Dr. Ritika Ladha

Lecture: 7 Cyber Security

- Vulnerability Assessment
- Types of Vulnerability Assessment
- Tools of Vulnerability Assessment

Vulnerability Assessment

The Information System is an integrated set of the component for collecting, storing, processing and communicating information. There are various phases involved in making an information system. One of such phases includes a review of the system security. All systems are prone to attacks like Cross-site scripting (XSS) and SQL injection. Thus, it is important that the organization reviews the system for possible threats beforehand. This helps in identifying the vulnerabilities and weaknesses of the system. This kind of systematic review of a system is called vulnerability assessment.

How does Vulnerability Assessment help?

It helps any organization safeguard itself from cyber-attacks by identifying the loopholes in advance. Here are some threats that we can prevent if we use vulnerability assessment.

- Injection attacks like XSS and SQL injection
- Authentication faults that lead to unidentified access to important data
- Insecure settings and weak defaults

What are the different types of Vulnerability Assessments?

Vulnerability assessments can be of different types depending on the need and type of a system.

- **Host Vulnerability Assessment:** Applications and information systems often use servers to work at the backend. Many attackers use these servers to inject threats in the system. Thus, it is important to test servers and review them for vulnerability.
- **Database Vulnerability Assessment:** Database is one of the most important aspect of any information system. It is where crucial user data is stored. Breach in a database system might lead to heavy losses. Thus, it is important to make sure that any outsider can neither access the data nor alter or destroy it. This can be done by assessing the database for possible threats and vulnerabilities.
- **Network Vulnerability Assessment:** Private as well as public networks are prone to injection attacks. Checking a network for possible issues is a better way to prevent huge losses in data.
- **Application Scan Vulnerability Assessment:** Most of the applications can be divided into two parts
    - The frontend
    - The backend

Both of these parts have their own source code which must be statically as well as dynamically analyzed for possible vulnerabilities. This assessment is often done through automated scans of the source code.

The Process of Vulnerability Assessment:

The process of Vulnerability Assessment is divided into four stages. Let us discuss them one by one.

- **Testing or Vulnerability Identification:** All the aspects of a system like networks, servers, and databases are checked for possible threats, weaknesses, and vulnerabilities. The goal of this step is to get a list of all the possible loopholes in the security of the system. The testing is done through machines as well as manually and all parameters are kept in mind while doing so.
- **Analysis:** From the first step, we get a list of vulnerabilities. Then, it is time that these are analyzed in detail. The goal of this analysis is to identify where things went wrong so that rectification can be done easily. This step aims at finding the root cause of vulnerabilities.
- **Risk Assessment:** When there are many vulnerabilities, it becomes important to classify them on the basis of risks they might cause. The main objective of this step is to prioritize vulnerabilities on the basis of data and systems they might affect. It also gauges the severity of attacks and the damage they can cause.
- **Rectification:** Once if have a clear layout of the risks, their root cause, and their severity, we can start making corrections in the system. The fourth step aims at closing the gaps in security by introducing new security tools and measures.

Tools for Vulnerability Assessment:

Manually testing an application for possible vulnerabilities might be a tedious job. There are some tools that can automatically scan the system for vulnerabilities. A few such tools include:

- Simulation tools that test web applications.
- Scanners that test network services and protocols.
- Network scanners that identify malicious packets and defects in IP addresses.

Advantages of Vulnerability Assessment:

- Detect the weakness of your system before any data breach occurs.
- A list of all possible vulnerabilities for each device present in the system.
- Record of security for future assessments.

Disadvantages of Vulnerability Assessment:

- Some advanced vulnerabilities might not be detected.
- Assessment tools might not give exact results.

Tools for Vulnerability Assessment

When it comes to vulnerability assessment, simulation tools are crucial for identifying, analyzing, and mitigating potential security risks. Here are some prominent simulation tools and frameworks you might find useful:

1. Nessus

- Type: Vulnerability Scanner

- Description: Nessus is one of the most widely used vulnerability assessment tools. It scans systems for known vulnerabilities and provides detailed reports and remediation guidance.

- Website: [Tenable Nessus](https://www.tenable.com/products/nessus)

2. Qualys

- Type: Cloud-based Vulnerability Management

- Description: Qualys offers a range of security and compliance solutions, including vulnerability management, which provides continuous monitoring and assessment of security risks.

- Website: [Qualys](https://www.qualys.com/)

3. OpenVAS

- Type: Open-Source Vulnerability Scanner

- Description: OpenVAS is part of the Greenbone Vulnerability Management (GVM) suite. It provides comprehensive vulnerability scanning and management.

- Website: [OpenVAS](https://www.openvas.org/)

4. Burp Suite

- Type: Web Application Security Testing

- Description: Burp Suite is a popular tool for web application security testing, including vulnerability scanning and penetration testing.

- Website: [Burp Suite](https://portswigger.net/burp)

5. Metasploit Framework

- Type: Penetration Testing Framework

- Description: Metasploit is widely used for penetration testing and exploitation. It allows for the testing of vulnerabilities and the exploitation of weaknesses in a controlled environment.

- Website: [Metasploit](https://www.metasploit.com/)

6. Rapid7 InsightVM

- Type: Vulnerability Management

- Description: InsightVM provides real-time vulnerability management with live dashboards and comprehensive reporting capabilities.

