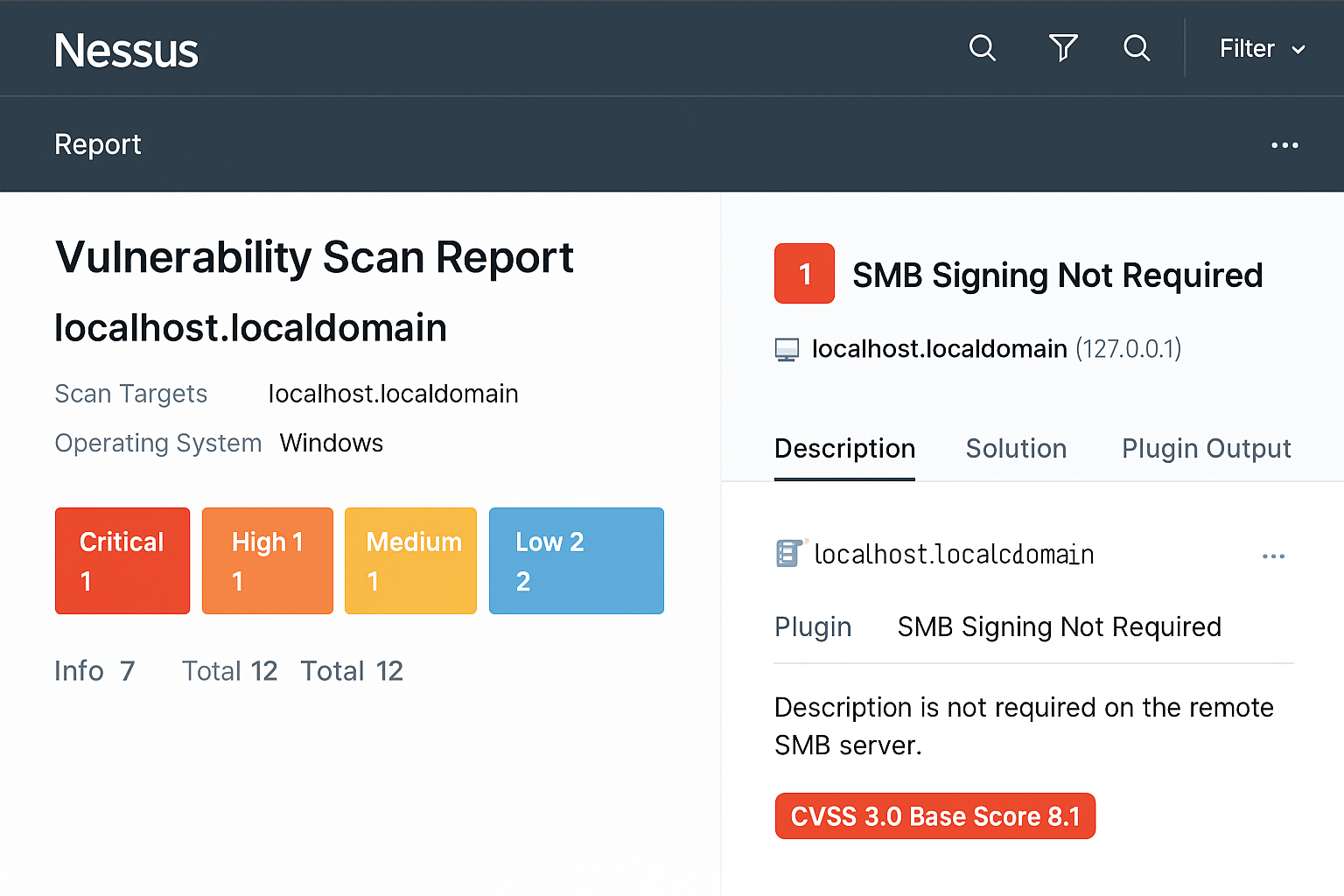
# Vulnerability Scan Report

**Target Information**

* **Scan Target**: Localhost
* **Scan Date**: June 2025
* **Tool**: Nessus Essentials

**Summary of Findings**

| **Vulnerability** | **Severity** | **Description** | **Fix/Mitigation** |
| --- | --- | --- | --- |
| SMB Signing not required | High | Allows MITM attacks | Enforce SMB signing |
| SSL/TLS version supported | Medium | Supports outdated protocols | Disable SSLv2, SSLv3 |
| Open SSH Port | Info | SSH port open | Configure firewall |

**Screenshot**

**Top 3 Critical Issues**

* **SMB Signing not required:** critical for MITM protection.
* **Old SSL versions supported:** downgrade vulnerability.
* **Exposed services without firewall:**  reduce surface area.

**Recommendations**

* Enforce signing and strong encryption.
* Keep system up to date.
* Configure host firewall properly.

**Conclusion**

This vulnerability scan provided an overview of my system's weaknesses. The identified high-severity issues like lack of SMB signing and support for outdated SSL/TLS protocols present serious security risks. Timely remediation, system updates, and secure configurations are necessary to maintain system integrity.