Paper-III(MIT-303/MCA-403):Network Management and Information Security

UNIT - I

Security and Cryptographic algorithm: Need for security, principle of security, types of attacks. Cryptographic techniques : cryptography terminology, substitution techniques, transposition techniques, Symmetric and asymmetric key algorithm, possible types of attack, key range, steganography. symmetric vs asymmetric, algorithm types and modes, DES, double and triple DES, AES, comparison of various cryptographic algorithm, requirement of good cryptographic algorithm.

UNIT - II

Asymmetric cryptographic algorithm and Message Authentication: Public key cryptography principles and algorithms, RSA algorithm, Diffe-Hellman key exchange. One way hash functions, message digest, MD5, SHA1, message authentication code, Digital envelope, Digital signatures.

UNIT - III

Network Management: Management Standards and Models, configuration management, configuration database and reports, fault management, identification and isolation, protecting sensitive information, host and user authentication, structure of management information, Standard management information base, SNPv1 protocol, acounting management, performance management, network usage, matrics and quotas.

Network security: Overview of IPV4: OSI model, maximum transfer unit, IP, TCP, UDP, ICMP, ARP, RARP and DNS, ping, traceroute. Network attacks: Buffer overflow, IP scheduling, TCP session hijacking, sequence guessing. Network scanning: ICMP, TCP sweeps, basic port scans. Denial of service attacks: SYN flood, teardrop attacks, land, smurf attacks. Visual and private network topology: tunneling, IPSEC. Traffic protocols: authentication headers, ESP internet key exchange, security association PPTP, L2TP.

UNIT - IV

Web Security and Application Security: Web servers and browsers: security features, server privileges, active pages, scripting, security configuration setting for browsers, security of active content: JAVA, JAVA script, Active x, plug-ins, cookies. SSL & SET, security mail: PEM and PGP.

Firewalls: Firewall characteristics & design principles, types of firewalls, packet filtering router, application level gateway or proxy, content filters, bastion host. Firewall architectures: dual homed host, screening router, screened host, screened suvnet. Firewall logs.

UNIT - V

Instruction detection system: component of an IDS, placement of IDS components, types of IDS: network based IDS, file integrity checkers, host based IDS, IDS evaluation parameters.

Recommended book: William Stallings: Network Security Essentials