Task 3 : Perform a Basic Vulnerability Scan on Your PC

Nessus is a widely used vulnerability scanning tool developed by Tenable, designed to identify security weaknesses within computer systems, networks, and applications. It performs automated vulnerability assessments by scanning hosts to detect known vulnerabilities, misconfigurations, default passwords, insecure protocols, and other potential security issues.

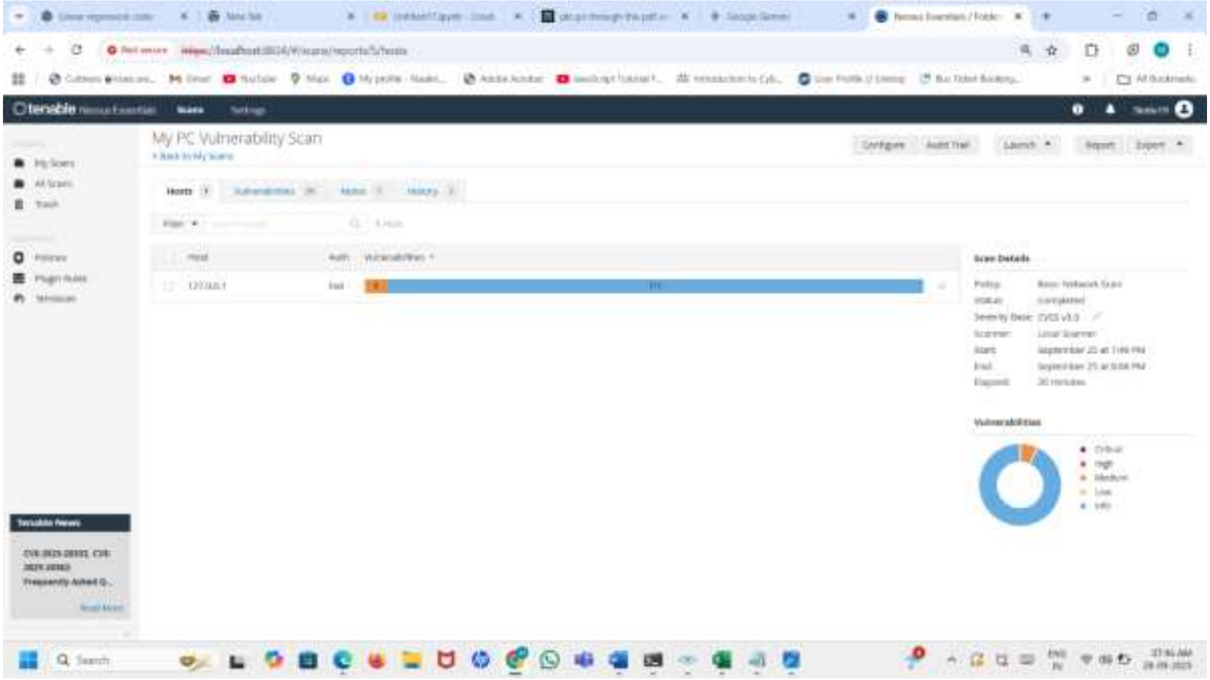
Nessus operates by leveraging an extensive and regularly updated database of vulnerability signatures and checks. It probes systems and services through techniques such as port scanning and service fingerprinting, then compares the results against its database to identify risks. Each vulnerability is rated based on severity levels using the Common Vulnerability Scoring System (CVSS), which helps prioritize remediation efforts.

Key features of Nessus include its ability to scan multiple platforms (Windows, Linux, macOS), support for network and web application scanning, configuration auditing, and reporting capabilities. It provides comprehensive and detailed reports that include vulnerability descriptions, impact assessments, and recommended fixes.

Nessus Essentials, the version used in this task, is a free edition that supports high-speed vulnerability scanning for up to 16 IPs, making it ideal for personal or small network assessments.

By automating vulnerability detection, Nessus helps organizations proactively secure their infrastructures, reduce exposure to cyber threats, and maintain compliance with security standards.

