What is OpenVAS?

Reading

35m

Status | Incomplete

Introduction

In this section, you will explore Open Vulnerability Assessment Scanner (OpenVAS), an open-source vulnerability scanner that you will make use of in our upcoming case study activity.

Why OpenVAS?

For Students using Eve

While there are other scanning tools available, OpenVAS is the one you will find in the EVE environment.

For Students Using VirtualBox

While there are other scanning tools available, OpenVAS is the one you will be using in the following exercises (on the KaliOpenVas VM).

Understanding how the tool works will help you be ready for the case study assignment later in this unit.

OpenVAS Overview

OpenVAS is an open-source Linux-based vulnerability scanner supported by a community spearheaded by the German organization Greenbone Networks. The major tool modules are all open source, but there is a turnkey appliance and a cloud service available for enterprise clients that wish to use a solution that is simpler to implement and use.

The architecture of the OpenVAS system includes three main parts:

- The scanner applications that run the vulnerability tests.
- The Greenbone Vulnerability Manager (GVM) database.
- The Greenbone Security Assistant (GSA).

What's in a Name?

In this course, you will see this system referred to as OpenVAS.

> In industry documentation, you may also see it referred to by its formal name, Greenbone Vulnerability Manager (GVM). Confusingly, the GVM name can also be used to refer specifically to the database portion of the architecture.
>
> Read more about the evolution of the system (and the names) here

> ⚠ When looking for supporting documentation, try searching under both names (OpenVAS and GVM) to find a wider breadth of information, and double-check which part of the system you are reading about.

Greenbone Vulnerability Manager

The Greenbone Vulnerability Manager daemon (GVMD) is the heart of the overall system. It brings functionality like the ability to control the scanner applications, directly and remotely, a database that stores configuration information and all scan results, user management and permissions control with groups and roles, as well as the ability to schedule tasks and other events.

Greenbone Security Assistant

The GSA is a web-based user interface that connects to and communicates with the GVMD. It acts as the main interface and control mechanism for users and is the way users control scans and access vulnerability information.

OpenVAS and Notus

The OpenVAS Scanner and the Notus Scanner are the scanning applications used by this system. They are the engines used to compare information from the target system(s) being scanned to known vulnerabilities, allowing the vulnerability management system to inform users of any discovered potential vulnerabilities.

Additional Tools

There are additional tools, such as Greenbone Vulnerability Management Tools (gvm-tools), that are also available to provide remote control of either the Community Edition or Enterprise Appliances, as well as other tools to allow more customizable communication and programming options for the system, but those are beyond the scope of this course.

OpenVAS vs. Other Systems

> ? How does the Greenbone OpenVAS/GVM system compare to a commercial system like Tenable's Nessus?

That is a good question. Although both systems have essentially the same purpose, they are very different tools and implementations.

Tenable's Nessus is an expensive, proprietary software aimed at large enterprises. It is also created and used in a way that it can be utilized by non-security persons, is a globally recognized name, and is partnered with other globally recognized names.

Greenbone's OpenVAS/GVM is a much smaller name, is aimed at any size of organization, is open source (and therefore free), and is community supported. Because the original and ongoing goal of this project is to provide vulnerability scanning and management capabilities to anyone and everyone, there aren't partnerships with all kinds of large global organizations. That also means that anyone out there can develop and submit fixes and features for it.

Both systems are able to be set to automate scans and provide information about discovered vulnerabilities, including severity, details, and remediation recommendations. However, Nessus also includes services like IDS/IPS alerts and firewall rule sets.

Does all this mean that you should go with the paid solution over the open-source one? Not necessarily.

The key to making the right choice is awareness. You should be aware of what you need to know and do in order to plan for, implement, use, and maintain the system you choose. If you don't have, or are not interested in investing the time to learn about and administrate a highly hands-on system like OpenVAS/GVM, it might be better to look into a system like the Greenbone Hardware Appliance or Cloud Service, or the Tenable Nessus software (or one of the many other paid solutions that are out there).

Further Reading

To learn more about OpenVAS and GVM projects and systems, you can begin by exploring and reading these pages:

- Greenbone OpenVAS
- Greenbone Community Documentation: Background
- Greenbone: Vulnerability Timeline
- Datamation, OpenVAS vs. Nessus: Top Vulnerability Scanners Compared

> **Learning How to Learn**
>
> Save the links to these readings into your PKM system, along with any accompanying notes or descriptions that you think might be useful in upcoming studies, or in your future Cyber Security career.

- What is OpenVAS?
- Accessing OpenVAS
- Using OpenVAS/GVM

W05D3 Schedule »