Course Curriculum for the subject of Cyber Security / Information Security

CYBER SECURITY – I *

Number of video programmes - 45
Number of e-content programmes - 45

Introduction: The Security, functionality and ease of use Triangle, Essential Terminology, Elements of Security, Difference between Penetration Testing and Ethical Hacking, Deliverables ethics and legality, Computer Crimes and Implications.

Reconnaissance: Information Gathering Methodology, Locate the Network Range, Active and Passive reconnaissance.

Scanning: Scanning, Elaboration phase, active scanning, scanning tools nmap, hping2. Enumeration, DNS Zone transfer.

Trojans and Backdoors: Effect on Business, Trojan?, Overt and Covert Channels, Working of Trojans, Different Types of Trojans, Different ways a Trojan can get into a system, Indications of a Trojan Attack, Some famous Trojans and ports used by them.

Sniffers: Definition of sniffing, How a Sniffer works?, Passive Sniffing, Active Sniffing, Ethreal tool, Man-in-the-Midle Attacks, Spoofing and Sniffing Attacks, ARP Poisoning and countermeasures.

Denial of Service: What is Denial of Service? , Goal of DoS (Denial of Service), Impact and Modes of Attack.

CYBER SECURITY – II *

Number of video programmes - 40
Number of e-content programmes - 40

Social Engineering: Social Engineering, Art of Manipulation, Human Weakness, Common Types of Social Engineering, Human Based Impersonation, Example of social engineering, Computer Based Social Engineering, Reverse Social Engineering, Policies and procedures, Security Policies-checklist.

Session Hijacking: Understanding Session Hijacking, Spoofing vs Hijacking, Steps in Session Hijacking, Types of Session Hijacking, TCP Concepts 3 Way and shake, Sequence numbers.

CRYPTOGRAPHY- I

Syllabus

Unit -1: History and overview of cryptograph

History &Timeline development, Need for security, Principles of Security, Introduction Cryptography, Encryption Terminology, Introduction Cryptography, Encryption Terminology, Meaning of Security, Attacks, Computer & Cyber Crime, Password protocols& their analysis, Key Range and Key Size, Crypto-analysis, Computer Security, Security services, Security mechanisms, Cipher Machines.

Unit -2: Classical Cryptography

Perfect secrecy and the one time pad, semantic security and Stream ciphers, Classical Cryptosystems, Shannon's Theory, Characteristics for perfect security, Limitations of perfectly secure encryption, Block and Stream ciphers, Cipher Modes, Substitution Ciphers, Mono-alphabetic Substitution and Poly-alphabetic Substitution, Polygram, Transposition Ciphers, Rail Fence, Scytale, Book cipher, Vernam cipher, Vigenere Tabluae, Playfair, Hill Cipher, Cryptanalysis of Classical Cryptosystems,

Unit -3: Attacks

Threats, Vulnerabilities, Attacks, Intrusions, Types of attacks, Internal and External Attacks, Attacks on Networks Layers, Flaws, Impersonation, Spoofing, Denial of Service, DDoS, Attacks on block ciphers, exhaustive search, time-space tradeoffs, differential & linear cryptanalysis, meet in the middle, side channels attack etc.

Unit -4: Mathematical Foundations

Probability and Information Theory, Elementary number theory, Finite fields, Arithmetic and algebraic algorithms, Algebraic Structures, Groups and subgroups, homomorphism theorems, cosets and normal subgroups, Lagrange's theorem, rings, finite fields. Graph theory, Graphs, Euler tours, planar graphs, graph colouring, Hamiltonian graphs, Euler's formula, applications of Kuratowski's theorem. Linear Algebra Functions; Linear transformations and their inverses; Properties of linear transformations; Orthogonality, Orthogonal transformations, Inner product spaces, Introduction to determinants, Eigenvectors and Eigen value , Definitions and examples of eigenvectors and eigen values; Computational methods for finding eigen vectors and eigen values; Properties of eigen vectors and eigen values; Matrix representations; Change of basis; Symmetric matrices and diagonalization. Number theory: Divisibility, gcd, prime numbers, fundamental theorem of arithmetic, Congruences, Fermat's theorem, Euler function, primality testing, solution of congruences, Chinese remainder theorem, Wilson's theorem, Congruences – Chinese Remainder theorem – Modular exponentiation – Fermat and Euler's theorem – Legendre and Jacobi symbols – Finite fields – continued fractions, Modulus Arithmetic and its Properties, Pseudo Random Permutations, Pseudo Random Functions.

