

COURSE TITLE : **INFORMATION SECURITY**
COURSE CODE : **5136**
COURSE CATEGORY : **ELECTIVE**
PERIODS/WEEK : **4**
PERIODS/SEMESTER : **52**
CREDITS : **4**

TIME SCHEDULE

MODULE	TOPICS	PERIODS
1	Introduction to Computer Security & Cryptography	13
2	User Authentication & Access Control	13
3	Intrusion Detection and Malicious Software	13
4	Denial of Service and Firewall	13

Course General Outcomes:

Sl.	G.O	On completion of this course the student will be able :
1	1	Understand concepts of computer security
	2	Understand cryptographic tools
2	1	Understand user authentication
	2	Study authentication methods
	3	Understand access control in computer security
3	1	Understand intrusion and its detection methods
	2	Understand malicious software
4	1	Understand Denial of service
	2	Understand Firewall

Specific Outcome:

MODULE I: Introduction to computer Security & Cryptography

- 1.1 To understand the concept of Computer Security
 - 1.1.1 Define computer Security.
 - 1.1.2 Explain Computer Security triad: Confidentiality, Integrity, Availability.
 - 1.1.3 Explain the terminologies: Authenticity, accountability.
 - 1.1.4. Explain the Model of Computer Security, Security concepts and relationships.
 - 1.1.4. Differentiate Threats and Attacks & Threats and Assets.
 - 1.1.5 Explain various Security aspects in Communication Lines and Networks.
 - 1.1.6 List security functional requirements.
 - 1.1.7 Explain Security architecture for OSI.
 - 1.1.8 Explain the Scope of Computer and Network Security with block diagram.
 - 1.1.9. Discuss three aspects of computer security strategy.
- 1.2 To Comprehend Cryptographic Tools
 - 1.2.1 Explain simplified model of symmetric encryption with block diagram.
 - 1.2.3 Explain Symmetric block encryption algorithms.
 - 1.2.3 Explain block and Stream Cipher encryption.
 - 1.2.4 Explain message authentication with symmetric encryption
 - 1.2.5 Describe message authentication without message encryption.
 - 1.2.6 Explain message authentication with message authentication code (MAC) using figure.
 - 1.2.7 Describe message authentication with one way hash functions
 - 1.2.8 Explain Public key cryptography
 - 1.2.9. Explain digital signature, public key certificates and Symmetric key exchange using public key encryption
 - 1.2.10 Explain the use of Random numbers in encryption
 - 1.2.11 Define pseudorandom numbers

MODULE II: User Authentication and Access Control

- 2.1 To understand User Authentication
 - 2.1.1 Define User Authentication
 - 2.1.2 Explain the means of authentication
 - 2.1.3 Describe Password based Authentication
 - 2.1.4 Explain Password attack strategies and countermeasures
 - 2.1.5 Explain the use of hashed passwords
 - 2.1.5 Explain the password cracking approaches and user password choices
 - 2.1.6 Explain password File access control
 - 2.1.7 Illustrate various password selection strategies
- 2.2 To Understand Various Authentication Methods
 - 2.2.1 Explain Token based authentication
 - 2.2.2 Explain Biometric Authentication
 - 2.2.3 Explain various physical characteristics used in biometric applications
 - 2.2.4 Explain the operation of a biometric authentication system
 - 2.2.5 Explain the biometric accuracy
 - 2.2.6 Discuss Remote User Authentication
 - 2.2.7 Explain various security issues for user authentication
- 2.3 To understand Access control in computer security
 - 2.3.1 Discuss Access Control Principles – Relationship among other security functions
 - 2.3.2 Explain various access control policies

- 2.3.3 Discuss various access control requirements
- 2.3.4 Explain the various basic elements of Access control: subject, object and Access right
- 2.3.5 Illustrate the UNIX File Access Control

MODULE III: Intrusion Detection & Malicious Software

3.1 To Know Intrusion and Detection

- 3.1.1 List various classes of intruders and the intruder behavior patterns.
- 3.1.2 Explain the Intrusion Detection System classification and the requirements of IDS.
- 3.1.3 Explain Host based Intrusion detection
- 3.1.4 Explain the relevance of audit records, anomaly detection, and signature detection
- 3.1.5 Explain Distributed host based intrusion detection
- 3.1.6 Discuss Network based intrusion detection
- 3.1.7 Discuss Intrusion Detection Exchange Format
- 3.1.8 Explain the functioning of Honey pots
- 3.1.9 Explain the functioning of SNORT IDS – Architecture and rules

