

## NETWORK AND WEB SECURITY

VI SEMESTER: CSE & CSIT									
Course Code	Category	Hours / Week			Credits	Maximum Marks			
ACIC03	CORE	L	T	P	C	CIA	SEE	Total	
		3	1	0	4	30	70	100	
<b>Contact Classes: 45</b>		<b>Tutorial Classes: Nil</b>		<b>Practical Classes: Nil</b>		<b>Total Classes: 45</b>			
<b>Prerequisites: Computer Networks</b>									
<b>I. COURSE OVERVIEW:</b>									
The course introduces application security in recommending proper mitigations for web security issues, and infrastructure security. The security problems, protocols who have an interest in enhancing the defense of web applications.									
<b>II. COURSE OBJECTIVES:</b>									
<b>The students will try to learn:</b>									
I. The basics of Cryptography and Network Security.									
II. The process of securing a message over insecure channel by various means									
III. The mechanisms for maintaining confidentiality, integrity and availability of a data									
IV. The various protocols for network security to protect against the threats in the networks.									
<b>III. COURSE OUTCOMES:</b>									
<b>After successful completion of the course, students should be able to:</b>									
CO 1	<b>Interpret various protocols(TCP,DNS,SMTP) for solving the security problems in the network</b>						Understand		
CO 2	<b>Solve unauthorized access from the internet by using firewalls, DNSSEC with NSEC3</b>						Apply		
CO 3	<b>Find computer and network security issues and classify the issues to prevent, detect and recover from the attacks</b>						Remember		
CO 4	<b>Summarize HTML elements and attributes for structuring and presenting the content of webpage based on the user requirement</b>						Understand		
CO 5	<b>Identify HTTP pollution and HTTP parameter tammpering attacks by various techniques</b>						Apply		
CO 6	<b>Explain the mechanisms for maintaining confidentiality,integrity and availability of a data</b>						Understand		
<b>IV. COURSE SYLLABUS:</b>									
<b>MODULE-I: SECURITY PROBLEMS IN NETWORK PROTOCOLS (10)</b>									
TCP, DNS, SMTP, ROUTING, Problems in TCP/IP protocol suite, survey of BGP security, DNS cache poisoning.									
<b>MODULE -II: NETWORK DEFENSE TOOLS (10)</b>									
Security evaluation of DNSSEC with NSEC3, distributed firewalls, detecting network intruders in real time, network security testing, art of port scanning.									
<b>MODULE -III: MALWARE AND ATTACKS (09)</b>									
Computer viruses, spyware and key, loggers, bot, nets, attacks and defenses, denial of service attacks									
Control hijacking attacks, exploits and defenses, exploitation techniques and fuzzing									
<b>MODULE -IV: BASICS OF WEB SECURITY (08)</b>									
Web Basics: HTML, CSS, JS, URLs, DOM, Frames, HTTP, Navigation, X-Domain communication, Network									

Attacks and HTTPS, Limitations of HTTPS, Same Origin Policy and Web Attacker Model, Injection Flaws (I): Cross, site Scripting (XSS), Injection Flaws (II) : XSS (contd.), SQL Injection, OS Command Injection, HTTP Header Injection

**MODULE –V: INSECURE WEB LOGIC (09)**

Logic Flaws, HTTP Pollution, HTTP Parameter Tampering, Cookie Flaws and Server Misconfiguration, Attacks on User Interfaces, Browser Design and Flaws, User Privacy: Browser and Device Fingerprinting, User Tracking, Browser Caching Flaws

**V. TEXT BOOKS:**

1. William Stallings, “Network Security Essentials: Applications and Standards”, Pearson Education Limited, 6<sup>th</sup> Edition, 2016.
2. Uttam K Roy, “Web Technologies”, Oxford University Press, Illustrated Edition, 2010.
3. Amanda Berlin and Lee Brotherston, “Defensive Security Handbook”, O’Reilly, 1<sup>st</sup> Edition, 2017.
4. John E. Canavan, " The Fundamentals of Network Security," Artech House Publishers, In-Print-Forever hardbound Edition, 2001.
5. Chris Bates, “Web Programming: Building Internet Applications”, Wiley, 3<sup>rd</sup> Edition, 2006.

**VI. REFERENCE BOOKS:**

1. Jon Duckett, “Beginning Web Programming with HTML, XHTML, and CSS”, WROX, 2<sup>nd</sup> Edition, 2008.
2. R. W. Sebesta, “Programming World Wide Web”, Pearson, 4<sup>th</sup> Edition, 2007.
3. Paul Dietel, “Internet and World Wide Web – How To Program”, Pearson, 4<sup>th</sup> Edition, 2007.
4. Juanita Ellis, Tim Speed, William P. Crowell, " The Internet Security Guidebook: From Planning to Deployment," Academic Press, 1<sup>st</sup> Edition, 2001.
5. Stephen Northcutt, Donald McLachlan, Judy Novak, " Network Intrusion Detection: An Analyst's Handbook", New Riders Publishing, 2<sup>nd</sup> Edition, 2000.

**VII. WEB REFERENCES:**

1. <http://nptel.ac.in/>
2. <https://ocw.mit.edu>