

VULNERABILITY ASSESSMENT REPORT

Tool Used: Tenable Nessus Essentials

Version: 10.11.2 Linux

Scanner: Local Scanner

Target: 127.0.0.1 (Localhost)

Scan Type: Basic Network Scan

Scan Duration: 41 Minutes

Date: February 15, 2026

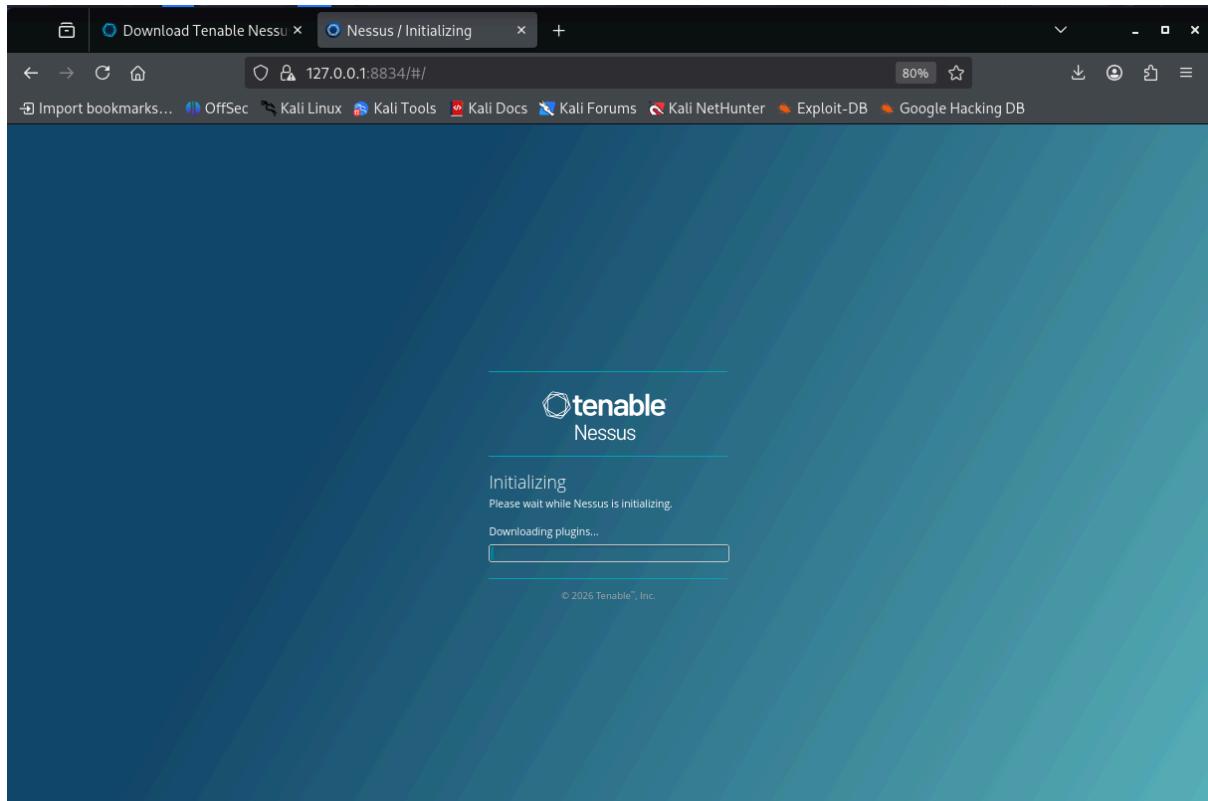
1. Installation & Service Verification

1.1 Nessus Installation

The Nessus package `Nessus-10.11.2-debian10_amd64.deb` was successfully installed using dpkg.

Screenshot Placement:

Insert screenshot:



Unique Identifying Clue:

Look for:

- "INSTALL PASSED"
- cryptographic self-tests (HMAC, SHA1, RSA, etc.)
- Message: *You can start Nessus Scanner by typing /bin/systemctl start nessusd.service*

This confirms successful installation.

