Software Requirements Specification (SRS)

Vulnerability Scanning and Applicable Patch Management

Problem Statement

A primary reason for security breaches is unpatched software. In many cases, identified vulnerabilities are not being patched by users, which makes their systems an easy target for malicious attackers. The reasons for incomplete and ineffective patch management are:

- Lack of awareness on vulnerabilities and patch availability
- Uncertainty on which patch to be applied considering dependencies.

It is proposed to build an application which scans for assets on a machine, identifies vulnerable assets using the NVD database and notifies the user about vulnerable assets and their corresponding patches.

User Profile

1. End users: these consist of **individuals** or **IT administrators** who are responsible for maintaining software security on personal or organization devices.

    - **Technical knowledge:** these users' technical expertise in vulnerability management may range from limited to adept, but at the bare minimum they would be comfortable navigating a command-line/application interface.

Project Modules

1. **Frontend/User Interface**: Command-line interface which the users will have direct access to. Will contain all accessible functionalities of the project.

(Tentatively it is a CLI, it could be changed to an application in the future)

a. Scanning functionality:
    - Initiates an asset scan on the user device, by triggering the Asset Scanner to check for installed software and packages.

b. Display vulnerabilities
    - Shows a list of detected vulnerabilities for each asset, fetched from the NVD Server.
    - Provides details on each vulnerability, including:
        - CVSS (Common Vulnerability Scoring System) score to help users prioritize patching based on severity.
        - Vulnerability description and any dependencies or patch prerequisites.
    - **Provision to Select Vulnerabilities for Patching**:
        - Users can review each vulnerability and select specific ones for patching.

2. **NVD Server**: a backend server which serves as the central component for vulnerability data. It maintains information on vulnerabilities sourced from the National Vulnerability Database (NVD), including associated CVSS scores, and provides this data to the frontend when queried.

   This component would be queried after the server has finished collecting information on the list of applications and packages using the Asset Scanner. It would return relevant vulnerability data for each asset.

    - **Vulnerability Database**: Stores information on each vulnerability, including:
        - Vulnerability description and associated CVSS scores.
        - Relevant metadata for each vulnerability, such as affected versions and recommended fixes.
    - **Query Interface**: The NVD Server provides an API that the frontend can query to retrieve vulnerability information for detected assets. The query

interface returns relevant vulnerabilities and CVSS scores for assets identified by the Asset Scanner.

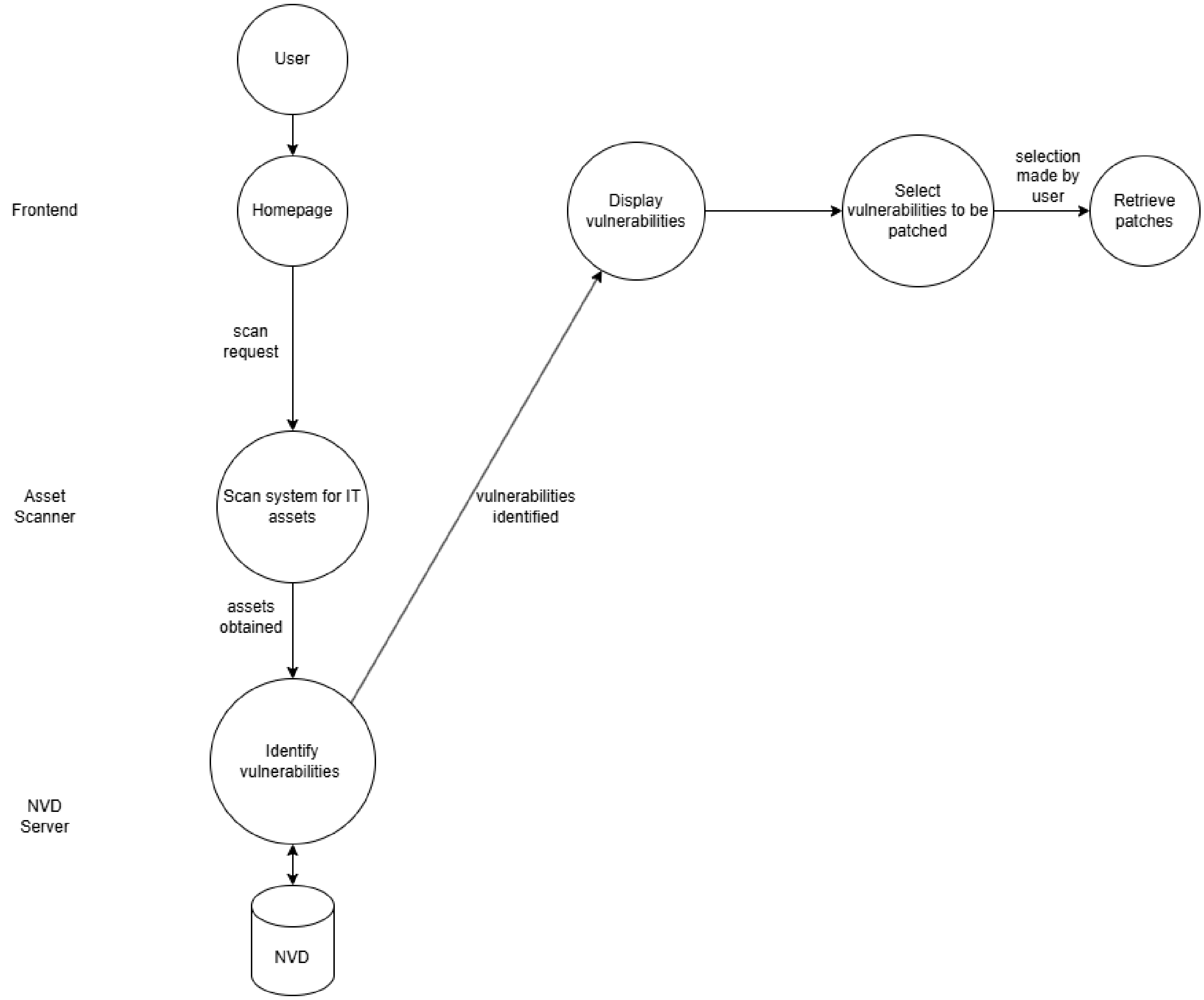
- **Daily Update Provision**:
    - Ensures the server database is updated daily with the latest vulnerability information from NVD.
    - Could use automated scripts to pull new vulnerabilities or updated CVSS scores, allowing the frontend to access current data.

3. **Asset Scanner**: The Asset Scanner is a utility that runs on the user’s device to detect and list all installed applications and packages. The list is sent to the **NVD Server** to check for vulnerabilities. The scanner can run on-demand or on a periodic basis.
    - **System Scan:**
        - Scans the device for installed software, packages, libraries, and relevant versions.
        - Maintains metadata in the form (Package Name, Version)

Feature Requirements

Sr No	Name	Description
1	Asset Detection	The system detects and lists all IT assets (applications, packages) on the user’s device.
2	Vulnerability Identification	The system accesses the National Vulnerability Database (NVD) and retrieve vulnerability information for each asset, along with CVSS scores.
3	Vulnerability Notification	The system notifies the user about vulnerabilities identified, along with CVSS severity score
4	Patch Selection	Users can review the list of vulnerabilities and choose which ones they wish to patch.
5	Patch Retrieval	The system retrieves the selected patches from the respective company websites.

Use-case diagram


User
Frontend
Homepage
scan request
Asset Scanner
Scan system for IT assets
assets obtained
NVD Server
Identify vulnerabilities
NVD
vulnerabilities identified
Display vulnerabilities
Select vulnerabilities to be patched
selection made by user
Retrieve patches