nessus file analyzer

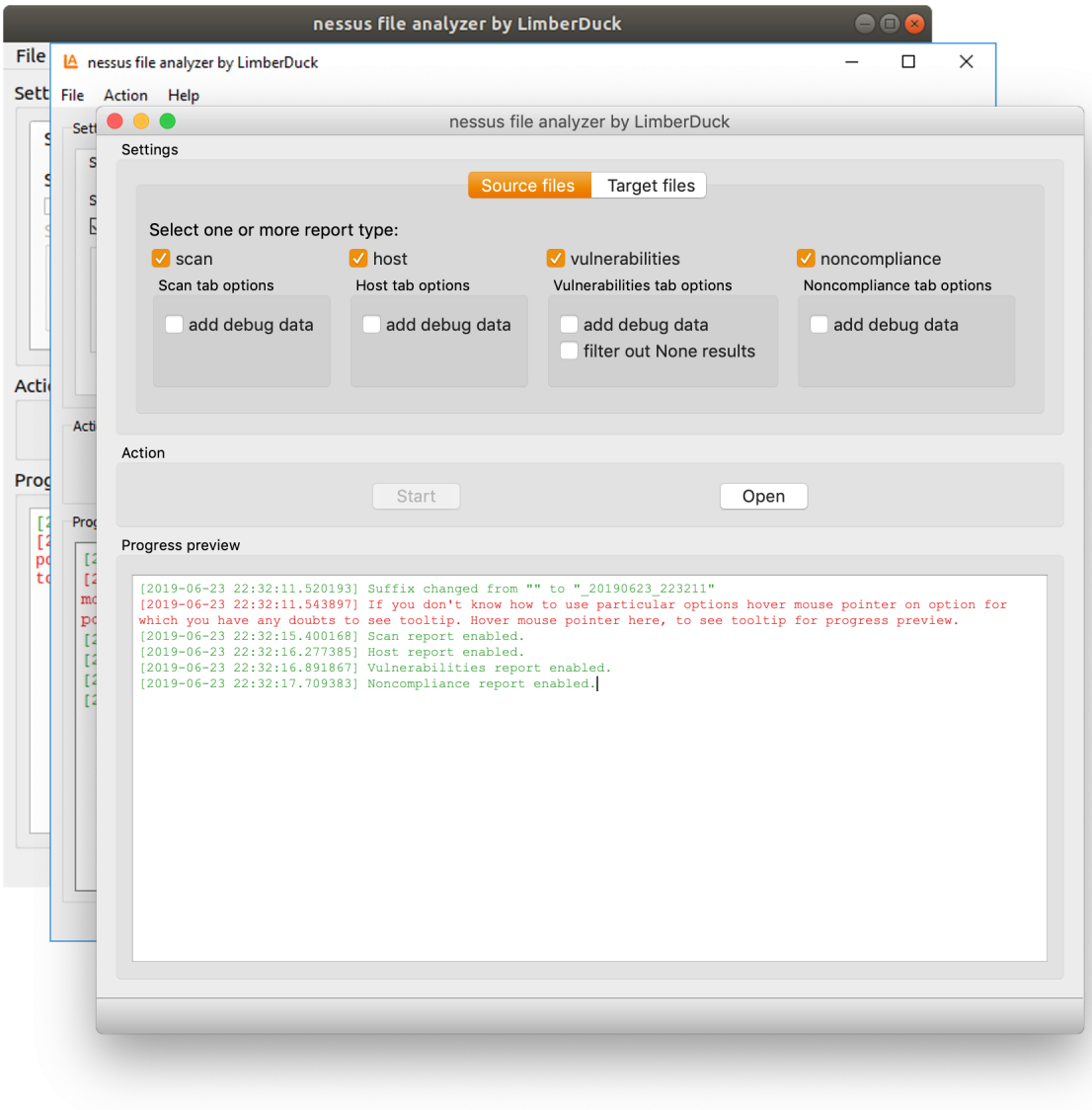
Release 0.6.0

May 13, 2022

Table of contents

nessus file analyzer by LimberDuck (pronounced *lm.b dk*) is a GUI tool which enables you to parse multiple nessus files containing the results of scans performed by using Nessus by (C) Tenable, Inc. and exports parsed data to a Microsoft Excel Workbook for effortless analysis.

Operational memory usage will be kept low while parsing even the largest of files. You can run it on your favourite operating system, whether it is Windows, macOS or GNU Linux. As a parsing result, you will receive spreadsheets with a summary view of the whole scan and/or all reported hosts. You will also be able to generate spreadsheets with a detailed view of all reported vulnerabilities and/or noncompliance. It's free and open source tool, which has been created to automate our work, decrease our workload and focus on data analysis.



Go through the first steps to quickly start using NFA (nessus-file-analyzer by Limberduck).

CHAPTER 1

Getting started

1.1 Run nessus file analyzer

Run NFA using python or prepare executable file as described in *Installation instructions*.

1.2 Open nessus files

You have five possibilities to open your nessus files in NFA, here they are.

OPTION 1 - by opening file-s

1. Open NFA.
2. Go to Menu *File*.
3. Choose *Open file-s* if you want to open one or more nessus files at once.

OPTION 2 - by opening directory

1. Open NFA.
2. Go to Menu *File*.
3. Choose *Open directory* if you want to open all nessus files from selected directory and its subdirectories.

OPTION 3 - by use of OS contextual menu

1. On OS (Operating System) level select one or more nessus files in your OS file browser.
2. Click RMB (Right Mouse Button) on selected file-s and choose from contextual menu option *Open with...*.
3. Choose NFA to open selected file-s.

OPTION 4 - by file-s Drag & Drop

1. On OS level select one or more nessus files in your OS file browser.
2. Simple drag and drop selected file-s on NFA window.

OPTION 5 - by directory Drag & Drop

1. On OS level select one or more directories containing nessus files in your OS file browser.
2. Simple drag and drop selected directory or directories on NFA window.

1.3 Select report type

Select one or more report types: scan, host, vulnerabilities, noncompliance.

1. **Select report type:**
    - `scan` - if you want to see sum-up from point of view of the whole scan.

        See also:

        Check *Scan section* description to get more details.
    - `host` - if you want to see sum-up from point of view of particular scanned host.

        See also:

        Check *Host section* description to get more details.
    - `vulnerabilities` - if you want to see list of vulnerabilities reported in this scan for all scanned hosts.

        See also:

        Check *Vulnerabilities section* description to get more details.
    - `noncompliance` - if you want to see list of noncompliance reported in this scan for all scanned hosts.

        See also:

        Check *Noncompliance section* description to get more details.
2. Play with NFA settings to fit target file to your exact needs.

    See also:

    Check *Settings details* to get more details.

1.4 Initialize analyze

Click `Start` button to initiate analyze of all provided nessus files.

1.5 Open target file

Click `Open` button to open target directory where output file has been saved.

CHAPTER 2

Settings details

Settings are divided into two tabs, separately for source files and target files, as follows.

2.1 Source files

Here are the options available for source files:

All report types:

- `add debug data` - turn on this option to get additional columns for selected report type like source file name with path, policy name and more.

  Note: Text in debug's columns headers is in blue color in the target file to let you quickly distinguish them from default columns.

  See also:

  Check *Target file sections* descriptions to get more details.

Vulnerability report type:

- `filter out None results` - turn on this option to automatically filter out plugins results with None Risk Factor and see in the target file only these which Risk Factor is equal to Low, Medium, High or Critical.

  Note: Plugins results with None Risk Factor are not removed from target file, to see them use filter option in column named *Risk Factor*.

- `skip None results` - turn on this option to completely skip plugins results with None Risk Factor and left in the target file only these which Risk Factor is equal to Low, Medium, High or Critical.

Note: To see plugins results with None Risk Factor in target file you need to disable this option and analyse selected files again.

2.2 Target files

Here are the options available for target files:

- `Change` button - click to change target directory and use it for generated output files.

  Note: `Change` button is placed next to target directory field.

- `set source directory as target directory` turn on this option to automatically change target directory each time when you select new source file/-s and set target directory to be the same as source file/-s directory.

  Note: If you use *Open directory* option to open source files this directory will be taken as target directory for all files including these from subdirectories.

- `add suffix with "_YYYYMMDD_HHMMSS"` - turn on this option to add suffix into target filename with date and time in format `_YYYYMMDD_HHMMSS`.

  Note: Take a look below this option to see example target filename received that way.

  If you already turned on `add custom suffix` option, turn it off and on again to change the sequence of these two options in target file name.

- `add custom suffix` - turn on this option if you want to add suffix into target filename which will contain text taken from field placed on the right side from this option.

  Note: Take a look below this option to see target filename example received that way.

  If you already turned on `add suffix with "_YYYYMMDD_HHMMSS"` option, turn it off and on again to change the sequence of these two options in target file name.

CHAPTER 3

Installation instructions

Note: It's advisable to use python virtual environment for below instructions. Read more about python virtual environment in The Hitchhiker's Guide to Python!

Read about virtualenvwrapper in The Hitchhiker's Guide to Python!: virtualenvwrapper provides a set of commands which makes working with virtual environments much more pleasant.

3.1 Installation

1. Install **nessus file analyzer**

   ```
   pip install nessus-file-analyzer
   ```

   Note: To upgrade to newer version run:

   ```
   pip install -U nessus-file-analyzer
   ```

2. Run **nessus file analyzer**

   ```
   nessus-file-analyzer
   ```

   Tip: Optionally for Linux and macOS:

   ```
   nessus-file-analyzer&
   ```

   Run with `&` at the end to start the process in the background.

