



# Tenable Cyber Exposure Study - Host Audit Data

---

Last Revised: April 26, 2024



## Table of Contents

Host Audit Data Overview .....	3
Host Audit Data Analysis .....	4
Tenable Security Center Compliance Elements .....	20
Benchmarks .....	22
Compliance Frameworks .....	28
Host Audit Plugin Type .....	40
Vendor-Based Audits .....	48
Learn More .....	52



# Host Audit Data Overview

---

Tenable has introduced key features and content that give you visualization of Compliance scan results through the built-in dashboards or custom dashboards using the newly added widgets. Detailed or summarized reports can also be generated in PDF format for the host audit findings. In support of these new features coming to Tenable Vulnerability Management, this guide serves as a tool to assist the user in utilizing the templates and filters to query host audit data. This study includes a detailed analysis section which breaks down data fields and gives example searches when querying the compliance data.

This Cyber Exposure Study provides guidance through the following subjects:

- Host Audit Data Analysis
- Benchmarks
  - Center for Internet Security
  - Defense Information Systems Agency
- Compliance Frameworks
- Host Audit Plugin Type
- Vendor-Based Audits



# Host Audit Data Analysis

When scanning assets with Tenable Audit files, the finding returned is slightly different than a vulnerability finding. The first step in analyzing audit results is to first understand the source.

## Key Data Fields

The audit file is an XML like file, which consists of several configuration checks. When the Tenable Research team examines the various benchmarks, for example Center for Internet Security (CIS), each CIS benchmark is broken into profiles (Level 1 and Level 2) and each profile is an item. The Tenable Audit files convert the “items” into XML like elements `<item>` or `<custom_item>` which then becomes an audit check name in Tenable Vulnerability Management or Tenable Security Center. From this point forward, `<item>` or `<custom_item>` in audit files are referred to as an **audit check name**, and the presence of an **audit check name** on an asset is called a finding.

More information on audit files can be found here:

- [Audits](#)
- [Nessus Compliance Checks Reference](#)

```
<custom_item>
  system      : "Linux"
  type        : FILE_CONTENT_CHECK
  description  : "5.3.3 Ensure password reuse is limited - system-auth"
  info        : "The /etc/security/opasswd ---TEXT OMITTED---"
  reference    : "800-171|3.5.2,800-53|IA-5(1),800-53r5|IA-5(1),CSCv7|4.4,CSF|PR.AC-1,GDPR|
32.1.b,HIPAA|164.306(a)(1),HIPAA|164.312(a)(2)(i),HIPAA|164.312(d),ITSG-33|IA-5(1),LEVEL|
15,NESA|T5.2.3,QCSC-v1|5.2.2,QCSC-v1|13.2,SWIFT-CSCv1|4.1"
  see_also    : "https://workbench.cisecurity.org/files/2449"
  file        : "/etc/pam.d/system-auth"
  regex       : "^[\\s]*password[\\s]+(sufficient[\\s]+pam_unix\\.so|required[\\s]
+pam_pwhistory\\.so).*remember"
  expect      : "remember[\\s]*=[\\s]*([5-9]|[1-9][0-9]+)"
</custom_item>
```

The description line becomes the audit check name, the other key field is the “reference” line, also known as the Cross Reference or XREF. The XREF is a mapping of this respective check to several compliance standards and benchmarks. Customers are able to search using the XREF in different methods based on the product, see below:

Product	Search Term	Example
---------	-------------	---------



t.io	800-53 ACCESS CONTROL	Compliance Framework= 800*53 Compliance Family= ACCESS CONTROL
t.sc	800-53 ACCESS CONTROL	Cross Reference = 800-53 AC*

To help customers verify the audit checks authority in the benchmark, the “see\_also” field provides the location a customer can download the benchmark from the provider. This benchmark is used to consolidate audit checks by the correct benchmark and version.

<https://workbench.cisecurity.org/files/2449>

When an asset is scanned using an audit file, and a check becomes a finding, the finding is returned in one of the following states: PASSED, FAILED, ERROR, WARNING. The state is converted into a severity level for use with Tenable Security Center, and for Tenable Vulnerability Management the state is retained. The color coding for the state coincides with the color for the severity levels as displayed on the following table.

State	Tenable Security Center Severity	Tenable Vulnerability Management State	Descriptions
PASSED	Informational	Passed	The audit check was within the tested parameters.
FAILED	High	Failed	The audit check was not within the tested parameters.
ERROR	Medium	Error	The audit check is not supported on the



			asset.
<b>WARNING</b>	Medium	Warning	The audit check was successful, however compliance cannot be determined and needs to be reviewed manually.

## Data Fields Explained

Now that we understand the key fields used for analysis there are a few other fields used to enhance search behaviors and are commonly used in the compliance dashboards and reports. In this section a detailed review of all the fields and how they work together are provided.

- [Tenable Vulnerability Management](#)
- [Tenable Security Center \(6.3\)](#)

## Audit File

The name of the Audit file the scanner used to perform the audit. Audit files are XML-based text files that contain the specific configuration, file permission, and access control tests to be performed. The audit file can be customized and should be changed if the customer edits the audit file. For example if the audit file provided by Tenable is named "CIS\_AlmaLinux\_OS\_8\_Server\_v3.0.0\_L1.audit" and the customer edits the parameters of the audit file, then the customer might change the name to be "ACME-Mar24-CIS\_AlmaLinux\_OS\_8\_Server\_v3.0.0\_L1.audit." This name suggests that the ACME corp added this audit file in March of 2024. In doing this, analysts are able to easily find the audit files edited by the organization and apply the filters correctly.

While changing the name of an audit file is not required, here is helpful information to consider if choosing to do so. Note that the names of the audit file are not to be confused with benchmark. Tenable names the audit files to coincide with the benchmark, but the name is just a name. When choosing the name for the audit files, consider the operating system the audit file is intended for, the benchmark (including the version) used to create the audit file, and the date the audit file is added. Note that audit files that are custom, meaning imported by the customer, are not updated and therefore need to be maintained.



## Tenable Vulnerability Management:

- Using the audit file name is supported in both the group-by options in the widget and in the filters.
- In the Bar Chart example, the bars represent the count of findings by the respective audit file. Other factors for example state, date, or etc. are not included.

### Create Custom Widget

#### General

CHART TYPE

NAME

DESCRIPTION

100 characters max

2000 characters max

#### Data

DATA SET

ENTITY

LIMIT

GROUP BY

STATS

SORT FIELDS

SORT ORDER

Select Filters Saved Filters Match All Advanced

Audit File: is equal to CIS\*

### Widget Preview

Title

Audit File	Count (approx.)
CIS_Red_Hat_EL8_Server_v2.0.0_L1.test.audit	1250
CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.test-2.audit	1050
CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.test.audit	1000
CIS_Oracle_Linux_8_Server_L1_v2.0.0.test.audit	1000
CIS_Ubuntu_22.04_LTS_v1.0.0_Workstation_L1.test.audit	1000

## Tenable Security Center:

- Analysis using an Audit Files is only available in a filter.
- Organizations can use this filter to focus the results using charts and tables, however the audit file is not displayed, only the display columns based on the selected tool.
- Dashboard component documentation is found [here](#).

## Audit Check Name

The name Tenable assigned to the audit, as previously mentioned see figure 1, is the value in the **description** field in the audit file. In some cases, the compliance control may be listed as the prefix within the name. This is often combined with a nomenclature from the benchmark. In CIS benchmark, the name is prefixed with a number and DISA uses the STIG-ID. Just note that



regardless of the benchmark used to create the audit file, review the descriptions that are provided in the audit file for a list of possible audit check names.

Using grep or similar tool, the user can search audit files and return all the descriptions which are converted into the audit check name: `grep -E '\s+description(\s):' *.audit`

- CIS Example: "4.5.3.3 Ensure default user umask is configured"
- DISA Example : "WG050 W22 - The web server service password(s) must be entrusted to the SA or Web Manager."

## Tenable Vulnerability Management:

- The audit check name is available using group by and filtering similar to the audit file above.
- Use the “\*” or wild card and the end of the string to search for all the audit check names that match the pre-fixed pattern. All the patterns below find audit check names with the relative pattern. Note, when using the \* as the first character in the search you will match any pattern. The samples below match each of the examples shown above.

Pattern	Result
4.5.*	Strings that begin with 4 <period> 5 <period> and followed by any character
WG*	Strings that begin with WG (case insensitive)
*W22*	String that begins with any character but contain W22 within the string, followed by any other characters
W*W22*	Strings that begin with “W” and contain W22

## Tenable Security Center:

- Audit Check Names become the plugin name. When an audit file is imported and used in a scan or filter, Tenable Security Center creates plugins for each of the <items> or <custom\_items> in the audit file. The plugins have an ID > 1,000,000 and the plugin ID will be unique to the installation. Also note, if an audit file is updated and re-added, new plugins are created, this is another reason why it's often a good idea to name the audit file during import.





- The plugin name field supports regex patterns allowing for very complex and flexible pattern matching, here are some examples:

Pattern	Result
<code>^4\5.*</code>	Strings that begin with 4 <period> 5 <period> and followed by any character
<code>^[Ww][Gg].*</code>	Strings that begin with WG (case sensitive, but account for both upper and lower case)
<code>^.*[Ww]22.*</code>	String that begin with any character but contain W22 within the string, followed by any other characters
<code>^[Ww].*[Ww]22.*</code>	Strings that begin with “W” and contain W22

## Benchmark

Benchmarks are published best practices released from source authorities, such as Center for Internet Security (CIS), United States Defense Information Systems Agency (DISA), and Microsoft. This filter provides a list of the supported benchmarks and the version of the benchmark. Tenable used the URL of the Benchmark to distinguish to which benchmark the audit file is mapped. The URL is stored in the SEE\_ALSO element found in the audit file.

- CIS: <https://workbench.cisecurity.org/benchmarks/12695>
- DISA: [https://iasecontent.disa.mil/stigs/zip/U\\_Apache\\_2-2\\_WIN\\_V1R13\\_STIG.zip](https://iasecontent.disa.mil/stigs/zip/U_Apache_2-2_WIN_V1R13_STIG.zip)
- Microsoft: <https://blogs.technet.microsoft.com/secguide/2018/04/30/security-baseline-for-windows-10-april-2018-update-v1803-final>

CIS Benchmarks are linked directly with See Also URL, in this example CIS Windows Server 2016 version 2.0.0 can be accessed via <https://workbench.cisecurity.org/benchmarks/12695>. Each of the audit files that support the benchmark are focused on the different role or functions of the asset. In this example the DC is the domain controller, and MS is a member server. The L1 and L2 describing the level 1 or level 2 checks depicted in the benchmark. To obtain full coverage with a benchmark all audit files from the specific role needs to be added to the targeted scan. Be careful not to scan a domain controller with a member server audit file, and there are different checks and some coverage could be mis-represented. This benchmark is covered by 6 audit files:



- CIS\_Microsoft\_Windows\_Server\_2016\_Benchmark\_v2.0.0\_DC\_NG.audit
- CIS\_Microsoft\_Windows\_Server\_2016\_Benchmark\_v2.0.0\_L1\_DC.audit
- CIS\_Microsoft\_Windows\_Server\_2016\_Benchmark\_v2.0.0\_L1\_MS.audit
- CIS\_Microsoft\_Windows\_Server\_2016\_Benchmark\_v2.0.0\_L2\_DC.audit
- CIS\_Microsoft\_Windows\_Server\_2016\_Benchmark\_v2.0.0\_L2\_MS.audit
- CIS\_Microsoft\_Windows\_Server\_2016\_Benchmark\_v2.0.0\_MS\_NG.audit

For a DISA STIG, there can be situations where there are more than one version of an Audit file that makes the STIG. For example, DISA STIG Apache Server 2.4 Unix in the URL [https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U\\_Apache\\_Server\\_2-4\\_Unix\\_Y23M07\\_STIG.zip](https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_Apache_Server_2-4_Unix_Y23M07_STIG.zip), contains several version files in version 2.4.0 and 2.6.0. Listed below are the audit files that comprise the STIG, much like the aforementioned CIS benchmark there can be different roles and the appropriate audit files should be deployed to targeted assets.

- DISA\_STIG\_Apache\_Server-2.4\_Unix\_v2r6.audit
- DISA\_STIG\_Apache\_Server-2.4\_Unix\_v2r6\_Middleware.audit
- DISA\_STIG\_Apache\_Site-2.4\_Unix\_v2r4.audit
- DISA\_STIG\_Apache\_Site-2.4\_Unix\_v2r4\_Middleware.audit"

After scanning with appropriate audit files here are examples on how to find the relevant data.

