

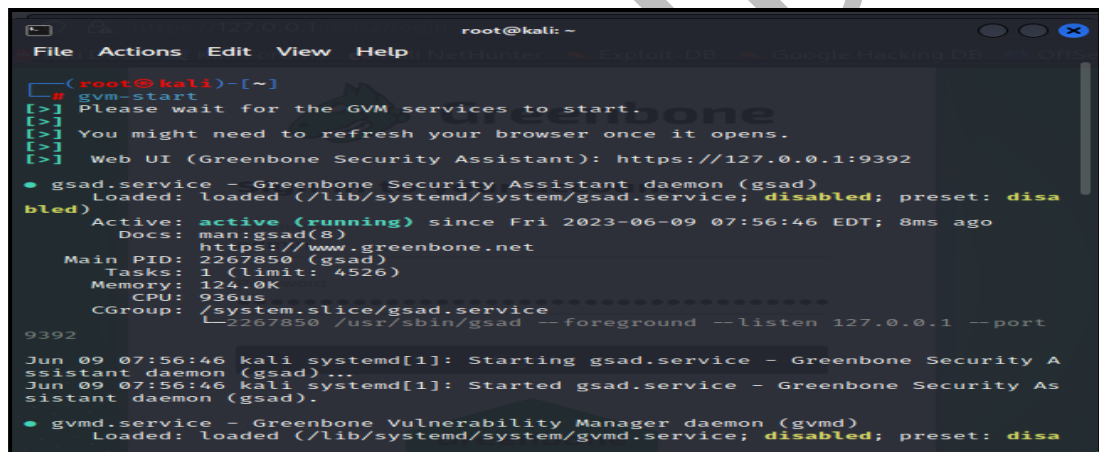
Lab Manual-Using OpenVAS/GVM tool for Vulnerability Assessment

GVM(earlier known as OpenVAS) is a full-featured vulnerability scanner. It is capable of performing unauthenticated /authenticated vulnerability testing. The scanner 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).

OpenVAS/GVM is a Linux-based scanner and can be installed on almost any Linux distribution. Kali Linux comes equipped with almost all the dependencies required by the tool.

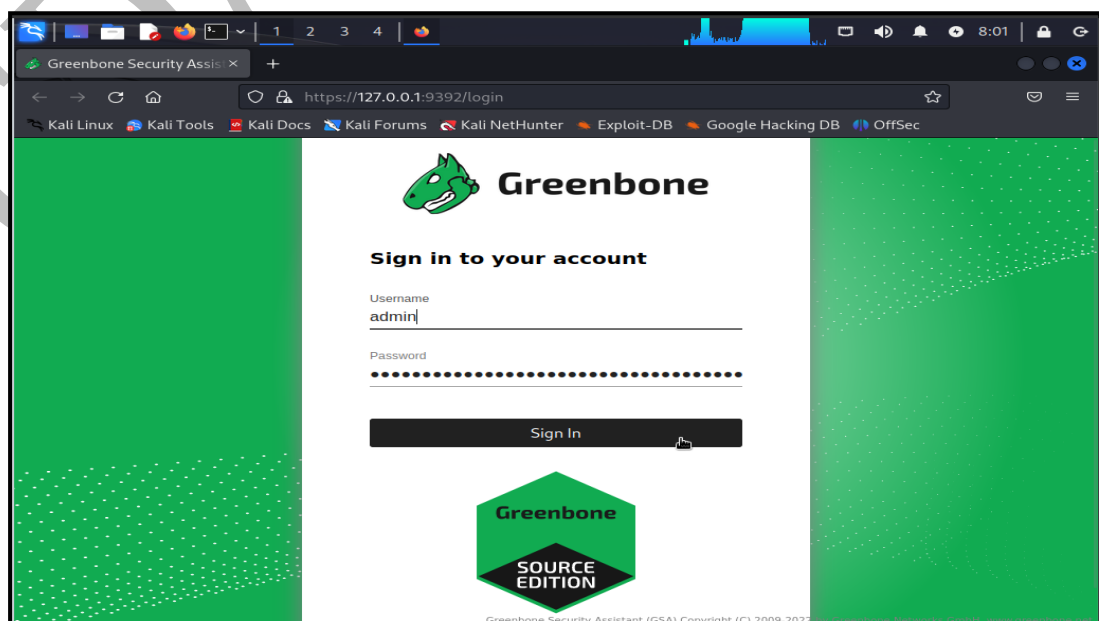
Vulnerability Scanning using OpenVAS/GVM:

1. Start OpenVAS/GVM
 - a. Open a terminal in Kali Linux and type gvm-start

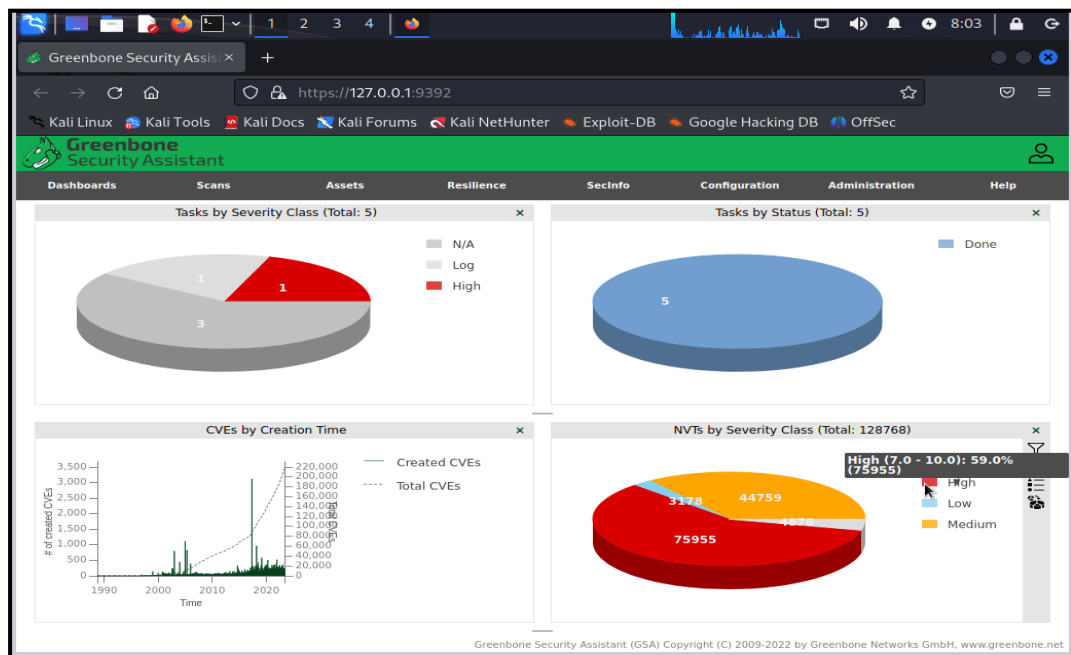


```
root@kali: ~  
File Actions Edit View Help  
[root@kali]~  
# gvm-start  
[>] Please wait for the GVM services to start.  
[>] You might need to refresh your browser once it opens.  
[>] Web UI (Greenbone Security Assistant): https://127.0.0.1:9392  
• gsad.service - Greenbone Security Assistant daemon (gsad)  
  Loaded: loaded (/lib/systemd/system/gsad.service; disabled; preset: disabled)  
  Active: active (running) since Fri 2023-06-09 07:56:46 EDT; 8ms ago  
    Docs: man:gsad(8)  
           https://www.greenbone.net  
  Main PID: 2267850 (gsad)  
    Tasks: 1 (limit: 4526)  
  Memory: 124.0K  
    CPU: 936us  
  CGroup: /system.slice/gsad.service  
          └─2267850 /usr/sbin/gsad - foreground --listen 127.0.0.1 --port 9392  
Jun 09 07:56:46 kali systemd[1]: Starting gsad.service - Greenbone Security Assistant daemon (gsad) ...  
Jun 09 07:56:46 kali systemd[1]: Started gsad.service - Greenbone Security Assistant daemon (gsad).  
• gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)  
  Loaded: loaded (/lib/systemd/system/gvmd.service; disabled; preset: disabled)
```

