Module 1

1. Introduction to Essential Terminology of VAPT
2. Elements of Information Security
   * 1. Discussion

Definition – Information Security is defined as “a state of well-being of information and infrastructure in which the possibility of theft, tampering, and disruption of information and services is kept low or tolerable.”

1. **Confidentiality:**

Confidentiality is the assurance that the information is accessible only to those who are authorised to access. Confidentiality breaches may occur due to improper data handling or being hacking attempt.

It controls includes data classification, data encryption, and proper equipment disposal (ie, pendrives, CDs, DVDs etc)

1. **Integrity:**

Integrity is the trustworthiness of data or resources in the prevention of improper and unauthorized changes – the assurance that information is sufficiently accurate for its purpose. To maintain the integrity, we may include checksum and access control.

1. **Availability**

Availability is the assurance that the system responsible for delivering, storing, and processing information are accessible when required by authorized users. Measures to maintain it are having anti-virus s/w to prevent destroying the networks, and DDoS prevention system.

1. **Authenticity**

Authenticity is to confirm that a user is genuine, one who he claims to be. Controls such as biometrics, smart cards, and digital certificates ensure the authenticity of the data, transactions, communications, or documents.

1. **Non-Repudiation**

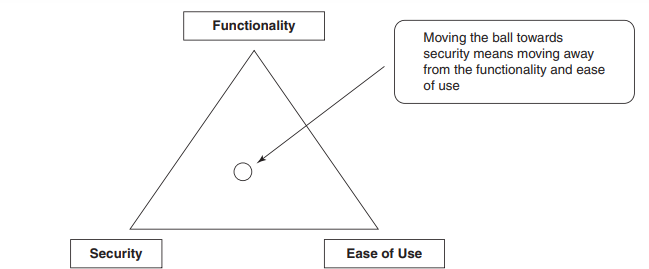
Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message, and that the recipient cannot deny having received the message. Individuals and organization use digital signatures to ensure non-repudiation.

* + 1. Identify the Elements of Information Security from the given scenarios

1. The security, usability, and functionality triangle
   * 1. Discussion

The security, usability, and functionality triangle is a concept that describes the trade-offs and balancing act that must be made when designing any technology product or system. The three factors are interdependent, and changes made to one will have an impact on the others.

1. **Security**: Refers to the protection of a software system against unauthorized access, data theft, and other malicious attacks. Security measures can include encryption, access controls, firewalls, and other security features.
2. **Usability**: Refers to the ease of use and learnability of a software system. A usable system is one that is intuitive, user-friendly, and requires minimal training to use effectively.
3. **Functionality**: Refers to the features and capabilities of a software system. A system with good functionality is one that is able to perform the tasks and functions it was designed for effectively and efficiently.



* + 1. Examples

Consider a banking app that allows users to transfer funds between accounts. To ensure security, the app may require users to provide a password and use two-factor authentication. However, if the security measures are too complex or cumbersome, users may find the app difficult to use, leading to poor usability. On the other hand, if the app prioritizes usability over security, it may be vulnerable to hacking and data breaches. Similarly, if the app lacks important functionality such as account history or transaction summaries, users may be dissatisfied with the app's performance. Therefore, the challenge for developers is to find a balance between security, usability, and functionality that meets the needs of users while minimizing risk.

1. Introduction to motives of security attack vectors
   * 1. Discussion
     2. Examples
2. Types of Information Security attack vectors
   * 1. Discussion
     2. Example
3. Types of attacks on the system
   * 1. Discussion
     2. Example
4. Types of information warfare

a. Discussion

1. Types of hackers

a. Discussion

1. Steps to Hacking phases
   * 1. Discussion
     2. Diagram
2. Introduction to Ethical Hacking
   * 1. Discussion
     2. Examples
     3. Limitation and scope
3. Introduction to Penetration testing
   * 1. Discussion
     2. Diagram
     3. Illustrate the steps of Penetration testing for the given scenarios
4. Types of Penetration testing
   * 1. Discussion
     2. Example
5. Phases of Penetration Testing Discussion
   * 1. Discussion
     2. Diagram
6. Introduction to Risk
   * 1. Discussion
     2. Examples
7. Ethical Disclouser
   * 1. Discussion
     2. Example
     3. RF Policy
     4. Zero Day Initiative
     5. CERT
8. CVSS
   1. Discussion
   2. Example
9. Exploit DB
   1. Discussion
   2. Example
10. Google Dork
    1. Discussion
    2. Example
11. OWASP Web Top 10
    1. Discussion
    2. Example
12. OWASP Mobile Top 10
    1. Discussion
    2. Example