Snapshots of scanning:



My PC Vulnerability Scan

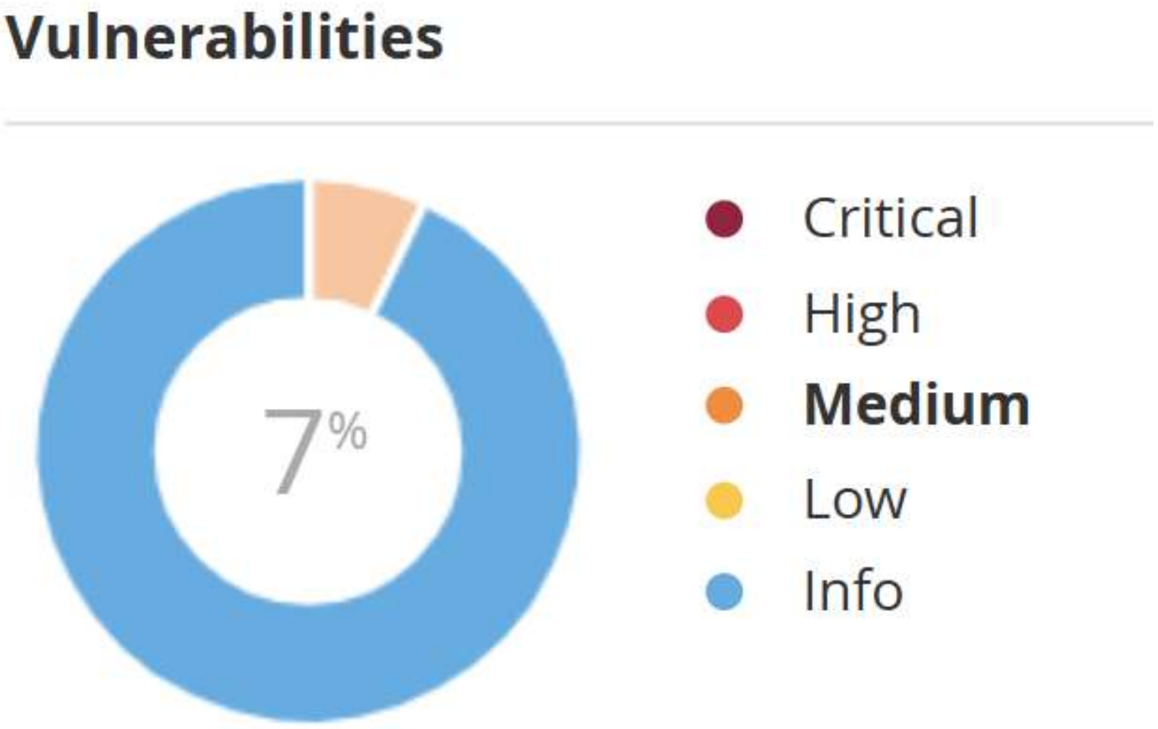
< Back to My Scans

Host	Auth	Vulnerabilities
127.0.0.1	Fail	[illegible]

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: September 25 at [illegible] PM
End: September 25 at [illegible] PM
Elapsed: 30 minutes

Vulnerabilities



Review of Vulnerabilities and Severity

After completing the scan, the Nessus report detailed multiple vulnerabilities on the local machine. These were categorized by severity using CVSS scores:

- **Critical:** No critical issues detected in this scan.
- **High:** Several high-risk findings, primarily outdated operating system patches and insecure protocols enabled.
- **Medium:** A handful of medium-severity issues related to legacy software versions and weak encryption settings.
- **Low / Info:** Numerous informational findings related to host configuration and network exposure, which offer guidance for further hardening.tenable+1

Simple Fixes and Mitigation Steps

For each vulnerability, Nessus provides recommended remediation in the report. The most common fixes and mitigations include:aventistech

- **Apply OS and software patches:** Ensure the operating system and key applications are fully updated via official channels. Regular patching removes many known vulnerabilities.
- **Disable obsolete or insecure protocols:** For example, disable SMBv1 and weak TLS versions to reduce risk from legacy attack vectors.
- **Enforce strong encryption:** Update configurations to require the latest TLS protocols and cipher suites.

- **Secure unused services:** Disable or restrict exposed network services that are not required for daily operations.
- **Follow principle of least privilege:** Limit access rights to necessary personnel and accounts only.

Most Critical Vulnerabilities Identified

The following table summarizes the critical and high-risk vulnerabilities from the scan, including their severity, impact, and recommended remediation:github+1

Vulnerability	Severity	Impact	Recommended Fix
Outdated Windows update	High	System may be vulnerable to known exploits	Install latest Windows patches
SMBv1 protocol enabled	High	Susceptible to ransomware, remote attacks	Disable SMBv1, use SMBv2/3
Weak TLS protocols	Medium	May allow attackers to intercept data	Disable TLS 1.0/1.1, enforce TLS 1.2/1.3
Third-party software outdated	Medium	Vulnerable applications could be exploited	Update to newest available versions

These vulnerabilities should be prioritized for remediation to minimize risk and maintain a secure environment. Nessus provided direct references and remediation steps within the scan report for each detected issue.