Procedures for Vulnerability Assessment (Windows Only)

Project: Vulnerability Assessment using Tenable Nessus Essentials
Student Name: Oswald Eyram Toku
Instructor: Dr. Noah Darko-Adjei
Date: 10th November 2025

1. Introduction

This document outlines the practical steps used to perform a vulnerability assessment using Tenable Nessus Essentials on a Windows system. It includes installation, software integrity verification, network and host scans, custom scan policy configuration, and exporting scan results.

2. System Requirements (Windows)

Requirement	Description
Operating System	Windows 10 / 11
Permissions	Administrator's rights required
Network Access	Internet connection required for plugin updates
Browser	Chrome, Edge, or Firefox

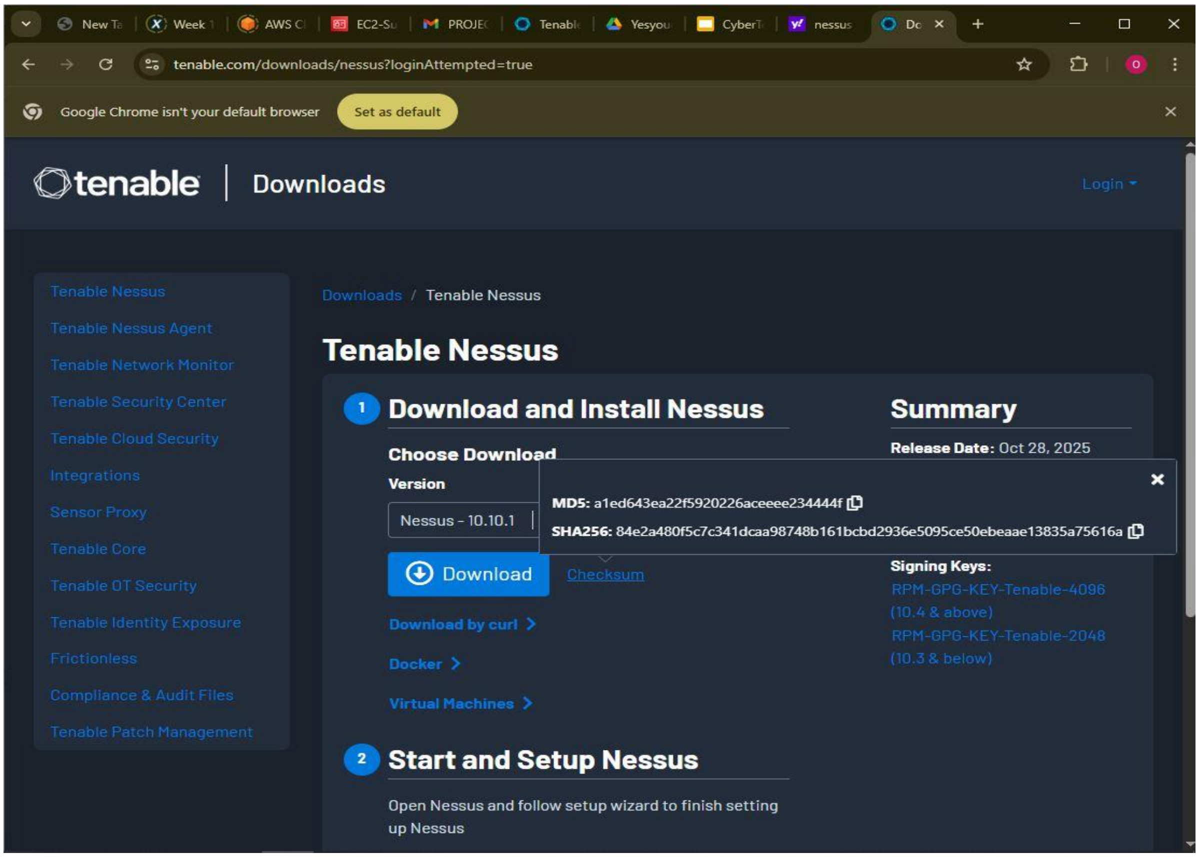
3. Installing Nessus Essentials (Windows)

1. 1. Visit the official Nessus Essentials download page.
2. 2. Download the Windows Installer (exe).
3. 3. Locate the installer in the Downloads folder.
4. 4. Double-click the installer to begin setup.
5. 5. Accept the license agreement and proceed with default installation settings.
6. 6. Once installation is completed, Nessus will automatically start.
7. 7. Open a browser and enter: https://localhost:8834
8. 8. Select Nessus Essentials, enter activation code, and allow plugin download to complete.

4. Verifying Installer Integrity (MD5 Hash)

Purpose: To confirm the downloaded Nessus installer has not been altered or corrupted by comparing the installer's MD5 hash with the official MD5 provided by Tenable.

Steps:
1. I Obtained the official MD5 hash of the installer from the Tenable download page. This is shown in Figure 1.1 below.


New Ta
Week 1
AWS C
EC2-Su
PROJEC
Tenabl
Yesyou
CyberT
nessus
Do
tenable.com/downloads/nessus?loginAttempted=true
Google Chrome isn't your default browser
Set as default
tenable
Login

Downloads

Tenable Nessus
Tenable Nessus Agent
Tenable Network Monitor
Tenable Security Center
Tenable Cloud Security
Integrations
Sensor Proxy
Tenable Core
Tenable OT Security
Tenable Identity Exposure
Frictionless
Compliance & Audit Files
Tenable Patch Management

Downloads / Tenable Nessus

Tenable Nessus

1 Download and Install Nessus

Choose Download

Version

Nessus - 10.10.1

Download

Checksum

MD5: a1ed643ea22f5920226aceeee234444f

SHA256: 84e2a480f5c7c341dcaa98748b161bcbd2936e5095ce50ebeaae13835a75616a

Download by curl >

Docker >

Virtual Machines >

Summary

Release Date: Oct 28, 2025

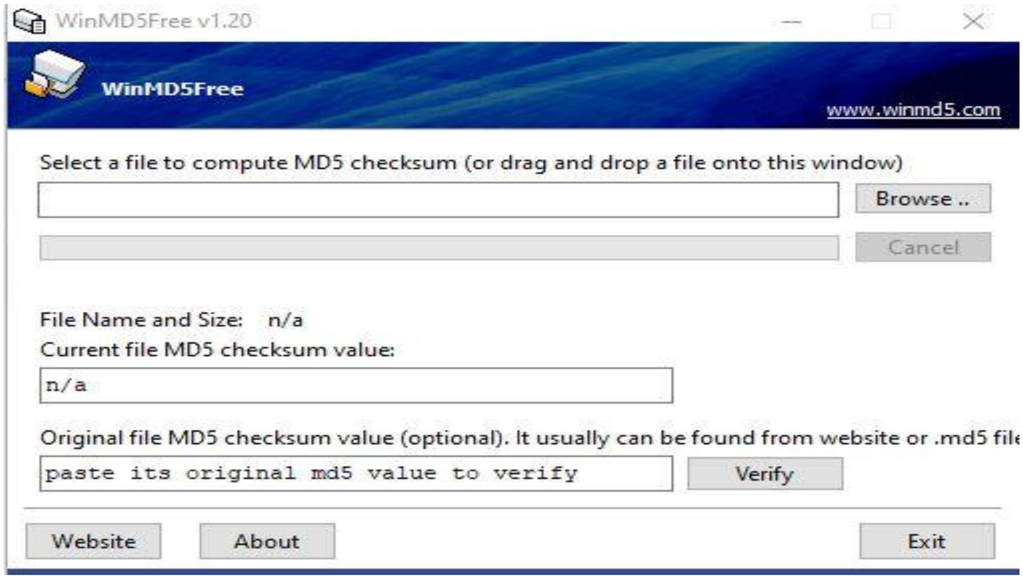
Signing Keys:
RPM-GPG-KEY-Tenable-4096 (10.4 & above)
RPM-GPG-KEY-Tenable-2048 (10.3 & below)

2 Start and Setup Nessus

Open Nessus and follow setup wizard to finish setting up Nessus

Figure 1.1

2. Then I located winMD5 on my pc and I launched I. As shown in Figure 1.2 below.



Select a file to compute MD5 checksum (or drag and drop a file onto this window)

File Name and Size: n/a

Current file MD5 checksum value:

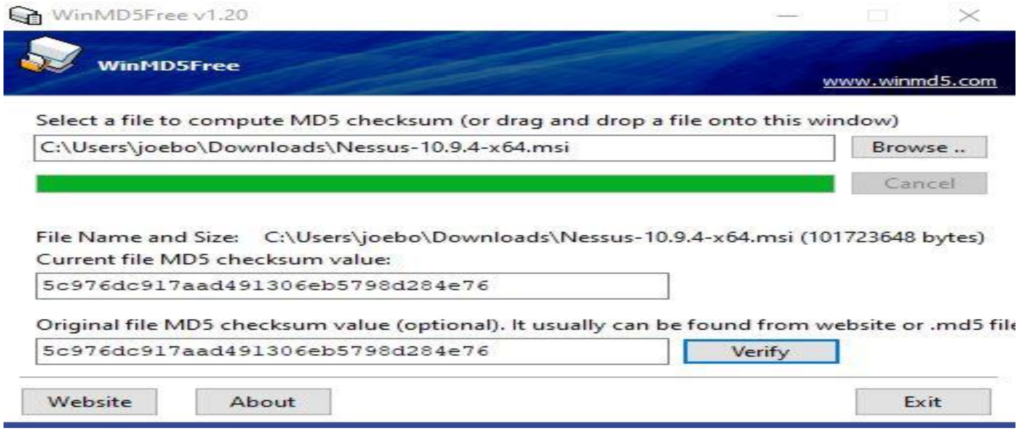
n/a

Original file MD5 checksum value (optional). It usually can be found from website or .md5 file

paste its original md5 value to verify

Figure 1.2

3. In the WinMD5 GUI, I Pasted the original hash function in the section designated for it. And this is shown below in Figure 1.3



Select a file to compute MD5 checksum (or drag and drop a file onto this window)

C:\Users\joebo\Downloads\Nessus-10.9.4-x64.msi

File Name and Size: C:\Users\joebo\Downloads\Nessus-10.9.4-x64.msi (101723648 bytes)

Current file MD5 checksum value:

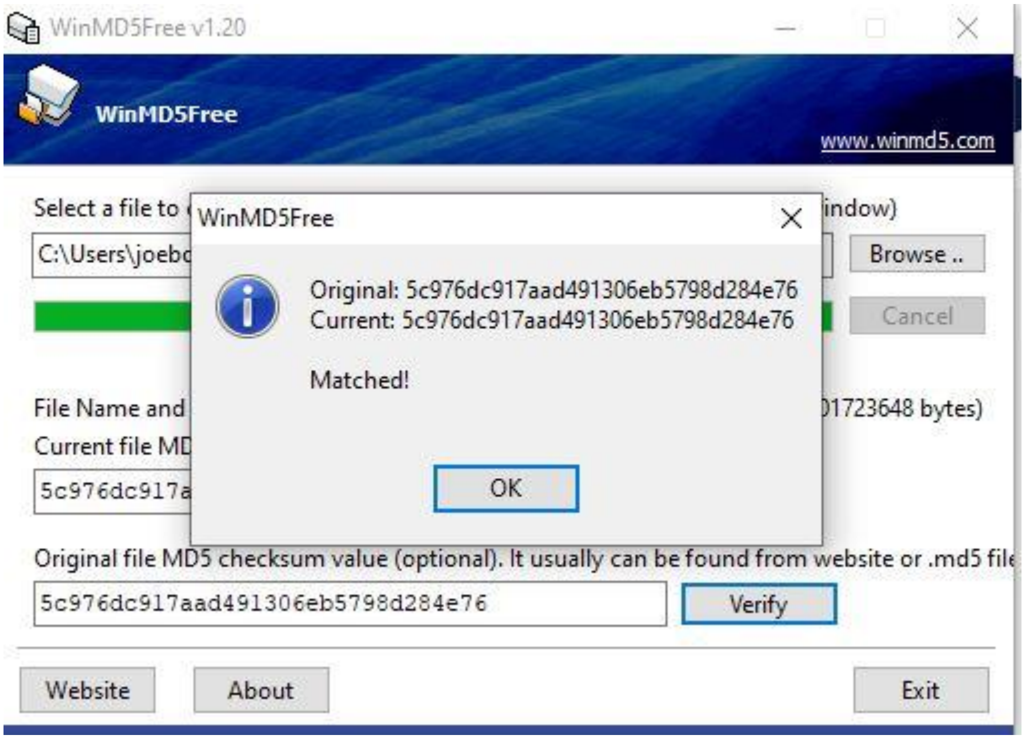
5c976dc917aad491306eb5798d284e76

Original file MD5 checksum value (optional). It usually can be found from website or .md5 fil

5c976dc917aad491306eb5798d284e76

Figure 1.3

4. Then I selected newly installed file of Nessus Essentials and proceeded to verify. The result was a match indicating that there was no comprise. This is shown below in Figure 1.4.



Select a file to ... indow)

C:\Users\joebo

File Name and ...)1723648 bytes)

Current file MD

5c976dc917a

Original: 5c976dc917aad491306eb5798d284e76
Current: 5c976dc917aad491306eb5798d284e76

Matched!

Original file MD5 checksum value (optional). It usually can be found from website or .md5 fil

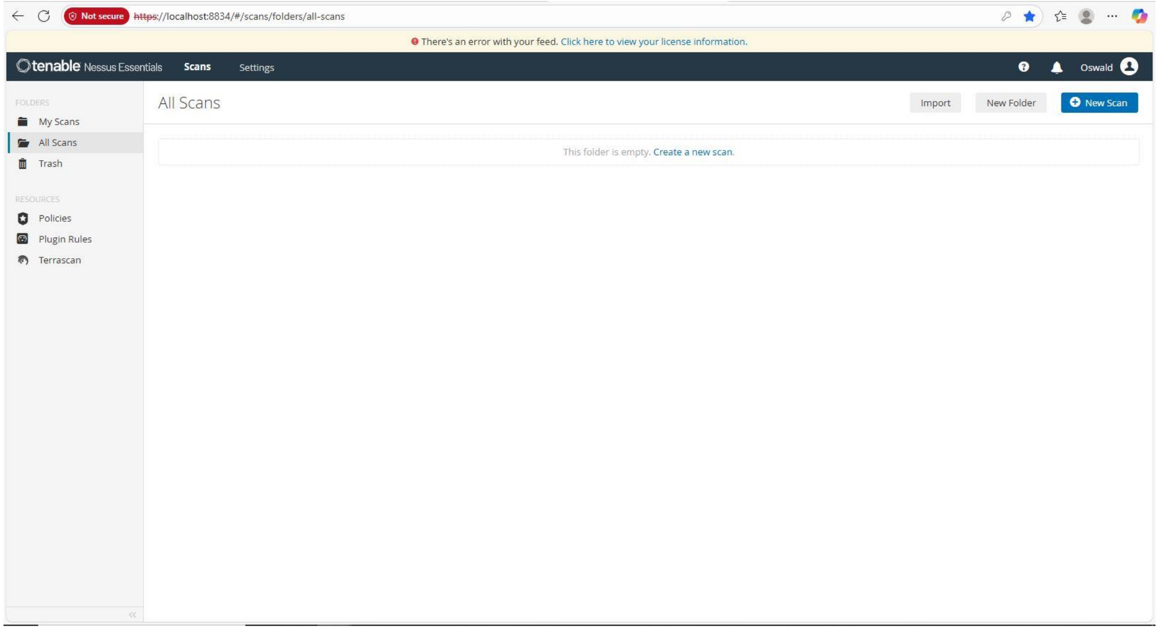
5c976dc917aad491306eb5798d284e76

Figure 1.4

5. Network Scan Procedure

The purpose of performing a network scan is to identify all active devices, open ports, running services, and potential vulnerabilities across the network. This helps in understanding the overall security posture of the network environment before performing more targeted or host-level assessments. The network scan provides visibility into what systems are present, how they communicate, and whether any exposed services or configurations may be exploited by attackers. By discovering these systems and services, the organization can proactively secure weak points, reduce attack surface, and prioritize remediation based on risk.

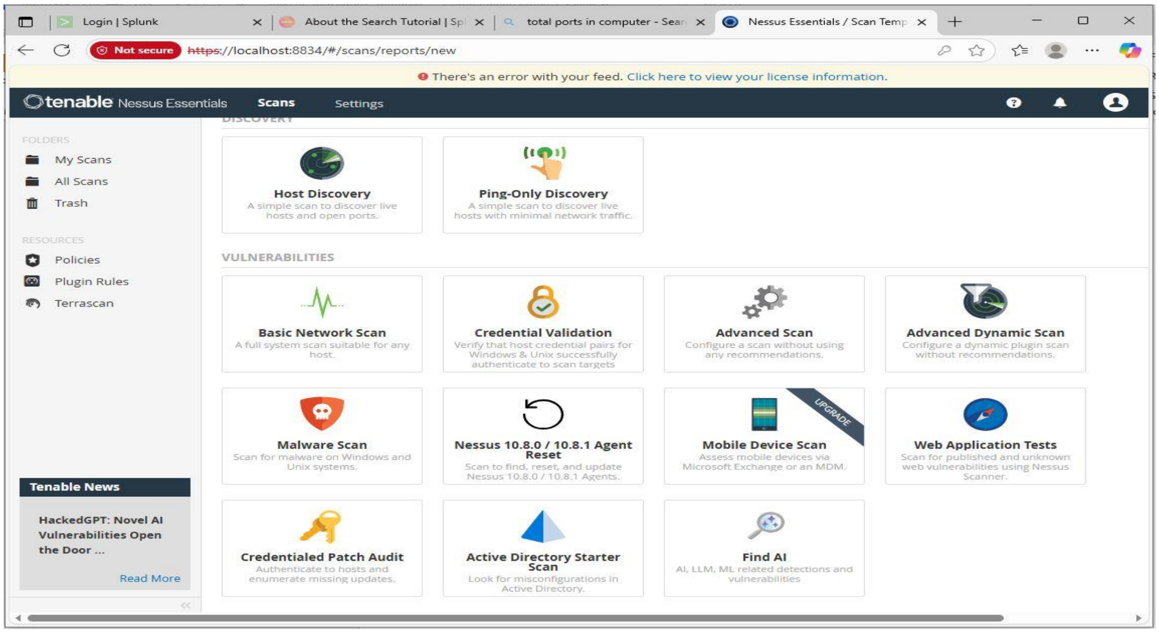
1. Open Nessus Web UI: https://localhost:8834. This is shown below in Figure 2.1.
2. Select new scan and among the options select basic network scan. As shown below in Figure 2.2
3. In basic network scan window, provide a name and description for the scan. This is shown below in Figure 2.3.
4. In Targets, enter your network range (example: 192.[redacted]). As shown below in Figure 2.3
5. Navigate to Settings →Discovery → Enumeration, change to Custom. As shown below in Figure 2.4
6. Save and navigate to My scans and launch the newly configured network scan. This is shown below in Figure 2.5
7. You select the basic network scan result then you navigate to report and the format you want the report to be generated in. In my case I selected CSV and in CSV window you select your preferred requirement, and you proceed to generate the report. This is shown below in Figure 2.6



There's an error with your feed. Click here to view your license information.

This folder is empty. Create a new scan.

Figure 2.1


Login | Splunk
About the Search Tutorial | Sp
total ports in computer - Sear
Nessus Essentials / Scan Temp
Not secure
https://localhost:8834/#/scans/reports/new
tenable Nessus Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
UPGRADE

There's an error with your feed. Click here to view your license information.

DISCOVERY

Host Discovery A simple scan to discover live hosts and open ports.

Ping-Only Discovery A simple scan to discover live hosts with minimal network traffic.

VULNERABILITIES

Basic Network Scan A full system scan suitable for any host.

Credential Validation Verify that host credential pairs for Windows & Unix successfully authenticate to scan targets

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.

Nessus 10.8.0 / 10.8.1 Agent Reset Scan to find, reset, and update Nessus 10.8.0 / 10.8.1 Agents.

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.

Active Directory Starter Scan Look for misconfigurations in Active Directory.

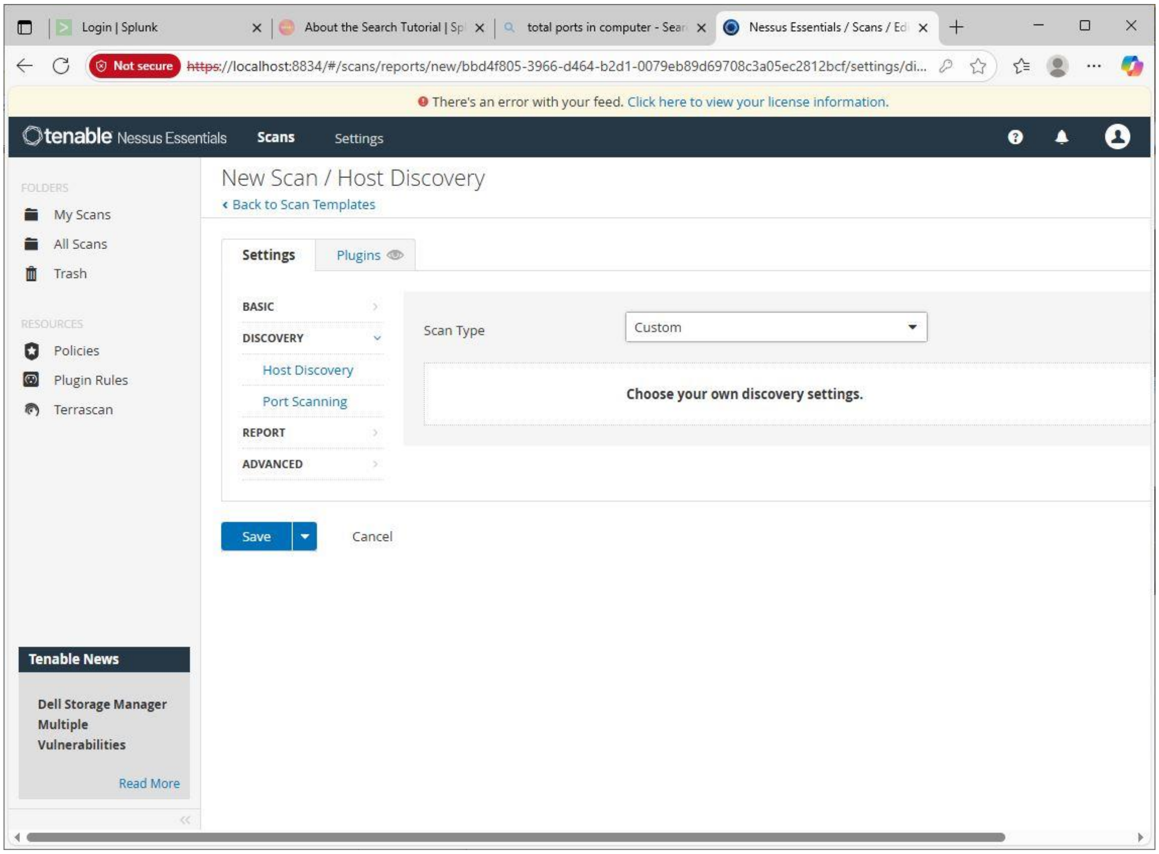
Find AI AI, LLM, ML related detections and vulnerabilities

Tenable News

HackedGPT: Novel AI Vulnerabilities Open the Door ...

Read More

Figure 2.2


Login | Splunk
About the Search Tutorial | Spl
total ports in computer - Sear
Nessus Essentials / Scans / Ed
Not secure
https://localhost:8834/#/scans/reports/new/bbd4f805-3966-d464-b2d1-0079eb89d69708c3a05ec2812bcf/settings/di...
There's an error with your feed. Click here to view your license information.
tenable Nessus Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Dell Storage Manager Multiple Vulnerabilities
Read More
Settings
Plugins
BASIC
DISCOVERY
Host Discovery
Port Scanning
REPORT
ADVANCED
Save
Cancel

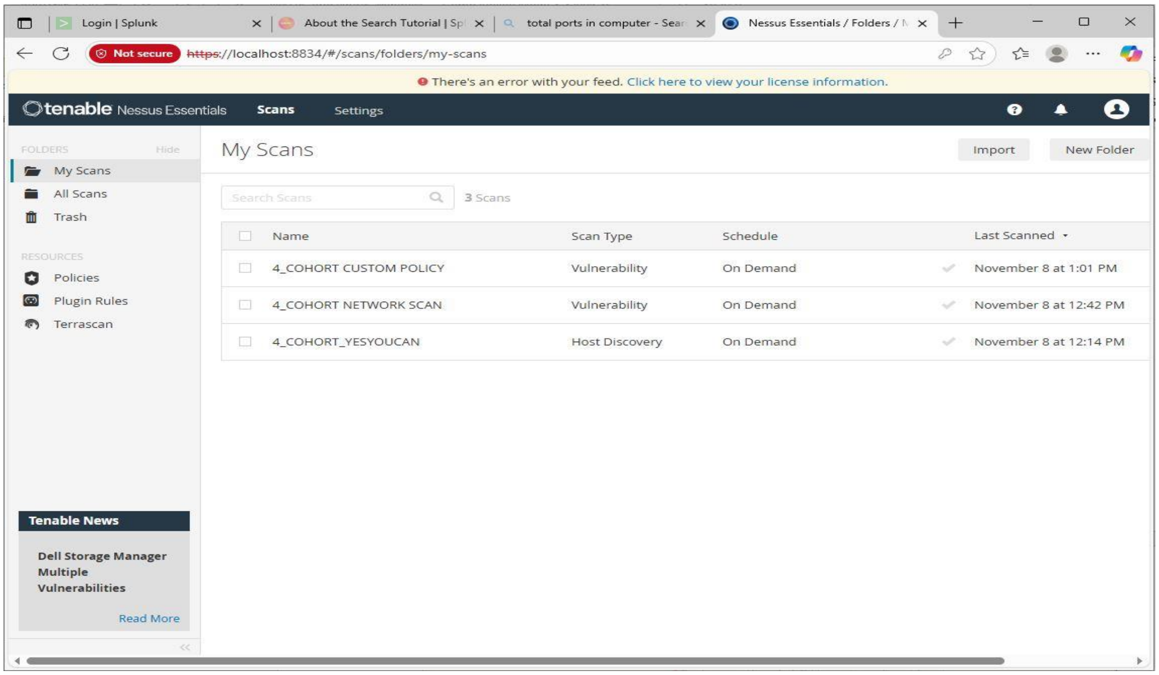
New Scan / Host Discovery

‹ Back to Scan Templates

Scan Type: Custom

Choose your own discovery settings.

Figure 2.4

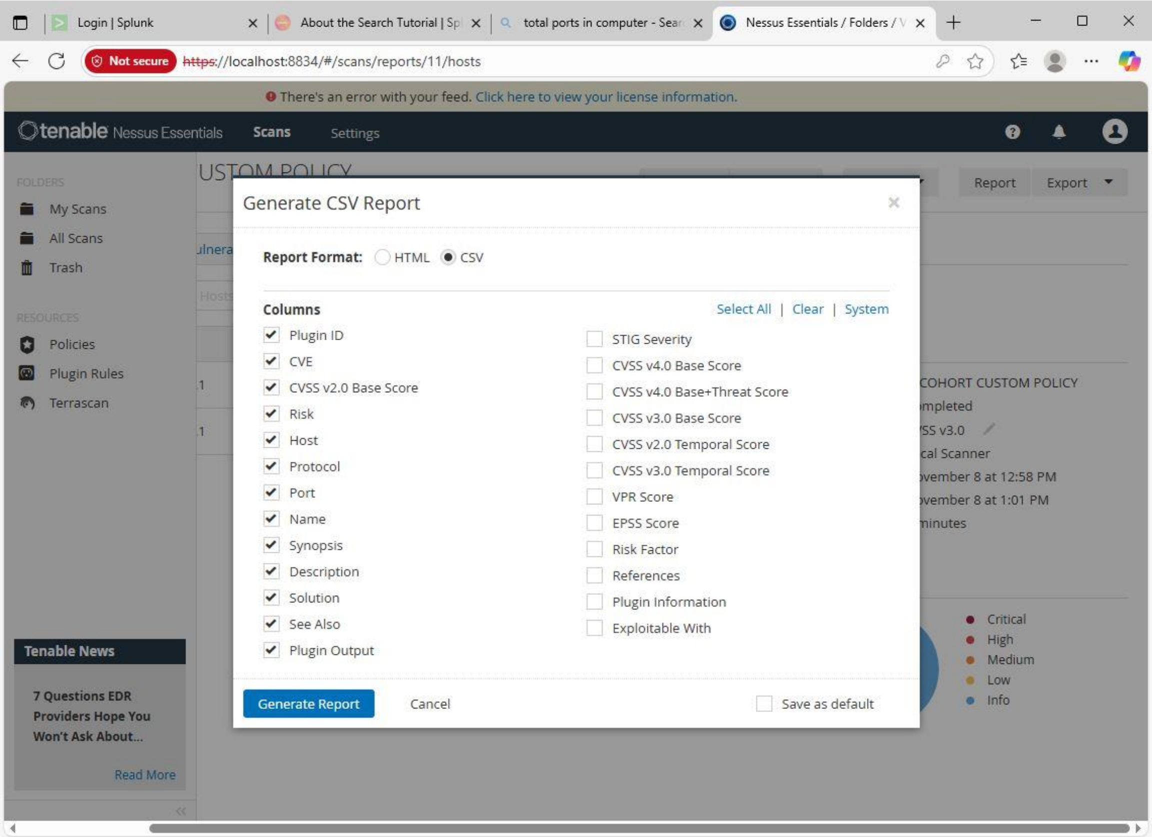

Login | Splunk
About the Search Tutorial | Spl
total ports in computer - Sear
Nessus Essentials / Folders / M
Not secure
https://localhost:8834/#/scans/folders/my-scans
There's an error with your feed. Click here to view your license information.
tenable Nessus Essentials
Scans
Settings
FOLDERS
Hide
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Dell Storage Manager Multiple Vulnerabilities
Read More
Import
New Folder
Search Scans

My Scans

3 Scans

Name	Scan Type	Schedule	Last Scanned
4_COHORT CUSTOM POLICY	Vulnerability	On Demand	✓ November 8 at 1:01 PM
4_COHORT NETWORK SCAN	Vulnerability	On Demand	✓ November 8 at 12:42 PM
4_COHORT_YESYOUCAN	Host Discovery	On Demand	✓ November 8 at 12:14 PM

Figure 2.5


Login | Splunk
About the Search Tutorial | Sp
total ports in computer - Sear
Nessus Essentials / Folders / V
Not secure
https://localhost:8834/#/scans/reports/11/hosts
There's an error with your feed. Click here to view your license information.
tenable Nessus Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
7 Questions EDR Providers Hope You Won't Ask About...
Read More
USTOM POLICY
Report
Export
COHORT CUSTOM POLICY
mpleted
SS v3.0
cal Scanner
vember 8 at 12:58 PM
vember 8 at 1:01 PM
minutes
Critical
High
Medium
Low
Info

Generate CSV Report

Report Format: ○ HTML ● CSV

Columns — Select All | Clear | System

☑ Plugin ID	□ STIG Severity
☑ CVE	□ CVSS v4.0 Base Score
☑ CVSS v2.0 Base Score	□ CVSS v4.0 Base+Threat Score
☑ Risk	□ CVSS v3.0 Base Score
☑ Host	□ CVSS v2.0 Temporal Score
☑ Protocol	□ CVSS v3.0 Temporal Score
☑ Port	□ VPR Score
☑ Name	□ EPSS Score
☑ Synopsis	□ Risk Factor
☑ Description	□ References
☑ Solution	□ Plugin Information
☑ See Also	□ Exploitable With
☑ Plugin Output	

Generate Report   Cancel   □ Save as default

Figure 2.6

6. Host Scan Procedure

The purpose of a host scan is to perform a detailed, in-depth assessment of a specific system to identify vulnerabilities, misconfigurations, missing patches, weak services, and security risks present on that individual machine. Unlike a network scan—which provides a broad overview of all devices on the network—a host scan focuses on one system at a deeper level, including its installed applications, running processes, open ports, system registry, patch status, and user account configurations.

This allows security teams to understand the exact weaknesses affecting that system and to prioritize targeted remediation actions based on severity and potential impact.

1. From Nessus homepage, you select new scan and in the new scan option you select Host discovery.
2. Then you follow the same procedures demonstrated in the network scan.

7. Creating a Custom Scan Policy

1. From the Nessus homepage, navigate to the Resources section and select Policies and select new policy. As shown in Figure 3.1

2. Click on Advanced Scan to create a new custom scan policy. This is shown in Figure 3.2

3. Enter a name and description of the policy to identify its purpose. This is shown in Figure 3.3

4. In the Targets field, enter the IP address of the host or network you intend to scan. As shown in Figure 3.4

5. Navigate to the Settings tab and configure the scanning parameters as required (e.g., scan performance, discovery settings, credential settings, and port scanning options)

6. Go to the Plugins tab and enable or disable the plugins you want to include in the scan based on your objectives. As shown in Figure 3.5

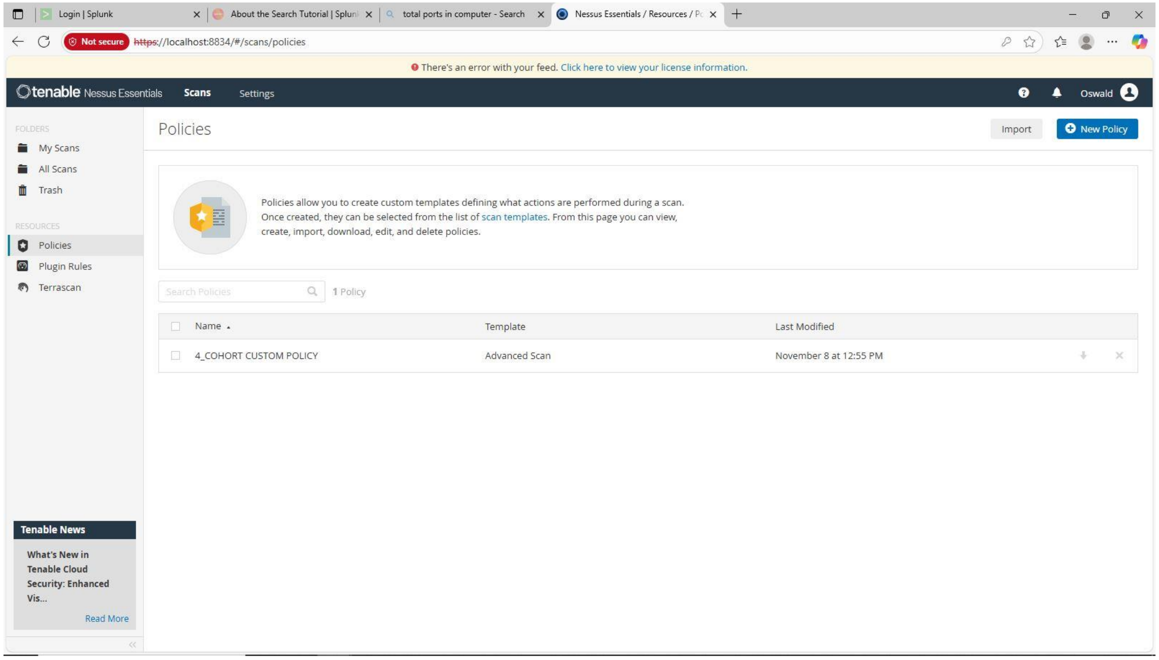
7. Click Save to store the custom policy.

8. To run the scan, go back to My Scans, select the newly created policy, and launch the scan. Refer to chapter five for the rest of the steps.

9. Once the scan is completed, open the scan results and analyze the findings.

10. To export the results, click the Report button, choose the desired format (in this case, CSV), and generate the report.

11. Save the exported CSV report for documentation and analysis.

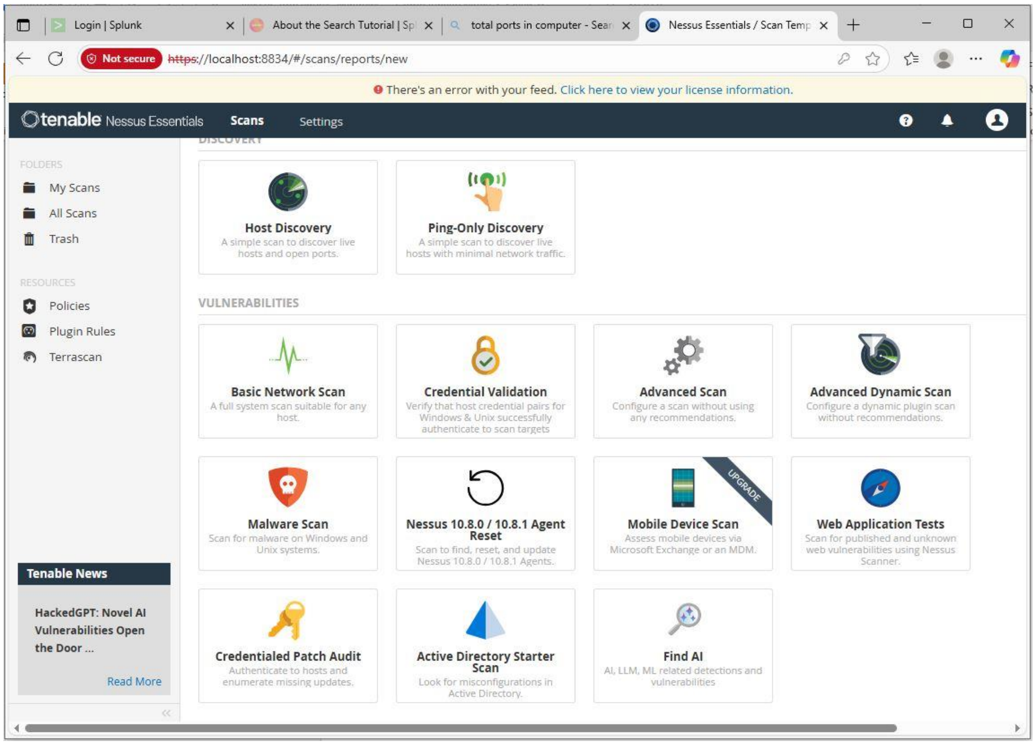

Login | Splunk
About the Search Tutorial | Splunk
total ports in computer - Search
Nessus Essentials / Resources / Po
Not secure
https://localhost:8834/#/scans/policies
There's an error with your feed. Click here to view your license information.
tenable Nessus Essentials
Scans
Settings
Oswald
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
What's New in Tenable Cloud Security: Enhanced Vis...
Read More
Import
New Policy
Search Policies
1 Policy

Policies

Policies allow you to create custom templates defining what actions are performed during a scan. Once created, they can be selected from the list of scan templates. From this page you can view, create, import, download, edit, and delete policies.

Name	Template	Last Modified
4_COHORT CUSTOM POLICY	Advanced Scan	November 8 at 12:55 PM

Figure 3.1


Login | Splunk
About the Search Tutorial | Sp
total ports in computer - Sear
Nessus Essentials / Scan Temp
Not secure
https://localhost:8834/#/scans/reports/new
There's an error with your feed. Click here to view your license information.
tenable Nessus Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
HackedGPT: Novel AI Vulnerabilities Open the Door ...
Read More
UPGRADE

DISCOVERY

Host Discovery
A simple scan to discover live hosts and open ports.

Ping-Only Discovery
A simple scan to discover live hosts with minimal network traffic.

VULNERABILITIES

Basic Network Scan
A full system scan suitable for any host.

Credential Validation
Verify that host credential pairs for Windows & Unix successfully authenticate to scan targets

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.

Nessus 10.8.0 / 10.8.1 Agent Reset
Scan to find, reset, and update Nessus 10.8.0 / 10.8.1 Agents.

Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.

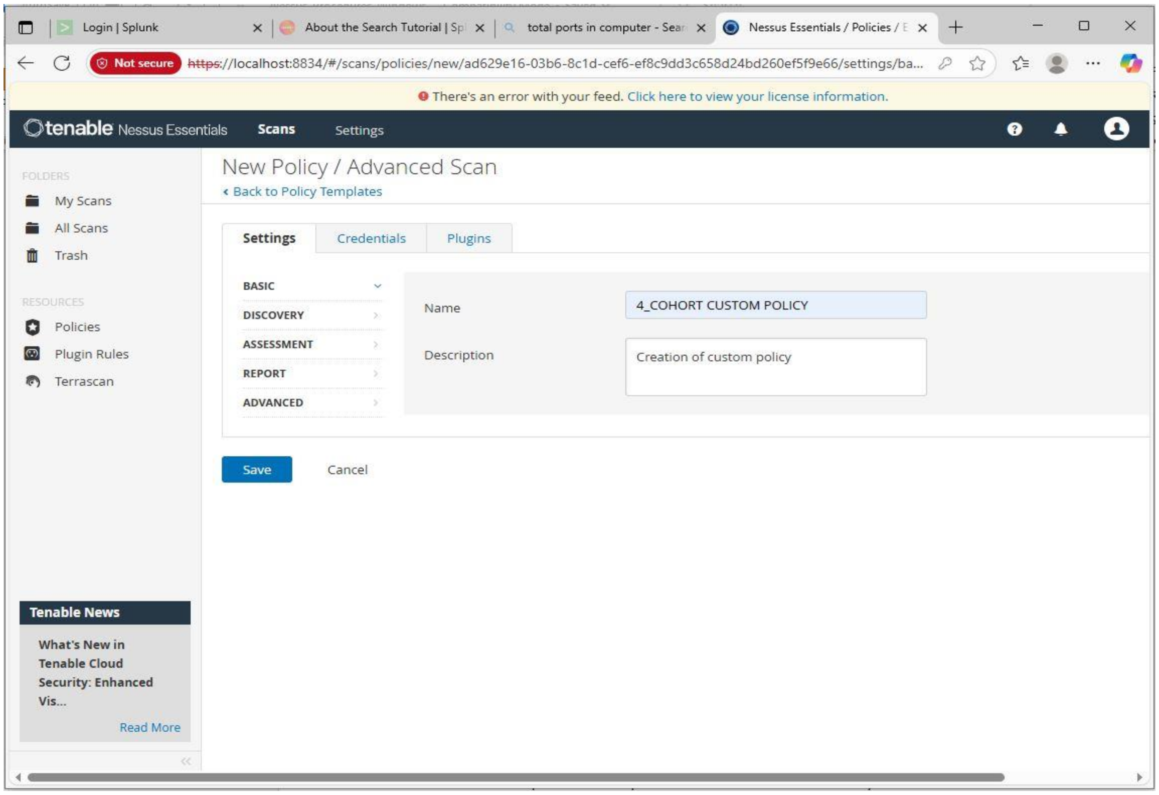
Web Application Tests
Scan for published and unknown web vulnerabilities using Nessus Scanner.

Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.

Active Directory Starter Scan
Look for misconfigurations in Active Directory.

Find AI
AI, LLM, ML related detections and vulnerabilities

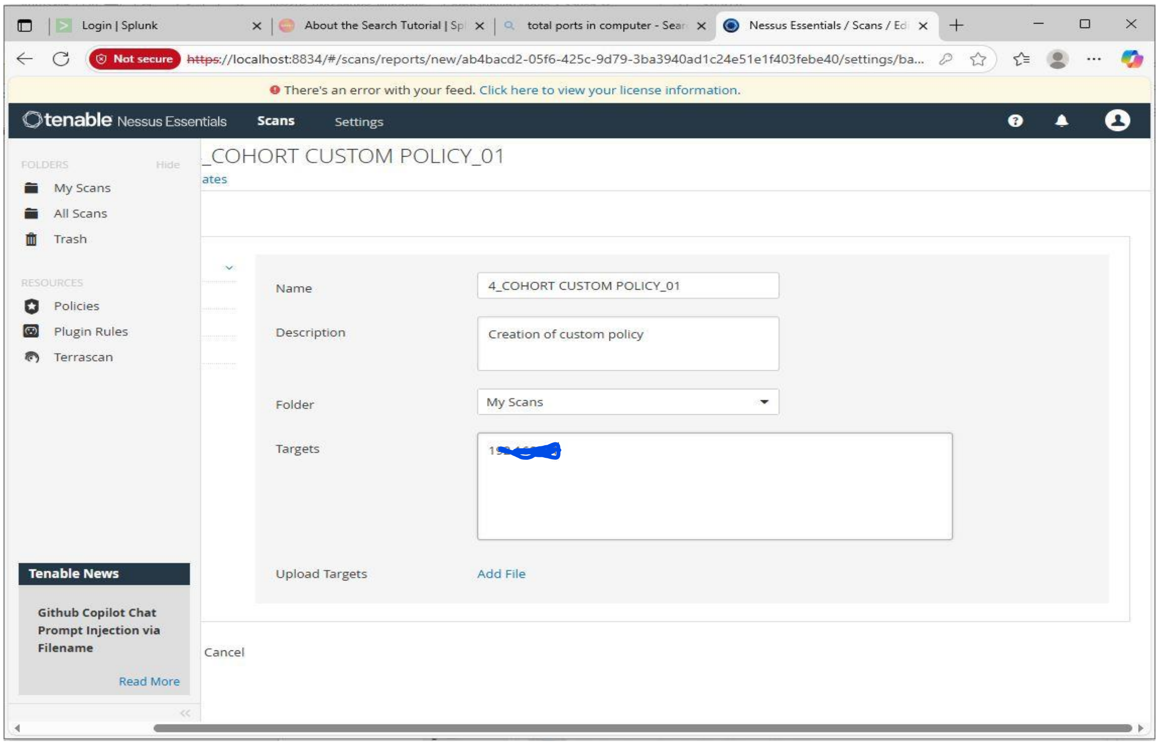
Figure 3.2


Login | Splunk
About the Search Tutorial | Sp
total ports in computer - Sear
Nessus Essentials / Policies / E
Not secure
https://localhost:8834/#/scans/policies/new/ad629e16-03b6-8c1d-cef6-ef8c9dd3c658d24bd260ef5f9e66/settings/ba...
There's an error with your feed. Click here to view your license information.
tenable Nessus Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
What's New in Tenable Cloud Security: Enhanced Vis...
Read More
New Policy / Advanced Scan
‹ Back to Policy Templates
Settings
Credentials
Plugins
BASIC
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Save
Cancel

Name: 4_COHORT CUSTOM POLICY

Description: Creation of custom policy

Figure 3.3


Login | Splunk
About the Search Tutorial | Sp
total ports in computer - Sear
Nessus Essentials / Scans / Ed
Not secure
https://localhost:8834/#/scans/reports/new/ab4bacd2-05f6-425c-9d79-3ba3940ad1c24e51e1f403febe40/settings/ba...
There's an error with your feed. Click here to view your license information.
tenable Nessus Essentials
Scans
Settings
FOLDERS
Hide
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Github Copilot Chat Prompt Injection via Filename
Read More
_COHORT CUSTOM POLICY_01
ates
Upload Targets
Add File
Cancel

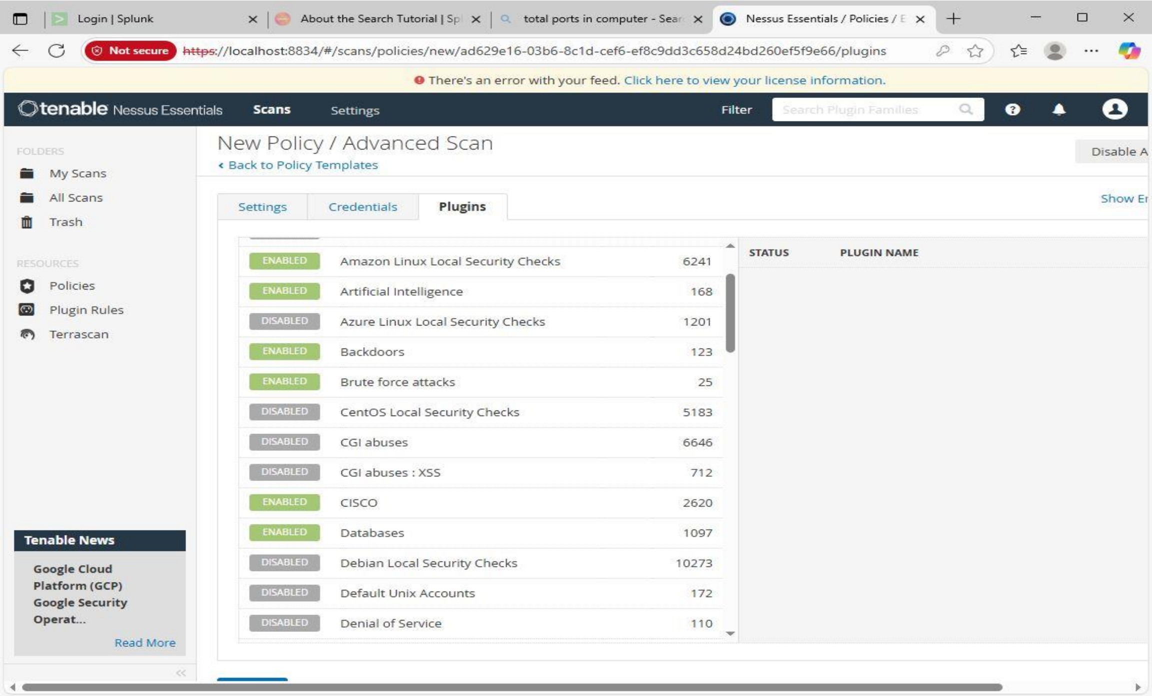
Name: 4_COHORT CUSTOM POLICY_01

Description: Creation of custom policy

Folder: My Scans

Targets: 1[redacted]

Figure 3.4


Login | Splunk
About the Search Tutorial | Sp
total ports in computer - Sear
Nessus Essentials / Policies / E
Not secure
https://localhost:8834/#/scans/policies/new/ad629e16-03b6-8c1d-cef6-ef8c9dd3c658d24bd260ef5f9e66/plugins
tenable Nessus Essentials
Scans
Settings
Filter
Search Plugin Families
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Google Cloud Platform (GCP) Google Security Operat...
Read More
Disable A
Back to Policy Templates
Settings
Credentials
Plugins
Show E

There's an error with your feed. Click here to view your license information.

New Policy / Advanced Scan

ENABLED	Amazon Linux Local Security Checks	6241
ENABLED	Artificial Intelligence	168
DISABLED	Azure Linux Local Security Checks	1201
ENABLED	Backdoors	123
ENABLED	Brute force attacks	25
DISABLED	CentOS Local Security Checks	5183
DISABLED	CGI abuses	6646
DISABLED	CGI abuses : XSS	712
ENABLED	CISCO	2620
ENABLED	Databases	1097
DISABLED	Debian Local Security Checks	10273
DISABLED	Default Unix Accounts	172
DISABLED	Denial of Service	110

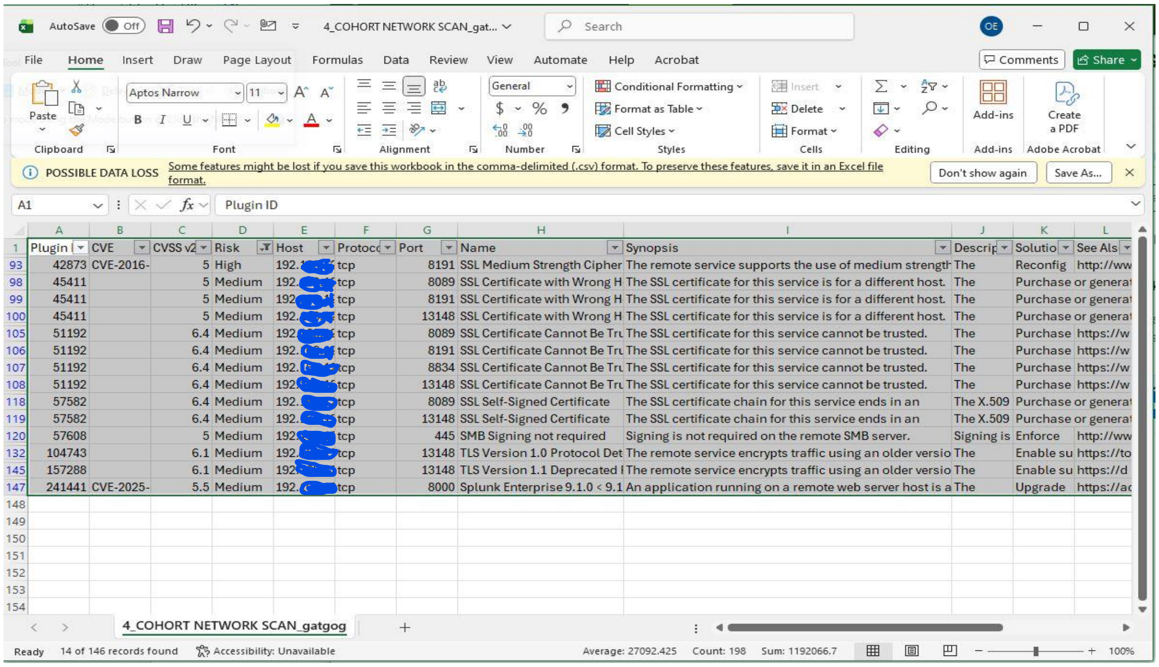
STATUS	PLUGIN NAME

Figure 3.5

8. Exporting and Sorting Scan Results

Steps to export CSV:

1. Open completed scan results.
2. Click Export → Select CSV.
3. Save the file. Refer to chapter 5 for step one to three.
4. Open the CSV in Excel.
5. Sort vulnerabilities by Severity. As shown in Figure 4.1


AutoSave Off
4_COHORT NETWORK SCAN_gat...
Search
File Home Insert Draw Page Layout Formulas Data Review View Automate Help Acrobat
Comments Share
Clipboard Font Alignment Number Styles Cells Editing Add-ins Adobe Acrobat
Aptos Narrow 11 General
Conditional Formatting
Format as Table
Cell Styles
Insert Delete Format
Add-ins
Create a PDF
Don't show again
Save As...
4_COHORT NETWORK SCAN_gatgog

POSSIBLE DATA LOSS Some features might be lost if you save this workbook in the comma-delimited (.csv) format. To preserve these features, save it in an Excel file format.

A1 Plugin ID

	A	B	C	D	E	F	G	H	I	J	K	L
1	Plugin I	CVE	CVSS v2	Risk	Host	Protoco	Port	Name	Synopsis	Descrip	Solutio	See Als
93	42873	CVE-2016-	5	High	[redacted]	tcp	8191	SSL Medium Strength Cipher	The remote service supports the use of medium strength	The	Reconfig	http://ww
98	45411		5	Medium	[redacted]	tcp	8089	SSL Certificate with Wrong H	The SSL certificate for this service is for a different host.	The	Purchase or generat	
99	45411		5	Medium	[redacted]	tcp	8191	SSL Certificate with Wrong H	The SSL certificate for this service is for a different host.	The	Purchase or generat	
100	45411		5	Medium	[redacted]	tcp	13148	SSL Certificate with Wrong H	The SSL certificate for this service is for a different host.	The	Purchase or generat	
105	51192		6.4	Medium	[redacted]	tcp	8089	SSL Certificate Cannot Be Tru	The SSL certificate for this service cannot be trusted.	The	Purchase	https://w
106	51192		6.4	Medium	[redacted]	tcp	8191	SSL Certificate Cannot Be Tru	The SSL certificate for this service cannot be trusted.	The	Purchase	https://w
107	51192		6.4	Medium	[redacted]	tcp	8834	SSL Certificate Cannot Be Tru	The SSL certificate for this service cannot be trusted.	The	Purchase	https://w
108	51192		6.4	Medium	[redacted]	tcp	13148	SSL Certificate Cannot Be Tru	The SSL certificate for this service cannot be trusted.	The	Purchase	https://w
118	57582		6.4	Medium	[redacted]	tcp	8089	SSL Self-Signed Certificate	The SSL certificate chain for this service ends in an	The X.509	Purchase or generat	
119	57582		6.4	Medium	[redacted]	tcp	13148	SSL Self-Signed Certificate	The SSL certificate chain for this service ends in an	The X.509	Purchase or generat	
120	57608		5	Medium	[redacted]	tcp	445	SMB Signing not required	Signing is not required on the remote SMB server.	Signing is	Enforce	http://ww
132	104743		6.1	Medium	[redacted]	tcp	13148	TLS Version 1.0 Protocol Det	The remote service encrypts traffic using an older versio	The	Enable su	https://to
145	157288		6.1	Medium	[redacted]	tcp	13148	TLS Version 1.1 Deprecated I	The remote service encrypts traffic using an older versio	The	Enable su	https://d
147	241441	CVE-2025-	5.5	Medium	[redacted]	tcp	8000	Splunk Enterprise 9.1.0 < 9.1	An application running on a remote web server host is a	The	Upgrade	https://ac
148												
149												
150												
151												
152												
153												
154												

Ready 14 of 146 records found Accessibility: Unavailable Average: 27092.425 Count: 198 Sum: 1192066.7 100%

Figure 4.1

9. Screenshot Submission Checklist

Step	Screenshot Required	Completed (Y/N)
Installer download	Yes	
Installation progress	Yes	
Activation & UI access	Yes	
MD5 verification	Yes	
Network Scan setup	Yes	
Host Scan setup	Yes	
Custom Policy screen	Yes	
CSV export & severity sort	Yes	

End of Procedures Document.

Windows Vulnerability Assessment — Executive Report

Prepared by: Oswald Eyram Toku
Tool: Tenable Nessus Essentials
Scan Date: 2025-11-10

1. Introduction

This report documents the results of a vulnerability assessment performed against Windows host(s) using Tenable Nessus Essentials. The emphasis is on technical findings, exploitability, and remediation guidance that IT teams can implement to reduce risk.

2. Scope & Methodology

Scope:
- Targets: Windows hosts in the lab/network (examples: workstations, servers).
- Scan Types: Network discovery scans, host-level (credentialed) scans and custom policy scan.

Methodology Summary:
- Nessus scan(s) launched using a custom policy with Enumeration set to Custom.
- Credentialed Windows checks were enabled where administrator credentials were available to reveal configuration/patch gaps.
- Results exported to CSV for triage and prioritization.

3. High-Level Results (Summary)

The scan results used in this report assume the following counts (replace with real scan counts after lab run):

Severity	Count
Critical	500
High	20
Medium	15
Low	25
Total	560

4. Technical Findings (Representative)

Below are representative technical findings that typically appear in Windows-focused scans. For each finding, capture the Nessus Plugin ID, affected host(s), CVSSv3 score, and the plugin synopsis/solution.

Plugin ID	Vulnerability / Title	Affected Host(s)	CVSSv3	Suggested Remediation
12345	Remote Code Execution in Service X	192.[redacted]	9.8	Apply vendor patch/upgrade service

				immediately
23456	Unpatched SMBv1 enabled	192.[redacted]	7.5	Disable SMBv1, apply security updates
34567	Weak/Default Credentials on RDP	192.[redacted]	8.2	Enforce strong passwords and enable MFA, restrict network access

5. Exploitability and Risk Prioritization

Prioritization criteria used:
- Exploitability (remote vs local)
- Asset criticality (internet-facing, contains sensitive data)
- CVSS and proof-of-concept availability

Focus remediation on vulnerabilities that are both high-severity and remotely exploitable first.

6. Remediation Recommendations (Technical Steps)

9. Critical (Immediate - within 24 hours)

- Identify each affected host and isolate from network segments if a patch cannot be applied immediately.

- Apply vendor patches or updates. For Windows hosts, use WSUS/Windows Update or vendor-specific patches.

- If patching is impossible, implement compensating controls (restrict access via firewall, disable vulnerable services).

- Rescan hosts after remediation to verify fixes.

10. High (3–7 days)

- Schedule and apply patches during approved maintenance windows.

- Address configuration issues (e.g., disable unnecessary services, enforce secure settings).

- Harden authentication: enforce complex passwords and deploy MFA for privileged accounts.

11. Medium (14 days)

- Plan and apply updates, track via ticketing system.

- Review and tune intrusion detection/prevention rules for the affected services.

12. Low (30 days)

- Evaluate and schedule non-urgent updates and configuration changes.

7. Verification and Validation Procedures

After remediation, perform the following to validate fixes:

1. Re-run the same Nessus scans using the identical policy and targets.
2. Confirm the specific Plugin ID(s) no longer appears for the remediated host(s).
3. Capture screenshots of the rescans and updated Executive Summary.
4. Maintain a remediation log: Plugin ID, Host, Action taken, Date, Verifier.

8. Remediation Policy & SLA (Recommended)

Severity	Proposed SLA	Actions Required	Owner
Critical	Within 24 hours	Patch or isolate; emergency change control	IT Ops / Sysadmin
High	3–7 days	Patch or apply mitigations; schedule maintenance	IT Ops
Medium	14 days	Plan and patch during maintenance window	IT Ops / App Owner
Low	30 days	Schedule and apply as part of routine updates	IT Ops

9. 30-Day Implementation Plan (Technical)

Timeline	Activities
Days 0–1	Triage critical vulnerabilities; isolate systems if necessary.
Days 2–7	Apply patches for Critical & High items; verify with rescans.
Days 8–14	Address Medium vulnerabilities and apply configuration hardening.
Days 15–30	Resolve Low items, deploy automation for patching, enable continuous scanning.

10. Appendix A — Evidence & Artifacts

Attach or reference the following generated artifacts:

- nessus_scan_results_<date>.csv
- nessus_exec_summary_<date>.pdf
- Screenshots: see Procedures screenshot checklist (installer, MD5, scan runs, CSV export, executive summary)

Ensure all filenames and timestamps are included when submitting.

11. Appendix B — Useful Commands / Remediation Examples

Windows Commands / Tips:
- Compute MD5 (Windows PowerShell / certutil): certutil -hashfile C:\Path\To\Nessus-Installer.exe MD5
- Check Windows Update status: Get-WindowsUpdateLog (or use WUA API / WSUS management)
- Disable SMBv1 via PowerShell: Set-SmbServerConfiguration -EnableSMB1Protocol $false

Remediation verification:
- After patching, rerun the Nessus scan and verify Plugin IDs are resolved.

End of Executive Report.