Scan Report

August 12, 2025

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone “Coordinated Universal Time”, which is abbreviated “UTC”. The task was “Full Vulnerability Scan - Localhost”. The scan started at Sat Aug 9 11:38:49 2025 UTC and ended at Sat Aug 9 11:45:28 2025 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.1.125	0	0	0	4	0
Total: 1	0	0	0	4	0

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level “Debug” are not shown.
Issues with the threat level “False Positive” are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 4 results selected by the filtering described above. Before filtering there were 4 results.

2 Results per Host

2.1 192.168.1.125

Host scan start	Sat Aug 9 11:42:48 2025 UTC
Host scan end	Sat Aug 9 11:45:20 2025 UTC

Service (Port)	Threat Level
general/CPE-T	Log
general/tcp	Log

2.1.1 Log general/CPE-T

Log (CVSS: 0.0)

NVT: CPE Inventory

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.

. . . continues on next page . . .

... continued from previous page ...

Quality of Detection (QoD): 80%

Vulnerability Detection Result

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

Solution:

Log Method

Details: `CPE Inventory`

OID:1.3.6.1.4.1.25623.1.0.810002

Version used: `2022-07-27T10:11:28Z`

References

```
url: https://nvd.nist.gov/products/cpe
```

[return to 192.168.1.125]

2.1.2 Log general/tcp

Log (CVSS: 0.0)

NVT: OS Detection Consolidation and Reporting

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.

Quality of Detection (QoD): 80%

Vulnerability 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 (ICM
↪P))
Concluded from ICMP based OS fingerprint
Setting key "Host/runs_unixoide" based on this information
```

Solution:

... continues on next page ...

. . . continued from previous page . . .

Log Method
Details: `OS Detection Consolidation and Reporting`
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: `2025-08-08T05:44:56Z`

References
`url: https://forum.greenbone.net/c/vulnerability-tests/7`

Log (CVSS: 0.0)

NVT: Traceroute

Summary
Collect information about the network route and network distance between the scanner host and the target host.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Network route from scanner (192.168.1.125) to target (192.168.1.125):
192.168.1.125
Network distance between scanner and target: 1
```

Solution:

Vulnerability Insight
For internal networks, the distances are usually small, often less than 4 hosts between scanner and target. For public targets the distance is greater and might be 10 hosts or more.

Log Method
A combination of the protocols ICMP and TCP is used to determine the route. This method is applicable for IPv4 only and it is also known as 'traceroute'.
Details: `Traceroute`
OID:1.3.6.1.4.1.25623.1.0.51662
Version used: `2022-10-17T11:13:19Z`

Log (CVSS: 0.0)

NVT: Hostname Determination Reporting

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Hostname determination for IP 192.168.1.125:
Hostname|Source
192.168.1.125|IP-address
```

Solution:

Log Method

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

[return to 192.168.1.125]

This file was automatically generated.