NeWT 2.1
User Guide

(December 2004)

TENABLE
Network Security®

Table of Contents

Introduction

This document will discuss the basic installation and usage of Tenable Network Security's "NeWT" and "NeWT Pro". NeWT is a Microsoft Windows based vulnerability scanner. NeWT stands for "Nessus Windows Technology".

Tenable is the primary manager and supporter of the Nessus project. More than 95% of all the plugins available for Nessus can be attributed to Tenable.

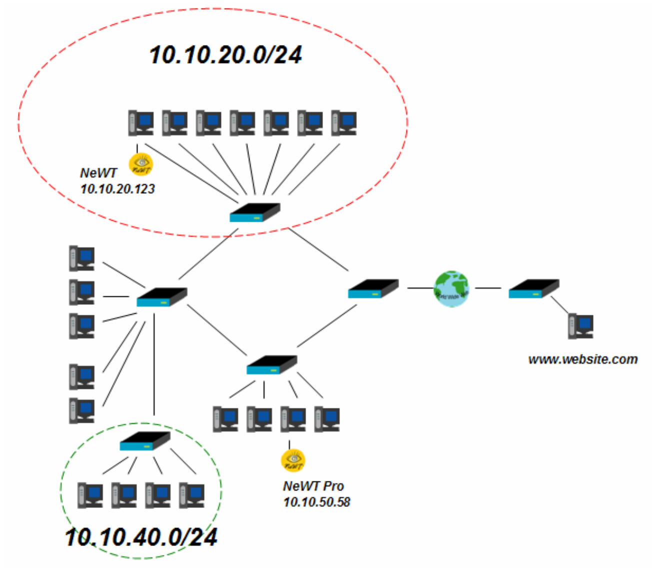
Prerequisites, deployment options, an example walk-through of an installation, and some initial 'quick start' strategies will be discussed in this document.

A basic understanding of Windows and vulnerability scanning is assumed. Throughout the documentation, filenames, daemons and executables will be indicated with an italicized font such a *setup.exe*.

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

NeWT and NeWT Pro Licenses

Two different types of licenses are available for NeWT. These are the NeWT and NeWT Pro licenses. These two products are identical except for one major feature difference. NeWT scanners can only scan their local "Class C" network space. NeWT Pro scanners can scan any desired IP address.



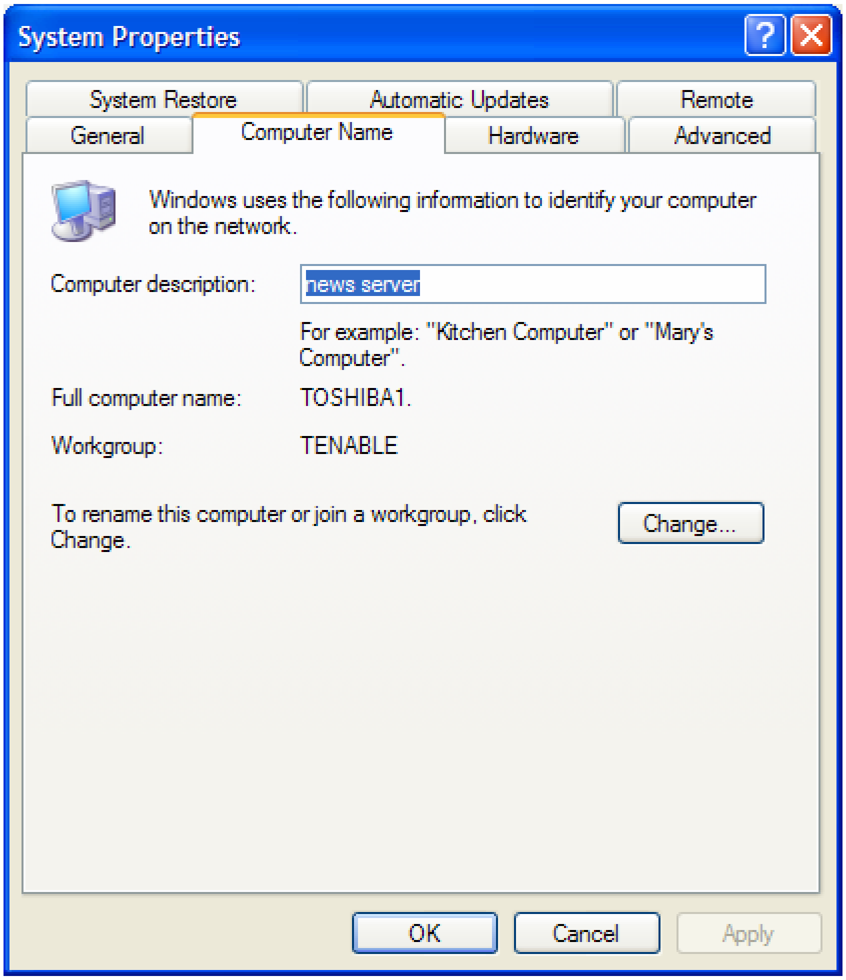
In the above diagram, a NeWT scanner is connected to the 10.10.20.0/24 subnet with a system IP address of 10.10.20.123. When launching vulnerability scans, a NeWT licenses would only permit scanning of the 10.10.20.0/24 subnet. Scanning of external websites (such as the www.website.com shown) or other networks (such as the 10.10.40.0/24 shown) would not be permitted.

