TENABLE
Network Security®

# Nessus 3.0
# Client Guide

**March 31, 2006**
**(Revision 3)**

# Table of Contents



**Note:** Currently Tenable Network Security, Inc. is going through a name change process for all of our products. The directories, commands, configuration files, etc. will still reflect the old names for the Log Correlation Engine and Passive Vulnerability Scanner until new versions are released. Tenable would like to thank you for your patience through this process.

Lightning will be known as **Security Center**
Thunder will be known as **Log Correlation Engine**
NeVO will be known as **Passive Vulnerability Scanner**

# Introduction

Welcome

Welcome to Tenable Network Security's **Nessus 3.0** Client Guide. As you read this document, please share your comments and suggestions with us by emailing them to support@tenablesecurity.com.

This document will discuss the different clients that are available for the Nessus vulnerability scanner. Originally created by Renaud Deraison, Tenable Network Security, Inc. (Tenable) is now the primary manager and supporter of Nessus. More than 95% of all the plugins available for Nessus can be attributed to Tenable.

Standards and Conventions

A basic understanding of UNIX, Windows, and vulnerability scanning is assumed.

Throughout the documentation, filenames, daemons, and executables will be indicated with an italicized font such as *setup.exe.*

Command line options and keywords will be printed with the following font. Command line options may or may not include the command line prompt and output text from the results of the command. Often, the command being run will be boldfaced to indicate what the user typed. Below is an example running of the UNIX *pwd* command.

```
# pwd
/opt/nessus/
```

Important notes and considerations will also be highlighted with this yield symbol and grey text boxes.

# NessusWX

NessusWX is a client program for Nessus which is designed specially for the Windows platform. It is distributed under the terms of GNU General Public License version 2. NessusWX was originally written by Victor Kirhenshtein, but Tenable has been maintaining it with bug fixes and new features. There is more information available for NessusWX at http://nessuswx.nessus.org.

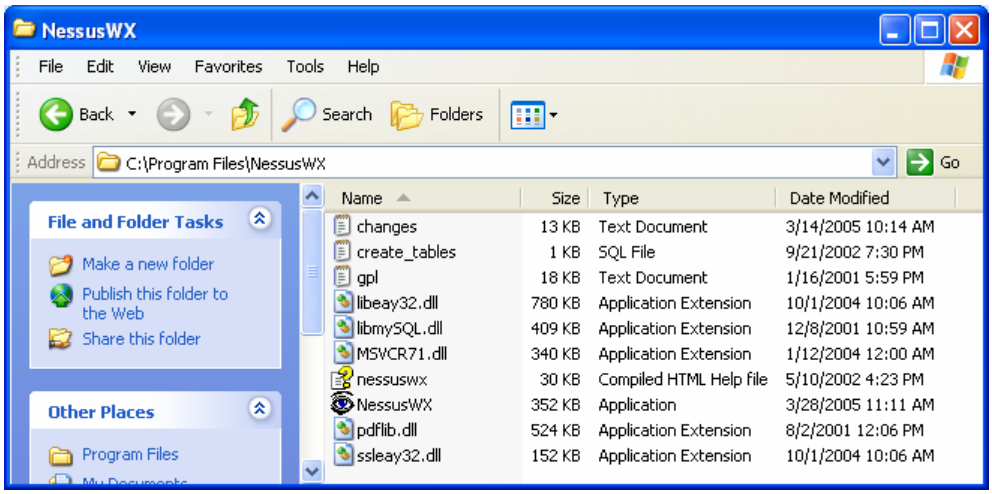
NessusWX uses a Windows-style user interface. It has support for both unencrypted and SSL communications as well as user authentication either by password or X.509 certificate. NessusWX is able to have multiple sessions each with their own specific settings and individual connection and plugins settings. There is a database where all session settings and results are saved for future use. NessusWX generates its reports in plain text, Adobe Acrobat (PDF), and HTML formats. These reports can be compared by creating reports with the differences between the two scans. In addition, scan results can be exported into NSR, extended NSR, NBE, CSV (Comma Separated Values), SQL command formats, or directly to a MySQL database. Results can be imported from NSR, extended NSR, or NBE formats.

