Scan Report

February 22, 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 "Immediate scan of IP 6.87.153.110". The scan started at Sat Feb 22 08:40:05 2025 UTC and ended at Sat Feb 22 08:50:40 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
6.87.153.110	0	0	0	3	0
Total: 1	0	0	0	3	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
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.

This report contains all 3 results selected by the filtering described above. Before filtering there were 3 results.

2 Results per Host

2.1 6.87.153.110

Host scan start	Sat Feb 22 08:40:21 2025 UTC
Host scan end	Sat Feb 22 08:50:40 2025 UTC

Service (Port)	Threat Level
general/tcp	Log
22/tcp	Log

2.1.1 Log general/tcp

Log (CVSS: 0.0)
NVT: OS Detection Consolidation and Reporting

Summary
This script consolidates the OS information detected by several NVTs 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 portal.

Vulnerability Detection Result
```
No Best matching OS identified. Please see the NVT 'Unknown OS and Service Banne
↪r Reporting' (OID: 1.3.6.1.4.1.25623.1.0.108441) for possible ways to identify
↪ this OS.
```

... 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: 2019-05-02T04:45:21+0000

References
Other:
URL:https://community.greenbone.net/c/vulnerability-tests

Log (CVSS: 0.0)
NVT: Traceroute

Summary
A traceroute from the scanning server to the target system was conducted. This traceroute is provided primarily for informational value only. In the vast majority of cases, it does not represent a vulnerability. However, if the displayed traceroute contains any private addresses that should not have been publicly visible, then you have an issue you need to correct.

Vulnerability Detection Result
Here is the route from 27.37.47.110 to 6.87.153.110:
27.37.47.110
6.87.153.110

Solution
Block unwanted packets from escaping your network.

Log Method
Details: Traceroute
OID:1.3.6.1.4.1.25623.1.0.51662
Version used: $Revision: 10411 $

[return to 6.87.153.110]

2.1.2 Log 22/tcp

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result

. . . continues on next page . . .

... continued from previous page ...

An ssh server is running on this port

Log Method
Details: Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: $Revision: 13541 $

[return to 6.87.153.110]