Course Code: BCSE317L

Course Title/Subject Title: INFORMATION SECURITY

Module 1: Information Security Concepts (4 hours)

1. **Information Security** – Protecting information from unauthorized access, disclosure, alteration, and destruction to ensure confidentiality, integrity, and availability.
2. **Computer Security** – Safeguarding computer systems and information from theft, disruption, and unauthorized use.
3. **Threats, Harm, and Vulnerabilities** – Understanding potential security risks such as malware, data breaches, and insider threats that exploit system weaknesses.
4. **Program Security** – Securing applications against unauthorized access and ensuring their safe execution.
5. **Malicious Code and Malware:**
    - **Viruses** – Self-replicating programs that spread by attaching to legitimate files.
    - **Trojan Horses** – Malicious programs disguised as legitimate software to gain control over a system.
    - **Worms** – Standalone malware that spreads across networks by exploiting vulnerabilities.
6. **Countermeasures** – Techniques such as antivirus, intrusion prevention systems, and security policies to mitigate security threats.

Module 2: Authentication and Access Control (6 hours)

1. **Authentication** – Verifying the identity of users or systems before granting access.
2. **Key Management Schemes** – Techniques for securely generating, distributing, and managing cryptographic keys.
3. **Hierarchical Key Management Techniques** – Structuring keys in a hierarchy to control access and limit exposure.
4. **Security Standards** – Guidelines such as ISO 27001, NIST, and PCI DSS that define best practices for securing information.

5. **User Authentication Protocols** – Protocols like Kerberos, OAuth, and SAML for secure user verification.
6. **Implementing Access Controls** – Enforcing policies to restrict access to sensitive information based on user roles.
7. **Access Control Models:**
    - **Role-Based Access Control (RBAC)** – Assigning permissions based on predefined roles.
    - **Attribute-Based Access Control (ABAC)** – Granting access based on attributes such as user, environment, and resource.
8. **Attribute-Based Encryption in Information Storage** – Encrypting data using attributes to restrict access based on defined policies.
9. **Physical Access Controls** – Restricting physical entry to sensitive systems and facilities using biometric devices, security guards, and access cards.

Module 3: Operating Systems Security (7 hours)

1. **Security in Operating Systems** – Enforcing security policies to prevent unauthorized access and system abuse.
2. **Security in OS Design:**
    - **Simplified Design** – Reducing complexity to minimize vulnerabilities.
    - **Layered Design** – Dividing functionality into layers to improve security management.
    - **Kernelized Design** – Using a secure kernel to mediate all system actions.
    - **Reference Monitor** – A trusted component that enforces access control policies.
    - **Trusted Systems** – Systems that meet established security standards.
    - **Trusted System Functions** – Core functionalities such as audit, identification, and access control.
3. **Trusted Operating System Design** – Incorporating security mechanisms to protect against system-level threats.
4. **Rootkit Attacks and Mitigation** – Detecting and removing hidden malicious programs that compromise the OS.

Module 4: Security Countermeasures (7 hours)

1. **Design of Firewalls** – Implementing security devices to monitor and control network traffic.
2. **Types of Firewalls:**
    - **Packet-Filtering Firewalls** – Inspecting packets and blocking unwanted traffic.
    - **Stateful Inspection Firewalls** – Tracking the state of active connections to allow or deny traffic.
    - **Application Layer Firewalls** – Analyzing application-level traffic for suspicious behavior.
3. **Personal Firewalls and Configurations** – Configuring firewalls on individual systems to prevent unauthorized access.
4. **Network Address Translation (NAT)** – Masking private IP addresses to enhance security and reduce IP conflicts.
5. **Data Loss Prevention (DLP)** – Implementing strategies to prevent unauthorized data access and transmission.
6. **Intrusion Detection and Prevention Systems (IDPS):**
    - **Types of IDS** – Network-based and host-based intrusion detection.
    - **Intrusion Prevention Systems (IPS)** – Actively blocking detected threats.
    - **Intrusion Response Mechanisms** – Incident handling and response techniques.
    - **Goals, Strengths, and Limitations of IDS** – Monitoring, alerting, and identifying weaknesses.

Module 5: Database Security (6 hours)

1. **Database Security Fundamentals** – Protecting database integrity, confidentiality, and availability.
2. **Database Security Requirements** – Ensuring controlled access, auditability, and data protection.
3. **Reliability and Integrity of Databases** – Maintaining accurate and consistent data through backups and integrity controls.
4. **Handling Sensitive Data** – Encrypting and masking sensitive information.
5. **Types of Data Disclosures** – Unintended data exposure, such as aggregation and inference.

6. **Methods for Preventing Disclosures** – Using encryption, access controls, and auditing to mitigate disclosure risks.
7. **Inference Attacks and Mitigation** – Preventing attackers from deducing sensitive information using statistical analysis.
8. **Multilevel Databases and Security** – Implementing multi-tiered security models to safeguard sensitive data.
9. **Database Attacks:**
    - **SQL Injection Attacks** – Exploiting SQL vulnerabilities to manipulate data.
    - **Other Common Database Exploits** – Buffer overflows, privilege escalation, and access violations.

Module 6: Web Security (6 hours)

1. **Browser Attacks:**
    - **Types of Browser-Based Attacks** – Drive-by downloads, malvertising, and browser exploits.
    - **Failed Identification and Authentication** – Exploiting weak authentication mechanisms.
2. **Misleading and Malicious Web Content** – Identifying fake and harmful content designed to deceive users.
3. **Protection Against Malicious Web Pages** – Implementing browser security extensions and sandboxing.
4. **Website Data Vulnerabilities:**
    - **Code within Data** – Embedding malicious scripts in input data.
    - **Cross-Site Scripting (XSS) Attacks** – Injecting malicious scripts into web pages.
    - **Prevention Techniques for Data Attacks** – Input validation, output encoding, and CSP implementation.
5. **Fake Emails and Email-Based Threats** – Identifying phishing, spoofing, and email-based malware.
6. **Spam Detection Techniques** – Using AI and machine learning to filter out spam emails.
7. **Phishing Attacks:**

- **Phishing URL Detection** – Identifying malicious links in emails.
- **Phishing Prevention Strategies** – Educating users and implementing anti-phishing filters.

Module 7: Privacy Issues (7 hours)

1. **Privacy Concepts:**
    - **Aspects of Information Privacy** – Data confidentiality, anonymity, and integrity.
    - **Computer-Related Privacy Concerns** – Monitoring, data retention, and tracking.
2. **Threats to Personal Data Privacy** – Unauthorized access, data breaches, and identity theft.
3. **People-Based Privacy Concerns** – Social engineering, surveillance, and profiling.
4. **Privacy Principles and Policies** – GDPR, HIPAA, and Indian IT Act regulations.
5. **Actions for Individual Privacy Protection** – Encryption, anonymization, and access control.
6. **Government Regulations on Privacy** – National and international privacy laws to safeguard individuals.
7. **Identity Theft and Prevention** – Recognizing and mitigating the risk of identity theft.
8. **Privacy Issues in Web Data Management** – Ensuring secure storage and processing of web data.
9. **Application of Cryptographic Techniques for Privacy Preservation** – Using encryption, digital signatures, and secure hashing to protect privacy.
