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

---

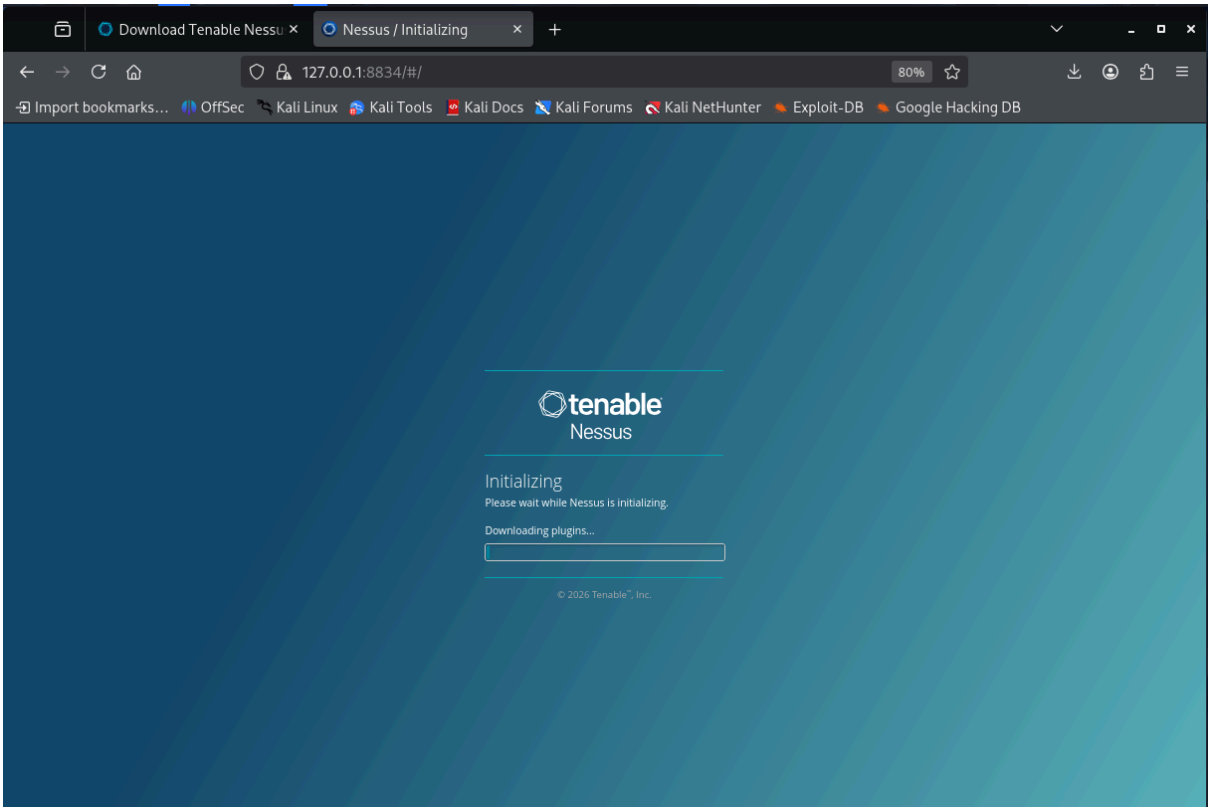
1. Installation & Service Verification

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

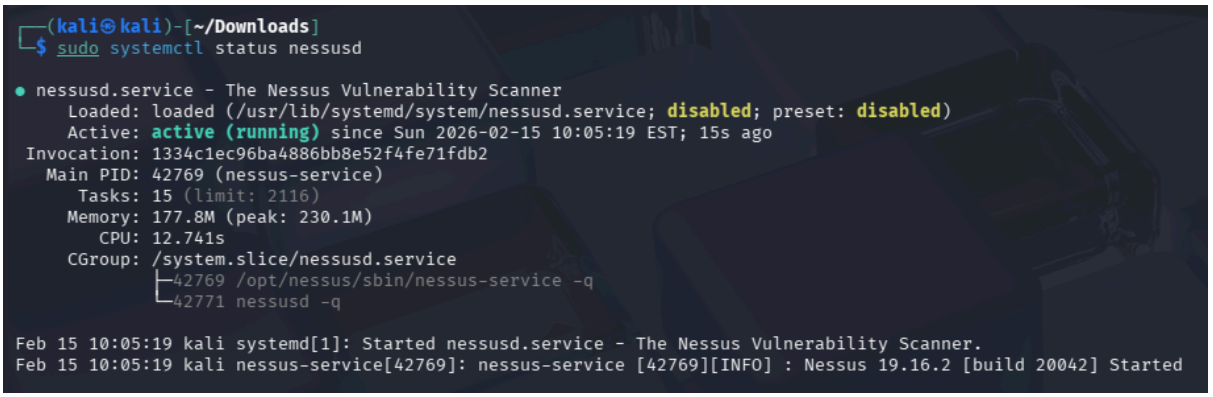
The Nessus service was verified using:

```
sudo systemctl status nessusd
```

Service status: **Active (running)**

Screenshot Placement:

Insert screenshot:



Unique Identifying Clue:

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

- Timestamp: Feb 15

---

2. Plugin Initialization & Updates

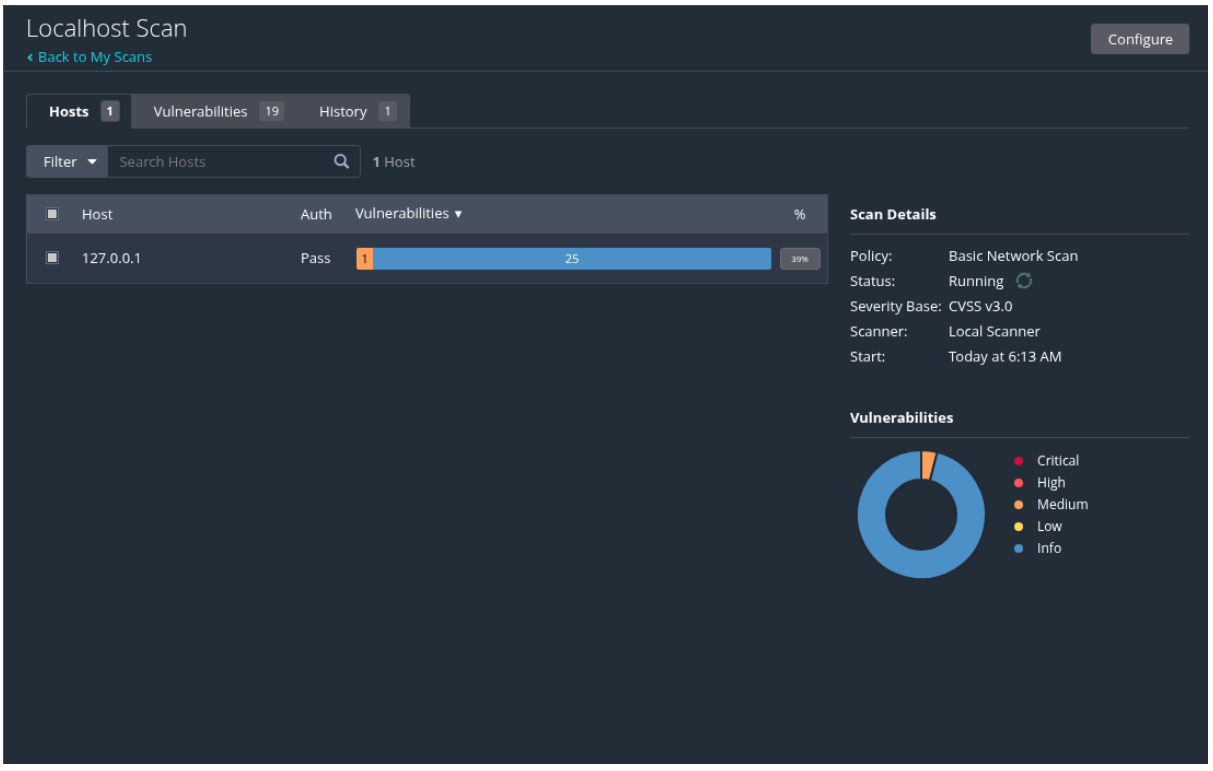
Initially, plugin downloads failed due to network issues. After resolving network/DNS configuration, plugins were successfully updated.

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

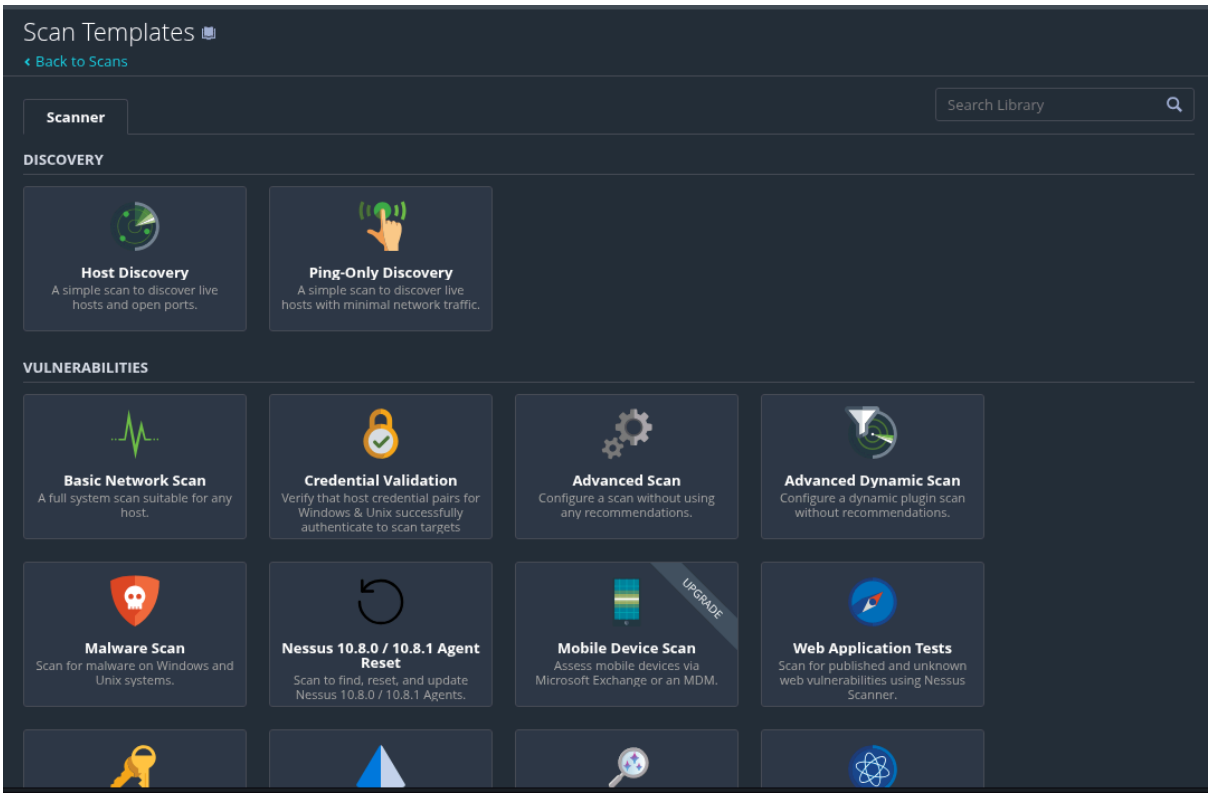
3. Dashboard & Scan Configuration

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.