However, the NeWT Pro license installed at 10.10.50.58 would have no limitation. It would be allowed to scan any host shown on the network.

⚠ If the NeWT license were moved to the 10.10.40.0/24 network, it would be able to scan that network.

Any NeWT scanner can be converted to a commercially supported NeWT Pro license by contacting sales@tenablesecurity.com.

Tenable uses a copy-protection scheme for NeWT Pro which is based on the hostname of the system it is being running on. To determine the hostname of a particular system, two techniques can be used. From the “Control Panel” and “System” menus, the tab for “Computer Name” can be selected as shown below. The hostname of the system shown below is “TOSHIBA1”. This would be the name to send to Tenable and the keys generated by Tenable would only work on this machine.



Windows uses the following information to identify your computer on the network.

Computer description: news server

For example: "Kitchen Computer" or "Mary's Computer".

Full computer name: TOSHIBA1.

Workgroup: TENABLE

To rename this computer or join a workgroup, click Change.

Prerequisites

NeWT and NeWT Pro are capable of running on Windows 2000 and Windows XP platforms. A resident copy of Microsoft's Internet Explorer is required.

To forge custom TCP/IP packets, NeWT uses the WinPcap driver. WinPcap is a freeware architecture for packet capture and network analysis on Win32 platforms. It includes a kernel-level packet filter, a low-level dynamic link library (packet.dll), and a high-level and system-independent library (wpcap.dll, based on libpcap version 0.6.2). It can be downloaded from http://winpcap.polito.it. If the system to be used for NeWT has already had a version of WinPcap installed, do not have the installation program re-install it.

Tenable recommends a minimum of a Pentium II 600 Mhz class system to operate NeWT on a "class C" network. For "class C" networks, a minimum of 512MB of memory is also suggested. To conduct larger scans of multiple networks, Pentium 4 class systems with at least 1 GB of memory are recommended. Modern hard drive space does not really impact NeWT, as worst case scans of Class C networks only take 1-2 MB of disk space. Scanning performance can be enhanced by using an NTFS file system.

NeWT can be run under a VMWARE instance, but if the simulated machine is using network address translation (NAT) to reach the network, many of NeWT's vulnerability checks, host enumeration and operating system identification will be negatively affected.

Network card compatibility for NeWT is mostly dependant on the WinPcap driver. Tenable provides free downloads of NeWT to facilitate testing for potential customers. Tenable is aware that some network cards, particularly 2-3 year old PCMCIA cards for laptops, do not work with the WinPcap driver.

