NIRMA UNIVERSITY

Institute:	Institute of Technology, School of Technology
Name of Programme:	M Tech CSE (Cyber Security)
Course Code:	6CS462ME25
Course Title:	Intrusion Detection and Prevention Systems
Course Type:	Department Elective-I
Year of Introduction:	2025-26

L	T	Practical Component				C
		LPW	PW	W	S	
3	0	2	-	-	-	4

Course Learning Outcomes (CLO):

At the end of the course, the students will be able to –

1. explain the practical aspects of intrusion detection systems (BL2)
2. relate user profile, attacks, reactions and responses in network systems (BL2)
3. apply machine learning techniques to optimize performance of intrusion detection system (BL3)
4. develop a customized Intrusion Detection and Prevention Systems, and Firewalls for organizational requirements. (BL6)

Unit	Contents	Teaching Hours (Total 45)
Unit-I	**Approaches in Anomaly-based IDS**: Introduction, Payload-based vs. header-based approaches, setting up an ABS, PAYL & POSEIDON	06
Unit-II	**Profiling of Program Behaviour**: Introduction, user profiling, program profiling, finite state automaton, implementation methodology, case studies of program behaviour and user behaviour profiling, Remus configuration	06
Unit-III	**Learning Behaviour Profiles from Noisy Sequences**: Introduction, learning by abstraction, Regular Expressions, String Alignment and Flexible Matching, Learning Algorithm, Evaluation of Artificial Traces, User Profiling	06
Unit-IV	**Correlation Analysis of Intrusion Alerts**: Introduction, Approaches based on similarity between Alert Attributes, approaches based on predefined attack scenarios, approaches based on prerequisites and consequences of attacks, approaches based on multiple information sources, Privacy issues in autocorrelation	06
Unit-V	**Multi-step network attacks**: Introduction, Related Work, preliminaries, hardening network to prevent multistep intrusions, Correlating and predicting multiple steps attacks	06
Unit-VI	**Threat Response**: Bridging the link between Intrusion Detection alerts and security policies: Security Policy Formalism, Threat Response system, From alerts to new policies	07
Unit-VII	**Intrusion Detection and Reaction**: An integrated approach to network security: Proposed Framework, Architecture for Intrusion Detection, Intrusion reactions, attack sessions, intrusion detection subsystem, traffic classification, and intrusion reaction, testing.	08

Self-Study:
The self-study contents will be declared at the commencement of the semester. Around 10% of the questions will be asked from self-study content.

Suggested Readings/ References:

1. Roberto Di Pietro and Luigi Mancini, Intrusion Detection Systems, Springer
2. Rafeeq Ur Rehman, Intrusion Detection Systems with Snort, Pearson Education, Prentice Hall
3. Guide to Intrusion Detection and Prevention Systems, National Institute of Science and Technology
4. Tim Crothers, Implementing Intrusion Detection Systems: A hands-on guide for Securing the Network.

Suggested List of Experiments:

Sr. No.	Name of Experiments/Exercises	Hours
1	Study of snort as an open-source intrusion detection system	02
2	Study of security implementation (firewall) in Nirma University – case study	02
3	Implement a statistical intrusion detection system	02
4	Implement a machine learning-based intrusion detection system	04
5	Implement a machine learning-based behavior profile based on activities carried out in a system	04
6	Implement an attack graph and identify the attack paths	04
7	Implement an Or-BAC policy for authenticating and authorizing	04
8	Write a typical network access policy for an organization	04
9	Generate IDMEF messages automatically from any alert logged in the firewall or intrusion detection system	02
10	Implement mandatory access control and discretionary access control for a typical web-based application.	02