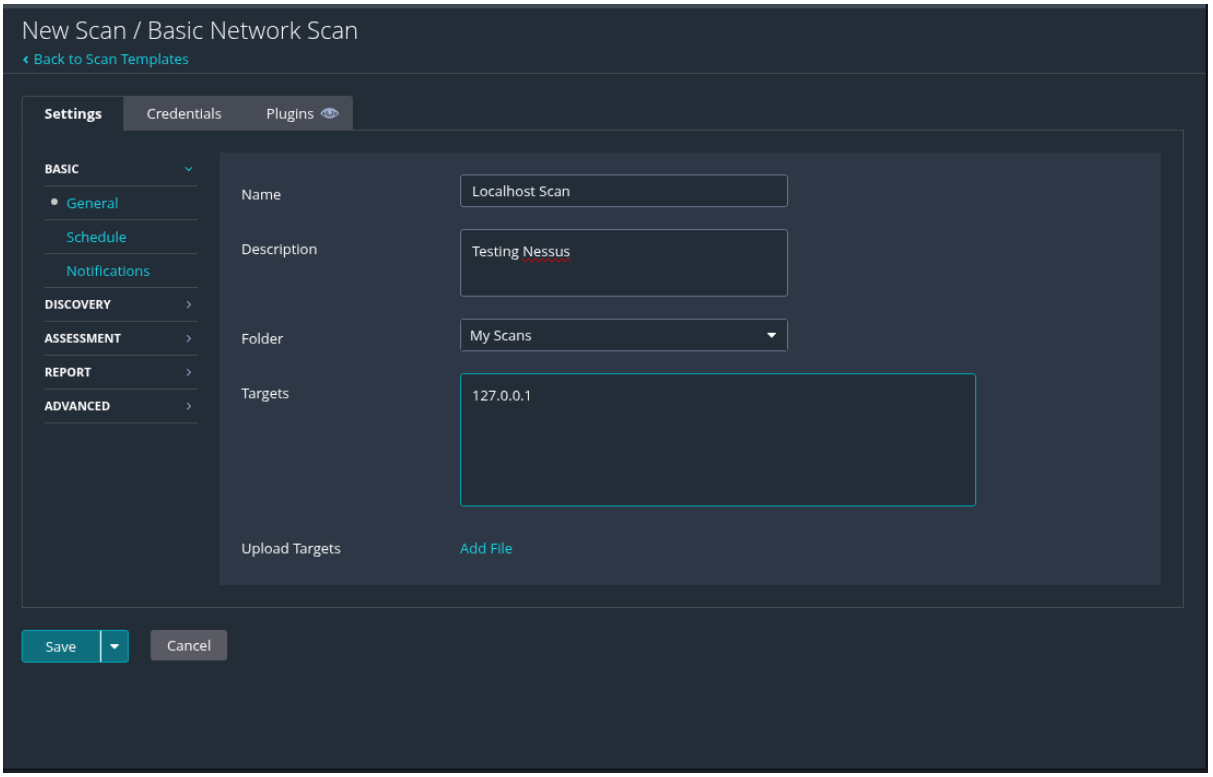
3.2 Scan Configuration

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

---

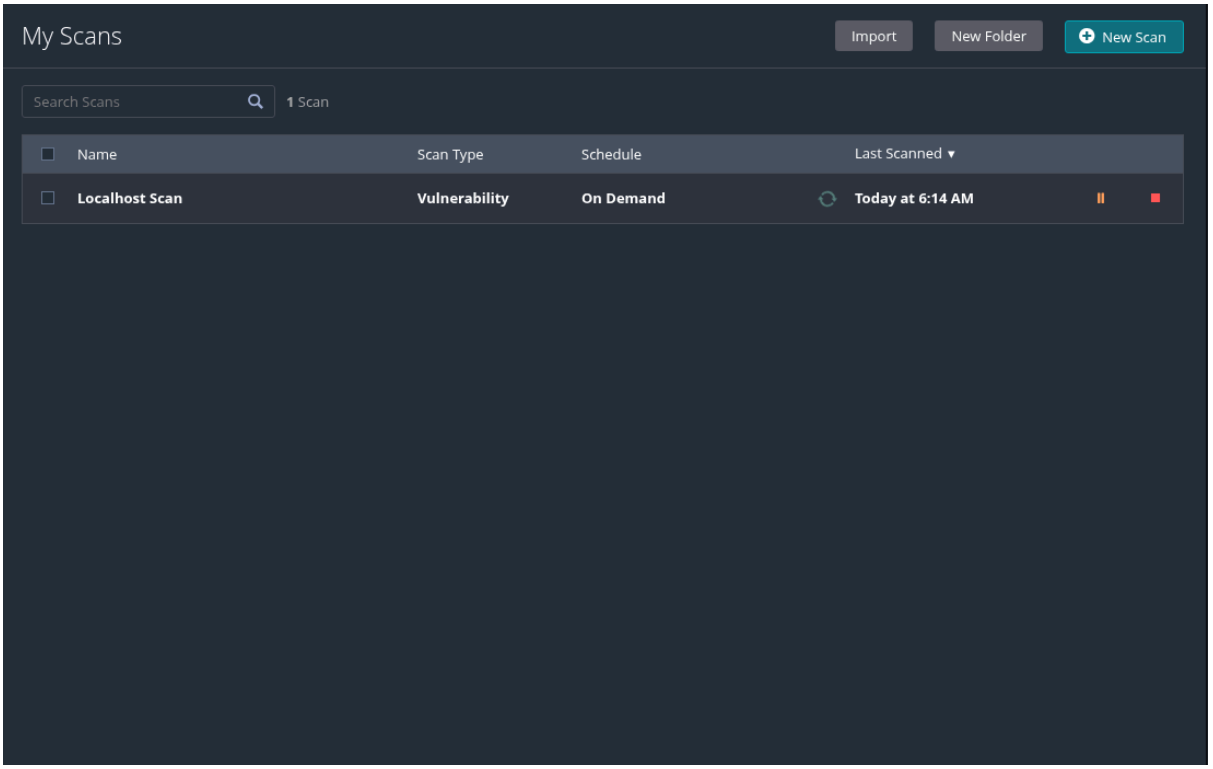
4. Scan Execution

Scan Status:

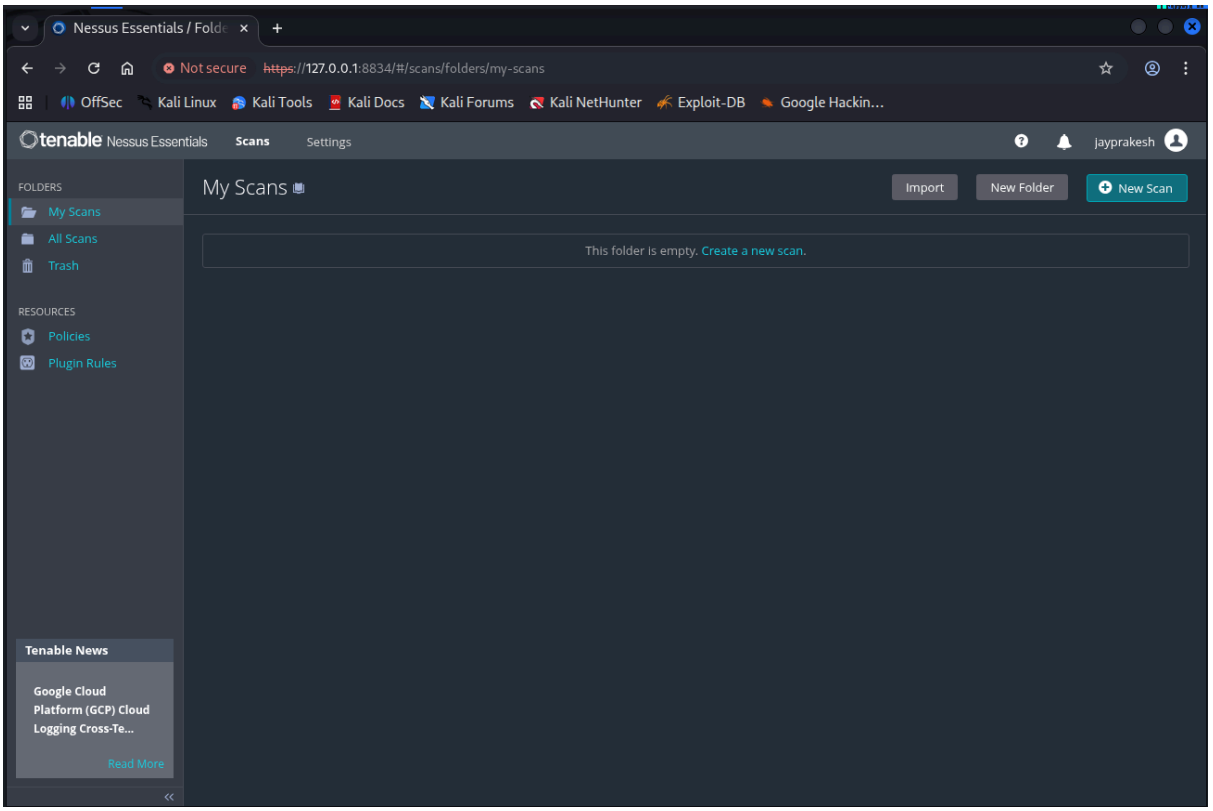
- Policy: Basic Network Scan
- Status: Completed
- Duration: 41 minutes
- Start Time: 6:13 AM
- End Time: 6:54 AM

Screenshot Placement:

Insert:



and then



Unique Clue:

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

---

5. Scan Results Overview

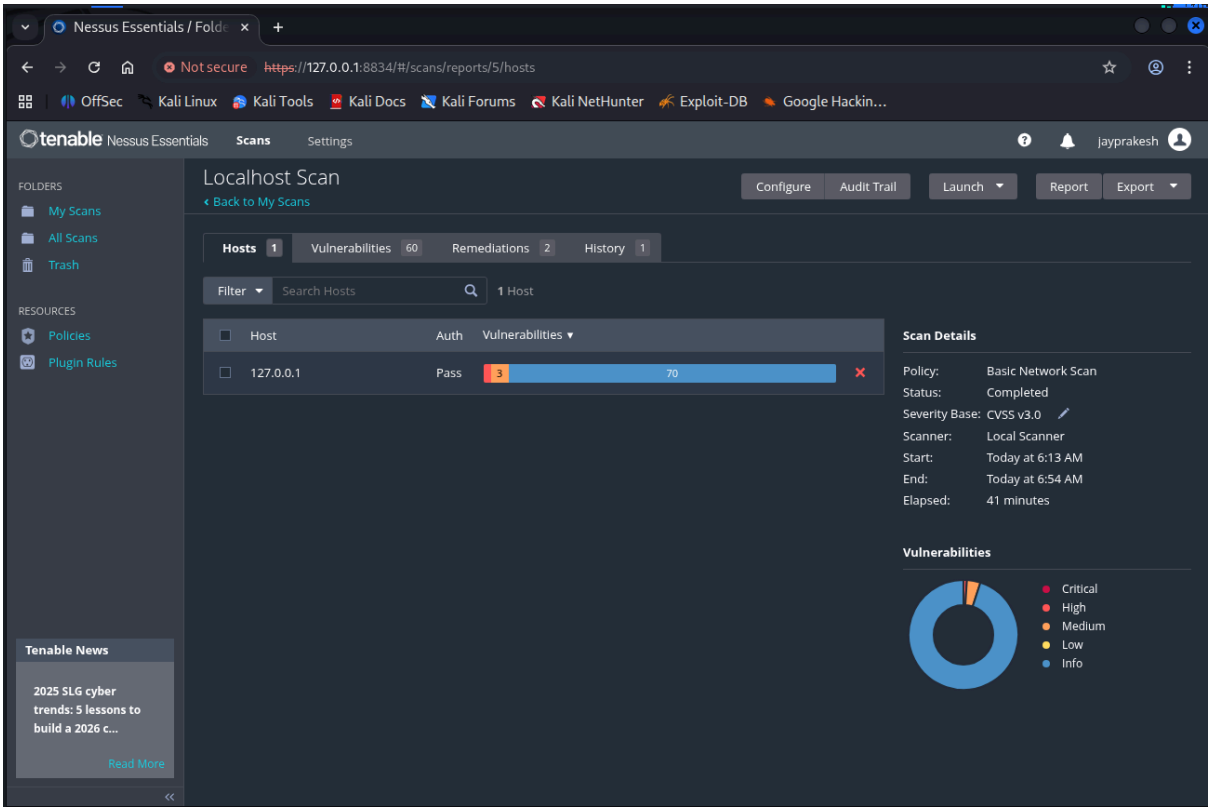
Total Vulnerabilities Detected: 60

Severity Distribution:

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

Screenshot Placement:

Insert:



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

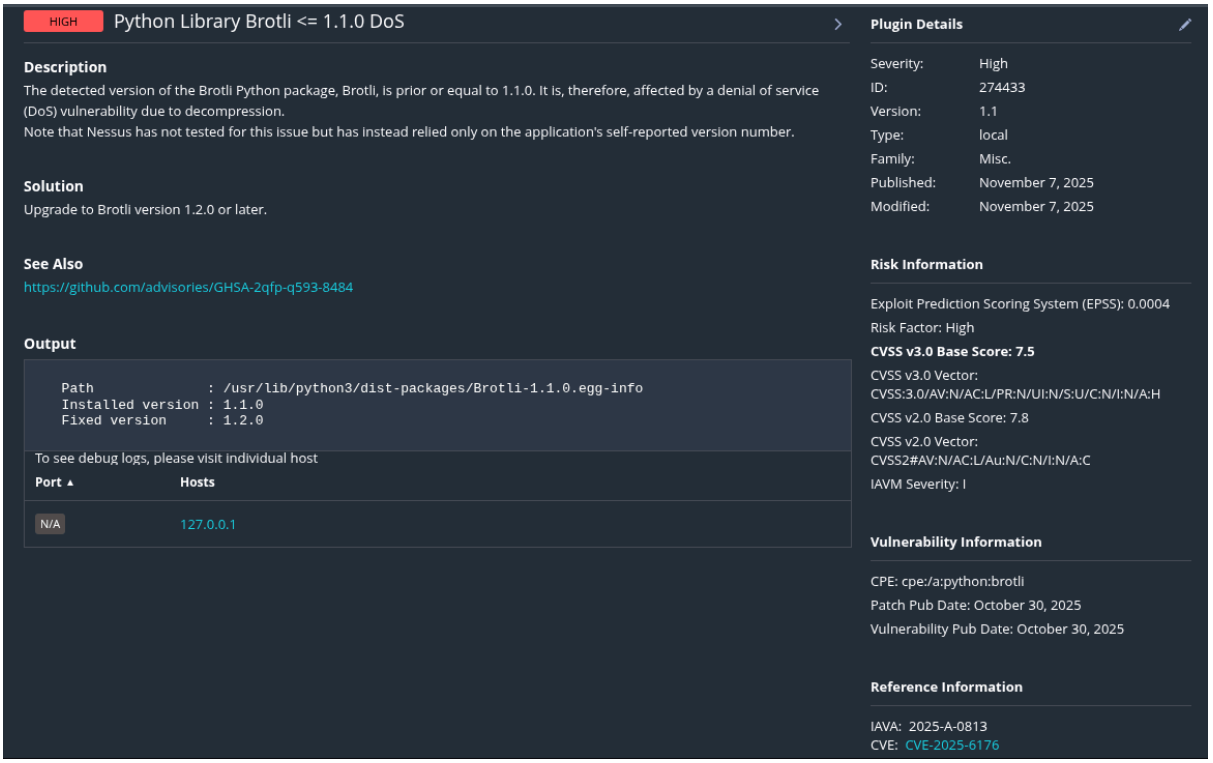
Technical Details:

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:



Unique Clue:

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

---

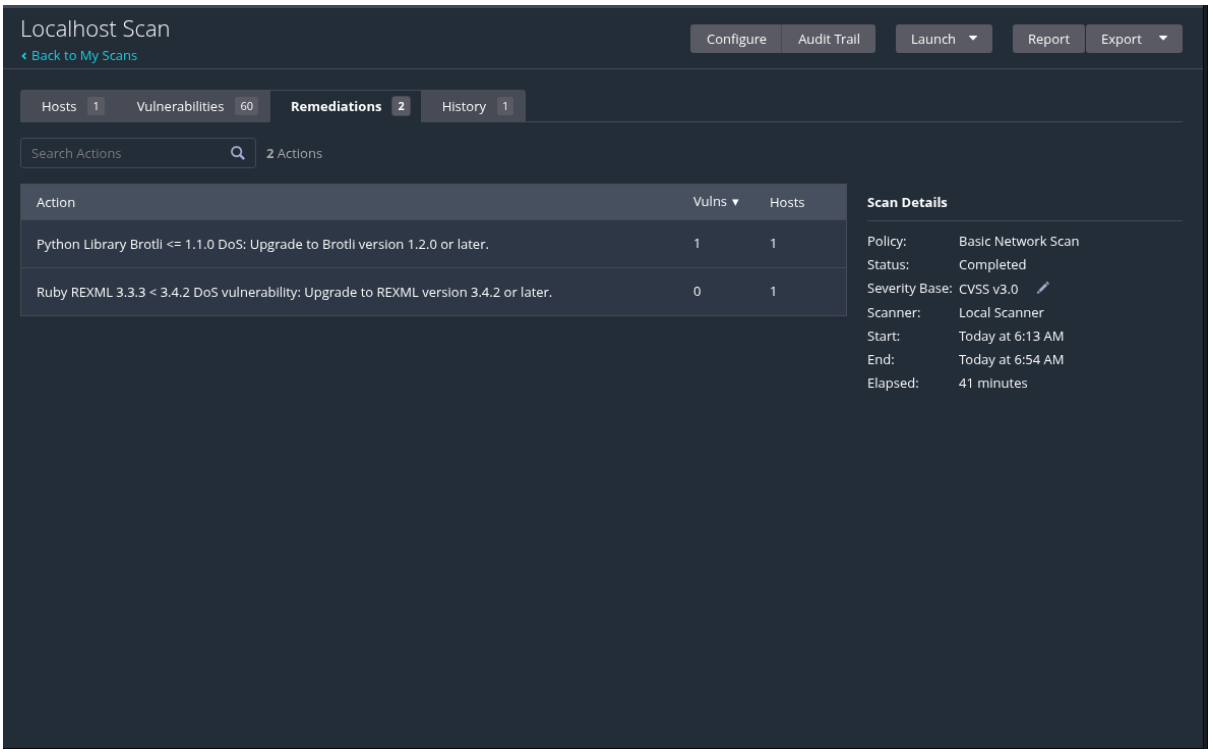
7. Remediation Summary

Two remediation actions identified:

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

Screenshot Placement:

Insert:



Unique Clue:

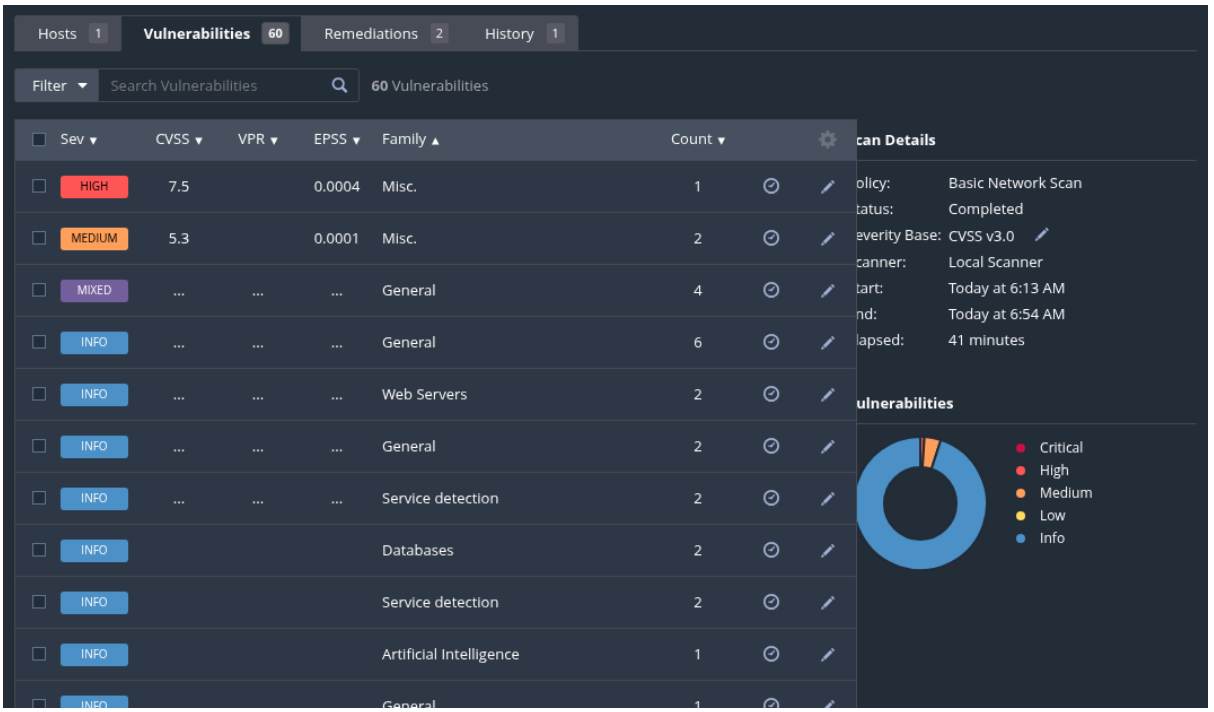
- Remediation tab selected
- Shows 2 Actions
- Mentions Brotli and REXML