When deploying NeWT, knowledge of routing, filters and firewall policies should be considered. NeWT should be deployed such that it has good IP connectivity to the networks it is scanning. Deploying behind a network address translation (NAT) device is not desirable unless it is scanning the inside of that devices network. Any time a vulnerability scan flows through a NAT or application proxy of some sort, the check can be distorted and a false positive or negative can result. Also, if the system running NeWT has personal or desktop firewalls in place, these tools can drastically limit the effectiveness of a vulnerability scan.

> ⚠ Host-based firewalls can interfere with network vulnerability scanning. Depending on how "locked down" a firewall is configured, it may prevent, distort or hide the probes of a NeWT scan.

Installation

This section will discuss installation of a NeWT.

Downloading NeWT

The latest version of NeWT is available from the Tenable Network Security web site at http://www.tenablesecurity.com. The public is required to enter in contact information to obtain the NeWT software.

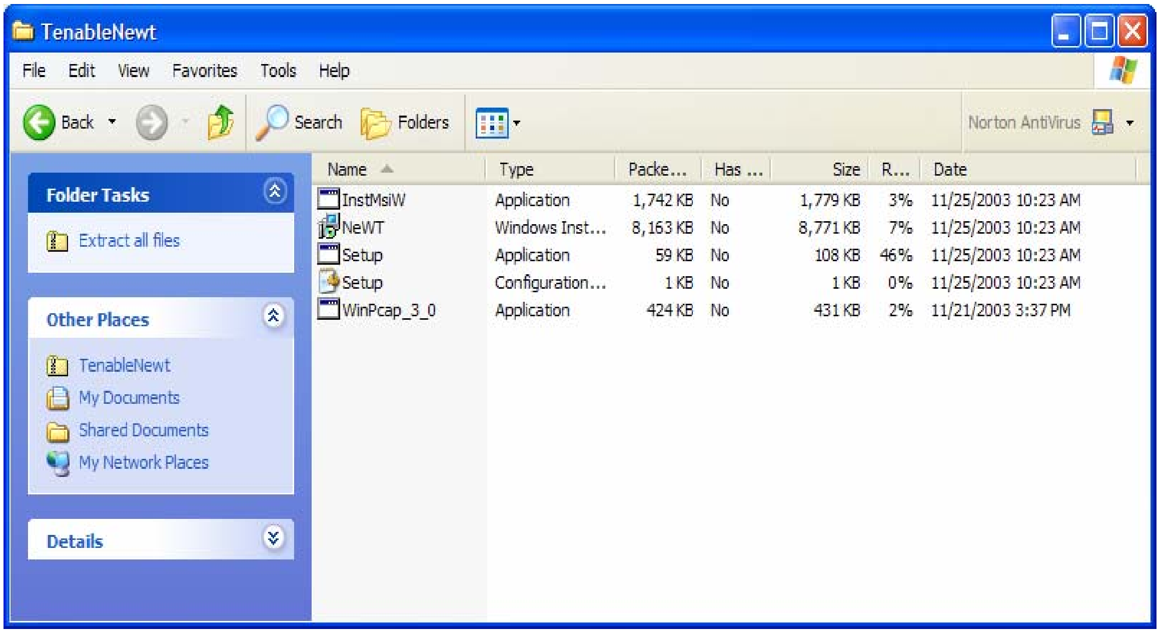
NeWT distribution file sizes and names vary slightly from release to release, but are approximately 8 MB in size.

Handling the ZIP File

Windows 2000 and Windows XP all handle ZIP archives slightly differently. Windows 2000 requires a third party tool to uncompress and unpack the NeWT distribution. On Windows 2000, all files in the NeWT distribution should be placed in a directory where they can be later executed. For Windows XP, simply clicking on the file comprising the NeWT distribution will launch a new window which is filled with all of the individual files needed to install NeWT.

