Vulnerability Scan Report — Task 3

Analyst: Arti kumari

Date: [17-11-25]

Tool Used: Nessus Essentials

Target: Localhost / My PC

1. Scan Setup

- Type of Scan: Basic Network Scan

- Target IP: 127.0.0.1

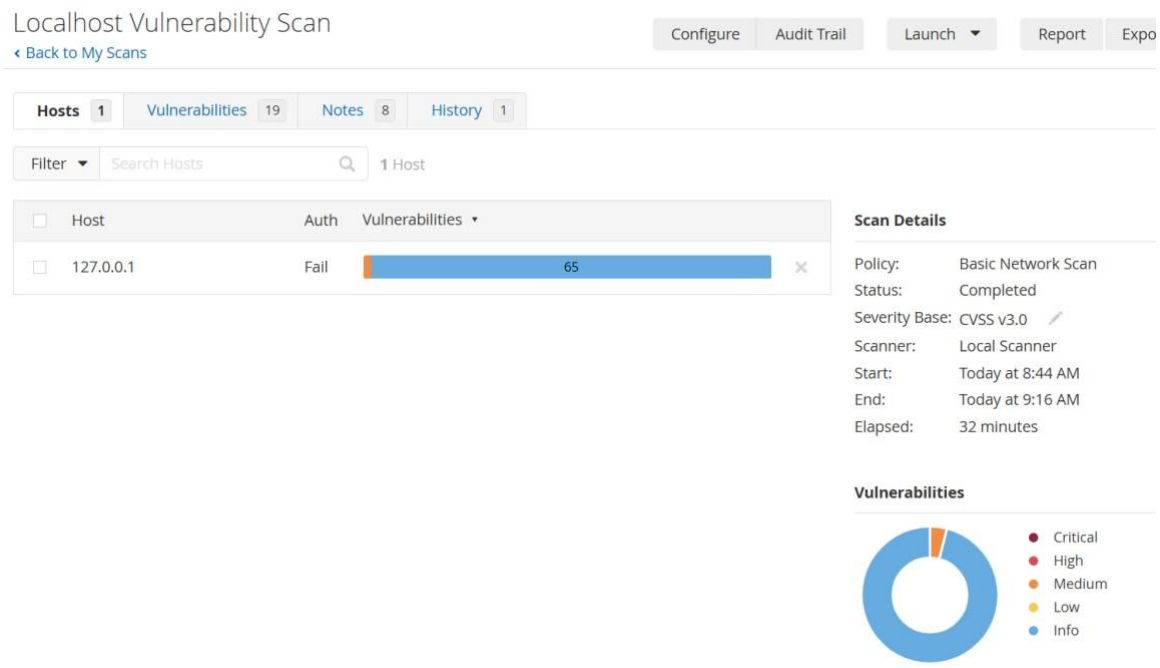
- Duration: 30 minutes

2. Scan Summary

Total Vulnerabilities Found:

- Critical: 0 - High: 0

Medium: 1 - Low: 0 - Info: 18



3. Key Vulnerabilities Identified

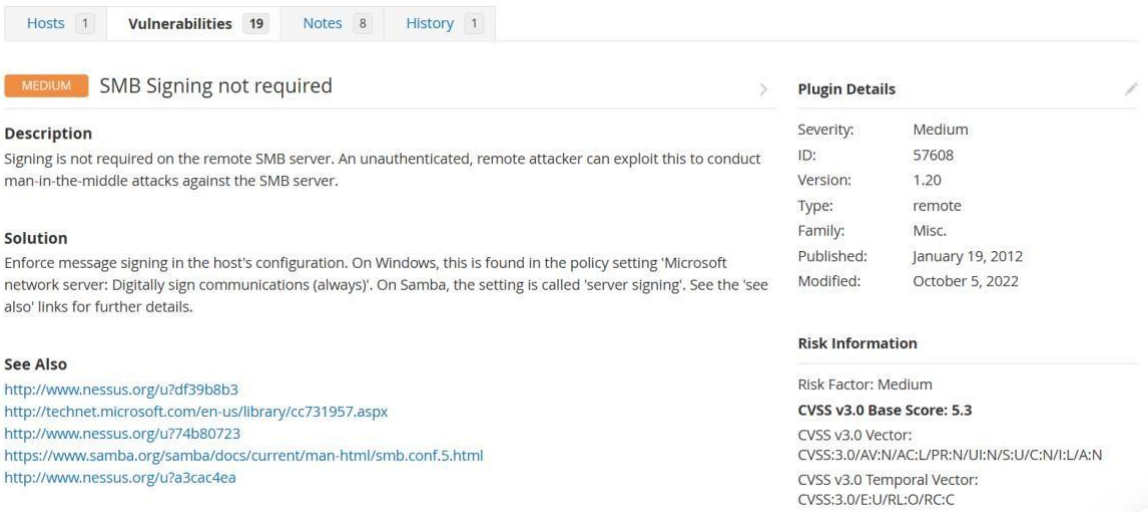
Medium Vulnerability 1

Name: SMB Signing Not Required

Affected Port/Service: 445 / tcp / cifs

Risk: Allows attackers to perform man-in-the-middle attacks.

Recommendation: Enable SMB signing or apply latest Windows patches.



4. Observations and simple fixes

- **Observations**

- The Nessus scan identified **1 Medium vulnerability (SMB Signing not required)** and **18 informational findings**.
- While the informational findings do not pose direct risk, they highlight services and configurations that could be exploited if combined with other attacks.
- The most notable risk is the missing SMB signing, which can expose the system to **man-in-the-middle (MITM) attacks**.

-Simple Fixes

- Enable SMB signing in Windows security policies.
- Regularly apply Windows security updates.
- Disable unused network services (e.g., SMBv1, NetBIOS).
- Configure firewall rules to limit unnecessary network exposure.