**Day 3**

**Threat**: A threat is danger or a malicious action that could exploit a vulnerability to harm a computer system, network, or digital information.  
**eg**: Malware, Phishing, Denial of Service (DoS), Distributed Denial of Service (DDoS), Man in the Middle Attack, etc.  
  
**Attack**: It refers to any action or attempt to exploit vulnerabilities in a system, network, or application to cause harm, steal data, or gain unauthorized access.

**eg**: Ransomware attacks, Password attacks, Social Engineering attacks, etc.

**Risk**: The possibility of loss of data, damage or modifying the data, data theft and also taking unauthorized access is a risk.   
  
**Exploit**: An exploit is a piece of code, software, or command s designed to take advantage of a vulnerability within a system, network, or application. Its main goal is to gaining unauthorized access, stealing data, or causing system damage.

**Asset**: An asset is an important data. Properly identifying and managing assets is important for developing effective security measures and ensuring that valuable resources are safeguarded against threats and vulnerabilities.

**Impact**: It refers to the potential consequences or damage resulting from a cyber attack or security breach. It assesses the severity of the harm that could occur if a threat successfully exploits a vulnerability.  
  
**Different types of Threat:**  
  
**Technical Threat** : Risks that come from technical flaws or vulnerabilities in computer systems or software, such as malware or hacking attacks.  
  
**Social Engineering:** Tactics that trick people into giving away confidential information or access, usually by pretending to be someone trustworthy.  
  
**Physical Threat**: Risks to security that involve physical harm or damage to hardware, like theft, breaking the hardware,etc.