Running the Installation Script

To install NeWT, simply execute the *Setup.exe* program contained within the distribution as shown below:



Name	Type	Packe...	Has ...	Size	R...	Date
InstMsiW	Application	1,742 KB	No	1,779 KB	3%	11/25/2003 10:23 AM
NeWT	Windows Inst...	8,163 KB	No	8,771 KB	7%	11/25/2003 10:23 AM
Setup	Application	59 KB	No	108 KB	46%	11/25/2003 10:23 AM
Setup	Configuration...	1 KB	No	1 KB	0%	11/25/2003 10:23 AM
WinPcap_3_0	Application	424 KB	No	431 KB	2%	11/21/2003 3:37 PM

Answering the Installation Questions

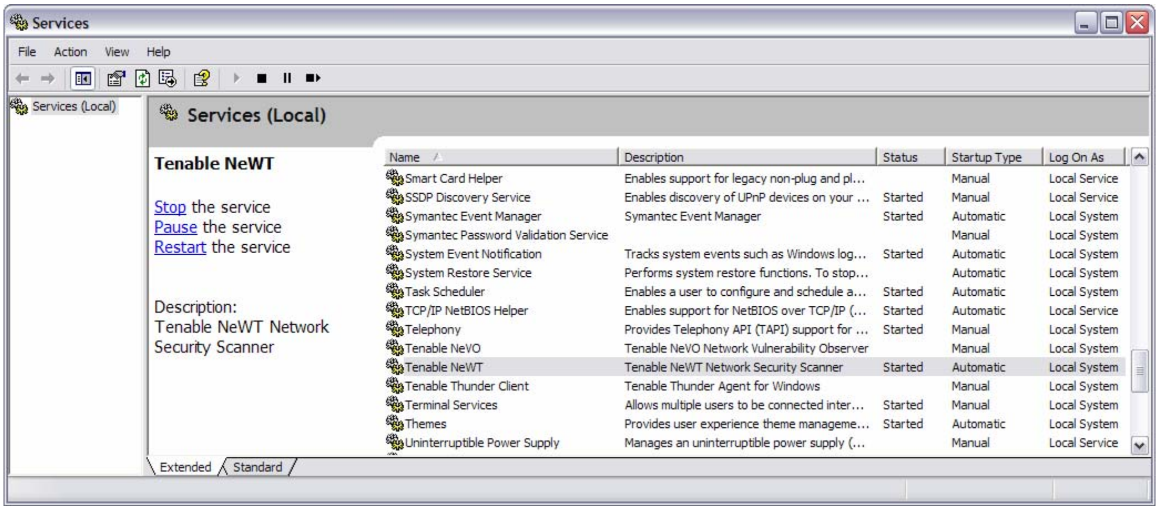
NeWT will prompt the user for some basic information such as installation directory location, software license compliancy and if the WinPcap packet driver is required.

Do not manually install the *WinPcap_3_0.exe* file unless you actually wish to install it before adding NeWT to the system. The *Setup.exe* file will prompt the user for WinPcap installation and invoke the *WinPcap_3_0.exe* file if needed.

Unless you are running Windows versions of NMAP (http://www.nmap.org) or SNORT (http://www.snort.org), you probably do not have WinPcap installed.

Tenable NeWT Service

NeWT and NeWT Pro both require a Windows service to perform their vulnerability scans. Upon installation, the “Tenable NeWT” service will be installed, configured to automatically start if the system reboots and launched. To view this service, as an administrator, log onto the “Control Panel”, select the “Administrative Tools” and then select the “Services” shortcut. The “Tenable NeWT” services should be listed as shown below:



