Vulnerability Management Lifecycle:

The Vulnerability Management Lifecycle is a continuous process used to identify, assess, prioritize, remediate, and monitor security vulnerabilities in systems and applications. It helps organizations reduce risk and maintain a strong security posture.

1. Asset Discovery:

- Identifying all devices, systems, and applications in the network.
- Identify all devices, systems, and applications in your network.
- Maintain an updated inventory of assets (e.g., servers, endpoints, IoT devices).
- Tools: Network scanners, asset management systems.

2. Vulnerability Scanning:

- Scanning and identifying security weaknesses.
- Use tools like Nessus, Qualys, or OpenVAS to scan for known vulnerabilities.
- Detect missing patches, outdated software, and misconfigurations.
- Perform both authenticated and unauthenticated scans.

3. Risk Assessment & Prioritization:

- Analyze vulnerabilities based on severity, asset importance, and exploitability.
- Prioritize critical issues on exposed or high-value assets.
- Focus on high-impact and easily exploitable issues first.
- Use threat intelligence to guide decision-making.

4. Remediation & Mitigation:

- Apply security patches and updates or configuration changes.
- Reconfigure insecure settings or disable unused services.
- If a patch is not available, use compensating controls (e.g., firewall rules, segmentation).

5. Rescan & Reporting:

- Rescan systems to verify that vulnerabilities have been fixed.
- Generate technical reports for IT/security teams and summary reports for management.
- Track progress and ensure compliance with security policies or regulations.
- Generate reports for management and compliance.
- Confirming resolution and communicating results.
- Continuously monitor for new vulnerabilities as the environment evolves.

Note:

This is a continuous cycle. As new assets and vulnerabilities emerge, the process should repeat regularly. Once the reporting is complete, you return to Asset Discovery—because environments change constantly (new devices, updates, threats).