TASK 15: VULNERABILITY ASSESSMENT & RISK PRIORITIZATION

1. Objective

To perform a vulnerability assessment on a target system, identify security weaknesses, analyze severity using CVE and CVSS scoring standards, prioritize risks based on impact and exposure, and recommend appropriate remediation strategies.

2. Scope of Assessment

Target System: Ubuntu Linux (Local VM)
Assessment Type: Internal vulnerability scan
Environment: Controlled lab setup
The assessment focused on identifying known vulnerabilities in exposed services and configurations.

3. Tools Used

- Nmap (Service and vulnerability scanning)
- National Vulnerability Database (NVD)
- Linux terminal utilities
- System log analysis tools

4. Methodology

A vulnerability scan was performed using the following command:

```
nmap -sV --script vuln
```

The scan identified open ports, service versions, and potential vulnerabilities associated with outdated software or misconfigurations.

5. Key Findings

Finding 1: Open SSH Port (22)
Potential Risk: Brute-force attack

Severity: High
Remediation: Disable root login and implement strong password policy.

Finding 2: Outdated Apache Service
Potential Risk: Remote Code Execution
Severity: High
Remediation: Update Apache to latest secure version.

Finding 3: Unrestricted Open Ports
Potential Risk: Unauthorized network access
Severity: Medium
Remediation: Restrict ports using firewall configuration.

6. Risk Prioritization

Priority 1: Internet-facing services with high CVSS score.
Priority 2: High severity vulnerabilities affecting authentication mechanisms.
Priority 3: Medium severity configuration weaknesses.
Low severity issues scheduled for routine patch cycles.

7. Risk Classification Criteria

Critical: CVSS 9.0–10.0
High: CVSS 7.0–8.9
Medium: CVSS 4.0–6.9
Low: Below 4.0
Classification also considered exposure level and exploit availability.

8. Remediation Plan

Immediate: Patch vulnerable services and enforce firewall rules.
Short-Term: Implement access control and strengthen authentication.
Long-Term: Deploy IDS and integrate centralized log monitoring (SIEM).

9. Conclusion

The vulnerability assessment identified multiple security weaknesses within the target system.
Based on CVE and CVSS evaluation, risks were prioritized to ensure effective mitigation.
Implementing the recommended controls significantly enhances system security posture.