**JEEVAN S U**

**241059038**

**CRYPTOLOGY**

**M.E – CYBER SECURITY**

**Different Kinds of Threats**

**1. Technical Threats**

* **Possible Attacks:**
  + **Malware Attacks:** Installation of malicious software (e.g., viruses, worms, Trojans).
  + **Denial of Service (DoS) / Distributed Denial of Service (DDoS):** Overloading systems to make them unavailable.
  + **SQL Injection:** Manipulating databases through malicious input in SQL queries.
  + **Man-in-the-Middle (MitM):** Intercepting communication between two parties.
  + **Zero-Day Exploits:** Attacks on vulnerabilities that are not yet patched.

**2. Social Engineering**

* **Possible Attacks:**
  + **Phishing:** Deceiving individuals into revealing confidential information (e.g., login credentials).
  + **Pretexting:** Creating a fabricated scenario to steal information.
  + **Baiting:** Leaving infected devices (e.g., USB drives) in public places to trick people into using them.
  + **Tailgating:** Unauthorized entry into restricted areas by following authorized personnel.

**3. Physical Threats**

* **Possible Attacks:**
  + **Theft of Equipment:** Stealing devices like laptops, servers, or drives containing sensitive data.
  + **Sabotage:** Intentional damage to physical hardware.
  + **Natural Disasters:** Destruction of data centers or hardware due to events like floods, fires, earthquakes.
  + **Unauthorized Access:** Physical intrusion into a facility or data center.

**4. Operational Threats**

* **Possible Attacks:**
  + **Insider Threats:** Employees intentionally or unintentionally compromising systems.
  + **Supply Chain Attacks:** Compromising systems through third-party suppliers or vendors.
  + **Policy Violations:** Employees not following security protocols, leading to vulnerabilities.
  + **Process Failures:** Inadequate procedures resulting in data leaks or system downtime.

**5. Strategic Threats**

* **Possible Attacks:**
  + **Corporate Espionage:** Competitors infiltrating an organization to steal trade secrets or intellectual property.
  + **Advanced Persistent Threats (APTs):** Long-term, targeted attacks against specific organizations or industries.

**6. Environmental Threats**

* **Possible Attacks:**
  + **Power Outages:** Sudden loss of electricity affecting data centers.
  + **Water Damage:** Flooding or humidity damage to critical hardware.
  + **Fire:** Fire incidents causing damage to systems and storage devices.

**7. Compliance Threats**

* **Possible Attacks:**
  + **Regulatory Violations:** Fines or penalties due to non-compliance with legal regulations (e.g., GDPR, HIPAA).
  + **Data Breaches:** Loss of sensitive customer or corporate data leading to legal actions and financial loss.

**8. Cyber Espionage**

* **Possible Attacks:**
  + **Data Exfiltration:** Unauthorized transfer of data from a system.
  + **Zero-Day Exploits:** Exploiting unknown vulnerabilities before they are patched.

**9. Strategic Threats**

* **Possible Attacks:**
  + **Nation-State Attacks:** Government-sponsored attacks on critical infrastructure.
  + **Corporate Espionage:** Competing companies stealing intellectual property.
  + **Disinformation Campaigns:** Spreading false information to manipulate public opinion.