## Tenable Vulnerability Management:

- In this field the benchmark name and version are combined into one string. Using regular search terms, the search can be limited to only the desired content.

Pattern	Result
CIS *	Strings that begin with CIS<space> followed by any other character.
CIS P*9*	Strings that begin with CIS<space>P followed by any other character but must contain a 9 in the string. Ex: CIS Palo Alto



	Firewall 9 v1.1.0
*v1.0.0*	Strings that begin with any character but contain v1.0.0 within the string, followed by any other characters

- For benchmarks that are no longer supported by Tenable, the “Deprecated <prefix> Benchmark” is available
  - Example: Deprecated CIS Benchmark
- DISA\_STIG\_Apache\_Site-2.4\_Unix\_v2r4.audit
  - CIS, DISA, MSCT, NetApp, TNS
- Custom audit files are also supported however the benchmark name will be “Custom”

### Tenable Security Center:

- For notes on how to search for specific elements in Security Center, review this section [Tenable Security Center Compliance Elements:](#)
- To locate the benchmark using the Vulnerability text for contains “cisecurity” or other relevant string, and then copy the link shown under the See Also, as shown below.

Vulnerability Detail List

## Vulnerability Detail List

Vulnerabilities

Web App Scanning

Queries

Events

Mobile

<

Apply

+ Customize

✕ Clear All

Load Query

> Plugin Type

> Severity

> Vulnerability Text

Contains

workbench.cisecurity.org/benchmarks

### 3.1.3 Ensure the logging collector is enabled

VULNERABILITY

HIGH

Accept Risk

Recast Risk

Rationale:

The logging collector approach is often more useful than logging to messages might not appear in syslog output. One common example message; another may be error messages produced by scripts such

Note: This setting must be enabled when log\_destination is either s lost. Certain other logging parameters require it as well.

See Also

LINKS:

[cisecurity.org](https://workbench.cisecurity.org/benchmarks/12695)

Policy Value

- When the “cisecurity.org” link is copied, this would be the string that is collected.
  - https://workbench.cisecurity.org/benchmarks/12695
- The Vulnerability Test filter example: <cm:compliance-see-also>https://workbench.cisecurity.org/benchmarks/12695</cm:compliance-see-also>
  - https://workbench.cisecurity.org/benchmarks/12695
- Add the string with <cm:compliance-see-also>URL-HERE</cm:compliance-see-also> to the Vulnerability Text field.

Benchmark Specification Name

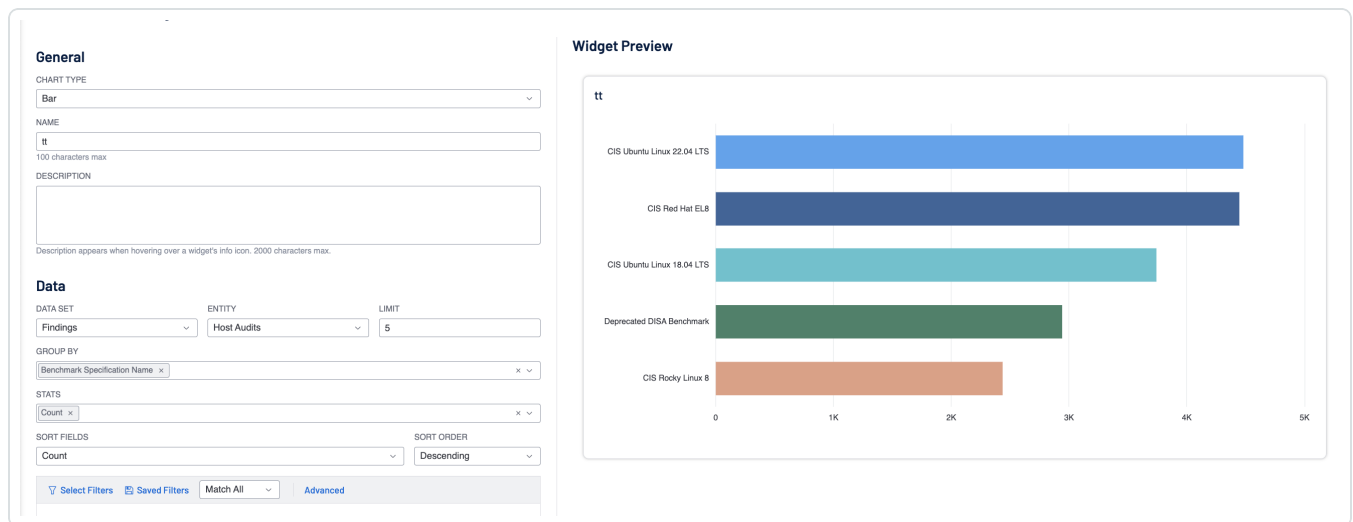


The benchmark name is the same as previously described but does not contain the version. Using only the benchmark name in the search merges the data collected using all versions of the respective benchmark.

After scanning with appropriate audit files here are examples on how to find the relevant data.

## Tenable Vulnerability Management:

- Tenable Vulnerability management supports widgets using a “Group By” using the Benchmark Name, as shown below, the chart quickly shows the benchmarks in use, allowing for more filtering options.



- Note that when a benchmark becomes deprecated and is no longer supported by the benchmark name is changed to Deprecated <TYPE> Tenable. By adding the filter Benchmark Specification Name = “\*deprecated\*”, you can see the use check found with deprecated audit

files.

The screenshot shows a configuration interface for a widget. On the left is the 'General' tab with fields for 'CHART TYPE' (set to 'Bar'), 'NAME' (set to 'tt'), and 'DESCRIPTION'. Below this is the 'Data' section with 'DATA SET' (Findings), 'ENTITY' (Host Audits), and 'LIMIT' (5). It also has 'GROUP BY' (Benchmark Specification Name), 'STATS' (Count), and 'SORT FIELDS' (Count) with 'SORT ORDER' (Descending). At the bottom, there are filter options: 'Select Filters', 'Saved Filters', 'Match All', and 'Advanced'. A filter is applied: 'Benchmark Specification Name: is equ...'. A red arrow points from the text 'filter = \*deprecated\*' to this filter field. On the right is the 'Widget Preview' showing a horizontal bar chart titled 'tt'. The chart has two bars: 'Deprecated DISA Benchmark' (blue, long bar) and 'Deprecated CIS Benchmark' (dark blue, short bar). The x-axis is labeled from 0 to 3K.

## Tenable Security Center:

- Use the same approach as before with Tenable Security Center, use the Vulnerability Text field and add the Benchmark Name.
- `<cm:compliance-benchmark-name>some text here</cm:compliance-benchmark-name>`

## Benchmark Version

The benchmark version should only be used with the Benchmark Specification Name filters, and the version is unique to each benchmark and provider. For example, version 2.0.0 on a CIS Benchmark could be the latest version on one benchmark and a deprecated version on another.

## Tenable Vulnerability Management:

- Use a string with or without wildcards just as other text-based search patterns

## Tenable Security Center:

- Use the same approach as before with Tenable Security Center, use the Vulnerability Text field and add the Benchmark Version.
- Note that if you search using a regex to combine the benchmark name and version, the regex pattern must include the match for the version to come before the name and after the name.



The order of the CM elements in the Vulnerability text is not consistent, so both possible patterns should be searched.

- `<cm:compliance-benchmark-version>some text here</cm:compliance-benchmark-version>`

## Compliance Framework

Tenable audits configuration compliance with a variety of standards including GDPR, ISO 27000, HIPAA, NIST 800-53, PCI DSS, and so on. This filter allows searching based on the respective framework.

### Tenable Vulnerability Management:

- Creating a custom widget using a table or bar chart, you can quickly see the number of compliance frameworks identified by the audit files used in the scans.
- By adding other fields as filters, such as audit file, result, or benchmark, you are able to focus on the data returned.

The screenshot shows the configuration interface for a Tenable widget. On the left, the 'General' tab is active, showing 'Table' as the chart type. The 'NAME' field is empty, and the 'DESCRIPTION' field contains the text 'Compliance Framework'. Below this, the 'Data' section shows 'Findings' as the data set, 'Host Audits' as the entity, and '10' as the limit. The 'GROUP BY' field is set to 'Compliance Framework', and the 'STATS' field is set to 'Count'. The 'SORT ORDER' is set to 'Descending'. On the right, the 'Widget Preview' shows a table with the following data:

Compliance Framework	Count
LEVEL	59600
CSCv7	54733
CSF	52015
CN-L3	49931
NIAv2	48317
QCSC-v1	47575
NESA	47159
CSCv8	44478
ITSG-33	37074
800-171	36535

### Tenable Security Center:

- The “Maintaining Data Protection Controls” Cyber Exposure Study has a good section that describes how to use the Cross Reference field.
  - <https://docs.tenable.com/cyber-exposure-studies/data-protection/Content/VerifyingDataProtectionControls.htm>



- Tenable audit checks contain a reference field that points to specific controls in a standard (ISO 27001), framework (NIST Cybersecurity Framework), or regulation (HIPAA) and is used by nearly all plugins. Any external reference can be identified using the Cross References field. References can be used to search or filter in Tenable Security Center. For example, the following References define requirements for the encryption of data at rest:
  - 800-171 - 3.13.16
  - 800-53 - SC-28
- Searching with the Cross Reference Field as described in the study allows for mapping controls to the respective benchmarks. In the example below, the search pattern is 800-53|\* for all audit checks for the framework NIST 800-53r4. By clicking on the Plugin ID, a window on the right is displayed showing plugin details, including the cross references.

**Cross Reference Framework**

**Vulnerability Summary**

Vulnerabilities Web App Scanning Queries Events Mobile

4,763 Result(s) [Go to Vulnerability Detail](#) [Export](#) [Save](#) [More](#)

**Plugin ID** **Name** **Severity**

<input type="checkbox"/>	1002893	1.2 Ensure that the SharePoint Central Administration Site is TLS-enabled - HTTPS	HIGH
<input type="checkbox"/>	1002894	1.2 Ensure that the SharePoint Central Administration Site is TLS-enabled - Port 443	HIGH
<input type="checkbox"/>	1002896	1.4 Ensure that the underlying Internet Information Services (IIS) Authentication module is set to use Kerb...	HIGH
<input type="checkbox"/>	1002900	2.4 Ensure SharePoint provides the ability to prohibit the transfer of unsanctioned information in accordanc...	HIGH
<input type="checkbox"/>	1002902	2.10 Ensure that the SharePoint Online Web Part Gallery component is configured with limited access	HIGH
<input type="checkbox"/>	1002905	3.4 Ensure SharePoint identifies data type, specification, and usage when transferring information between...	HIGH
<input type="checkbox"/>	1002906	3.5 Ensure that SharePoint specific malware (i.e. anti-virus) protection software is integrated and configure...	HIGH
<input type="checkbox"/>	1002907	3.5 Ensure that SharePoint specific malware (i.e. anti-virus) protection software is integrated and configure...	HIGH
<input type="checkbox"/>	1002908	3.5 Ensure that SharePoint specific malware (i.e. anti-virus) protection software is integrated and configure...	HIGH
<input type="checkbox"/>	1002913	3.8 Ensure that On-Premise SharePoint servers is configured without OneDrive redirection linkages.	HIGH
<input type="checkbox"/>	1002915	4.2 Ensure claims-based authentication is used for all web applications and zones of a SharePoint 2016 fa...	HIGH
<input type="checkbox"/>	1002916	4.3 Ensure Windows Authentication uses Kerberos and not the NT Lan Manager (NTLM) authentication pr...	HIGH
<input type="checkbox"/>	1002917	4.4 Ensure Anonymous authentication is denied	HIGH
<input type="checkbox"/>	1002920	6.3 Ensure that SharePoint user sessions are terminated upon user logout and when the idle time limit is e...	HIGH
<input type="checkbox"/>	1002924	7.4 Ensure the SharePoint CallStack and AllowPageLevelTrace 'SafeMode' parameters are set to false - C...	HIGH
<input type="checkbox"/>	1002925	7.4 Ensure the SharePoint CallStack and AllowPageLevelTrace 'SafeMode' parameters are set to false - A...	HIGH

**Plugin Details**

PLUGIN ID: 1002896  
FAMILY: N/A  
PLUGIN NAME: 1.4 Ensure that the underlying Internet Information Services (IIS) Authentication module is set to use Kerberos as its Auth Provider

**Cross-References**

LEVEL:1NS  
CSCv6:16.9  
CSF:PR.DS-5  
800-53-SC-13  
800-171:3.13.11  
ITSG-33-SC-13  
auditFile:windows  
NESA:M5.2.6  
NESA:T7.4.1  
NIAV2:CY3  
NIAV2:CY4  
NIAV2:CY5b  
NIAV2:CY5c  
NIAV2:CY5d  
NIAV2:CY7  
NIAV2:NS5e  
IEC-27001-A.10.1.1  
QCSC-v1.6.2  
HIPAA:164.312(a)(2)(iv)  
HIPAA:164.312(e)(2)(ii)  
ITSG-33-SC-13a.  
GDPR:32.1.b  
HIPAA:164.306(a)(1)  
GDPR:32.1.a





- As mentioned in the [Key Data Fields](#) section and “Maintaining Data Protection Controls” Cyber Exposure Study, the search needs to be the full cross reference, as shown below.

**Vulnerability Summary**

Vulnerabilities Web App Scanning Queries Events Mobile

47 Result(s) Go to Vulnerability Detail Export Save More

**Cross Reference**

800-53:SC-13

Plugin ID	Name	Severity
1002838	1.4 Ensure that the underlying Internet Information Services (IIS) Authentication module is set to use Kerberos authentication	HIGH
1002916	4.3 Ensure Windows Authentication uses Kerberos and not the NT Lan Manager (NTLM) authentication protocol	HIGH
1002936	1.4 Ensure that the underlying Internet Information Services (IIS) Authentication module is set to use Kerberos authentication	HIGH
1005780	7.2 Ensure SSLv2 is disabled	HIGH
1005781	7.3 Ensure SSLv3 is disabled	HIGH
1005795	7.10 Ensure RC4 Cipher Suites is disabled - RC4 128/128	HIGH
1005797	7.12 Ensure AES 128/128 Cipher Suite is configured	HIGH
1005799	7.13 Ensure AES 256/256 Cipher Suite is enabled - Enabled	HIGH
1005786	7.5 Ensure TLS 1.0 is disabled	HIGH
1010809	Ensure 'TLS 1.0' is set for HTTPS access	HIGH
1018701	NET1638 - Management connections must be established using secure protocols with FIPS 140-2 cryptog...	HIGH

**Plugin Details**

PLUGIN ID: 1002896  
FAMILY: N/A  
PLUGIN NAME: 1.4 Ensure that the underlying Internet Information Services (IIS) Authentication module is set to use Kerberos as its Auth Provider

**Cross-References**

LEVEL:1NS  
CSCv6:16.9  
CSF:PR.DS-5  
800-53:SC-13  
800-171:3.13.11  
ITSG-33:SC-13  
auditFile:windows  
NESA:M5.2.6  
NESA:T7.4.1  
NIAv2:CY3  
NIAv2:CY4  
NIAv2:CY5b  
NIAv2:CY5c  
NIAv2:CY5d  
NIAv2:CY7  
NIAv2:NS5e

## Compliance Family Name

There are a series of designations within compliance frameworks that Tenable calls control. For example: ISO/IEC-27001:A.12.4.1, or CSF:DE.CM-1. This filter groups the controls into families for easier and more efficient queries. For example: A12 - Operations security or CSF:Detect. Use this filter in conjunction with the Compliance Framework filter.

## Tenable Vulnerability Management:

- Listed in this section is a list of the supported frameworks and the corresponding families. Much like the Compliance Control filters, the Compliance Family Name should be used with framework filters.

**Basic Mode**

**General**

CHART TYPE: Table

NAME: [REDACTED]

DESCRIPTION: [REDACTED]

**Compliance Controls**

**Data**

DATA SET: Findings

ENTITY: Host Audits

LIMIT: 20

GROUP BY: Compliance Control

STATS: First Value of Benchmark Specification Name, Count

Sort FIELDS: Compliance Control

Sort ORDER: Descending

**Widget Preview**

Compliance Control	First Value of Benchmark Specification Name	Count
A.12.6.2	CIS Debian 9	256
A.12.6.1	CIS Windows Server 2012	70
A.12.5.1	CIS Docker Community Edition	76
A.12.4.4	CIS Check Point Firewall	23
A.12.4.3	Deprecated DISA Benchmark	306
A.12.4.2	CIS Ubuntu 12.04 LTS	386
A.12.4.1	CIS Check Point Firewall	1132
A.12.3.1	DISA STIG Arista MLS DCS-7000 Series	2
A.12.2.1	CIS Debian 9	160
A.12.1.2	CIS Check Point Firewall	36

**Count of Findings**


**Compliance Framework ISO/IEC-27001**

**Compliance Family A12 - Operations security**

- This example shows the benefit of combining the various aspects of the compliance filtering, and illustrates how Tenable Vulnerability Management is able to track the compliance with several frameworks and benchmarks at the same time.

## Tenable Security Center:

- As mentioned in the [Key Data Fields](#) section and “Maintaining Data Protection Controls” Cyber Exposure Study, searching for families is accomplished by using wildcard patterns in the Cross Reference search.



Vulnerability Summary

## Vulnerability Summary

Vulnerabilities Web App Scanning Queries Events Mobile

Mitigated Cumulative

449 Result(s) [Go to Vulnerability Detail](#) [Export](#) [Save](#) [More](#)

**Cross References**

**Severity**

**Address**

**Plugin Name**

Plugin ID	Name
1006988	8.6.1 Set 'Use SmartScreen Filter' to 'Enabled:Enable'
1006990	8.7.2 Set 'Use SmartScreen Filter' to 'Enabled:Enable'
1007062	8.1.17 Set 'Allow installation of desktop items' to 'Enabled:Disable'
1007065	8.1.20 Set 'Enable MIME Sniffing' to 'Enabled:Enable'
1007091	8.3.11 Set 'Allow installation of desktop items' to 'Enabled:Disable'
1007096	8.3.16 Set 'Enable MIME Sniffing' to 'Enabled:Enable'
1007105	8.3.25 Set 'Use SmartScreen Filter' to 'Enabled:Enable'
1007123	8.4.2 Set 'Use SmartScreen Filter' to 'Enabled:Enable'
1007130	8.8.3 Set 'Use SmartScreen Filter' to 'Enabled:Enable'
1007132	8.9.2 Set 'Use SmartScreen Filter' to 'Enabled:Enable'
1007134	8.10.2 Set 'Use SmartScreen Filter' to 'Enabled:Enable'
1000833	1.3.1 Ensure AIDE is installed
1020898	WNDF-AV-000007 - Microsoft Defender AV must be configured to enable the Automatic Exclusion

**Plugin Details**

PLUGIN ID: 1007091  
FAMILY: N/A  
PLUGIN NAME: 8.3.11 Set 'Allow installation of desktop items' to 'Enabled:Disable'

**Cross-References**

CSF:PR,IP-1  
CSF:PR,PT-3  
ITSG-33:CM-7  
LEVEL:1S  
SWIFT-CSCv1:2.3  
auditFile:windows  
800-171:3.4.8  
**IEC-27001:A.12**  
NIAv2:SS13a  
TBA-FIISB:44.2.2  
TBA-FIISB:49.2.3  
QCSC-v1:3.2  
800-53:CM-7(4)  
GDPR:32.1.b  
HIPAA:164.306(a)(1)

- In this search example we are using “ISO/IEC-27001|A.12\*” to search for the family ISO/IEC-27001: A12 - Operations security.

<https://docs.tenable.com/vulnerability-management/Content/Explore/Findings/FindingsFilters.htm>



## Tenable Security Center Compliance Elements

- The compliance attributes are added to the plugin output as embedded XML elements.
- Using a grep command against a .nessus file, you can discover all the attributes in a scan result.
  - `cat host_audit_scan.nessus | grep "<cm:com" | sort | uniq | cut -d">" -f1 | uniq`
- Listed below are some of the common elements:
  - `<cm:compliance-actual-value>some text here</cm:compliance-actual-value>`
  - `<cm:compliance-audit-file>some text here</cm:compliance-audit-file>`
  - `<cm:compliance-benchmark-name>some text here</cm:compliance-benchmark-name>`
  - `<cm:compliance-benchmark-profile>some text here</cm:compliance-benchmark-profile>`
  - `<cm:compliance-benchmark-version>some text here</cm:compliance-benchmark-version>`
  - `<cm:compliance-check-id>some text here</cm:compliance-check-id>`
  - `<cm:compliance-check-name>some text here</cm:compliance-check-name>`
  - `<cm:compliance-control-id>some text here</cm:compliance-control-id>`
  - `<cm:compliance-error>some text here</cm:compliance-error>`
  - `<cm:compliance-full-id>some text here</cm:compliance-full-id>`
  - `<cm:compliance-functional-id>some text here</cm:compliance-functional-id>`
  - `<cm:compliance-info>some text here</cm:compliance-info>`
  - `<cm:compliance-informational-id>some text here</cm:compliance-informational-id>`
  - `<cm:compliance-policy-value>some text here</cm:compliance-policy-value>`
  - `<cm:compliance-reference>some text here</cm:compliance-reference>`
  - `<cm:compliance-result>some text here</cm:compliance-result>`



- `<cm:compliance-see-also>some text here</cm:compliance-see-also>`
- `<cm:compliance-solution>some text here</cm:compliance-solution>`
- `<cm:compliance-source>some text here</cm:compliance-source>`
- Using a regex pattern, you can search solutions with a keyword
  - Solution requires a firewall setting
    - regex: `compliance-solution.*[fF]irewall.*compliance-solution`
  - Solution requires a firewall setting and the firewall is not configured
    - regex: `compliance-actual-value.*NULL.*cm:compliance-actual-value.*compliance-solution.*Firewall.*compliance-solution`
- Note in both examples the regex searches for the open and close tag elements. This approach is best used to ensure there is a less likelihood of an incorrect match.
- The pluginText field is a single-line string when compared to the regex pattern. Shown in the image below is a sample pattern from the Security Center pluginText field.

```
<cm:compliance-check-name>9.3.1 Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)'</cm:compliance-check-name>\n<cm:compliance-benchmark-version>1.0.0</cm:compliance-benchmark-version>\n<cm:compliance-actual-value>NULL</cm:compliance-actual-value>\n<cm:compliance-source>custom</cm:compliance-source>\n<cm:compliance-audit-file>b56bb719-6959-5f4c-9840-4a7e9a52a64f-1710294-scfile_HR50tg</cm:compliance-audit-file>\n<cm:compliance-check-id>c1f6867c488748f381f883ed82c808c42e867f5863f990b8f79e52f900e7ebd1</cm:compliance-check-id>\n<cm:compliance-policy-value>1</cm:compliance-policy-value>\n<cm:compliance-functional-id>6061b1aa15</cm:compliance-functional-id>\n<cm:compliance-info>Select On (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select Off, Windows Firewall with Advanced Security will not use any of the firewall rules or connection security rules for this profile.\n\nThe recommended state for this setting is: On (recommended).\n\nRationale:\n\nIf the firewall is turned off all traffic will be able to access the system and an attacker may be more easily able to remotely exploit a weakness in a network service.\n\nImpact:\n\nNone - this is the default behavior.</cm:compliance-info>\n<cm:compliance-result>FAILED</cm:compliance-result>\n<cm:compliance-informational-id>c3ad6703cffc329a1ffae881958fc4c8f9596168de2ed37c78e6f7482303a25f</cm:compliance-informational-id>\n<cm:compliance-reference>800-171|3.13.1,800-171|3.13.5,800-171|3.13.6,800-53|SC-7,800-53|SC-7(5),800-53r5|SC-7,800-53r5|SC-7(5),CN-L3|7.1.2.2(c),CN-L3|8.1.10.6(j),CSCv7|9.4,CSCv8|4.5,CSF|DE.CM-1,CSF|PR.AC-5,CSF|PR.DS-5,CSF|PR.PT-4,GDPR|32.1.b,HIPAA|164.306(a)(1),ISO/IEC-27001|A.13.1.3,ITSG-33|SC-7,ITSG-33|SC-7(5),LEVEL|1A,NESA|T4.5.4,NIAv2|GS1,NIAv2|GS2a,NIAv2|GS2b,NIAv2|GS7b,NIAv2|NS25,PCI-DSSv3.2.1|1.1,PCI-DSSv3.2.1|1.2,PCI-DSSv3.2.1|1.2.1,PCI-DSSv3.2.1|1.3,PCI-DSSv4.0|1.2.1,PCI-DSSv4.0|1.4.1,QCSC-v1|5.2.1,QCSC-v1|5.2.2,QCSC-v1|6.2,QCSC-v1|8.2.1,TBA-FIISB|43.1</cm:compliance-reference>\n<cm:compliance-solution>To establish the recommended configuration via GP, set the following UI path to On (recommended):\n\nComputer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Firewall state\n\nDefault Value:\n\nOn (recommended). (The Windows Firewall with Advanced Security will be active in this profile.)</cm:compliance-solution>\n<cm:compliance-benchmark-name>CIS Microsoft Windows 11 Stand-alone Benchmark L1</cm:compliance-benchmark-name>\n<cm:compliance-control-id>0ae0803e39b6e095a01fa2313ebf05500f26481d0a32f87f3247d19bbd16ff2</cm:compliance-control-id>\n<cm:compliance-see-also>https://workbench.cisecurity.org/files/4167</cm:compliance-see-also>\n<cm:compliance-full-id>c1f6867c488748f381f883ed82c808c42e867f5863f990b8f79e52f900e7ebd1</cm:compliance-full-id>
```

- Note that the End of Line characters are stored as a “\n”, as shown here:
  - `\n<cm:compliance-source>custom</cm:compliance-source>\n`



## Benchmarks

Tenable is partnered with two major organizations which provide and maintain compliance benchmarks, the Center for Internet Security (CIS) and Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG). CIS developed a series of best practice benchmarks for a variety of applications, operating systems, servers, and databases used within organizations today. Each benchmark contains recommended security settings designed to harden systems and applications from attack while maintaining overall system functionality. Tenable has been certified by CIS to perform a wide variety of platform and application audits based on the best practice consensus benchmarks developed by CIS. Tenable submits example test cases for all of the criteria within each unique benchmark, and then submits our results to CIS personnel for official certification. Tenable has developed audit files based on the CIS Benchmarks tested on systems, and has been approved and certified by CIS staff members.

DISA's selection of Tenable as the foundation of its Assured Compliance Assessment Solution (ACAS) cements Tenable's standing as the undisputed leader in vulnerability management in the U.S. Federal government. The ACAS mission is simple: Assess DoD enterprise networks and connected IT systems against DoD standards, as well as identify any known system vulnerabilities.

For DISA and its constituents, ACAS, powered by Tenable, provides the sophistication and flexibility needed to satisfy the wide variety of security needs the Department of Defense must support, and provides the most comprehensive and integrated view of security posture to reduce risk and exceed DoD compliance. Both Tenable Security Center and Tenable Vulnerability Management support the creating, running, and importing of Policy Compliance scans.

### Tenable Security Center CIS / DISA:

Tenable Security Center's CIS and DISA reports and widgets utilize the Vulnerability Text filter to parse through the policy compliance scan results for a specific tag called "see\_also." The "see\_also" tag is present in the audit files used in the policy compliance scans used and the tag describes the benchmark that the audit file relates to. The CIS MS Server 2012 R2 Level 1 v3.0.0 audit file and the DISA STIG Oracle Linux 7 v2r14 audit file snippets show what the see\_also tag looks like.

```
<then>
  <report type:"PASSED">
    description : "CIS_MS_SERVER_2012_R2_Level_1_v3.0.0.audit from CIS Microsoft Windows Server 2012 R2 Benchmark"
    see_also    : "https://workbench.cisecurity.org/benchmarks/15273"
  </report>
```



```
<then>
  <report type:"PASSED">
    description : "DISA STIG Oracle Linux 7 v2r14 audit from DISA Oracle Linux 7 v2r14 STIG"
    see_also    : "https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_Oracle_Linux_7_V2R14_STIG.zip"
  </report>
```

Reports and widgets also use severity filters to differentiate between the three possible result types of the benchmark. A passed benchmark result carries an Info level severity while a failed benchmark result carries a High level severity. The third and last benchmark result type is Manual; these are represented using Medium level severity and are given when the benchmark test requires manual verification. When manual verification is needed the actions required to follow are in the “Steps to remediate” section of the plugin followed by an “Information” section which gives some background on the benchmark.

In the **Vulnerability Detail List View** one can also see the steps to remediate for Passed, Failed, and Manual results.



Vulnerability Summary > Vulnerability List > Vulnerability Detail List

## Vulnerability Detail List

Options

Vulnerabilities Web App Scanning Queries Events Mobile

### FFOX-00-000037 - Firefox encrypted media extensions must be disabled (1009529)

VULNERABILITY INFO

Accept Risk Recast Risk

Result 1 of 1

#### Steps to Remediate

Windows group policy: 1. Open the group policy editor tool with 'gpedit.msc'. 2. Navigate to Policy Path: Computer Configuration\Administrative Templates\Firefox\Encrypted Media Extensions Policy Name: Enable Encrypted Media Extensions Policy State: Disabled Policy Name: Lock Encrypted Media Extensions Policy State: Enabled

macOS 'plist' file: `<key>EncryptedMediaExtensions</key> <dict> <key>Enabled</key> <false/> <key>Locked</key> <true/>`

Linux 'policies.json' file: Add the following in the policies section: 'EncryptedMediaExtensions': { 'Enabled': false, 'Locked': true }

#### Audit File

DISA\_STIG\_Mozilla\_Firefox\_v6r5\_Windows.audit

#### Information

Enable or disable Encrypted Media Extensions and optionally lock it.

If 'Enabled' is set to 'false', Firefox does not download encrypted media extensions (such as Widevine) unless the user consents to installing them.

If 'Locked' is set to 'true' and 'Enabled' is set to 'false', Firefox will not download encrypted media extensions (such as Widevine) or ask the user to install them.

It is detrimental for applications to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Applications are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

Examples of non-essential capabilities include but are not limited to advertising software or browser plug-ins that are not related to requirements or provide a wide array of functionality not required for every mission but that cannot be disabled.

#### See Also

LINKS:  
[cyber.mil](#)

#### Policy Value

PASSED

#### Output

RESULT:

PASSED

OUTPUT:

All of the following must pass to satisfy this requirement:

Copy

PASSED - Enabled:  
Remote value: 0  
Policy value: 0

PASSED - Locked:  
Remote value: 1  
Policy value: 1

#### Discovery

FIRST DISCOVERED: 4 months ago

LAST OBSERVED: 4 months ago

#### Host Information

IP ADDRESS: 172.26.25.14 ( TCP )

AGENT ID: 7ceab8db-26ee-4dc8-aa86-66ce71c6d122

MAC ADDRESS: 00:50:56:a6:20:bc

REPOSITORY: Cesar's Testing

#### Asset Criticality Rating

ACR: N/A

ACR KEY DRIVERS:

internet exposure: Internal

device capability: N/A

device type: N/A

#### Asset Exposure Score

AES: 0

#### Plugin Details

PLUGIN ID: 1009529

FAMILY: N/A

#### Reference Information

CAT: II

CCI: CCI-000381

DISA\_BENCHMARK: MOZ\_Firefox\_STIG

RULE-ID: SV-251581r879587\_rule

STIG-ID: FFOX-00-000037

VULN-ID: V-251581

For results that are Passed or Failed, an Output section is at the bottom and shows the values found. For Manual verification results, represented as Medium level severity, there is no Output as the user needs to follow the Steps to Remediate to verify compliance with the benchmark.





## Tenable Vulnerability Management CIS / DISA:

Tenable Vulnerability Management Host Audit reports, chapters, and widgets utilize the Compliance Benchmark filter to search for the specific audit file or benchmark used in the scan. Compliance chapters and reports by default also filter on compliance benchmarks last observed within the last 90 days. The last observed filter means if the policy compliance scan was completed more than 90 days in the past, the result will not show up in the chapter or report being run. The **Tenable Vulnerability Management Findings View** can be used to look at compliance results easily by using the Benchmark filter.

**Findings**

Vulnerabilities Cloud Misconfigurations **Host Audits** Web Application Findings

Advanced Saved Filters Search by Agent Name, NetBios Name, DNS (FQDN), or IP Address, \* for wildcard Apply

Benchmark: is equal to CIS Ubuntu Linux 22.0... Result: is equal to Failed Reset

Filters 1,447 Host Audits Refresh

Fetch At: 10:24 AM Grid: Basic View Columns 1 to 50 of 1447 Page 1 of 29

Audit Check Name	Audit File	Result	Asset Name	State	Asset Tags	Actions
4.1.3.5 Ensure events that modify the sy...	CIS_Ubuntu_22.04_LTS_v1.0.0_Server...	Failed	ec2-54-242-230-79.comput...	New	net1: Small Group	See All details
5.5.1.4 Ensure inactive password lock is...	CIS_Ubuntu_22.04_LTS_v1.0.0_Server...	Failed	audit-2204	New		See All details
4.1.3.5 Ensure events that modify the sy...	CIS_Ubuntu_22.04_LTS_v1.0.0_Server...	Failed	audit-2204	New		See All details
4.1.3.9 Ensure discretionary access con...	CIS_Ubuntu_22.04_LTS_v1.0.0_Server...	Failed	audit-2204	New		See All details
4.1.3.10 Ensure successful file system ...	CIS_Ubuntu_22.04_LTS_v1.0.0_Server...	Failed	ubu2204desk.target.tenable...	Active	net1: site48	See All details
1.4.3 Ensure authentication required for ...	CIS_Ubuntu_22.04_LTS_v1.0.0_Server...	Failed	ip-10-20-0-162	New	net1: Small Group	See All details
3.3.7 Ensure Reverse Path Filtering is e...	CIS_Ubuntu_22.04_LTS_v1.0.0_Server...	Failed	audit-2204	New		See All details
4.2.2.5 Ensure logging is configured - 'h...	CIS_Ubuntu_22.04_LTS_v1.0.0_Server...	Failed	ec2-23-20-233-28.compute...	New	net1: Small Group	See All details
4.1.3.6 Ensure use of privileged comman...	CIS_Ubuntu_22.04_LTS_v1.0.0_Server...	Failed	ubu2204serv.target.tenable...	Active	net1: site48	See All details
3.3.1 Ensure source routed packets are ...	CIS_Ubuntu_22.04_LTS_v1.0.0_Workst...	Failed	audit-2204	New		See All details
5.3.7 Ensure access to the su command...	CIS_Ubuntu_22.04_LTS_v1.0.0_Workst...	Failed	ec2-54-236-13-189.comput...	New	net1: Small Group	See All details
5.1.9 Ensure at is restricted to authorize...	CIS_Ubuntu_22.04_LTS_v1.0.0_Server...	Failed	audit-2204	New		See All details
1.1.3.1 Ensure separate partition exists f...	CIS_Ubuntu_22.04_LTS_v1.0.0_Server...	Failed	ec2-54-242-230-79.comput...	New	net1: Small Group	See All details
1.1.2.4 Ensure nosuid option set on /tm...	CIS_Ubuntu_22.04_LTS_v1.0.0_Server...	Failed	audit-2204	New		See All details
4.1.3.16 Ensure successful and unsucc...	CIS_Ubuntu_22.04_LTS_v1.0.0_Server...	Failed	ec2-54-242-230-79.comput...	New	net1: Small Group	See All details
4.1.3.19 Ensure kernel module loading ...	CIS_Ubuntu_22.04_LTS_v1.0.0_Server...	Failed	ec2-54-242-230-79.comput...	New	net1: Small Group	See All details

The user is able to further drill within the **Findings -> Host Audits** page into the results by selecting one from the list given and then clicking on 'See All details.' This action pulls up all the details of the selected audit check.



