Appendix-A
Noti.No. NU-49
Acad.Cou.mtg.-15.07.22

NIRMA UNIVERSITY

Institute:	Institute of Technology
Name of Programme:	Integrated B.Tech.(CSE)-MBA
Course Code:	CSI0901
Course Title:	Intrusion Detection Systems
Course Type:	(□ Core/ □ Value Added Course / √ **Department Elective** / □ Institute Elective/ □ University Elective/ □ Open Elective / □ Any other)
Year of Introduction:	2022-23

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

Course Learning Outcomes (CLOs):

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

1. define the practical aspects of intrusion detection systems (BL1)
2. apply machine learning techniques to optimize performance of intrusion detection system (BL2)
3. develop formal Or-BAC technique for dynamic policy adaptation (BL3)
4. analyze user profile, attacks, reactions and responses in network systems (BL4)

Syllabus: **Total Teaching hours: 30**

Unit	Syllabus	Teaching hours
Unit-I	Approaches in Anomaly based Intrusion Detection Systems: Introduction, Payload based vs. header-based approaches, setting up an ABS, PAYL & POSEIDON	05
Unit-II	Formal Specification for Fast Automatic Profiling of Program Behavior: Introduction, Related Works, Methodology, Case Study, Remus configuration	03
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	05
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	05
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	06

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

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 Publication
4. Tim Crothers, Implementing Intrusion Detection Systems: A hands-on guide for Securing the Network, Wiley

Suggested List of Experiments:

Sr. No.	Title	Hours
1	Implement an anomaly-based intrusion detection system using statistical techniques.	02
2	Implement an anomaly-based intrusion detection system using machine learning techniques.	04
3	Implement a simple user profiling system.	02
4	Implement the attack graph.	04
5	Study working of Snort.	02
6	Perform alert correlation using alerts from an intrusion detection system.	04
7	Implement a simple Or-BAC formalism for sample deployment.	02

Suggested Case List: -NA-