Task 15: Vulnerability Assessment & Risk Prioritization:

📌 Interview Questions & Answers

1. What is vulnerability assessment?

- Vulnerability assessment (VA) is the process of **systematically scanning, identifying, and analyzing security weaknesses** in systems, networks, or applications.
- It helps organizations understand their exposure to threats and provides a foundation for remediation.
- Tools like **Nessus Essentials** or **OpenVAS** automate this process by detecting misconfigurations, missing patches, and known vulnerabilities.

2. What is CVE?

- **CVE (Common Vulnerabilities and Exposures)** is a standardized identifier system for publicly known cybersecurity vulnerabilities.
- Each CVE entry provides:
    - A unique ID (e.g., CVE-2025-12345)
    - A description of the vulnerability
    - References to advisories or patches
- CVEs ensure consistency across tools and reports when discussing vulnerabilities.

3. What is CVSS?

- **CVSS (Common Vulnerability Scoring System)** is a framework used to assign a numerical score (0–10) to vulnerabilities based on their severity.
- It considers:
    - **Base metrics** (impact on confidentiality, integrity, availability)
    - **Temporal metrics** (exploit maturity, remediation level)
    - **Environmental metrics** (importance of affected systems in a specific organization)
- Example: A CVSS score of **9.8 (Critical)** indicates urgent remediation is needed.

4. VA vs Penetration Testing?

5. Why prioritization is important?

- Not all vulnerabilities pose the same level of risk.
- Prioritization ensures:
    - **Critical issues** (e.g., remote code execution, privilege escalation) are fixed first.
    - Resources are allocated efficiently.
    - Compliance with security standards (ISO, NIST, PCI-DSS).
- Without prioritization, teams may waste time fixing low-risk issues while attackers exploit high-risk ones.

📑 Deliverables for Task 15

1. **Vulnerability Assessment Report**
    - Scope, methodology, tools used (Nessus/OpenVAS)
    - List of identified vulnerabilities with CVE references
    - CVSS scores and severity ratings
2. **Risk Priority List**

- Categorization: Critical, High, Medium, Low
- Business impact analysis

PREPARED BY : MOHAMMED JAVEETH .M