## Findings

Last 30 Days

Vulnerabilities Cloud Misconfigurations **Host Audits** Web Application Findings

> ▾ Advanced Saved Filters Search by Agent Name, NetBios Name, DNS (FQDN), or IP Address, \* for wildcard Apply

Benchmark: is equal to CIS Ubuntu Linux 22.0... Last Audited: within last 30 days State: is equal to Active, Resurfaced, New Reset

Audit Check Name	Audit File	Result	Asset Name	State	Asset Tags	Actions
<input type="checkbox"/> 1.1.1.1 Ensure mounting of cramfs filesystems is ...	CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.test...	✓ Passed	ip-10-20-0-162	New	net1: Small Group	
<input type="checkbox"/> 1.1.1.1 Ensure mounting of cramfs filesystems is ...	CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.test...	✗ Failed	audit-2204	New		
<input type="checkbox"/> 1.1.1.1 Ensure mounting of cramfs filesystems is ...	CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit	✗ Failed	audit-2204	New		
<input type="checkbox"/> 1.1.1.1 Ensure mounting of cramfs filesystems is ...	CIS_Ubuntu_22.04_LTS_v1.0.0_Workstation_L1...	✗ Failed	audit-2204	New		
<input type="checkbox"/> 1.1.1.1 Ensure mounting of cramfs filesystems is ...	CIS_Ubuntu_22.04_LTS_v1.0.0_Workstation_L1...	✓ Passed	ip-10-20-0-162	New	net1: Small Group	

### 1.1.1.1 Ensure mounting of cramfs filesystems is disabled

See All Details

#### Asset Information

NAME audit-2204  
IPV4 ADDRESS 172.26.24.239  
NETWORK Default

#### Asset Scan Information

FIRST SEEN 03/20/2024 at 10:56 AM  
LAST SEEN 03/20/2024 at 11:01 AM  
LAST AUTHENTICATED SCAN 03/20/2024 at 11:01 AM  
LAST LICENSED SCAN 03/20/2024 at 11:01 AM  
SOURCE [Nessus Scan](#)

#### Host Audit Information

AUDIT CHECK NAME 1.1.1.1 Ensure mounting of  
cramfs filesystems is disabled  
AUDIT FILE CIS\_Ubuntu\_22.04\_LTS\_v1.0.  
0\_Server\_L1.test-2.audit  
BENCHMARK CIS Ubuntu Linux 22.04 LTS  
v1.0.0  
BENCHMARK SPECIFICATION NAME CIS Ubuntu Linux 22.04 LTS  
BENCHMARK VERSION 1.0.0  
CONTROL ID dbe8c33f9830ce3a6ab966544  
337e6eb7cdfb240bf570708f22  
87ac327de781f  
PLUGIN NAME Unix Compliance Checks  
RESULT ✗ Failed  
STATE NEW  
SOURCE [custom](#)

#### Overview Audit Output

##### Policy Value

```
cmd: multiple line script
dont_echo_cmd: NO
expect: \*\* PASS \*\*
system: Linux
```

##### Actual Value

The command script with multiple lines returned :

```
-- INFO --
- module: "cramfs" exists in:
  - "/lib/modules/5.15.0-69-generic/kernel/fs"
  - "/lib/modules/5.15.0-84-generic/kernel/fs"
- Audit Result:
  ** FAIL **
```

Within the **Finding Details** page, a user is able to view all relevant information about the selected audit check. The Solution section is present for all result types and can be used to correct any failed audit checks as well as manually verify checks that were neither passed or failed.



[← Back to Findings](#)

## 1.71 Ensure message of the day is configured properly - banner

HOST AUDITS **ERROR**

### Description

The contents of the /etc/motd file are displayed to users after login and function as a message of the day for authenticated users.

Unix-based systems have typically displayed information about the OS release and patch level upon logging in to the system. This information can be useful to developers who are developing [More](#)

### Audit File

CIS\_Ubuntu\_22.04\_LTS\_v1.0.0\_Workstation\_L1.audit

### Solution

Edit the /etc/motd file with the appropriate contents according to your site policy, remove any instances of m, r, s, v or references to the OS platform OR if the motd is not used, this file can be removed. Run the following command to remove the motd file:

[More](#)

### See Also

<https://workbench.cisecurity.org/files/4068>

Previous Next Actions ⌵

### Result ⓘ

**Error**

### Finding State ⓘ

**New**

### Host Audit Information

AUDIT CHECK NAME	1.7.1 Ensure message of the day is configured properly - banner
AUDIT FILE	CIS_Ubuntu_22.04_LTS_v1.0.0_Workstation_L1.audit
BENCHMARK	CIS Ubuntu Linux 22.04 LTS v1.0.0
BENCHMARK SPECIFICATION NAME	CIS Ubuntu Linux 22.04 LTS
BENCHMARK VERSION	1.0.0
CONTROL ID	c08b92939fe7306dbee1f942e462368ce464d83df3fd71ef6c326d4030b5ba15
PLUGIN NAME	Unix Compliance Checks
RESULT	<b>Error</b>
STATE ⓘ	<b>NEW</b>
SOURCE	<b>custom</b>

### Audit Discovery

FIRST SEEN	03/20/2024 at 10:56 AM
LAST AUDIT	03/20/2024 at 10:56 AM

### Asset Affected

[View Asset Details](#) ⓘ

#### Asset Information

ASSET ID	d1808abf-ddd1-4088-9301-8ab305e9b14d
NAME	audit-2204
IPV4 ADDRESS	172.26.24.239
PUBLIC	No

#### Asset Scan Information

FIRST SEEN	03/20/2024 at 10:56 AM
LAST SEEN	03/20/2024 at 11:01 AM
LAST AUTHENTICATED SCAN	03/20/2024 at 11:01 AM
LAST LICENSED SCAN	03/20/2024 at 11:01 AM
SOURCE	<a href="#">Nessus Scan</a>

#### Additional Information

NETWORK	Default
MAC ADDRESS	00:50:56:a6:03:43
TENABLE ID	0db3b8cf9557427ab2d084b92dac912d

#### Policy Value

No Output

#### Actual Value

No Output



---

## Compliance Frameworks

---

In response to increased cyberthreats, governments are enacting mandates and legislation. For example, in the U.S., Executive Order 14028 focuses on improving the security of the software supply chain. In the European Union, the Cyber Resilience Act – published by the European Commission in September 2022 – looks to ensure hardware and software products are placed on the market with fewer vulnerabilities. Such measures not only place new requirements on government agencies, they extend broadly to the organizations these agencies do business with, including cloud service providers, software development organizations, software as a service (SaaS) providers, hardware manufacturers, and virtually any organization creating digital products and services.

The legislative and regulatory changes in the U.S. are not limited to the federal government – they’re also cascading down to state and local governments. Likewise, in addition to the E.U. regulations, nations within the union may also have their own requirements. In the United States, for example, 36 states have enacted new cybersecurity laws in the past two years, with many more in the works as the public sector looks to mitigate the risk of cyberthreats.

Adding to government regulations, industries have also begun to define their own mandates in an effort to improve security posture and minimize risk to consumers and investors. One example of this is PCI DSS in the payment card industry.

For the security teams that must implement these mandates, the challenge is in translating what are often general legislative guidelines and controls into specific policies, tools, and processes. Further, security teams are responsible for enforcing those policies in a scalable and consistent way across the enterprise. For security teams working in multinational enterprises, these challenges are compounded exponentially.

The regulatory environment impacts all aspects of cybersecurity, including traditional IT infrastructure and operational technology. In order to understand how the regulatory environment affects cloud security, you first need an understanding of which regulations apply to your particular business. The table below highlights several regulations with broad sweeping cloud security implications – and the risks that come with non-compliance. Regulations and penalties with cloud security implications.

### CIS Critical Security Controls v8 (CSCv8)



Origin: On May 18, 2021 CIS published version 8 of their Critical Security Controls and they provide specific and actionable ways to protect against today's most pervasive and dangerous attacks.

Requirement: The Critical Security Controls are created for organizations of any size or sector.

TVM Compliance Family	TSC Cross Reference
Inventory and Control of Enterprise Assets	CSCv8 1.*
Inventory and Control of Software Assets	CSCv8 2.*
Data Protection	CSCv8 3.*
Secure Configuration of Enterprise Assets and Software	CSCv8 4.*
Account Management	CSCv8 5.*
Access Control Management	CSCv8 6.*
Continuous Vulnerability Management	CSCv8 7.*
Audit Log Management	CSCv8 8.*
Email and Web Browser Protections	CSCv8 9.*
Malware Defenses	CSCv8 10.*
Data Recovery	CSCv8 11.*
Network Infrastructure Management	CSCv8 12.*
Network Monitoring and Defense	CSCv8 13.*
Security Awareness and Skills Training	CSCv8 14.*
Service Provider Management	CSCv8 15.*
Application Software Security	CSCv8 16.*
Incident Response Management	CSCv8 17.*

## General Data Protection Regulation (GDPR)



Origin: Approved by the European Union in 2016, GDPR looks to enforce data protection guidelines for the collection and processing of personal information for anyone living in the European Union.

Requirement: Applies to any entity with a website that attracts European visitor traffic, whether that entity is actively marketing to EU residents or not. Data breaches must be reported within 72 hours.

TVM Search Pattern: Compliance Framework = GDPR

TVM Compliance Family	TSC Cross Reference
32 Security of processing	GDPR 32.*

## Health Insurance Portability and Accountability Act (HIPAA)

Origin: Passed by the U.S. Congress, the intent of the HIPAA Privacy Rule is to limit the use and disclosure of electronically protected healthcare information (ePHI), such as medical records, without explicit authorization by individuals.

Requirement: The regulation applies to healthcare providers, health plans, and healthcare clearinghouses that conduct healthcare transactions electronically.

TVM Search Pattern: Compliance Framework = HIPAA

TVM Compliance Family	TSC Cross Reference
164.306 Security standards: General rules	HIPAA 164.306*
164.308 Administrative safeguards	HIPAA 164.308*
164.312 Technical safeguards	HIPAA 164.312*

## ISO/IEC 27001

Origin: Many organizations, especially multinationals, have chosen to utilize ISO/IEC 27001/27002 frameworks to help them continually identify security gaps, comply with numerous compliance requirements and obtain international certification.

Requirement: The ISO 27001, a broadly recognized standard for information security management systems (ISMS). While not directly provided by ISO, organizations can obtain third-party certification of compliance with ISO 27001.

TVM Search Pattern: Compliance Framework = ISO/IEC-27001



TVM Compliance Family	TSC Cross Reference
A 6 - Organization of information security	ISO/IEC-27001 A.6.*
A 8 - Asset management	ISO/IEC-27001  A.8.*
A 9 - Access control	ISO/IEC-27001  A.9.*
A10 - Cryptography	ISO/IEC-27001  A.10.*
A11 - Physical and environmental security	ISO/IEC-27001  A.11.*
A12 - Operations security	ISO/IEC-27001  A.12.*
A13 - Communications security	ISO/IEC-27001  A.13.*

## IT Security Risk Management: A Lifecycle Approach (ITSG-33)

Origin: Released in November 2012, the ITSG-33 publication describes the roles, responsibilities, and activities that help (Government of Canada) GC departments manage IT security risks.

Requirement: The ITSG-33 was developed as a series of guidelines for security practitioners to manage information technology (IT) security risks for Government of Canada (GC) information systems.

Search Pattern: Compliance Framework =

TVM Compliance Family	TSC Cross Reference
CONFIGURATION MANAGEMENT	ITSG-33 CM*
AUDIT AND ACCOUNTABILITY	ITSG-33 AU*
MEDIA PROTECTION	ITSG-33 MP*
SYSTEM AND SERVICES ACQUISITION	ITSG-33 SA*
MAINTENANCE	ITSG-33 MA*
SECURITY ASSESSMENT AND AUTHORIZATION	ITSG-33 CA*
SYSTEM AND COMMUNICATIONS	ITSG-33 SC*



PROTECTION	
IDENTIFICATION AND AUTHENTICATION	ITSG-33 IA*
SYSTEM AND INFORMATION	ITSG-33 SI*
CONTINGENCY PLANNING (CONTINUITY PLANNING)	ITSG-33 CP*
RISK ASSESSMENT	ITSG-33 RA*
ACCESS CONTROL	ITSG-33 AC*
INCIDENT RESPONSE	ITSG-33 IR*
AWARENESS AND TRAINING	ITSG-33 AT*

## Payment Card Industry Data Security Standard (PCI DSS)

Origin: Released in December 2004, PCI DSS was an industry-led initiative created to better manage cardholder data and reduce credit card fraud. The Standard was defined by the PCI Security Standards Council (PCI SSC), which includes American Express, Visa, MasterCard, Discover, and others.

Requirement: While not a federal regulation, the industry standard is mandatory for all entities that store, process, and/or transmit cardholder data. The standard includes specific cloud computing guidelines which provide guidance on the use of cloud technologies and for maintaining controls in cloud environments.

TVM Compliance Family	TSC Cross Reference
Build and Maintain a Secure Network and Systems	PCI-DSSV4.0 1.*
Protect Account Data	PCI-DSSV4.0 3.*
Maintain a Vulnerability Management Program	PCI-DSSV4.0 5.*
Implement Strong Access Control Measures	PCI-DSSV4.0 7.*
Regularly Monitor and Test Networks	PCI-DSSV4.0 10*





## NIST Cyber Security Framework (CSF)

Origin: Developed by the National Institute of Standards and Technology (NIST), the NIST Cybersecurity Framework (CSF) is composed of best practice guidelines to help organizations identify, implement, and enhance their cybersecurity practices and use a common language to communicate issues to stakeholders.

Requirement: All federal government agencies and any federal contractors handling government data must be NIST-compliant. Contractors that fail to meet NIST compliance (or have a history of NIST non-compliance) risk losing future contracts.

TVM Compliance Family	TSC Cross Reference
Protect	CSF PR.*
Respond	CSF RS.*
Recover	CSF RC.*
Detect	CSF DE.*
Identify	CSF ID.*

## NIST SP 800-171

Origin: NIST Special Publication 800-171, Protecting Controlled Unclassified Information (CUI) in Nonfederal Information Systems and Organizations, defines the type of security requirements service providers are likely to be contractually obligated to.

Requirement: The U.S. Government must safeguard Controlled Unclassified Information (CUI) and Covered Defense Information. Consequently, civilian agencies and the DoD contractually obligate many nonfederal organizations that process, store, or transmit protected information to comply with NIST SP 800-171. These nonfederal service providers must monitor and assess SP 800-171 controls to obtain permission to operate and safeguard CUI on an ongoing basis.

TVM Compliance Family	TSC Cross Reference
3. 1 ACCESS CONTROL	800-171 3.1.*
3. 2 AWARENESS AND TRAINING	800-171 3.2.*



3. 3 AUDIT AND ACCOUNTABILITY	800-171 3.3.*
3. 4 CONFIGURATION MANAGEMENT	800-171 3.4.*
3. 5 IDENTIFICATION AND AUTHENTICATION	800-171 3.5.*
3. 6 INCIDENT RESPONSE	800-171 3.6.*
3. 7 MAINTENANCE	800-171 3.7.*
3. 8 MEDIA PROTECTION	800-171 3.8.*
3.11 RISK ASSESSMENT	800-171 3.11.*
3.12 SECURITY ASSESSMENT	800-171 3.12.*
3.13 SYSTEM AND COMMUNICATIONS PROTECTION	800-171 3.13.*
3.14 SYSTEM AND INFORMATION INTEGRITY	800-171 3.14.*

## NIST SP 800-53r5

Origin: The NIST 800-53 provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations.

Requirement: Most U.S. federal information systems must base their security and privacy controls in NIST Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations. However, compliance is not limited to the federal government. Many other organizations are required to comply with SP 800-53.

TVM Compliance Family	TSC Cross Reference
AWARENESS AND TRAINING	800-53 AT*
INCIDENT RESPONSE	800-53 IR*
RISK ASSESSMENT	800-53 RA*
ACCESS CONTROL	800-53 AC*
IDENTIFICATION AND AUTHENTICATION	800-53 IA*



SYSTEM AND COMMUNICATIONS PROTECTION	800-53 SC*
CONTINGENCY PLANNING	800-53 CP*
MAINTENANCE	800-53 CA*
SECURITY ASSESSMENT AND AUTHORIZATION	800-171 3.11.*
SYSTEM AND SERVICES ACQUISITION	800-53 SA*
PLANNING	800-53 PL*
CONFIGURATION MANAGEMENT	800-53 CM*
AUDIT AND ACCOUNTABILITY	800-53 AU*
MEDIA PROTECTION	800-53 MP*
PROGRAM MANAGEMENT	800-53 PM*
SYSTEM AND INFORMATION INTEGRITY	800-53 SI*

Fortunately, a number of federal and industry sponsored organizations have been established to help enterprise and government organizations improve their cybersecurity posture. These organizations collect best practices and define risk frameworks, as well as supporting cybersecurity controls and benchmarks.

Frameworks provide a set of processes, best practices, and specifications to help organizations assess and manage risk. They lay the foundation for effective cybersecurity programs.

Controls identify ‘what should happen’ in order to mitigate a specific category of risk. Inventory of software assets, data protection, and secure configuration are examples of control categories. Each control category has a set of safeguards outlining what steps should be taken.

Benchmarks take the concept of controls to the next level, providing prescriptive guidance on how to implement and configure specific technology, such as cloud instances, applications, and identities, in a secure way.

In Tenable Vulnerability Management, a user is able to filter their compliance data by compliance framework by using the **Compliance Framework** filter.

tenable

Vulnerability Management

[Explore Overview](#)
[Findings](#)

Quick Actions

?

CE

Findings

Vulnerabilities

Cloud Misconfigurations

Host Audits

Web Application Findings

Advanced

Saved Filters

Search by Agent Name, NetBios Name, DNS (FQDN), or IP Address, \* for wildcard

Apply

Compliance Framework: is equal to GDPR

Result: is equal to Failed

Reset

Filters

10,531 Host Audits

Refresh

Fetch At: 10:08 AM

Grid: Basic View

Columns

1 to 50 of 10531

Page 1 of 211

Audit Check Name	Audit File	Result	Asset Name	State	Asset Tags	Actions
18.9.11.2.12 Ensure 'Configure use of p...	CIS_Microsoft_Windows_10_Stand-alo...	Failed	WIN1064	Active	net1: Small ... +2	
RHEL-08-010671 - RHEL 8 must disabl...	DISA_STIG_Red_Hat_Enterprise_Linux...	Failed	rhel8.target.tenablesecurity...	New	net1: site48	
Internet Explorer Processes - FEATUR...	MSCT_Windows_Server_2016_MS_v1....	Failed	WIN2016	New	net1: os cody 1 +1	
18.8.34.6.6 Ensure 'Require a passwor...	CIS_Microsoft_Windows_10_Stand-alo...	Failed	WIN11	Active	net1: site48	
18.10.15.8 Ensure 'Toggle user control o...	139311d6-6d34-500d-8fc1-d6e806b4ac...	Failed	sms.in.reach.com	New		
4.1.3.10 Ensure successful file system ...	CIS_Ubuntu_22.04_LTS_v1.0.0_Server...	Failed	ubu2204desk.target.tenable...	Active	net1: site48	
6.2.6 Ensure users' home directories pe...	CIS_Ubuntu_20.04_LTS_v1.0.0_Server...	Failed	ubuntu2004desk.target.tena...	Active	net1: site48	
WN12-CC-000048 - Copying of user inp...	DISA_STIG_Server_2012_and_2012_R...	Failed	ORACLE11G	New	net1: os cody 1 +2	
WN12-CC-000134 - The system must b...	DISA_STIG_Server_2012_and_2012_R...	Failed	ORACLE11G	New	net1: os cody 1 +2	
2.2.17 Ensure 'Deny log on as a batch j...	CIS_Microsoft_Windows_10_Stand-alo...	Failed	WIN1064	Active	net1: Small ... +2	
1.3.1 Ensure AIDE is installed - aide-co...	CIS_Ubuntu_18.04_LTS_Server_v2.1.0...	Failed	172.26.31.219	New		
Use Pop-up Blocker - Restricted Sites Z...	MSCT_Windows_Server_2016_MS_v1....	Failed	WIN2016	New	net1: os cody 1 +1	
WN12-SO-000021 - The machine inacti...	DISA_STIG_Server_2012_and_2012_R...	Failed	ORACLE11G	New	net1: os cody 1 +2	
SYMP-AG-000190 - Symantec ProxySG...	DISA_STIG_Symantec_ProxySG_ALG...	Failed	bluecoatproxysg.lab.tenable...	New	net1: site0	
Allow only approved domains to use the...	MSCT_Windows_Server_2016_MS_v1....	Failed	ORACLE12G	New	net1: os cody 1 +2	
1.1.2 Ensure only trusted users are allo...	CIS_Docker_v1.6.0_L1_Docker_Linux.a...	Failed	audit-docker-ee-2	New		

Select Filters

Reset

Compliance Framework

is equal to

GDPR

Find Result

Failed

Error

Info

Passed

Skipped

Unknown

Warning

The Compliance Framework filter looks at the **Reference Information** section of the finding to determine which frameworks the audit check is related to.

tenable

Vulnerability Management

[Explore Overview](#)
[Findings](#)
[Finding Details](#)

Quick Actions

?

CE

[Back to Findings](#)

Network access: Let Everyone permissions apply to anonymous users

HOST AUDITS PASSED

Previous

Next

Actions

Description

Network access: Let Everyone permissions apply to anonymous users

This security setting determines what additional permissions are granted for anonymous connections to the computer.

More

Audit File

MSCT\_Windows\_Server\_2016\_MS\_v1.0.0.audit

Solution

Policy Path: Local Policies\Security Options

Policy Name: Network access: Let Everyone permissions apply to anonymous users

See Also

<https://blogs.technet.microsoft.com/secguide/2016/10/17/security-baseline-for-windows-10-v1607-anniversary-edition-and-windows-server-2016/>

Reference Information

800-171	3.1.7
800-53	AC-6(10)
800-53R5	AC-6(10)
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.8(a)
CSCV6	14
CSCV6	16
CSF	PR.AC-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAPV2	AM1
NIAPV2	AM23f
NIAPV2	SS13c
NIAPV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
SWIFT-CSCV1	5.1
TBA-FISIR	31.4.2

Asset Affected

View Asset Details

Asset Information

ASSET ID	230f2108-4483-45d0-8a3b-9e183b6ebff
NAME	SQL2016
IPV4 ADDRESS	172.26.48.14
OPERATING SYSTEM	Microsoft Windows
SYSTEM TYPE	general-purpose
PUBLIC	No

Asset Scan Information

FIRST SEEN	01/04/2022 at 09:05 PM
LAST SEEN	03/25/2024 at 08:28 PM
LAST AUTHENTICATED SCAN	03/25/2024 at 10:53 AM
LAST LICENSED SCAN	03/25/2024 at 08:28 PM
SOURCE	NM Nessus Scan

Additional Information

NETWORK	Default
DNS (FQDN)	sql2016.target.tenablesecurity.com
TENABLE ID	4f023c4accf049d3831a07c18e583e9
INSTALLED SOFTWARE	cpe:/a:microsoft:sql_server:13.0.4001.0

Policy Value

0

Actual Value

0



In Tenable Security Center, a user is able to filter their compliance data by compliance framework by using the **Cross References** filter.

The screenshot shows the Tenable Security Center interface for the Vulnerability List. The sidebar on the left contains filters for Cross References and Severity. The Cross References filter is highlighted with a red box and shows 'GDPR' selected. The Severity filter shows 'High' selected. The main table displays 4,520 results, with the first 10 rows visible, all showing a severity of 'HIGH'.

Plugin ID	Pl...	Family	Severity	VPR	IP Address	ACR	AES	N...	DNS	M...	Port	Protocol	Re.
1006959	1...	N/A	HIGH		172.26.25.75	4	0			00...	0	TCP	C
1006961	1...	N/A	HIGH		172.26.25.75	4	0			00...	0	TCP	C
1006962	1...	N/A	HIGH		172.26.25.75	4	0			00...	0	TCP	C
1006963	1...	N/A	HIGH		172.26.25.75	4	0			00...	0	TCP	C
1006967	1...	N/A	HIGH		172.26.25.75	4	0			00...	0	TCP	C
1007012	2...	N/A	HIGH		172.26.25.75	4	0			00...	0	TCP	C
1007021	2...	N/A	HIGH		172.26.25.75	4	0			00...	0	TCP	C
1007025	2...	N/A	HIGH		172.26.25.75	4	0			00...	0	TCP	C
1007026	2...	N/A	HIGH		172.26.25.75	4	0			00...	0	TCP	C
1007027	2...	N/A	HIGH		172.26.25.75	4	0			00...	0	TCP	C
1007032	2...	N/A	HIGH		172.26.25.75	4	0			00...	0	TCP	C
1007053	2...	N/A	HIGH		172.26.25.75	4	0			00...	0	TCP	C
1007054	2...	N/A	HIGH		172.26.25.75	4	0			00...	0	TCP	C
1007055	2...	N/A	HIGH		172.26.25.75	4	0			00...	0	TCP	C

Each of the audit file types has a corresponding plugin ID; however, in Tenable Security Center, the audit file plugin ID is not used. In Security Center when you install an audit file, a new plugin higher than plugin ID 1000000 is created for each check. To retain the audit file type, there is a cross reference called "auditFile." In the Reference Information of the Vulnerability Detail List tool, you can see the auditFile value. When adding a filter for the audit file type, the XREF Type, left side of the pipe (|), is the auditFile type. To the right of the pipe (|), the XREF ID is placed. For example, "auditFile|bluecoat" would locate any audit check used to audit a Bluecoat configuration. There are currently 47 auditFile types:



## Discovery

FIRST DISCOVERED: Today

LAST OBSERVED: Today

## Host Information

IP ADDRESS: 172.26.25.122 ( TCP )

AGENT ID: e0089e39-18f5-49c9-bb9e-d7a86956bdc5

DNS: desktop-bbdnfc3.lab.tenablesecurity.com

REPOSITORY: Individual Scan


## Asset Criticality Rating

ACR: N/A 

ACR KEY DRIVERS:

 internet exposure: Internal

 device capability: N/A

 device type: N/A

## Asset Exposure Score

AES: 0

## Plugin Details

PLUGIN ID: 1007017

FAMILY: N/A

## Reference Information

LEVEL: 1A

CROSS REFERENCES: GDPR:32.1.b, HIPAA:164.306(a)(1), 800-171:3.1.9, TBA-FIISB:45.2.4, 800-53:AC-8, ITSG-33:AC-8, NESA:M1.3.6, LEVEL:1A, auditFile:windows, 800-53r5:AC-8



It is important to note that when looking at the cross references in the Vulnerability details section, the cross reference appears to be separated using a colon (GDPR:32.1b); to search for this specific cross reference you would replace the colon with a pipe (GDPR|32.1b).



