**Task 3: Perform a Basic Vulnerability Scan on Your PC**

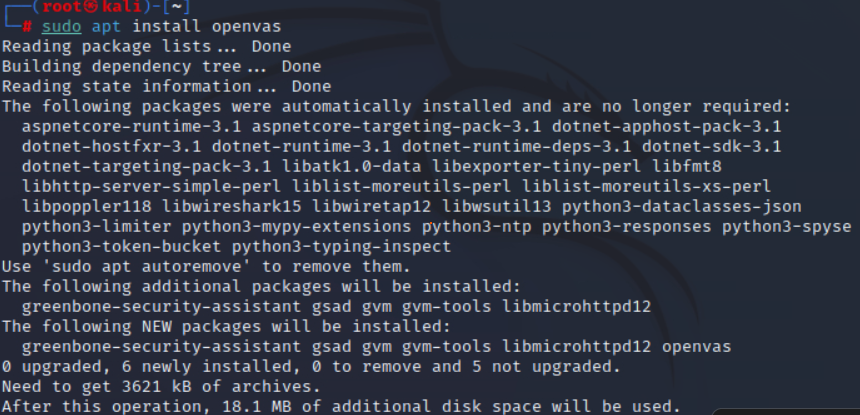
**Objective**: Use free tools to identify common vulnerabilities on your computer.

**Tools**: OpenVAS Community Edition (free vulnerability scanner) or Nessus Essentials.

**Deliverables**: Vulnerability scan report with identified issues

**Outcome**: Introductory vulnerability assessment experience and understanding of common PC risks

***1. Install OpenVAS using the GVM setup***



***sudo gvm-setup***

***sudo gvm-check-setup***

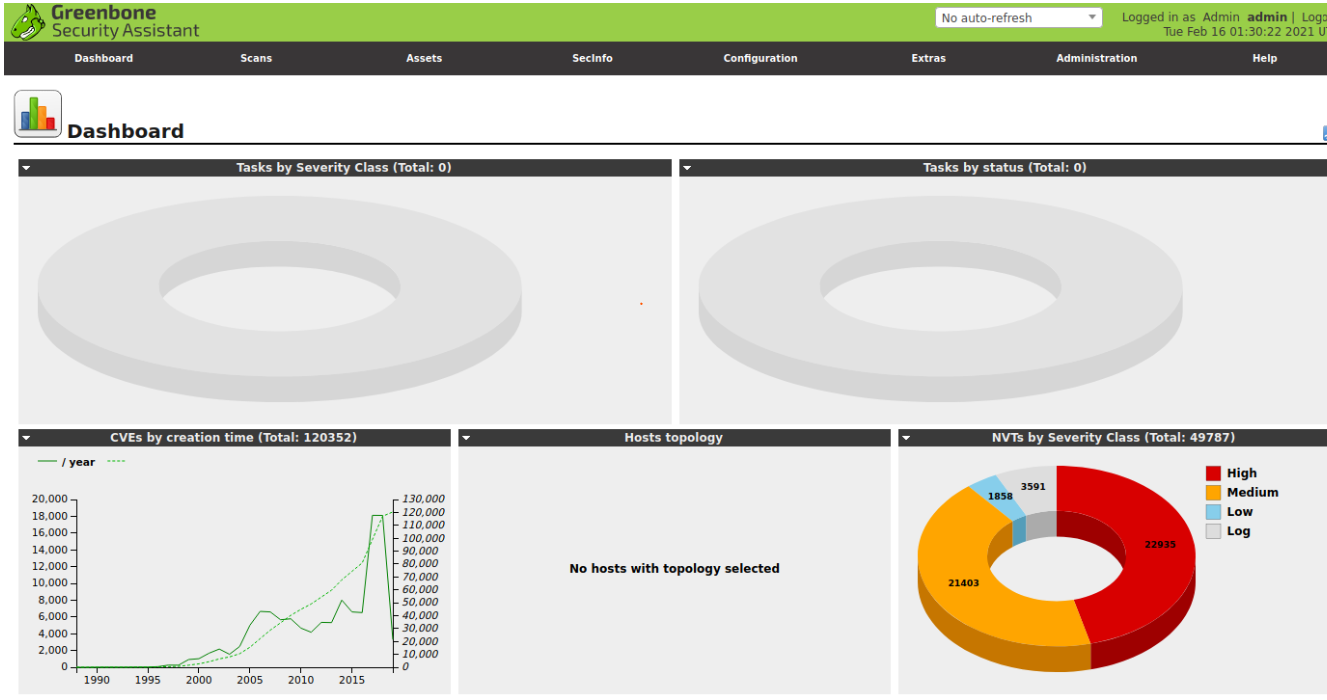
***2. Set up the scan target as your local machine IP or localhost.***

