

Vulnerability Assessment with OpenVAS Module

(20-25 mins)

Learning Outcomes

- Understand the importance of discovering system vulnerabilities using detailed scans.
- Analyze the severity of their impacts and potential solutions to patch critical vulnerabilities.

About OpenVAS:

OpenVAS is a framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution. The framework is part of Greenbone Networks' commercial vulnerability management solution from which developments are contributed to the Open Source community since 2009.

Open “**team#_wadc-adversary**” VM console

```
Username: root
Password: root
```

Procedure:

Step 1: Starting OpenVAS

To start OpenVAS, open the wadc-adversary VM terminal and execute the command on the terminal:

```
openvas-start
```

Step 2: Login and Starting a Scan

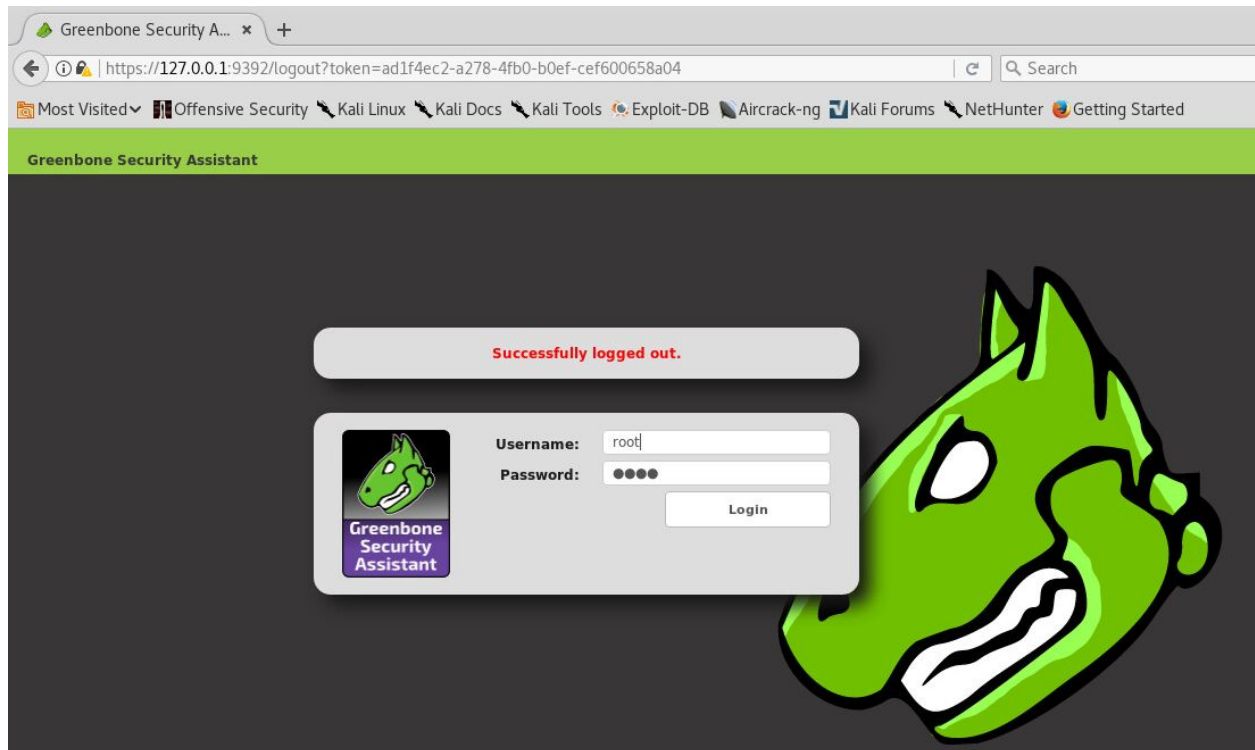
Open a web browser (Firefox ESR) and navigate to:

<https://127.0.0.1:9392/login/login.html>

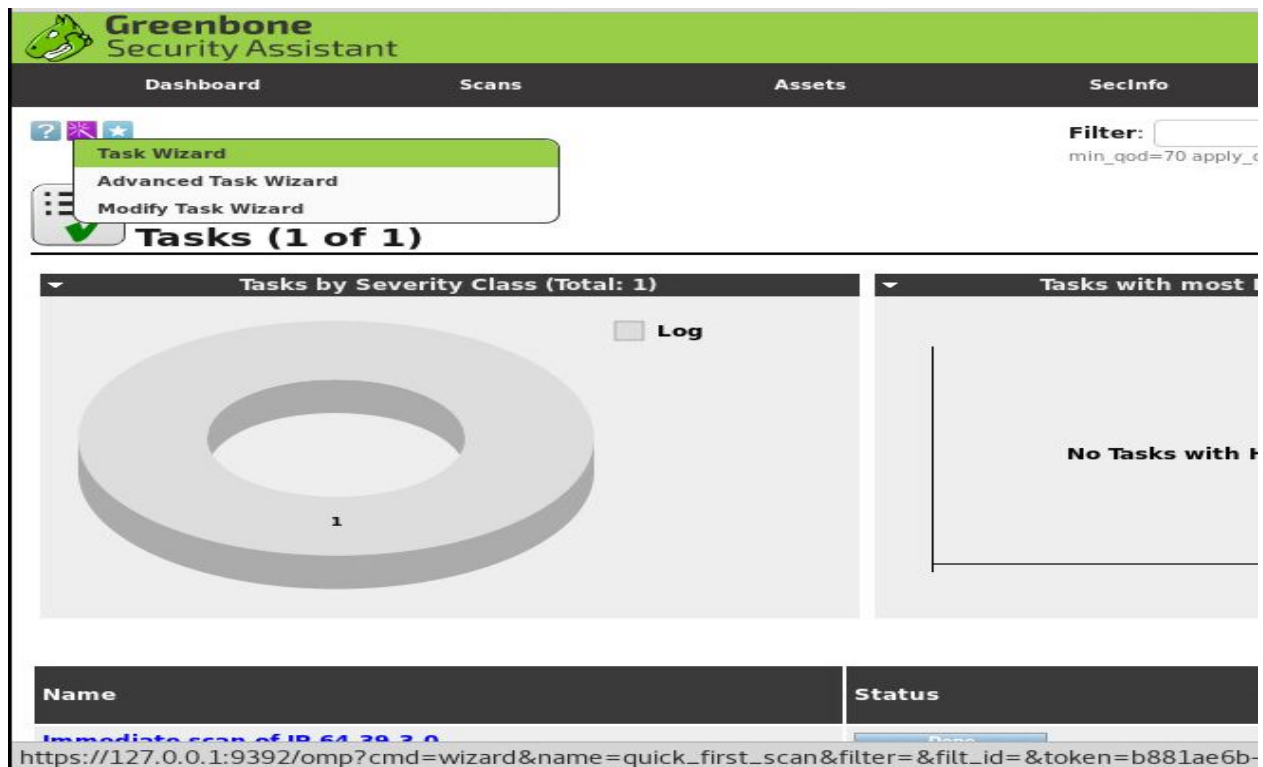
We have placed a bookmark on the browser's toolbar with a link to this page. Click on Greenbone Security Assistant and it will take you to the webpage

The login credentials are as follows:

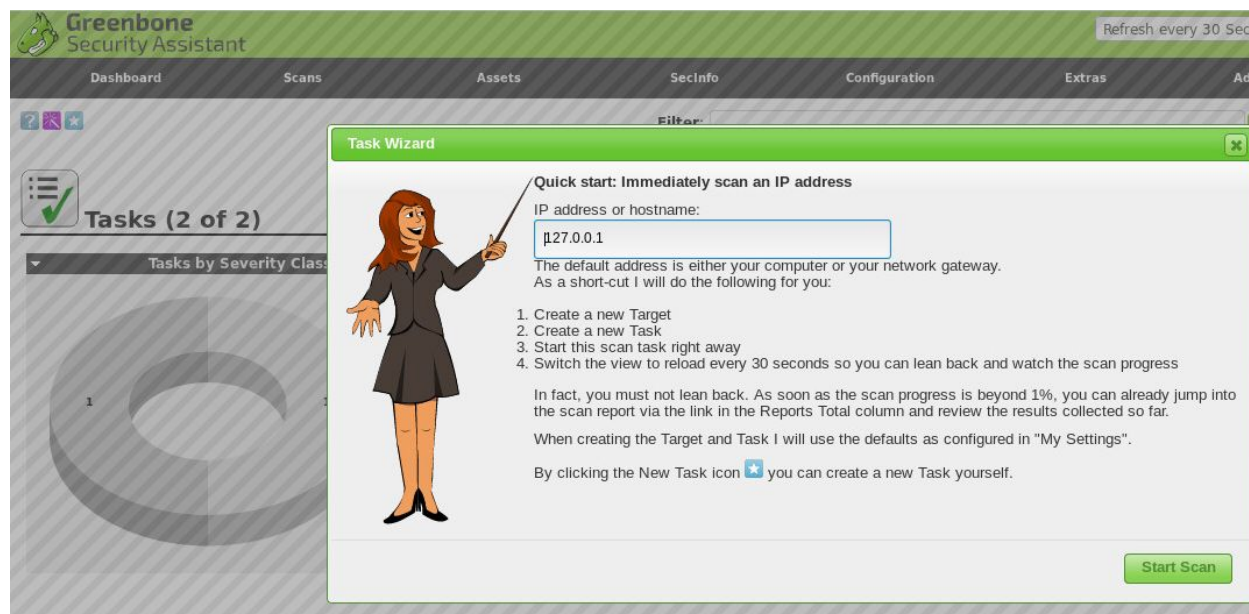
```
Username: root
Password: root
```



To start a scan, Click on Scans ---> Tasks and then click on **Task Wizard**.

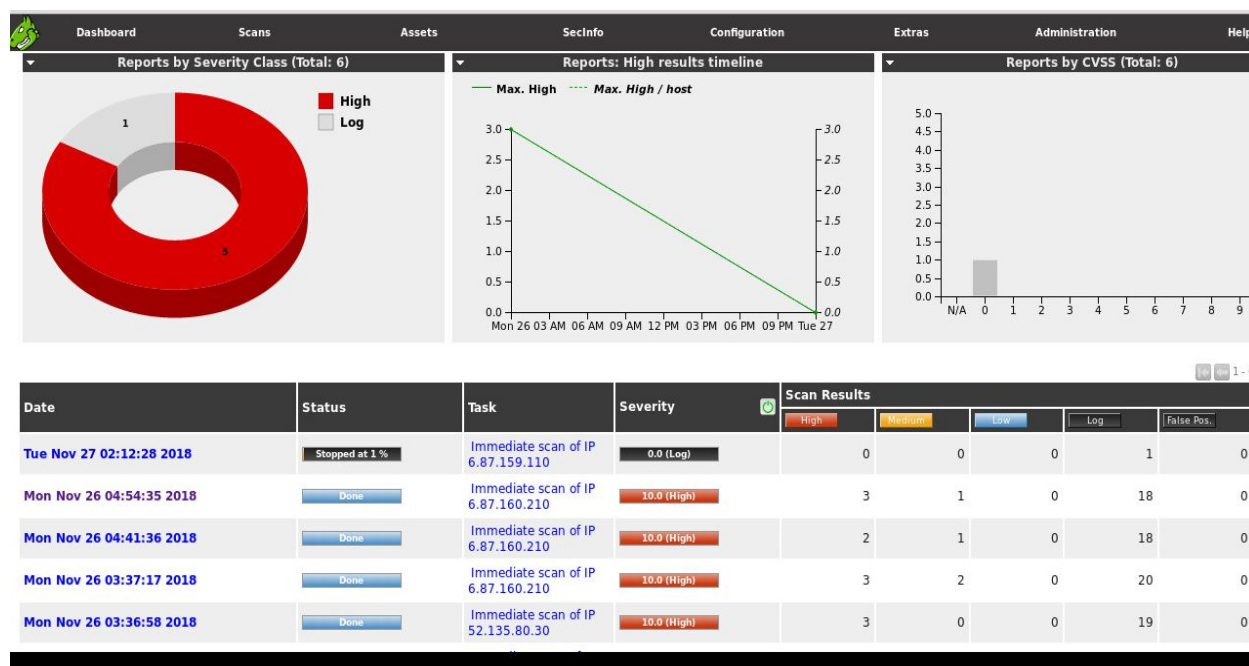


Enter an IP address in the Task Wizard and click “Start Scan”
 You should then see a new scan appear in progress in the list of tasks

