**TASK-3**

**1️What is Vulnerability Scanning?**

**Vulnerability scanning** is an automated process that identifies security weaknesses in systems, networks, or applications. It involves using specialized tools (like Nessus or OpenVAS) to:

* Detect misconfigurations
* Identify outdated software
* Find known vulnerabilities (e.g., those listed in CVE databases)
* Assess exposure to potential threats

Scanners typically compare system data against a database of known vulnerabilities to generate a report with severity ratings and suggested fixes.

**2️ Difference Between Vulnerability Scanning and Penetration Testing**

| **Feature** | **Vulnerability Scanning** | **Penetration Testing** |
| --- | --- | --- |
| **Method** | Automated | Manual + automated |
| **Goal** | Identify known vulnerabilities | Exploit vulnerabilities to test defenses |
| **Depth** | Surface-level detection | Deep, real-world attack simulation |
| **Tools Used** | Nessus, OpenVAS | Metasploit, Burp Suite, custom scripts |
| **Frequency** | Regular (weekly/monthly) | Periodic (quarterly/yearly) |
| **Expertise Required** | Basic | Advanced cybersecurity skills |

**3️ Common Vulnerabilities in Personal Computers**

Here are some frequently found issues:

* **Outdated operating system or software**
* **Unpatched security flaws (e.g., CVE vulnerabilities)**
* **Weak or default passwords**
* **Enabled SMBv1 protocol (vulnerable to ransomware)**
* **Open ports with unnecessary services (FTP, RDP)**
* **Unsecured Wi-Fi or network settings**
* **Running outdated antivirus or firewall software**
* **Use of deprecated encryption protocols (TLS 1.0/1.1)**

**4️ How Do Scanners Detect Vulnerabilities?**

Scanners use a combination of techniques:

* **Banner grabbing**: Identifying software versions from service responses
* **Port scanning**: Detecting open ports and associated services
* **Fingerprinting**: Determining OS and software details
* **Database matching**: Comparing findings against known vulnerabilities (e.g., CVE database)
* **Plugins/scripts**: Running checks for specific misconfigurations or flaws

**5️ What is CVSS?**

**CVSS (Common Vulnerability Scoring System)** is a standardized framework for rating the severity of security vulnerabilities.

* **Score Range**: 0.0 (no risk) to 10.0 (critical risk)
* **Categories**:
  + **Base Score**: Intrinsic characteristics (e.g., exploitability, impact)
  + **Temporal Score**: Factors that change over time (e.g., patch availability)
  + **Environmental Score**: Context-specific impact (e.g., business risk)

Example:

* CVE-2017-0144 (WannaCry) has a CVSS score of **8.1** – high severity.

**6️ How Often Should Vulnerability Scans Be Performed?**

Best practices suggest:

* **Monthly scans** for personal devices
* **Weekly or bi-weekly scans** for enterprise systems
* **After major updates or configuration changes**
* **Before and after deploying new applications or services**

Regular scanning helps catch new vulnerabilities and ensure timely patching.

**7️ What is a False Positive in Vulnerability Scanning?**

A **false positive** occurs when a scanner reports a vulnerability that doesn’t actually exist.

Example:

* A scanner flags a service as outdated based on version number, but it’s been patched manually.

False positives can lead to wasted time and misdirected efforts, so manual verification is often necessary.

**8️ How Do You Prioritize Vulnerabilities?**

Prioritization depends on:

* **Severity (CVSS score)**: Critical vulnerabilities come first
* **Exploitability**: Is there a known exploit in the wild?
* **Asset value**: Is the vulnerable system mission-critical?
* **Exposure**: Is the system accessible from the internet?
* **Compliance requirements**: Are there legal or regulatory risks?