Plugin Functionality Analysis: Plugin Workflow:

Initialization: Plugins activate based on scan configurations like target selection and scan types.

Discovery: Nessus identifies active hosts, open ports, and services on the network.

Execution: Plugins execute vulnerability checks, compliance audits, etc., against discovered services.

Identification: Plugins scan for known vulnerabilities, misconfigurations, and threats using signature databases.

Scripting & Custom Checks: Some plugins support custom scripts for specific checks or configurations.

Exploitability Testing: Certain plugins simulate attacks to confirm vulnerability severity.

Protocol-Specific Scans: Plugins detect vulnerabilities unique to various protocols (HTTP, SMTP, etc.).

Reporting: Identified vulnerabilities are compiled into reports with details and recommended fixes.

Feature Examination:

Scripting: Assess plugins allowing custom script creation for tailored checks.

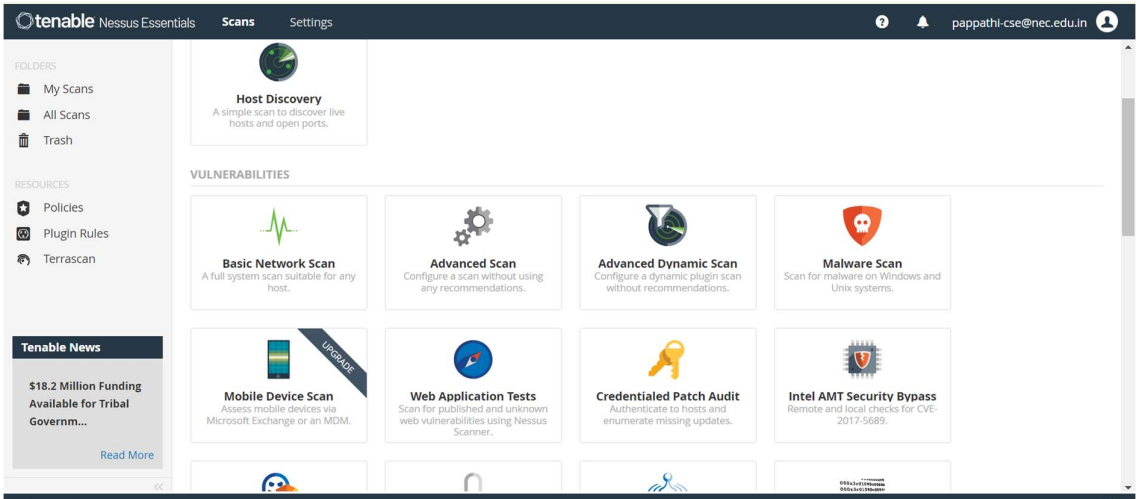
Exploitability Checks: Explore plugins simulating attacks to confirm and measure potential risks.

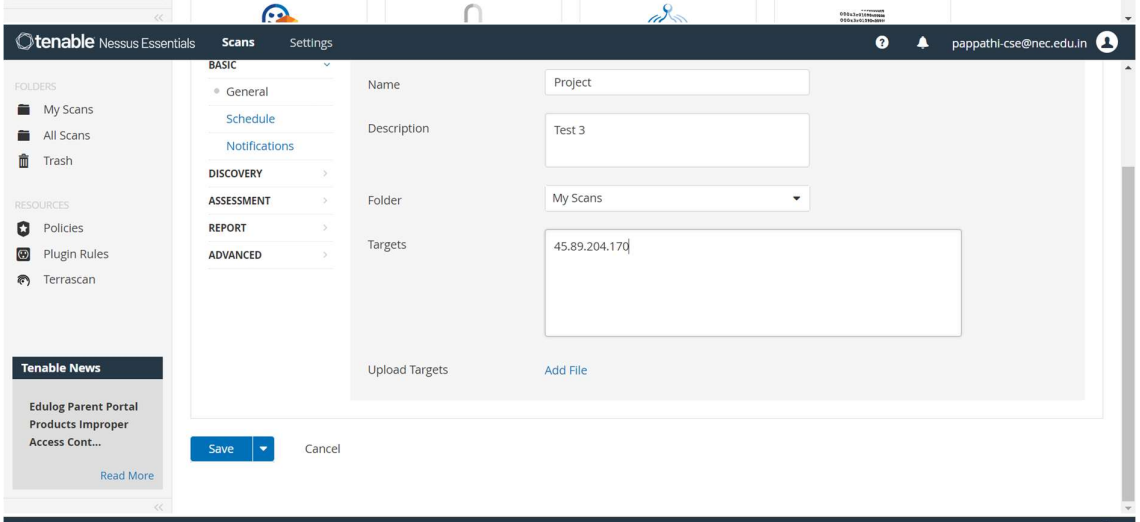
Protocol-Specific Detection: Review plugins targeting vulnerabilities specific to particular protocols.

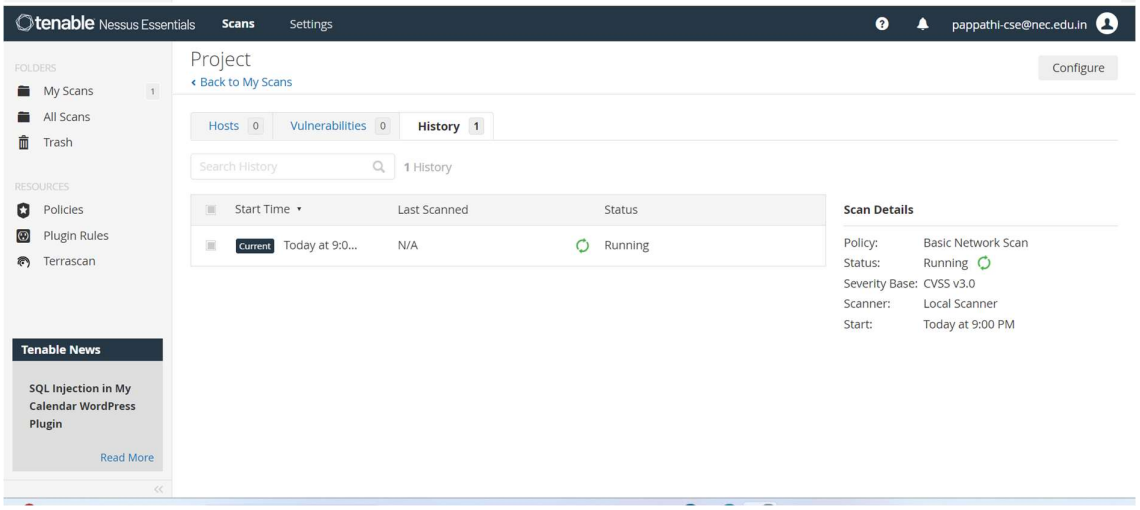
Deep Scans: Evaluate plugins offering extensive system-level or privileged-access scans.

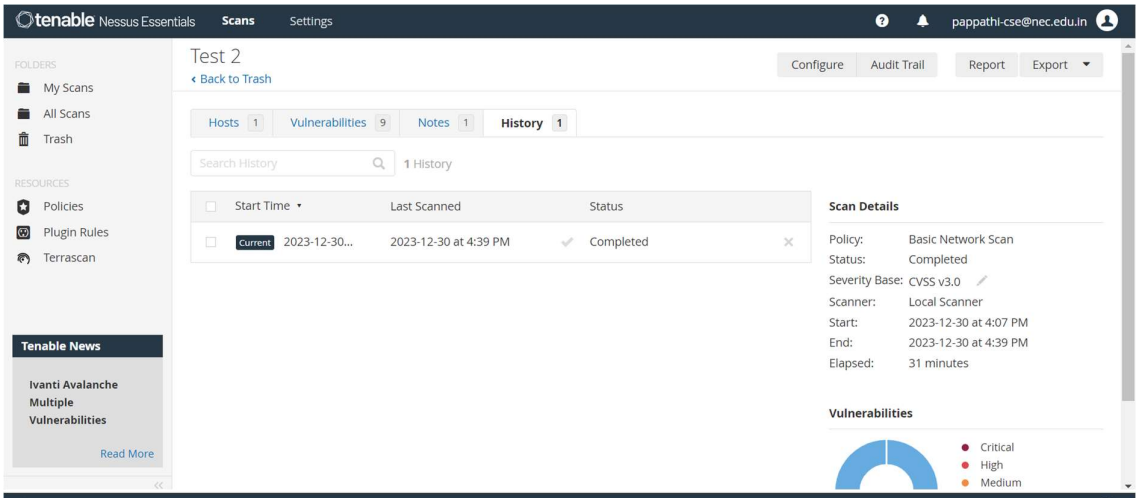
Custom Policies: Analyze plugins allowing custom risk scoring or compliance settings.

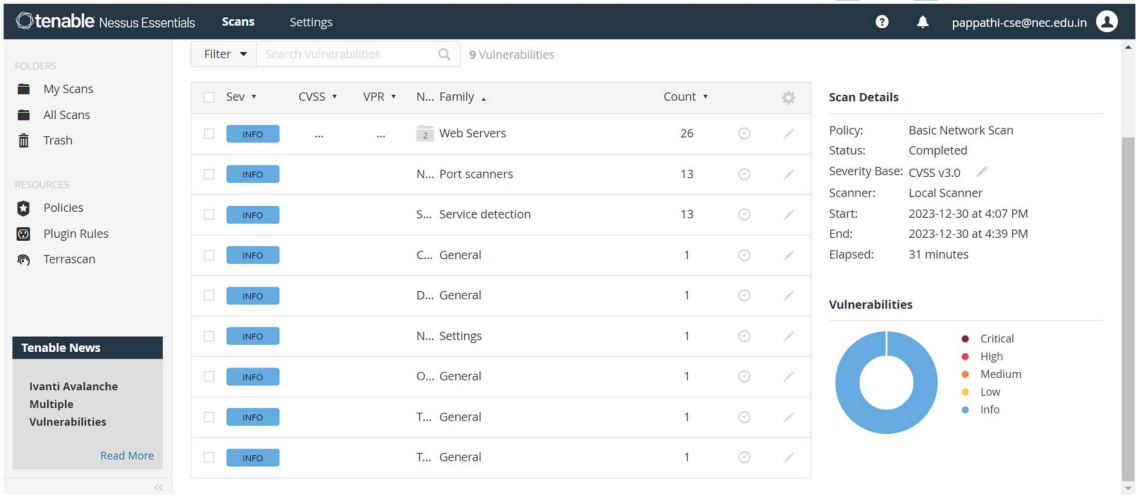
CVE/CPE Integration: Plugins leveraging CVE/CPE databases for accurate vulnerability identification.


tenable Nessus Essentials
Scans
Settings
pappathi-cse@nec.edu.in
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
$18.2 Million Funding Available for Tribal Governm...
Read More
Host Discovery
A simple scan to discover live hosts and open ports.
VULNERABILITIES
Basic Network Scan
A full system scan suitable for any host.
Advanced Scan
Configure a scan without using any recommendations.
Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.
Malware Scan
Scan for malware on Windows and Unix systems.
UPGRADE
Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.
Web Application Tests
Scan for published and unknown web vulnerabilities using Nessus Scanner.
Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.
Intel AMT Security Bypass
Remote and local checks for CVE-2017-5689.


tenable Nessus Essentials
Scans
Settings
pappathi-cse@nec.edu.in
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Edulog Parent Portal Products Improper Access Cont...
Read More
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
Project
Description
Test 3
Folder
My Scans
Targets
45.89.204.170
Upload Targets
Add File
Save
Cancel


tenable Nessus Essentials
Scans
Settings
pappathi-cse@nec.edu.in
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
SQL Injection in My Calendar WordPress Plugin
Read More
Project
Back to My Scans
Configure
Hosts 0
Vulnerabilities 0
History 1
Search History
1 History
Start Time
Last Scanned
Status
Current
Today at 9:0...
N/A
Running
Scan Details
Policy: Basic Network Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 9:00 PM


tenable Nessus Essentials
Scans
Settings
pappathi-cse@nec.edu.in
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Ivanti Avalanche Multiple Vulnerabilities
Read More
Test 2
Back to Trash
Configure
Audit Trail
Report
Export
Hosts 1
Vulnerabilities 9
Notes 1
History 1
Search History
1 History
Start Time
Last Scanned
Status
Current
2023-12-30...
2023-12-30 at 4:39 PM
Completed
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: 2023-12-30 at 4:07 PM
End: 2023-12-30 at 4:39 PM
Elapsed: 31 minutes
Vulnerabilities
Critical
High
Medium


tenable Nessus Essentials
Scans
Settings
pappathi-cse@nec.edu.in
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Ivanti Avalanche Multiple Vulnerabilities
Read More
Filter
Search Vulnerabilities
9 Vulnerabilities
Sev
CVSS
VPR
N...
Family
Count
INFO ... ... 2 Web Servers 26
INFO N... Port scanners 13
INFO S... Service detection 13
INFO C... General 1
INFO D... General 1
INFO N... Settings 1
INFO O... General 1
INFO T... General 1
INFO T... General 1
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: 2023-12-30 at 4:07 PM
End: 2023-12-30 at 4:39 PM
Elapsed: 31 minutes
Vulnerabilities
Critical
High
Medium
Low
Info