Analyzing the Results of a Credentialed Vulnerability Scan
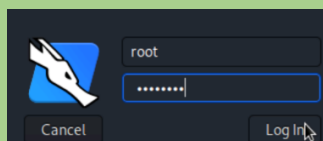
(CompTIA Security + SY – 601)

Objectives:

1. To perform vulnerability scanning
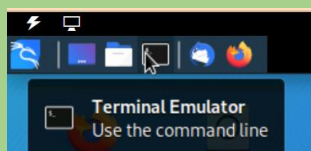2. To analyze scan reports

Resources:

1. PT1 – Kali VM
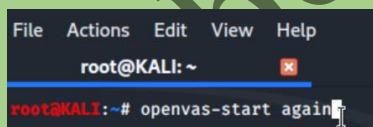2. OpenVAS Scanner

Instructions:
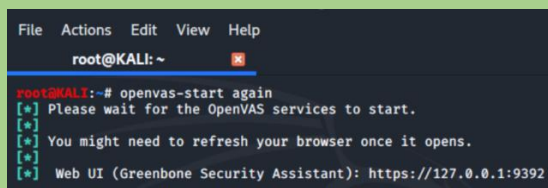
1. Connect to the **PT1-Kali VM**

2. In the menu at the top of the desktop, select the **terminal**
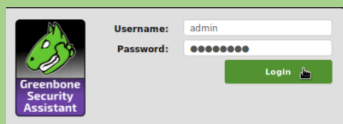

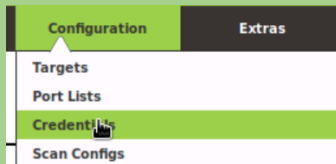**3.** In the terminal window, type openvas-start and press **ENTER**

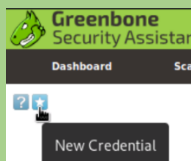4. The firefox browser automatically launches when the **openvas-service** starts. It connects to https://127.0.0.1:9392

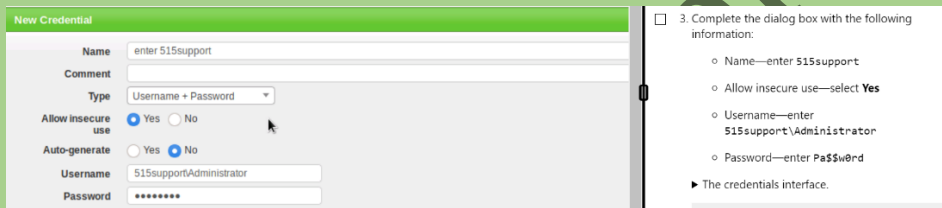**5.** Log on with **username** admin and **password**

6. From the configuration menu select **credentials**

7. Select the **blue star icon** on the left to open the **new credential** web dialog box
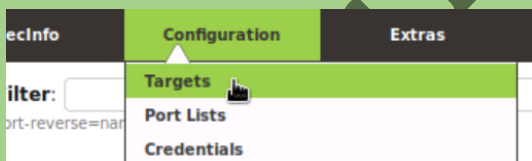

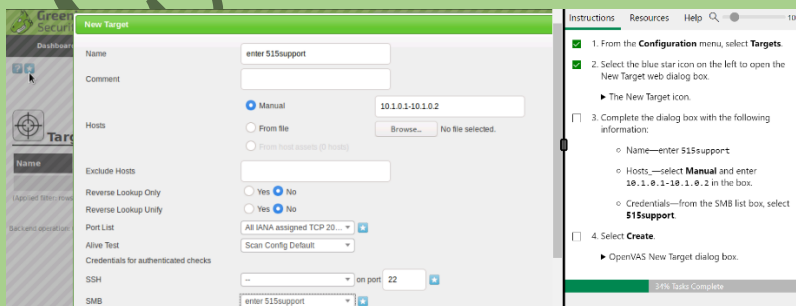8. Complete the **dialog box** with the given information:

9. Select **create**
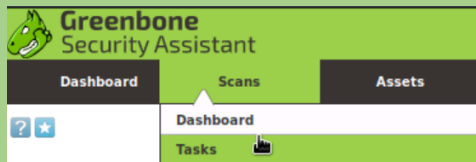10. From the configuration menu select **Targets**

11. Select the **blue star icon** on the left to open the **New Target** web dialog
12. Complete the **dialog box** with the following information

