# **Vulnerability Assessment Report — Localhost (Greenbone Security Assistant)**

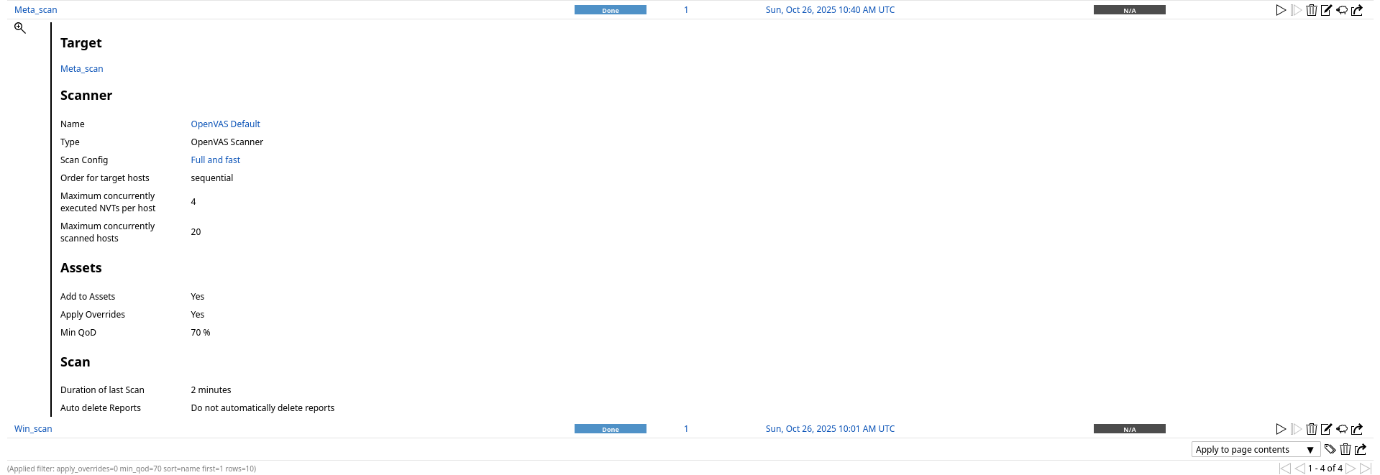
**1. Objective**

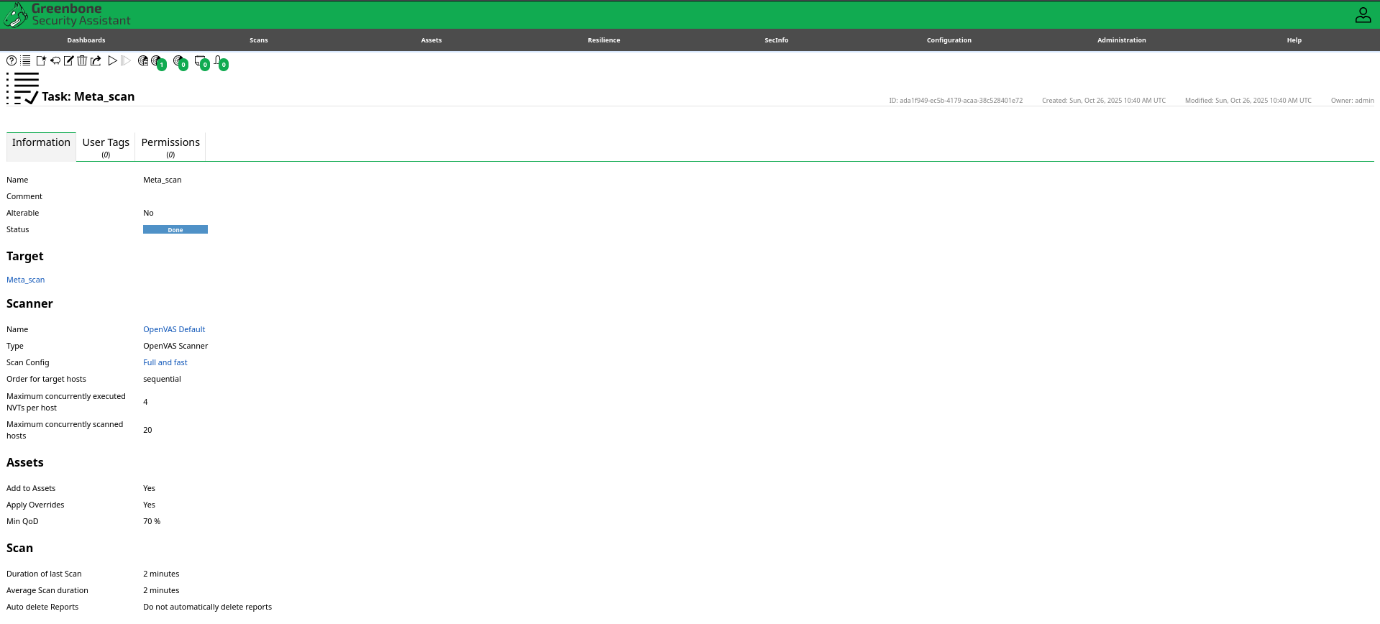
To perform a vulnerability assessment on the local host machine using Greenbone Security Assistant (OpenVAS) to identify potential security weaknesses and recommend mitigations.

