DAY -7

- **Social Engineering:** The manipulation of people to perform actions or divulge confidential information.
- **Physical Threats:** Potential harm or damage to physical assets, infrastructure, or personnel.
- **Operational Threats:** Risks to the normal operation of systems or processes, often due to internal factors.

Vulnerabilities

Social Engineering Vulnerabilities

- **Human Error:** Lack of awareness, training, or phishing susceptibility.
- **Trust and Goodwill:** Overreliance on relationships or a desire to help.
- **Impersonation:** Deception through mimicking legitimate entities.
- **Pretexting:** Creating a believable scenario to gain trust.
- **Baiting:** Offering something desirable to entice users to click or download.

Physical Threats Vulnerabilities

- **Unauthorized Access:** Lack of physical security controls (locks, guards, surveillance).
- **Environmental Hazards:** Fire, flood, natural disasters, or power outages.
- **Equipment Failure:** Hardware malfunctions or breakdowns.
- **Theft or Vandalism:** Loss or damage to physical assets.

Operational Threats Vulnerabilities

- **Process Failures:** Inefficient or poorly defined procedures.
- **System Failures:** Software bugs, hardware malfunctions, or network outages.
- **Human Error:** Mistakes made by employees during operations.
- **Insider Threats:** Malicious actions by employees or contractors.
- **Supply Chain Risks:** Vulnerabilities in third-party products or services.