***ELEVATE LABS CYBER SECURITY INTERNSHIP***

***Task 3: Perform a Basic Vulnerability Scan on your PC***

**1. What is vulnerability scanning?**

**Vulnerability scanning** is an automated process that identifies and assesses security weaknesses in computer systems, networks, and applications. The scanner searches for known flaws, misconfigurations, and outdated software versions by comparing the target system's details against a database of known vulnerabilities.

**2. Difference between vulnerability scanning and penetration testing?**

While both aim to improve security, they have a key difference:

* **Vulnerability scanning** is like a doctor's check-up. It's an automated, non-intrusive process that identifies *potential* weaknesses and provides a report on them. It tells you what's wrong.
* **Penetration testing** (or pen testing) is like a simulated burglary. It's a manual, goal-oriented process where a security professional (a "pen tester") actively tries to exploit the vulnerabilities found to see how far they can get into the system. It shows you the *real-world impact* of a vulnerability.

**3. What are some common vulnerabilities in personal computers?**

Common vulnerabilities in personal computers often include:

* **Outdated Software:** Unpatched operating systems, web browsers, and applications often contain known security flaws that can be exploited.
* **Weak Passwords:** Using simple, easily guessable passwords or reusing the same password across multiple accounts makes a system vulnerable to brute-force attacks.
* **Malware:** Viruses, ransom ware, spyware, and other malicious software can be unknowingly downloaded or installed, leading to data theft or system damage.
* **Misconfigurations:** Incorrect firewall settings, leaving default credentials enabled, or using insecure network protocols can create an easy entry point for attackers.
* **Phishing:** Tricking users into revealing sensitive information through fraudulent emails, websites, or messages.

**4. How do scanners detect vulnerabilities?**

Vulnerability scanners work in a multi-step process:

1. **Asset Discovery:** The scanner first identifies all active devices, services, and applications on the network.
2. **Information Gathering:** It then probes these assets to collect details such as operating system versions, open ports, and installed software.
3. **Vulnerability Matching:** The collected information is compared against a large, constantly updated **vulnerability database** (often containing Common Vulnerabilities and Exposures, or CVEs).
4. **Reporting:** Based on the matches, the scanner generates a report that lists the identified vulnerabilities, their severity, and often provides recommendations for remediation.

**5. What is CVSS?**

**CVSS** stands for **Common Vulnerability Scoring System**.It's an open framework for rating the severity of a vulnerability. The score, which ranges from 0.0 to 10.0, is calculated based on several metrics, including:

* **Base Metrics:** How easy is it to exploit the vulnerability and what is the potential impact on confidentiality, integrity, and availability?
* **Temporal Metrics:** Has a fix been released? Is there an exploit available "in the wild"?
* **Environmental Metrics:** How critical is the affected system to the organization?

The final CVSS score helps security teams prioritize which vulnerabilities to fix first.

**6. How often should vulnerability scans be performed?**

The frequency of vulnerability scans depends on the organization's risk profile, regulatory requirements, and the nature of its systems. A general guideline is to perform scans:

* **Quarterly:** This is often a minimum requirement for compliance standards like PCI DSS.
* **Monthly or Weekly:** Recommended for high-risk assets, such as internet-facing web servers or systems containing sensitive data.
* **After Major Changes:** A scan should be performed immediately after significant changes to the network or infrastructure, such as deploying new software, adding new devices, or reconfiguring a firewall.

**7. What is a false positive in vulnerability scanning?**

A **false positive** occurs when a vulnerability scanner flags an issue that is not a real vulnerability. This can happen for several reasons:

* The scanner might make an assumption based on limited information (e.g., an outdated version number displayed in a banner) even if a patch has been applied.
* It might not have the correct permissions to fully authenticate and check for a patch or a specific configuration.

False positives can waste time and resources by forcing a security team to investigate and "fix" non-existent problems.

**8. How do you prioritize vulnerabilities?**

Prioritizing vulnerabilities is crucial to ensure that the most critical issues are addressed first. Simply relying on the CVSS score isn't enough. A more effective approach involves a **risk-based model** that considers:

1. **CVSS Score/Technical Severity:** The inherent severity of the vulnerability itself.
2. **Asset Criticality:** How important is the affected system to the business? (e.g., a customer-facing web server is more critical than a test machine).
3. **Threat Intelligence:** Is this vulnerability being actively exploited by attackers in the real world? Lists like CISA's Known Exploited Vulnerabilities (KEV) catalog are invaluable for this.
4. **Existing Controls:** Are there other security measures in place (e.g., a firewall, a web application firewall) that can mitigate the risk even if the vulnerability exists?