

Publication Date: 9/19/2004

Running your first scan using NessusWX

Author

Lew Newlin is CTO of [SiteRecon](#), a provider of internet [email monitoring](#) and [web site monitoring](#) services for business.

Guide

The following is a simple how-to guide for installing, configuring, and running your first vulnerability scan using the NessusWX Windows client. The instructions do not include in depth explanations as it is assumed that you are familiar with benefits of using Nessus and have a general working knowledge of Windows.

As with any software installation, your results may vary depending on the machine operating system and patch levels being used. The installation steps were conducted using of NessusWX 1.4.4 on several Windows operating systems and patch levels including XP, 2000, and 2003 Server to insure accuracy. It is recommended that the installation be conducted using the "admin" account or equivalent to avoid rights issues.

Install NessusWX

- Download and save the self-extracting version of NessusWX for Intel platforms from <http://nessuswx.nessus.org/> to a temp directory on your hard drive. (nessuswx-1.4.4-install.exe, 1413KB in size);
- Double-click NessusWX-1.4.4-install.Exe to start the installation process;
- If using XP/SP2 you may be prompted with a warning message that "the publisher could not be verified" click <Run>;
- At the "Welcome to the Installation Wizard" screen click <Next>;
- At the "License Agreement" screen read the license terms, check "Yes, I agree with all the terms of this license agreement", click <Next>;
- At the "Destination Folder" screen enter the desired location for NessusWX, or accept the default of C:\Program Files\NessusWX, click <Next>;
- At the "Setup Type" screen select "Binaries Only", or if you wish the source files included select "Binaries & Source", click <Next>;
- At the "Program Group" screen select the desired program group, or leave at the default of NessusWX, click <Next>;
- At the "Ready to Install the Program" screen click <Next>;
- At the "Installation Complete" screen click <Ok>.

If the installation process completed successfully, you now have a NessusWX desktop icon and Start/Programs/NessusWX menu listing.

Configuration of NessusWX

Before configuring the NessusWX client, you need some information concerning the Nessus server you will be using. Please contact you Nessus server administrator for assistance if needed.

Nessus server IP: _____
Nessus port number: _____ (default is 1241)
Max simultaneous hosts: _____ (default is 16)
Max security checks per host: _____ (default is 10)
Your Nessus login name: _____
Your Nessus login password: _____

Maximum simultaneous hosts, and maximum security checks per host, refers to the number simultaneous scans that will be performed. It is possible to optimize a Nessus server to support more then the default settings and to use a different port. If in this information is not available or unknown use the default values.

Your Nessus Server administrator has the ability to limit what IP range(s) you can scan based on your login name. Speak with your Nessus server administrator and determine what limits, if any, have been established.

- Upon executing NessusWX you will be prompted with the “Settings” screen, “General” tab, requesting database directory information. By default NessusWX uses C:\NessusDB to store scan result. The database location can be a network drive if you wish to store results on a network drive for security purposes. Select the defaults value or change to the desired directory, click <Ok>;
- If the directory you selected does not exist, you will be prompted with a creation message, click <Yes>;
- Select “Communications/Connect” menu option
 - Change the default Server “Name”, from 127.0.0.1, to the desired Nessus server;
 - Change the default Server “Port Number”, from 1241, to the desired Nessus server port if needed;
 - By default, NessusWX selects TLSv1 as encryption option;
 - Select “Authentication by Password” radio button;
 - Check save password checkbox;
 - Change the default Authentication “Login” value to your Nessus login name;
 - Enter your Nessus login name password, click <Connect>;
 - You will be prompted with “New Server Certificate” window displaying the Nessus server certificate information, click <Accept & Save>.

If the userid/password information you entered is correct, you will receive a brief message that NessusWX is downloading plugin information. Upon download completion, something similar to the following will be displayed at the bottom of the NessusWX screen:

```
Using <NTP/1.2>
Connection with the server [xxx.xxx.xxx.xxx] established
xxxx plugins loaded
xxxx preferences received
xxxx rules received
```

You now have a fully functioning copy of NessusWX installed, have connected to the Nessus Server, and are ready to being performing vulnerability scans.

