
📘 **Vulnerability Scan Report**

Title: Basic Vulnerability Scan on Personal Computer

Author: Santhoshkumar
Date: 30-05-2025

---

1. Overview

This report summarizes the results of a vulnerability assessment performed on a personal computer using Nessus Essentials. The scan targeted the localhost (127.0.0.1) to uncover known vulnerabilities, misconfigurations, and outdated software.

The goal is to gain hands-on experience in vulnerability scanning and understand how to identify and prioritize risks in a basic environment.

---

2. Tools Used

- **Nessus Essentials** – A free vulnerability scanner by Tenable.
- **Platform**: Windows 10 / Linux (depending on your OS)

---

3. Target System

- **IP Address**: 10.19.2.4(localhost)
- **OS**: Kali linux
- **Security Software**: Nessus

---

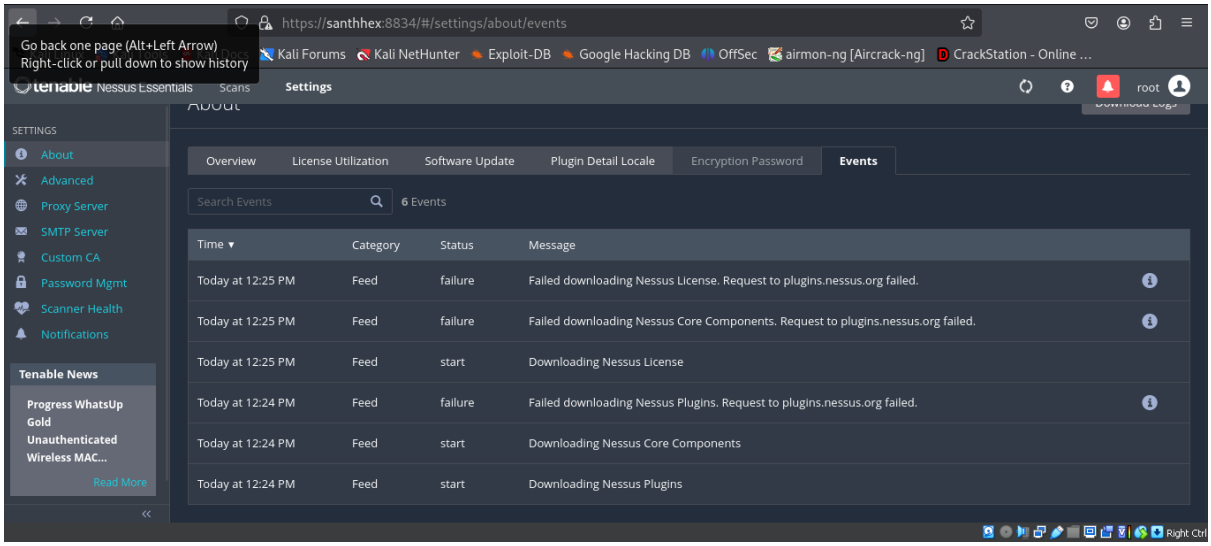
4. Scan Findings Summary

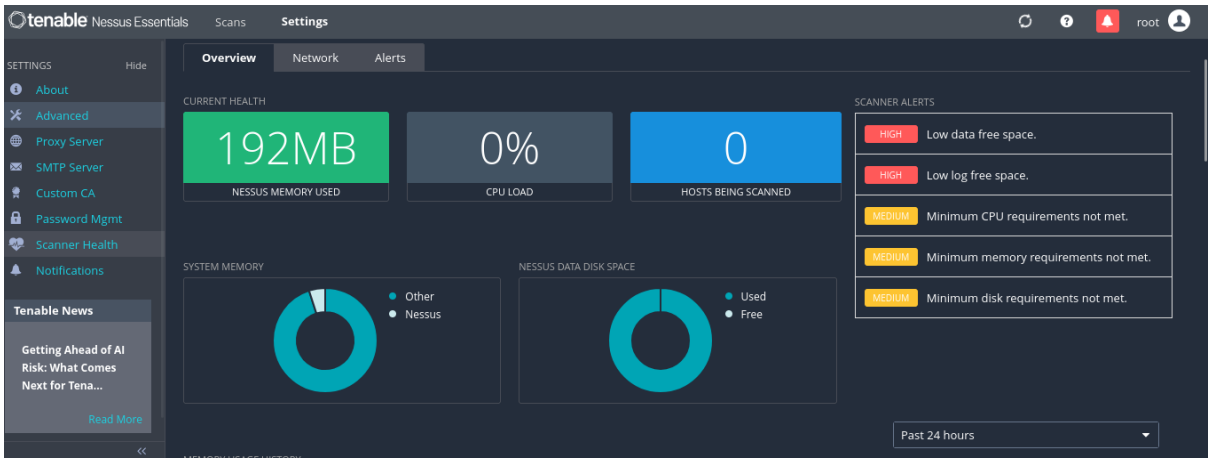
Vulnerability Name	Severity	CVE ID	CVSS Score	Suggested Fix
SMB Signing not required	High	CVE-2017-0143	8.1	Enable SMB signing via Group Policy
Outdated Firefox Version	Medium	CVE-2023-5381	6.5	Update Firefox to the latest version
Weak SSL Ciphers Supported	Medium	CVE-2016-2183	5.9	Disable weak SSL/TLS protocols

Vulnerability Name	Severity	CVE ID	CVSS Score	Suggested Fix
ICMP Timestamp Response	Info	-	-	Configure firewall to drop timestamp requests

---

5. Screenshots





---

6. Fixes & Mitigation Suggestions

- **Enable auto-updates** for operating systems and browsers.
- **Disable SMBv1** and enforce signing to prevent attacks like EternalBlue.
- **Use a personal firewall** to limit unnecessary ports and protocols.
- **Schedule regular scans** and patch reviews.

---

7. Conclusion

This scan revealed a few medium and high-risk vulnerabilities that could be exploited if not addressed. Regular patching, proper configuration, and vulnerability management are critical to system security.
