NETWORK SECURITY

V Semester: CSE (CS)

Course Code	Category	Hours / Week			Credits	Maximum Marks		
		L	T	P	C	CIA	SEE	Total
ACCC03	Core	3	1	0	4	30	70	100
Contact Classes: 45	Tutorial Classes: 15	Practical Classes: Nil				Total Classes: 60		

Prerequisite: Computer Networks

I.COURSE OVERVIEW:

This course introduces different Security Concepts in network Security.In this course students are going to learn about different policies, processes and practices adopted to prevent, detect and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.Especially different types of Network scanning Tools are going to learn to monitor and scanning the Network.

II.COURSE OBJECTIVES:

The students will try to learn:

1. The Fundamental practices, policies, technologies and standards in providing security on network.
2. The TCP/IP networking mechanism to diagnose the security problems in network.
3. The different network and communication protocols presence in the network to apply some security factors.

III. COURSE OUTCOMES:

After successful completion of the course, students should be able to:

CO 1	**Demonstrate** various security problems that implemented in Tcp/ipprotocol suite.	Understand
CO 2	**Recall** Denial of Service (DoS) attacks can cause the problems innetwork.	Remember
CO 3	**Compare** different practices, policies and standards that provides sety on network.	Understand
CO 4	**Analyze** Internet Control Message Protocol (ICMP) utilities that help to monitor the networking mechanism.	Analyze
CO 5	**Utilize** the different Pretty Good Privacy(PGP) services that offeredon Email Security.	Apply
CO 6	**Summarize** the Concept of Transport Layer Security(TLS) provides security against on web threats	Understand

IV.COURSE SYLLABUS:

MODULE-I: INTRODUCTION ON NETWORKING AND SECURITY (10)

Access Control and Site Security- Virtual Local Area Network (VLAN), Demilitarized zone (DMZ)attacks, services mechanisms. Attack Methods–TCP/IP, Internetworking, Security problems in TCP/IP protocol suite, BGP security attacks, DNS Cache poisoning, Denial of Service(DoS) attacks, Distributed Denial of Service (DDoS) attacks, IP Trace back attacks.

MODULE-II: REAL-TIME COMMUNICATION SECURITY (08)

Introduction to TCP/IP protocol stack – Implementation layers for security protocols and implications-Psec: A Hand ESP-IP sec: IKE-SSL/TLS –Distribution lists –Establishing keys-Privacy, Source Authentication, Message Integrity, Non-Repudiation, Proof of Submission, Proof of Delivery, Message Flow Confidentiality, Anonymity–Packet filters – Application level gate ways.

MODULE-III: INTERNET CONTROL MESSAGE PROTOCOL (ICMP) (09)

ICMP Messages - Attacks Using ICMP Messages - reconnaissance scanning - ICMP sweep-Trace route - firewalk - inverse mapping - OS finger printing - exploiting systems.

ICMP- ICMP Route Redirect - ICMP informational messages - ICMP Router Discovery Messages - ICMP Floods - Smurf-Keeping Access Covering the Tracks.

MODULE-IV: ELECTRONIC MAIL SECURITY (09)

Pretty Good Privacy–PGP services–Transmission and Reception of PGP Messages– PGP message generation–PGP message reception.

MODULE-V WEB SECURITY (09)

Threats on the web –Secure Socket Layer and Transport Layer Security: SSL architecture– SSL record protocol– Handshake protocols.

V. TEXT BOOKS:

1. W. Stallings, "Cryptography and Network Security: Principles and Practice", Boston: Prentice Hall, 5th Edition, 2010.
2. A.Das and C.Veni Madhavan, "Public-key Cryptography: Theory and Practice", New Delhi, India: Pearson Education India, 2009.