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	**CSOE16**	**No. of Credits**	**03**
Course Code of Pre-requisite subject(s)	**CSMI17**		
Session	**January 2021**	**Section (if, applicable)**	
Name of Faculty	**Dr. M. Sai Krishna**	**Department**	**CSE**
Email	**saikrishna@nitt.edu**	**Telephone No.**	**9885648901**
Name of Course Coordinator(s) (if, applicable)	**NIL**		
E-mail	**NIL**	**Telephone No.**	**NIL**
Course Type	**Open Elective course**		

Syllabus (approved in BoS)

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).*

*Programming assignments are mandatory.

Text Books

1. W. Stallings, “Cryptography and Network Security: Principles and Practice”, 5/E, Prentice Hall, 2013
2. Yang Xiao and Yi Pan, “Security in Distributed and Networking Systems”, World Scientific, 2007, Chapter 1.

3. Aaron E. Earle, “Wireless Security Handbook”, Auerbach publications, Taylor & Francis Group, 2006.

Reference Books

1. AtulKahate, “Cryptography and Network Security”, Tata McGraw-Hill, 2003

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.

COURSE OUTCOMES (CO)

Course Outcomes	**Aligned Programme Outcomes (PO)**
1. Ability to determine appropriate mechanisms for protecting the network	**1,5,6**
2. Ability to design and develop security solutions for a given application or system	**3,5**
3. Ability to develop a secure network stack	**1,3,5,6**

COURSE PLAN – PART II

COURSE OVERVIEW

This course mainly describes the network attacks, vulneratbilities and mechanisms for protecting the network.The course also covers the security solutions, authentication services and algorithms. It introduces the wireless network security and threats of wireless networks.

COURSE TEACHING AND LEARNING ACTIVITIES

S.No.	**Week/Contact Hours**	**Topic**	**Mode of Delivery**
1	19/01/2021 to 22/01/2021 1 hour	Unit –I Introduction	PPT and MS Teams
2	19/01/2021 to 22/01/2021 1 hour	Overview of Network Security	PPT and MS Teams
3	19/01/2021 to 22/01/2021 1 hour	Security services	PPT and MS Teams
4	25/01/2021 to 29/01/2021 1 hour	attacks	PPT and MS Teams

5	25/01/2021 to 29/01/2021 1 hour	Security Issues in TCP/IP suite-Sniffing,	PPT and MS Teams
6	25/01/2021 to 29/01/2021 1 hour	Security Issues in TCP/IP suite-Sniffing,	PPT and MS Teams
7	01/02/2021 to 05/02/2021 1 hour	spoofing	PPT and MS Teams
8	01/02/2021 to 05/02/2021 1 hour	buffer overflow	PPT and MS Teams
9	01/02/2021 to 05/02/2021 1 hour	ARP poisoning	PPT and MS Teams
10	08/02/2021 to 12/02/2021 1 hour	ICMP Exploits	PPT and MS Teams
11	08/02/2021 to 12/02/2021 1 hour	IP address spoofing, IP fragment attack	PPT and open board
12	08/02/2021 to 12/02/2021 1 hour	routing exploits	PPT and MS Teams
13	15/02/2021 to 19/02/2021 1 hour	UDP exploits, TCP exploits	PPT and MS Teams
14	15/02/2021 to 19/02/2021 1 hour	Unit-II Authentication requirements	PPT and MS Teams
15	15/02/2021 to 19/02/2021 1 hour	Authentication functions, Message Authentication Codes	PPT and MS Teams
16	22/02/2021 to 26/02/2021 1 hour	Hash Functions, Security of Hash Functions and MACs	PPT and MS Teams
17	22/02/2021 to 26/02/2021 1 hour	MD5 message Digest algorithm, Secure Hash Algorithm	PPT and MS Teams

