|  |  |  |  |
| --- | --- | --- | --- |
| **Weekly break up for Theory** | | | |
| **Week** | **Topics Covered** | **CLOs** |
|  | Information security foundations, Security components, Security design principles, Security mechanisms, Attack surfaces and Attack trees, Computer Security Strategies, IS certifications | **1** |
|  | Key Concepts in cryptography, cryptosystem, cryptanalysis, Symmetric encryption, Classical Encryption Techniques: Substitution technique, Caesar Cipher, Vigenère Cipher, One Time Pad, Transposition Techniques: Rail fence technique, Columnar transposition | **1** |
|  | Block cipher and stream cipher, modes of block cipher, Data Encryption Standard (structure, strength), Triple DES (3DES), AES encryption process, Key Distribution Problem, Asymmetric cryptography, Diffie-Hellman Key Exchange | **1** |
|  | Man-in-the-Middle Attack, RSA algorithm, Message Authentication, Message Security Requirements, message authentication using encryption (symmetric and asymmetric) | **1** |
|  | Hash Function, Message Authentication Code, technique and its requirement, Digital signature, Digital Signature Model, Digital Signature Algorithm | **1,4** |
|  | User Authentication: Model for Electronic User Authentication, Means of User Authentication, Risk Assessment, Password Authentication, Vulnerabilities and countermeasures, Token-based authentication, Biometric authentication, Authentication Protocol: kerberos | **4** |
|  | Access control, Components, Access Rights, Requirements, Access control policies: Discretionary Access Control, DAC Matrix, Mandatory Access Control, Role-Based Access Control, Role Hierarchy, RBAC Constraints, case study | **4** |
|  | Software security, Software Security Issues, Handling Program Input and output, Types of Malicious Software, Advanced Persistent Threat, Viruses, Worms, Spam E-Mail, Trojan Horse, Attack Agent: Zombie, Bots, Information Theft—Key loggers, Phishing, Spyware, Countermeasures | **1,2** |
|  | Denial-of-Service Attacks, Flooding Attacks, Distributed Denial-of-Service Attacks, Defenses Against Denial-of-Service Attacks | **1** |
|  | Database Security, SQL Injection Attacks, Database Access Control, Cloud Security Risks And Countermeasures, Internet Security Protocols and Standards, | **4** |
|  | Firewall Characteristics and Access Policy, Types of Firewalls, Bastion Host, Host-Based Firewalls, DMZ Networks, Virtual Private Networks, Distributed Firewalls | **3,4** |
|  | Network Intrusion detection and prevention systems: Inside attack, Approaches to Intrusion Detection, Rule-based detection, Statistical anomaly detection | **3,4** |
|  | Security Auditing, Audit Trail, Audit Trail Analysis | **2,3** |
|  | Security Risk Assessment, Baseline Approach, Informal Approach, Risk Analysis | **3** |
|  | Law and Ethics in Information Security, Types of Computer Crime, Law Enforcement Challenges, Intellectual Property, copyright, patent, Digital Rights Management, Ethics and the IS Professions, Codes of Conduct | **2** |
|  | Privacy Law and Regulation, Privacy and Data Surveillance, anonymity of data | **3** |