2/3 MCA Second Semester

CA4T2 INFORMATION SECURITY Credits : 4

Lecture Hours : 4 periods / week Internal assessment : 30 Marks
Semester and Examination: 70 Marks

Course Description:

This course introduces the concepts and issues related to securing information systems and the development of policies to implement information security controls. Topics include the historical view of networking and security, security issues, trends, security resources, and the role of policy, people, and processes in information security. Upon completion, students should be able to identify information security risks, create an information security policy, and identify processes to implement and enforce policy.

Course Objective:

- Develops an understanding of information assurance as practiced in computer operating systems, distributed systems, networks and representative applications.
- Gain familiarity with prevalent network and distributed system attacks, defenses against them, and forensics to investigate the aftermath.

- Develops a basic understanding of cryptography, how it has evolved, and some key encryption techniques used today.
- Develops an understanding of security policies (such as authentication, integrity and confidentiality), as well as protocols to implement such policies in the form of message exchanges.
- Develops an understanding of SNMP and Firewalls.

UNIT-I

Security Attacks: (Interruption, Interception, Modification and Fabrication), Security Services (Confidentiality, Authentication, Integrity, Non-repudiation, access Control and Availability) and Mechanisms, A model for Internetwork security, Internet Standards and RFCs, Buffer overflow & format string vulnerabilities, TCP session hijacking, ARP attacks, route table modification, UDP hijacking, and man-in-the-middle attacks.

UNIT-II

Conventional Encryption: Principles, Conventional encryption algorithms, cipher block modes of operation, location of encryption devices, key distribution Approaches of Message Authentication, Secure Hash Functions and HMAC,

UNIT-III

Cryptography: Public key cryptography principles, public key cryptography algorithms, digital signatures, digital Certificates, Certificate Authority and key management Kerberos, X.509 Directory Authentication Service

UNIT-IV

Email privacy: Pretty Good Privacy (PGP) and S/MIME.

UNIT-V

IP Security Overview: IP Security Architecture, Authentication Header, Encapsulating Security Payload, Combining Security Associations and Key Management

UNIT-VI

Web Security Requirements: Secure Socket Layer (SSL) and Transport Layer Security (TLS), Secure Electronic Transaction (SET)

UNIT-VII

SNMP: Basic concepts of SNMP, SNMPv1 Community facility and SNMPv3, Intruders, Viruses and related threats

UNIT-VIII

Firewalls: Firewall Design principles, Trusted Systems, Intrusion Detection Systems

Learning Resources

Text Books:

1. Network Security Essentials (Applications and Standards) by William Stallings Pearson Education.3rd edition, 2009.
2. Hack Proofing your network by Ryan Russell, Dan Kaminsky, Rain Forest Puppy, Joe Grand, David Ahmad, Hal Flynn Ido Dubrawsky, Steve W.Manzuik and Ryan Permeh, wiley Dreamtech, 2002.

Reference Books:

1. Fundamentals of Network Security by Eric Maiwald (Dreamtech press) 2008.
2. Principles of Information Security, Whitman, Thomson.4th edition, 2012.
3. Cryptography and network Security, 4th edition, William Stallings, PHI/ Pearson, 2009
4. Network Security: The complete reference, Robert Bragg, Mark Rhodes, TMH, 2002