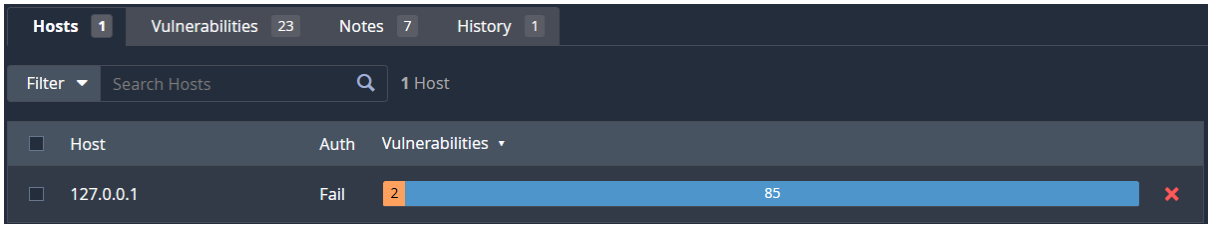
Executive Summary

This scan was done accordance with the given instructions, as of now there isn't a major vulnerability found and due to the lack of authorised certificate of the local host, the scan parameters were limited, this report consist of vulnerabilities found, remediation that should be taken and actionable prevention methods.

Scan and Analysis

Nessus was used to perform scan and analytics on Localhost. A full unauthenticated scan was initiated and completed



The most significant finding was the limitation of the scan itself. The primary "vulnerability" is the lack of insight due to the unauthenticated nature of the scan. Key findings are documented below.

Critical Findings

Risk Factor: Medium

CVSS v3.0 Base Score: 5.3

CVSS v3.0 Vector:
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

CVSS v3.0 Temporal Vector:
CVSS:3.0/E:U/RL:O/RC:C

CVSS v3.0 Temporal Score: 4.6

CVSS v2.0 Base Score: 5.0

CVSS v2.0 Temporal Score: 3.7

CVSS v2.0 Vector:
CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N

CVSS v2.0 Temporal Vector:
CVSS2#E:U/RL:OF/RC:C

Severity:	Medium
ID:	51192
Version:	1.20
Type:	remote
Family:	General
Published:	December 15, 2010
Modified:	June 16, 2025

Risk Information

Risk Factor: Medium

CVSS v3.0 Base Score: 6.5

CVSS v3.0 Vector:
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

CVSS v2.0 Base Score: 6.4

CVSS v2.0 Vector:
CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N

The scan was unable to authenticate to the Windows host via SMB or any other method. Nessus logs indicated repeated failures to access critical system components required for deep analysis, such as the Windows Registry. This prevents the scanner from accurately assessing the system's patch level, checking for insecure configurations, or identifying vulnerabilities in installed software.

Risks

Without a credentialed scan, the host is a "black box." There is no visibility into whether critical security updates from Microsoft or third-party vendors are missing. An attacker who gains access to the machine could potentially exploit unpatched software.

Other Issues Found

TCP Open Ports

Nessus Web Interface (Port 8834)

Finding: The service is running with a self-signed, untrusted SSL certificate. This is normal for a default Nessus installation but is an important configuration note.

Windows File Sharing (SMB on Port 445)

Finding: The service is active and listening. The scanner was unable to authenticate to it, preventing any deeper analysis of share permissions or system security.

Unknown Web Service (Port 50128)

Finding: An active web server (Microsoft-HTTPAPI/2.0) is running but returned "Unauthorized" errors to the scanner. The purpose of this service is unknown.

Microsoft RPC (Port 135 and others)

Finding: The standard Windows RPC endpoint mapper and several dynamic RPC ports are open and accessible on the network.

UDP Open Ports

Port 53: DNS (Domain Name System)
Port 137: NetBIOS Name Service
Port 138: NetBIOS Datagram Service
Port 547: DHCPv6 Client
Port 1900: SSDP (Simple Service Discovery Protocol)
Port 5050
Port 5353: mDNS (Multicast DNS)
Port 5355: LLMNR (Link-Local Multicast Name Resolution)
Port 27036
Port 51043
Port 59227
Port 64986

As of now there’s no known vulnerability and risk found in these ports yet or the risks are too minor for CVSS scoring to identify it as a risk

Conclusion

This vulnerability scan provided a valuable baseline assessment of the network footprint for the Windows 11 host, "GHOST". The scan successfully enumerated a number of open TCP and UDP services, including Microsoft SMB, RPC, and web services on ports 8834 and 50128.

However, the most significant finding is that the scan was performed without authentication credentials. This limited the assessment to an external "black-box" perspective.