Installation

Download the NessusWX client utility for Win32 platforms, which can be found at:

www.nessus.org/download/

The NessusWX client will download as a zip file. Unzip its entire contents, *dll*, *exe*, and other miscellaneous files into the same directory. There is no need to register the *dlls* or *exe*. The following is a screen shot of the NessusWX binaries and associated files unzipped in a Windows Directory.



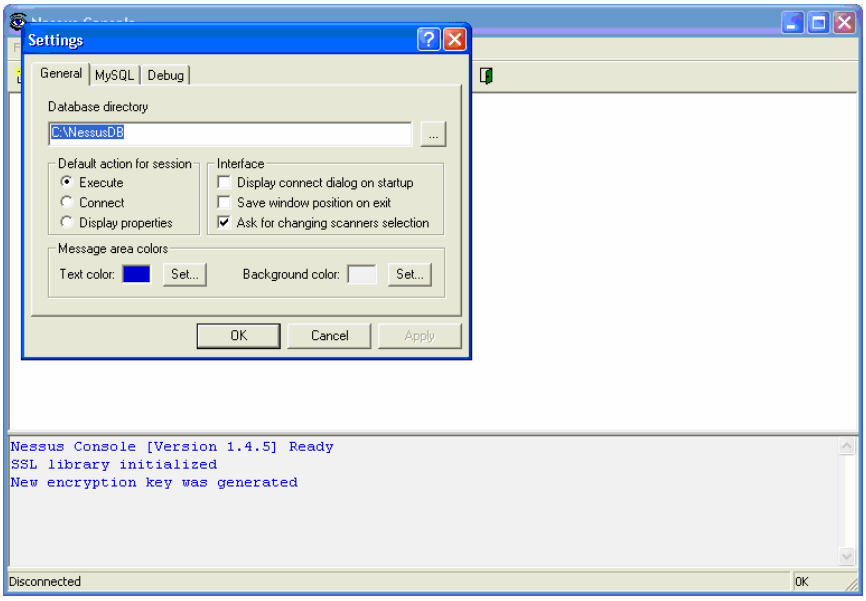

Updating NessusWX with New Releases

Download the newest version of the NessusWX utility which can be found at www.nessus.org/download/.

The NessusWX client will download as a zip file. Unzip its entire contents, *dll*, *exe*, and other miscellaneous files and copy them into the same directory where NessusWX is currently located (should be in C:\Program Files\NessusWX), overwriting the existing files. The database for Nessus is in a different location. Therefore, all the previous scan reports will be preserved.

Run NessusWX

Run the NessusWX executable by clicking on the NessusWX logo. The first time the executable is run you will be prompted for a database directory which the NessusWX client will use as a working directory for miscellaneous work files. Accept the default by clicking click OK, shown below. You will be asked to confirm your choice, click “Yes”.



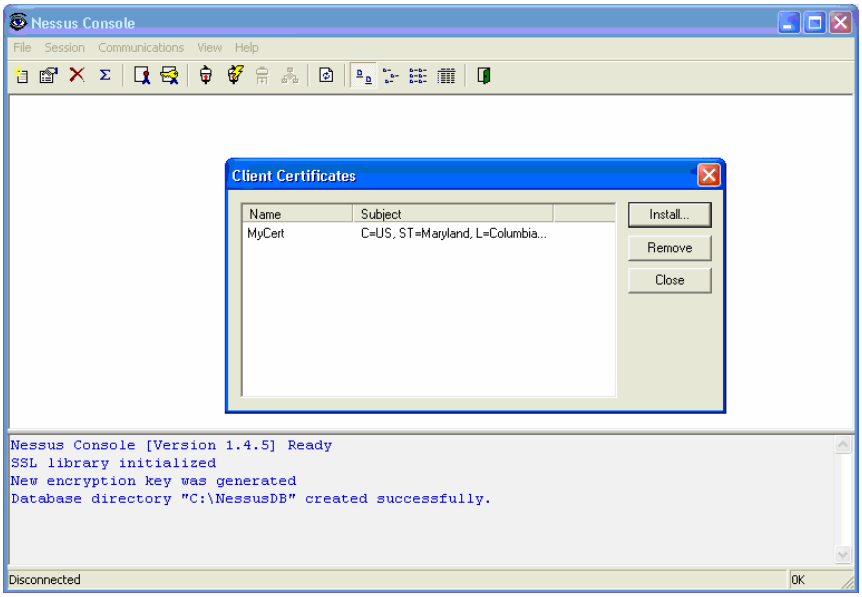

## Check Connectivity to a Nessus Scanner

Before configuring the NessusWX client to connect to a Nessus scanner, ensure there is an IP route from the NessusWX host to the Nessus scanner's management interface IP. Open a Command Prompt window and use the `tracert` command, using the IP address where the Nessus scanner is located.