18	22/02/2021 to 26/02/2021 1 hour	**First Assessment**	PPT and MS Teams
19	01/03/2021 to 05/03/2021 1 hour	RIPEMD - HMAC Digital Signatures,	PPT and open board
20	01/03/2021 to 05/03/2021 1 hour	Authentication protocols-Kerberos, X.509	PPT and MS Teams
21	01/03/2021 to 05/03/2021 1 hour	Unit-III	PPT and MS Teams
22	08/03/2021 to 12/03/2021 1 hour	IP Security	PPT and MS Teams
23	08/03/2021 to 12/03/2021 1 hour	AH and ESP	PPT and MS Teams
24	08/03/2021 to 12/03/2021 1 hour	SSL/TLS	PPT and MS Teams
25	15/03/2021 to 19/03/2021 1 hour	SSH	PPT and MS Teams
26	15/03/2021 to 19/03/2021 1 hour	Web Security-HTTPS	PPT and MS Teams
27	15/03/2021 to 19/03/2021 1 hour	DNS Security	PPT and MS Teams
28	22/03/2021 to 26/03/2021 1 hour	Electronic Mail Security (PGP, S/MIME)	PPT and MS Teams
29	22/03/2021 to 26/03/2021 1 hour	**Second Assessment**	PPT and MS Teams
30	22/03/2021 to 26/03/2021 1 hour	Unit-IV	PPT and MS Teams

31	30/03/2021 to 02/04/2021 1 hour	Intruders	PPT and MS Teams
32	30/03/2021 to 02/04/2021 1 hour	Viruses	PPT and MS Teams
33	30/03/2021 to 02/04/2021 1 hour	Worms	PPT and MS Teams
34	05/04/2021 to 09/04/2021 1 hour	Trojan horses	PPT and MS Teams
35	05/04/2021 to 09/04/2021 1 hour	Distributed Denial-Of-Service (DDoS)	PPT and MS Teams
36	05/04/2021 to 09/04/2021 1 hour	Firewalls	PPT and MS Teams
37	12/04/2021 to 16/04/2021 1 hour	IDS	PPT and MS Teams
38	12/04/2021 to 16/04/2021 1 hour	Honey nets	PPT and MS Teams
39	12/04/2021 to 16/04/2021 1 hour	Honey pots	PPT and MS Teams
40	19/04/2021 to 23/04/2021 1 hour	Unit-V Introduction	PPT and MS Teams
41	19/04/2021 to 23/04/2021 1 hour	wireless network security	PPT and MS Teams
42	19/04/2021 to 23/04/2021 1 hour	wireless network security	PPT and MS Teams
43	26/04/2021 to 30/04/2021 1 hour	Risks and Threats of Wireless networks	PPT and MS Teams

44	26/04/2021 to 30/04/2021 1 hour	Risks and Threats of Wireless networks	PPT and MS Teams
45	26/04/2021 to 30/04/2021 1 hour	Wireless LAN Security (WEP, WPA)	PPT and MS Teams
46	03/05/2021 to 07/05/2021 1 hour	**Compensation Assessment**	PPT and MS Teams
47	03/05/2021 to 07/05/2021 1 hour	Wireless LAN Security (WEP, WPA)	PPT and MS Teams
48	03/05/2021 to 07/05/2021 1 hour	Wireless LAN Security (WEP, WPA)	PPT and MS Teams

COURSE ASSESSMENT METHODS (shall range from 4 to 6)

S.No.	Mode of Assessment	Week/Date	Duration	% Weightage
1	First Assesment	As per Academic schedule	1 hour	20
2	Second Assesment		1 hour	20
3	Programming Assginment	FEB 3rd Week	-	15
4	Quiz	APRIL 3rd Week	-	15
CPA	Compensation Assessment*	As per Academic schedule	1 hour	20
5	Final Assessment *		2 hours	30

COURSE EXIT SURVEY (mention the ways in which the feedback about the course shall be assessed)

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)

Through Email

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. The 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

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

M. Saikrishna

Course Faculty __________ **CC-Chairperson** ________________ **HOD** ____________