NATIONAL INSTITUTE OF TECHNOLOGY, TIRUCHIRAPPALLI

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

COURSE PLAN – PART I			
Name of the programme and specialization	B.Tech. / CSE		
Course Title	Network Security		
Course Code	CSPE75	**No. of Credits**	3
Course Code of Pre-requisite subject(s)	CSPC63	**Semester**	VII
Session	July 2022	**Section (if, applicable)**	A & B
Name of Faculty	Dr. Kamalika Bhattacharjee	**Department**	CSE
Official Email	kamalika@nitt.edu	**Telephone No.**	
Name of Course Coordinator(s)	NIL		
Official E-mail	NIL	**Telephone No.**	
Course Type	Elective Course		

Syllabus (approved in BoS)

UNIT I Overview of Network

Overview of Network Security - Security services - attacks - Security Issues in TCP/IP suite - Sniffing - spoofing - buffer overflow - ARP poisoning - ICMP Exploits - IP address spoofing - IP fragment attack - routing exploits - UDP exploits - TCP exploits.*

UNIT II Message Authentication Code

Authentication requirements - Authentication functions - Message Authentication Codes - Hash Functions - Security of Hash Functions and MACs - MD5 message Digest algorithm - Secure Hash Algorithm - RIPEMD - HMAC Digital Signatures - Authentication protocols - Kerberos - X.509.*

UNIT III IP Security

IP Security - AH and ESP - SSL/TLS - SSH - Web Security - HTTPS - DNS Security - Electronic Mail Security (PGP - S/MIME).*

UNIT IV Viruses

Intruders - Viruses - Worms - Trojan horses - Distributed Denial-Of-Service (DDoS) - Firewalls - IDS - Honey nets - Honey pots.*

UNIT V Introduction to Wireless Network Security

Introduction to wireless network security - Risks and Threats of Wireless networks - Wireless LAN Security (WEP - WPA).*

*Programming assignments are mandatory.

TEXT BOOKS

1. W. Stallings, "Cryptography and Network Security: Principles and Practice", Fifth Edition, Prentice Hall, 2013.
2. Yang Xiao, Yi Pan, "Security in Distributed and Networking Systems", World Scientific, 2007.

REFERENCE BOOKS

1. Behrouz A Forouzan, Debdeep Mukhopadhyay, Cryptography and Network Security, McGraw Hill Education (India) Private Limited, 2010
2. Aaron E. Earle, "Wireless Security Handbook", Auerbach Publications, Taylor & Francis Group, 2006.
3. Atul Kahate, "Cryptography and Network Security", Tata McGraw Hill, 2003.

COURSE OBJECTIVES

1. To understand the network security, services, attacks, mechanisms, types of attacks
2. To comprehend and apply authentication services
3. To apply authentication algorithms
4. To comprehend and apply network layer security protocols, Transport layer security protocols, Web security protocols

MAPPING OF COs with POs

Course Outcomes	Programme Outcomes (PO)
1. Determine appropriate mechanisms for protecting the network	2, 6, 11
2. Design and develop security solutions for a given application or system	3, 6, 7, 12
3. Apply Authentication algorithms for Security	1, 3, 5, 6, 9, 11
4. Ability to develop a secure network stack	1, 3, 6, 7, 12

COURSE PLAN – PART II

COURSE OVERVIEW

This course covers basic concepts of combinatorics and graph theory, focusing on ways to handle graphs, trees and networks efficiently for developing real time application using graph theory. It provides the application of theoretical concepts in various scenrios and its analysis by discussing several examples.

COURSE TEACHING AND LEARNING ACTIVITIES

S.No.	Week/Contact Hours	Topic	Mode of Delivery
1	16/08/2022 to 19/01/2022 3 hours	Overview of Network Security - Security services - attacks	PPT/Chalk and Talk

