NIRMA UNIVERSITY
Institute of Technology
B Tech, Computer Science and Engineering
Semester-VI
Department Elective-II

L	T	P	C
3	0	2	4

Course Code	2CSDE62
Course Title	Intrusion Detection Systems

Course Outcomes:

After successful completion of the course, student will be able to -

1. describe the practical aspects of intrusion detection systems
2. apply machine learning techniques to optimize performance of intrusion detection system
3. correlate user profile, attacks, reactions and responses in network systems
4. implement formal Or-BAC technique for dynamic policy adaptation.

Syllabus:

Teaching Hours: 45

Unit I **06**

Approaches in Anomaly based Intrusion Detection Systems: Introduction, Payload based vs. header based approaches, setting up an ABS, PAYL & POSEIDON

Unit II **06**

Formal Specification for Fast Automatic Profiling of Program Behavior: Introduction, Related Works, Methodology, Case Study, Remus configuration

Unit III **06**

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

Unit V **06**

Multi-step network attacks: Introduction, Related work, preliminaries, Hardening network to prevent multistep intrusions, Correlating and predicting multiple steps attacks

Unit VI **07**

Threat Response: Bridging the link between Intrusion Detection alerts and security policies: Security Policy Formalism, Threat Response system, From alerts to new policies

Unit VII **08**

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

Self-Study:

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

Laboratory Work:

Laboratory work will be based on the above syllabus with minimum 7 experiments to be incorporated.

Suggested Readings^:

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

L=Lecture, T=Tutorial, P=Practical, C=Credit

^this is not an exhaustive list