Task 3: Performing a Basic Vulnerability Scan

Cybersecurity Lab Report

KANDI TEJASREE
ELEVATE LABS

Task 3:

Performing a Basic Vulnerability Scan

Index:

1. Install Nessus Essentials.
2. Setting up target as our local machine IP.
3. Starting a vulnerability Scan.
4. Reviewing the report for vulnerabilities and severity.
5. Research to find mitigations for found Vulnerabilities.
6. Documentation of the most critical Vulnerabilities found during the scan.

Objective:

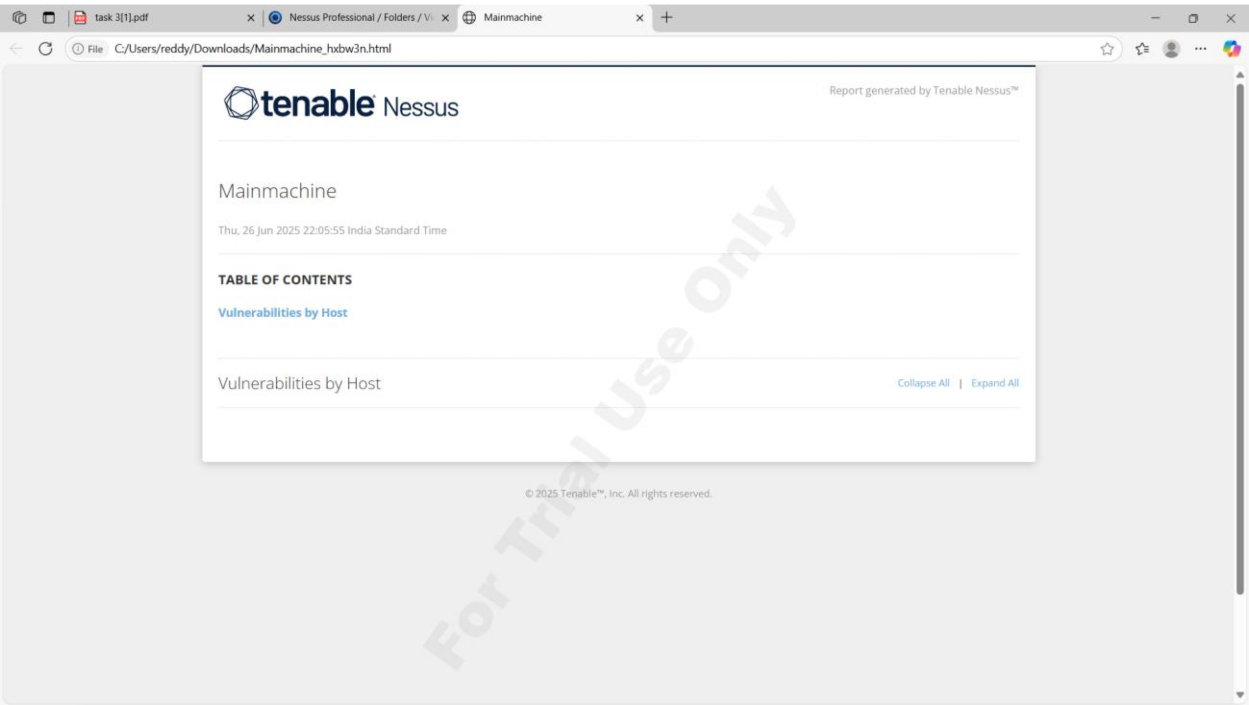
Using Open-Source tools to identify common vulnerabilities on our computer.

Tools Used:

- Nessus Essentials

Steps Performed:

Installation of Nessus Essentials



task 3[1].pdf
Nessus Professional / Folders / V
Mainmachine
File C:/Users/reddy/Downloads/Mainmachine_hxbw3n.html
tenable Nessus

