**WEEK 1**

**What is Cyber Security?**

Cyber Security is the protection of internet-connected systems, including hardware, software, and data, from cyberattacks.

* We give our details like Aadhar card number in many places. If any data breach happens then our details will be leaked to cyber criminals.
* Recently, Aadhar biometrics were leaked, and without our consciousness money from bank accounts was deduced.

**CIA Triad (3 pillars of cyber security)**

**Confidentiality:**

Let us take an example and understand the concept of confidentiality.

If two persons A and B are chatting in WhatsApp and there enter a person C (unauthorized) and watch what they are chatting about. This causes the loss of confidentiality.

* Confidentiality refers to avoiding a data breach.
* Encryption of data helps protect confidentiality.

**Integrity:**

Let us take the above example, if two persons A and B are chatting and the third person C (unauthorized) modifies the which is sent by A to B, this causes loss of integrity.

* Integrity refers to avoiding the modification of data.

**Availability:**

* Availability of data for genuine users.

**Needs for Cyber Security:**

* Basic computer skills
* Basics of networking
* Understanding basic cyber security measures

**Types of Hackers:**

1. **Black Hat Hacker:**

These types of hackers take advantage of vulnerabilities and destroy an organization or a business.

1. **Grey Hat Hackers:**

These types of hackers move from black hat hackers to white hat hackers. They do the job of both black and white hat hackers.

1. **White Hat Hackers:**

These types of hackers are sometimes called ethical hackers. They belong to the blue team. They help governments and organizations.

**Popular Attacks:**

* **Social Engineering Attacks**
* **Cryptocurrency Hijacking**
* **Ransomware:**
* In this attack attacker enters the network and holds the system. Then they encrypt the data and to decrypt the data they ask for money.
* Eg: WannaCry ransomware attack in May 2017
* **Botnets Attacks**
* Groups of bots are called botnets or zombies
* Attacker initiates attacks through botnet to the victim
* **Phishing**
  + In this attack the attacker sends links or makes the victim download a file that contains malicious software.

**Steps to fix a cybercrime:**

1. Identify
2. Having access to authorization
3. Treat it

**Risk:** A possible threat exploiting a vulnerability causing a negative impact.

**Cryptography:**

* It is a technique to hide the information.
* Crypto means secret or hidden.

**Types of Cryptography:**

* Symmetric or Private key Cryptography
* Has only one key and use that key to encrypt and decrypt
* At first normal message is converted into a hex message and then a bit message.
* The receiver has the private key and decrypts the message.
* Symmetric algorithm is further divided into 2 types:
  + Stream Cipher (each bit is encrypted at a time, with no definite length, slow)
  + Block Cipher (take a block of bits and encrypt it using a key that we were having
* Asymmetric or Public-key Cryptography
* Has 2 keys (private and public key)
* Public key can be shared with the outside world

**Security goals & it’s implementations:**

**Authentication:** It is the process of giving individuals access to system objects based on their identity.

**Ways to authenticate a person:**

* Something you know (Password)
* Something you have (Token)
* Something you are

**Authorization:** It is the function of specifying access rights/privileges to resources.

**Confidentiality:** It refers to protecting information from being accessed by unauthorized parties.

**Accountability:** It means that every individual who works with a system should have specific responsibilities for information assurance.

**Non-Repudiation:** It is the assurance that someone cannot deny the validity of something.

**Design a Security System**

* Security in Software Requirements
* Robust, consistent error handling
* Share requirements w/QA team
* Handle internal errors securely
* Use of “defensive programming”
* Validation and Frauds Checks
* “Security or Bust” Policy

**Buffer Overflow:** A buffer overflow, or buffer overrun, is a common software coding mistake that an attacker could exploit to gain a access to your system.