3. Make a shortcut for **nessus file analyzer**

   Windows:

- Run in cmd `where nessus-file-analyzer.exe`
- Copy returned path.
- Go to e.g. to Desktop.
- Right click on Desktop and choose `New > Shortcut`.
- Paste returned path.
- Click `Next`, `Finish`.

Linux (Ubuntu) / macOS

- Run in Terminal `which nessus-file-analyzer`
- Run in Terminal `ln -s path_returned_in_previous_command ~/Desktop/`

macOS

- Run in Terminal `which nessus-file-analyzer`
- Open `bin` folder where `nessus-file-analyzer` is located.
- Right click on `nessus-file-analyzer` and choose `Make alias`.
- Move your alias e.g. to Desktop.

3.1.1 Additional steps

3.1.1.1 Linux (Ubuntu)

If you installed without python virtual environment, and you see below error:

```
~$ nessus-file-analyzer
nessus-file-analyzer: command not found
```

Add below to `~/.bashrc`

```
# set PATH so it includes user's private ~/.local/bin if it exists
if [ -d "$HOME/.local/bin" ] ; then
    PATH="$HOME/.local/bin:$PATH"
fi
```

If you see below error:

```
~$ nessus-file-analyzer
qt.qpa.plugin: Could not load the Qt platform plugin "xcb" in "" even though it was␣
↪found.
This application failed to start because no Qt platform plugin could be initialized.␣
↪Reinstalling the application may fix this problem.

Available platform plugins are: eglfs, linuxfb, minimal, minimalegl, offscreen, vnc,␣
↪wayland-egl, wayland, wayland-xcomposite-egl, wayland-xcomposite-glx, webgl, xcb.

Aborted (core dumped)
```

Run below to fix the error:

```
sudo apt-get install --reinstall libxcb-xinerama0
```

3.2 Build executable file

3.2.1 Windows

1. Clone **nessus file analyzer** repository using below command in Git Bash:

```
git clone https://github.com/LimberDuck/nessus-file-analyzer.git
```

2. Install requirements using below command

```
pip install -r .\requirements.txt
```

3. Run **nessus file analyzer** using below command

```
python -m nessus_file_analyzer
```

4. Upgrade setuptools using below command

```
pip install --upgrade setuptools
```

5. Install PyInstaller

```
pip install PyInstaller
```

6. Build your own executable file using below command

```
pyinstaller --onefile --windowed --version-file=.\version.rc --icon=.
↪\icons\LimberDuck-nessus-file-analyzer.ico  --name nessus-file-analyzer␣
↪nessus_file_analyzer\__main__.py
```

7. Go to `dist` catalog to find executable file `nessus-file-analyzer.exe`

3.2.2 Linux (Ubuntu)

1. Clone **nessus file analyzer** repository using below command

```
git clone https://github.com/LimberDuck/nessus-file-analyzer.git
```

2. Install requirements using below command

```
pip install -r ./requirements.txt
```

3. Run **nessus file analyzer** using below command

```
python -m nessus_file_analyzer
```

4. Upgrade setuptools using below command

```
pip install --upgrade setuptools
```

5. Install PyInstaller

```
pip install PyInstaller
```

6. Build your own executable file using below command

```
~/.local/bin/pyinstaller --onefile --windowed --icon=./icons/LimberDuck-
↪nessus-file-analyzer.ico --name nessus-file-analyzer nessus_file_
↪analyzer\__main__.py
```

7. Go to `dist` catalog to find executable file `nessus-file-analyzer`.

3.2.3 macOS

1. Clone **nessus file analyzer** repository using below command

```
git clone https://github.com/LimberDuck/nessus-file-analyzer.git
```

2. Install requirements using below command

```
pip3.6 install -r ./requirements.txt
```

3. Run **nessus file analyzer** using below command

```
python -m nessus_file_analyzer
```

4. Upgrade setuptools using below command

```
pip install --upgrade setuptools
```

5. Install PyInstaller

```
pip install PyInstaller
```

6. Build your own executable file using below command

```
pyinstaller --onefile --windowed --icon=./icons/LimberDuck-nessus-file-
↪analyzer.ico --name nessus-file-analyzer nessus_file_analyzer\__main__.
↪py
```

7. Go to `dist` catalog to find executable file `nessus-file-analyzer`.

CHAPTER 4

Target file sections

Generated target file can consist of up to four sections:

- `scan` - sum-up from point of view of the whole scan.

  See also:

  Check *Scan section* description to get more details.

- `host` - sum-up from point of view of particular scanned host.

  See also:

  Check *Host section* description to get more details.

- `vulnerabilities` - list of vulnerabilities reported in this scan for all scanned hosts.

  See also:

  Check *Vulnerabilities section* description to get more details.

- `noncompliance` - list of noncompliance reported in this scan for all scanned hosts.

  See also:

  Check *Noncompliance section* description to get more details.

4.1 Scan section

Here you will find all details about data visible in target file in *Scan* section.

Table 1: Column details explanation

Header name	Column name.
Description	Short description for particular data.
Source	Information about exact source from where data is being taken.
Post-processing	Information how the gathered data is processed, if post-processed at all.
Column type	`default` - column always appears in report. `debug` - column appears in report only if `add debug data` option has been enabled.

Note: Some of the columns are visible only if you use `add debug data` option for analysis (see *Settings details* to adhere more information about this option). For all of these columns you will find below information **Column type** : `debug`.

4.1.1 Nessus scan name

Table 2: Nessus scan name - column details

Header name	Nessus scan name
Description	Scan name given by user during scan setting up.
Source	nessus file > `Report/name`
Post-processing	*none*
Column type	`debug`

4.1.2 Nessus file name

Table 3: Nessus file name - column details

Header name	Nessus file name
Description	Nessus file name assigned during the file downloading.
Source	nessus file
Post-processing	Absolute path of the given file.
Column type	`debug`

4.1.3 nessus file size

Table 4: nessus file size - column details

Header name	nessus file size
Description	Nessus file size in human readable format, e.g. b, B, KiB, MiB, GiB.
Source	nessus file
Post-processing	Converting from bytes to human readable format.
Column type	`debug`

4.1.4 Target hosts

Table 5: Target hosts - column details

Header name	Target hosts
Description	Number of target hosts given by user during scan setting up.
Source	nessus file > `Preferences/ServerPreferences/preference/[name='TARGET']/value`
Post-processing	1. Value split by comma `,`. 2. Text changed to lowercase. 3. If nessus file comes from Tenable.sc string `[ip]` is removed from corresponding target. 4. If nessus file comes from Tenable.sc IP ranges in corresponding target is converted into separate IP addresses.
Column type	`debug`, `default`

4.1.5 Target hosts (without duplicates)

Table 6: Target hosts (without duplicates) - column details

Header name	Target hosts (without duplicates)
Description	Number of distinct values from the list of target hosts.
Source	nessus file > `Preferences/ServerPreferences/preference/[name='TARGET']/value`
Post-processing	The same as for *Target hosts*
Column type	`debug`, `default`

4.1.6 Scanned hosts

Table 7: Scanned hosts - column details

Header name	Scanned hosts
Description	Number of all ReportHost items listed in provided nessus file.
Source	nessus file > `ReportHost`
Post-processing	*none*
Column type	`debug`, `default`

4.1.7 Scanned hosts with credentialed checks

Table 8: Scanned hosts with credentialed checks - column details

Header name	Scanned hosts with credentialed checks
Description	Number of all ReportHost items listed in provided nessus file where Plugin ID 10506 "Nessus Scan Information" output contains `Credentialed checks : yes`.
Source	nessus file > `ReportHost/ReportItem/[pluginID="19506"]/plugin_output`
Post-processing	*none*
Column type	`debug`, `default`

See also:

Read more about this plugin on Tenable website https://www.tenable.com/plugins/nessus/19506

4.1.8 Unreachable hosts

Table 9: Unreachable hosts - column details

Header name	Unreachable hosts
Description	Number of target hosts left after subtracting of scanned hosts list from target hosts list.
Source	nessus file > `Preferences/ServerPreferences/preference/[name='TARGET']/value` - `ReportHost`
Post-processing	*none*
Column type	`debug`, `default`

4.1.9 Scan started

Table 10: Scan started - column details

Header name	Scan started
Description	Exact date and time when scan of the first host has been initiated.
Source	nessus file > `ReportHost/HostProperties/tag/[@name='HOST_START']`
Post-processing	Date and time returned in format `%a %b %d %H:%M:%S %Y`.
Column type	`debug`, `default`

4.1.10 Scan ended

Table 11: Scan ended - column details

Header name	Scan ended
Description	Exact date and time when scan of the last host has been ended.
Source	nessus file > `ReportHost/HostProperties/tag/[@name='HOST_END']`
Post-processing	Date and time returned in format `%a %b %d %H:%M:%S %Y`.
Column type	`debug`, `default`

4.1.11 Elapsed time per scan

Table 12: Elapsed time per scan - column details

Header name	Elapsed time per scan
Description	Duration of the entire scan, based on subtraction Scan Start Time of first host scanned from Scan End Time of last host scanned.
Source	nessus file > `ReportHost/HostProperties/tag/[@name='HOST_END']` - `ReportHost/HostProperties/tag/[@name='HOST_START']`
Post-processing	Elapsed time returned in format `HH:MM:SS`.
Column type	`debug`, `default`

4.1.12 Policy name

Table 13: Policy name - column details

Header name	Policy name
Description	Policy name selected by user during scan setting up.
Source	nessus file > `Policy/policyName`
Post-processing	*none*
Column type	`debug`