VulnerabilitiesCloud MisconfigurationsHost AuditsWeb Application Findings

< ⌵AdvancedSaved Filters 🔽Search by Agent Name, NetBios Name, DNS (FQDN), or IP Address, \* for wildcard

Compliance Framework: is equal to 800-53 ✕Plugin Name: is equal to Windows Compliance... ✕Result: is equal to Failed ✕Reset

Filters

Apply

Select FiltersReset

▼ Compliance Framework ⌵

is equal to

800-53

▼ Plugin Name ⌵

is equal to

Windows Compliance Checks

▼ Result ⌵

Find Result

☒ Failed

☐ 5,613 Host AuditsRefresh

Fetches At: 03:18 PMGrid: Basic View ▼

Audit Check Name	Audit File	Result	Plugin Name
<input type="checkbox"/> 18.9.11.2.12 Ensure 'Confi...	CIS_Microsoft_Windows_1...	<input checked="" type="radio"/> Failed	Windows Compliance Checks
<input type="checkbox"/> Internet Explorer Processe...	MSCT_Windows_Server_2...	<input checked="" type="radio"/> Failed	Windows Compliance Checks
<input type="checkbox"/> 18.8.34.6.6 Ensure 'Requir...	CIS_Microsoft_Windows_1...	<input checked="" type="radio"/> Failed	Windows Compliance Checks
<input type="checkbox"/> 18.10.15.8 Ensure 'Toggle ...	139311d6-6d34-500d-8fc1-...	<input checked="" type="radio"/> Failed	Windows Compliance Checks
<input type="checkbox"/> WN12-CC-000048 - Copyi...	DISA_STIG_Server_2012_...	<input checked="" type="radio"/> Failed	Windows Compliance Checks
<input type="checkbox"/> WN12-CC-000134 - The sy...	DISA_STIG_Server_2012_...	<input checked="" type="radio"/> Failed	Windows Compliance Checks
<input type="checkbox"/> 2.2.17 Ensure 'Deny log on...	CIS_Microsoft_Windows_1...	<input checked="" type="radio"/> Failed	Windows Compliance Checks
<input type="checkbox"/> Use Pop-up Blocker - Restr...	MSCT_Windows_Server_2...	<input checked="" type="radio"/> Failed	Windows Compliance Checks
<input type="checkbox"/> WN12-SO-000021 - The m...	DISA_STIG_Server_2012_...	<input checked="" type="radio"/> Failed	Windows Compliance Checks
<input type="checkbox"/> Allow only approved domai...	MSCT_Windows_Server_2...	<input checked="" type="radio"/> Failed	Windows Compliance Checks
<input type="checkbox"/> 2.3.11.4 Ensure 'Network s...	CIS_MS_SERVER_2012_...	<input checked="" type="radio"/> Failed	Windows Compliance Checks
<input type="checkbox"/> Configure local setting over...	MSCT_Windows_Server_2...	<input checked="" type="radio"/> Failed	Windows Compliance Checks
<input type="checkbox"/> 18.5.20.1 Ensure 'Configur...	CIS_Microsoft_Windows_1...	<input checked="" type="radio"/> Failed	Windows Compliance Checks

- 40 -







## Compliance Summary (Explore)

All Jump to Dashboard Dashboards Share Export More

### Compliance by Benchmark Category

	Passed	Failed	Other
CIS	29.9K	19.5K	3.5K
DISA	4.9K	5.3K	2.1K
MSCT	1.8K	2.3K	63
NIST	0	0	0
Other Sources	7.7K	7.7K	1.2K

### Compliance Summary by Framework

Compliance Frame...	Reference Count	All Value of Result
LEVEL	56678	<div><div></div></div>
CSCv7	51599	<div><div></div></div>
CSF	49217	<div><div></div></div>
CN-L3	47605	<div><div></div></div>
QCSC-v1	45433	<div><div></div></div>
CSA	44910	<div><div></div></div>

### Compliance Result Summary by Plugins

Plugin Name	Count	All Value of Result
Unix Compliance C...	53168	<div><div></div></div>
Windows Complian...	26456	<div><div></div></div>
Cisco IOS Complia...	2398	<div><div></div></div>
Palo Alto Networks...	496	<div><div></div></div>
Fortigate FortiOS ...	221	<div><div></div></div>
OpenShift Compla...	403	<div><div></div></div>

### Audit File Result Summary



### Compliance Checks Summary

Audit Check Name	Count	All Value of Result
1.7.4 Ensure permissions on /etc/...	92	<div><div></div></div>
1.7.5 Ensure permissions on /etc/...	81	<div><div></div></div>
1.7.6 Ensure permissions on /etc/...	81	<div><div></div></div>
1.9 Ensure updates, patches, and ...	74	<div><div></div></div>
4.2.1.1 Ensure rsyslog is installed	73	<div><div></div></div>
6.2.1 Ensure accounts in /etc/pass...	72	<div><div></div></div>
1.1.5.2 Ensure nodev option set o...	67	<div><div></div></div>
6.2.3 Ensure all groups in /etc/pas...	67	<div><div></div></div>
1.1.5.3 Ensure noexec option set ...	67	<div><div></div></div>

There are 58 available Compliance check plugins. All the possible Compliance check plugins can be seen by using [Tenable's Plugins Search](#) and searching for "Compliance Checks" and using the "Policy Compliance" Family filter.

## Plugins Search

Compliance Checks

Filters (1)

Relevance

Family (1)

Clear All

<< Previous

Page 1 of 2 • 58 Total

Next >>

ID	Name	Product	Family	Published	Updated	Severity
109580	Office 365 Compliance Checks (deprecated)	Nessus	Policy Compliance	6/30/2016	1/25/2023	INFO
161406	OpenShift Compliance Checks	Nessus	Policy Compliance	6/1/2022	3/19/2024	INFO
33814	Database Compliance Checks	Nessus	Policy Compliance	10/13/2008	3/29/2024	INFO
148944	PostgreSQL DB Compliance Checks	Nessus	Policy Compliance	10/24/2022	3/19/2024	INFO
62680	Juniper Junos Compliance Checks	Nessus	Policy Compliance	10/31/2012	3/29/2024	INFO



A more detailed breakdown of Host Audit Plugin Types can be seen by navigating to the Widget Library and selecting the **Host Audit Plugin Type Group**. This action results in currently 62 widgets, four widgets come from the Compliance Summary dashboard and the other 58 widgets represent each of the 58 available compliance check plugins. Each of the 58 Compliance check widgets are laid out as a matrix and display benchmark run on the y-axis labels of the matrix, and the result types on the x axis. The counts inside the matrices represent the count of the specific result type for the benchmark which was selected.

Widget Library

Latest

New Custom Widget

Back to Dashboards

< >

Search Widgets

Groups

All

My Widgets

New and Updated (879)

Vulnerability Management

Web Application Scanning

Lumin

Host Audit

Center for Internet Security

Compliance Framework

DISA STIG

Host Audit Plugin Type

Tenable Best Practice Audits

Vendor Based Audits

Host Audit Plugin Type

62 Widgets

Grid

List

Page 1 of 4

Audit Benchmarks Collected using OpenShift Container Platform C...  
Updated 3/21/2024

	PASSED	WARNING	FAILED	ERROR
CIS Redhat OpenShift Container Platform 4 v1.4.0	91	87	10	0
Operating Systems and applications Redhat OpenShift Container Platform 4 v1.3.0 UI	87	66	7	0
CIS Redhat OpenShift Container Platform 4 v1.3.0 UI	0	42	0	2
Operating Systems and applications Redhat OpenShift Container Platform 4 v1.3.0 UI	20	10	3	0

Audit Benchmarks Collected using Huawei VRP Checks (Explore)  
Updated 3/21/2024

Vulnerabilities By State

	EXPLOITED	CRITICAL	HIGH	MEDIUM
New	12	12	12	12
Active	12	12	12	12
Pending	12	12	12	12
Resolved	12	12	12	12

Most Prevalent Vulnerabilities Discovered in The Last 14 Days

100 Vulnerabilities

Top 100 Vulnerabilities With Patch Available More Than 120 Days

PLUGINS	NAME	SEVERITY	HOST TOTAL	AT-RISK	AGE	VALUE TOTAL	VULNERABILITIES
87246	MS17-010 Security Update - Windows Microsoft...	Critical	4	168.1.1.12	N/A	19	
63542	MS17-010 Security Update - Windows Microsoft...	Critical	3	168.1.1.31	N/A	17	
63544	MS17-010 Security Update - Windows Microsoft...	Critical	3	168.1.1.32	N/A	16	
64570	MS17-010 Security Update - Windows Microsoft...	Critical	3	168.1.1.29	N/A	15	

Audit Benchmarks Collected using SonicWALL SonicOS Checks (Ex...  
Updated 3/21/2024

	FAILED	PASSED	WARNING
TNS SonicWALL v5.0 v2.0.0	79	17	5

Audit Benchmarks Collected using Windows File Contents Checks (E...  
Updated 3/21/2024

Operating Systems and Applications File Analysis - Social Security Number (Firestorm) v1.0 UI	1
---	---

Within Tenable Security Center there are 47 Available Compliance Plugins that can be queried. All the available compliance plugins are below; the text in the parenthesis is the reader-friendly name of the plugin so, for example, when querying the plugin you'll want to use 'oracledb' for Oracle DB.

adtran (Adtran NetVanta)	mongodb (MongoDB)
alcatel (Alcatel TiMOS)	ms_sqldb (MS SQL DB)
amazon_aws (Amazon AWS)	mysqldb (MySQL DB)
arista (Arista EOS)	netapp (NetApp Data ONTAP)
arubaos (ArubaOS)	netapp_api (Netapp API)

- 43 -



as/400 (IBM iSeries)	openshift (OpenShift Container Platform)
bluecoat (BlueCoat ProxySG)	oracledb (Oracle DB)
brocade (Brocade FabricOS)	ovalUnix (OVAL Unix)
checkpoint (Check Point GAIa)	ovalWindows (OVAL Windows)
cisco (Cisco IOS)	palo_alto (Palo Alto Networks PAN-OS)
cisco_aci (Cisco ACI)	postgresqldb (PostgreSQL DB)
cisco_firepower (Cisco Firepower)	rhev (RHEV)
citrix_application_delivery (Citrix Application Delivery)	scapLinux (SCAP Linux)
database (Database)	scapWindows (SCAP Windows)
extreme_extremexos (Extreme ExtremeXOS)	sonicwall (SonicWALL SonicOS)
f5 (F5 Networks)	sybasedb (Sybase DB)
fortigate (Fortigate FortiOS)	watchguard (WatchGuard)
genericssh (Generic SSH)	windows (Windows)
hprocurve (HP ProCurve)	windowsfiles (Windows File Contents)
huawei (Huawei VRP)	xenserver (Citrix XenServer)
ibm_db2db (IBM DB2 DB)	zte_rosng (ZTE ROSNG)
juniper (Juniper Junos)	

When trying to have a specific query unix and 800-53 benchmarks run, one would think utilizing the Cross Reference filter with 'auditFile|unix, 800-53|\*' would work but this would not. The Cross Reference filter has an implied 'OR' operator to it. The above example would result in all unix audit file benchmarks as well as all benchmarks that have 800-53 as a reference including non-unix audit files. In this scenario we want to utilize the two filters;