Once it is complete you can then navigate to [https://127.0.0.1](https://127.0.0.1/) in your preferred browser and OpenVAS will be setup and ready to go!

Below are the default credentials to access OpenVAS/GVM:

**Username:** admin

**Password:** admin



***3. Start a full vulnerability scan.***

Begin by navigating to *Scans > Tasks* and clicking on the purple magic wand icon to begin the basic configuration wizard. We recommend beginning a scan on 127.0.0.1 to test out your installation and ensure it is working properly.

A screenshot of a computer

AI-generated content may be incorrect.

If you successfully navigated to the wizard, you should see a pop-up similar to the one above. This is where you will set up your initial scan against your localhost to ensure everything is properly configured.

The scan may take a while to complete, allow OpenVAS enough time to finish the scan, and then you will be met with a new dashboard for monitoring and analyzing your complete and ongoing scans like the one below.

A screenshot of a computer

AI-generated content may be incorrect.

Once your scan has finished you can navigate to *Scans > Reports* and click on your newly created report from your previous task.

A screenshot of a computer

AI-generated content may be incorrect.

If correctly configured you should see three different vulnerabilities reported all originating from OpenVAS itself. This is normal behavior and can be configured/changed to maintain your OpSec.

A screenshot of a computer

AI-generated content may be incorrect.

Scan as the same for our IP address ***192.168.1.98***.

***4. Review the report for vulnerabilities and severity.***

The automated report from OpenVAS begins with some basic host and task information, including Host, Start, End, and Vulnerability categories. It will also check for host authentications and an overall summary of open ports on the host.

A screenshot of a computer

AI-generated content may be incorrect.

***5. Research simple fixes or mitigations for found vulnerabilities***

After the basic host and task information, OpenVAS will report on each of the vulnerabilities found.

A screenshot of a computer

AI-generated content may be incorrect.

***6. Vulnerability Documentation***

Vulnerability Name: OS End of Life Detection  
Severity: High (CVSS: 10.0)

Affected System

* Operating System: Ubuntu Linux
* Version: 8.04
* CPE: cpe:/o:canonical:ubuntu\_linux:8.04
* End of Life Date: 2013-05-09
* Reference: Ubuntu Releases Wiki

Summary

The operating system installed on the host has reached end-of-life (EOL). This means it no longer receives security updates, patches, or support from the vendor. Using EOL software exposes the system to known and unknown vulnerabilities, making it highly susceptible to attacks.

Vulnerability Detection Result

* The scanner detected that Ubuntu 8.04 is installed.
* The system has exceeded its EOL date (May 9, 2013).
* The system is at risk because it does not receive security patches or updates.

Solution / Mitigation

Recommended Action: Upgrade the operating system to a supported version (e.g., Ubuntu 24.04 LTS or the latest supported LTS).

* Backup critical data before upgrading.
* Test critical applications on the new OS version to ensure compatibility.
* Apply the latest patches and updates after the OS upgrade.

Solution Type: Mitigation

Vulnerability Detection Method

* Method Used: OS End of Life Detection
* OID: 1.3.6.1.4.1.25623.1.0.103674
* Version used by scanner: $Revision: 8927 $

----------------------------------------------------------------------------------------------