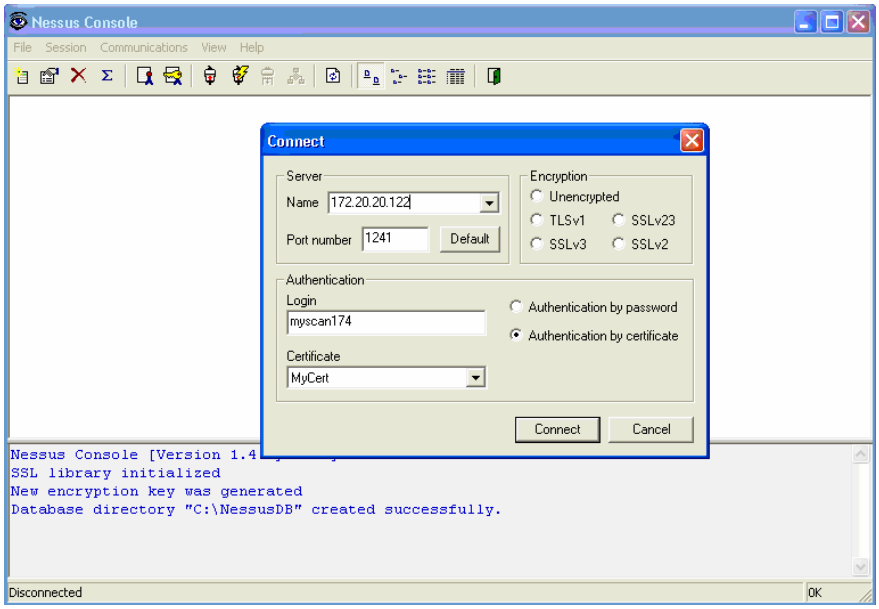
```
C:\>tracert 10.10.20.102

Tracing route to 10.10.20.102 over a maximum of 30 hops

1   <1 ms   <1 ms   <1 ms 10.10.101.1
2   1 ms    <1 ms   <1 ms 10.10.20.102

Trace complete.

C:\>
```

## Connect to a Nessus Scanner

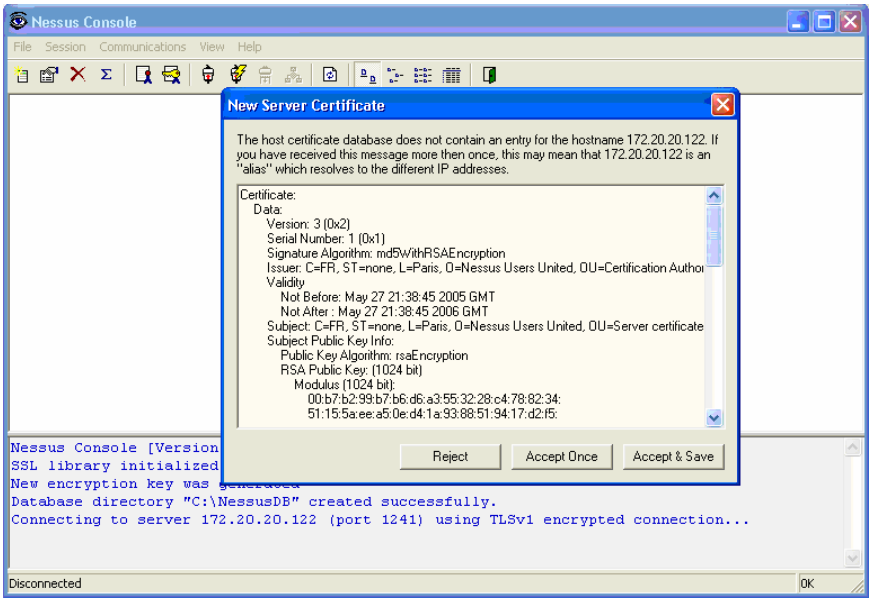
If you configured the Nessus scanner with a user for certificate authentication, copy the *cert_nessuswx_**user**.pem* certificate file to the NessusWX host. Then, import it into the NessusWX client using the client certificate install function. To do this, go to the "File" menu and clicking on "Client certificate". Here is an example screen shot below:



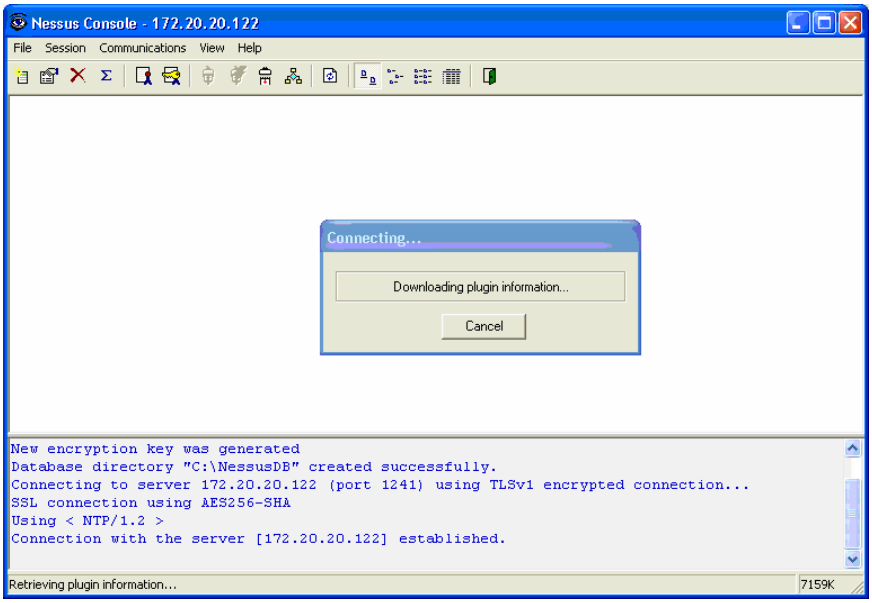

In the NessusWX GUI go to the "Communications" menu and choose "Connect". Enter the Nessus scanner IP and port (1241 is the default port). Enter the Nessus user details which will be used to authenticate the connection to the Nessus scanner. If you are using the certificate based authentication and installed the client certificate, then it should be listed in the certificate drop down list when the "Authentication by certificate" radio button is clicked, as seen below. Otherwise, enter the password.




Click "Connect" and NessusWX will attempt to connect to the Nessus scanner. If a successful connection is made you will be prompted to accept the Nessus server certificate, as shown below. Click Accept Once.




The Nessus plugins will be retrieved from the scanner and a pop-up window will indicate that NessusWX is downloading the plugins.



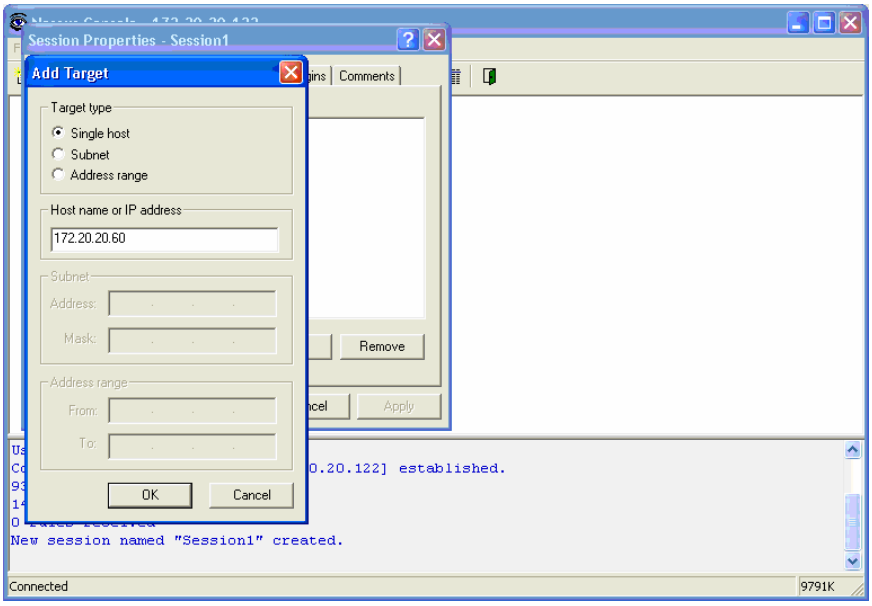

NessusWX downloads the Nessus scanner's plugin titles so that when configuring a scan you will have the ability to pick and choose plugins to be executed.

## Creating an Initial Test Scan Session

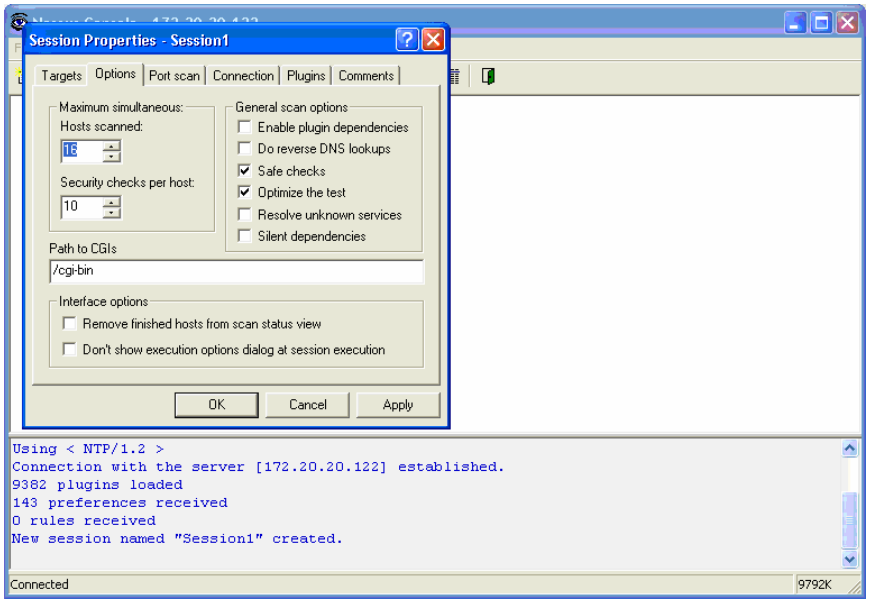
Please note that when the previous section is completed a connection is left open to a Nessus scanner. This connection must be up to follow the next step precisely.

To run a test vulnerability scan, you first create a scan session using the NessusWX client. Go to the "Session" menu and choose "New". Accept the default name and click "Create".

Under the “Targets” tab click the “Add” button and enter the IP of a host you can safely run a test scan against and click “OK”.




It would be wise to look under the “Options” tab to ensure that “Safe checks” is checked. Refer to the “Configuring NessusWX” for more information on the configuration options.



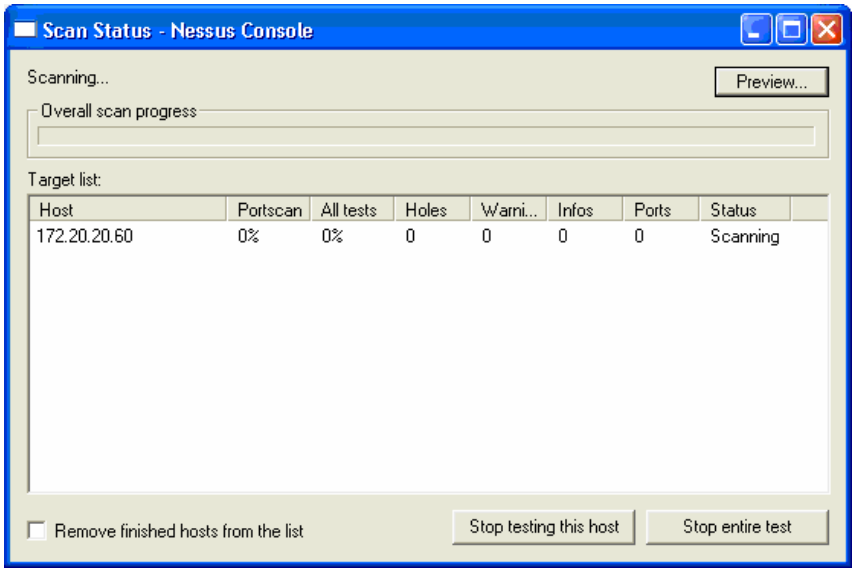

Click “Apply” to accept the changes made for the host to be scanned, the target, and then click “OK”.