- b. Click on Login (The user Id and password have already been stored in the browser).



c. You should then see the dashboard of OpenVAS/GVM as shown here:

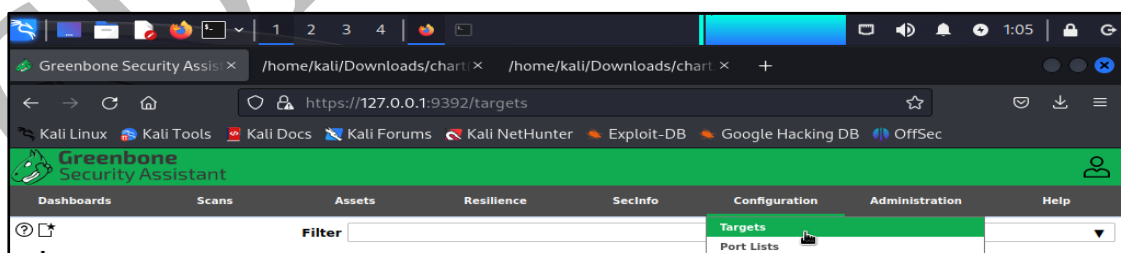


2. Creating a target in OpenVAS

The first step is to create and configure a target (the machine/computer to scan) using the OpenVAS/Green bone Security Assistant web interface. This newly created target is selected in the following step while configuring a scanning task.

To create a target, follow 2 steps:

1. Go to 'Configuration' in the top menu and select 'Targets'.
2. Click the Star icon in the top left corner to create a new target.

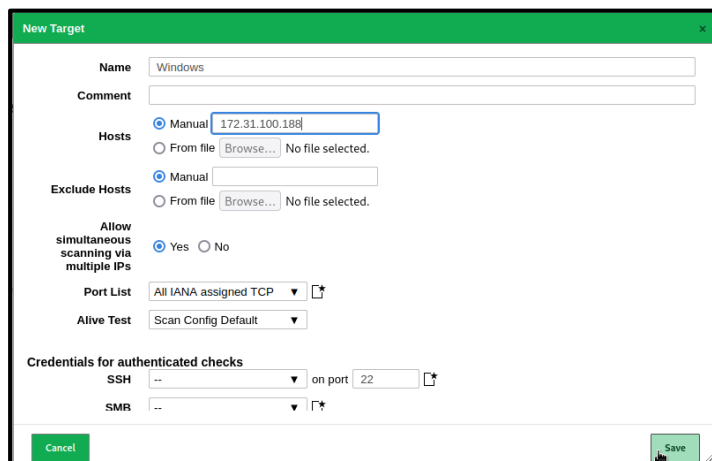


Click configuration and then new target. (The blue star can also be clicked).

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 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 'Save' button.