Before You Scan

Before performing vulnerability scanning, a few cautions and recommendations should be considered:

- Make sure you are acting within your authority. Most companies have strict policies about who can perform vulnerability scanning and on what equipment. Acting outside your authority with a vulnerability scanner could lead to your dismissal;
- Absent Nessus server based rules that limit what IP ranges you can test, obtain written permission on what you are and are not permitted to perform vulnerability test on;
- Vulnerability scanning can leave equipment in an unstable state. This is practically true if performing Denial of Service tests and/or testing systems are very poorly configured. Nessus vulnerability scanning is normally not destructive and rebooting the affected equipment will return it to the correct operational state;
- NessusWX has a selection for “Safe checks” that disables the most dangerous scripts from executing and instead relies on banners information to determine vulnerability rather than exploiting the real flaw. However, it is still possible to leave equipment in an unstable state;
- If your company uses an intrusion detection system, performing vulnerability scanning on the network will most likely trigger intrusion alerts. Vulnerability scanning is very “noisy” and easily detected by most intrusion detection systems;
- If you are performing vulnerability scans across the internet verify your ISP will not object, that your scanning will not trigger their intrusion detection system, and request documentation concerning scanning polices and rules that you must follow;
- Exercise common sense when performing vulnerability scans. For example, it's most likely not a good idea to run a Denial of Services test on your core router during normal business hours;

- NEVER SCAN EQUIPMENT THAT YOU ARE NOT EXPRESSLY AUTHORIZED TO SCAN. Doing so could result in lawsuits, bad press, jail, ISP termination, and unemployment just to name a few. Running a Denial of Services test against your competitor's web site for example, will most likely result in several unwanted events occurring once you and your company are identified as the cause.

Performing Your First Scan

To perform your first vulnerability scan, you must create a Session (job) outlining the targets and scanning options desired.

- Click menu selection Session/New;
- You will be prompted to enter a session name or accept the default of "Session1". Enter "First Scan", leave "Define additional properties" checked, click <Create>;
- At the "Session Properties – Test Scan", click the "Targets" tab, then click <Add>;
- At the "Add Target" screen you have the option of entering a single host, a subnet, or IP range depending on scanning needs. For our test session, select a single IP address and enter the IP or Host name of your workstation, click <Ok>;
- Click <Apply>.
- Click the "Options" tab:
 - Change "Maximum simultaneous" default value if needed;
 - Change "Security checks per host" default value if needed;
 - "General scan options/Enable plugin dependencies". Nessus uses many plugins (tests) that require the use of other plugins to operate correctly. Checking this box permits Nessus to automatically enable test dependencies as needed. For our test scan, "Enable plugin dependencies" should be checked;
 - "General scan options/Do reverse DNS lookups" simply performs a DNS lookup on the target to determine the host name. For our test scan, check "Do reverse DNS lookups";
 - "General scan options/Safe checks". As stated previously, Safe Checks disables the most dangerous scripts from executing and instead relies on banners information to determine vulnerability rather than exploiting the real flaw. For our test scan, leave "Safe checks" checked;
 - "General scan options/Optimize the test" lets Nessus avoid all apparently irreverent tests. For example, tests will not be conducted for web site unless a web site is detected. For our test scan, leave "Optimize the test" checked;
 - "General scan options/Resolve unknown services" will permit Nessus to resolve any unknown services that may be operating on the system. For our test scan, leave "Resolve unknown services" checked;
 - "Path to CGI's". Nessus has the ability to check for generic CGI vulnerabilities that may be present. For our test scan, leave "Path to CGI's" at the default of "/cgi-bin";
 - "Interface options" permits you to limit the results that are displayed on the screen while scanning is occurring. For our test scan, leave both items unchecked to display the maximum amount of information;
 - Click <Apply>.
- Click the "Port scan" tab:
 - "Port range to scan" permits you to enter the ports Nessus will scan. For our test scan, we will use the default of "Privileged ports (1-1024)";
 - "Port scanners" permits the use of a wide range of port scanners depending on your needs. For our test scan, leave the default of "Ping the report host" and "tcp connect scan" checked.
 - Click <Apply>.
- Click the "Connection" tab will permit you to enter and store specifics about the Nessus server to be used for the session. Since we are currently connected to a specific Nessus server, no need exists to enter this information for our test scan;
- Click the "Plugins" tab:
 - To test for system vulnerability we must enable plugins. Check the "Use session-specific plugin" checkbox. You will notice that currently "0 plugins currently are selected for execution";
 - Click the "Select plugins..." button to display the "Plugin List" screen. For our test scan, click the "Enable All" button, click <Yes>, when prompted with "Do you wish to enable all port scanners as well", click <Close>. You will notice that 2400 or so plugins are now selected for execution;
 - Click <Apply>.

- Click the “Comments” tab and input any remarks you have concerning this session or its settings, then click <Ok> to save your Session;

To execute the Session, right-click on the icon and then select <Execute>. When prompted at the “Execute Session” screen simply click Execute and vulnerability scanning will commence.

Take some time, experiment, and learn what NessusWX and Nessus have to offer. Patch systems and rescan to verify vulnerability have been closed. Using NessusWX and Nessus will permit you to find system vulnerabilities before hackers and virus/worm writers have opportunity to do it for you!

Copyright 2004, Information Solutions, Inc., All rights reserved.