1.2 Nessus Service Status Verification

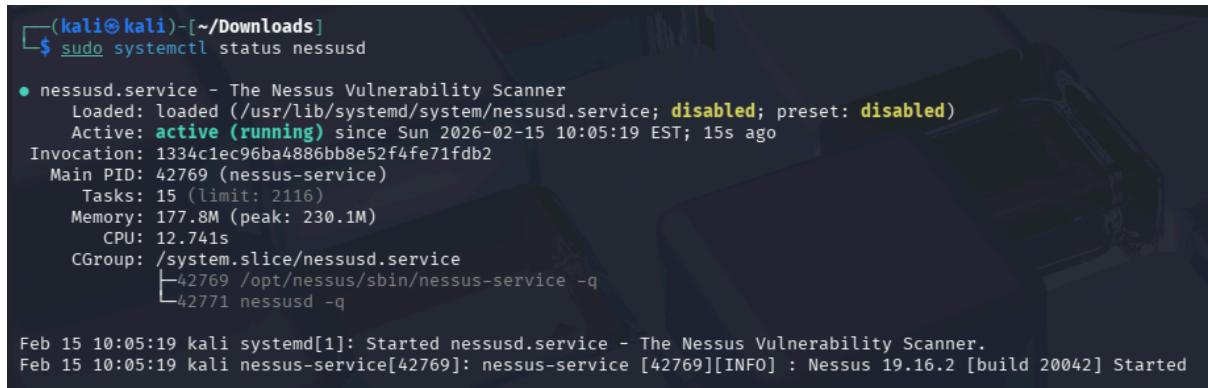
The Nessus service was verified using:

```
sudo systemctl status nessusd
```

Service status: **Active (running)**

Screenshot Placement:

Insert screenshot:



```
(kali㉿kali)-[~/Downloads]
$ sudo systemctl status nessusd
● nessusd.service - The Nessus Vulnerability Scanner
  Loaded: loaded (/usr/lib/systemd/system/nessusd.service; disabled; preset: disabled)
  Active: active (running) since Sun 2026-02-15 10:05:19 EST; 15s ago
    Invocation: 1334c1ec96ba4886bb8e52f4fe71fdb2
    Main PID: 42769 (nessus-service)
      Tasks: 15 (limit: 2116)
     Memory: 177.8M (peak: 230.1M)
        CPU: 12.741s
       CGroup: /system.slice/nessusd.service
           └─42769 /opt/nessus/sbin/nessus-service -q
               ├─42771 nessusd -q

Feb 15 10:05:19 kali systemd[1]: Started nessusd.service - The Nessus Vulnerability Scanner.
Feb 15 10:05:19 kali nessus-service[42769]: nessus-service [42769][INFO] : Nessus 19.16.2 [build 20042] Started
```

Unique Identifying Clue:

- Service name: nessusd.service
- Status: Active (running)
- Main PID visible

- Timestamp: Feb 15
-

2. Plugin Initialization & Updates

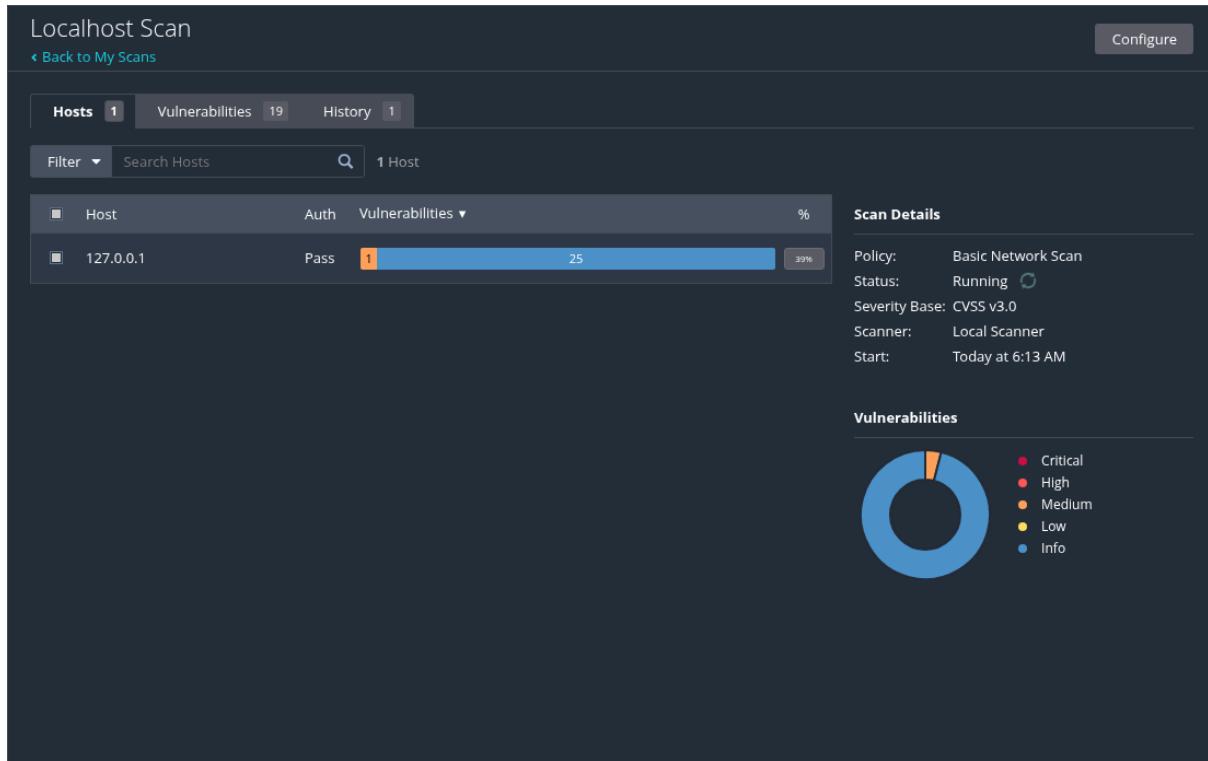
Initially, plugin downloads failed due to network issues. After resolving network/DNS configuration, plugins were successfully updated.