4.1.13 Login used

Table 14: Login used - column details

Header name	Login used
Description	Login name used during scan of reported host.
Source	nessus file > `ReportHost/HostProperties/tag/[@name='login-used']`
Post-processing	*none*
Column type	`debug`, `default`

4.1.14 DB SID

Table 15: DB SID - column details

Header name	DB SID
Description	Database SID set by user during scan setting up.
Source	nessus file > `Preferences/PluginsPreferences/item/[fullName='Database settings[entry]:Database SID :']/selectedValue`
Post-processing	*none*
Column type	`debug`, `default`

4.1.15 DB port

Table 16: DB port - column details

Header name	DB port
Description	Database port set by user during scan setting up.
Source	nessus file > `Preferences/PluginsPreferences/item/[fullName='Database settings[entry]:Database port to use :']/selectedValue`
Post-processing	*none*
Column type	`debug`, `default`

4.1.16 Reverse lookup

Table 17: Reverse lookup - column details

Header name	Reverse lookup
Description	Information if option *Settings* > *Report* > *Output* > *'Designate hosts by their DNS name'* has been turned on in policy used during scan.
Source	nessus file > `Preferences/ServerPreferences/preference/[name='reverse_lookup']/value`
Post-processing	*none*
Column type	`debug`

4.1.17 Max hosts

Table 18: Max hosts - column details

Header name	Max hosts
Description	Value set for Max simultaneous hosts per scan in policy used during scan.
Source	nessus file > `Preferences/ServerPreferences/preference/[name='max_hosts']/value`
Post-processing	*none*
Column type	`debug`

4.1.18 Max checks

Table 19: Max checks - column details

Header name	Max checks
Description	Value set for Max simultaneous checks per host in policy used during scan.
Source	nessus file > `Preferences/ServerPreferences/preference/[name='max_checks']/value`
Post-processing	*none*
Column type	`debug`

4.1.19 Network timeout

Table 20: Network timeout - column details

Header name	Network timeout
Description	Value set for Network timeout (in seconds) in policy used during scan.
Source	nessus file > `Preferences/ServerPreferences/preference/[name='checks_read_timeout']/value`
Post-processing	*none*
Column type	`debug`

4.1.20 Used plugins

Table 21: Used plugins - column details

Header name	Used plugins
Description	Number of all plugins used during scans.
Source	nessus file > `Preferences/ServerPreferences/preference/[name='plugin_set']/value`
Post-processing	Value split by semicolon `;`.
Column type	`debug`

4.1.21 ALL plugins

Table 22: ALL plugins - column details

Header name	ALL plugins
Description	Number of reported plugins for all hosts in scan.
Source	nessus files > `ReportHost/ReportItem`
Post-processing	*none*
Column type	`debug`, `default`

4.1.22 Critical plugins

Table 23: Critical plugins - column details

Header name	Critical plugins
Description	Number of reported plugins for all hosts in scan with Critical Risk Factor.
Source	nessus file > `ReportHost/ReportItem/risk_factor/"Critical"`
Post-processing	*none*
Column type	`debug`, `default`

4.1.23 High plugins

Table 24: High plugins - column details

Header name	High plugins
Description	Number of reported plugins for all hosts in scan with High Risk Factor.
Source	nessus file > `ReportHost/ReportItem/risk_factor/"High"`
Post-processing	*none*
Column type	`debug`, `default`

4.1.24 Medium plugins

Table 25: Medium plugins - column details

Header name	Medium plugins
Description	Number of reported plugins for all hosts in scan with Medium Risk Factor.
Source	nessus file > `ReportHost/ReportItem/risk_factor/"Medium"`
Post-processing	*none*
Column type	`debug`, `default`

4.1.25 Low plugins

Table 26: Low plugins - column details

Header name	Low plugins
Description	Number of reported plugins for all hosts in scan with Low Risk Factor.
Source	nessus file > `ReportHost/ReportItem/risk_factor/"Low"`
Post-processing	*none*
Column type	`debug`, `default`

4.1.26 None plugins

Table 27: None plugins - column details

Header name	*none* plugins
Description	Number of reported plugins for all hosts in scan with None Risk Factor.
Source	nessus file > `ReportHost/ReportItem/risk_factor/"None"`
Post-processing	*none*
Column type	`debug`, `default`

4.1.27 ALL compliance

Table 28: ALL compliance - column details

Header name	ALL compliance
Description	Number of reported compliance plugins for all hosts in scan.
Source	nessus file > `ReportHost/ReportItem/compliance/"True"`
Post-processing	*none*
Column type	`debug`, `default`

4.1.28 Passed compliance

Table 29: Passed compliance - column details

Header name	Passed compliance
Description	Number of reported compliance plugins for all hosts in scan with PASSED compliance result.
Source	nessus file > `ReportHost/ReportItem/"cm:compliance-result", namespaces={'cm': 'http://www.nessus.org/cm'}/"PASSED"`
Post-processing	*none*
Column type	`debug`, `default`

4.1.29 Failed compliance

Table 30: Failed compliance - column details

Header name	Failed compliance
Description	Number of reported compliance plugins for all hosts in scan with FAILED compliance result.
Source	nessus file > `ReportHost/ReportItem/"cm:compliance-result", namespaces={'cm': 'http://www.nessus.org/cm'}/"FAILED"`
Post-processing	*none*
Column type	`debug`, `default`

4.1.30 Warning compliance

Table 31: Warning compliance - column details

Header name	Warning compliance
Description	Number of reported compliance plugins for all hosts in scan with WARNING compliance result.
Source	nessus file > `ReportHost/ReportItem/"cm:compliance-result", namespaces={'cm': 'http://www.nessus.org/cm'}/"WARNING"`
Post-processing	*none*
Column type	`debug`, `default`

4.2 Host section

Here you will find all details about data visible in target file in *Host* section.

Table 32: Column details explanation

Header name	Column name.
Description	Short description for particular data.
Source	Information about exact source from where data is being taken.
Post-processing	Information how the gathered data is processed, if post-processed at all.
Column type	`default` - column always appears in report. `debug` - column appears in report only if `add debug data` option has been enabled.

Note: Some of the columns are visible only if you use `add debug data` option for analysis (see *Settings details* to adhere more information about this option). For all of these columns you will find below information **Column type** : `debug`.

4.2.1 Nessus scanner IP

Table 33: Nessus scanner IP - column details

Header name	Nessus scanner IP
Description	Scanner IP used during scan of reported host based on Plugin ID 19506 output.
Source	nessus file > `ReportHost/ReportItem/[pluginID="19506"]/plugin_output`
Post-processing	1. If Plugin ID 19506 output exist extract Scanner IP from output line with `Scanner IP :` 2. **If Plugin ID 19506 output does not exist return:** • `No output recorded.` - if plugin appeared in the report but does no return any output, • `Check Audit Trail.` - if plugin does not appeared in the report but used during scan, • `{plugin_id} not enabled.` - if plugin has not been enabled in policy used during scan.
Column type	`debug`

See also:

Read more about plugin which source for this column on Tenable website https://www.tenable.com/plugins/nessus/19506

4.2.2 Nessus scan name

Table 34: Nessus scan name - column details

Header name	Nessus scan name
Description	Scan name given by user during scan setting up.
Source	nessus file > `Report/name`
Post-processing	*none*
Column type	`debug`

4.2.3 Nessus file name

Table 35: Nessus file name - column details

Header name	Nessus file name
Description	Nessus file name assigned during the file downloading.
Source	nessus file
Post-processing	Absolute path of the given file.
Column type	`debug`

4.2.4 Target

Table 36: Target - column details

Header name	Target
Description	Name of reported host. This can be either IP (Intrnet Protocol Address) or FQDN (Fully Qualified Domain Name), depending on this what has been given as target.
Source	nessus file > `ReportHost/[@name='name']` nessus file > `Preferences/ServerPreferences/preference/[name='TARGET']/value`
Post-processing	*none*
Column type	`debug`, `default`

4.2.5 Hostname

Table 37: Hostname - column details

Header name	Hostname
Description	Hostname of reported host.
Source	nessus file > `ReportHost/HostProperties/tag/[@name='hostname']`
Post-processing	1. Value changed to lowercase. 2. If hostname field contains FQDN only hostname will be returned.
Column type	`debug`, `default`

4.2.6 FQDN

Table 38: FQDN - column details

Header name	FQDN
Description	FQDN of reported host.
Source	nessus file > `ReportHost/HostProperties/tag/[@name='host-fqdn']`
Post-processing	Value changed to lowercase.
Column type	`debug`, `default`

4.2.7 NetBIOS Computer name

Table 39: NetBIOS Computer name - column details

Header name	NetBIOS Computer name
Description	NetBIOS Computer name of reported host.
Source	nessus file > `ReportHost/ReportItem/[pluginID="10150"]/plugin_output`
Post-processing	1. If Plugin ID 10150 output exist extract computer name from output line with `Computer name` 2. Value changed to lowercase. 3. **If Plugin ID 10150 output does not exist return:** • `No output recorded.` - if plugin appeared in the report but does no return any output, • `Check Audit Trail.` - if plugin does not appeared in the report but used during scan, • `{plugin_id} not enabled.` - if plugin has not been enabled in policy used during scan.
Column type	`debug`

See also:

Read more about plugin which source for this column on Tenable website https://www.tenable.com/plugins/nessus/10150

