SOLUTION ARCHITECTURE

Testing and findings

Scanning Tool Effectiveness

Testing Approach:

- Deploy Nessus, OpenVAS, and Nexpose on a test network containing known vulnerabilities (e.g., outdated software, misconfigured services).
- Conduct both credentialed and non-credentialed scans.
- Compare detection rates and accuracy**.**

Findings:

- Nessus provides the most comprehensive vulnerability database with detailed risk scoring.
- OpenVAS is effective for open-source environments but has a higher false-positive rate.
- Nexpose offers strong integration with SIEM but requires tuning for optimal performance.

2. Threat Categories and Detection

Testing Approach:

- Simulate various cyber threats like malware injection, phishing attempts, and denial-of-service (DoS) attacks.
- Use scanning tools to detect these threats before and after execution**.**

Findings:

- Phishing and malware detection rely more on endpoint protection than scanning tools.
- Nessus and Nexpose detect missing patches and weak configurations effectively.
- OpenVAS struggles with zero-day vulnerabilities compared to proprietary tools.

3. Scanning Techniques

Testing Approach:

- Perform different types of scans:
- Network-based scanning to identify open ports and misconfigurations.
- Host-based scanning to detect vulnerabilities within OS and applications.
- Credentialed vs. non-credentialed scans for deeper insights.

Findings:

- Credentialed scans provide more accurate results but require proper privilege management.
- Non-credentialed scans detect fewer vulnerabilities but are useful for external threat analysis.
- Network scans are efficient but may cause performance degradation in active environments.

4. Risk Assessment & CVSS Scoring

Testing Approach:

- Assign severity levels (Low, Medium, High, Critical) to detected vulnerabilities.
- Compare risk scoring across different tools.

Findings:

- Nessus follows the CVSS scoring system accurately.
- OpenVAS sometimes misclassifies risks due to outdated threat intelligence.
- Risk prioritization helps focus on fixing critical issues first.

5. Remediation Strategies

Testing Approach:

- Implement patches, firewall rules, and security controls based on scanning results.
- Conduct re-scans after applying fixes to verify remediation effectiveness**.**

Findings:

- Patch management significantly reduces vulnerability risks.
- Misconfigurations remain a major security issue, requiring continuous monitoring.
- Firewall and IDS rules prevent unauthorized access but must be regularly updated.