Day 4 - Explore various types of Threat. Identify the possible attack based on the threat (05/08/2024)

Threats - The **actions** carried out primarily by hackers or attackers with malicious intent, to steal data, cause damage, or interfere with computer systems.

A **Threat** can be anything that can **take advantage of a vulnerability** to breach security and negatively alter, erase, or harm objects. A threat is any potential danger that can harm your systems, data, or operations.

Types of Threats -

1. **Technical Threats** - These are threats that target the technical aspects of systems, software, and networks.

   Possible Attacks:

   ➔ **Malware**: Viruses, worms, Trojan horses, ransomware.
   ➔ **Phishing**: Deceptive emails or websites designed to steal personal information.
   ➔ **Denial of Service (DoS)**: Overloading systems to make them unavailable to users.
   ➔ **SQL Injection:** Exploiting vulnerabilities in web applications to execute arbitrary SQL commands.
   ➔ **Zero-day Exploits**: Attacks that target vulnerabilities unknown to the software vendor.

2. **Social Engineering -** Manipulating individuals into divulging confidential information or performing actions that compromise security.

   Possible Attacks:

   ➔ **Phishing:** Crafting emails that appear legitimate to trick individuals into providing sensitive information.
   ➔ **Spear Phishing:** Targeted phishing attacks aimed at specific individuals or organizations.
   ➔ **Pretexting:** Creating a fabricated scenario to persuade a target to disclose information.
   ➔ **Baiting:** Leaving infected physical media (like USB drives) in places where people will find them and use them.
   ➔ **Tailgating:** Gaining unauthorized access to secure areas by following authorized personnel.

3. **Physical Threats** - Threats that involve physical harm to systems, facilities, or individuals.

   Possible Attacks:

   ➔ **Theft:** Stealing hardware, sensitive documents, or other physical assets.
   ➔ **Vandalism:** Damaging equipment or infrastructure.
   ➔ **Natural Disasters:** Earthquakes, floods, fires that can destroy or disrupt physical assets.
   ➔ **Sabotage:** Deliberate destruction or disruption of systems or facilities by insiders or external agents.

4. **Operational Threats** - Threats arising from inadequate or failed internal processes, people, and systems.

   Possible Attacks:

➔ **Process Failures:** Errors in business processes leading to data breaches or service disruptions.
➔ **Insider Threats:** Employees or contractors misusing their access to harm the organization.
➔ **Third-Party Risk:** Suppliers or partners introducing vulnerabilities.
➔ **System Failures:** Hardware or software failures causing data loss or service interruptions.

5. **Strategic Threats** - Long-term threats that can affect the overall strategic objectives of an organization.

   Possible Attacks:

➔ **Reputation Damage:** Negative publicity from data breaches or operational failures.
➔ **Market Changes:** Competitors leveraging advanced technology to gain an edge.
➔ **Regulatory Changes:** New laws or regulations imposing stringent security requirements.

6. **Compliance Threat** - Threats related to failing to adhere to laws, regulations, and standards.

   Possible Attacks:

➔ **Non-compliance Penalties:** Fines and legal actions due to non-compliance with regulations like GDPR, HIPAA.
➔ **Audit Failures:** Security audits revealing non-compliance and leading to penalties or loss of certifications.

7. **Environmental Threats** - Threats arising from the physical environment.

   Possible Attacks:

➔ **Natural Disasters:** Earthquakes, floods, hurricanes causing physical damage to infrastructure.
➔ **Man-made Disasters:** Accidents or deliberate acts causing environmental damage (e.g., chemical spills).

8. **Supply Chain Threats** - Threats related to vulnerabilities in the supply chain.

   Possible Attacks:

➔ **Counterfeit Hardware/Software:** Introducing malicious components through suppliers.
➔ **Supply Chain Disruptions:** Interruptions in the supply chain affecting availability of critical components.
➔ **Third-Party Breaches:** Compromises in vendor systems leading to data breaches.