4.2.8 NetBIOS Domain name

Table 40: NetBIOS Domain name - column details

Header name	NetBIOS Domain name
Description	NetBIOS Domain name of reported host.
Source	nessus file > `ReportHost/ReportItem/[pluginID="10150"]/plugin_output`
Post-processing	1. If Plugin ID 10150 output exist extract domain name from output line with `Workgroup / Domain name` 2. Value changed to lowercase. 3. **If Plugin ID 10150 output does not exist return:** • `No output recorded.` - if plugin appeared in the report but does no return any output, • `Check Audit Trail.` - if plugin does not appeared in the report but used during scan, • `{plugin_id} not enabled.` - if plugin has not been enabled in policy used during scan.
Column type	`debug`

See also:

Read more about plugin which source for this column on Tenable website https://www.tenable.com/plugins/nessus/10150

4.2.9 IP

Table 41: IP - column details

Header name	IP
Description	IP of reported host.
Source	nessus file > `ReportHost/HostProperties/tag/[@name='host-ip']`
Post-processing	*none*
Column type	`debug`, `default`

4.2.10 Scanned

Table 42: Scanned - column details

Header name	Scanned
Description	Information if target host has been scanned. • `yes` if target host is on the list of reported hosts. • `no` if target host is not on the list of reported hosts.
Source	nessus file > `Preferences/ServerPreferences/preference/[name='TARGET']/value` nessus file > `ReportHost/[@name='name']`
Post-processing	*none*
Column type	`debug`, `default`

4.2.11 Credentialed checks

Table 43: Credentialed checks - column details

Header name	Credentialed checks
Description	Information if reported host has been scanned with credentialed checks.
Source	nessus file > `ReportHost/ReportItem/[pluginID="19506"]/plugin_output`
Post-processing	1. If Plugin ID 19506 output exist extract `yes` or `no` from output line with `Credentialed checks :`. 2. If Plugin ID 19506 output does not exist return `no`.
Column type	`debug`, `default`

See also:

Read more about this plugin on Tenable website https://www.tenable.com/plugins/nessus/19506

4.2.12 Scan started

Table 44: Scan started - column details

Header name	Scan started
Description	Exact date and time when scan of the reported host has been initiated.
Source	nessus file > `ReportHost/HostProperties/tag/[@name='HOST_START']`
Post-processing	Date and time returned in format `%a %b %d %H:%M:%S %Y`.
Column type	`debug`, `default`

4.2.13 Scan ended

Table 45: Scan ended - column details

Header name	Scan ended
Description	Exact date and time when scan of the reported host has been ended.
Source	nessus file > `ReportHost/HostProperties/tag/[@name='HOST_END']`
Post-processing	Date and time returned in format `%a %b %d %H:%M:%S %Y`.
Column type	`debug`, `default`

4.2.14 Elapsed time per host

Table 46: Elapsed time per host - column details

Header name	Elapsed time per host
Description	Duration of the particular host scanned based on subtraction Scan Start Time from Scan End Time.
Source	nessus file > `ReportHost/HostProperties/tag/[@name='HOST_END']` - `ReportHost/HostProperties/tag/[@name='HOST_START']`
Post-processing	Elapsed time returned in format `HH:MM:SS`.
Column type	`debug`, `default`

4.2.15 Elapsed time per scan

Table 47: Elapsed time per scan - column details

Header name	Elapsed time per scan
Description	Duration of the entire scan, based on subtraction Scan Start Time of first host scanned from Scan End Time of last host scanned.
Source	nessus file > `ReportHost/HostProperties/tag/[@name='HOST_END']` - `ReportHost/HostProperties/tag/[@name='HOST_START']`
Post-processing	Elapsed time returned in format `HH:MM:SS`.
Column type	`debug`, `default`

4.2.16 Policy name

Table 48: Policy name - column details

Header name	Policy name
Description	Policy name selected by user during scan setting up.
Source	nessus file > `Policy/policyName`
Post-processing	*none*
Column type	`debug`

4.2.17 Login used

Table 49: Login used - column details

Header name	Login used
Description	Login name used during scan of reported host.
Source	nessus file > `ReportHost/HostProperties/tag/[@name='login-used']` nessus file > `Preferences/PluginsPreferences/item/[fullName='VMware vCenter SOAP API Settings[entry]:VMware vCenter user name :']/selectedValue` nessus file > `Preferences/PluginsPreferences/item/[fullName='Database settings[entry]:Login :']/selectedValue` nessus file > `Preferences/PluginsPreferences/item/[fullName='Login configurations[entry]:SMB account :']/selectedValue` nessus file > `Preferences/PluginsPreferences/item/[fullName='SSH settings[entry]:SSH user name :']/selectedValue` nessus file > `Preferences/PluginsPreferences/item/[fullName='Login configurations[entry]:SMB domain (optional) :']/selectedValue`
Post-processing	For `Preferences/PluginsPreferences/item/[fullName='Login configurations[entry]:SMB account :']/selectedValue` information about domain is added `Preferences/PluginsPreferences/item/[fullName='Login configurations[entry]:SMB domain (optional) :']/selectedValue`
Column type	`debug`, `default`

4.2.18 DB SID

Table 50: DB SID - column details

Header name	DB SID
Description	Database SID set by user during scan setting up.
Source	nessus file > `Preferences/PluginsPreferences/item/[fullName='Database settings[entry]:Database SID :']/selectedValue`
Post-processing	*none*
Column type	`debug`, `default`

4.2.19 DB port

Table 51: DB port - column details

Header name	DB port
Description	Database port set by user during scan setting up.
Source	nessus file > `Preferences/PluginsPreferences/item/[fullName='Database settings[entry]:Database port to use :']/selectedValue`
Post-processing	*none*
Column type	`debug`, `default`

4.2.20 Reverse lookup

Table 52: Reverse lookup - column details

Header name	Reverse lookup
Description	Information if option *Settings* > *Report* > *Output* > *'Designate hosts by their DNS name'* has been turned on in policy used during scan.
Source	nessus file > `Preferences/ServerPreferences/preference/[name='reverse_lookup']/value`
Post-processing	*none*
Column type	`debug`

4.2.21 Max hosts

Table 53: Max hosts - column details

Header name	Max hosts
Description	Value set for Max simultaneous hosts per scan in policy used during scan.
Source	nessus file > `Preferences/ServerPreferences/preference/[name='max_hosts']/value`
Post-processing	*none*
Column type	`debug`

4.2.22 Max checks

Table 54: Max checks - column details

Header name	Max checks
Description	Value set for Max simultaneous checks per host in policy used during scan.
Source	nessus file > `Preferences/ServerPreferences/preference/[name='max_checks']/value`
Post-processing	*none*
Column type	`debug`

4.2.23 Network timeout

Table 55: Network timeout - column details

Header name	Network timeout
Description	Value set for Network timeout (in seconds) in policy used during scan.
Source	nessus file > `Preferences/ServerPreferences/preference/[name='checks_read_timeout']/value`
Post-processing	*none*
Column type	`debug`

4.2.24 Operating System

Table 56: Operating System - column details

Header name	Operating System
Description	Information about Operating System of reported host.
Source	nessus file > `ReportHost/HostProperties/tag/[@name='operating-system']`
Post-processing	*none*
Column type	`debug`, `default`

4.2.25 ALL plugins

Table 57: ALL plugins - column details

Header name	ALL plugins
Description	Number of reported plugins for particular reported host.
Source	nessus files > `ReportHost/ReportItem`
Post-processing	*none*
Column type	`debug`, `default`

4.2.26 Critical plugins

Table 58: Critical plugins - column details

Header name	Critical plugins
Description	Number of reported plugins for particular reported host with Critical Risk Factor.
Source	nessus file > `ReportHost/ReportItem/risk_factor/"Critical"`
Post-processing	*none*
Column type	`debug`, `default`

4.2.27 High plugins

Table 59: High plugins - column details

Header name	High plugins
Description	Number of reported plugins for particular reported host in scan with High Risk Factor.
Source	nessus file > `ReportHost/ReportItem/risk_factor/"High"`
Post-processing	*none*
Column type	`debug`, `default`

4.2.28 Medium plugins

Table 60: Medium plugins - column details

Header name	Medium plugins
Description	Number of reported plugins for particular reported host in scan with Medium Risk Factor.
Source	nessus file > `ReportHost/ReportItem/risk_factor/"Medium"`
Post-processing	*none*
Column type	`debug`, `default`

4.2.29 Low plugins

Table 61: Low plugins - column details

Header name	Low plugins
Description	Number of reported plugins for particular reported host in scan with Low Risk Factor.
Source	nessus file > `ReportHost/ReportItem/risk_factor/"Low"`
Post-processing	*none*
Column type	`debug`, `default`

4.2.30 None plugins

Table 62: None plugins - column details

Header name	*none* plugins
Description	Number of reported plugins for particular reported host in scan with None Risk Factor.
Source	nessus file > `ReportHost/ReportItem/risk_factor/"None"`
Post-processing	*none*
Column type	`debug`, `default`

4.2.31 ALL compliance

Table 63: ALL compliance - column details

Header name	ALL compliance
Description	Number of reported compliance checks for particular reported host in scan.
Source	nessus file > `ReportHost/ReportItem/compliance/"True"`
Post-processing	*none*
Column type	`debug`, `default`

4.2.32 Passed compliance

Table 64: Passed compliance - column details

Header name	Passed compliance
Description	Number of reported compliance checks for particular reported host in scan with PASSED compliance result.
Source	nessus file > `ReportHost/ReportItem/"cm:compliance-result", namespaces={'cm': 'http://www.nessus.org/cm'}/ "PASSED"`
Post-processing	*none*
Column type	`debug`, `default`