**2. Tools Used**

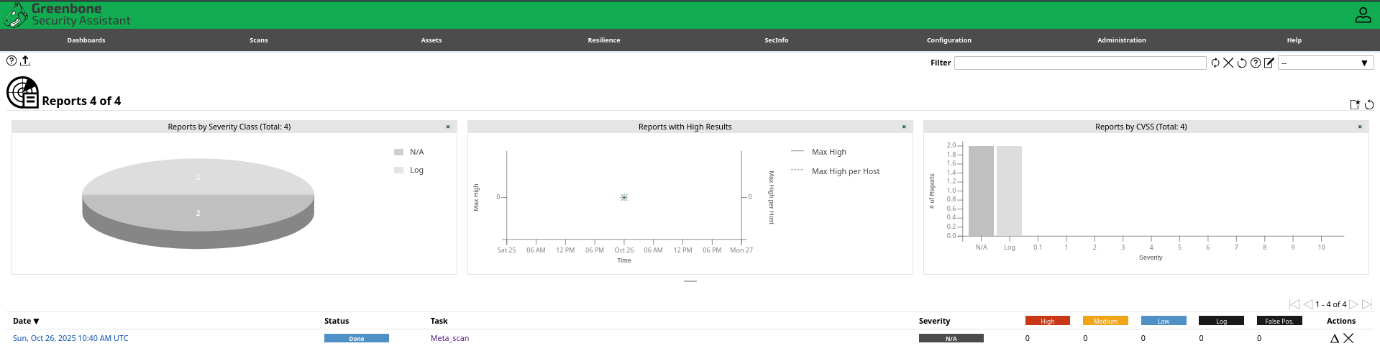
| **Tool** | **Description** |
| --- | --- |
| **Greenbone Security Assistant (GSA)** | **Web interface for OpenVAS vulnerability scanning** |
| **Greenbone Vulnerability Manager (GVM)** | **Core engine managing scan configurations and reports** |
| **Operating System** | **Kali Linux** |
| **Scan Configuration** | **Full and Fast** |
| **Date of Scan** | **October 25**  **, 2025** |

**3. Target Information**

****

**task**

**report**



**4. Scan Summary**

| **Metric** | **Result** |
| --- | --- |
| Total Hosts Scanned | 1 |
| Total Vulnerabilities Detected | 0 |
| High Severity | 0 |
| Medium Severity | 0 |
| Low Severity | 0 |
| Log/Informational | 0 |
| Total Scan Duration | 3 minutes |

**Observation:**

The scan completed successfully, identifying 0 informational (log-level) results. No exploitable or high-severity vulnerabilities were detected on this host.

**5. Mitigation Summary**

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

| **Severity** | **Recommended Action** |
| --- | --- |
| **High** | None detected |
| **Medium** | None detected |
| **Low** | None detected |
| **Informational** | Verify host configuration, kernel version, and maintain regular vulnerability scans. |

**7. Conclusion**

The vulnerability assessment on the meta os 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.