Final Status:

- Nessus Plugins: Complete
- Nessus Core Components: Complete

Screenshot Placement:

Insert screenshot:



Unique Identifying Clue:

- Shows "Nessus Plugins: Complete"
- Mentions copying templates version 202601121526

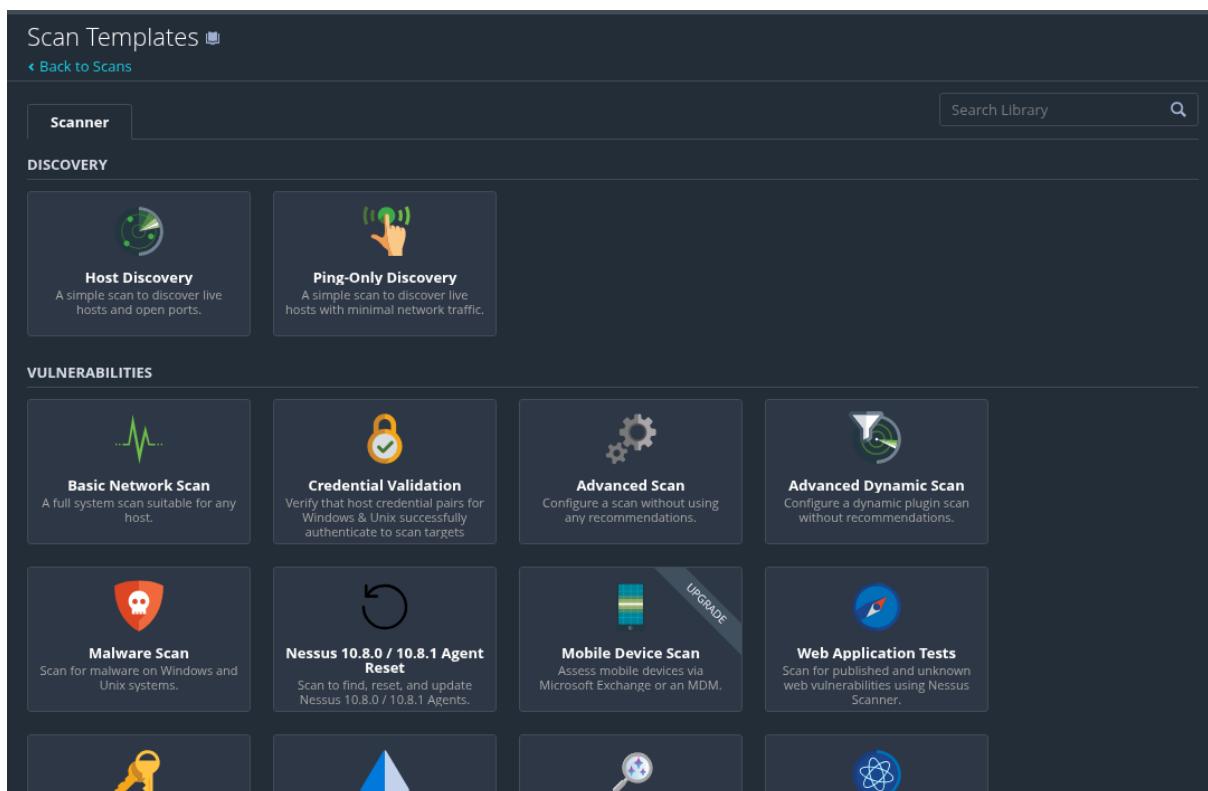
3. Dashboard & Scan Configuration

3.1 Scan Template Selection

Basic Network Scan template was selected.

Screenshot Placement:

Insert:



Unique Clue:

- Template name: Basic Network Scan
- Other templates visible: Malware Scan, Advanced Scan, etc.