13. Select **create**
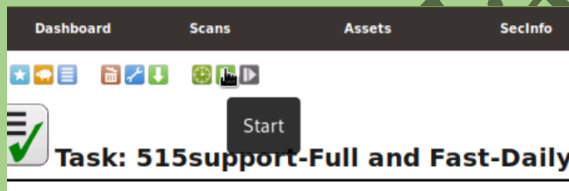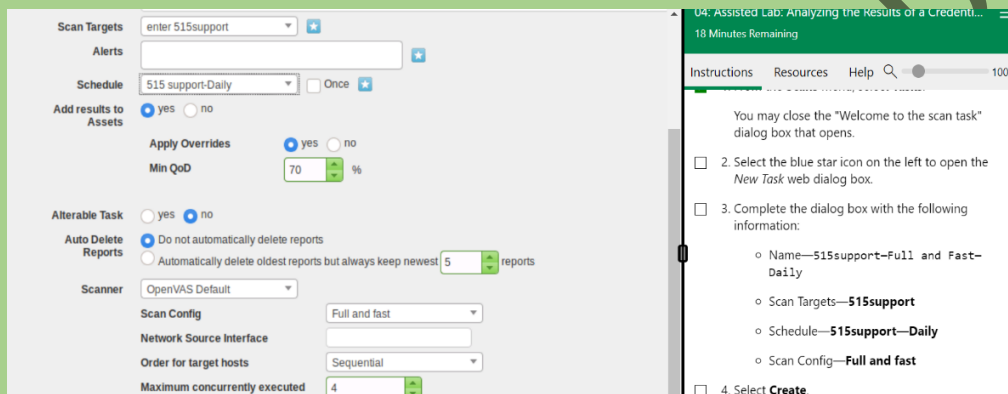14. From the **Scans** menu, select **Tasks**

15. Select the **blue star icon** on the left to open the **New Task** web dialog box
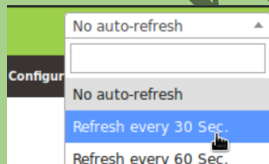16. Complete the **dialog box** with the following information:
17. Select **create**
18. Under name at the bottom of the screen, select the **'515support-Full and Fast-Daily'** task
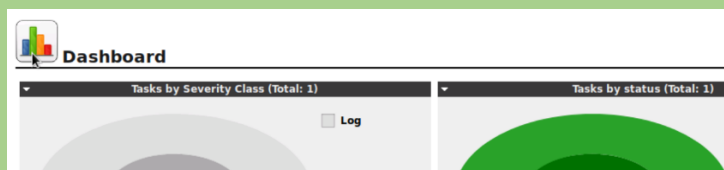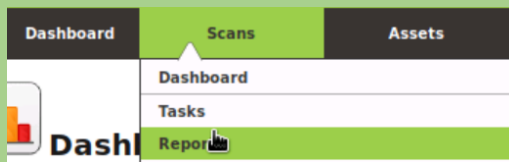19. Select the **start green arrow button** to run the scan manually

20. In the **No auto-refresh box** in the green header bar, select **Refresh every 30 seconds**

21. In the **Greenbone web app**. Select the Dashboard link to display the current information

22. Select **Scans** > **Reports**

23. In the **Date column** at the bottom of the **Reports page**, select the task with **today's date** to view the results

24. Browse the **report** and specifically observe the **CVE entries**

25. From the **small triangle**, pull down menu by the **'ReportResults'** title, choose **Report: Hosts** to display the discovered hosts and their related vulnerabilities

Observations:

1. The OpenVAS scanner was initiated on the PT1-Kali VM.
2. Credentials and targets were configured in OpenVAS.
3. A vulnerability scan was performed using the "Full and Fast" option.

4. The scan results were viewed in the Greenbone web app, displaying current vulnerabilities.
5. CVE entries and discovered hosts with related vulnerabilities were specifically observed in the report.

Results:

1. The scan identified multiple vulnerabilities across different hosts.
2. CVE entries provided detailed information about the nature and severity of the vulnerabilities.
3. The report categorized vulnerabilities by host, enabling targeted analysis and remediation.

Conclusion:

The lab successfully demonstrated how to perform and analyze a credentialed vulnerability scan using OpenVAS. The process included configuring credentials and targets, running the scan, and interpreting the results, focusing on CVE entries and host vulnerabilities.

Future Work:

Future work should include deeper analysis of specific vulnerabilities, remediation steps for identified issues, and exploring more advanced scanning options within OpenVAS to cover a broader range of security checks.