sensor: sensor functions, sensor deployment and security. Agents: agent functions, agent deployment and security. Manager component: manager functions, manager deployment and security. Information flow in IDS and IPS, defending IDS/IPS

UNIT V IDP TOOLS 9

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

TOTAL : 45 Periods

G. Learning Resources

i . TEXT BOOKS

1. Ali A. Ghorbani, Network intrusion detection and prevention concepts and techniques, Springer, 2010
2. C. Endorf, E. Schultz and J. Mellander, Intrusion Detection & Prevention, McGraw-Hill/Osborne, 2004.
3. Rafeeq Rehman : " Intrusion Detection with SNORT, Apache, MySQL, PHP and ACID," 1st Edition, Prentice Hall , 2003

ii . 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

iii .ONLINE RESOURCES

1. https://opensourceforu.com/2017/04/best-open-source-network-intrusion-detection-tools/
2. https://security.berkeley.edu/intrusion-detection-guideline
3. https://www.snort.org/