OpenVas security assessment using Greenbone Vulnerability Management, GVM.

Kali Linux:

Step 1: Update Your System

Before installing any new software, it's a good practice to update your system. Open a terminal and run the following commands:

sudo apt update

sudo apt full-upgrade -y

sudo reboot

Step 2: Install GVM

Kali Linux has GVM in its repositories, so you can install it directly using the apt command. In your terminal, run:

sudo apt install -y gvm

Step 3: Run the Setup

After installing GVM, you need to run the initial setup. This will configure the various components of GVM, including creating the database. Execute:

sudo gvm-setup

Step 4: Check GVM Status

You can check the status of GVM services by running:

sudo gvm-check-setup

This command verifies that your GVM setup is configured correctly.

Step 5: Start Greenbone Security Assistant

GVM comes with a web interface called Greenbone Security Assistant (GSA) that allows you to manage your scans via a web browser.

The setup script should have already started the GSA service, but you can ensure it's running by checking the service status:

sudo systemctl status gvmd

By default, GSA is accessible at https://<Your-Kali-IP-Address>:9392. You might need to configure your firewall to allow access to this port if you're accessing it from a different machine.

Step 6: Log in to GSA

Open your web browser and navigate to https://<Your-Kali-IP-Address>:9392.

Log in using the credentials provided by the gvm-setup command. If you didn't note the credentials or need to change them, you can create a new admin user with the following command:

sudo gvm-create-user <username> --password=<password>

Replace <username> and <password> with your desired username and password.

Scanning Process

The steps outlined for setting up and using GVM (Greenbone Vulnerability Management) on Kali Linux will allow you to perform vulnerability scans on Windows machines within your network as well. GVM is designed to be agnostic to the operating systems of the target machines. It can scan and identify vulnerabilities in various operating systems, including Windows, by checking for known vulnerabilities in the software and configurations used by the devices on your network.

Here's how GVM can verify Windows machines on your network:

Target Configuration:

When you configure your scan within GVM, you specify the targets (IP addresses or ranges) that you want to scan. Include the IP addresses of your Windows machines in this target configuration.

GVM uses a comprehensive and regularly updated database of vulnerability tests, known as Network Vulnerability Tests (NVTs), to scan targets for known vulnerabilities. These tests cover a wide range of software and operating systems, including various versions of Windows.

Scanning Process

During the scanning process, GVM will attempt to identify the operating system and installed software on each target machine using banner grabbing and other enumeration techniques.

Once it has identified the software and its versions, GVM will check against its database of known vulnerabilities that match the identified software and configurations.

If vulnerabilities are found, GVM will include them in the scan report, indicating the severity and providing references for further information.

Reporting

The final report generated by GVM will detail the vulnerabilities discovered during the scan. This report includes information specific to the Windows machines scanned, such as vulnerability descriptions, severity ratings, and recommendations for remediation.

The report can be used to prioritize and address vulnerabilities within your network, including those on Windows systems.

Considerations:

Ensure your Windows machines are configured to allow scans. In some cases, firewall or security settings may block scanning attempts from tools like GVM. Adjusting these settings may be necessary to ensure accurate and comprehensive scanning.

Regularly update the vulnerability feed of GVM to ensure it can detect the latest known vulnerabilities, including those affecting Windows systems.

REFERENCES:

1. Greenbone Networks. (n.d.). Documentation. Retrieved from https://docs.greenbone.net/

2. Offensive Security. (n.d.). Kali Linux Documentation. Retrieved from https://www.kali.org/docs/

3. OpenVAS. (n.d.). OpenVAS - Open Vulnerability Assessment Scanner. Retrieved from http://www.openvas.org/

4. Kali Linux. (n.d.). Tools Listing. Retrieved from https://www.kali.org/tools/

5. Tutorials Point. (n.d.). Kali Linux Tutorial. Retrieved from https://www.tutorialspoint.com/kali_linux/index.htm