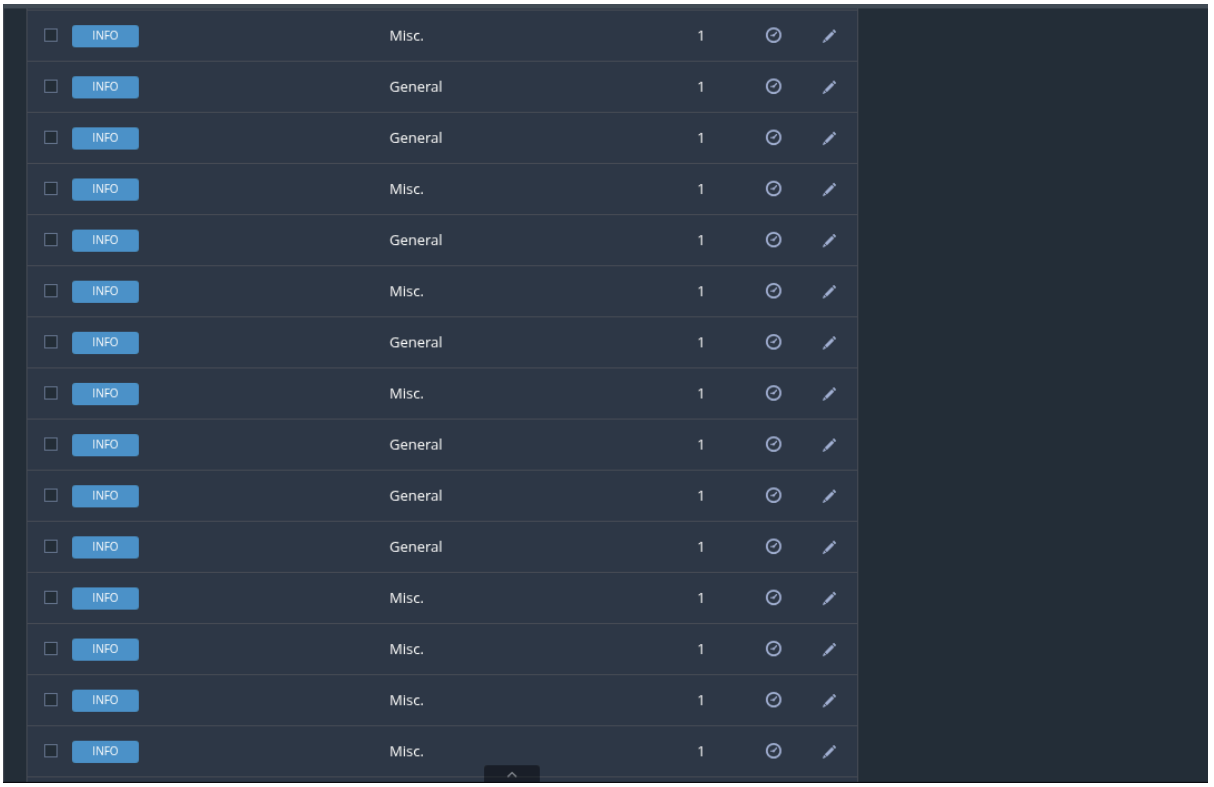
---

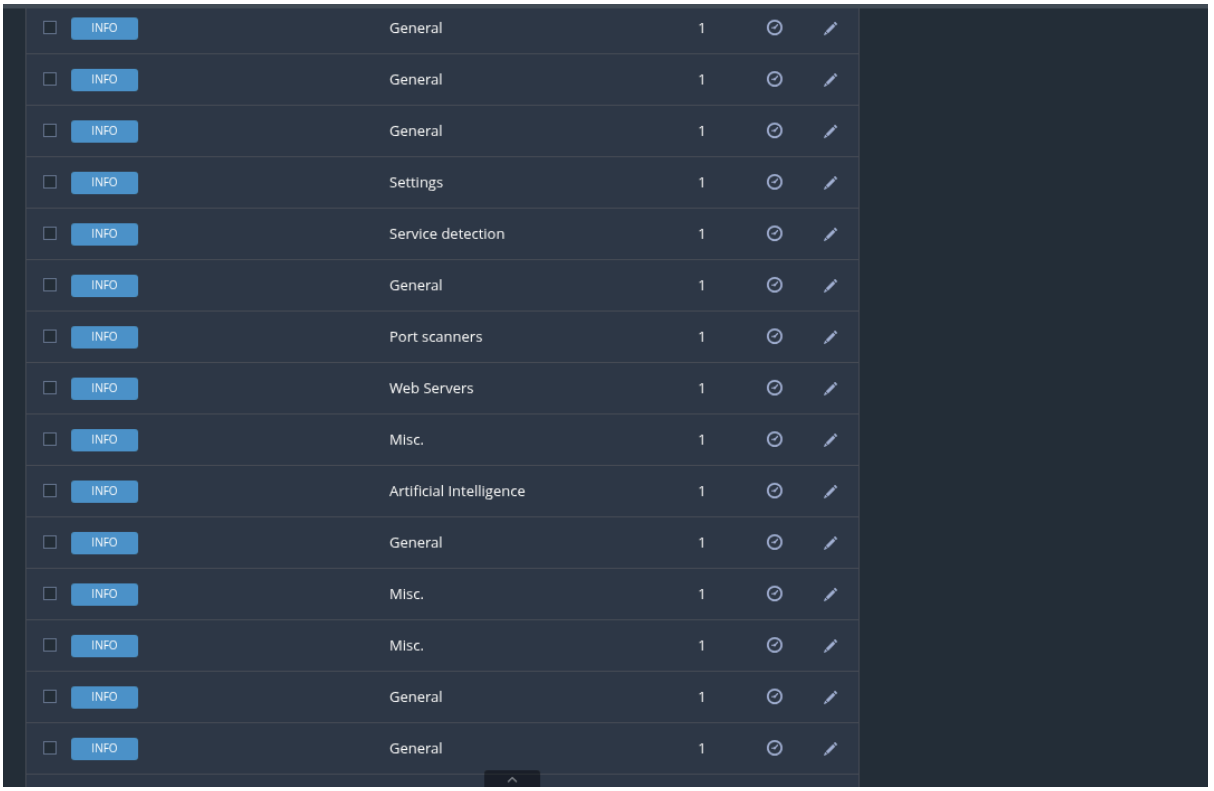
8. Vulnerability Listings (Evidence Section)