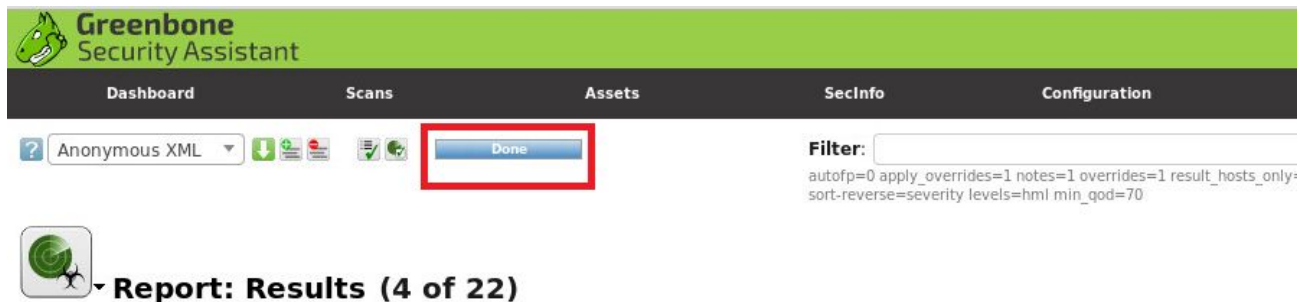


Step 3: Report Viewing

To view the report of the scan, go to **Scans** → **Reports**. The first column “Date” shows the date/time when the task was started and the third column “Task” shows the IP address that is being scanned.



To view a report, click on the date of a task which will navigate you to the results of the scan for that particular task. This can be done even if the scan is not completed yet. Now click on the “Done” button at the top to get a list of reports available for download for that task.



The screenshot shows the Greenbone Security Assistant interface. The top navigation bar includes Dashboard, Scans, Assets, SecInfo, and Configuration. Below the navigation bar, there is a search bar with 'Anonymous XML' and a 'Done' button highlighted with a red box. To the right of the 'Done' button, there is a 'Filter:' section with a text input field and a list of filter parameters: autofp=0, apply_overrides=1, notes=1, overrides=1, result_hosts_only=1, sort-reverse=severity, levels=hml, min_qod=70.