4.2.33 Failed compliance

Table 65: Failed compliance - column details

Header name	Failed compliance
Description	Number of reported compliance checks for particular reported host in scan with FAILED compliance result.
Source	nessus file > `ReportHost/ReportItem/"cm:compliance-result", namespaces={'cm': 'http://www.nessus.org/cm'}/ "FAILED"`
Post-processing	*none*
Column type	`debug`, `default`

4.2.34 Warning compliance

Table 66: Warning compliance - column details

Header name	Warning compliance
Description	Number of reported compliance checks for particular reported host in scan with WARNING compliance result.
Source	nessus file > `ReportHost/ReportItem/"cm:compliance-result", namespaces={'cm': 'http://www.nessus.org/cm'}/"WARNING"`
Post-processing	*none*
Column type	`debug`, `default`

4.2.35 10180: Ping to remote host

Table 67: 10180: Ping to remote host - column details

Header name	10180: Ping to remote host
Description	Plugin ID 10180 output.
Source	nessus file > `ReportHost/ReportItem/[pluginID="10180"]/plugin_output`
Post-processing	1. If Plugin ID 10180 output exist return it **in unchanged form**. 2. **If Plugin ID 10180 output does not exist return:** • `No output recorded.` - if plugin appeared in the report but does no return any output, • `Check Audit Trail.` - if plugin does not appeared in the report but used during scan, • `{plugin_id} not enabled.` - if plugin has not been enabled in policy used during scan.
Column type	`debug`

See also:

Read more about this plugin on Tenable website https://www.tenable.com/plugins/nessus/10180

4.2.36 10287: Traceroute Information

Table 68: 10287: Traceroute Information - column details

Header name	10287: Traceroute Information
Description	Plugin ID 10287 output.
Source	nessus file > `ReportHost/ReportItem/[pluginID="10287"]/plugin_output`
Post-processing	1. If Plugin ID 10287 output exist return it **in unchanged form**. 2. **If Plugin ID 10287 output does not exist return:** • `No output recorded.` - if plugin appeared in the report but does no return any output, • `Check Audit Trail.` - if plugin does not appeared in the report but used during scan, • `{plugin_id} not enabled.` - if plugin has not been enabled in policy used during scan.
Column type	`debug`

See also:

Read more about this plugin on Tenable website https://www.tenable.com/plugins/nessus/10287

4.2.37 11936: OS Identification

Table 69: 11936: OS Identification - column details

Header name	11936: OS Identification
Description	Plugin ID 11936 output.
Source	nessus file > `ReportHost/ReportItem/[pluginID="11936"]/plugin_output`
Post-processing	1. If Plugin ID 11936 output exist return it **in unchanged form**. 2. **If Plugin ID 11936 output does not exist return:** • `No output recorded.` - if plugin appeared in the report but does no return any output, • `Check Audit Trail.` - if plugin does not appeared in the report but used during scan, • `{plugin_id} not enabled.` - if plugin has not been enabled in policy used during scan.
Column type	`debug`

See also:

Read more about this plugin on Tenable website https://www.tenable.com/plugins/nessus/11936

4.2.38 45590: Common Platform Enumeration (CPE)

Table 70: 45590: Common Platform Enumeration (CPE) - column details

Header name	45590: Common Platform Enumeration (CPE)
Description	Plugin ID 45590 output.
Source	nessus file > `ReportHost/ReportItem/[pluginID="45590"]/plugin_output`
Post-processing	1. If Plugin ID 45590 output exist return it **in unchanged form**. 2. **If Plugin ID 45590 output does not exist return:** • `No output recorded.` - if plugin appeared in the report but does no return any output, • `Check Audit Trail.` - if plugin does not appeared in the report but used during scan, • `{plugin_id} not enabled.` - if plugin has not been enabled in policy used during scan.
Column type	`debug`

See also:

Read more about this plugin on Tenable website https://www.tenable.com/plugins/nessus/45590

4.2.39 54615: Device Type

Table 71: 54615: Device Type - column details

Header name	54615: Device Type
Description	Plugin ID 54615 output.
Source	nessus file > `ReportHost/ReportItem/[pluginID="54615"]/plugin_output`
Post-processing	1. If Plugin ID 54615 output exist return it **in unchanged form**. 2. **If Plugin ID 54615 output does not exist return:** • `No output recorded.` - if plugin appeared in the report but does no return any output, • `Check Audit Trail.` - if plugin does not appeared in the report but used during scan, • `{plugin_id} not enabled.` - if plugin has not been enabled in policy used during scan.
Column type	`debug`

See also:

Read more about this plugin on Tenable website https://www.tenable.com/plugins/nessus/54615

4.2.40 21745: Authentication Failure - Local Checks Not Run

Table 72: 21745: Authentication Failure - Local Checks Not Run - column details

Header name	21745: Authentication Failure - Local Checks Not Run
Description	Plugin ID 21745 output.
Source	nessus file > `ReportHost/ReportItem/[pluginID="21745"]/plugin_output`
Post-processing	1. If Plugin ID 21745 output exist return it **in unchanged form**. 2. **If Plugin ID 21745 output does not exist return:** • `No output recorded.` - if plugin appeared in the report but does no return any output, • `Check Audit Trail.` - if plugin does not appeared in the report but used during scan, • `{plugin_id} not enabled.` - if plugin has not been enabled in policy used during scan.
Column type	`debug`

See also:

Read more about this plugin on Tenable website https://www.tenable.com/plugins/nessus/21745

4.2.41 12634: Authenticated Check : OS Name and Installed Package Enumeration

Table 73: 12634: Authenticated Check : OS Name and Installed Package Enumeration - column details

Header name	12634: Authenticated Check : OS Name and Installed Package Enumeration
Description	Plugin ID 12634 output.
Source	nessus file > `ReportHost/ReportItem/[pluginID="12634"]/plugin_output`
Post-processing	1. If Plugin ID 12634 output exist return it **in unchanged form**. 2. **If Plugin ID 12634 output does not exist return:** • `No output recorded.` - if plugin appeared in the report but does no return any output, • `Check Audit Trail.` - if plugin does not appeared in the report but used during scan, • `{plugin_id} not enabled.` - if plugin has not been enabled in policy used during scan.
Column type	`debug`

See also:

Read more about this plugin on Tenable website https://www.tenable.com/plugins/nessus/12634

4.2.42 110385: Authentication Success Insufficient Access

Table 74: 110385: Authentication Success Insufficient Access - column details

Header name	110385: Authentication Success Insufficient Access
Description	Plugin ID 110385 output.
Source	nessus file > `ReportHost/ReportItem/[pluginID="110385"]/plugin_output`
Post-processing	1. If Plugin ID 110385 output exist return it **in unchanged form**. 2. **If Plugin ID 110385 output does not exist return:** • `No output recorded.` - if plugin appeared in the report but does no return any output, • `Check Audit Trail.` - if plugin does not appeared in the report but used during scan, • `{plugin_id} not enabled.` - if plugin has not been enabled in policy used during scan.
Column type	`debug`

See also:

Read more about this plugin on Tenable website https://www.tenable.com/plugins/nessus/110385

4.2.43 102094: SSH Commands Require Privilege Escalation

Table 75: 102094: SSH Commands Require Privilege Escalation - column details

Header name	102094: SSH Commands Require Privilege Escalation
Description	Plugin ID 102094 output.
Source	nessus file > `ReportHost/ReportItem/[pluginID="102094"]/plugin_output`
Post-processing	1. If Plugin ID 102094 output exist return it **in unchanged form**. 2. **If Plugin ID 102094 output does not exist return:** • `No output recorded.` - if plugin appeared in the report but does no return any output, • `Check Audit Trail.` - if plugin does not appeared in the report but used during scan, • `{plugin_id} not enabled.` - if plugin has not been enabled in policy used during scan.
Column type	`debug`, `default`

See also:

Read more about this plugin on Tenable website https://www.tenable.com/plugins/nessus/102094

4.2.44 10394: Microsoft Windows SMB Log In Possible

Table 76: 10394: Microsoft Windows SMB Log In Possible - column details

Header name	10394: Microsoft Windows SMB Log In Possible
Description	Plugin ID 10394 output.
Source	nessus file > `ReportHost/ReportItem/[pluginID="10394"]/plugin_output`
Post-processing	1. If Plugin ID 10394 output exist return it **in unchanged form**. 2. **If Plugin ID 10394 output does not exist return:** • `No output recorded.` - if plugin appeared in the report but does no return any output, • `Check Audit Trail.` - if plugin does not appeared in the report but used during scan, • `{plugin_id} not enabled.` - if plugin has not been enabled in policy used during scan.
Column type	`debug`

See also:

Read more about this plugin on Tenable website https://www.tenable.com/plugins/nessus/10394

4.2.45 24786: Nessus Windows Scan Not Performed with Admin Privileges

Table 77: 24786: Nessus Windows Scan Not Performed with Admin Privileges - column details

Header name	24786: Nessus Windows Scan Not Performed with Admin Privileges
Description	Plugin ID 24786 output.
Source	nessus file > `ReportHost/ReportItem/[pluginID="24786"]/plugin_output`
Post-processing	1. If Plugin ID 24786 output exist return it **in unchanged form**. 2. **If Plugin ID 24786 output does not exist return:** • `No output recorded.` - if plugin appeared in the report but does no return any output, • `Check Audit Trail.` - if plugin does not appeared in the report but used during scan, • `{plugin_id} not enabled.` - if plugin has not been enabled in policy used during scan.
Column type	`debug`