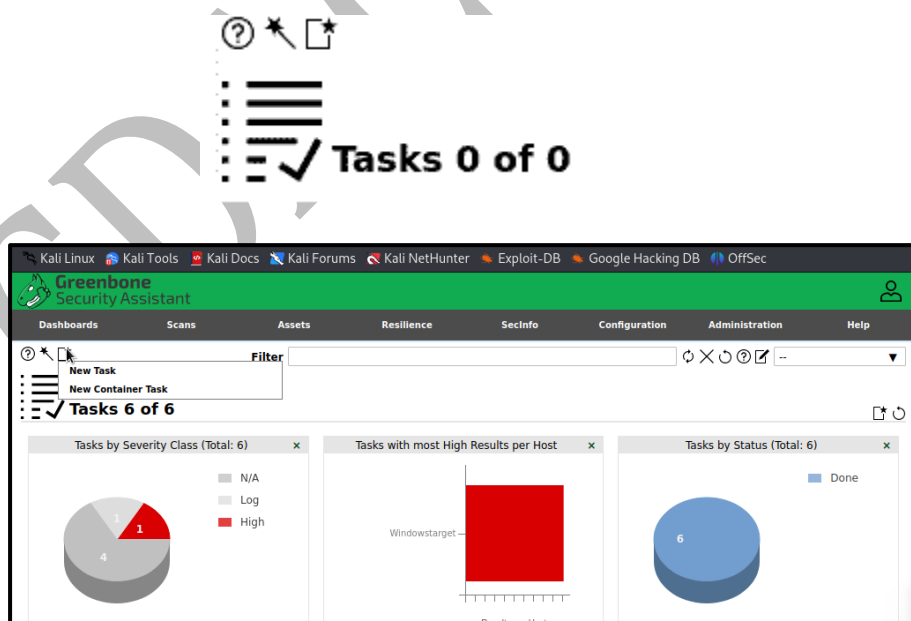
3. Enter the target name, IP and click save.
4. The newly created target will now appear in the list of available targets:

3. Configuring a scanning task in OpenVAS/GVM:

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, we have to perform the following steps:

To conduct a new scan, we follow the path of Scans > Tasks

Once the page loads, there is an option to create a new task on the top left of the screen:

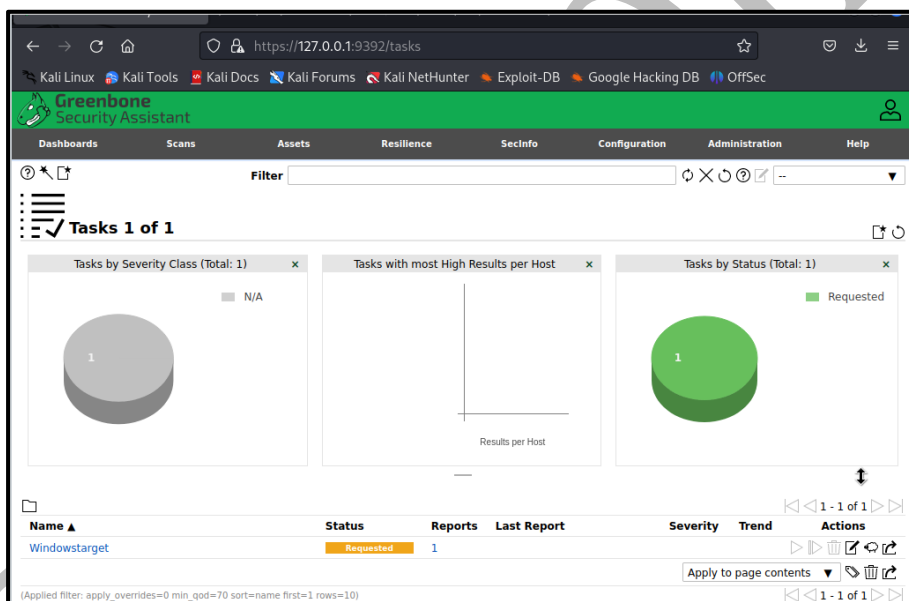


Click scans -> Tasks and then new task.

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 'Windowstarget'.
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 'save' button to create the new task.

The newly created task will now appear in the task list as follows:



There are also a few other options to create scan tasks. The scan task wizard can be used to instantly scan a target and also the advanced scan task wizard which gives a few more options to configure.