- Website: [InsightVM](https://www.rapid7.com/products/insightvm/)

7. IBM Security QRadar

- Type: Security Information and Event Management (SIEM)

- Description: QRadar provides vulnerability management as part of its broader SIEM capabilities, integrating log management and security analytics.

- Website: [IBM QRadar](https://www.ibm.com/security/security-intelligence/qradar)

8. Cuckoo Sandbox

- Type: Malware Analysis

- Description: Cuckoo Sandbox is an open-source automated malware analysis system that can simulate malware behavior and assess vulnerabilities in a controlled environment.

- Website: [Cuckoo Sandbox](https://cuckoosandbox.org/)

9. Threat Simulator

- Type: Threat Simulation

- Description: Threat simulators are used to mimic real-world attacks to test an organization’s defenses and response capabilities.

- Example: [AttackIQ](https://www.attackiq.com/), [SafeBreach](https://www.safebreach.com/)

10. GVM (Greenbone Vulnerability Manager)

- Type: Vulnerability Management

- Description: GVM is an open-source framework for vulnerability management that includes OpenVAS.

- Website: [GVM](https://www.greenbone.net/en/)

These tools vary in their focus and capabilities, so the best choice will depend on your specific needs, such as whether you are focusing on web applications, network infrastructure, or broader vulnerability management.

Dr. Ritika Ladha

Nessus Vulnerability Assessment Tool

Certainly! Here's a basic tutorial on using Nessus for vulnerability scanning and assessment. Nessus is a powerful tool developed by Tenable, designed to help you identify vulnerabilities in your network and systems.

Getting Started with Nessus

1. Installation

a. Download Nessus

- Visit the [Tenable Nessus download page](https://www.tenable.com/products/nessus/nessus-essentials).

- Choose the appropriate version for your operating system (Windows, macOS, or Linux) and download the installer.

b. Install Nessus

- Follow the installation instructions provided by Tenable. For example, on Linux, you might use `dpkg` or `rpm` commands, while on Windows, it's a standard installer.

c. Start the Nessus Service

- On Linux: `sudo systemctl start nessusd`

- On Windows: The Nessus service should start automatically after installation.

d. Access the Nessus Web Interface

- Open a web browser and go to `https://localhost:8834/` (replace `localhost` with your server's IP if accessing remotely).

2. Initial Setup

a. Create an Account

- When you first access Nessus, you'll be prompted to create an account. This is used to manage scans and access the interface.

b. Configure Nessus

- After creating an account, you'll need to set up the initial configuration. This includes activating your Nessus license (you'll receive a license key upon registration) and updating the Nessus plugins.

3. Creating and Running a Scan

a. Log In

- Log in to the Nessus web interface with your credentials.

b. Create a New Scan

- Navigate to the “Scans” tab on the dashboard.

- Click on “New Scan” to create a new scan.

c. Choose a Scan Template

- Nessus offers several scan templates, such as:

  - Basic Network Scan: For general network vulnerability assessments.

  - Web Application Tests: For assessing web application security.

  - Compliance Audits: For checking compliance with various standards.

d. Configure Scan Settings

- Name: Give your scan a descriptive name.

- Targets: Enter the IP addresses or hostnames of the systems you want to scan.

- Credentials: (Optional) If you want Nessus to perform authenticated scans, provide credentials here. This allows Nessus to log in to systems and perform more in-depth checks.

- Policies: Adjust scan policies as needed. This includes settings for the scan speed, the types of vulnerabilities to check, and other options.

e. Launch the Scan

- After configuring your scan, click “Save” and then “Launch” to start the scan.

- You can monitor the progress of the scan from the “Scans” tab.

4. Reviewing Scan Results

a. View Results

- Once the scan is complete, navigate to the “Scans” tab and select the completed scan.

- Click on the scan to view the results, which include:

  - Summary: Overview of vulnerabilities detected.

  - Vulnerabilities: Detailed list of vulnerabilities with descriptions, severity levels, and affected systems.

  - Reports: Generate and download reports in various formats (PDF, HTML, CSV).

b. Analyze Findings

- Review the findings to understand the vulnerabilities and risks associated with your systems.

- Use the information to prioritize remediation efforts.

5. Remediation

a. Address Vulnerabilities

- Follow the remediation steps provided in the Nessus reports. This may involve patching software, changing configurations, or other security measures.

b. Re-scan

- After addressing vulnerabilities, you should re-scan to ensure that the issues have been resolved.

6. Best Practices

a. Regular Scanning

- Perform regular scans to continuously monitor for vulnerabilities and ensure your systems remain secure.

b. Update Plugins

- Regularly update Nessus plugins to ensure you have the latest vulnerability checks.

c. Use Policies

- Create and use different scan policies for various types of assessments, such as network scans, web application tests, and compliance audits.

d. Secure Your Nessus Server

- Ensure that the Nessus server is properly secured and only accessible by authorized personnel.

Additional Resources

- Nessus Documentation: [Tenable Nessus Documentation](https://docs.tenable.com/nessus)

- Tenable Community Forums: [Tenable Community](https://community.tenable.com/)

By following these steps, you should be able to effectively use Nessus for vulnerability assessment.