**The Cross References Filter and the Vulnerability Text Filter.**



Apply

[+ Customize](#) [✕ Clear All](#)

Load Query

## Cross References

=

auditFileWindows

## Plugin Type

☐ Active☒ Compliance☐ Event☐ Passive☐ WAS

## Vulnerability Text

Regex Match

cm:compliance-reference.\*800-53.\*cm:compliance-reference

1,466 Result(s)

[Go to Vulnerability Detail](#)

Plugin ID

Name

[1008422](#)

WNDF-AV-000007 - Microsoft

[1008424](#)

WNDF-AV-000009 - Microsoft

[1008425](#)

WNDF-AV-000010 - Microsoft

[1008426](#)

WNDF-AV-000011 - Microsoft

[1008440](#)

WNDF-AV-000025 - Microsoft

[1008441](#)

WNDF-AV-000026 - Microsoft

[1008442](#)

WNDF-AV-000027 - Microsoft

[1008445](#)

WNDF-AV-000030 - Microsoft

[1008446](#)

WNDF-AV-000031 - Microsoft

[1008447](#)

WNDF-AV-000031 - Microsoft

[1008448](#)

WNDF-AV-000040 - Microsoft

[1008449](#)

WNDF-AV-000040 - Microsoft

[1008450](#)

WNDF-AV-000041 - Microsoft

[1008451](#)

WNDF-AV-000041 - Microsoft

[1008452](#)

WNDF-AV-000042 - Microsoft



Why the Cross References Filter for Windows audit files and not the framework? The Cross References filter is used for the 'auditFile|Windows' and a Regex Match paired with Vulnerability Text Filter to look for the tag 'cm:compliance-reference.\*800-53.\*cm:compliance-reference.' This query grabs all the Benchmark results that use a Windows Audit file and are related to the framework 800-53. It is important to note that while we can do 'auditFile|Windows' in the Cross References Filter and cm:compliance-reference.\*800-53.\*cm:compliance-reference' in the Vulnerability Text Filter, we cannot do the inverse; this would look like '800-53|\*' in the Cross References Filter and cm:compliance-reference.\*auditFile|Windows.\*cm:compliance-reference.' The latter query would not result in anything as the plugin text does not include the 'auditFile' tag and instead the tag is inside of the 'xref' tag within the scan. In the Tenable Security Center Compliance Elements section some of the most common compliance elements are listed for ease of use in any regex query.

An example of a similar query is present in compliance reports and components. Inside the reports or components, the filters being used consistently are the Plugin Type and Vulnerability Text filters. In the following example, from the **CIS Windows Server 2012 v3.0.0** Report template, shows a table which shows results that have names starting with 1.1 (Plugin Name with regex match of ^1.1) that are Compliance Plugin Type, have failed (Severity equal to 'High'), and looks inside the vulnerability text to determine if the result originates from a CIS Windows Server 2012 v3.0.0 audit (the 'see\_also' tag is a direct reference to the audit on CIS' website).



## Data

TYPE Vulnerability ▾

QUERY *Select a Query* ▾

SOURCE Cumulative ▾

TOOL Vulnerability Summary - IP ... ▾

### FILTERS

Plugin Name	Regex Match ^1.1.
-------------	-------------------

Plugin Type	Compliance
-------------	------------

Severity	High
----------	------

Vulnerability Text	Contains <cm:compliance-see-also>https://workbench.cisecurity.org/benchmarks/15290</cm:compliance-see-also>
--------------------	---

[+ Add Filter](#)



---

## Vendor-Based Audits

---

Apart from DISA and CIS benchmarks Tenable also offers the support of audits based on vendors. Some of the Vendor Based Audits tenable provides are: VMware, Juniper, IBM, Microsoft Security Compliance Toolkit (MSCT), and more. The creation of these audit files originates from these vendors create guides or best practices based on some of their products. This is evident when opening and looking at the first description lines of the audit files. For example, in the Juniper Hardening Junos Devices audit file the description reads:

*# Description: This audit is based on the checklist for the book*

*# "This Week: Hardening Junos Devices, Second Edition"*

*# by John Weidley, available at <http://www.juniper.net/dayone>*

The description mentions where the audit checks come from and if available =, the description also provides a link where the user can get more information on the topic.

Tenable Vulnerability Management splits the Vendor-Based Audits into two sections in the **Template Library**.





## Groups

All

My Widgets

New and Updated (879)

Vulnerability Management

Web Application Scanning

Lumin

---

### Host Audit

---

Center for Internet Security

Compliance Framework

DISA STIG

Host Audit Plugin Type

Tenable Best Practice Audits

Vendor Based Audits

Tenable Best Practice Audits include those benchmarks which were created by Tenable based on best practice guides of vendors. Within the Vendor-Based Audits section there are templates for benchmarks like the MSCT, which have been created based on baselines set by the vendor.



MSCT is a set of tools that allows enterprise security administrators to download, analyze, test, edit, and store Microsoft-recommended security configuration baselines for Windows and other Microsoft products. Tenable creates MSCT audit files that perform a detailed configuration review for these benchmarks. When scanning assets utilizing the appropriate MSCT audit file, the organization is able to perform detailed configuration checks. Tenable Vulnerability Management is able to perform a wide variety of platform and application audits based on the best practice consensus benchmarks developed by using these audit files. If more information is needed on auditing MSCT Baselines, this blog post provides more MSCT context.

In the other sections the Cross References and Vulnerability Text Filters have been mentioned and shown off to show how one could query their compliance data based on framework, plugin type, and frameworks like CIS or DISA; Vendor-Based Audit and Tenable Best Practice templates utilize the **Compliance Benchmark Filter**.

## Findings

[Vulnerabilities](#) [Cloud Misconfigurations](#) [Host Audits](#) [Web Application Findings](#)

< 🔍

Advanced

Saved Filters ▾

Search by Agent Name, NetBios Name, DNS (FQDN), or IP Address, \* for wildcard

Benchmark: is equal to TNS\*, MSCT\* x

Result: is equal to Failed x

Reset

Filters

Apply

Select Filters

Reset

▼ Benchmark

is equal to ▾

TNS\*, MSCT\*

▼ Result

Find Result

☒ Failed

☐ Error

☐ Info

☐ Passed

☐ Skipped

☐ Unknown

☐ Warning

☐ 2,568 Host Audits

Refresh

	Audit Check Name	Audit File	Result
<input type="checkbox"/>	Do not allow drive redirection	MSCT_Windows_11_v1.0.0.test-1...	Failed
<input type="checkbox"/>	Internet Explorer Processes - FEAT...	MSCT_Windows_11_v23H2_v1.0.0...	Failed
<input type="checkbox"/>	Internet Explorer Processes - FEAT...	MSCT_Windows_Server_2016_MS...	Failed
<input type="checkbox"/>	Use Pop-up Blocker - Restricted Sit...	MSCT_Windows_Server_2016_MS...	Failed
<input type="checkbox"/>	Allow only approved domains to us...	MSCT_Windows_Server_2016_MS...	Failed
<input type="checkbox"/>	Configure local setting override for ...	MSCT_Windows_Server_2016_MS...	Failed
<input type="checkbox"/>	Configure RPC connection settings...	MSCT_Windows_11_v23H2_v1.0.0...	Failed
<input type="checkbox"/>	Set document behavior if file valida...	MSCT_Office_2016_v1.0.0.test-1.a...	Failed
<input type="checkbox"/>	Navigate URL - powerpnt.exe	MSCT_Office_2016_v1.0.0.test-1.a...	Failed
<input type="checkbox"/>	Turn on SmartScreen Filter scan - ...	MSCT_Windows_Server_2016_MS...	Failed
<input type="checkbox"/>	Object Caching Protection - excel.exe	MSCT_Office_2016_v1.0.0.test-1.a...	Failed
<input type="checkbox"/>	Turn On Virtualization Based Secur...	MSCT_Windows_Server_2016_MS...	Failed
<input type="checkbox"/>	Extreme : SNMP community name ...	TNS_ExtremeXOS_Best_Practice....	Failed



The benchmark filter within the Host Audits section of the Findings page can be used to find any benchmark by entering in the name, though the benchmark filter is also the best way to query all of Vendor Based Audits and/or Tenable Best Practice audits. The filter operator used in the screenshot above is equal too but the filter accepts an asterisk (\*) to represent all characters after the given string. For example, “TNS\*” would query every Benchmark with “TNS” in the start of the name. This behavior is the same as regular expression, though if you wanted to do multiple searches one would query something similar to the above (“TNS\*, MSCT\*). The search in the screenshot uses a comma to act as an OR within the query, this behavior results in all benchmarks matching the first value OR the other value coming up in one query search.

This query is also possible in Tenable Security Center by utilizing the Vulnerability Text Filter with a regular expression, as shown in the **Vulnerability Summary Tool** example.

### Vulnerability Summary

[Vulnerabilities](#) [Web App Scanning](#) [Queries](#) [Events](#) [Mobile](#)

▼

Apply

+ Customize

✕ Clear All

Load Query

▼ Plugin Type

☐ Active

☒ Compliance

☐ Event

☐ Passive

☐ WAS

> Severity

▼ Vulnerability Text

Regex Match

cm:compliance-benchmark-name.\*(TNS|MSCT).\*cm:compliance-benchmark-name

350 Result(s)

[Go to Vulnerability Detail](#) [Export](#) [Save](#) [More](#)

1 to 50 of 350

<input type="checkbox"/>	Plugin ID	Name	Severity
<input type="checkbox"/>	1005079	Ensure 'Password Policy' is enabled - minimum-length	HIGH
<input type="checkbox"/>	1005083	Ensure 'aaa local authentication max failed attempts' is set to less than or equal to '3'	HIGH
<input type="checkbox"/>	1005086	Ensure 'SSH source restriction' is set to an authorized IP address	HIGH
<input type="checkbox"/>	1005087	Ensure 'TLS 1.0' is set for HTTPS access	HIGH
<input type="checkbox"/>	1005088	Ensure 'console session timeout' is less than or equal to '5' minutes	HIGH
<input type="checkbox"/>	1005089	Ensure 'HTTP session timeout' is less than or equal to '5' minutes	HIGH
<input type="checkbox"/>	1005094	Ensure 'syslog hosts' is configured correctly	HIGH
<input type="checkbox"/>	1005096	Ensure 'logging buffer size' is greater than or equal to '524288' bytes (512kb)	HIGH
<input type="checkbox"/>	1005097	Ensure 'logging buffered severity' is greater than or equal to '3'	HIGH
<input type="checkbox"/>	1005110	Ensure 'noproxyarp' is enabled for untrusted interfaces	HIGH
<input type="checkbox"/>	1005115	Ensure DNS services are configured correctly - name-server	HIGH
<input type="checkbox"/>	1005116	Ensure intrusion prevention is enabled for untrusted interfaces	HIGH
<input type="checkbox"/>	1005120	Ensure 'ip verify' is set to 'reverse-path' for untrusted interfaces	HIGH
<input type="checkbox"/>	1005081	Ensure 'Failover' is enabled	HIGH
<input type="checkbox"/>	1005090	Ensure timezone is properly configured	HIGH

In the example above we use a Regex Match with the Vulnerability Text Filter and set the text as `cm:compliance-benchmark-name.*(TNS|MSCT).*cm:compliance-benchmark-name`. The compliance benchmark name is what we target in the query to determine the name and filter out results. In the example above the text uses a pipe (|) as an OR operator to query any benchmark names with TNS OR MSCT in their name.

- 51 -



---

## Learn More

---

### Tenable Resources

- [Auditing Microsoft Security Compliance Toolkit Baselines](#)
- [Plugins Search](#)
- [Tenable Vulnerability Management Findings Filters](#)
- [Tenable Security Center \(6.3\) Vulnerability Analysis Filter Components](#)
- [Audits Documentation](#)
- [Compliance Checks Reference](#)

### Compliance References

- [CIS CSCv8 - CIS Critical Security Controls Version 8](#)
- [GDPR - General Data Protection Regulation](#)
- [HIPAA - Health Insurance Portability and Accountability Act](#)
- [PCI-DSS - Payment Card Industry Data Security Standard \(PCI DSS\)](#)
- [ITSG-33 - IT Security Risk Management: A Lifecycle Approach \(ITSG-33\)](#)
- [800-171 - NIST SP 800-171](#)
- [CSF - NIST Cyber Security Framework \(CSF\)](#)