Intrusion Detection and Information Warfare	L	T	P	Computer Networks, Information Security
	3	1		

Course Objective: To equip the students with knowledge about detection and prevention of various intrusions.

S. NO	Course Outcomes (CO)
CO1	Students will be introduced to basic concepts of intrusion detection system.
CO2	Students will be able to understand Intrusion Prevention Systems, Network IDs protocol and model for intrusion analysis.
CO3	To Apply knowledge of the fundamentals and history of Intrusion Detection in order to avoid common pitfalls in the creation and evaluation of new Intrusion Detection Systems.
CO4	To Understand when, where, how, and why to apply Intrusion Detection tools and techniques in order to improve the security posture of an enterprise.

S. NO	Contents	Contact Hours
UNIT 1	Introduction: Introduction to Intrusion Detection and Snort, Network Traffic Analysis Working with Snort Rules, Plugins, Preprocessors and Output Modules, Using Snort with MySQL, Using ACID and Snort Snarf with Snort, Miscellaneous Tools, Intrusion Prevention.	10
UNIT 2	Intrusion detection techniques: techniques to provide privacy in Internet Application and protecting digital contents (music, video, software) from unintended use, authentication.	8
UNIT 3	System and Application Security- mail security (PGP etc) file System security, program and security, memory security, Sandboxing.	8
UNIT 4	Security threads protection intruders: Viruses-trusted system. Secure programming languages- concepts structured multiprogramming, shared classes, cooperating sequential processes, structure of the multiprogramming system RC-4000 software. Information Warfare: offensive information warfare, defensive information warfare.	8

UNIT 5	Key management in Group communication systems, Router security, Denial of service and side-channel attacks, Intrusion detection systems, Intrusion detection techniques-centralized and distributed.	**8**
	TOTAL	**42**