See also:

Read more about this plugin on Tenable website https://www.tenable.com/plugins/nessus/24786

4.2.46 24269: Windows Management Instrumentation (WMI) Available

Table 78: 24269: Windows Management Instrumentation (WMI) Available - column details

Header name	24269: Windows Management Instrumentation (WMI) Available
Description	Plugin ID 24269 output.
Source	nessus file > `ReportHost/ReportItem/[pluginID="24269"]/plugin_output`
Post-processing	1. If Plugin ID 24269 output exist return it **in unchanged form**. 2. **If Plugin ID 24269 output does not exist return:** • `No output recorded.` - if plugin appeared in the report but does no return any output, • `Check Audit Trail.` - if plugin does not appeared in the report but used during scan, • `{plugin_id} not enabled.` - if plugin has not been enabled in policy used during scan.
Column type	`debug`

See also:

Read more about this plugin on Tenable website https://www.tenable.com/plugins/nessus/24269

4.2.47 11011: Microsoft Windows SMB Service Detection

Table 79: 11011: Microsoft Windows SMB Service Detection - column details

Header name	11011: Microsoft Windows SMB Service Detection
Description	All occurrences of Plugin ID 11011 output.
Source	nessus file > `ReportHost/ReportItem/[pluginID="11011"]/plugin_output`
Post-processing	1. If Plugin ID 11011 output exist return it **in unchanged form**. 2. If more than one Plugin ID 11011 outputs exist, concatenate their **unchanged form** and return as one. 3. **If Plugin ID 11011 output does not exist return:** • `No output recorded.` - if plugin appeared in the report but does no return any output, • `Check Audit Trail.` - if plugin does not appeared in the report but used during scan, • `{plugin_id} not enabled.` - if plugin has not been enabled in policy used during scan.
Column type	`debug`

See also:

Read more about this plugin on Tenable website https://www.tenable.com/plugins/nessus/11011

4.2.48 10400: Microsoft Windows SMB Registry Remotely Accessible

Table 80: 10400: Microsoft Windows SMB Registry Remotely Accessible - column details

Header name	10400: Microsoft Windows SMB Registry Remotely Accessible
Description	Plugin ID 10400 output.
Source	nessus file > `ReportHost/ReportItem/[pluginID="10400"]/plugin_output`
Post-processing	1. If Plugin ID 10400 output exist return it **in unchanged form**. 2. **If Plugin ID 10400 output does not exist return:** • `No output recorded.` - if plugin appeared in the report but does no return any output, • `Check Audit Trail.` - if plugin does not appeared in the report but used during scan, • `{plugin_id} not enabled.` - if plugin has not been enabled in policy used during scan.
Column type	`debug`

See also:

Read more about this plugin on Tenable website https://www.tenable.com/plugins/nessus/10400

4.2.49 26917: Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry

Table 81: 26917: Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry - column details

Header name	26917: Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
Description	Plugin ID 26917 output.
Source	nessus file > `ReportHost/ReportItem/[pluginID="26917"]/plugin_output`
Post-processing	1. If Plugin ID 26917 output exist return it **in unchanged form**. 2. **If Plugin ID 26917 output does not exist return:** • `No output recorded.` - if plugin appeared in the report but does no return any output, • `Check Audit Trail.` - if plugin does not appeared in the report but used during scan, • `{plugin_id} not enabled.` - if plugin has not been enabled in policy used during scan.
Column type	`debug`

See also:

Read more about this plugin on Tenable website https://www.tenable.com/plugins/nessus/26917

4.2.50 42897: SMB Registry : Start the Registry Service during the scan (WMI)

Table 82: 42897: SMB Registry : Start the Registry Service during the scan (WMI) - column details

Header name	42897: SMB Registry : Start the Registry Service during the scan (WMI)
Description	Plugin ID 42897 output.
Source	nessus file > `ReportHost/ReportItem/[pluginID="42897"]/plugin_output`
Post-processing	1. If Plugin ID 42897 output exist return it **in unchanged form**. 2. **If Plugin ID 42897 output does not exist return:** • `No output recorded.` - if plugin appeared in the report but does no return any output, • `Check Audit Trail.` - if plugin does not appeared in the report but used during scan, • `{plugin_id} not enabled.` - if plugin has not been enabled in policy used during scan.
Column type	`debug`

See also:

Read more about this plugin on Tenable website https://www.tenable.com/plugins/nessus/42897

4.2.51 20811: Microsoft Windows Installed Software Enumeration (credentialed check)

Table 83: 20811: Microsoft Windows Installed Software Enumeration (credentialed check) - column details

Header name	20811: Microsoft Windows Installed Software Enumeration (credentialed check)
Description	Plugin ID 20811 output.
Source	nessus file > `ReportHost/ReportItem/[pluginID="20811"]/plugin_output`
Post-processing	1. If Plugin ID 20811 output exist return it **in unchanged form**. 2. **If Plugin ID 20811 output does not exist return:** • `No output recorded.` - if plugin appeared in the report but does no return any output, • `Check Audit Trail.` - if plugin does not appeared in the report but used during scan, • `{plugin_id} not enabled.` - if plugin has not been enabled in policy used during scan.
Column type	`debug`

See also:

Read more about this plugin on Tenable website https://www.tenable.com/plugins/nessus/20811

4.2.52 91825: Oracle DB Login Possible

Table 84: 91825: Oracle DB Login Possible - column details

Header name	91825: Oracle DB Login Possible
Description	Plugin ID 91825 output.
Source	nessus file > `ReportHost/ReportItem/[pluginID="91825"]/plugin_output`
Post-processing	1. If Plugin ID 91825 output exist return it **in unchanged form**. 2. **If Plugin ID 91825 output does not exist return:** • `No output recorded.` - if plugin appeared in the report but does no return any output, • `Check Audit Trail.` - if plugin does not appeared in the report but used during scan, • `{plugin_id} not enabled.` - if plugin has not been enabled in policy used during scan.
Column type	`debug`

See also:

Read more about this plugin on Tenable website https://www.tenable.com/plugins/nessus/91825

4.2.53 91827: Microsoft SQL Server Login Possible

Table 85: 91827: Microsoft SQL Server Login Possible - column details

Header name	91827: Microsoft SQL Server Login Possible
Description	Plugin ID 91827 output.
Source	nessus file > `ReportHost/ReportItem/[pluginID="91827"]/plugin_output`
Post-processing	1. If Plugin ID 91827 output exist return it **in unchanged form**. 2. **If Plugin ID 91827 output does not exist return:** • `No output recorded.` - if plugin appeared in the report but does no return any output, • `Check Audit Trail.` - if plugin does not appeared in the report but used during scan, • `{plugin_id} not enabled.` - if plugin has not been enabled in policy used during scan.
Column type	`debug`

See also:

Read more about this plugin on Tenable website https://www.tenable.com/plugins/nessus/91827

4.2.54 47864: Cisco IOS Version

Table 86: 47864: Cisco IOS Version - column details

Header name	47864: Cisco IOS Version
Description	Plugin ID 47864 output.
Source	nessus file > `ReportHost/ReportItem/[pluginID="47864"]/plugin_output`
Post-processing	1. If Plugin ID 47864 output exist return it **in unchanged form**. 2. **If Plugin ID 47864 output does not exist return:** • `No output recorded.` - if plugin appeared in the report but does no return any output, • `Check Audit Trail.` - if plugin does not appeared in the report but used during scan, • `{plugin_id} not enabled.` - if plugin has not been enabled in policy used during scan.
Column type	`debug`

See also:

Read more about this plugin on Tenable website https://www.tenable.com/plugins/nessus/47864

4.2.55 67217: Cisco IOS XE Version

Table 87: 67217: Cisco IOS XE Version - column details

Header name	67217: Cisco IOS XE Version
Description	Plugin ID 67217 output.
Source	nessus file > `ReportHost/ReportItem/[pluginID="67217"]/plugin_output`
Post-processing	1. If Plugin ID 67217 output exist return it **in unchanged form**. 2. **If Plugin ID 67217 output does not exist return:** • `No output recorded.` - if plugin appeared in the report but does no return any output, • `Check Audit Trail.` - if plugin does not appeared in the report but used during scan, • `{plugin_id} not enabled.` - if plugin has not been enabled in policy used during scan.
Column type	`debug`

See also:

Read more about this plugin on Tenable website https://www.tenable.com/plugins/nessus/67217

4.3 Vulnerabilities section

Here you will find all details about data visible in target file in *Vulnerabilities* section.

Table 88: Column details explanation

Header name	Column name.
Description	Short description for particular data.
Source	Information about exact source from where data is being taken.
Post-processing	Information how the gathered data is processed, if post-processed at all.
Column type	`default` - column always appears in report. `debug` - column appears in report only if `add debug data` option has been enabled.

Note: Some of the columns are visible only if you use `add debug data` option for analysis (see *Settings details* to adhere more information about this option). For all of these columns you will find below information **Column type** : `debug`.