2	22/08/2022 to 26/01/2022 3 hours	Security Issues in TCP/IP suite - Sniffing - spoofing - buffer overflow - ARP poisoning- ICMP Exploits	PPT/Chalk and Talk
3	29/08/2022 to 02/09/2022 2 hours	IP address spoofing - IP fragment attack - routing exploits - UDP exploits - TCP exploits.	PPT/Chalk and Talk
4	05/09/2022 to 09/09/2022 3 hours	Authentication requirements - Authentication functions - Message Authentication Codes	PPT/Chalk and Talk
5	12/09/2022 to 16/09/2022 3 hours	Hash Functions - Security of Hash Functions and MACs	PPT/Chalk and Talk
6	19/09/2022 to 23/09/2022 1 hour	**Cycle Test 1**	**Written**
7	26/09/2022 to 30/09/2022 2 hours	MD5 message Digest algorithm - Secure Hash Algorithm	PPT/Chalk and Talk
8	26/09/2022 to 30/09/2022 1 hour	RIPEMD - HMAC Digital Signatures -	PPT/Chalk and Talk
9	03/10/2022 to 07/10/2022 2 hours	Authentication protocols - Kerberos - X.509.	PPT/Chalk and Talk
10	10/10/2022 to 14/10/2022 3 hours	IP Security - AH and ESP - SSL/TLS - SSH - Web Securi ty- HTTPS	PPT/Chalk and Talk
11	17/10/2022 to 21/10/2022 3 hours	DNS Security - Electronic Mail Security (PGP - S/MIME).*	PPT/Chalk and Talk
12	25/10/2022 to 28/10/2022 2 hours	Intruders - Viruses - Worms	PPT/Chalk and Talk
13	31/10/2022 to 02/11/2022 3 hours	Trojan horses - Distributed Denial-Of-Service (DDoS)- Firewalls	PPT/Chalk and Talk
14	07/11/2022 to 11/11/2022 2 hours	IDS - Honey nets - Honey pots.	PPT/Chalk and Talk

15	14/11/2022 to 18/11/2022 2 hours	Introduction to wireless network security - Risks and Threats of Wireless networks	PPT/Chalk and Talk
16	14/11/2022 to 18/11/2022 1 hour	**Assignment 2/Quiz**	
17	21/11/2022 to 25/11/2022 2 hours	Wireless LAN Security (WEP - WPA).	PPT/Chalk and Talk
18	21/11/2022 to 25/11/2022 1 hour	**Cycle Test 2**	**Written**
19	28/11/2022 to 30/11/2022 3 hours	Research Papers	PPT/Chalk and Talk

COURSE ASSESSMENT METHODS (shall range from 4 to 6)

S.No.	Mode of Assessment	Week/Date	Duration	% Weightage
1	Cycle Test 1	19/09/2022 to 23/09/2022	1 hour	20
2	Cycle Test 2	21/11/2022 to 25/11/2022	1 hour	20
3	Assignment 1	12/09/2022 to 16/09/2022	--	10
4	Assignment 2/Quiz	14/11/2022 to 18/11/2022	--	10
CPA	Compensation Assessment*	As per academic schedule	1 hour	20
5	Final Assessment *	As per academic schedule	3 hours	40

***mandatory; refer to guidelines on page 4**

COURSE EXIT SURVEY

1. Students' feedback through class committee meetings
2. Feedbacks are collected before final examination through MIS or any other standard format followed by the institute
3. Students, through their Class Representatives, may give their feedback at any time to the course faculty which will be duly addressed.

COURSE POLICY (preferred mode of correspondence with students, compensation assessment policy to be specified)

MODE OF CORRESPONDENCE (email/ phone etc)

Email/ Phone, in-person – after 4.00 pm.

COMPENSATION ASSESSMENT POLICY

1. One compensation assessment will be given after completion of Cycle Test 1 and 2 for the students those who are absent for any assessment due to genuine reason.
2. Compensatory assessments would cover the syllabus of Cycle tests 1 & 2.
3. Prior permission and required documents must be submitted for absence.

ATTENDANCE POLICY (A uniform attendance policy as specified below shall be followed)

- At least 75% attendance in each course is mandatory.
- A maximum of 10% shall be allowed under On Duty (OD) category.

Students with less than 65% of attendance shall be prevented from writing the final assessment and shall be awarded 'V' grade.

ACADEMIC DISHONESTY & PLAGIARISM

- Possessing a mobile phone, carrying bits of paper, talking to other students, copying from others during an assessment will be treated as punishable dishonesty.
- Zero mark to be awarded for the offenders. For copying from another student, both students get the same penalty of zero mark.
- The departmental disciplinary committee including the course faculty member, PAC chairperson and the HoD, as members shall verify the facts of the malpractice and award the punishment if the student is found guilty. The report shall be submitted to the Academic office.

The above policy against academic dishonesty shall be applicable for all the programmes.

ADDITIONAL INFORMATION, IF ANY

1. The Course Coordinator is available for consultation during the time intimated to the students then and there.
2. Relative grading adhering to the instructions from the office of the Dean (Academic) will be adopted for the course.

FOR APPROVAL

Kamalika Bhattacharjee

Course Faculty: _____ **CC- Chairperson:** _____ **HOD:** _____ 22/8/2022