# ***Introduction to Ethical Hacking***

# ***Elements of information security***

# ***Information security is a state of wellbeing of information and infrastructure in which the possibility of theft tempering and Disruption of information and services is low or tolerable***

|  |  |
| --- | --- |
| ***Confidentiality*** | ***Assurance that information is accessible only to those authorized to have access*** |
| ***Integrity*** | ***The thrust worthiness of data or resources in terms of preventing improper or not Unauthorized changes*** |
| ***Availability*** | ***Residents that the systems responsible for delivering strong and processing information are accessible when required by the authorized users*** |
| ***Authenticity*** | ***Refers to the characteristic of a communication document or any data that ensures the Quality of being genuine*** |
| ***Non repudiation*** | ***He guaranteed that the sender of a message cannot later deny having sent a message that the recipient cannot deny having received the message*** |

# 

**Confidentiality:**

* **Confidentiality is the assurances that the information is Accessible only to authorized.**
* **Confidentiality breaches may occur due to improper data handling or hacking attempt.**
* **Confidentiality controls include data classification data inscription and proper disposal of equipment (such as DVD’s USB drivers and blue-ray discs)**

**Integrity:**

* **Integrity is the truth worthiness of data or resources in the prevention of improper and Unauthorized changes – The assurance that information is sufficiently accurate for its purpose. Measures to maintain data integrity may include a checksum ( a number produced by a mathematical function to verify that a given block of data is not changed) and access control (which ensures that only authorized people can update, add or delete data)**

**Availability:**

* **Availability is the assurance that the systems responsible for delivering, storing, andprocessing information are accessible when required by authorized users. Measures to maintain data availability can include disk arrays for redundant systems and clustered machines, antivirus software to combat malware, and distributed denial-of-service (DDoS) prevention systems.**

**Authenticity:**

* **Authenticity refers to the characteristic of communication, documents, or any data that ensures the quality of being genuine or uncorrupted. The major role of authentication is to confirm that a user is genuine. Controls such as biometrics, smart cards, and digital certificates ensure the authenticity of data, transactions, communications, and documents**

**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 organizations use digital signatures to ensure non-repudiation.**

**Mottos goals and objectives of Information Security attacks**

**Attack = Motive (Goal) + Method + Vulnerability**

**Attackers generally have motives (goals), and objectives behind their information security attacks. A motive originates out of the notion that a target system stores or processes something valuable, which leads to the threat of an attack on the system. The purpose of the attack may be to disrupt the target organization’s business operations, to steal valuable information for the sake of curiosity, or even to exact revenge. Therefore, these motives or goals depend on the attacker’s state of mind, their reason for carrying out such an activity, as well as their resources and capabilities. Once the attacker determines their goal, they can employ various tools, attack techniques, and methods to exploit vulnerabilities in a computer system or security policy and controls.**

**Motives behind information security attacks**

**▪ Disrupt business continuity**

**▪ Perform information theft**

**▪ Manipulating data**

**▪ Create fear and chaos by disrupting critical infrastructures**

**▪ Bring financial loss to the target▪ Propagate religious or political beliefs**

**▪ Achieve a state’s military objectives**

**▪ Damage the reputation of the target**

**▪ Take revenge**

**▪ Demand ransom**

**Classification of attacks**

**According to IATF, security attacks are classified into five categories: passive, active, close-in, insider, and distribution.**

* **Passive attacks:**

**Passive attacks involve intercepting and monitoring network traffic and data flow on the target network and do not tamper with the data. Attackers perform reconnaissance on network activities using sniffers. These attacks are very difficult to detect as the attacker has no active interaction with the target system or network. Passive attacks allow attackers to capture the data or files being transmitted in the network without the consent of the user. For example, an attacker can obtain information such as unencrypted data in transit, clear-text credentials, or other sensitive information that is useful in performing active attacks.**