🔒 Vulnerability Assessment Report — Localhost (Greenbone Security Assistant)

1. Objective

To perform a vulnerability assessment on the local host machine using Greenbone Security Assistant (OpenVAS) to identify potential security weaknesses and recommend mitigations.

2. Tools Used

Tool	Description
Greenbone Security Assistant (GSA)	Web interface for OpenVAS vulnerability scanning
Greenbone Vulnerability Manager (GVM)	Core engine managing scan configurations and reports
Operating System	Kali Linux
Scan Configuration	Full and Fast
Date of Scan	October 26, 2025

3. Target Information

Parameter	Details
Target Name	Localhost
IP Address	192.168.1.39
Host OS	Linux Kernel (detected via ICMP fingerprinting)
Scan Type	Full and Fast

Parameter	Details
Port List	All TCP and top 1000 UDP

4. Scan Summary

Metric	Result
Total Hosts Scanned	1
Total Vulnerabilities Detected	4
High Severity	0
Medium Severity	0
Low Severity	0
Log/Informational	4
Total Scan Duration	8 minutes

Observation:

The scan completed successfully, identifying 4 informational (log-level) results. No exploitable or high-severity vulnerabilities were detected on this host.

5. Detailed Findings

#	Vulnerability Name	Severity	Host	Description	Recommendation
1	**CPE Inventory**	Log	192.168.1.39	Reports detected Common Platform Enumeration (CPE)	No action required — informational only.

#	Vulnerability Name	Severity	Host	Description	Recommendation
				information for asset inventory purposes.	
2	**Hostname Determination Reporting**	Log	192.168.1.39	The scanner successfully determined the system hostname.	Ensure hostnames are properly configured and consistent across the network.
3	**OS Detection Consolidation and Reporting**	Log	192.168.1.39	Consolidates OS detection information and reports Linux Kernel as the best match.	Verify that the host is running an up-to-date Linux kernel.
4	**Traceroute**	Log	192.168.1.39	Displays the network path from the scanner to the host for topology mapping.	No action required — used for network mapping.

6. Mitigation Summary

Although no critical vulnerabilities were detected, some best practices are recommended:

Severity	Recommended Action
High	None detected
Medium	None detected

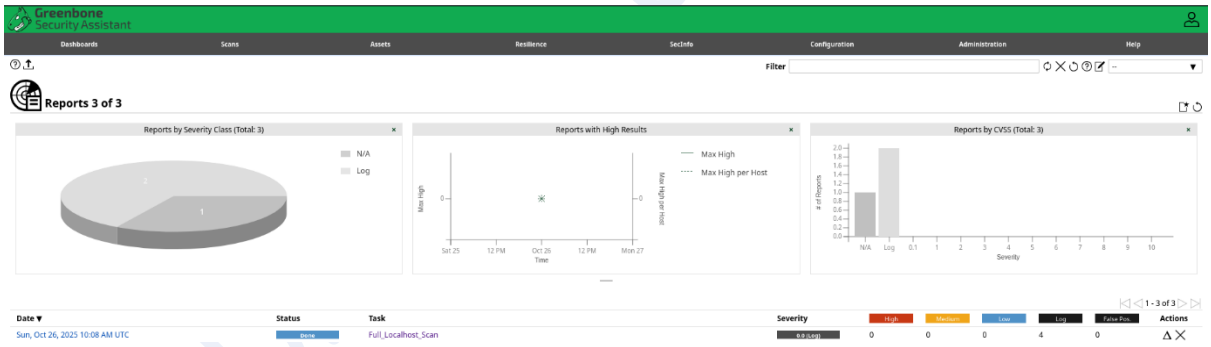
Severity	Recommended Action
Low	None detected
Informational	Verify host configuration, kernel version, and maintain regular vulnerability scans.

7. Conclusion

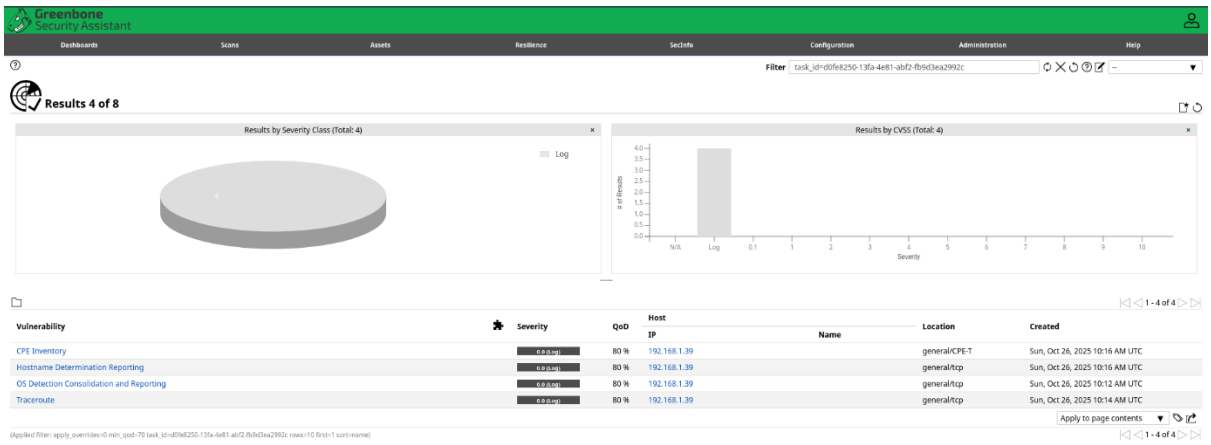
The vulnerability assessment on the localhost (192.168.1.39) completed successfully using Greenbone Security Assistant. No exploitable vulnerabilities were found — only informational findings related to host and OS identification. The system appears to be secure and up-to-date at the time of testing. Future scans should be scheduled periodically to ensure continued compliance and security posture.

