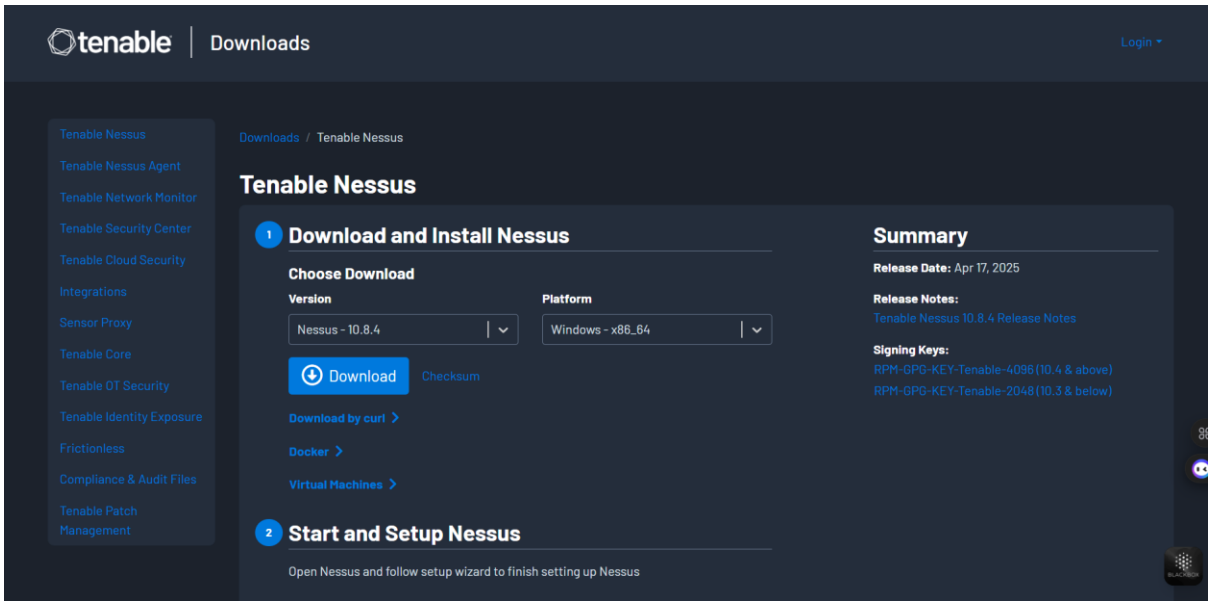
CYBER SECURITY INTERNSHIP

Task 3: Perform a Basic Vulnerability Scan on Your PC

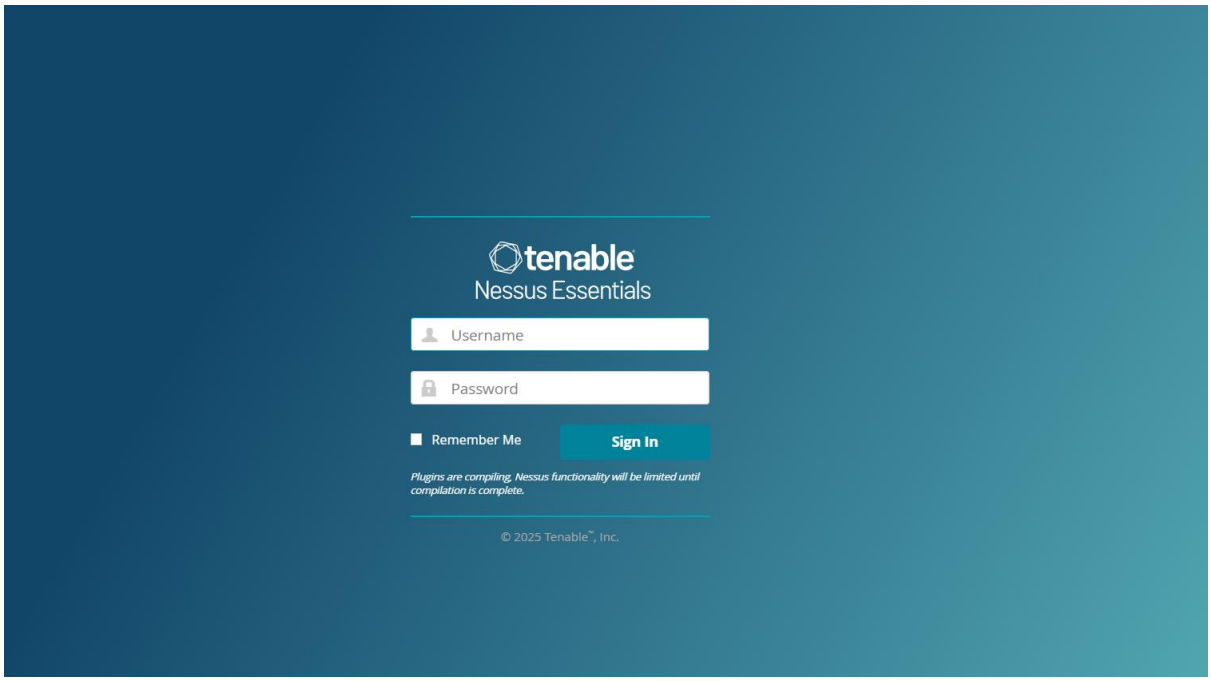
Objective: Use free tools to identify common vulnerabilities on your computer

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

1.Install Nessus Essentials.