1. Running the OpenVAS/GVM vulnerability scan

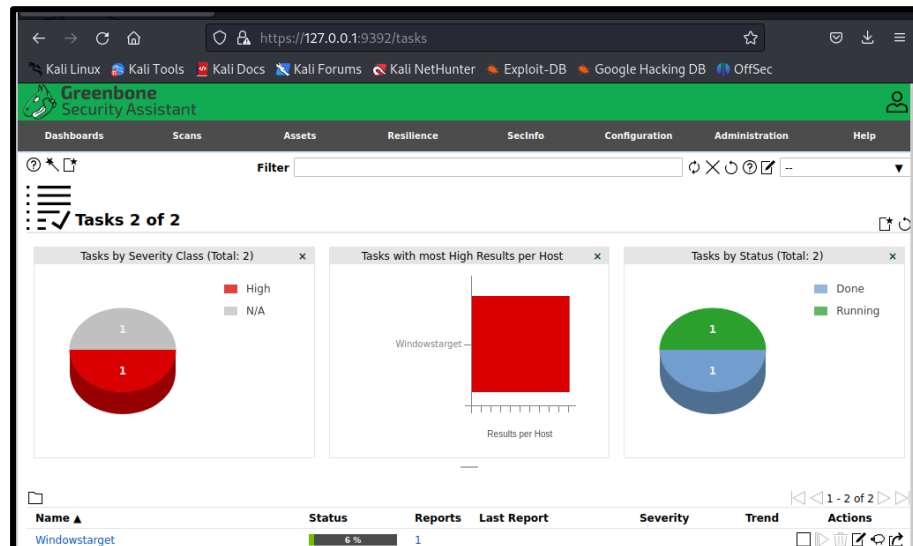
To run the newly created task we just have to click the start button as follows:



Run the scan task.

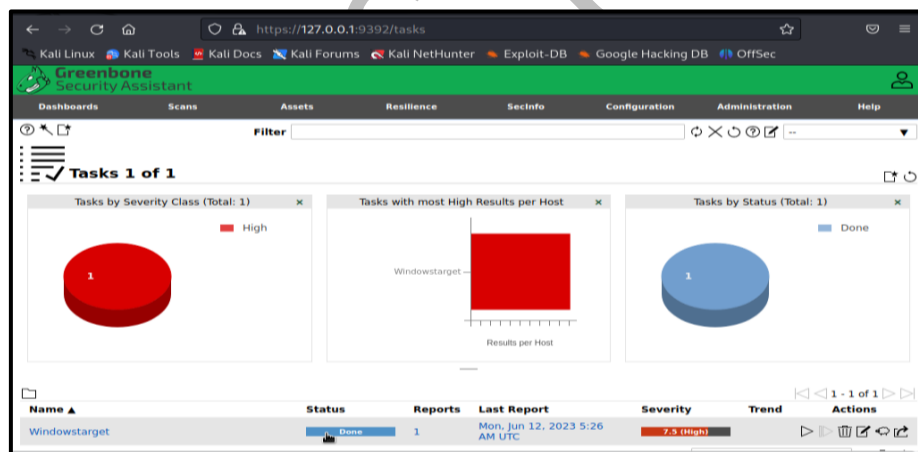
The scan task will now execute against the selected target. Please note that full scan may take a while to complete. The progress for the executed task can be checked by refreshing the tasks page.

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



Vulnerability scan in progress...

After waiting a while the scan task is finished and the status changes to 'Done':



