



SCHOOL OF COMPUTING
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
REVISION CARRIED OUT -2017-2018
2018-EVEN

Red color- content deleted

Yellow color-Content added

SCS1309	NETWORK SECURITY	L	T	P	Credits	Total Marks
		3	1	0	4	100

Unit 1 Introduction 12Hrs.

Services-Mechanisms and attacks- the OSI Security architecture – A model for network security –Classical encryption Technique –Symmetric cipher model-Substitution techniques –Steganography

Unit II BLOCK CIPHER AND PUBLIC KEY ENCRYPTION AND KEY MANAGEMENT 12Hrs.

Simplified DES- Block cipher principles- The data Encryption standarad- The strength of DES- Confidentiality using symmetric encryption –Placement of encryption – Traffic Confidentiality- key, introduction to number theory- public key cryptography and RSA- Key management-Diffie –hellman key exchange

Unit III THREATS IN NETWORKS 12Hrs.

Intruder - Intrusion detection system- Rule based Detection- Statistical anamoly Detection-Password Management-Password Protection-Vulnerability of password- Virus and related threats- Counter measures- firewalls-Firewalls design principles-trusted systems.

Unit IV NETWORK SECURITY DESIGN 12Hrs.

Hacking –Vulnerabilities –Design Issues- Human Issues- Implementation issues- Threats- Reconnaissance Attacks- Access Attacks- Information Disclosure Attacks- Denial of Service Attacks- Threat defense-Secure communication- Network Security Best Practices- SAFE Campus Design

Unit V E-MAIL, IP & WEB SECURITY 12Hrs.

E-mail security: Security Services- Pretty Good Privacy- S/MIME, IPSecurity: Overview of IPsec- IP Sec Architecture- IP and IPV6-Authentication Header- Encapsulation Security Payload(ESP)- Internet Key Exchange(Phase of IKE, ISAKMP/IKE Encoding). Web Security: SSI/TLS Basic protocol- computing the keys- Client authentication – PKI as deployed by SSL Attacks fixed in v3- Exportability – Encoding- Secure Electronic transaction(SET) 60 Hrs

TEXT / REFERENCE BOOKS

1. William Stallings, Cryptography and Network Security, 6th Edition, Pearson Education, March 2013.
2. Diane Tiare and Catherine Paquet, "Campus Network Design Fundamentals", Pearson Education, 2006.
3. William Stallings, "Network Security Essentials : Applications and Standards", Fourth Edition, Pearson Education.

END SEMESTER EXAM QUESTION PAPER PATTERN

Max. Marks : 100

Exam Duration : 3 Hrs.

PART A : 10 questions of 2 marks each- No choice

20 Marks

PART B : 2 questions from each unit of internal choice, each carrying 16 marks

80 Marks

SCS1309	NETWORK SECURITY	L	T	P	Credits	Total Marks
		3	1	0	4	100

UNIT 1 NETWORK SECURITY DESIGN

12 Hrs.

Hacking - Vulnerabilities - Design Issues - Human Issues - Implementation Issues - Threats - Reconnaissance Attacks - Access Attacks - Information Disclosure Attacks - Denial of Service Attacks - Threat Defense - Secure Communication - Network Security Best Practices - SAFE Campus Design.

UNIT 2 THREATS IN NETWORKS

12Hrs.

Network Security Controls - Firewalls - Intrusion Detection Systems - Secure Email - Intruder - Intrusion detection system - Virus and related threats - Countermeasures - Firewalls design principles - Trusted systems

UNIT 3 SECURITY PRACTICE

12 Hrs.

X.509 Authentication services - E-mail security - IP security - Web security - Network perimeter security - Secured router configuration - Firewall - Design principle - Trusted systems - VPN - IDS - IPS penetration testing - NAT - Implementation of cryptography and security

UNIT 4 NETWORK SECURITY PROTOCOLS

12Hrs.

SSH - RADIUS - SSL - Kerberos - TLS - IPSec - Voice over IP - IPSEC - X.509 Authentication service - Electronic mail security S/MIME - Application security - SSL - PGP - SET.

UNIT 5 SECURITY SERVICES

12Hrs.

Computer Forensics and Cyber Laws - Data Recovery - Security Policies and Procedures - Security Lifestyle Management - Security Audit - Managed Security Services

Max. 60 Hours

COURSE OUTCOMES

On completion of the course, student will be able to

CO1 : Comprehend type of attacks and network security violations.

CO2 : Apply ciphering techniques to secure data transfer

CO3 : Analyse authentication techniques for different network scenarios..

CO4 : Design Internet Protocol Security architecture to identify the vulnerability of the Internet systems..

CO5 : Develop an intrusion detection system to find the attacks in networks.

CO6 : Conduct a case study on recent threats and attacks.

TEXT / REFERENCE BOOKS

1. William Stallings, Cryptography and Network Security, 6th Edition, Pearson Education, March 2013.
2. Behrouz A. Forouzan, Debdeep Mukhopadhyay, Cryptography and Network Security, 2nd edition, McGraw Hill, 2012 .
3. William Stallings, "Network Security Essentials : Applications and Standards", Fourth Edition, Pearson Education.

END SEMESTER EXAM QUESTION PAPER PATTERN

Max. Marks : 100

Exam Duration : 3 Hrs.

PART A : 10 questions of 2 marks each- No choice

20 Marks

PART B : 2 questions from each unit of internal choice, each carrying 16 marks

80 Marks