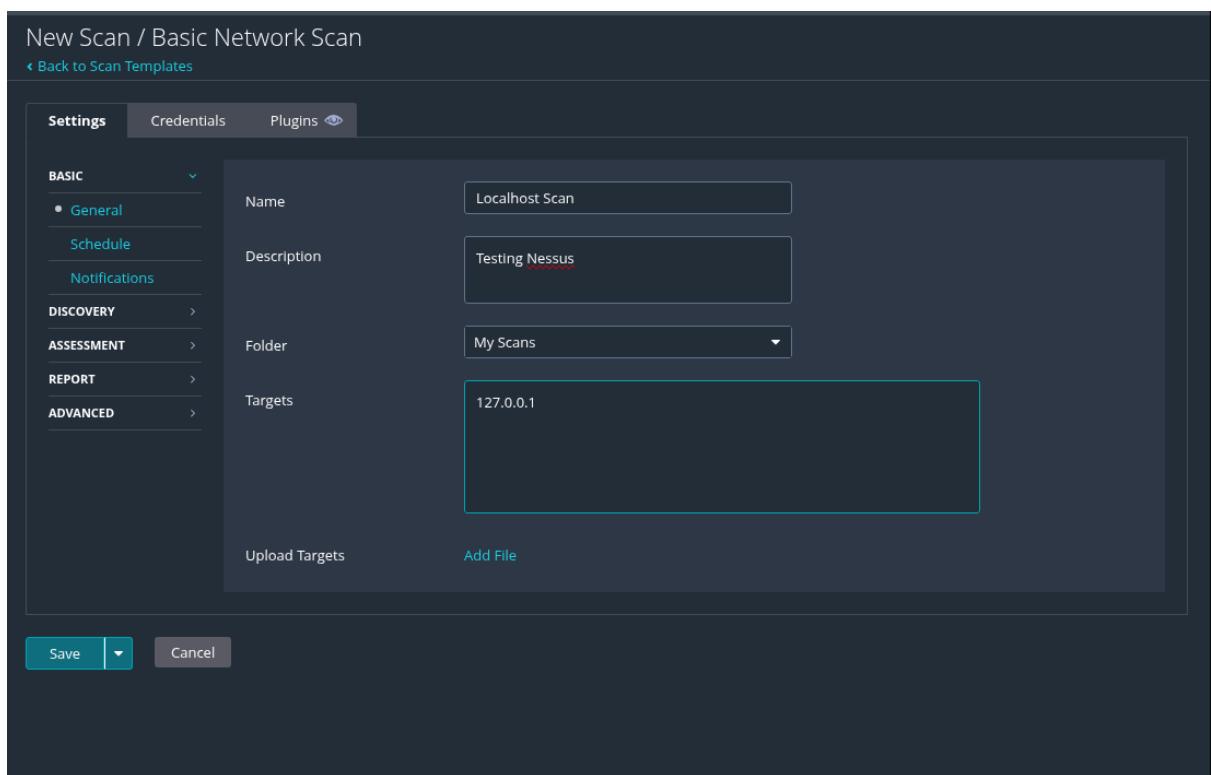
3.2 Scan Configuration

Configured:

- Name: Localhost Scan
- Target: 127.0.0.1
- Folder: My Scans

Screenshot Placement:

Insert:



Unique Clue:

- Target field contains: 127.0.0.1
 - Description: Testing Nessus
-

4. Scan Execution

Scan Status:

- Policy: Basic Network Scan
- Status: Completed
- Duration: 41 minutes
- Start Time: 6:13 AM
- End Time: 6:54 AM

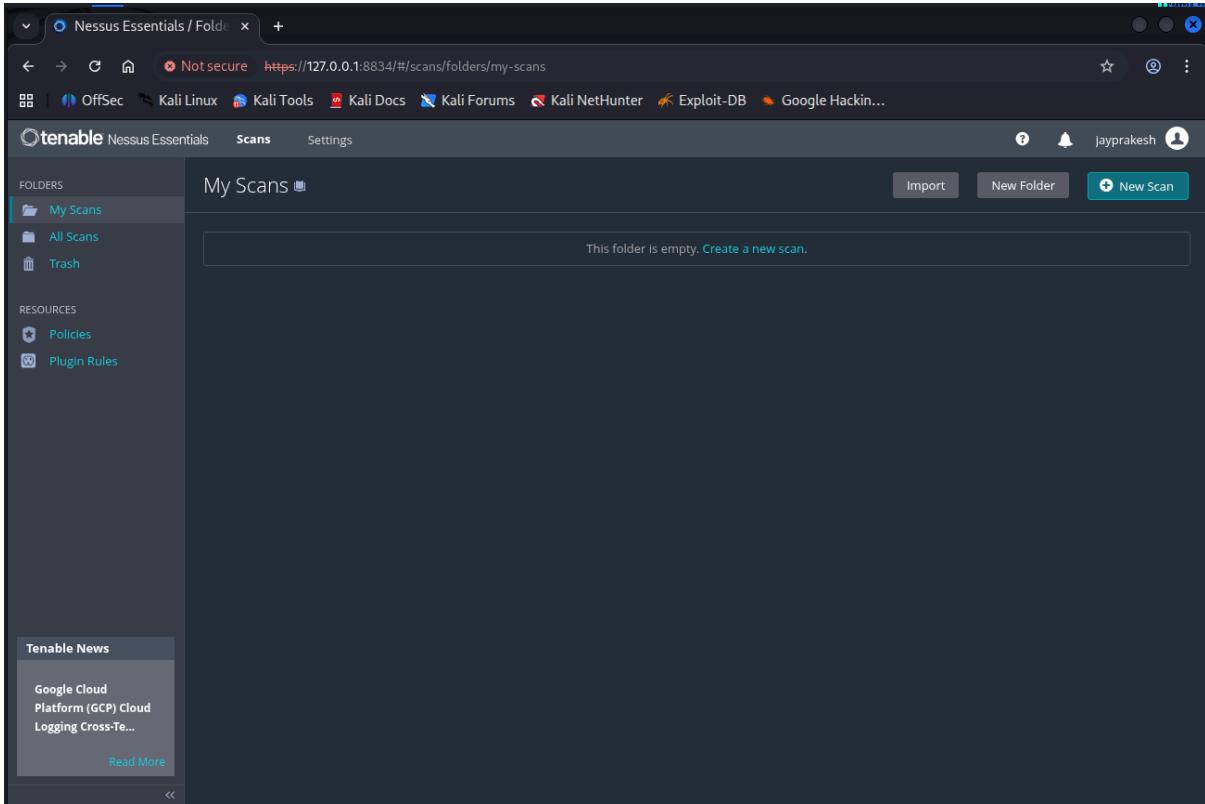
Screenshot Placement:

Insert:

The screenshot shows a dark-themed user interface for managing scans. At the top, there are three buttons: 'Import', 'New Folder', and a teal-colored 'New Scan' button. Below this is a search bar labeled 'Search Scans' with a magnifying glass icon and the text '1 Scan'. A table below the search bar displays the following information for one scan:

| Name | Scan Type | Schedule | Last Scanned | Actions |
|----------------|---------------|-----------|------------------|---------------------------------|
| localhost Scan | Vulnerability | On Demand | Today at 6:14 AM | (play/pause), red square (stop) |

and then



Unique Clue:

- Elapsed: 41 minutes
 - Scanner: Local Scanner
 - Status: Completed
-

5. Scan Results Overview

Total Vulnerabilities Detected: 60

Severity Distribution:

- High: 3
- Medium: 2
- Info: Remaining

Screenshot Placement:

Insert:

The screenshot shows the Tenable Nessus Essentials web application interface. The top navigation bar includes links for OffSec, Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, and Google Hackin... The main content area is titled "Localhost Scan" and displays the results of a scan. The "Hosts" tab is selected, showing one host (127.0.0.1) with a status of "Pass". The "Vulnerabilities" tab shows a count of 60. A donut chart in the "Vulnerabilities" section indicates the severity distribution: Critical (red), High (orange), Medium (yellow), Low (light blue), and Info (dark blue). On the right, "Scan Details" provide information about the scan: Policy (Basic Network Scan), Status (Completed), Severity Base (CVSS v3.0), Scanner (Local Scanner), Start (Today at 6:13 AM), End (Today at 6:54 AM), and Elapsed (41 minutes). The left sidebar contains sections for FOLDERS (My Scans, All Scans, Trash), RESOURCES (Policies, Plugin Rules), and Tenable News (2025 SLG cyber trends: 5 lessons to build a 2026 c...).

Unique Clue:

- Vulnerabilities count shows: 60
 - Host: 127.0.0.1
 - Donut severity chart visible
-

6. High Severity Vulnerability Analysis

Vulnerability Identified:

Python Library Brotli <= 1.1.0 DoS

Severity: HIGH

CVSS v3.0 Score: 7.5

CVE: CVE-2025-6176

Technical Details:

Installed Version: 1.1.0

Fixed Version: 1.2.0

Path:

/usr/lib/python3/dist-packages/Brotli-1.1.0.egg-info

Screenshot Placement:

Insert:

The screenshot shows a detailed analysis of a security vulnerability. At the top, it indicates a severity of HIGH and the specific issue: Python Library Brotli <= 1.1.0 DoS. The report is structured into several sections: Description, Solution, See Also, Output, Plugin Details, Risk Information, Vulnerability Information, and Reference Information. The 'Description' section notes that the detected version (1.1.0) is affected by a denial of service (DoS) vulnerability due to decompression. The 'Solution' section advises upgrading to version 1.2.0 or later. The 'Output' section provides command-line details: Path /usr/lib/python3/dist-packages/Brotli-1.1.0.egg-info, Installed version 1.1.0, Fixed version 1.2.0. It also suggests looking at debug logs on individual hosts. The 'Plugin Details' section lists the following metadata: Severity: High, ID: 274433, Version: 1.1, Type: local, Family: Misc., Published: November 7, 2025, Modified: November 7, 2025. The 'Risk Information' section includes EPSS: 0.0004, Risk Factor: High, and CVSS v3.0 Base Score: 7.5. The 'Vulnerability Information' section lists CPE: cpe:/a:python:brotli, Patch Pub Date: October 30, 2025, and Vulnerability Pub Date: October 30, 2025. The 'Reference Information' section includes IAVA: 2025-A-0813 and CVE: CVE-2025-6176.

