INDIAN INSTITUTE OF TECHNOLOGY ROORKEE

NAME OF DEPT./CENTRE: **Electronics and Computer Engineering**

1. Subject Code: **EC – 656N** Course Title: **Intrusion Detection Systems**

2. Contact Hours: **L: 3 T: 0 P: 0**

3. Examination Duration (Hrs.): **Theory** **0 3** **Practical** **0 0**

4. Relative Weight: **CWS** **15** **PRS** **00** **MTE** **35** **ETE** **50** **PRE** **00**

5. Credits: **0 3** 6. Semester: □ **Autumn** ☑ **Spring** □ **Both**

7. Pre-requisite: **EC - 351**

8. Subject Area: **MSC**

9. Objective: To introduce the elements of intrusion detection systems and its models.

10. Details of the Course:

Sl. No.	Contents	Contact Hours
1.	Intruder types, intrusion methods, processes and detection, message integrity and authentication, honey pots.	8
2.	General IDS model, data mining based IDS, Denning model, data mining framework for constructing features and models for intrusion detection systems.	6
3.	Unsupervised anomaly detection, CV5 clustering, SVM, probabilistic and statistical modeling, general IDS model and taxonomy, evaluation of IDS, cost sensitive IDS.	8
4.	NBAD, specification based and rate based DDOS, scans/probes, predicting attacks, network based anomaly detection, stealthy surveillance detection; Defending against DOS attacks in scout: signature-based solutions, snort rules.	6
5.	Host-based anomaly detection, taxonomy of security flaws in software, self-modeling system calls for intrusion detection with dynamic window size.	6
6.	Secure intrusion detection systems, network security, secure intrusion detection environment, secure policy manager, secure IDS sensor, alarm management, intrusion detection system signatures, sensor configuration, signature and intrusion detection configuration, IP blocking configuration, intrusion detection system architecture.	8
	Total	**42**

11. Suggested Books:

Sl. No.	Name of Books/Authors	Year of Publication
1.	Endorf, C., Schultz E. and Mellander J., “Intrusion Detection and Prevention,” McGraw-Hill.	2003
2.	Bhatnagar, K., “Cisco Security”, Course Technology.	2002
3.	Marchette, D. J., “Computer Intrusion Detection and Network Monitoring: A Statistical Viewpoint”, Springer.	2001
4.	Rash, M., Orebaugh, A. and Clark, G., “Intrusion Prevention and Active Response: Deploying Network and Host IPS”, Syngress.	2005
5.	Cooper, M., Northcutt, S., Fearnow, M. and Frederick, K., “Intrusion Signatures and Analysis”, Sams.	2001