OpenVAS Cheat Sheet

A comprehensive cheat sheet for using OpenVAS, covering installation, configuration, scanning, and reporting.

Installation and Setup

Installation (Kali Linux)

1. **Update Package Lists:**
   ```
   sudo apt update
   ```
2. **Install OpenVAS:**
   ```
   sudo apt install openvas
   ```
3. **Setup OpenVAS:**
   ```
   sudo openvas-setup
   ```
   Note: This process can take a significant amount of time as it downloads and configures vulnerability tests.
4. **Start OpenVAS Services:**
   ```
   sudo systemctl start openvas-scanner
   sudo systemctl start openvas-manager
   ```
5. **Verify Services Status:**
   ```
   sudo systemctl status openvas-scanner
   sudo systemctl status openvas-manager
   ```

Initial Configuration

1. **Access Web Interface:**
   Open a web browser and navigate to `https://localhost:9392`.
2. **Login:**
   Use the credentials created during `openvas-setup` or default credentials if not changed.
3. **Update Feeds:**
   Ensure vulnerability feeds are up-to-date to get the latest vulnerability definitions. This is usually handled automatically but can be triggered manually if needed.

Troubleshooting Installation

1. **Feed Status:**
   Check the feed status to ensure vulnerability definitions are current:
   ```
   sudo openvas-feed-update
   ```
2. **Service Issues:**
   If services fail to start, check logs for errors:
   ```
   sudo tail -f
   /var/log/openvas/openvasmd.log
   sudo tail -f
   /var/log/openvas/openvassd.messages
   ```
3. **Rebuild Database:**
   If issues persist, try rebuilding the OpenVAS database:
   ```
   sudo openvasmd --rebuild
   ```

Basic Scanning Operations

Creating a New Target

1. **Navigate to Targets:**
   In the OpenVAS web interface, go to 'Configuration' -> 'Targets'.
2. **Create New Target:**
   Click on the '+' icon to create a new target.
3. **Define Target Details:**
   Enter the target's name, IP address, and other relevant details.
   Ensure the 'Alive Test' is configured correctly (e.g., ping, TCP port).

Creating a New Task

1. **Navigate to Tasks:**
   Go to 'Scans' -> 'Tasks'.
2. **Create New Task:**
   Click on the '*' icon to create a new task.
3. **Define Task Details:**
   - Enter a task name.
   - Select the target created earlier.
   - Choose a scan configuration (e.g., Full and Fast).
4. **Start the Task:**
   Click 'Create' to create the task, then click the 'Play' button to start the scan.

Monitoring a Scan

1. **Task Status:**
   Monitor the task status in the 'Tasks' section. It will show the progress, current stage, and any errors.
2. **Real-time Updates:**
   The web interface provides real-time updates as the scan progresses.

Reporting and Analysis

Viewing Scan Results

1. **Access Results:**
   Once the scan is complete, click on the task to view the results.
2. **Vulnerability Details:**
   The results show a list of vulnerabilities found, their severity, and details.
3. **Filtering and Sorting:**
   You can filter and sort the results based on severity, CVSS score, and other criteria.

Generating Reports

1. **Report Formats:**
   OpenVAS supports generating reports in various formats (e.g., PDF, XML, HTML).
2. **Generating a Report:**
   Click on the 'Report' icon for the completed task and choose the desired format.
3. **Customizing Reports:**
   You can customize reports by including or excluding specific vulnerability details.

Analyzing Vulnerabilities

1. **Understanding Vulnerability Details:**
   Each vulnerability report includes detailed information about the vulnerability, its potential impact, and recommended solutions.
2. **CVSS Scores:**
   Pay attention to the CVSS (Common Vulnerability Scoring System) score, which indicates the severity of the vulnerability.
3. **Remediation Steps:**
   Follow the recommended remediation steps provided in the report to mitigate the vulnerabilities.

Advanced Configuration

Configuring Scan Targets

1. **Target Alive Test:**
   Configure the 'Alive Test' settings to accurately determine if a target is online (e.g., using ping, TCP, or ARP).
2. **Port Lists:**
   Define custom port lists to specify which ports to scan on the target.
3. **Excluding Hosts:**
   Exclude specific hosts or networks from the scan if needed.

Scan Configuration

1. **Scan Configuration Sets:**
   OpenVAS provides various scan configuration sets (e.g., Full and Fast, Discovery).
2. **Custom Scan Configurations:**
   You can create custom scan configurations to tailor the scan to your specific needs.
3. **QoS (Quality of Service):**
   Configure QoS settings to limit the impact of the scan on network resources.

User Management

1. **Creating Users:**
   Create new user accounts with specific roles and permissions.
2. **Role-Based Access Control (RBAC):**
   Use RBAC to control access to different features and functionalities in OpenVAS.
3. **Authentication Methods:**
   Configure different authentication methods for users (e.g., local authentication, LDAP).