Internet Security, tools & techniques	Code & No:	CS 444
	Credits:	3 (3,0,1)
	Pre-requisite:	IT 341
	Co-requisite:	None
	Level:	9 or 10

Course Description:

This course aims to introduce security issues arising primarily from computer networks. Topics include node and service authentication, address spoofing, hijacking, SYN floods, smurfing, sniffing, routing tricks, and privacy of data en route. Buffer overruns and other exploitation of software development errors. Hardening of operating systems. Intrusion detection. Firewalls. Ethics.

Course Aims:

1) Apply key concepts of internet security in organizations
2) Analyze and evaluate security in networks
3) Analyze security requirements and help design policy related to network security
4) Reflect upon criminal acts, ethics, legal frameworks and how that impact on internet security
5) Analyze intrusion detection system (IDS) requirements and evaluate such technologies
6) Analyze firewall requirements and evaluate such technologies

Student Outcomes (SOs):

☐(a) An ability to apply knowledge of computing and mathematics appropriate to the program's student outcomes and to the discipline

☐(b) An ability to analyze a problem, and identify and define the computing requirements appropriate to its solution

☐(c) An ability to design, implement, and evaluate a computer-based system, process, component, or program to meet desired needs

☐(d) An ability to function effectively on teams to accomplish a common goal

☒(e) An understanding of professional, ethical, legal, security and social issues and responsibilities

☐(f) An ability to communicate effectively with a range of audiences

☐(g) An ability to analyze the local and global impact of computing on individuals, organizations, and society

☐(h) Recognition of the need for and an ability to engage in continuing professional development

☒(i) An ability to use current techniques, skills, and tools necessary for computing practice.

☒(j) An ability to apply mathematical foundations, algorithmic principles, and computer science theory in the modeling and design of computer-based systems in a way that demonstrates comprehension of the tradeoffs involved in design choices. [CS]

☒(k) An ability to apply design and development principles in the construction of software systems of varying complexity. [CS]

☐(j) An ability to use and apply current technical concepts and practices in the core information technologies of human computer interaction, information management, programming, networking, and web systems and technologies. [IT]

☐(k) An ability to identify and analyze user needs and take them into account in the selection, creation, evaluation, and administration of computer-based systems. [IT]

☐(l) An ability to effectively integrate IT-based solutions into the user environment. [IT]

☐(m) An understanding of best practices and standards and their application. [IT]

☐(n) An ability to assist in the creation of an effective project plan. [IT]

Course Learning Outcomes (CLOs):

1. Identify and discuss the fundamental reasons why Internet security is such a critical element in today's business, government, education, and home technology-based environments.
2. Review and develop the key elements of Internet security management program.
3. Understand the awareness about the issues involving information security among functional and information resource managers.
4. Familiarize the manager with the threats, technologies, and issues to the degree that they can make effective security planning, policy and deployment decisions.
5. Develop and implement security schemes designed to protect the organization's internet/network systems

SOs and CLOs Mapping:

CLO/SO	a	b	c	d	e	f	g	h	i	j	k	l	m	n
CLO1														
CLO2									√					
CLO3					√									
CLO4					√				√					

CLO5									√	√				

No.	Topics	Weeks	Teaching hours
1	Node and service authentication	1	3
2	Address spoofing, hijacking	2	6
3	SYN floods, Smurfing	2	6
4	Sniffing, routing tricks, and privacy of data en route	2	6
5	Buffer overruns and other exploitation of software development errors	2	6
6	Hardening of operating systems.	2	6
7	Intrusion detection	2	6
8	Firewalls Ethics	1	3
	Total	**14**	**42**

Textbook:

- "Internet Security: How To Defend Against Attackers On The Web", by Mike Harwood, Jones & Bartlett Learning Information Systems Security & Assurance, 2nd Edition (August 4, 2015), ISBN-10: 1284090558, ISBN-13: 978-1284090550

Essential references:

- "Information Security: Principles and Practices", by Mark S. Merkow, Jim Breithaupt, Pearson IT Certification; 2 edition (June 14, 2014), ISBN-10: 0789753251, ISBN-13: 978-0789753250