Unique Clue:

- CVSS v3.0 Base Score: 7.5
 - EPSS: 0.0004
 - Shows "Upgrade to Brotli version 1.2.0 or later"
-

7. Remediation Summary

Two remediation actions identified:

1. Upgrade Brotli to 1.2.0+
2. Upgrade Ruby REXML to 3.4.2+

Screenshot Placement:

Insert:

The screenshot shows a dark-themed web application interface for a 'Localhost Scan'. At the top, there are navigation buttons: 'Configure', 'Audit Trail', 'Launch', 'Report', and 'Export'. Below these are tabs for 'Hosts' (1), 'Vulnerabilities' (60), 'Remediations' (2), and 'History' (1). A search bar labeled 'Search Actions' with a magnifying glass icon shows '2 Actions'. The main content area displays two remediation items in a table:

| Action | Vulns ▾ | Hosts |
|--------------------------------------------------------------------------------------|---------|-------|
| Python Library Brotli <= 1.1.0 DoS: Upgrade to Brotli version 1.2.0 or later. | 1 | 1 |
| Ruby REXML 3.3.3 < 3.4.2 DoS vulnerability: Upgrade to REXML version 3.4.2 or later. | 0 | 1 |

To the right of the table, a 'Scan Details' panel provides the following information:

| | |
|----------------|--------------------|
| Policy: | Basic Network Scan |
| Status: | Completed |
| Severity Base: | CVSS v3.0 |
| Scanner: | Local Scanner |
| Start: | Today at 6:13 AM |
| End: | Today at 6:54 AM |
| Elapsed: | 41 minutes |

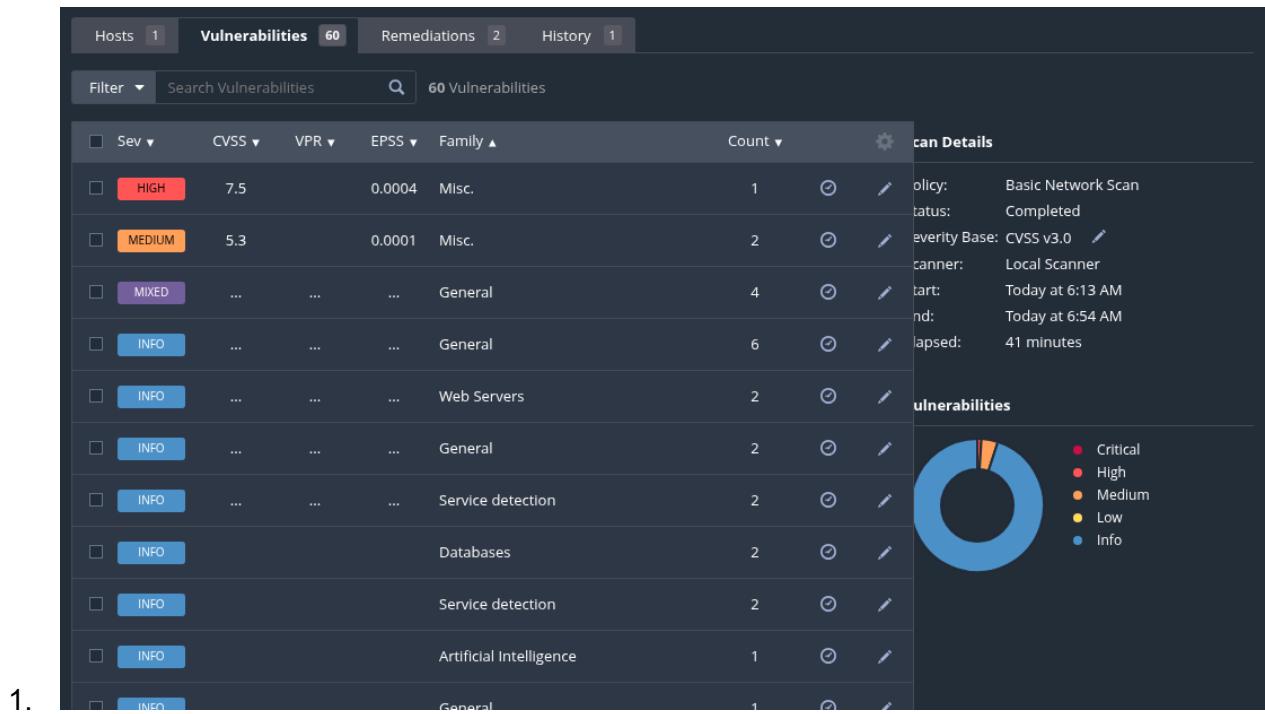
Unique Clue:

- Remediation tab selected
 - Shows 2 Actions
 - Mentions Brotli and REXML
-

8. Vulnerability Listings (Evidence Section)

These screenshots show categorized vulnerability listings.