4.3.1 Nessus scanner IP

Table 89: Nessus scanner IP - column details

Header name	Nessus scanner IP
Description	Scanner IP used during scan of reported host based on Plugin ID 19506 output.
Source	nessus file > `ReportHost/ReportItem/[pluginID="19506"]/plugin_output`
Post-processing	1. If Plugin ID 19506 output exist extract Scanner IP from output line with `Scanner IP :` 2. **If Plugin ID 19506 output does not exist return:** • `No output recorded.` - if plugin appeared in the report but does no return any output, • `Check Audit Trail.` - if plugin does not appeared in the report but used during scan, • `{plugin_id} not enabled.` - if plugin has not been enabled in policy used during scan.
Column type	`debug`

See also:

Read more about plugin which source for this column on Tenable website https://www.tenable.com/plugins/nessus/19506

4.3.2 Nessus scan name

Table 90: Nessus scan name - column details

Header name	Nessus scan name
Description	Scan name given by user during scan setting up.
Source	nessus file > `Report/name`
Post-processing	*none*
Column type	`debug`

4.3.3 Nessus file name

Table 91: Nessus file name - column details

Header name	Nessus file name
Description	Nessus file name assigned during the file downloading.
Source	nessus file
Post-processing	Absolute path of the given file.
Column type	`debug`

4.3.4 Target

Table 92: Target - column details

Header name	Target
Description	Name of reported host. This can be either IP or FQDN, depending on this what has been given as target.
Source	nessus file > `ReportHost/[@name='name']`
Post-processing	*none*
Column type	`debug`, `default`

4.3.5 Hostname

Table 93: Hostname - column details

Header name	Hostname
Description	Hostname of reported host.
Source	nessus file > `ReportHost/HostProperties/tag/[@name='hostname']`
Post-processing	1. Value changed to lowercase. 2. If hostname field contains FQDN only hostname will be returned.
Column type	`debug`, `default`

4.3.6 FQDN

Table 94: FQDN - column details

Header name	FQDN
Description	FQDN of reported host.
Source	nessus file > `ReportHost/HostProperties/tag/[@name='host-fqdn']`
Post-processing	Value changed to lowercase.
Column type	`debug`, `default`

4.3.7 IP

Table 95: IP - column details

Header name	IP
Description	IP of reported host.
Source	nessus file > `ReportHost/HostProperties/tag/[@name='host-ip']`
Post-processing	*none*
Column type	`debug`, `default`

4.3.8 Scanned

Table 96: Scanned - column details

Header name	Scanned
Description	Information if target host has been scanned. • `yes` if target host is on the list of reported hosts. • `no` if target host is not on the list of reported hosts.
Source	nessus file > `Preferences/ServerPreferences/preference/[name='TARGET']/value` nessus file > `ReportHost/[@name='name']`
Post-processing	*none*
Column type	`debug`, `default`

4.3.9 Credentialed checks

Table 97: Credentialed checks - column details

Header name	Credentialed checks
Description	Information if reported host has been scanned with credentialed checks.
Source	nessus file > `ReportHost/ReportItem/[pluginID="19506"]/plugin_output`
Post-processing	1. If Plugin ID 19506 output exist extract `yes` or `no` from output line with `Credentialed checks :`. 2. If Plugin ID 19506 output does not exist return `no`.
Column type	`debug`, `default`

See also:

Read more about this plugin on Tenable website https://www.tenable.com/plugins/nessus/19506

4.3.10 Policy name

Table 98: Policy name - column details

Header name	Policy name
Description	Policy name selected by user during scan setting up.
Source	nessus file > `Policy/policyName`
Post-processing	*none*
Column type	`debug`

4.3.11 Protocol

Table 99: Protocol - column details

Header name	Protocol
Description	Exact protocol type returned by Nessus.
Source	nessus file > `ReportHost/ReportItem/[@protocol]`
Post-processing	*none*
Column type	`debug`, `default`

4.3.12 Service Name

Table 100: Service Name - column details

Header name	Service Name
Description	Exact service name returned by Nessus.
Source	nessus file > `ReportHost/ReportItem/[@svc_name]`
Post-processing	*none*
Column type	`debug`, `default`

4.3.13 Port

Table 101: Port - column details

Header name	Port
Description	Exact port returned by Nessus.
Source	nessus file > `ReportHost/ReportItem/[@port]`
Post-processing	*none*
Column type	`debug`, `default`

4.3.14 Plugin ID

Table 102: Plugin ID - column details

Header name	Plugin ID
Description	Exact Plugin ID returned by Nessus.
Source	nessus file > `ReportHost/ReportItem/[@pluginID]`
Post-processing	*none*
Column type	`debug`, `default`

4.3.15 Plugin name

Table 103: Plugin name - column details

Header name	Plugin name
Description	Exact Plugin Name returned by Nessus.
Source	nessus file > `ReportHost/ReportItem/[@pluginName]`
Post-processing	*none*
Column type	`debug`, `default`

4.3.16 Plugin type

Table 104: Plugin type - column details

Header name	Plugin type
Description	Exact Plugin type returned by Nessus.
Source	nessus file > `ReportHost/ReportItem/plugin_type`
Post-processing	*none*
Column type	`debug`, `default`

4.3.17 Risk Factor

Table 105: Risk Factor - column details

Header name	Risk Factor
Description	Exact Plugin Risk Factor returned by Nessus.
Source	nessus file > `ReportHost/ReportItem/risk_factor`
Post-processing	*none*
Column type	`debug`, `default`

4.3.18 Plugin family

Table 106: Plugin family - column details

Header name	Plugin family
Description	Exact Plugin Family returned by Nessus.
Source	nessus file > `ReportHost/ReportItem/[@pluginFamily]`
Post-processing	*none*
Column type	`debug`, `default`

4.3.19 Plugin file name

Table 107: Plugin file name - column details

Header name	Plugin file name
Description	Exact Plugin file name returned by Nessus.
Source	nessus file > `ReportHost/ReportItem/fname`
Post-processing	*none*
Column type	`debug`

4.3.20 Plugin version

Table 108: Plugin version - column details

Header name	Plugin version
Description	Exact Plugin version returned by Nessus.
Source	nessus file > `ReportHost/ReportItem/script_version`
Post-processing	*none*
Column type	`debug`, `default`

4.3.21 Plugin publication date

Table 109: Plugin publication date - column details

Header name	Plugin publication date
Description	Exact Plugin publication date returned by Nessus.
Source	nessus file > `ReportHost/ReportItem/plugin_publication_date`
Post-processing	Return in format `yyyy-mm-dd`.
Column type	`debug`, `default`

4.3.22 Plugin modification date

Table 110: Plugin modification date - column details

Header name	Plugin modification date
Description	Exact Plugin modification date returned by Nessus.
Source	nessus file > `ReportHost/ReportItem/plugin_modification_date`
Post-processing	Return in format `yyyy-mm-dd`.
Column type	`debug`, `default`

4.3.23 Plugin description

Table 111: Plugin description - column details

Header name	Plugin description
Description	Exact Plugin description returned by Nessus.
Source	nessus file > `ReportHost/ReportItem/description`
Post-processing	*none*
Column type	`debug`, `default`

4.3.24 Solution

Table 112: Solution - column details

Header name	Solution
Description	Exact Plugin solution returned by Nessus.
Source	nessus file > `ReportHost/ReportItem/solution`
Post-processing	*none*
Column type	`debug`, `default`

4.3.25 Plugin output

Table 113: Plugin output - column details

Header name	Plugin output
Description	Exact Plugin output returned by Nessus.
Source	nessus file > `ReportHost/ReportItem/plugin_output`
Post-processing	*none*
Column type	`debug`, `default`

4.3.26 CVE counter

Table 114: CVE counter - column details

Header name	CVE counter
Description	Number of CVE (Common Vulnerabilities and Exposures) assigned to particular Plugin returned by Nessus.
Source	nessus file > `ReportHost/ReportItem/cve`
Post-processing	*none*
Column type	`debug`, `default`

4.3.27 CVE number

Table 115: CVE number - column details

Header name	CVE number
Description	List of CVE assigned to particular Plugin returned by Nessus.
Source	nessus file > `ReportHost/ReportItem/cve`
Post-processing	*none*
Column type	`debug`, `default`

4.3.28 Exploit available

Table 116: Exploit available - column details

Header name	Exploit available
Description	Information if Exploit is available.
Source	nessus file > `ReportHost/ReportItem/exploit_available`
Post-processing	*none*
Column type	`debug`, `default`

4.3.29 Exploit code maturity

Table 117: Exploit code maturity - column details

Header name	Exploit code maturity
Description	Information about Exploit code maturity.
Source	nessus file > `ReportHost/ReportItem/exploit_code_maturity`
Post-processing	*none*
Column type	`debug`, `default`

4.3.30 Exploit framework metasploit

Table 118: Exploit framework metasploit - column details

Header name	Exploit framework metasploit
Description	Information about Exploit framework metasploit.
Source	nessus file > `ReportHost/ReportItem/exploit_framework_metasploit`
Post-processing	*none*
Column type	`debug`, `default`

4.3.31 Exploitability ease

Table 119: Exploitability ease - column details

Header name	Exploitability ease
Description	Information if Exploitability is ease.
Source	nessus file > `ReportHost/ReportItem/exploitability_ease`
Post-processing	*none*
Column type	`debug`, `default`

4.4 Noncompliance section

Here you will find all details about data visible in target file in *Noncompliance* section.

Table 120: Column details explanation

Header name	Column name.
Description	Short description for particular data.
Source	Information about exact source from where data is being taken.
Post-processing	Information how the gathered data is processed, if post-processed at all.
Column type	`default` - column always appears in report. `debug` - column appears in report only if `add debug data` option has been enabled.

Note: Some of the columns are visible only if you use `add debug data` option for analysis (see *Settings details* to adhere more information about this option). For all of these columns you will find below information **Column type** : `debug`.