These screenshots show categorized vulnerability listings.

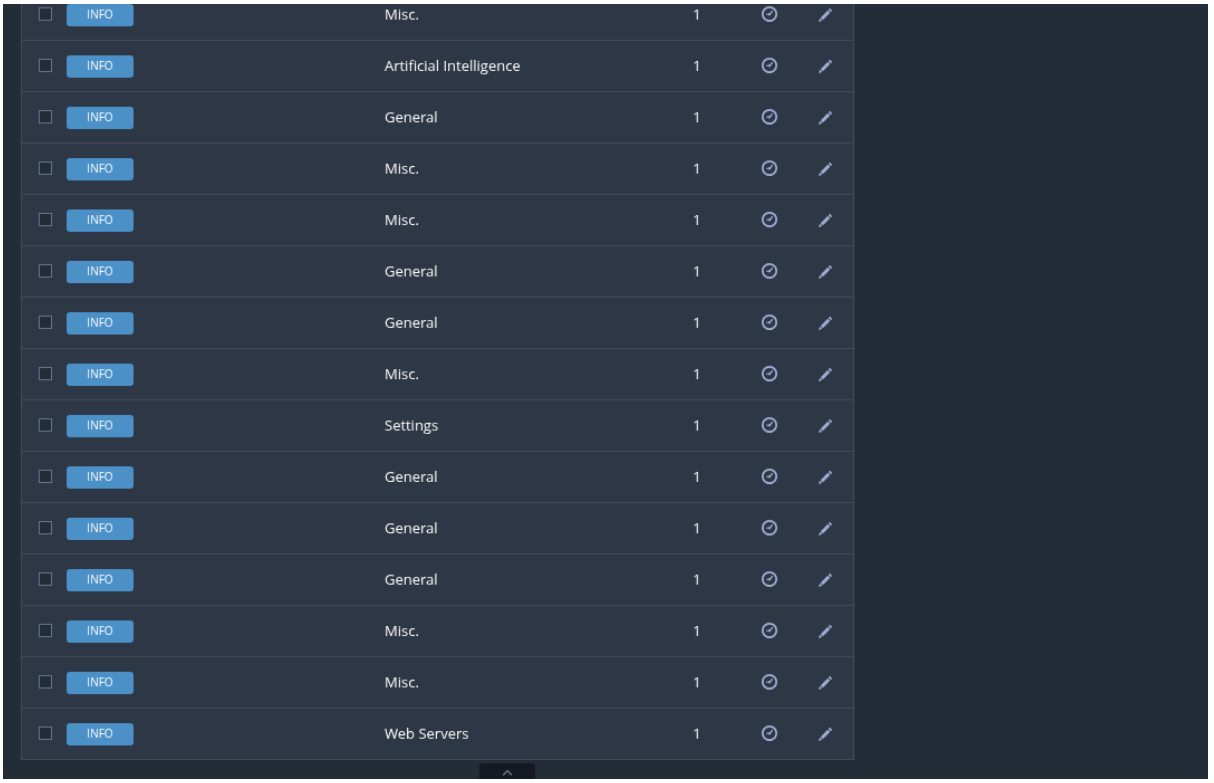
Insert in this order:

1. 

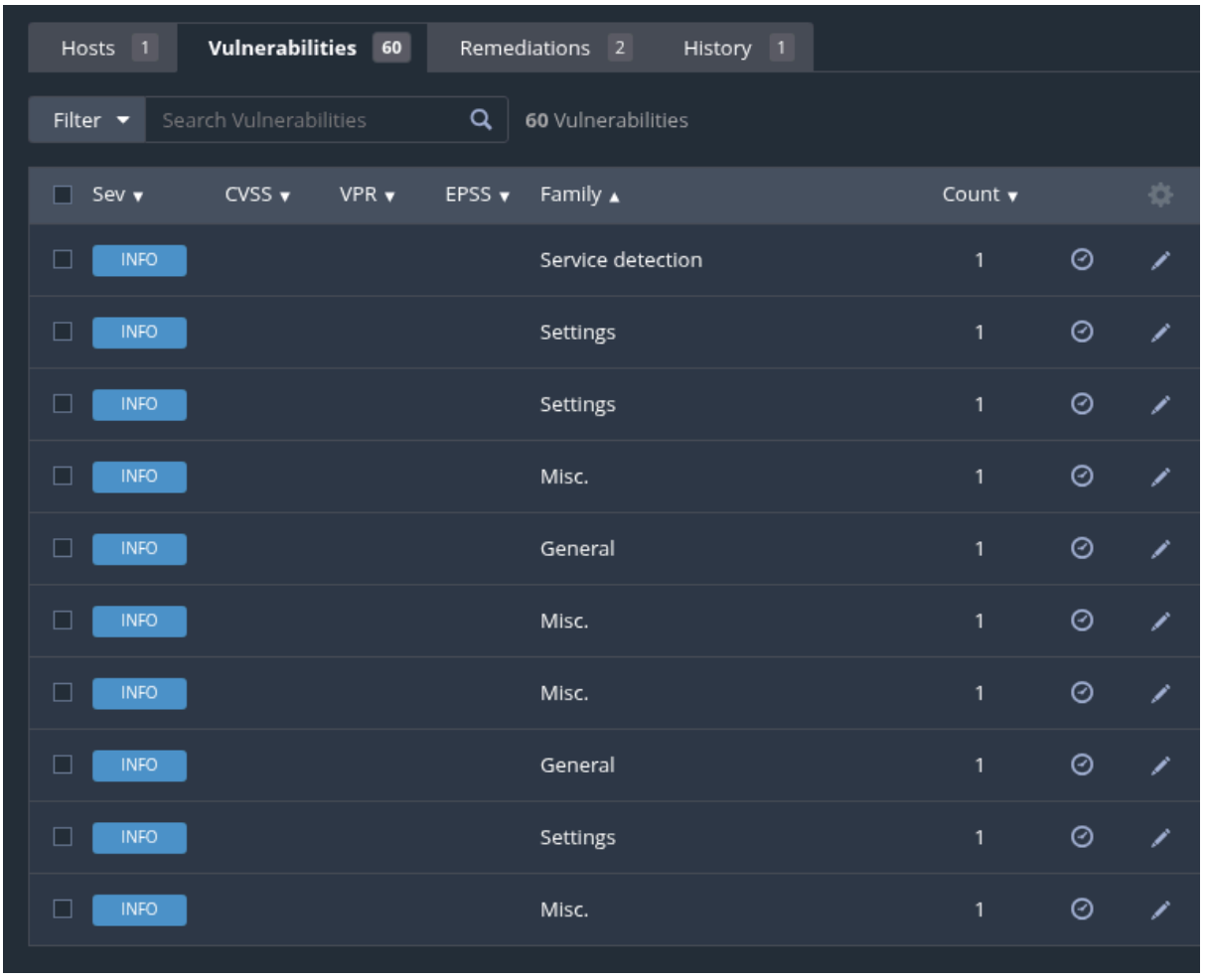
2. 
INFO Misc. 1
INFO General 1
INFO General 1
INFO Misc. 1
INFO General 1
INFO Misc. 1
INFO General 1
INFO Misc. 1
INFO General 1
INFO General 1
INFO General 1
INFO Misc. 1
INFO Misc. 1
INFO Misc. 1
INFO Misc. 1

