**DAY 3**

 **Threat**:

* **Definition**: A potential cause of an unwanted incident that may result in harm to a system or organization.
* **Examples**: Hackers, natural disasters, insider threats, malware.

 **Vulnerability**:

* **Definition**: A weakness in a system, network, or application that can be exploited by a threat to gain unauthorized access or cause damage.
* **Examples**: Unpatched software, weak passwords, lack of encryption, misconfigured systems.

 **Attack**:

* **Definition**: An attempt to exploit a vulnerability to compromise the security of a system or data.
* **Examples**: Phishing, Denial of Service (DoS), Man-in-the-Middle (MitM), SQL injection.

 **Risk**:

* **Definition**: The potential for loss, damage, or destruction of an asset as a result of a threat exploiting a vulnerability.
* **Examples**: Financial loss due to data breach, operational downtime from a cyber attack.

 **Exploit**:

* **Definition**: A piece of software, data, or sequence of commands that takes advantage of a vulnerability to cause unintended behavior or access in a system.
* **Examples**: Buffer overflow exploits, zero-day exploits, social engineering techniques.

 **Asset**:

* **Definition**: Anything of value to an organization that needs protection.
* **Examples**: Data, hardware, software, intellectual property, reputation.

 **Impact**:

* **Definition**: The extent of damage that can be caused by a threat exploiting a vulnerability.
* **Examples**: Financial losses, reputational damage, legal consequences, loss of customer trust