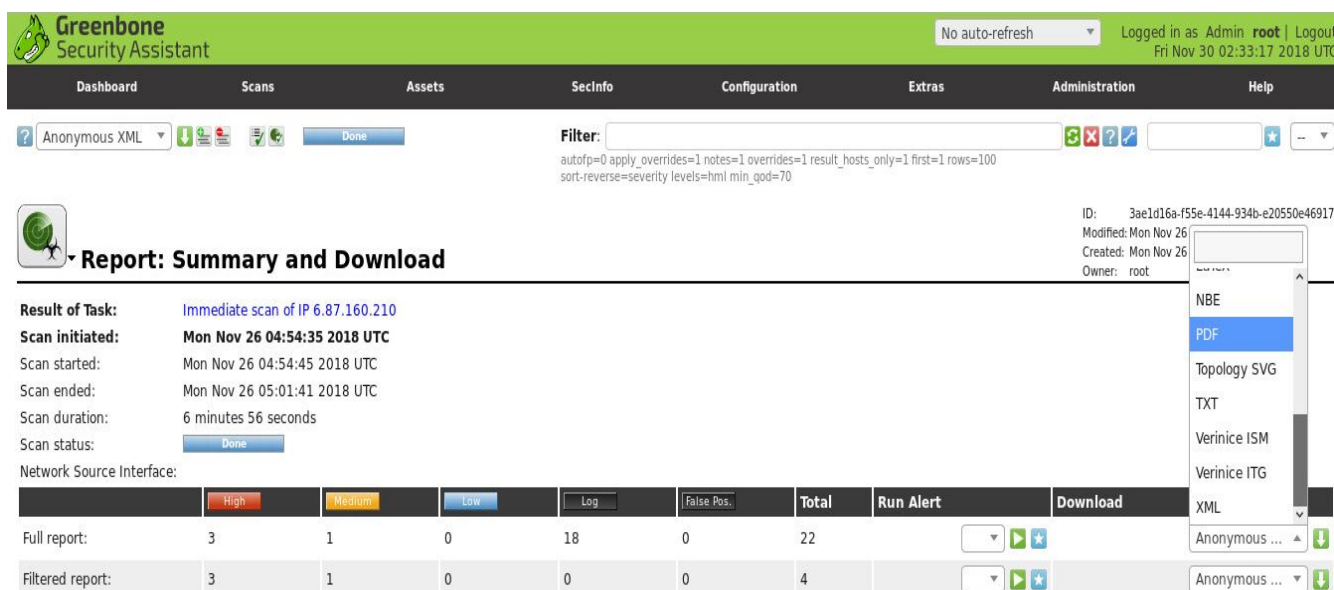


Report: Results (4 of 22)

Vulnerability	Severity
OS End Of Life Detection	10.0 (High)
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	9.3 (High)
Generic HTTP Directory Traversal	7.8 (High)
Cogent DataHub Multiple Vulnerabilities	5.0 (Medium)

(Applied filter:autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70)

You can see there are two reports that you can download. One is a “Full Report” and the other is a “Filtered Report”.



The screenshot shows the Greenbone Security Assistant interface. The top navigation bar includes Dashboard, Scans, Assets, SecInfo, Configuration, Extras, Administration, and Help. Below the navigation bar, there is a search bar with 'Anonymous XML' and a 'Done' button. To the right of the 'Done' button, there is a 'Filter:' section with a text input field and a list of filter parameters: autofp=0, apply_overrides=1, notes=1, overrides=1, result_hosts_only=1, first=1, rows=100, sort-reverse=severity, levels=hml, min_qod=70.

The main content area is titled 'Report: Summary and Download'. It displays the following information:

- Result of Task:** Immediate scan of IP 6.87.160.210
- Scan initiated:** Mon Nov 26 04:54:35 2018 UTC
- Scan started:** Mon Nov 26 04:54:45 2018 UTC
- Scan ended:** Mon Nov 26 05:01:41 2018 UTC
- Scan duration:** 6 minutes 56 seconds
- Scan status:** Done
- Network Source Interface:**

Below this information, there is a table with columns: High, Medium, Low, Log, False Pos., Total, Run Alert, and Download. The table shows the following data:

High	Medium	Low	Log	False Pos.	Total	Run Alert	Download
3	1	0	18	0	22		
3	1	0	0	0	4		

The 'Download' column has a dropdown menu with options: NBE, PDF, Topology SVG, TXT, Verinice ISM, Verinice ITG, XML, Anonymous ...

We want to view the full report of the scan. Select “PDF” from the dropdown list under the column “Download” and download the report by clicking on the “Down Arrow” right next to it. Open/Save the file to investigate all the results from the scan.

Step 4: Further Scanning

Once you are familiar with the procedure to scan a particular host, please try to scan other hosts that you had identified earlier in each of the corporate, control and substation networks.

Take some time to look through the various types of results from each scan to understand the type of vulnerabilities hosts have and how those could potentially affect the overall system availability/reliability.

Report:

1. Once you get familiar with the procedure to scan a particular host, please try to scan other hosts that you had identified earlier in each of the corporate, control and substation networks.
2. Take some time to look through the various types of results from each scan to understand the type of vulnerabilities hosts have and how those could potentially affect the overall system availability/reliability.
3. With the scan results obtained from the first two labs and any other information, you might have collected from the SCADA system, try to come up with one or two possible attacks as a penetration tester (Do not need to implement it).