Database Scanning with Scuba

Objective: Conduct database security assessments with Scuba.

Steps: 1. Install Scuba on your system.
2. Perform a database scan on a sample database.
3. Review the security assessment report.

Scuba is a free database vulnerability scanner developed by Imperva. It helps to identify potential security risks in various types of databases, including Oracle, SQL Server, MySQL, DB2, and others. Below is a detailed process on how to perform database scanning with Scuba, along with an example.

1. Download and Install Scuba
• Step 1: Download Scuba
Visit the Imperva website to download Scuba.
You'll need to register with Imperva to get the download link.

• Step 2: Install Scuba
Extract the downloaded zip file. Scuba is a Java-based application, so ensure you have Java installed on your machine.
No complex installation is required. Just extract the files and run the executable.

2. Setting Up Scuba for Scanning
• Step 1: Launch Scuba
Navigate to the Scuba directory and run the Scuba executable (scuba.sh for Linux or scuba.exe for Windows or scuba.command for Mac).
• Step 2: Configure the Database Connection
You need to provide details of the database you want to scan.

Enter the following details:

▪ Database Type: Select the database type (e.g., MySQL, Oracle, SQL Server).

▪ Hostname: Enter the IP address or hostname of the database server.

▪ Port: Enter the port number (default is 3306 for MySQL, 1521 for Oracle, etc.).

▪ Username and Password: Enter the credentials of a user with sufficient privileges to scan the database.

3. Running a Scan with Scuba

• Step 1: Choose a Scan Profile

Scuba provides predefined scan profiles based on common security best practices.

You can select a full scan or focus on specific areas like permissions, database configuration, or user account security.

• Step 2: After configuring the database connection and selecting the scan profile, click the "Start Scan" button.

Scuba will begin analyzing the selected database for potential vulnerabilities.

Step 3: Monitor the Scan Progress

Scuba provides real-time feedback on the scanning process. You can monitor the progress and see which checks are being performed.

4. Reviewing the Scan Results

• Step 1: View the Scan Summary

After the scan is complete, Scuba presents a summary of the findings, highlighting the most critical issues.

The summary includes an overview of the total number of vulnerabilities found and their severity levels (Critical, High, Medium, Low).

• Step 2: Detailed Vulnerability Analysis

Click on individual findings to see detailed information about each vulnerability.

Scuba provides:

▪ Description: A brief explanation of the vulnerability.

▪ Risk Level: The severity of the vulnerability.

▪ Recommendation: Steps to remediate the issue.

▪ Affected Objects: Specific database objects (e.g., tables, views) impacted by the vulnerability.

Conclusion

Scuba provides a powerful and user-friendly tool for scanning databases for vulnerabilities. By following the detailed steps outlined above, you can ensure that your databases are regularly assessed for security risks and that appropriate measures are taken to protect sensitive data. Regular scanning, combined with timely remediation, forms the backbone of a robust database security strategy.

LINKS

For scuba installation

https://www.imperva.com/resources/free-cyber-security-testing-tools/scuba-database-vulnerability-scanner/

For java installation

https://youtu.be/Co5DMRh9RjE?si=UlxolQ-viREPzgrh