Analyzing the Results of a Credentialed Vulnerability Scan

(CompTIA Security + SY – 601)

Objectives:

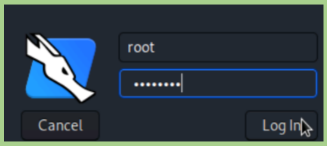
- To perform vulnerability scanning
- To analyze scan reports

Resources:

- PT1 – Kali VM
- OpenVAS Scanner

Instructions:

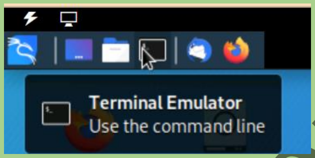
1. Connect to the **PT1-Kali VM**



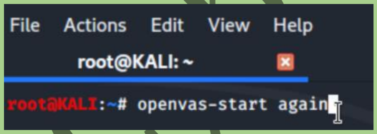
root

••••••••

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

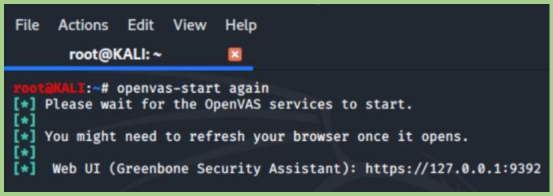


3. In the terminal window, type openvas-start and press **ENTER**



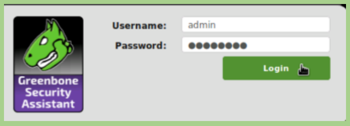
```
root@KALI:~# openvas-start again
```

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



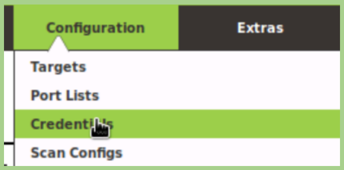
```
root@KALI:~# openvas-start again
[*] Please wait for the OpenVAS services to start.
[*]
[*] You might need to refresh your browser once it opens.
[*]
[*]  Web UI (Greenbone Security Assistant): https://127.0.0.1:9392
```

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

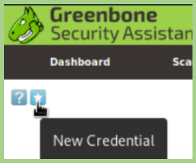


Username: admin
Password: ●●●●●●●●

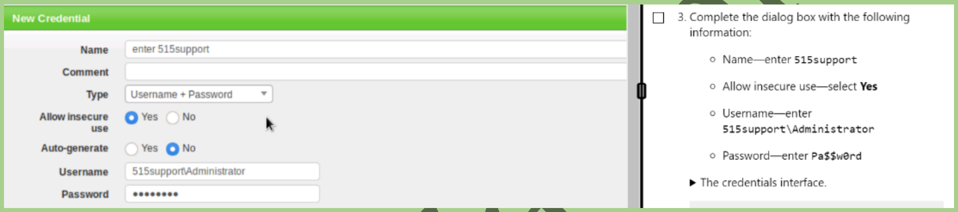
6. From the configuration menu select **credentials**



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:



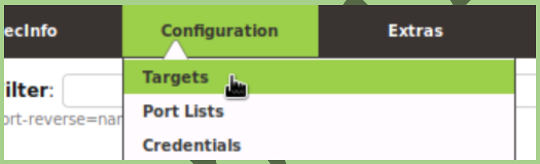
Name	enter 515support
Comment	
Type	Username + Password
Allow insecure use	● Yes ○ No
Auto-generate	○ Yes ● No
Username	515support\Administrator
Password	●●●●●●●●

□ 3. Complete the dialog box with the following information:

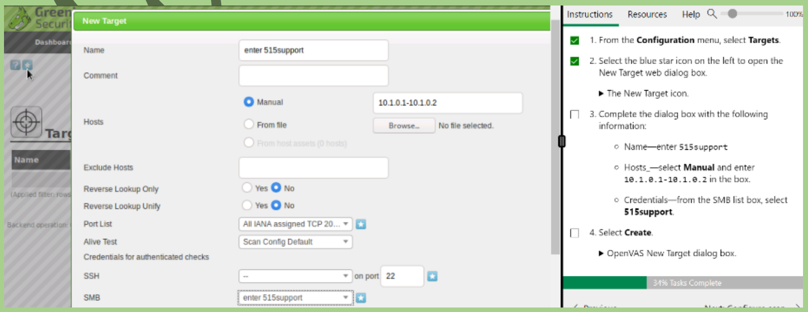
- Name—enter `515support`
- Allow insecure use—select **Yes**
- Username—enter `515support\Administrator`
- Password—enter `Pa$$w0rd`

▸ The credentials interface.

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



Name	enter 515support	
Comment		
Hosts	● Manual	10.1.0.1-10.1.0.2
	○ From file	Browse... No file selected.
	○ From host assets (0 hosts)	
Exclude Hosts		
Reverse Lookup Only	○ Yes ● No	
Reverse Lookup Unify	○ Yes ● No	
Port List	All IANA assigned TCP 20...	
Alive Test	Scan Config Default	
Credentials for authenticated checks		
SSH	--	on port 22
SMB	enter 515support	

☑ 1. From the **Configuration** menu, select **Targets**.