Screenshots

Task dashboard



Vulnerability



CPE Inventory

Vulnerability	Severity	QoD	Host IP	Host Name	Location	Created
CPE Inventory	0.0 (Log)	80 %	192.168.1.39		general/CPE-T	Sun, Oct 26, 2025 10:16 AM UTC

Summary

This routine uses information collected by other routines about
CPE identities of operating systems, services and applications detected during the scan.

Note: Some CPEs for specific products might show up twice or more in the output. Background:

After a product got renamed or a specific vendor was acquired by another one it might happen that
a product gets a new CPE within the NVD CPE Dictionary but older entries are kept with the older
CPE.

Detection Result

```
192.168.1.39|cpe:/o:linux:kernel
```

Detection Method

Details: CPE Inventory OID: 1.3.6.1.4.1.25623.1.0.810002
Version used: 2022-07-27T10:11:28Z

References

Other https://nvd.nist.gov/products/cpe

Hostname Determination Reporting

Hostname Determination Reporting	0.0 (Log)	80 %	192.168.1.39		general/tcp	Sun, Oct 26, 2025 10:16 AM UTC

Summary

The script reports information on how the hostname of the target
was determined.

Detection Result

```
Hostname determination for IP 192.168.1.39:

Hostname|Source
192.168.1.39|IP-address
```

Detection Method

Details: Hostname Determination Reporting OID: 1.3.6.1.4.1.25623.1.0.108449
Version used: 2022-07-27T10:11:28Z

Os Detection consolidation and Reporting

OS Detection Consolidation and Reporting	0.0 (Log)	80 %	192.168.1.39		general/tcp	Sun, Oct 26, 2025 10:12 AM UTC

Summary

This script consolidates the OS information detected by several
VTs and tries to find the best matching OS.

Furthermore it reports all previously collected information leading to this best matching OS. It
also reports possible additional information which might help to improve the OS detection.

If any of this information is wrong or could be improved please consider to report these to the
referenced community forum.

Detection Result

```
Best matching OS:

OS:           Linux Kernel
CPE:          cpe:/o:linux:kernel
Found by VT:  1.3.6.1.4.1.25623.1.0.102002 (Operating System (OS) Detection (ICMP))
Concluded from ICMP based OS fingerprint
Setting key "Host/runs_unixoide" based on this information
```

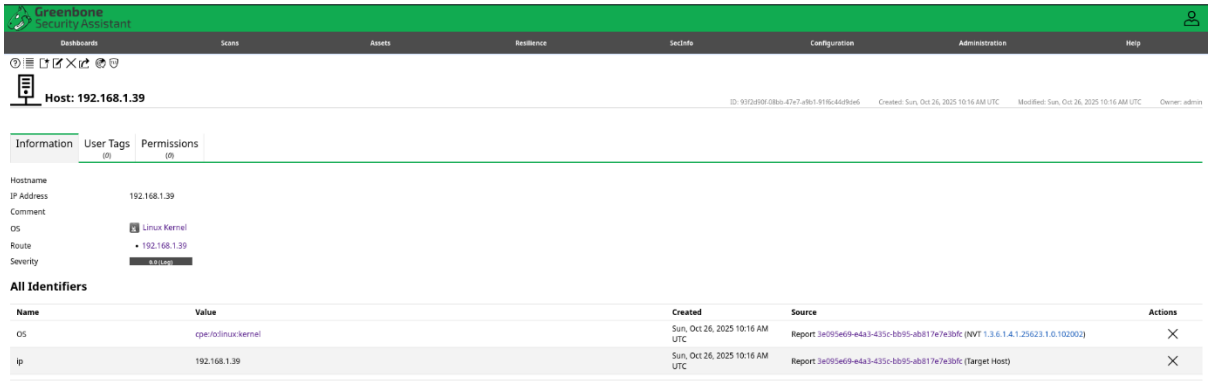
Detection Method

Details: OS Detection Consolidation and Reporting OID: 1.3.6.1.4.1.25623.1.0.105937
Version used: 2025-10-17T05:39:07Z

References

Other https://forum.greenbone.net/c/vulnerability-tests/7

Os Identifier



Traceroute