Insert in this order:



2.

| | | | | |
|-------------------------------|---------|---|-----------------------|--|
| <input type="checkbox"/> INFO | Misc. | 1 | <input type="radio"/> | |
| <input type="checkbox"/> INFO | General | 1 | <input type="radio"/> | |
| <input type="checkbox"/> INFO | General | 1 | <input type="radio"/> | |
| <input type="checkbox"/> INFO | Misc. | 1 | <input type="radio"/> | |
| <input type="checkbox"/> INFO | General | 1 | <input type="radio"/> | |
| <input type="checkbox"/> INFO | Misc. | 1 | <input type="radio"/> | |
| <input type="checkbox"/> INFO | General | 1 | <input type="radio"/> | |
| <input type="checkbox"/> INFO | Misc. | 1 | <input type="radio"/> | |
| <input type="checkbox"/> INFO | General | 1 | <input type="radio"/> | |
| <input type="checkbox"/> INFO | General | 1 | <input type="radio"/> | |
| <input type="checkbox"/> INFO | Misc. | 1 | <input type="radio"/> | |
| <input type="checkbox"/> INFO | Misc. | 1 | <input type="radio"/> | |
| <input type="checkbox"/> INFO | Misc. | 1 | <input type="radio"/> | |
| <input type="checkbox"/> INFO | Misc. | 1 | <input type="radio"/> | |

3.

| | | | | |
|-------------------------------|-------------------------|---|-----------------------|--|
| <input type="checkbox"/> INFO | General | 1 | <input type="radio"/> | |
| <input type="checkbox"/> INFO | General | 1 | <input type="radio"/> | |
| <input type="checkbox"/> INFO | General | 1 | <input type="radio"/> | |
| <input type="checkbox"/> INFO | Settings | 1 | <input type="radio"/> | |
| <input type="checkbox"/> INFO | Service detection | 1 | <input type="radio"/> | |
| <input type="checkbox"/> INFO | General | 1 | <input type="radio"/> | |
| <input type="checkbox"/> INFO | Port scanners | 1 | <input type="radio"/> | |
| <input type="checkbox"/> INFO | Web Servers | 1 | <input type="radio"/> | |
| <input type="checkbox"/> INFO | Misc. | 1 | <input type="radio"/> | |
| <input type="checkbox"/> INFO | Artificial intelligence | 1 | <input type="radio"/> | |
| <input type="checkbox"/> INFO | General | 1 | <input type="radio"/> | |
| <input type="checkbox"/> INFO | Misc. | 1 | <input type="radio"/> | |
| <input type="checkbox"/> INFO | Misc. | 1 | <input type="radio"/> | |
| <input type="checkbox"/> INFO | General | 1 | <input type="radio"/> | |
| <input type="checkbox"/> INFO | General | 1 | <input type="radio"/> | |

4.

| | | | | | |
|--------------------------|-------------------|-------------------------|---|--|--|
| <input type="checkbox"/> | INFO | Misc. | 1 | | |
| <input type="checkbox"/> | INFO | Artificial Intelligence | 1 | | |
| <input type="checkbox"/> | INFO | General | 1 | | |
| <input type="checkbox"/> | INFO | Misc. | 1 | | |
| <input type="checkbox"/> | INFO | Misc. | 1 | | |
| <input type="checkbox"/> | INFO | General | 1 | | |
| <input type="checkbox"/> | INFO | General | 1 | | |
| <input type="checkbox"/> | INFO | Misc. | 1 | | |
| <input type="checkbox"/> | INFO | Settings | 1 | | |
| <input type="checkbox"/> | INFO | General | 1 | | |
| <input type="checkbox"/> | INFO | General | 1 | | |
| <input type="checkbox"/> | INFO | Misc. | 1 | | |
| <input type="checkbox"/> | INFO | Misc. | 1 | | |
| <input type="checkbox"/> | INFO | Web Servers | 1 | | |

5.

| Hosts | 1 | Vulnerabilities | 60 | Remediations | 2 | History | 1 |
|----------------------------------------------------------------|-------------------|-----------------|--------|-------------------|---------|---------|----|
| Filter ▾ | | | | | | | |
| Search Vulnerabilities <input type="text"/> 60 Vulnerabilities | | | | | | | |
| □ Sev ▾ | CVSS ▾ | VPR ▾ | EPSS ▾ | Family ▲ | Count ▾ | | ⚙️ |
| <input type="checkbox"/> | INFO | | | Service detection | 1 | | |
| <input type="checkbox"/> | INFO | | | Settings | 1 | | |
| <input type="checkbox"/> | INFO | | | Settings | 1 | | |
| <input type="checkbox"/> | INFO | | | Misc. | 1 | | |
| <input type="checkbox"/> | INFO | | | General | 1 | | |
| <input type="checkbox"/> | INFO | | | Misc. | 1 | | |
| <input type="checkbox"/> | INFO | | | Misc. | 1 | | |
| <input type="checkbox"/> | INFO | | | General | 1 | | |
| <input type="checkbox"/> | INFO | | | Settings | 1 | | |
| <input type="checkbox"/> | INFO | | | Misc. | 1 | | |

