

## Day 3 - Task 3

**Objective:** Use free tools to identify common vulnerabilities on your computer.

**Tools:** OpenVAS Community Edition (free vulnerability scanner) or Nessus Essentials.

**Deliverables:** Vulnerability scan report with identified issues

## Vulnerability Assessment Report

**Tool Used:** Tenable Nessus Essentials

**Scan Name:** basic\_scan

**Date of Scan:** 08-Aug-2025

**Scan Target:** 10.0.2.15 (Local Machine)

**Policy:** Basic Network Scan

**Scanner:** Basic Vulnerability Scan

**Duration:** 19 minutes

---

### 1. Objective

The objective of this assessment was to use a free vulnerability scanner to identify potential security weaknesses on the local machine, evaluate their severity, and document findings for remediation.

---

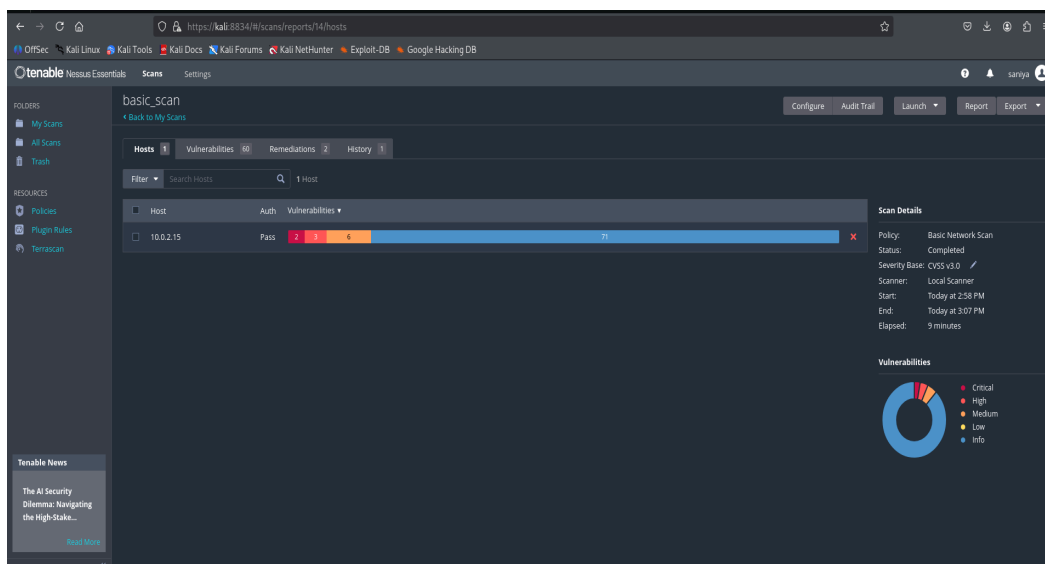
### 2. Methodology

1. Installed **Nessus Essentials** on Kali Linux.
  2. Set up the scan target as the local machine IP (10.0.2.15).
  3. Selected **Basic Network Scan** template.
  4. Launched the scan and allowed it to complete.
  5. Exported the scan results in PDF format and reviewed them.
- 

### 3. Summary of Findings

The scan identified a total of **75 vulnerabilities**:

- **Critical:** 2
- **High:** 3
- **Medium:** 6
- **Low:** 0
- **Informational:** 64



#### 4. Top Critical & High Vulnerabilities

Severity	CVSS v3.0 Score	Vulnerability	Description
Critical	9.8	Node.js < 18.19.1 / 20.11.1 / 21.6.2 Multiple Vulnerabilities	Multiple security flaws in Node.js that may allow remote code execution or denial of service.
Critical	9.1	Node.js < 20.19.4 / 22.17.1 / 24.4.1 Multiple Vulnerabilities	Potentially exploitable flaws that may compromise the system.
High	8.2	Node.js < 18.20.1 / 20.12.1 / 21.7.2 Multiple Vulnerabilities	Remote exploitation possible via crafted input.

High	8.1	Node.js < 18.20.4 / 20.15.1 / 22.4.1 Multiple Vulnerabilities	May allow attackers to bypass security controls.
High	7.7	Node.js < 18.20.6 / 20.18.2 / 22.13.1 Multiple Vulnerabilities	Weaknesses in Node.js security updates.

