CSE4151: Network Security

Programme: B.Tech. (CSE)	Year: 4th year	Semester: 7th
Course: Program Elective	Credits: 03	Hours: 40

Course Context and Overview (100 words):

Network Security is concerned to introduce the students to the security aspects of computer networks. The goal of this course is to provide the students adequate foundation to apply cryptographic and other security technique to emerging area of information and network security.

Prerequisites Courses: Computer Networks

Course Outcomes (COs):

On completion of this course, the students will have the ability to:
CO1: Understand existing security threats against computer systems.
CO2: Understand concepts of symmetric and asymmetric encryption.
CO3: Understand concepts of Kerberos and X.509 Authentication service.
CO4: Analyse and detect malicious code and network defences against them using firewall and Intrusion Detection system.
CO5: Understand and apply IP Security and Web security.

Course Topics:

Contents	Lecture Hours	
UNIT – 1 Basis of Network Security Concepts		2
1.1 Threats, Attacks, and Assets	1	
1.2 Security Functional Requirements (Confidentiality, integrity, availability, authentication, security objectives and types of attacks.	1	
UNIT –2 Encryption		7
2.1 **Classical Encryption:** Symmetric cipher models, Vigenere cipher, stream ciphers	1	
2.2 ***Block Ciphers:*** Substitution and permutation networks (SPN), Feistel structure, description of Data Encryption Standard (DES), Double and triple DES.	2	

2.3 Advanced Encryption Standard (AES). Linear and differential attacks on block ciphers	2	
2.4. ***Public-Key Encryption (RSA)***: Principles of public key cryptosystems, RSA. Testing primality, Chinese Remainder Theorem (CRT)	2	
3 **UNIT-3 Hash Functions**		
3.1 Security of hash functions	1	5
3.2 Merkel Damgard iterative construction.	1	
3.3 Message Authentication and hash functions.	1	
3.6 Authentication Application: Kerberos. X.509 Authentication service.	2	
UNIT-4 Malicious code and network defenses		7
4.1 Trojan horses, viruses and worms,	2	
4.2 Denial-of-Service Attacks; Flooding Attacks; Distributed Denial-of-Service Attacks;	2	
4.3 Application-Based Bandwidth Attacks	1	
4.4 Defenses Against Denial-of-Service Attacks; Responding to a Denial-of-Service Attack.	2	
4 **UNIT-5 Intrusion Detection and Prevention System**		6
5.1 Intrusion Detection; Host-Based Intrusion Detection.	1	
5.2 Distributed Host-Based Intrusion Detection; Network-Based Intrusion Detection.	1	
5.3 Need for Firewalls; Firewall Characteristics; Types of Firewalls; Firewall Location and Configurations;	2	
5.4 Intrusion Prevention Systems and Honeypots	2	
Unit -6 Electronic Mail Security		4
6.1 Pretty Good Privacy (PGP)	2	
6.2 S/MIME	2	
Unit -7 Transport Layer Security		5
7.1 Web Security Issues	1	
7.2 Secure Socket Layer (SSL)	2	
7.3 Transport Layer Security (TLS)	2	
Unit -8 IP Security		4
8.1 IP security overview & architecture	1	
8.2 Encapsulating Security Policy	2	
8.3 Internet Key Exchange	1	

Suggested Reading: Reference Books / Journals:

Text Book:

1. Stallings W., "*Cryptography and Network Security"*, 4/E, Pearson Education India. 2006
2. Forouzan, B.A., "*Cryptography and Network Security"*, Tata McGraw-Hill. 2007

Reference books:

1. Paar, C., "*Understanding Cryptography* ", 1/E, Springer 2009
2. Pieprzyk J., Hardjono T. and Seberry J. "*Fundamentals of Computer Security"*, Springer (International Edition) (First Indian reprint 2008) 2003

Additional Resources (Web resources etc.):

Evaluation Methods:

Evaluation criteria will be shared by the concerned course instructor.

Prepared By: Poonam Gera
Last Update: 30/4/2019