Vulnerability Assessment & Risk Prioritization

Introduction

Vulnerability Assessment is a structured process used to identify security weaknesses in systems, networks, and applications. Every organization faces cyber threats, and unpatched vulnerabilities can be exploited by attackers. The purpose of vulnerability assessment is to find these weaknesses early, understand their risk level, and take corrective action before damage occurs.

This task focuses on performing a vulnerability assessment using automated scanning tools and prioritizing risks based on severity and impact.

Scope Definition

Defining the scope is the first step in vulnerability assessment. Scope ensures that only authorized systems are scanned and helps avoid unnecessary risks.

Scope includes:

- Target systems or IP addresses
- Network type (internal or external)
- Scan type (credentialed or non-credentialed)
- Excluded systems if required

A well-defined scope makes the assessment safe, legal, and effective.

Vulnerability Scanning Tools

Vulnerability scanners are used to automate the discovery of security issues.

Commonly used tools:

- Nessus Essentials
- OpenVAS

These tools help identify:

- Missing patches
- Outdated software

- Weak configurations
- Known security vulnerabilities

Scan Configuration

Before running the scan, proper configuration is required to get accurate results.

Important configuration settings:

- Select appropriate scan template
- Enable required plugins
- Define port range
- Add system credentials for deep scanning

Credentialed scans provide more detailed and reliable results than non-credentialed scans.

Running the Scan

Once configured, the scan is executed on the target systems. During the scan, the tool checks open ports, services, system settings, and software versions.

Scan duration depends on:

- Number of systems
- Network speed
- Scan depth

Monitoring the scan ensures it completes successfully.

Reviewing Scan Results

After the scan completes, vulnerabilities are displayed based on severity levels.

Severity levels include:

- Critical
- High
- Medium
- Low

- Informational

These levels help determine how serious each vulnerability is and which ones require urgent attention.

CVE (Common Vulnerabilities and Exposures)

CVE is a standardized identification system for known vulnerabilities.

Key points:

- Each vulnerability has a unique CVE ID
- CVEs help in tracking and fixing issues
- Widely used across security tools

Example: CVE-2023-12345

CVSS (Common Vulnerability Scoring System)

CVSS is used to measure the severity of a vulnerability using a score between 0 and 10.

CVSS Score Classification:

- 9.0–10.0: Critical
- 7.0–8.9: High
- 4.0–6.9: Medium
- 0.1–3.9: Low

Higher scores indicate higher risk.

Risk Classification

Risk is determined by combining the likelihood of exploitation and the potential impact.

Risk evaluation considers:

- Ease of exploitation
- Impact on business operations
- Asset importance

Not all vulnerabilities with high severity create high risk in every environment.

Risk Prioritization

Risk prioritization helps organizations fix the most dangerous vulnerabilities first.

Prioritization factors include:

- CVSS score
- System criticality
- Internet exposure
- Availability of exploits

Priority levels:

- P1: Immediate action
- P2: High priority
- P3: Medium priority
- P4: Low priority

Remediation Recommendations

Remediation involves fixing or reducing vulnerabilities to lower risk.

Common remediation actions:

- Apply security patches
- Update outdated software
- Disable unused services
- Close unnecessary ports
- Strengthen access controls

Vulnerability Assessment Report

The vulnerability assessment report summarizes the findings and recommendations.

Report includes:

- Scope and objectives
- Tools used

- Vulnerability summary
- Risk prioritization
- Recommended actions

A clear report helps management understand security risks easily.

VA vs Penetration Testing

Vulnerability Assessment focuses on identifying vulnerabilities, while Penetration Testing focuses on exploiting them. VA is preventive and automated, whereas penetration testing is more aggressive and manual.

Importance of Prioritization

Prioritization is important because time and resources are limited. Fixing critical vulnerabilities first reduces the chance of serious security breaches and improves overall system security.

Final Outcome

This task builds the ability to identify vulnerabilities, assess risk, prioritize threats, and recommend effective remediation. Vulnerability assessment and risk prioritization are essential skills for maintaining a secure IT environment.

Prepered by:

Megaraj S