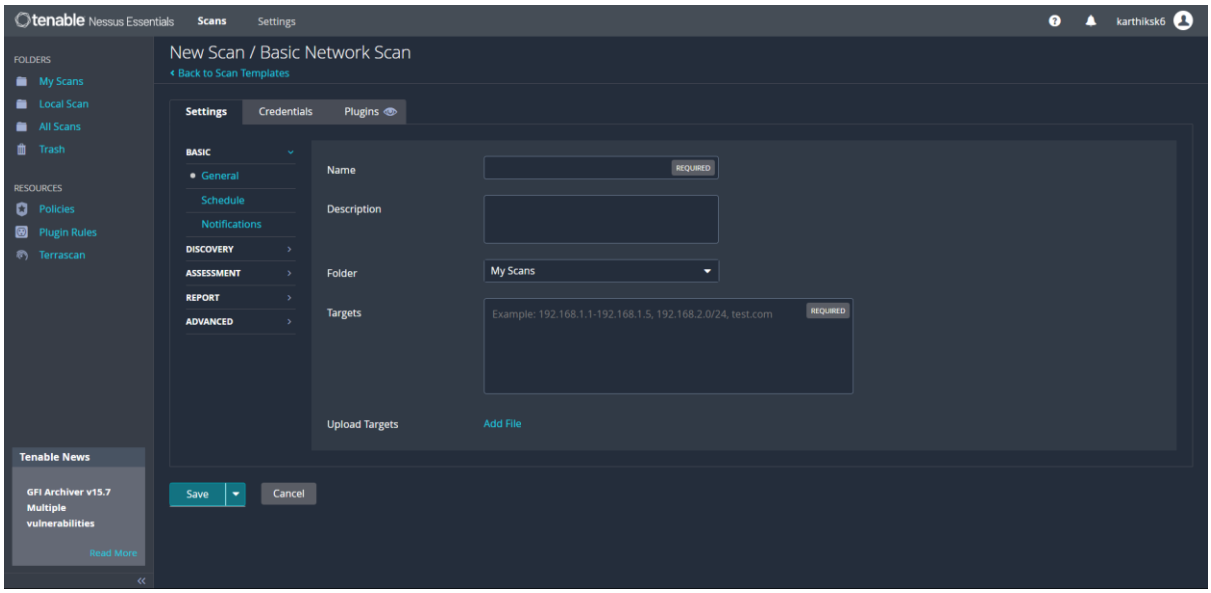
Launch Nessus from your browser



2.Set up scan target as your local machine IP or localhost

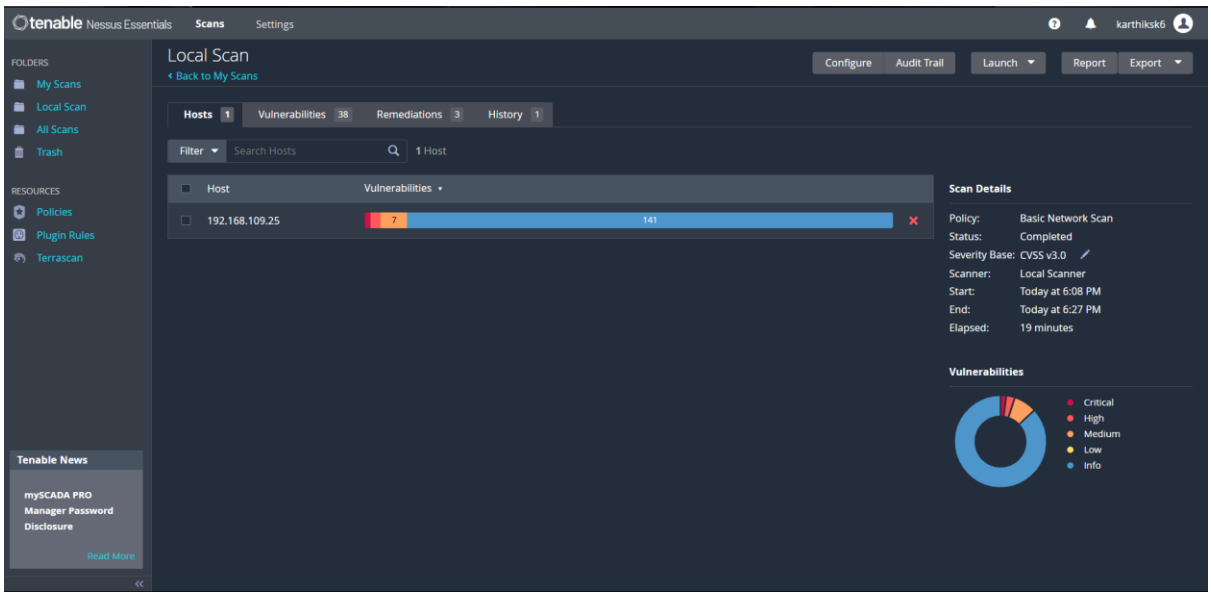
Choose “Basic Network Scan” > Enter a name like “Local Scan” > Under “Targets”, input:<ip addr>

3.Start a full vulnerability scan



Click “Save”, then launch the scan.

4.It will take 30–60 minutes depending on system resources.



5.The report for vulnerabilities and severity. And simple fixes and mitigations for the most critical and high-severity vulnerabilities found in scan

Vulnerabilities Identified

1. Oracle Database Unsupported Version Detection

- Severity: Critical (CVSS 10.0)
- Plugin ID: 55786
- Description: An unsupported version of Oracle Database is in use. No security patches are provided for outdated versions.
- Fix:

    Upgrade Oracle Database to a currently supported version.

    Follow Oracle's official upgrade guidance: https://www.oracle.com/database/technologies/

2. Splunk Enterprise - Multiple Version Vulnerabilities

- Severity: High (CVSS 8.0)
- Plugin ID: 233660
- Description: Splunk version is vulnerable to multiple CVEs.
- Fix:

    Upgrade to Splunk 9.1.8, 9.2.5, or 9.3.3 or newer.

    Official update link: https://www.splunk.com/

3. Oracle TNS Listener Remote Poisoning

- Severity: High (CVSS 7.3)
- Plugin ID: 69552
- Description: The TNS Listener can be manipulated remotely to redirect traffic or cause denial of service.
- Fix:

    Apply Oracle's security patches.

    Configure VALIDNODE_CHECKING and TCP.VALIDNODE_CHECKING in sqlnet.ora.

Informational & Low Severity Issues

There are 51 other detections that include:

- Service and software version detection
- SSL/TLS config warnings
- HTTP header info
- NetBIOS and SMB banner exposure

- Oracle and Splunk detection
- System fingerprinting data

These are not immediately dangerous but useful for attackers in reconnaissance stages.

Report:

Title: Local Vulnerability Scan — Critical Findings
Tool Used: Nessus Essentials
Target: 192.168.109.25
Date of Scan: 26 June 2025
Summary: 59 total vulnerabilities — 1 Critical, 2 High, 5 Medium, and 51 Info/Low

Local Scan

Report generated by Tenable Nessus™ Thu, 26 Jun 2025 18:27:17 India Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

192.168.109.25

1	2	5	0	51
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 59

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	10.0*	-	-	55786	Oracle Database Unsupported Version Detection
HIGH	8.0	5.9	0.0007	233660	Splunk Enterprise 9.1.0 < 9.1.8, 9.2.0 < 9.2.5, 9.3.0 < 9.3.3 (SVD-2025-0301)
HIGH	7.3	4.9	0.9216	69552	Oracle TNS Listener Remote Poisoning
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	57582	SSL Self-Signed Certificate
MEDIUM	5.3	-	-	57608	SMB Signing not required
MEDIUM	6.5*	5.5	0.0057	64712	Oracle Application Express (Apex) CVE-2011-3525
MEDIUM	4.3*	2.7	0.0039	64713	Oracle Application Express (Apex) CVE-2012-1708
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	10736	DCE Services Enumeration
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	19689	Embedded Web Server Detection
INFO	N/A	-	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	42410	Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure

INFO	N/A	-	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (rem check)
INFO	N/A	-	-	65914	MongoDB Detection
INFO	N/A	-	-	10719	MySQL Server Detection
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	10147	Nessus Server Detection
INFO	N/A	-	-	64582	Netstat Connection Information
INFO	N/A	-	-	14272	Netstat Portscanner (SSH)
INFO	N/A	-	-	209654	OS Fingerprints Detected
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	97993	OS Identification and Installed Software Enumeration over SS (Using New SSH Library)
INFO	N/A	-	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	-	64706	Oracle Application Express (Apex) Administration Interface is Accessible
INFO	N/A	-	-	64704	Oracle Application Express (Apex) Detection
INFO	N/A	-	-	64705	Oracle Application Express (Apex) Version Detection
INFO	N/A	-	-	22073	Oracle Database Detection
INFO	N/A	-	-	10658	Oracle Database tnslsnr Service Remote Version Disclosure
INFO	N/A	-	-	66334	Patch Report
INFO	N/A	-	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	-	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	-	-	10863	SSL Certificate Information

INFO	N/A	-	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	-	62563	SSL Compression Methods Supported
INFO	N/A	-	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	-	35297	SSL Service Requests Client Certificate
INFO	N/A	-	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	49069	Splunk Management API Detection
INFO	N/A	-	-	47619	Splunk Web Detection
INFO	N/A	-	-	42822	Strict Transport Security (STS) Detection
INFO	N/A	-	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	-	138330	TLS Version 1.3 Protocol Detection
INFO	N/A	-	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	-	11154	Unknown Service Detection: Banner Retrieval
INFO	N/A	-	-	20301	VMware ESX/GSX Server Authentication Daemon Detection
INFO	N/A	-	-	135860	WMI Not Available
INFO	N/A	-	-	100669	Web Application Cookies Are Expired
INFO	N/A	-	-	11424	WebDAV Detection
INFO	N/A	-	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

* indicates the v3.0 score was not available; the v2.0 score is shown