OpenVAS

OpenVAS is an open-source vulnerability scanning and management tool that helps to identify security issues like misconfigurations, outdated software, and weak passwords that could be exploited by attackers. OpenVAS is widely used by security professionals to assess and improve the security posture of their networks and is known for its effectiveness and flexibility. This article explores how OpenVAS works, its features, and how it can be used to enhance cybersecurity.

1. What is OpenVAS?

Open Vulnerability Assessment System (OpenVAS) is free software that is used to detect and manage vulnerabilities in computer systems and networks. It provides various services and tools for vulnerability assessment such as identifying and analyzing security issues such as misconfigurations, outdated software, and weak passwords that could be exploited by attackers.

2. Working of OpenVAS

OpenVAS consists of a server and various client-side tools for scanning and reporting. It uses a regularly updated database of known vulnerabilities and checks systems against these to detect potential weaknesses. The tool performs a comprehensive scan of the specified targets, identifying potential vulnerabilities such as outdated software, misconfigurations, and weak passwords and generates comprehensive reports detailing the identified vulnerabilities and provide recommendations for remediation.

A vulnerability assessment tool works in the following way as follows.

1. Classifies the system resources.
2. Allocates the enumerable values to the classified resources.
3. Detects the possible threats (vulnerabilities) in each resource.
4. Eliminates the vulnerabilities on a priority basis.

3. Components of OpenVAS architecture

a. OpenVAS Scanner:

The primary engine that performs the actual scanning of target systems. It uses Network Vulnerability Tests (NVTs) to detect security vulnerabilities.

b. OpenVAS Manager:

Manages scan configurations, schedules, and stores scan results. It acts as an intermediary between the scanner and the user interfaces, handling scan requests and processing results.

c. Greenbone Security Assistant (GSA):

A web-based graphical user interface (GUI) that allows users to manage scans, configure settings, and view scan results. It provides an easy-to-use platform for interacting with OpenVAS.

d. OpenVAS CLI:

A command-line interface for users who prefer scripting and command-line operations. It enables management of scans, targets, and results through commands and scripts.

e. Greenbone Security Feed (GSF):

A continuously updated feed that provides the latest Network Vulnerability Tests (NVTs) and security information. It ensures OpenVAS can detect the most recent vulnerabilities.

f. OpenVAS Libraries:

These libraries provide essential functionalities required by the scanner and manager, such as network communication, data storage, and cryptographic operations.

g. Database:

The database stores scan results, configurations, and other essential data. It ensures data persistence and retrieval for analysis and reporting purposes.

4. Leveraging OpenVAS in Vulnerability Management

Vulnerability management is an essential aspect of cybersecurity, and OpenVAS plays a pivotal role in this process. Here's how:

1. Detection

OpenVAS helps organizations detect vulnerabilities by scanning their network and systems regularly. This proactive approach allows for early detection and mitigation, reducing the window of opportunity for potential attackers.

2. Prioritization

Not all vulnerabilities are created equal. OpenVAS assists in prioritizing remediation efforts by categorizing vulnerabilities based on their severity and potential impact. This ensures that resources are allocated to address the most critical issues first.

3. Remediation

Once vulnerabilities are identified, OpenVAS provides guidance on how to remediate them effectively. After implementing remediation measures, subsequent scans can verify the success of these actions.

4. Compliance Reporting

For organizations subject to regulatory requirements, OpenVAS generates compliance reports that demonstrate adherence to security standards and provide evidence of vulnerability assessment efforts.

References:

- https://eunishap.medium.com/vulnerability-scanning-with-openvas-unveiling-cybersecurity-insights-eff56de79276
- https://www.geeksforgeeks.org/security-assessment-openvas/