## Start a Scan

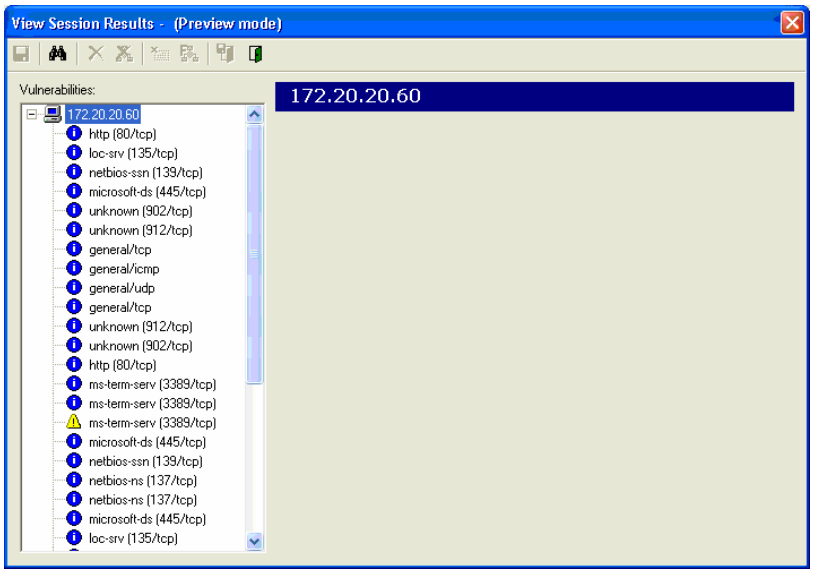
To start a scan with the session attributes we just configured right click on the session icon and select “Execute”. The scan is going to use the existing connection to the Nessus scanner, provided the connection is still active, and will start executing. If the connection is

not available, return to the previous step to reinitiate a connection. Please note for multiple scanners it is possible to set up connection attributes on a per session configuration basis. But, by default a session will be configured to use the current Nessus scanner connection initiated in the NessusWX client from the main menu bar.

At the pop-up Execute Scan window accept all defaults and click Execute. A window will indicate the progress of your scan, as seen below:




When the scan status is “Finished” click the preview button to see the results of the scan.




Configuring NessusWX

To configure a specific scan session, right click on the session and choose “Properties…”. You will be presented with various tabs that each contain different configuration options.

The first tab is called “Targets”. This is where you add the IP of a host you want to run a scan against. You can choose to enter a single host, a subnet, or a mask to scan. You can also import, edit, and remove the targets.

Next is the “Options” tab. Here you choose how many simultaneous hosts you want scanned and how many simultaneous security checks per host to perform at the same time. You can also choose options such as enabling plugin dependencies, safe checks, optimize the test, silent dependencies, etc. In addition, this is where you specify the path to check for CGIs, choose to remove finished hosts from the scan status view, and choose to not show the execution options dialog at session execution.

Within the “Port scan” tab you can specify the port range to scan. You can choose to scan well-known services, privileged ports, or a specific range of ports. Then, you select the port scanners you want to use. Port scanners are a category of plugins specific to scanning ports. Therefore, they are kept separate from the rest of the plugins.

The next tab is the “Connection” tab. If you want each session to be connected to a different server, this is where you choose to do that. After you check the box “Use session-specific connection information”, you enter in the connection information for the server.

In the “Plugins” tab you can choose to use specific plugins for the session. After checking the box “Use session-specific plugin set”, you can browse and choose the plugin families or individual plugins that you want. Also, you can disable all of the Denial of Service plugins.

The final tab is the “Comments” tab. Here you can add any additional comments about the particular session.