4.4.1 Nessus scanner IP

Table 121: Nessus scanner IP - column details

Header name	Nessus scanner IP
Description	Scanner IP used during scan of reported host based on Plugin ID 19506 output.
Source	nessus file > `ReportHost/ReportItem/[pluginID="19506"]/plugin_output`
Post-processing	1. If Plugin ID 19506 output exist extract Scanner IP from output line with `Scanner IP :` 2. **If Plugin ID 19506 output does not exist return:** • `No output recorded.` - if plugin appeared in the report but does no return any output, • `Check Audit Trail.` - if plugin does not appeared in the report but used during scan, • `{plugin_id} not enabled.` - if plugin has not been enabled in policy used during scan.
Column type	`debug`

See also:

Read more about plugin which source for this column on Tenable website https://www.tenable.com/plugins/nessus/19506

4.4.2 Nessus scan name

Table 122: Nessus scan name - column details

Header name	Nessus scan name
Description	Scan name given by user during scan setting up.
Source	nessus file > `Report/name`
Post-processing	*none*
Column type	`debug`

4.4.3 Nessus file name

Table 123: Nessus file name - column details

Header name	Nessus file name
Description	Nessus file name assigned during the file downloading.
Source	nessus file
Post-processing	absolute path of the given file
Column type	`debug`

4.4.4 Target

Table 124: Target - column details

Header name	Target
Description	Name of reported host. This can be either IP or FQDN, depending on this what has been given as target.
Source	nessus file > `ReportHost/[@name='name']`
Post-processing	*none*
Column type	`debug`, `default`

4.4.5 Hostname

Table 125: Hostname - column details

Header name	Hostname
Description	Hostname of reported host.
Source	nessus file > `ReportHost/HostProperties/tag/[@name='hostname']`
Post-processing	1. Value changed to lowercase. 2. If hostname field contains FQDN only hostname will be returned.
Column type	`debug`, `default`

4.4.6 FQDN

Table 126: FQDN - column details

Header name	FQDN
Description	FQDN of reported host.
Source	nessus file > `ReportHost/HostProperties/tag/[@name='host-fqdn']`
Post-processing	Value changed to lowercase.
Column type	`debug`, `default`

4.4.7 IP

Table 127: IP - column details

Header name	IP
Description	IP of reported host.
Source	nessus file > `ReportHost/HostProperties/tag/[@name='host-ip']`
Post-processing	*none*
Column type	`debug`, `default`

4.4.8 Scanned

Table 128: Scanned - column details

Header name	Scanned
Description	Information if target host has been scanned. • `yes` if target host is on the list of reported hosts. • `no` if target host is not on the list of reported hosts.
Source	nessus file > `Preferences/ServerPreferences/preference/[name='TARGET']/value` nessus file > `ReportHost/[@name='name']`
Post-processing	*none*
Column type	`debug`, `default`

4.4.9 Credentialed checks

Table 129: Credentialed checks - column details

Header name	Credentialed checks
Description	Information if reported host has been scanned with credentialed checks.
Source	nessus file > `ReportHost/ReportItem/[pluginID="19506"]/plugin_output`
Post-processing	1. If Plugin ID 19506 output exist extract `yes` or `no` from output line with `Credentialed checks :`. 2. If Plugin ID 19506 output does not exist return `no`.
Column type	`debug`, `default`

See also:

Read more about this plugin on Tenable website https://www.tenable.com/plugins/nessus/19506

4.4.10 Policy name

Table 130: Policy name - column details

Header name	Policy name
Description	Policy name selected by user during scan setting up.
Source	nessus file > `Policy/policyName`
Post-processing	*none*
Column type	`debug`

4.4.11 Plugin ID

Table 131: Plugin ID - column details

Header name	Plugin ID
Description	Exact Plugin ID returned by Nessus.
Source	nessus file > `ReportHost/ReportItem/[@pluginID]`
Post-processing	*none*
Column type	`debug`, `default`

4.4.12 Plugin name

Table 132: Plugin name - column details

Header name	Plugin name
Description	Exact Plugin Name returned by Nessus.
Source	nessus file > `ReportHost/ReportItem/[@pluginName]`
Post-processing	*none*
Column type	`debug`, `default`

4.4.13 Plugin type

Table 133: Plugin type - column details

Header name	Plugin type
Description	Exact Plugin type returned by Nessus.
Source	nessus file > `ReportHost/ReportItem/plugin_type`
Post-processing	*none*
Column type	`debug`, `default`

4.4.14 Risk Factor

Table 134: Risk Factor - column details

Header name	Risk Factor
Description	Exact Plugin Risk Factor returned by Nessus.
Source	nessus file > `ReportHost/ReportItem/risk_factor`
Post-processing	*none*
Column type	`debug`, `default`

4.4.15 Plugin family

Table 135: Plugin family - column details

Header name	Plugin family
Description	Exact Plugin Family returned by Nessus.
Source	nessus file > `ReportHost/ReportItem/[@pluginFamily]`
Post-processing	*none*
Column type	`debug`, `default`

4.4.16 Compliance plugin file

Table 136: Compliance plugin file - column details

Header name	Compliance plugin file
Description	Information if this is Compliance plugin.
Source	nessus file > `ReportHost/ReportItem/compliance/`
Post-processing	*none*
Column type	`debug`

4.4.17 Plugin file name

Table 137: Plugin file name - column details

Header name	Plugin file name
Description	Exact Plugin file name returned by Nessus.
Source	nessus file > `ReportHost/ReportItem/fname`
Post-processing	*none*
Column type	`debug`

4.4.18 Plugin version

Table 138: Plugin version - column details

Header name	Plugin version
Description	Exact Plugin version returned by Nessus.
Source	nessus file > `ReportHost/ReportItem/script_version`
Post-processing	*none*
Column type	`debug`, `default`

4.4.19 Plugin publication date

Table 139: Plugin publication date - column details

Header name	Plugin publication date
Description	Exact Plugin publication date returned by Nessus.
Source	nessus file > `ReportHost/ReportItem/plugin_publication_date`
Post-processing	Return in format `yyyy-mm-dd`.
Column type	`debug`, `default`

4.4.20 Plugin modification date

Table 140: Plugin modification date - column details

Header name	Plugin modification date
Description	Exact Plugin modification date returned by Nessus.
Source	nessus file > `ReportHost/ReportItem/plugin_modification_date`
Post-processing	Return in format `yyyy-mm-dd`.
Column type	`debug`, `default`

4.4.21 Check name

Table 141: Check name - column details

Header name	Check name
Description	Exact Compliance Check name returned by Nessus.
Source	nessus file > `ReportHost/ReportItem/"cm:compliance-check-name", namespaces={'cm': 'http://www.nessus.org/cm'}/`
Post-processing	*none*
Column type	`debug`, `default`

4.4.22 Audit file name

Table 142: Audit file name - column details

Header name	Audit file name
Description	Exact Compliance Audit file name returned by Nessus.
Source	nessus file > `ReportHost/ReportItem/"cm:compliance-audit-file", namespaces={'cm': 'http://www.nessus.org/cm'}/`
Post-processing	*none*
Column type	`debug`, `default`

4.4.23 Check ID

Table 143: Check ID - column details

Header name	Check ID
Description	Exact Compliance Check ID returned by Nessus.
Source	nessus file > `ReportHost/ReportItem/"cm:compliance-check-id", namespaces={'cm': 'http://www.nessus.org/cm'}/`
Post-processing	*none*
Column type	`debug`

4.4.24 Current value

Table 144: Current value - column details

Header name	Current value
Description	Exact Compliance Check current value returned by Nessus.
Source	nessus file > `ReportHost/ReportItem/"cm:compliance-actual-value", namespaces={'cm': 'http://www.nessus.org/cm'}/`
Post-processing	*none*
Column type	`debug`, `default`

4.4.25 Uname

Table 145: Uname - column details

Header name	Uname
Description	Exact Compliance Check uname returned by Nessus.
Source	nessus file > `ReportHost/ReportItem/"cm:compliance-uname", namespaces={'cm': 'http://www.nessus.org/cm'}/`
Post-processing	*none*
Column type	`debug`

4.4.26 Description

Table 146: Description - column details

Header name	Description
Description	Exact Compliance Check description returned by Nessus.
Source	nessus file > `ReportHost/ReportItem/"cm:compliance-info", namespaces={'cm': 'http://www.nessus.org/cm'}/`
Post-processing	*none*
Column type	`debug`, `default`

4.4.27 Check status

Table 147: Check status - column details

Header name	Check status
Description	Exact Compliance Check status returned by Nessus.
Source	nessus file > `ReportHost/ReportItem/"cm:compliance-result", namespaces={'cm': 'http://www.nessus.org/cm'}/`
Post-processing	*none*
Column type	`debug`, `default`

4.4.28 Reference

Table 148: Reference - column details

Header name	Reference
Description	Exact Compliance Check reference returned by Nessus.
Source	nessus file > `ReportHost/ReportItem/"cm:compliance-reference", namespaces={'cm': 'http://www.nessus.org/cm'}/`
Post-processing	*none*
Column type	`debug`, `default`

4.4.29 Error

Table 149: Error - column details

Header name	Error
Description	Exact Compliance Check error returned by Nessus, if error occur.
Source	nessus file > `ReportHost/ReportItem/"cm:compliance-error", namespaces={'cm': 'http://www.nessus.org/cm'}/`
Post-processing	*none*
Column type	`debug`, `default`

CHAPTER 5

Meta

5.1 Changelog

See CHANGELOG.

5.2 Licence

GNU GPLv3: LICENSE.

5.3 Authors

Damian Krawczyk created *nessus file analyzer* by LimberDuck.