Tenable Useful Plugins Guide

Useful Plugins for Tenable Products

Last Revised: February 15, 2024

Table of Contents

Introduction

The following document highlights several useful plugins for customers.

> **Note:** This document is static and is meant to act as an aid when using Tenable plugins. For a dynamic view of all Tenable plugins, see the Tenable Plugins site.

This document covers plugins from the following Tenable products:

- Tenable Vulnerability Management. For more information, see the *Tenable Vulnerability Management User Guide*.
- Tenable Nessus. For more information, see the *Tenable Nessus User Guide*.
- Tenable Security Center. For more information, see the *Tenable Security Center User Guide*.
- Tenable Nessus Network Monitor. For more information, see the *Tenable Nessus Network Monitor User Guide*.

Plugin Families

Tenable plugins fall into the following ranges per product:

Product	Plugin Ranges
Tenable Nessus	10,001 – 699,999
Tenable Security Center	N/A
Tenable Nessus Network Monitor	• 0-10,000 • (Passive) 700,000-712,000
Tenable Vulnerability Management / Tenable Web App Scanning	• 98,000-98,999 • 112,290-117,290
Custom	900,000 – 999,999
Compliance	1,000,000 (all unique to sites) **Note:** Compliance plugins are numbered according to which plugin a customer uses first.

Tenable Nessus Troubleshooting Plugins

The following plugins can be used when troubleshooting issues with Tenable Nessus.

Tip: Click on a plugin number to view a full description on the Tenable Plugins site.

Plugin Type	Plugin ID	Definition
Successful Login (Windows)	10394	Microsoft Windows SMB Log In Possible
	10400	Microsoft Windows SMB Registry Remotely Accessible
	20811	Microsoft Windows Installed Software Enumeration (credentialed check)
	24269	WMI (Windows Management Instrumentation) Available
Successful Login (Linux)	12634	Authenticated Check: OS Name and Installed Package Enumeration
	22869	Software Enumeration (SSH)
	27576	Firewall Detection
	110095	Target Credential Issues by Authentication Protocol - No Issues Found
Successful Login (Windows or Linux)	141118	Target Credential Status by Authentication Protocol - Valid Credentials Provided
	122502	Integration Credential Status by Authentication Protocol - Valid Credentials Provided
	110095	Target Credential Issues by Authentication Protocol - No Issues Found
Login Failure (Windows or Linux)	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
	104410	Target Credential Status by Authentication Protocol - Failure for Provided Credentials
	110385	Target Credential Issues by Authentication Protocol -

		Insufficient Privilege
	117885	Target Credential Issues by Authentication Protocol - Intermittent Authentication Failure
	122503	Integration Credential Status by Authentication Protocol - Failure for Provided Credentials
	21745	Authentication Failure - Local Checks Not Run
	24786	Nessus Windows Scan Not Performed with Admin Privileges
	10428	Microsoft Windows SMB Registry Not Fully Accessible Detection
	26917	Microsoft Windows SMB Registry: Nessus Cannot Access the Windows Registry
	91822	Database Authentication Failure(s) for Provided Credentials
	11149	HTTP login page
	21745	OS Security Patch Assessment Failed **Note:** This indicates Tenable Nessus is unable to connect to the system, usually for one of the following reasons: • Nessus is unable to connect due to network issues • A network or host-based firewall is blocking the connection attempts • Due to network latency, a timeout is reached before the connection occurs • The user that started the scan does not have permission to scan the given host and/or port. Nessus users have no restrictions by default, so this only happens if an administrator puts a restriction on a user. • Nessus has too many open sockets during a scan. If this happens the nessusd.dump or nessusd.messages indicate the error.

Nessus Scan Information (All Scans)	19506	Nessus Scan Information • Tenable Security Center Filter: Vulnerability Text Contains "Credentialed checks : yes" • Tenable Vulnerability Management Filter: Plugin Output Contains "Credentialed checks : yes"
	112154	Nessus Launched Plugin List **Note:** To use this plugin, you must enable the debug setting. For more information, see Advanced Settings in the *Tenable Nessus User Guide*.
Other	10919	Open Port Re-Check
	35453	Microsoft Windows Update Reboot Required
	35703	SMB Registry: Start the Registry Service During the Scan
	35704	SMB Registry: Stop the Registry Service After the Scan
	35705	SMB Registry: Starting the Registry Service during the Scan Failed
	35706	SMB Registry : Stopping the Registry Service after the Scan Failed
	84239	Debugging Log Report

Other Useful Tenable Nessus Plugins

The following is a list of other useful plugins for Tenable Nessus.

Tip: Click on a plugin number to view a full description on the Tenable Plugins site.

Plugin Type	Plugin ID	Description
Vulnerabilities to Look For	26921	Windows Service Pack Out-of-Date
	33851	Network Daemons Not Managed by the Package System
	59275	Malicious Process Detection
Agent Plugins	100574	Tenable Windows Nessus Agent Installed
	110230	Tenable Nessus Agent Installed (Linux)
	110231	Tenable Nessus Agent Installed (macOS)

System Information	10107	HTTP Server Type and Version
	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
	10395	Microsoft Windows SMB Shares Enumeration
	10396	Microsoft Windows SMB Shares Access
	11936	OS Identification
	12053	Host Fully Qualified Domain Name (FQDN) Resolution
	20811	Microsoft Windows Installed Software Enumeration (Credentialed Check)
	24272	Network Interfaces Enumeration (WMI)
	25203	Enumerate IPv4 Interfaces via SSH
	25221	Remote Listeners Enumeration (Linux / AIX)
	34252	Microsoft Windows Remote Listeners Enumeration (WMI)
	35453	Microsoft Windows Update Reboot Required
	55472	Device Hostname
	64582	Netstat Connection Information
	66334	Patch Report
	93561	Docker Service Detection
	112154	Nessus Launched Plugin List **Note:** To use this plugin, you must enable the debug setting. For more information, see Advanced Settings in the *Tenable Nessus User Guide*.

Nessus Discovery Plugins

The following plugins can be used for Tenable Nessus discovery within Tenable Vulnerability Management and Tenable Security Center.

Note: In the Tenable Nessus interface, enable the **Hide results from plugins initiated as a dependency** option to ensure IPs do not count toward your license if they are scanned with one of the following plugins. For more information, see Report Scan Settings in the *Tenable Nessus User Guide*.

Tip: Click on a plugin number to view a full description on the Tenable Plugins site.

Note: The following plugins do not count towards your Tenable Vulnerability Management or Tenable Security Center licenses.

Plugin ID	Description	Plugin Family
45590	Common Platform Enumeration (CPE)	General
54615	Device Type	General
12053	Host Fully Qualified Domain Name (FQDN) Resolution	General
11936	OS Identification	General
10287	Traceroute Information	General
22964	Service Detection	Service Detection
11933	Do not Scan Printers	Settings
87413	Host Tagging	Settings
19506	Nessus Scan Information	Settings
33812	Port Scanners Settings	Settings

33813	Port Scanner Dependency	Settings
112154	Nessus Launched Plugin List	Settings (Tenable Security Center only) **Note:** To use this plugin, you must enable the debug setting. For more information, see Advanced Settings in the *Tenable Nessus User Guide*.

You can copy and paste all of the aforementioned plugins directly from the text below:

- Tenable Vulnerability Management:
  `[10287,11936,12053,54615,45590,22964,11933,19506,33812,33813,87413]`
- Tenable Security Center:
  `[10287,11936,12053,54615,45590,22964,11933,19506,33812,33813,87413,112154]`

The following plugins apply to configuration settings, but do not appear in the plugin list.

Plugin ID	Description	Configuration Settings
10180	Ping the Remote Host	Port Scanners
10335	Nessus TCP Scanner	Port Scanners
11219	Nessus SYN Scanner	Port Scanners
14272	Netstat Portscanner (SSH)	Port Scanners
14274	Nessus SNMP Scanner	Port Scanners
34220	Netstat Portscanner (WMI)	Port Scanners
34277	Nessus UDP Scanner	Port Scanners

Tenable Nessus Network Monitor Discovery Plugins

The following plugins can be used for Tenable Nessus Network Monitor discovery within Tenable Vulnerability Management and Tenable Security Center.

Note: Any IPs detected with the following plugins do not count towards your license.

Tip: Click on a plugin number to view a full description on the Tenable Plugins site.

Note: The following plugins do not count towards your Tenable Vulnerability Management or Tenable Security Center licenses.

Plugin ID	Description	Plugin Family
0	Open Port	
12	Host TTL Discovered	
18	Generic Protocol Detection	
19	VLAN ID Detection	
20	Generic IPv6 Tunnel Traffic Detection	
113	VXLAN ID Detection	
132	Host Attribute Enumeration	

You can copy and paste all of the aforementioned plugins directly from the text below:

- Tenable Vulnerability Management/Tenable Security Center: `[0,12,18,19,20,113,132]`

Tenable Nessus Compliance Plugins

While all of the compliance plugins are part of the Policy Compliance family, these other plugins can provide additional useful information about the target or about credentialed login success. Tenable suggests using these following plugins alongside discovery plugins.

Note: Remember to enable the entire policy compliance family.

Tip: Click on a plugin number to view a full description on the Tenable Plugins site.

Plugin ID	Description	Plugin Family	Host Discovery?
10287	Traceroute Information	General	Yes
11936	OS Identification	General	Yes
12053	Host Fully Qualified Domain Name (FQDN) Resolution	General	Yes
11933	Do Not Scan Printers	Settings	Yes
19506	Nessus Scan Information	Settings	Yes
33813	Port Scanner Dependency	Settings	Yes
21745	OS Security Patch Assessment Failed	Settings	No
24786	Nessus Windows Scan Not Performed with Admin Privileges	Settings	No
10394	Microsoft Windows SMB Log In Possible	Windows	No
10400	Microsoft Windows SMB Registry Remotely Accessible	Windows	No
10428	Microsoft Windows SMB Registry Not Fully Accessible Detection	Windows	No
24269	WMI Available	Windows	No
26917	Microsoft Windows SMB Registry: Nessus Cannot Access the Windows Registry	Windows	No

Resolving Plugin 51192

To resolve plugin 51192 in Tenable Vulnerability Management:

1. Copy your PEM encoded certificate into a text file and name it custom_CA.txt.

   Note: Be sure to include everything between, and including, the `---BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` lines.

   Tip: If you need to upload multiple certificates, paste each certificate back-to-back within the same file.

2. Save the .txt file.
3. Log into Tenable Nessus.
4. Navigate to **Settings** > **Custom CA**.
5. Copy and paste the text from the custom_CA.txt file into the **Certificate** text box.
6. Click **Save**.

To resolve plugin 51192 in Tenable Security Center:

1. Copy your PEM encoded certificate into a text file and name it custom_CA.inc.

   Note: Be sure to include everything between, and including, the `---BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` lines.

   Tip: If you need to upload multiple certificates, paste each certificate back-to-back within the same file.

2. Save the .txt file.
3. Create a text file named custom_feed_info.inc and include the following lines:

```
PLUGIN_SET = "201310161758";
PLUGIN_FEED = "Custom";
```

> **Note:** The plugin set date should be the same as the time you upload the bundle to Tenable Security Center. It cannot be after the present date/time.

> **Tip:** The typical format for PLUGIN_SET is a string of numbers in the format "YYYYMMDDHHMM" for the regular feed, so that format is copied here.

4. Tar the two files into a .tar.gz archive:

```
# tar -zcvf upload_this.tar.gz custom_feed_info.inc custom_CA.inc
```

> **Note:** You cannot use 7-zip or run tar on macOS for this step.

5. Log into Tenable Security Center as an administrator.
6. Navigate to **Plugins** > **Upload Custom Plugins**.
7. Click **Submit**.
8. On your machine, navigate to **System** > **System Logs** and verify the logs indicate that zero plugins have been updated.

   Tenable Security Center pushes the plugins to the appropriate scanners during its normal update process.
9. To verify the issue is resolved, run another scan including plugin 51192. To verify that Tenable Nessus has the custom plugin bundle, check its plugin directory.

Notes

Updating Tenable Security Center plugins to initiate a plugin push to the Tenable Nessus scanners only works if the plugin feed downloaded by Tenable Security Center is newer than the plugin set on the Tenable Nessus scanners. If Tenable has not yet released a newer plugin feed, wait for the next plugin feed to be available before updating.

The custom_CA.inc file is overwritten every time it is uploaded. When adding additional CA certificates, start with a copy of the existing custom_CA.inc and append the new certificate. If there are multiple certificates in the file, it should look like this:

```
-----BEGIN CERTIFICATE-----
Lorem ipsum dolor sit amet
consectetuer adipiscing elit
```

```
Phasellus hendrerit Pellentesque
aliquet nibh nec urna.
-----END CERTIFICATE----
-----BEGIN CERTIFICATE-----
Lorem ipsum dolor sit amet
consectetuer adipiscing elit
Phasellus hendrerit Pellentesque
aliquet nibh nec urna.
-----END CERTIFICATE----
```

Troubleshooting

If the above instructions do not work, check the following items:

Custom_CA.inc Format

The CA certificate should be in PEM (Base64) format. To verify, open it in a text editor. The certificate should be between `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----`. If you do not see these lines, the file is in the wrong format. Change the file to PEM (Base64) format either through a conversion or through a fresh export.

Plugin Output

Other issues can be, for example, that the service is missing intermediate certificate(s), the service has a self-signed or default certificate (if not self-signed with the server name, it may be issued by a vendor name like "Nessus Certification Authority") and not a certificate signed by their custom CA, the certificate is expired, etc. Look at the detailed plugin output of 51192 to see exactly why the certificate is untrusted. If updating custom_CA.inc can fix the error, the output indicates that the certificate at the top of the certificate chain is unrecognized. The certificate it shows is either issued by the custom CA (matching the name *exactly*) or the actual custom CA self-signed certificate.