## Nessus GTK Client

NessusClient is a new X11/GTK UNIX GUI for Nessus that is based on the historic “nessus” client. The Nessus GTK Client has been available for several years and has been maintained by Tenable. In the fall of 2005, with the help of Tenable, Intevation GmbH extended this client to include support for scanning sessions and ported released a GTK build for the Windows platform.

NessusClient has a nicer and easier to use GUI. It contains support for “Scopes” and “Tasks” which will keep track of all the past scans and past plugin settings. NessusClient has the ability to run multiple scans at the same time. The reports can be exported as PDF, HTML, XML, etc. In addition, NessusClient contains a “Scan Assistant” feature that takes you through a step by step process of creating a task, a scope, and running a scan.

You can download NessusClient RPM from www.nessus.org/download/. For further information on using the NessusClient, there is a User Guide included with the download under the “Help” menu item.

## Command Line Operation

Running a Scan

Users are not required to use a client to connect to the *nessusd* server and run a scan. They can choose to use command line operation to do this.

In order to run a scan using command line operation, you must run the scan in batch mode. To do this, use the following command:

**# /opt/nessus/bin/nessus –q [-pPS] <host> <port> <user> <password> <targets-file> <result-file>**

The table below explains the various arguments used to run a scan in batch mode.

| Argument | Description |
|---|---|
| -p | Obtain a list of the plugins installed on the server. |
| -P | Obtain a list of the server and plugin preferences. |
| -S | Issue SQL output for -p and -P. |
| <host> | The *nessusd* host to connect to. |
| <port> | The port to which you will connect to on the remote *nessusd* host. |
| <user> | The user name to connect to *nessusd* with. |
| <password> | The password associated with user name. |
| <targets> | The name of the file containing the target machines to be scanned. |
| <results> | The name of the file where the results will be stored at the completion of the scan. |

There are other options that are also available when running a scan in batch mode. These are explained in the following table.

| Option | Description |
|---|---|
| -V | Make the batch mode display status messages to the screen. |
| -x | Do not check SSL certificates. |
| -v | Display the version number and exit. |
| -h | Show a summary of the commands and exit. |
| -T <type> | Save the data as <type>, where <type> can be “nbe”, “text”, “xml”, or “nsr”. |

Converting a Report

You can use nessus to do a conversion between report formats. Nessus can take any NSR or NBE reports and change them into XML, NSR, NBE, or text reports.

Use the following command to convert a report:

```
# /opt/nessus/bin/nessus –i in.[nsr|nbe] –o out.[xml|nsr|nbe|txt]
```

The option `–i` specifies the file that is being converted, which can be either NSR or NBE reports. The option `–o` specifies the file name and type that the report will be converted to, which can be XML, NSR, NBE, or text reports.

## For Further Information

Tenable hopes your experience with Nessus is very positive, and we strongly encourage you to contact us via email or phone to discuss any issues you have. Tenable has produced a variety of other documents detailing Nessus' installation, deployment, configuration, user operation, and overall testing. These are listed here:

- **Nessus Installation Guide** – step by step walk through of installation
- **Nessus Advanced User Guide** – elaborates on some of Nessus' "dustier corners" by explaining additional features
- **Nessus Credential Checks for UNIX and Windows –** information on how to perform authenticated network scans with the Nessus vulnerability scanner

Please feel free to contact us at support@tenablesecurity.com, sales@tenablesecurity.com or visit our web site at http://www.tenablesecurity.com. For more information about Nessus, please visit http://www.nessus.org.

## *About Tenable Network Security*

*Tenable, located in Columbia, Md., develops enterprise security solutions that provide vulnerability management, intrusion detection, and security event notifications across entire organizations for effective network security management. Tenable is uniquely positioned to detect vulnerabilities with active and passive scanning and analysis, and host-based patch monitoring for enterprise networks. Key product lines include: Nessus Vulnerability Scanner, the leading global technology utilized for vulnerability scanning; Passive Vulnerability Scanner (formerly NeVO), for passive vulnerability monitoring; Security Center (formerly Lightning Console), for enterprise security management; and Log Correlation Engine (formerly Thunder), for secure log aggregation and analysis. For more information, please visit us at www.tenablesecurity.com.*

**TENABLE Network Security, Inc.**
8830 Stanford Blvd.
Suite 312
Columbia, MD 21045
TEL: 1-877-448-0489
www.tenablesecurity.com