3.2 To Study about Malicious Software

- 3.2.1 Explain various types of Malicious Software
- 3.2.2 Discuss Viruses – The nature of viruses, Virus structure, Virus classification
- 3.2.3 Explain various Antivirus approaches & Antivirus techniques
- 3.2.4 Describe Study Worms- Worm propagation model, requirements for Worm Countermeasures
- 3.2.5 Discuss BOT and RCF
- 3.2.6 Discuss about Constructing the Attack Network
- 3.2.7 Explain ROOTKIT functions, classifications, installation

MODULE IV: Denial of Service and Firewall

4.1 To Understand Denial of Service

- 4.1.1 Define a Denial of Service (DoS)
- 4.1.2 Explain the effect of DoS on Network bandwidth, System resources and Application resources
- 4.1.3 Explain classic Denial of Service Attacks
- 4.1.4 Discuss about Source Address Spoofing
- 4.1.5 Explain the SYN Spoofing
- 4.1.6 Explain Flooding Attacks- ICMP Flood, UDP Flood, TCP SYN Flood
- 4.1.7 Explain the Distributed Denial of Service Attacks, and DDoS attack architecture
- 4.1.8 Discuss the Reflector and Amplifier attacks
- 4.1.9 Explain defenses against DoS Attacks, and how to respond to DoS Attacks

4.2. To Understand Firewall

- 4.2.1 List the need for firewall
- 4.2.2 List various characteristics of a Firewall
- 4.2.3 Discuss various types of firewalls:
- 4.2.4 Illustrate Bastion Host, Host based firewalls and Personal firewalls
- 4.2.5 Explain Internal and external Firewall Configuration
- 4.2.6 Explain Distributed Firewalls

CONTENT DETAILS

MODULE I : Introduction to Computer Security & Cryptography

Computer Security : Definition – Triad – Authenticity, Accountability – Model – Security concepts – relationships – Threats , Attack, Assets – Security aspects in communication lines and networks – Security requirements – OSI architecture – Scope – Strategy.

Cryptography : Symmetric encryption – Algorithms – Block and Stream Cipher encryption – Message authentication – MAC – One way Hash Function – Public key cryptography – digital signature – public key exchange – symmetric key exchange – Random numbers in encryption – pseudorandom numbers

MODULE II : User Authentication and Access Control

User Authentication: means of authentication - Password based Authentication - Password attack strategies and countermeasures - hashed passwords - password cracking - user password choices - password File access control - password selection.

Authentication Methods: Token based authentication - Biometric Authentication - physical characteristics in biometric applications - operation – accuracy - Remote User Authentication - security issues

Access control: Principles – Relationship among other security functions - access control policies - access control requirements - basic elements of Access control: subject, object and Access right - UNIX File Access Control

MODULE III : Intrusion Detection & Malicious Software

Intrusion and Detection: Classes of intruders - Intruder behavior patterns - classification - requirements of IDS - Host based Intrusion detection - audit records - anomaly detection - signature detection - Distributed host based intrusion detection - Network based intrusion detection - Intrusion Detection Exchange Format - Honey pots - SNORT IDS – Architecture and rules

Malicious Software: Different types - Viruses – nature - Virus structure – Classification - Antivirus approaches - Antivirus techniques – Worms - Propagation model - Worm Countermeasures - BOT – Uses - RCF, Attack Network - ROOTKIT – functions – classifications – installation.

MODULE IV : Denial of Service and Firewall

Denial of Service: Definition - Effect of DoS on Network bandwidth - System resources - Application resources - Classic Denial of Service Attacks - Source Address Spoofing - SYN Spoofing - Flooding Attacks - ICMP Flood - UDP Flood - TCP SYN Flood - Distributed Denial of Service Attacks - DoS attack architecture - Reflector and Amplifier attacks - Defenses against DoS Attacks – Response to DoS Attacks

Firewall: Need - Characteristics - Packet filtering - Stateful inspection - Application level - Circuit level gateway - Bastion Host - Host based firewalls - Personal firewalls - Internal and external Firewall Configuration - Distributed Firewalls

TEXT BOOK:

1. Computer Security- Principles and Practice - Author: William Stallings & Lawrie Brown
Publisher: Pearson Prentice Hall 2010

REFERENCE BOOKS:

1. Cryptography and Security - Author: C K Chyamala, N Harini & Dr T R Padmanabhan
Publisher: Wiley – India 2010
2. Network Security – [M.V. Arun Kumar](#), USP2011 First Edition