3. 
INFO General 1
INFO General 1
INFO General 1
INFO Settings 1
INFO Service detection 1
INFO General 1
INFO Port scanners 1
INFO Web Servers 1
INFO Misc. 1
INFO Artificial Intelligence 1
INFO General 1
INFO Misc. 1
INFO Misc. 1
INFO General 1
INFO General 1

4.


INFO Misc. 1
INFO Artificial Intelligence 1
INFO General 1
INFO Misc. 1
INFO Misc. 1
INFO General 1
INFO General 1
INFO Misc. 1
INFO Settings 1
INFO General 1
INFO General 1
INFO General 1
INFO Misc. 1
INFO Misc. 1
INFO Web Servers 1

5.


Hosts 1
Vulnerabilities 60
Remediations 2
History 1
Filter
Search Vulnerabilities
60 Vulnerabilities
Sev
CVSS
VPR
EPSS
Family
Count
INFO Service detection 1
INFO Settings 1
INFO Settings 1
INFO Misc. 1
INFO General 1
INFO Misc. 1
INFO Misc. 1
INFO General 1
INFO Settings 1
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.

---

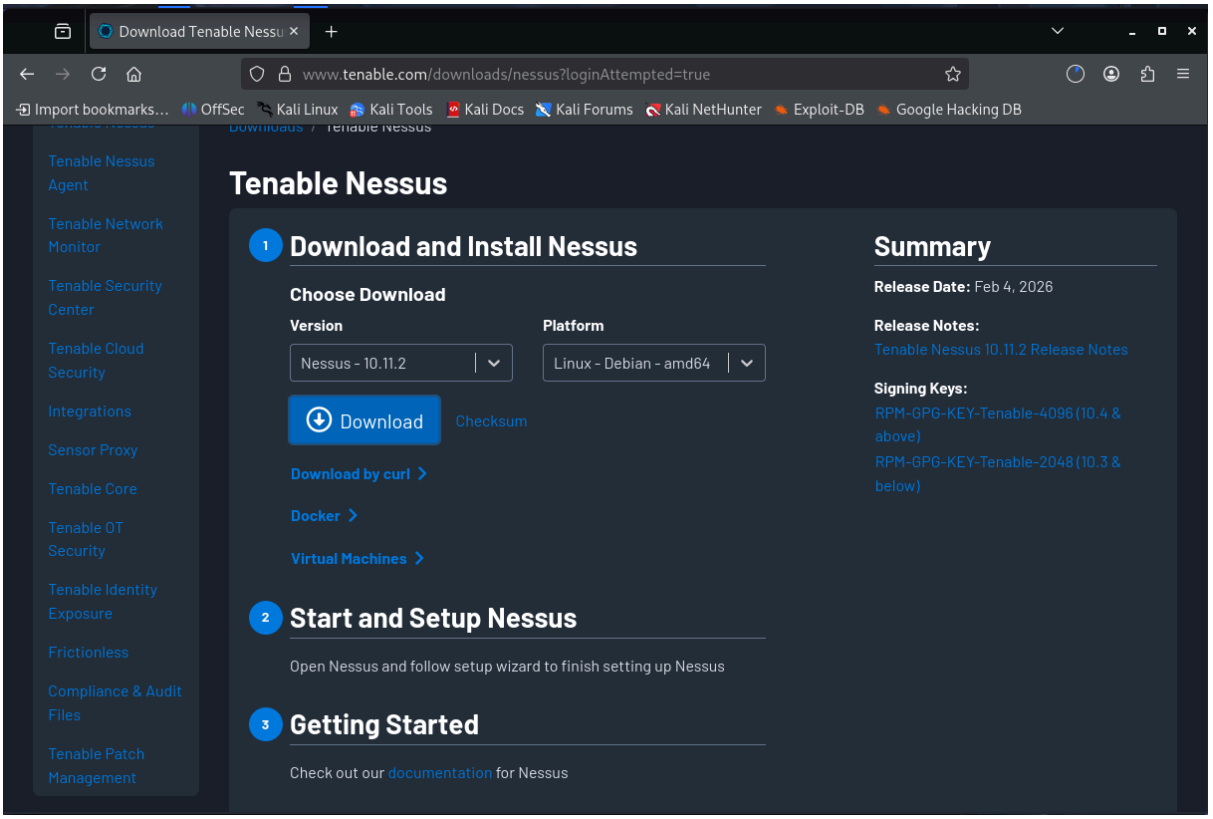
9. License & About Information

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