Report generated by Tenable Nessus™

Mainmachine

Thu, 26 Jun 2025 22:05:55 India Standard Time

TABLE OF CONTENTS

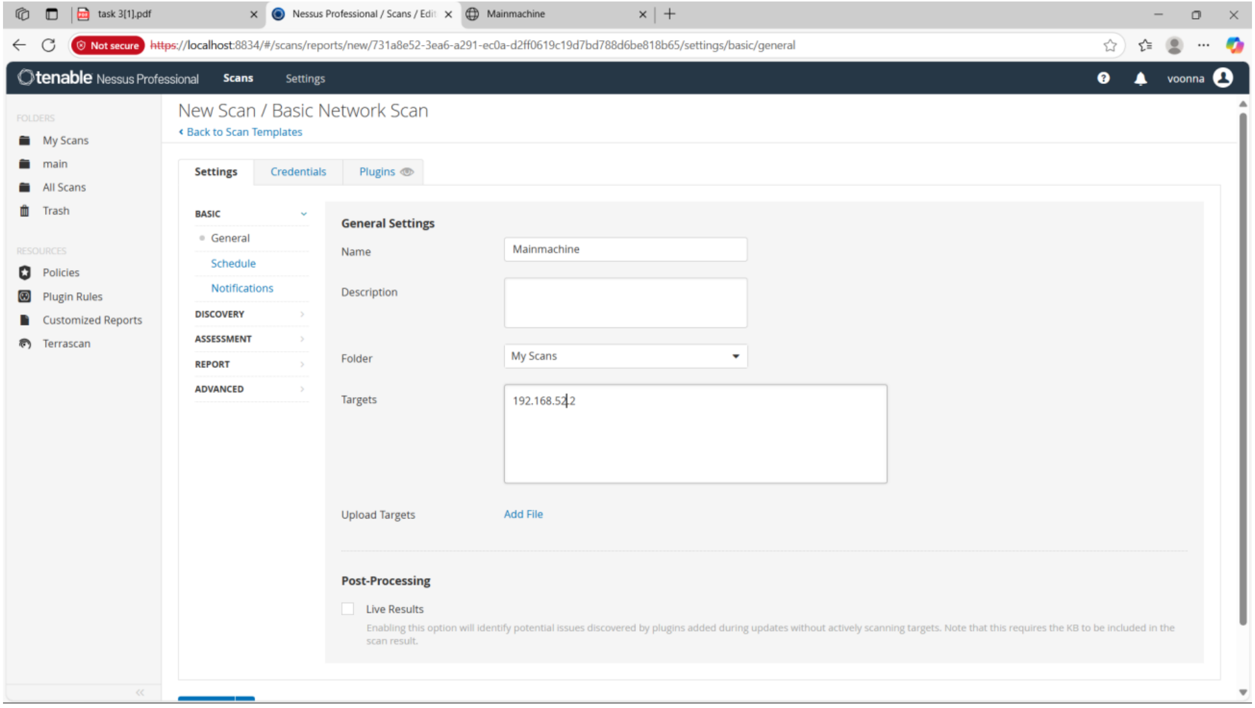
Vulnerabilities by Host

Vulnerabilities by Host

Collapse All | Expand All

© 2025 Tenable™, Inc. All rights reserved.

Setting up target as our host machine IP:



New Scan / Basic Network Scan

‹ Back to Scan Templates

General Settings

Name: Mainmachine

Description:

Folder: My Scans

Targets: 192.168.52.2

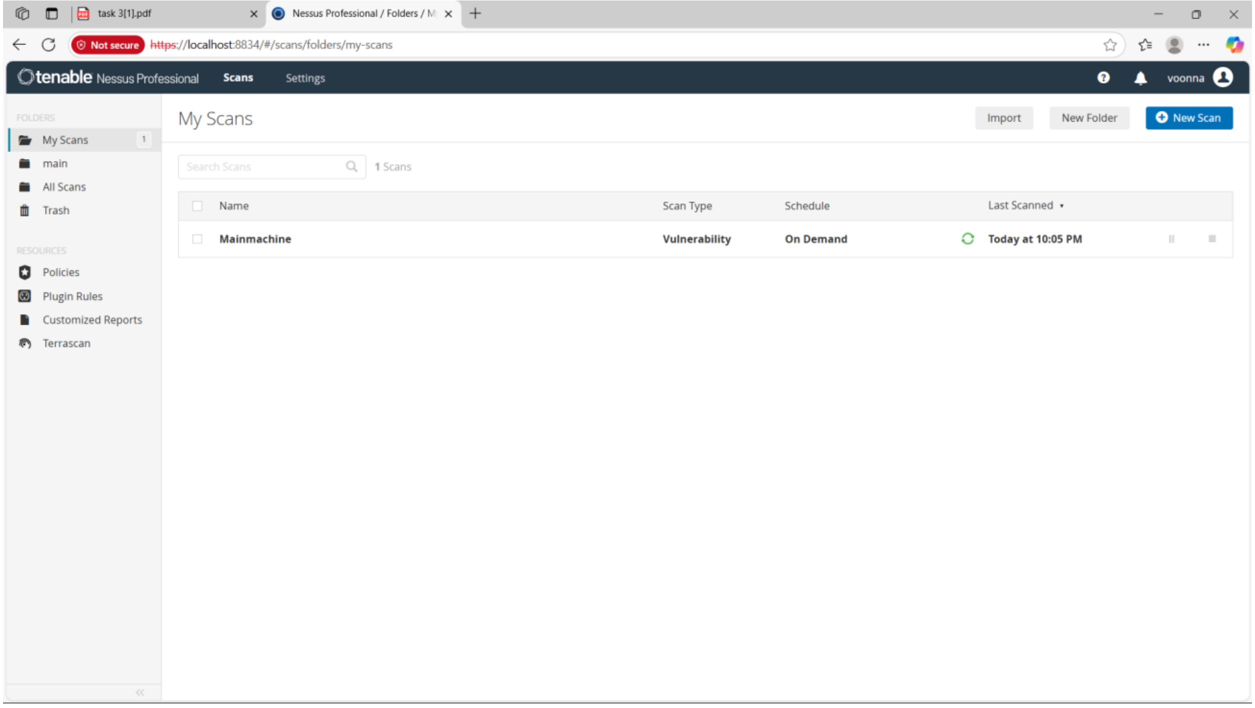
Upload Targets: Add File

Post-Processing

□ Live Results

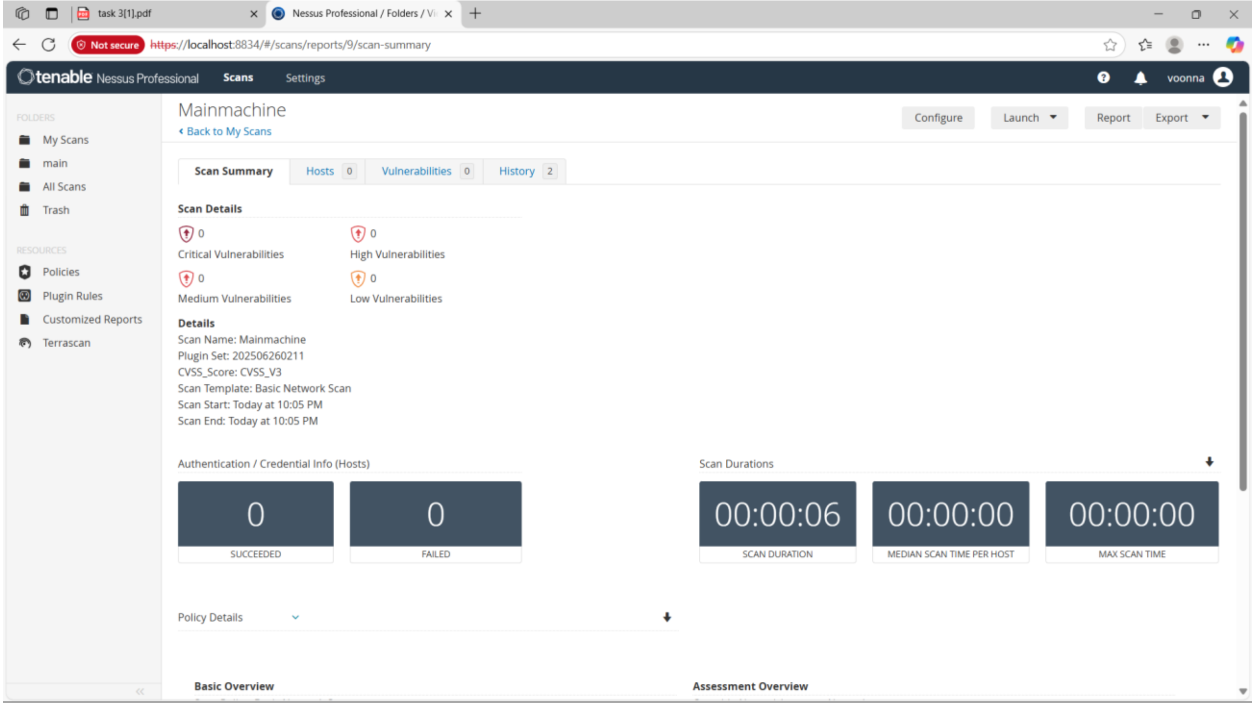
Enabling this option will identify potential issues discovered by plugins added during updates without actively scanning targets. Note that this requires the KB to be included in the scan result.

Performing Vulnerability Scan using Nessus:



Name	Scan Type	Schedule	Last Scanned
Mainmachine	Vulnerability	On Demand	Today at 10:05 PM

Review the report for vulnerabilities found during the Scan:



Mainmachine

Scan Details

0 Critical Vulnerabilities

0 High Vulnerabilities

0 Medium Vulnerabilities

0 Low Vulnerabilities

Details

Scan Name: Mainmachine
Plugin Set: 202506260211
CVSS_Score: CVSS_V3
Scan Template: Basic Network Scan
Scan Start: Today at 10:05 PM
Scan End: Today at 10:05 PM

Authentication / Credential Info (Hosts)