The screenshot shows the Tenable Nessus Essentials interface. The main panel displays a table of vulnerabilities for a scan named 'basic\_scan'. The table has columns for Severity, CVSS, VPR, EPSS, Name, Family, and Count. The vulnerabilities listed include several Node.js related issues with high severity (CVSS 9.8, 9.1, 8.2, 8.1, 7.7) and two SQLite issues with medium severity (CVSS 6.9, 6.5). On the right side, the 'Scan Details' section shows the policy as 'Basic Network Scan', status as 'Completed', and the scanner as 'Local Scanner'. Below this, a 'Vulnerabilities' donut chart shows the distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

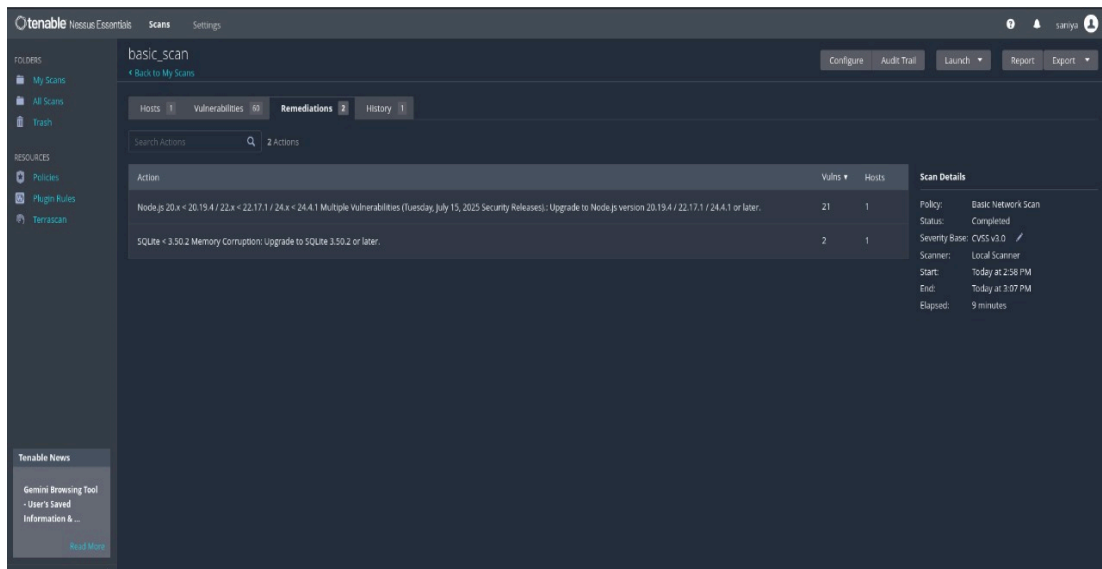
Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	9.8	5.9	0.1041	Node.js 18.x < 18.19.1 / 20.x < 20.11.1 / 21.x < 21.6.2 Multiple Vulnerabilities (Wednesday Febua...	Misc.	1
CRITICAL	9.1	6.1	0.0041	Node.js 20.x < 20.19.4 / 22.x < 22.17.1 / 24.x < 24.4.1 Multiple Vulnerabilities (Tuesday, July 15, 20...	Misc.	1
HIGH	8.2	5.0	0.6865	Node.js 18.x < 18.20.1 / 20.x < 20.12.1 / 21.x < 21.7.2 Multiple Vulnerabilities (Wednesday, April 3...	Misc.	1
HIGH	8.1	6.7	0.0074	Node.js 18.x < 18.20.4 / 20.x < 20.15.1 / 22.x < 22.4.1 Multiple Vulnerabilities (Monday, July 8, 202...	Misc.	1
HIGH	7.7	6.0	0.0006	Node.js 18.x < 18.20.6 / 20.x < 20.18.2 / 22.x < 22.13.1 / 23.x < 23.6.1 Multiple Vulnerabilities (Tue...	Misc.	1
MEDIUM	6.9 *	6.7	0.0006	SQLite 3.44.0 < 3.49.1 Multiple Vulnerabilities	Misc.	2
MEDIUM	6.5			SSL Certificate Cannot Be Trusted	General	1
MEDIUM	6.4	9.4	0.0004	SQLite < 3.50.2 Memory Corruption	Misc.	2
MEDIUM	6.2	3.6	0.0004	Node.js 20.x < 20.19.2 / 22.x < 22.15.1 / 22.x < 22.15.1 / 23.x < 23.11.1 / 24.x < 24.0.2 Multiple Vul...	Misc.	1
INFO				PostgreSQL Client/Server Installed (Linux)	Databases	2
INFO				Service Detection	Service detection	2
INFO				AI/LLM Software Report	Artificial Intelligence	1

## 5. Other Notable Issues

- **Medium:** SSL Certificate Cannot Be Trusted.
- **Medium:** SQLite < 3.50.2 Memory Corruption vulnerability.
- Multiple informational findings such as software enumeration, service detection, and SSL/TLS configuration details.

## 6. Recommendations

- **Update Node.js** to the latest stable version to patch all listed vulnerabilities.
- **Update SQLite** to a secure version (> 3.50.2).
- Replace or reconfigure **SSL certificates** to use a trusted Certificate Authority (CA).
- Review and harden services revealed by **service detection** to minimize exposure.



## 7. Conclusion

The scan revealed multiple severe vulnerabilities, primarily due to outdated Node.js and SQLite versions. Immediate patching is required to prevent potential exploitation. Informational findings should also be reviewed to reduce unnecessary exposure of system details.