☑ 2. Select the blue star icon on the left to open the New Target web dialog box.

▸ The New Target icon.

□ 3. Complete the dialog box with the following information:

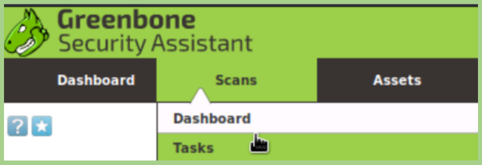
- Name—enter `515support`
- Hosts_—select **Manual** and enter `10.1.0.1-10.1.0.2` in the box.
- Credentials—from the SMB list box, select **515support**.

□ 4. Select **Create**.

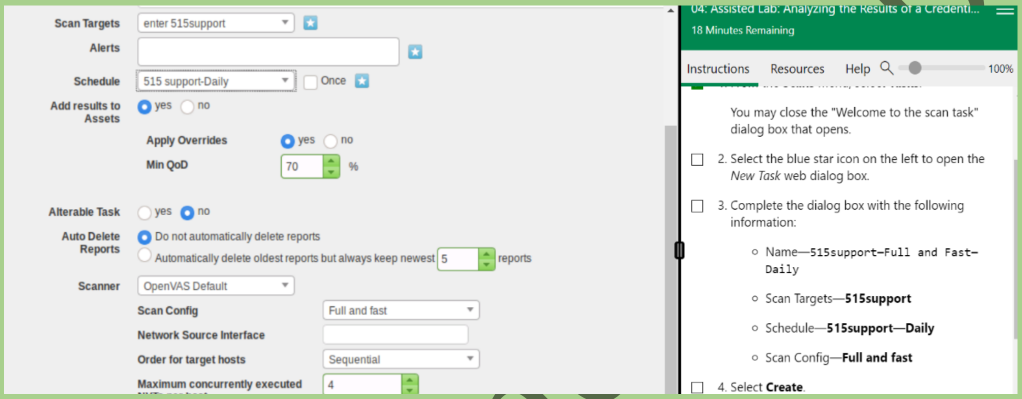
▸ OpenVAS New Target dialog box.

34% Tasks Complete

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



Scan Targets: enter 515support
Alerts:
Schedule: 515 support-Daily □ Once
Add results to Assets: ● yes ○ no
Apply Overrides: ● yes ○ no
Min QoD: 70 %
Alterable Task: ○ yes ● no
Auto Delete Reports: ● Do not automatically delete reports
○ Automatically delete oldest reports but always keep newest 5 reports
Scanner: OpenVAS Default
Scan Config: Full and fast
Network Source Interface:
Order for target hosts: Sequential
Maximum concurrently executed: 4

04: Assisted Lab: Analyzing the Results of a Credenti...
18 Minutes Remaining
Instructions Resources Help 100%

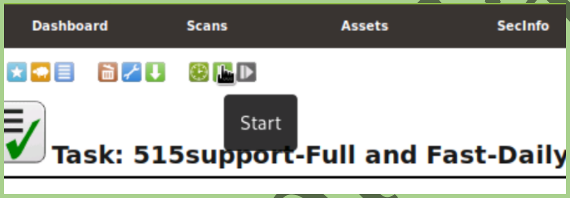
You may close the "Welcome to the scan task" dialog box that opens.

□ 2. Select the blue star icon on the left to open the *New Task* web dialog box.

□ 3. Complete the dialog box with the following information:

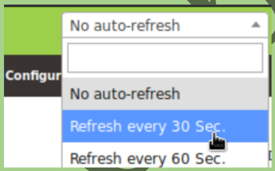
- Name—`515support-Full and Fast-Daily`
- Scan Targets—**515support**
- Schedule—**515support—Daily**
- Scan Config—**Full and fast**

□ 4. Select **Create**.

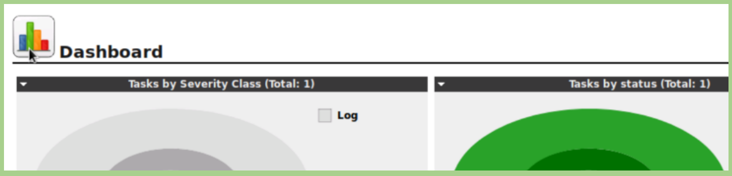


Task: 515support-Full and Fast-Daily

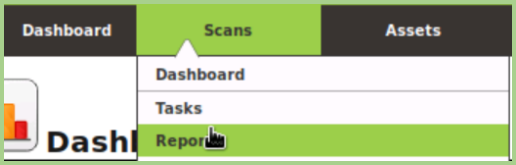
20. In the **No auto-refresh box** in the green header bar, select **Refresh every 30 seconds**



