NATIONAL INSTITUTE OF TECHNOLOGY, TIRUCHIRAPPALLI

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

COURSE PLAN – PART I			
Name of the programme and specialization	B.Tech		
Course Title	Network Security		
Course Code	CSHO22	No. of Credits	03
Course Code of Pre-requisite subject(s)	-	Semester	VIII
Session	Jan 2020	Section (if, applicable)	A & B
Name of Faculty	Mrs.A.Lavanya Mathiyalagi	Department	CSE
Official Email	lavanyaa@nitt.edu	Telephone No.	0431 2502202
Name of Course Coordinator(s) (if, applicable)	-		
Official E-mail	-	Telephone No.	-
Course Type (please tick appropriately)	Core course	✓ Elective course	

Syllabus (approved in Senate)

Unit -I

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

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

Unit-IV

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

Unit-V

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

NATIONAL INSTITUTE OF TECHNOLOGY, TIRUCHIRAPPALLI

COURSE OBJECTIVES

- To understand the network security, services, attacks, mechanisms, types of attacks
- To comprehend and apply authentication services, authentication algorithms
- 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.To understand the network security, services, attacks, mechanisms, types of attacks	PO1,PO5,PO6
2.To comprehend and apply authentication services, authentication algorithms	PO3,PO5
3.To comprehend and apply network layer security protocols, Transport layer security protocols, Web security protocols.	PO1,PO3,PO5,PO6

COURSE PLAN – PART II

COURSE OVERVIEW

- This course emphasizes about network attacks and vulnerabilities as well as current defenses and mechanisms for protecting the network.
- This course covers the security solutions,authentication services, authentication algorithms.
- This course provides an overview on network layer, security protocols,we security protocols.

COURSE TEACHING AND LEARNING ACTIVITIES

S.No.	Week/Contact Hours	Topic	Mode of Delivery
1	Week 1	Overview of Network Security, Security services	L,C&T,Presentation
2	Week 1	Types of attacks with example	L,C&T,Presentation
3	Week 1	Security Issues in TCP/IP suite-Sniffing	L,C&T,Presentation
4	Week 2	spoofing, buffer overflow, ARP poisoning	L,C&T,Presentation
5	Week 2	ICMP Exploits, IP address spoofing, IP fragment attack, routing exploits,	L,C&T,Presentation
6	Week 2	UDP exploits, TCP exploits	L,C&T,Presentation
7	Week 3	Authentication requirements, Authentication functions	L,C&T,Presentation
8	Week 3	Message Authentication Codes - Hash Functions - Security of Hash Functions and MACs	L,C&T,Presentation
9	Week 3	MD5 message Digest algorithm	L,C&T,Presentation

10	Week 4	Secure Hash Algorithm I, 512	L,C&T,Presentation
11	Week 4	RIPEMD algorithm with implementation	L,C&T,Presentation
12	Week 4	HMAC Digital Signatures	L,C&T,Presentation
13	Week 5	Authentication protocol Kerberos	L,C&T,Presentation
14	Week 5	Authentication protocol X.509	L,C&T,Presentation
15	Week 5	IP Security	L,C&T,Presentation
16	Week 6	AH and ESP	L,C&T,Presentation
17	Week 6	SSL/TLS, SSH	L,C&T,Presentation
18	Week 6	Web Security-HTTPS	L,C&T,Presentation
19	Week 7	DNS Security, Electronic Mail Security	L,C&T,Presentation
20	Week 7	PGP, S/MIME	L,C&T,Presentation
21	Week 7	Intruders, Viruses	L,C&T,Presentation
22	Week 8	Worms, Trojan horses	L,C&T,Presentation
23	Week 8	Distributed Denial-Of-Service (DDoS)	L,C&T,Presentation
24	Week 8	Firewalls,IDS	L,C&T,Presentation
25	Week 9	Honey nets, Honey pots	L,C&T,Presentation
26	Week 9	Introduction to wireless network security	L,C&T,Presentation
27	Week 9	Risks and Threats of Wireless networks	L,C&T,Presentation
28	Week 10	Wireless LAN Security	L,C&T,Presentation
29	Week 10	WEP,WPA	L,C&T,Presentation
30	Week 10	Substitution techniques	L,C&T,Presentation
31	Week 11	Transposition techniques	L,C&T,Presentation

32	Week 11	DES implementation	L,C&T,Presentation
33	Week 11	Modular arithmetic-Euclid"s algorithm	L,C&T,Presentation
34	Week 12	AES implementation	L,C&T,Presentation
35	Week 12	RSA Algorithm	L,C&T,Presentation
36	Week 12	Algorithm implementation	L,C&T,Presentation

COURSE ASSESSMENT METHODS

S.No.	Mode of Assessment	Week/Date	Duration	% Weightage
1	Cycle Test - 1	Feb 3rd week	1 hour	20
2	Cycle Test -2	March 4th week	1 hour	20
3	Assignment	April 1st Week	2 weeks	10
CPA	Compensation Assessment	April 2nd week	1 hour	20
4	Final Assessment *	May 1st Week	3 hours	50

***mandatory; refer to guidelines on page 6**

COURSE EXIT SURVEY

- Feedback is collected before every cycle test and after the end semester exam in the feedback forms through MIS.
- Suggestions from the students for incorporated for making the course more understanding and interesting.
- Students, through their class representative may give their feedback at any time to the course faculty which will be duly addresses.
- Students may also give their feedback during class committee meeting.

COURSE POLICY (including compensation assessment to be specified)

MODE OF CORRESPONDENCE

- Email , phone or in person

COMPENSATION ASSESSMENT

- Retest will be conducted if there is any valid reason for the absentees of cycle test.

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

- The students can clear their doubts during working hours.

FOR APPROVAL

Course Faculty	CC- Chairperson	HOD
A.	25/2/20	25/2/2020

Guidelines

a) The number of assessments for any theory course shall range from 4 to 6.

b) Every theory course shall have a final assessment on the entire syllabus with at least 30% weightage.

c) One compensation assessment for absentees in assessments (other than final assessment) is mandatory. Only genuine cases of absence shall be considered.

d) The passing minimum shall be as per the regulations.

B.Tech. Admitted in				P.G.
2018	2017	2016	2015	
35% or (Class average/2) whichever is greater.		(Peak/3) or (Class Average/2) whichever is lower		40%

e) Attendance policy and the policy on academic dishonesty & plagiarism by students are uniform for all the courses.

f) Absolute grading policy shall be incorporated if the number of students per course is less than 10.

g) Necessary care shall be taken to ensure that the course plan is reasonable and is objective.