Task 3 : Perform a Basic Vulnerability Scan on Your PC.

**Vulnerability:-**

A vulnerability is a weakness or flaw in a system, software, network, or process that can be exploited by a threat actor (like a hacker) to gain unauthorized access, cause harm, or perform malicious actions.

**What Can Vulnerabilities Cause:-**

Vulnerabilities can lead to serious **security incidents** such as:

1. **Unauthorized Access**  
   Hackers can gain access to sensitive data or systems.
2. **Data Breaches**  
   Confidential information (like passwords, credit card numbers, health records) can be leaked or stolen.
3. **Malware Infections**  
   Attackers may exploit a flaw to install malware (e.g., viruses, ransomware).
4. **System Compromise**  
   Entire systems or devices can be taken over and controlled remotely.
5. **Denial of Service (DoS) Attacks**  
   Systems may be overwhelmed and made unavailable to legitimate users.
6. **Financial Loss**  
   Due to theft, ransom payments, or system downtime.
7. **Reputation Damage**  
   Organizations may lose customer trust and face legal consequences.

**Prevent or Reduce Vulnerabilities**

* Regular software updates and patching
* Using strong authentication methods
* Conducting security audits and vulnerability assessments
* Employing firewalls and intrusion detection systems
* Educating users about security best practices

**Vulnerability scanning:-**

Vulnerability scanning is the automated process of identifying known security weaknesses in systems, networks, or applications. It helps detect flaws that could be exploited by hackers such as outdated software, misconfigurations, or open ports.

**Uses of Vulnerability Scanning:-**

1. **Identify Security Flaws**
   * Detects known vulnerabilities before attackers do.
2. **Compliance**
   * Helps meet security standards (e.g., PCI-DSS, HIPAA, ISO 27001).
3. **Risk Management**
   * Assesses and prioritizes threats based on severity.
4. **Continuous Monitoring**
   * Ensures ongoing protection as systems evolve.
5. **Support in Patch Management**
   * Helps determine which vulnerabilities need patching.

**Popular Tools Used for Vulnerability Scanning:-**

* Nessus
* OpenVAS
* Qualys
* Nikto
* Acunetix
* Burp Suite
* Nmap + NSE Script

**How It Works:-**

1. Target Identification – Choose the system, app, or network to scan.
2. Scan Execution – The tool sends probes to detect open ports, services, OS, etc.
3. Vulnerability Detection – Compares results with a database of known vulnerabilities (like CVE).
4. Report Generation – Shows vulnerabilities with severity levels and recommendations.

**Risk Assessment:-**

Risk assessment is the process of identifying, analyzing, and evaluating risks to an organization’s systems, data, and operations.

**Steps in Risk Assessment:**

1. Identify Assets – What are you trying to protect? (e.g., servers, databases)
2. Identify Threats – What could go wrong? (e.g., malware, insider threats)
3. Identify Vulnerabilities – What weaknesses exist? (e.g., unpatched software)
4. Determine Impact – What damage would occur if exploited?
5. Evaluate Likelihood – How likely is the threat to occur?
6. Calculate Risk – Risk = Threat × Vulnerability × Impact
7. Mitigate or Accept Risk – Choose controls or accept low-level risks.

**CVSS (Common Vulnerability Scoring System):-**

**CVSS** is a standardized method to **rate the severity of vulnerabilities** on a scale of **0.0 (lowest) to 10.0 (highest)**.

**CVSS Factors:**

* **Base Score** – Exploitability (how easy to exploit), Impact (how bad if exploited)
* **Temporal Score** – Changes over time (e.g., availability of patch)
* **Environmental Score** – Customized to specific environments

**Remediation**

Remediation is the process of fixing or mitigating vulnerabilities found during a scan or risk assessment.

**Common Remediation Methods:**

* Patching – Apply software updates.
* Configuration Changes – Disable unused ports, enforce strong authentication.
* Access Control – Limit who can access sensitive data.
* Network Segmentation – Isolate critical systems.
* Monitoring & Alerts – Detect future attempts.