Unit -5: Private/Symmetric Key Cryptography

Overview of Symmetric key Cryptography, Data Encryption Standards(DES)& its variants, Advanced Encryption Standards (AES), International Data Encryption Algorithm (IDEA), Feistel networks, RC4, RC5, Blowfish, Modes of operation of Block Ciphers, ECB, CBC, OFB, CFB, Counter modes, Uses of Secret key Cryptography.

Unit -6: Public/Asymmetric Key Cryptography

Brief history and overview, applications of Asymmetric Key Cryptography, RSA Algorithm, Diffie Hellman Algorithm, Symmetric and Asymmetric key cryptography together, Digital Signatures, DSS and Knapsack Algorithm.

Unit -7: Key Exchange Protocols

Traditional key distribution techniques, Problems with key exchange, Key distribution center, Certificate based key distribution, Key management , Key distribution centers, Public key directories, Key recovery and Kew Escrow, Public Key Infrastructure, Web of Trust, Identity, X.509 Certificates, Digital Certificates, Private Key Management, The PKIX Model, Public Key Cryptography Standards, PKI and Security, Hash functions, Key Predistribution, Blom's Scheme, Diffie-Hellman Key Predistribution, Kerberos, Diffie-Hellman Key Exchange, CCA security certificates and trust management, password-based key exchange, Secret Sharing Schemes.

Unit -8: Applications of Cryptographic Protocols

Hash Functions, Digital Signatures, One-time signatures, Rabin and ElGamal signatures schemes, Digital Signature Standard (DSS) Merkle-Damgard and Davies-Meyer, Message Authentication Codes, MACs from collision resistance, SHA and HMAC, Hash functions and message digests, Length of hash, uses, algorithms (MD2, MD4, MD5, SHS) MD2: Algorithm (Padding, checksum, passes.) MD4 and 5: algorithm (padding, stages, digest computation.) SHS: Overview, padding, Stages.

CRYPTOGRAPHY- II

Unit -9: Advanced Cryptographic Protocols

Elliptic curve based cryptography, ElGamal Encryption Algorithm, Zero knowledge interactive protocols, Formal verification, Hard problems& cryptography, NP Complete Problems, Randomness and Pseudo randomness & Testing, topics of current research

Unit -10: Communication Security

Brief introduction to ISO's OSI model TCP/IP models, Networks security control, Access control, Protection, Authentication applications – Kerberos, X.509, PKI, Electronic Mail security – PGP, PEM, S/MIME, IP security, IPSec Protocol, SSL, TLS, User Authentication, Authentication basics, Passwords, Authentication Tokens, Certificate-based Authentication, Biometric Authentication, Kerberos, Key Distribution Center , Security Handshake Pitfalls, Single Sign On (SSO) Approaches, Firewalls, Intrusion Detection Systems, The Station-to-station Protocol Network Security, Virtual Private Networks, Remote user authentication.

Unit -11: System Security

Program security, Control against program threats, Viruses, Malicious Codes, protection mechanisms, OS security, OS Security policies, characterstics, features of Secure/Trusted OS, Trust models, and their limitations, Access Control, File Protection, User Authentication, Security Policies, Databases security, DB Security requirements, Reliability and Integrity, Protecting sensitive data, Multilevel security privacy vs precision, Inference and attacks on databases, Security in Windows, Linux, Social & Ethical issues of Information Security, Information Security management, Mobile code security Digital Defense: Issues in Security, and Critical Infrastructure Protection: Threats of viruses, worms, malicious codes, models of propagation and their epidemic spread. Application Security, and current trends Case studies,

Unit -12: Web Security

Security on the Internet and the World Wide Web, Secure Hyper Text Transfer Protocol (SHTTP), Kerberos, Time Stamping Protocol (TSP), Secure Electronic Transaction (SET), SSL vs SET, 3-D Secure Protocol, Electronic Money, HTTPS, Electronic billing systems, Micropayments, Fair exchange protocols.

Unit -13: Miscellaneous

Security Policies, Physical Security, Protection of data and Information Laws, Employees rights, Software failure, Computer Crime, Cyber Crime, Privacy, Ethics, Wireless Application Protocol (WAP) Security, Security in GSM, Security in 3G , Advanced Crypto Algorithms

and Protocols , Oblivious Transfer, Secure Multiparty Computation, Digital Cash, Steganography and Water marking, Cryptography Standards, Cryptography Patents, Cryptography related Legal Issues- Copyright, Patents, Trade secrets, Law, Cyber Acts and Laws.

Unit -14: Laboratory Exercises

In the cryptographic laboratory 15-20 experiments will be performed, based on the syllabi of cryptography. List is attached as under: