

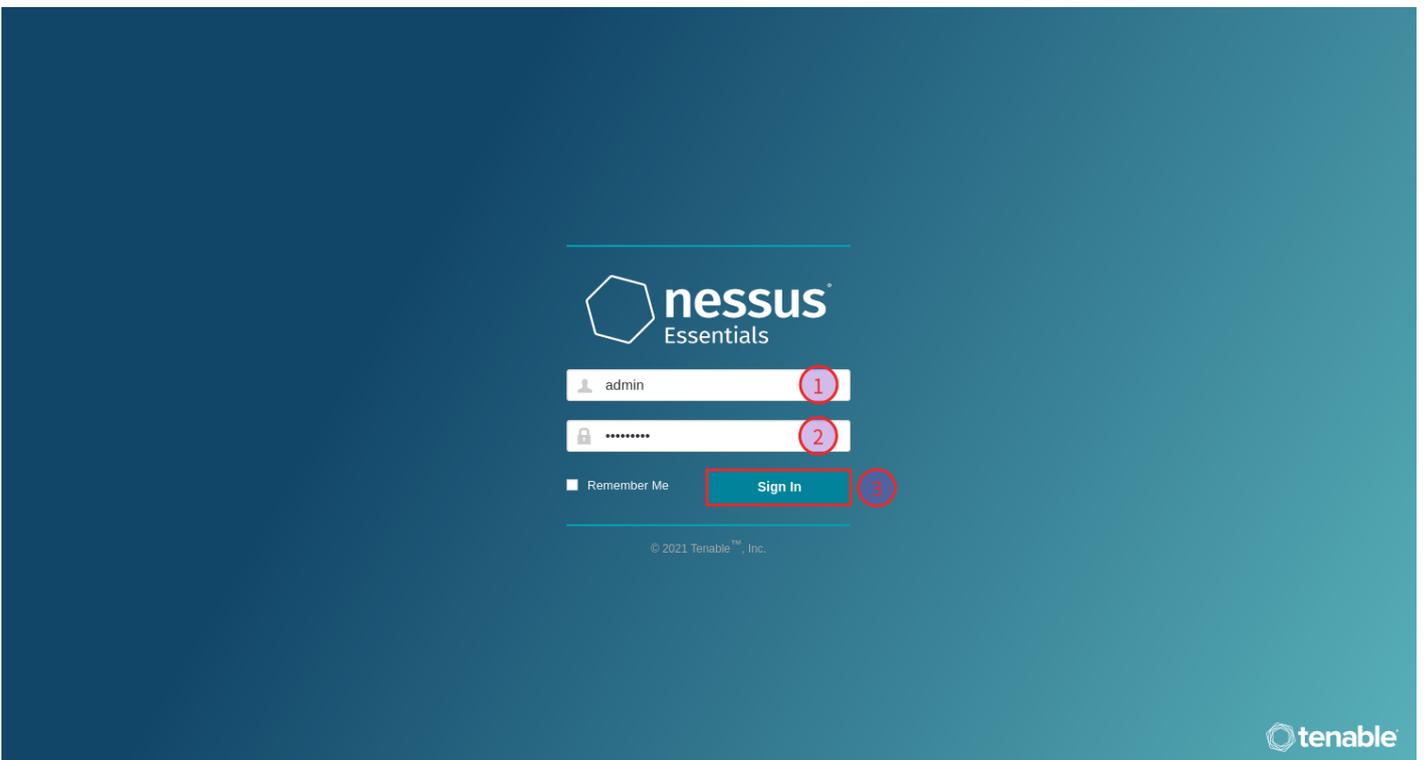
4.

EPower Nessus

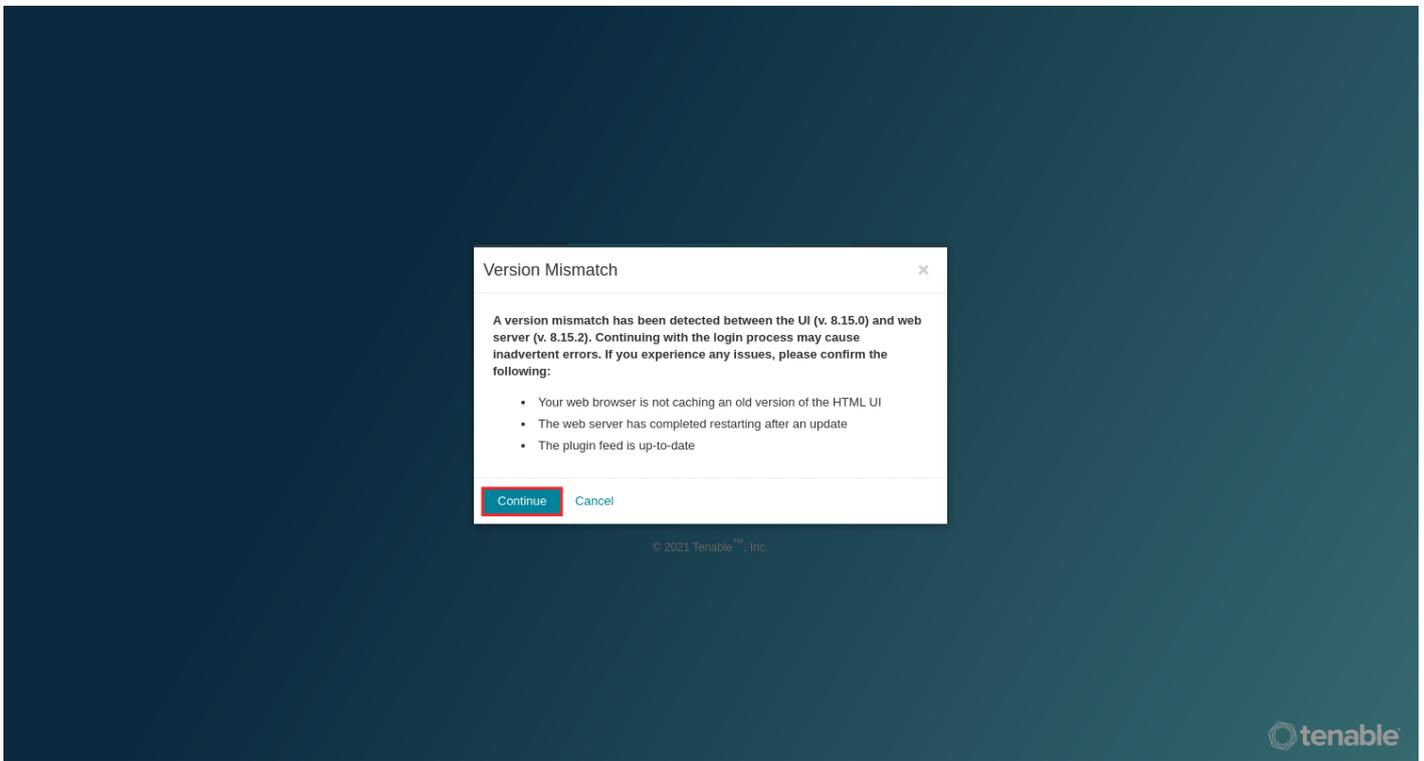
1. Nessus

Username Password

Sign In



Continue



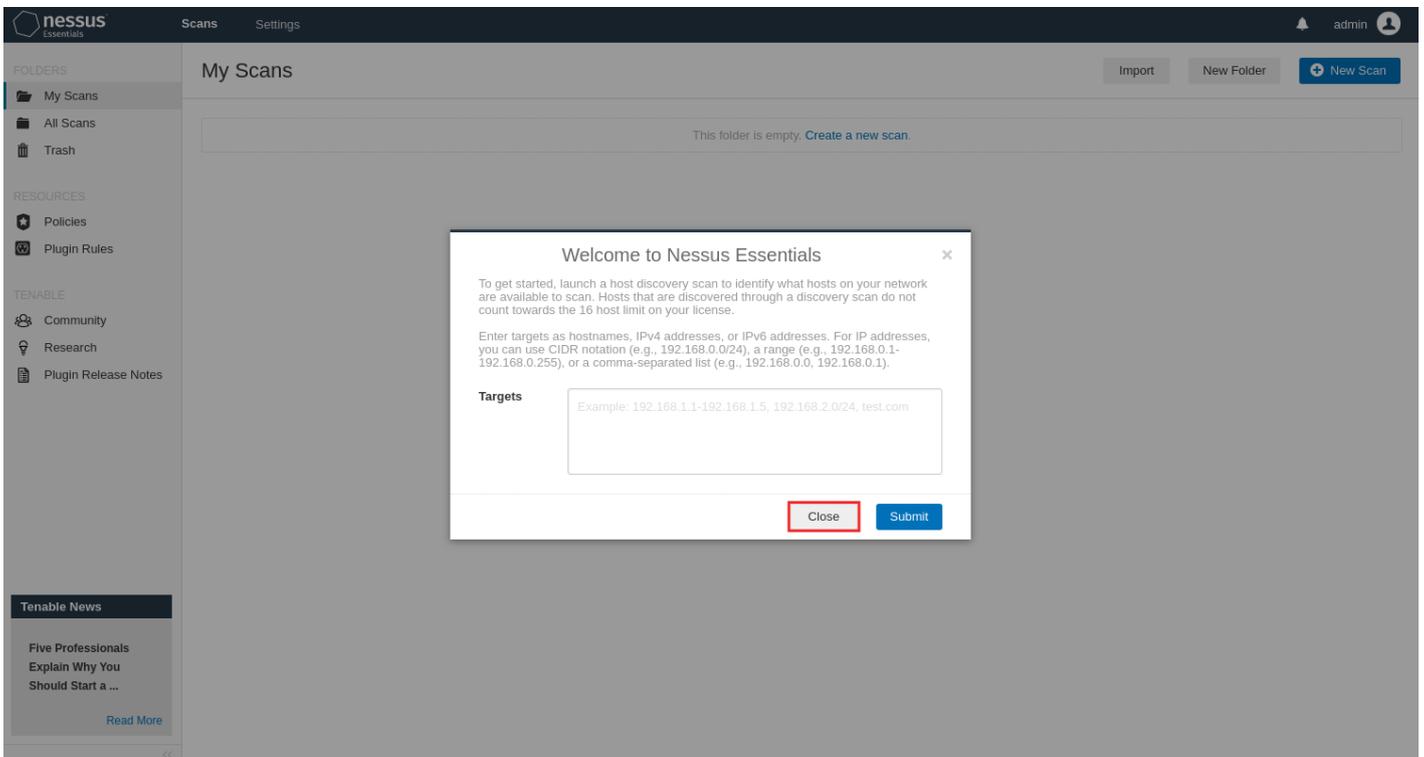
2.

Nessus

IP

Close

IP



New Scan

nessus Essentials Scans Settings admin

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules

TENABLE

- Community
- Research
- Plugin Release Notes

Tenable News

TikTok LIVE Scams: Stolen Live Footage Used to Ear...
[Read More](#)

My Scans

Import New Folder **New Scan**

This folder is empty. [Create a new scan.](#)

Advanced Scan

nessus Essentials Scans Settings admin

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules

TENABLE

- Community
- Research
- Plugin Release Notes

Tenable News

CODESYS V2 Web Server Multiple Vulnerabilities
[Read More](#)

Scan Templates

[Back to Scans](#) Search Library

Scanner

DISCOVERY

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

VULNERABILITIES

<p>Basic Network Scan A full system scan suitable for any host.</p>	<p>Advanced Scan Configure a scan without using any recommendations.</p>	<p>Advanced Dynamic Scan Configure a dynamic plugin scan without recommendations.</p>	<p>Malware Scan Scan for malware on Windows and Unix systems.</p>	<p>Mobile Device Scan Assess mobile devices via Microsoft Exchange or an MDM.</p>
<p>Web Application Tests Scan for published and unknown web vulnerabilities.</p>	<p>Credentialed Patch Audit Authenticate to hosts and enumerate missing updates.</p>	<p>Intel AMT Security Bypass Remote and local checks for CVE-2017-5689.</p>	<p>Spectre and Meltdown Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754.</p>	<p>WannaCry Ransomware Remote and local checks for MS17-010.</p>

Name Description Targets

Save

nessus Essentials Scans Settings admin

New Scan / Advanced Scan

[Back to Scan Templates](#)

Settings Credentials Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name: test (1)

Description: test (2)

Folder: My Scans

Targets: 192.168.1.88 (3)

Upload Targets [Add File](#)

Save (4) Cancel

Tenable News: Five Professionals Explain Why You Should Start a ... [Read More](#)

Launch

nessus Essentials Scans Settings admin

My Scans

Import New Folder [New Scan](#)

Search Scans 1 Scan

<input type="checkbox"/>	Name	Schedule	Last Modified	
<input type="checkbox"/>	test	On Demand	N/A	▶ ✕

Tenable News: Arris SurfBoard SB8200 Cross Site Request Forgery [Read More](#)

nessus Essentials Scans Settings admin

test Configure

[Back to My Scans](#)

Hosts 1 Vulnerabilities 24 History 1

Filter Search Hosts 1 Host

Host	Vulnerabilities	%
192.168.1.88	2	6%

Scan Details

Policy: Basic Network Scan
 Status: Running
 Severity Base: CVSS v3.0
 Scanner: Local Scanner
 Start: Today at 1:59 PM

Vulnerabilities

Tenable News
 Five Professionals Explain Why You Should Start a ...
[Read More](#)

Vulnerabilities

nessus Essentials Scans Settings admin

test Configure Audit Trail Launch Report Export

[Back to My Scans](#)

Hosts 1 **Vulnerabilities 36** VPR Top Threats History 1

Filter Search Vulnerabilities 36 Vulnerabilities

Sev	Name	Family	Count
MIXED	2 IETF Md5 (Multiple Issues)	General	4
MIXED	8 SSL (Multiple Issues)	General	24
MEDIUM	SMB Signing not required	Misc.	1
MIXED	3 SSH (Multiple Issues)	Misc.	3
INFO	8 SMB (Multiple Issues)	Windows	9
INFO	Nessus SYN scanner	Port scanners	9
INFO	2 TLS (Multiple Issues)	Service detection	6
INFO	Service Detection	Service detection	5
INFO	2 LDAP (Multiple Issues)	Misc.	4
INFO	2 DNS (Multiple Issues)	DNS	3
INFO	2 HTTP (Multiple Issues)	Web Servers	3

Scan Details

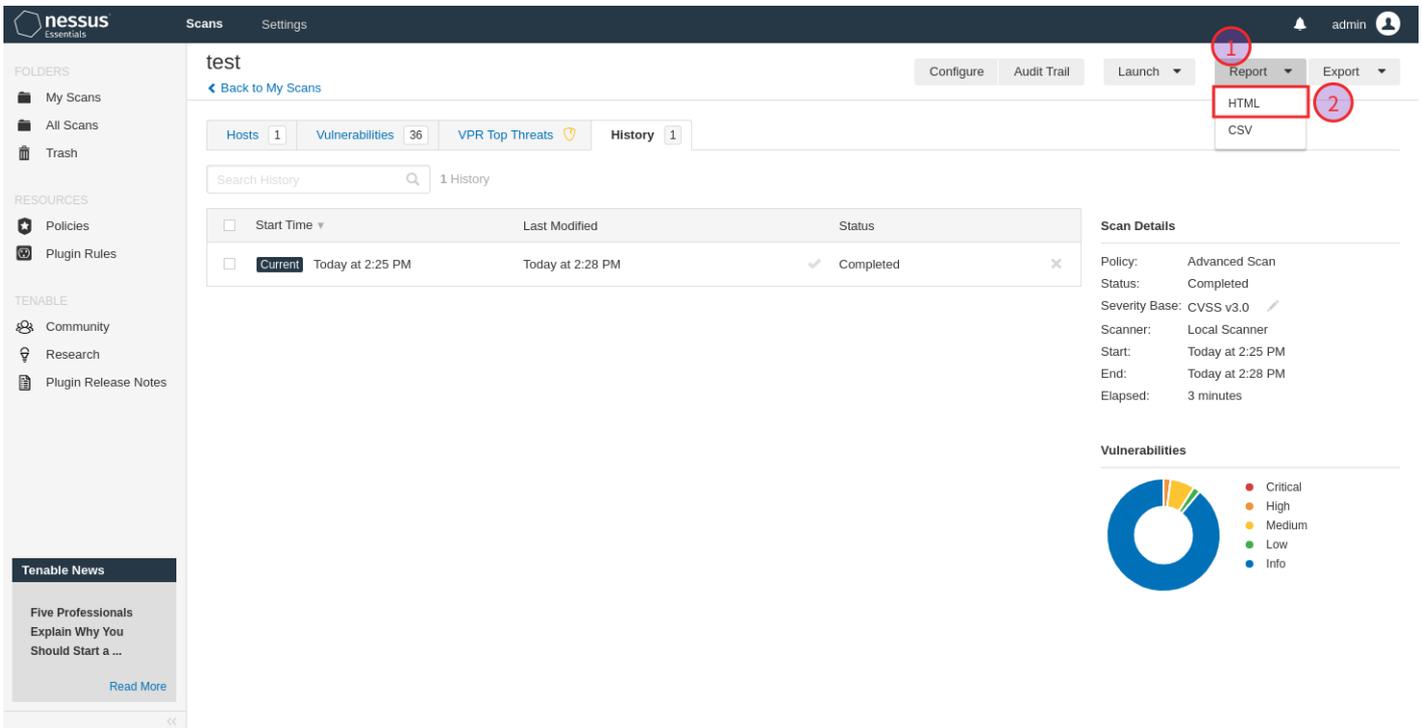
Policy: Advanced Scan
 Status: Completed
 Severity Base: CVSS v3.0
 Scanner: Local Scanner
 Start: Today at 2:25 PM
 End: Today at 2:28 PM
 Elapsed: 3 minutes

Vulnerabilities

Tenable News
 Arris SurfBoard SB8200 Cross Site Request Forgery
[Read More](#)

3.

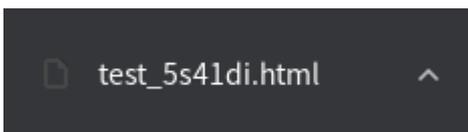
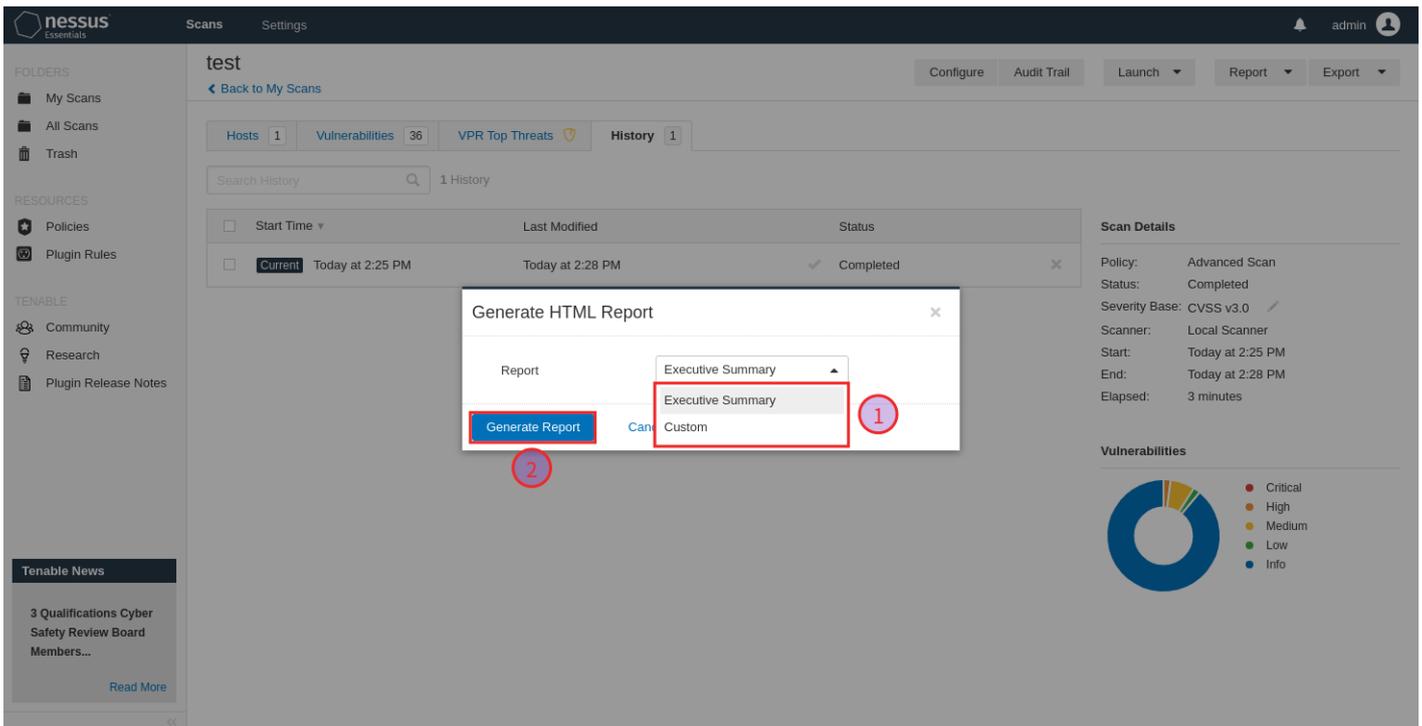
Report→HTML



Executive Summary

Custom

Generate Report



test

Thu, 28 Oct 2021 14:28:36 CST

TABLE OF CONTENTS

Hosts Executive Summary

- [192.168.31.120](#)

Hosts Executive Summary

[Collapse All](#) | [Expand All](#)

192.168.31.120



Severity	CVSS v3.0	Plugin	Name
HIGH	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	5.0	45411	SSL Certificate with Wrong Hostname

Revision #20

Created 22 October 2021 09:00:21 by Epower

Updated 5 December 2021 01:11:07 by Epower