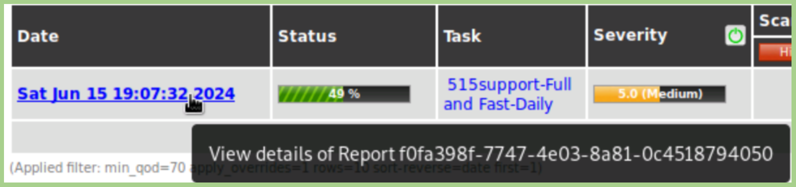
21. In the **Greenbone web app**. Select the Dashboard link to display the current information


Dashboard
Tasks by Severity Class (Total: 1)
Log
Tasks by status (Total: 1)

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

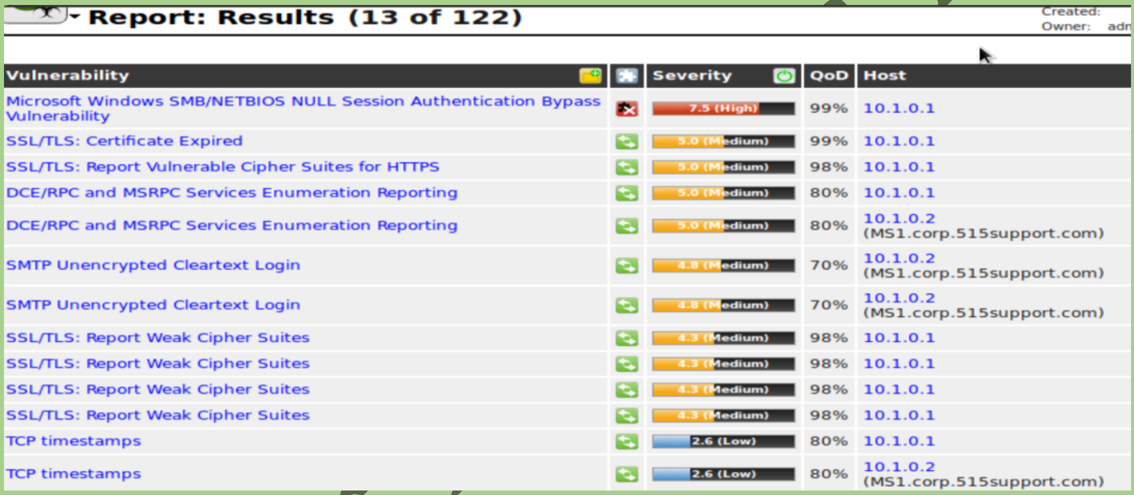


Date	Status	Task	Severity	Sca
Sat Jun 15 19:07:32 2024	49 %	515support-Full and Fast-Daily	5.0 (Medium)	H

View details of Report f0fa398f-7747-4e03-8a81-0c4518794050

(Applied filter: min_qod=70 apply_overrides=1 rows=10 sort-reverse=date first=1)

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

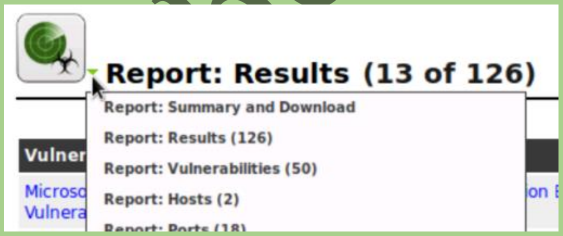


Report: Results (13 of 122)

Created:
Owner: adm

Vulnerability		Severity	QoD	Host
Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability	☒	7.5 (High)	99%	10.1.0.1
SSL/TLS: Certificate Expired		5.0 (Medium)	99%	10.1.0.1
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS		5.0 (Medium)	98%	10.1.0.1
DCE/RPC and MSRPC Services Enumeration Reporting		5.0 (Medium)	80%	10.1.0.1
DCE/RPC and MSRPC Services Enumeration Reporting		5.0 (Medium)	80%	10.1.0.2 (MS1.corp.515support.com)
SMTP Unencrypted Cleartext Login		4.8 (Medium)	70%	10.1.0.2 (MS1.corp.515support.com)
SMTP Unencrypted Cleartext Login		4.8 (Medium)	70%	10.1.0.2 (MS1.corp.515support.com)
SSL/TLS: Report Weak Cipher Suites		4.3 (Medium)	98%	10.1.0.1
SSL/TLS: Report Weak Cipher Suites		4.3 (Medium)	98%	10.1.0.1
SSL/TLS: Report Weak Cipher Suites		4.3 (Medium)	98%	10.1.0.1
SSL/TLS: Report Weak Cipher Suites		4.3 (Medium)	98%	10.1.0.1
TCP timestamps		2.6 (Low)	80%	10.1.0.1
TCP timestamps		2.6 (Low)	80%	10.1.0.2 (MS1.corp.515support.com)

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


Report: Results (13 of 126)
Report: Summary and Download
Report: Results (126)
Report: Vulnerabilities (50)
Report: Hosts (2)
Report: Ports (18)
Vulner
Microso
Vulnera
on E

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:

- The scan identified multiple vulnerabilities across different hosts.
- CVE entries provided detailed information about the nature and severity of the vulnerabilities.
- 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.