DAY 03 Exploring

Threat

A threat is a potential danger or harmful event that could exploit a vulnerability and cause harm to a system, organization, or individual.

Examples: Malware, ransomware, phishing, natural disasters, human error.

Vulnerability

A vulnerability is a weakness in a system (hardware, software, or process) that can be exploited by a threat to compromise its security.

- **Examples:** Weak passwords, unpatched software, outdated systems, insecure configurations.

Attack

An attack is an action taken by a threat actor to exploit a vulnerability and compromise a system or asset.

- **Examples:** Phishing attack, DDoS attack, malware infection, SQL injection.

Risk

Risk is the potential for loss, damage, or destruction of an asset as a result of a threat exploiting a vulnerability.

- **Example:** The risk of a data breach due to a weak password policy.

Exploit

An exploit is a piece of software, code, or technique used to take advantage of a vulnerability.

- **Example:** A malicious script used to exploit a software bug.

Asset

An asset is anything of value to an organization, including hardware, software, data, people, and infrastructure.

- **Examples:** Servers, databases, customer information, intellectual property, employees.

Impact

Impact is the measure of harm or loss resulting from a successful attack.

Example: The impact of a ransomware attack could include financial loss due to ransom payment, data loss, and business disruption.

DAY 03 Exploring