Unique Clue for Each:

All contain:

- Severity column (INFO, MEDIUM, HIGH)
- CVSS column
- Family column
- Count column

Each screenshot scroll position differs — that proves they are separate captures.

9. License & About Information

Nessus Essentials Version:

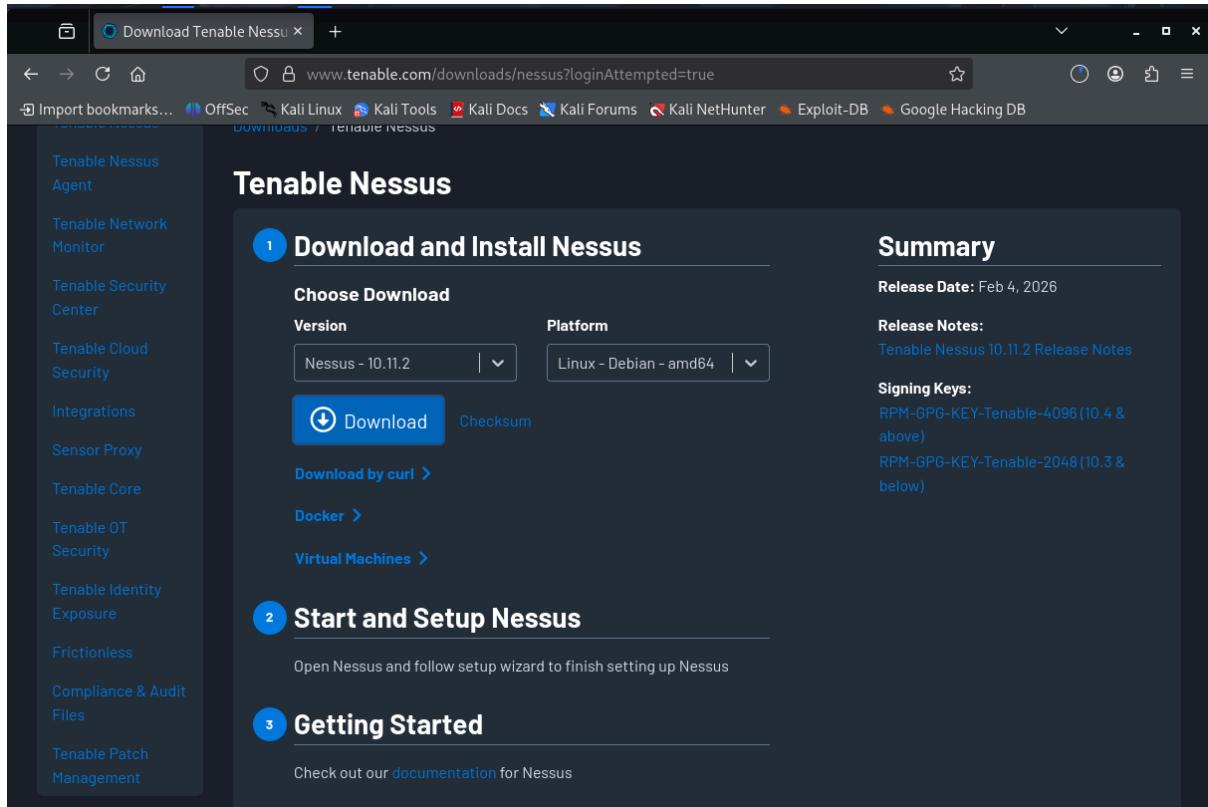
10.11.2 (#42) LINUX

License Expiration:

March 17, 2026

Screenshot Placement:

Insert:



Unique Clue:

- Licensed Hosts: 0 of 5 used
- Activation Code visible

10. Conclusions

- Nessus was successfully installed and configured.
 - Plugins were updated after resolving network issues.
 - A full Basic Network Scan was conducted.
 - 60 vulnerabilities detected.
 - 3 High Severity vulnerabilities found.
 - Primary high-risk issue: Brotli library DoS vulnerability.
 - Immediate remediation recommended.
-

11. Recommendations

1. Upgrade Brotli to version 1.2.0+
2. Update Ruby REXML library
3. Regularly update Nessus plugins
4. Schedule weekly vulnerability scans
5. Enable automatic updates