Hello Everyone! In this exercise You will learn about OpenVAS scanner which is a vulnerability assessment system that can detect security issues in all manner of servers and network devices.

OpenVAS is developed and maintained by Greenbone Networks since 2009. The works are contributed as Open Source to the community under the GNU General Public License (GNU GPL). It is a Linux-based scanner and can be installed on almost any Linux distribution. To perform vulnerability scanning using OpenVAS, first, install OpenVAS on a Linux OS. Then open a terminal and type OpenVAS-start to start it. The OpenVAS tool will be started in a browser. Login using user id and password.

To start the vulnerability scanning using Open VAS, the first step is to create and configure a target (the machine/computer to scan) using the OpenVAS/Greenbone Security Assistant web interface. Click configuration and then new target.(The blue star can also be clicked). After hitting the new target button, a dialog screen appears where we have to enter the following information:

1. Target name,
2. The target IP host which is the IP address of the target machine.(addresses can also be provided In the form of CIDR range or in a file. Keep all other settings default and click the ‘Create’ button.

The next step is to create a new scanning task. A scanning task defines which targets will be scanned and also the scanning options such as a schedule, scanning configuration and concurrently scanned targets and NVTs per host. To create a new scan task, Click scans -> Tasks and then new task. After clicking the new scan option, a dialog screen appears where we have to enter the following information:

1. Task name, we'll name it 'Scan target name'.
2. Make sure that the target, created earlier is selected.
3. Tick the schedule once checkbox.
4. Keep all other settings default and click the 'Create' button to create the new task.

The newly created task will now appear in the task list.
To run the newly created task we just have to click the green start button.

The scan task will now execute against the selected target. Please note that full scan may take a while to complete. The progress for the executed task can be checked by refreshing the task page.

1. Reload the page.
2. Check task status/progress.

After waiting a while, the scan task is finished and the status changes to 'Done'. The vulnerability scan is finished after this.

Now that the vulnerability scan is finished report can be browsed by clicking on ‘Scans -> Reports’ in the top menu. On the reports page, a report for the completed scanning tasks can be found. By clicking the report name, an overview of all discovered vulnerabilities on the target machine can be displayed. The results are ordered on severity rate by default.

By clicking on the vulnerability name ,an overview of the details regarding the vulnerability can be found. Finally, the report can also be exported in a variety of formats, such as: XML, HTML and PDF. It can be done by selecting the desired format from the drop-down menu and clicking the green export icon.

Thank You.