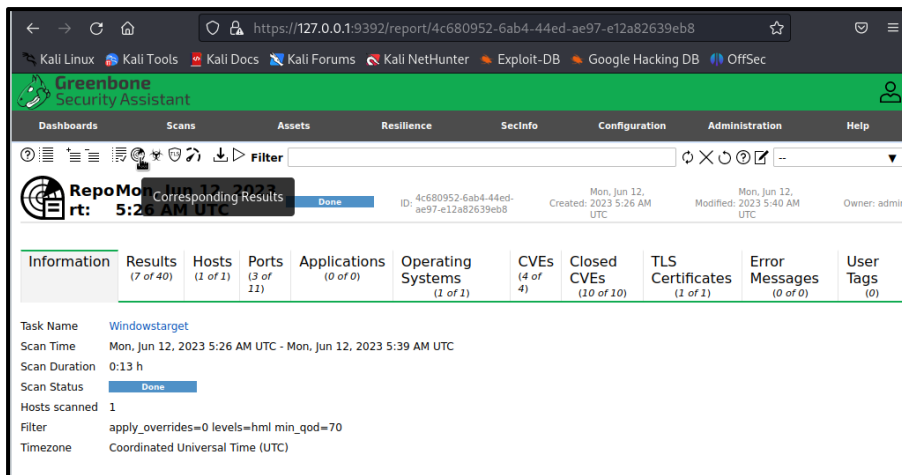
Vulnerability scan finished

4. Interpreting the scan results

Now that the vulnerability scan is finished report can be browsed by clicking to 'Scans -> Reports' in the top menu. On the reports page, report for the completed scanning tasks can be found.



Once the scan is complete, we can look at the results under: Scans > Reports.



Analyzing the results

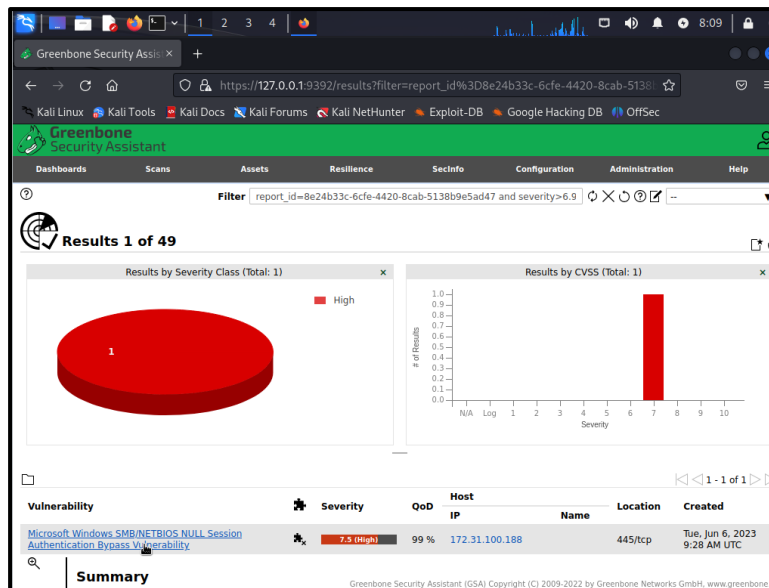
Ignore all results with "of 0" present for now.

The Results tab provides us with a broad outlook of what occurred.

By clicking the report name, an overview of all discovered vulnerabilities on the target machine can be displayed, which is a lot as already expected. The results are ordered on severity rate by default:

Name	Oldest Result	Newest Result	Severity	QoD	Results	Hosts
Check for Accessible Registry (Windows SMB Login)	Tue, Jun 6, 2023 9:23 AM UTC	Tue, Jun 6, 2023 9:23 AM UTC	0.0 (Log)	97 %	1	1
CPE Inventory	Tue, Jun 6, 2023 9:33 AM UTC	Tue, Jun 6, 2023 9:33 AM UTC	0.0 (Log)	80 %	1	1
DCE/RPC and MSRPC Services Enumeration	Tue, Jun 6, 2023 9:22 AM UTC	Tue, Jun 6, 2023 9:22 AM UTC	0.0 (Log)	80 %	1	1
DCE/RPC and MSRPC Services Enumeration Reporting	Tue, Jun 6, 2023 9:27 AM UTC	Tue, Jun 6, 2023 9:27 AM UTC	5.0 (Medium)	80 %	8	1
Hostname Determination Reporting	Tue, Jun 6, 2023 9:33 AM UTC	Tue, Jun 6, 2023 9:33 AM UTC	0.0 (Log)	80 %	1	1
ICMP Timestamp Reply Information Disclosure	Tue, Jun 6, 2023 9:26 AM UTC	Tue, Jun 6, 2023 9:26 AM UTC	2.1 (Low)	80 %	1	1
Microsoft Remote Desktop Protocol (RDP) Detection	Tue, Jun 6, 2023 9:23 AM UTC	Tue, Jun 6, 2023 9:23 AM UTC	0.0 (Log)	80 %	1	1
Microsoft Windows SMB Accessible Shares	Tue, Jun 6, 2023 9:27 AM UTC	Tue, Jun 6, 2023 9:27 AM UTC	0.0 (Log)	80 %	1	1
Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability	Tue, Jun 6, 2023 9:28 AM UTC	Tue, Jun 6, 2023 9:28 AM UTC	7.5 (High)	99 %	1	1
OS Detection Consolidation and Reporting	Tue, Jun 6, 2023 9:25 AM UTC	Tue, Jun 6, 2023 9:25 AM UTC	0.0 (Log)	80 %	1	1

By clicking on the vulnerability name, an overview of the details regarding the vulnerability can be found.



Greenbone Security Assistant

Summary

Microsoft Windows is prone to an authentication bypass vulnerability via SMB/NETBIOS.

Detection Result

It was possible to login at the share 'IPC\$' with an empty login and password.

Insight

The flaw is due to an SMB share, allows full access to Guest users. If the Guest account is enabled, anyone can access the computer without a valid user account or password.

Detection Method

Details: [Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulne...OID: 1.3.6.1.4.1.25623.1.0.801991](#)

Version used: 2022-03-03T10:23:45Z

<https://127.0.0.1:9392/mv/1.3.6.1.4.1.25623.1.0.801991>

Greenbone Security Assistant (GSA) Copyright (C) 2009-2022 by Greenbone Networks GmbH, www.greenbone.net

Greenbone Security Assistant

Detection Method

Details: [Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulne...OID: 1.3.6.1.4.1.25623.1.0.801991](#)

Version used: 2022-03-03T10:23:45Z

Affected Software/OS

- Microsoft Windows 95
- Microsoft Windows 98
- Microsoft Windows NT
- Microsoft Windows 2000
- Microsoft Windows in other implementations / versions might be affected as well

Impact

Successful exploitation could allow attackers to use shares to cause the system to crash.

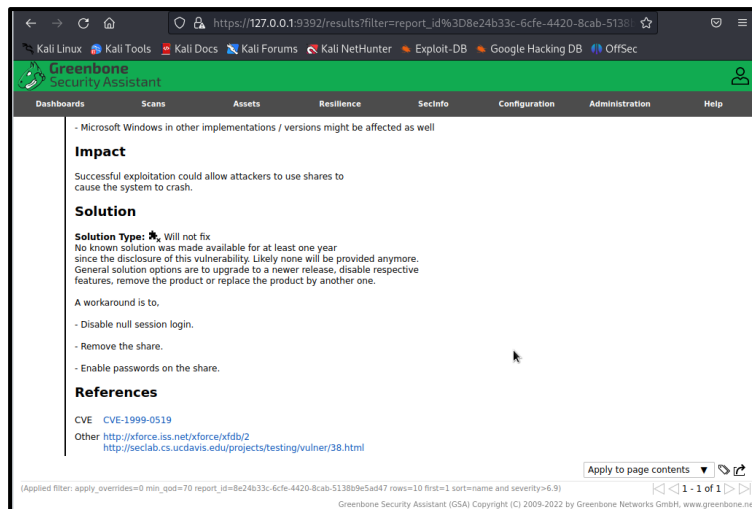
Solution

Solution Type: ✖ Will not fix

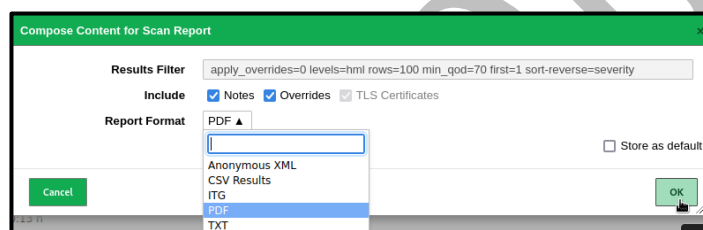
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