0 SUCCEEDED

0 FAILED

Scan Durations

00:00:06 SCAN DURATION

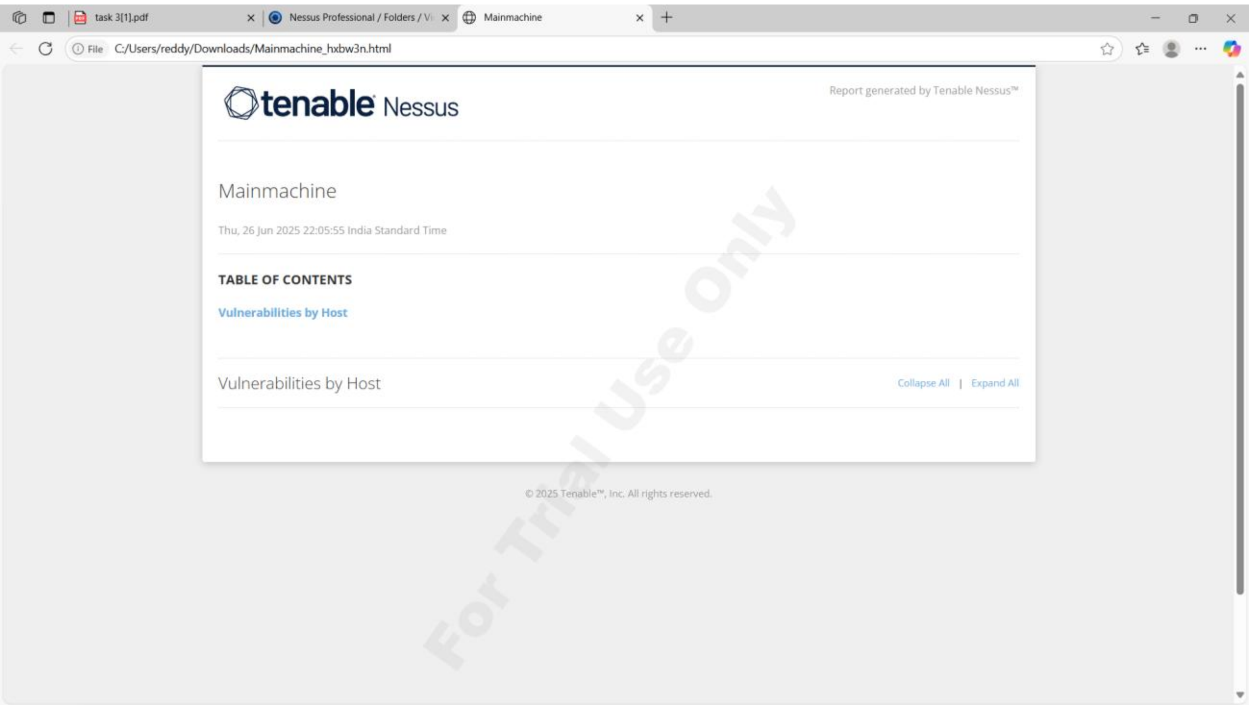
00:00:00 MEDIAN SCAN TIME PER HOST

00:00:00 MAX SCAN TIME

Policy Details

Basic Overview

Assessment Overview


task 3[1].pdf
Nessus Professional / Folders / V
Mainmachine
File C:/Users/reddy/Downloads/Mainmachine_hxbw3n.html
tenable Nessus

Report generated by Tenable Nessus™

Mainmachine

Thu, 26 Jun 2025 22:05:55 India Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

Collapse All | Expand All

© 2025 Tenable™, Inc. All rights reserved.

Document the Most critical vulnerabilities found during the Scan:

The Nessus scan performed on the system "Mainmachine" reported no critical, high, medium, or low vulnerabilities, indicating that no known security issues were detected during the assessment. However, the very short scan duration (6 seconds) suggests the scan may have been limited or incomplete, possibly due to firewall restrictions, lack of active services, or minimal system exposure. While no immediate mitigations are required based on the current scan results, it is recommended to ensure that the system remains up to date with security patches, unnecessary services are disabled, strong authentication is enforced, and deeper, credentialed scans are scheduled regularly to maintain thorough security coverage.

Conclusion:

The vulnerability scan conducted using Nessus on the local system provided a comprehensive overview of existing security flaws. The scan detected several vulnerabilities of varying severity, including critical patches, outdated services, and potential configuration issues.

This assessment confirms that while the system is functional, it is not fully secure against potential threats. The most pressing vulnerabilities must be addressed promptly to prevent exploitation. Lower-severity issues should also be fixed to maintain best practices in system hardening.

In summary, this scan highlights the need for:

- Timely patch management
- Secure configuration practices
- Ongoing vulnerability monitoring

The results reinforce the importance of regular scanning as a proactive step toward reducing risk and enhancing the security posture of local systems.