A workaround is to

Greenbone Security Assistant (GSA) Copyright (C) 2009-2022 by Greenbone Networks GmbH, www.greenbone.net



Finally, the report can also be exported in a variety of formats, such as XML, TXT, and PDF. It can be done by selecting the desired format from the drop-down menu and clicking the Ok button to download the report.



Scan result save in PDF format



Other notable features

The Resilience tab contains some interesting features. Here you can view existing Remediation tickets, and create and view both Compliance Policies and Compliance Audits.

Greenbone Security Assistant

Dashboards Scans Assets Resilience SecInfo Configuration Administration Help

Filter Remediation Tickets Compliance Policies Compliance Audits

Policies 6 of 6

Name Actions

EulerOS Linux Security Configuration (Check compliance status of EulerOS 2.0 SP3/SP5/SP8 installation against above named Policy as distributed by Huawei. Version 20201215.)

GaussDB 100 V300R001C00 Security Hardening Guide (Standalone) (Check compliance status of GaussDB installation against above named Policy as distributed by Huawei (based on Issue 5). Version 20201215.)

GaussDB Kernel V500R001C00 Security Hardening Guide (Check compliance status against mentioned policy (based on Issue 01 from 2020-07-21). Version 20201222.)

Huawei Datacom Product Security Configuration Audit Guide (Check compliance status of Huawei Datacom Device against above named Policy as distributed by Huawei. Version 20211209.)

IT-Grundschrift Kompendium (Policy für Bausteine: SYS 1.2.2, SYS 2.2.2, SYS 2.2.3, SYS 1.3, SYS 2.3. Version 20210318.)

openGauss Security Hardening Guide (Check compliance status against mentioned policy (based on Issue 01 from 2020-10-14). Version 20201222.)

Apply to page contents

(Applied filter: sort=name first=1 rows=10)

https://127.0.0.1:9392/policies

Greenbone Security Assistant (GSA) Copyright (C) 2009-2022 by Greenbone Networks GmbH. www.greenbone.net

The SecInfo tab is probably one of the most exciting features including different options like NVT (Network Vulnerability Tests), CVE (Common Vulnerabilities and Exposure), CERT-Bund Advisories and more.

Greenbone Security Assistant

Dashboards Scans Assets Resilience SecInfo Configuration Administration Help

Filter NVTs CVEs CPEs CERT-Bund Advisories DFN-CERT Advisories

NVTs 128768 of 128768

NVTs by Severity Class (Total: 128768)

NVTs by Creation Time

NVTs by Family (Total: 128768)

Name Family Created Modified CVE Severity QoD

SUSE: Security Advisory (SUSE-SU-2023:2360-1) SuSE Local Security Checks Mon, Jun 5, 2023 4:22 AM UTC Mon, Jun 5, 2023 4:22 AM UTC CVE-2021-36980 CVE-2022-32166 CVE-2022-4337 CVE-2022-4338 9.8 (High) 97 %

SUSE Local Security Mon, Jun 5, 2023 4:22 AM UTC Mon, Jun 5, 2023 4:22 AM UTC CVE-2021-3929 CVE-2021-4206 CVE-2021-4206 8.2 (High) 97 %

https://127.0.0.1:9392/nvts

Greenbone Security Assistant (GSA) Copyright (C) 2009-2022 by Greenbone Networks GmbH. www.greenbone.net