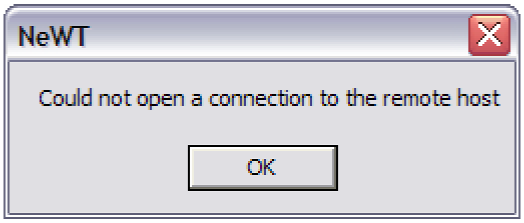
Tenable NeWT

Stop the service
Pause the service
Restart the service

Description:
Tenable NeWT Network Security Scanner

Name	Description	Status	Startup Type	Log On As
Smart Card Helper	Enables support for legacy non-plug and pl...		Manual	Local Service
SSDP Discovery Service	Enables discovery of UPnP devices on your ...	Started	Manual	Local Service
Symantec Event Manager	Symantec Event Manager	Started	Automatic	Local System
Symantec Password Validation Service			Manual	Local System
System Event Notification	Tracks system events such as Windows log...	Started	Automatic	Local System
System Restore Service	Performs system restore functions. To stop...		Automatic	Local System
Task Scheduler	Enables a user to configure and schedule a...	Started	Automatic	Local System
TCP/IP NetBIOS Helper	Enables support for NetBIOS over TCP/IP (...	Started	Automatic	Local Service
Telephony	Provides Telephony API (TAPI) support for ...	Started	Manual	Local System
Tenable NeVO	Tenable NeVO Network Vulnerability Observer		Manual	Local System
Tenable NeWT	Tenable NeWT Network Security Scanner	Started	Automatic	Local System
Tenable Thunder Client	Tenable Thunder Agent for Windows		Manual	Local System
Terminal Services	Allows multiple users to be connected inter...	Started	Manual	Local System
Themes	Provides user experience theme manageme...	Started	Automatic	Local System
Uninterruptible Power Supply	Manages an uninterruptible power supply (...		Manual	Local Service

This service can be configured to be launched manually, but the NeWT user must remember to start it when performing a scan. If the "Tenable NeWT" service is not running, the user will be prompted with an error (shown below) when a scan is launched.

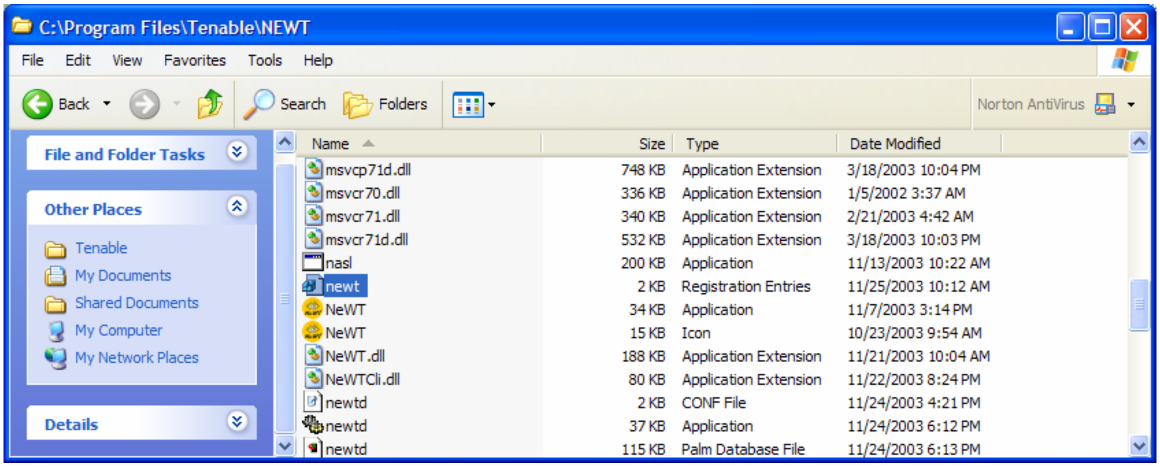


Could not open a connection to the remote host

NeWT Pro and NeWT Pro Demo Keys

The NeWT distribution does not include any demo license keys and does not expire in any way. To test the functionality of NeWT Pro, or to upgrade NeWT to a NeWT Pro commercial license, Tenable will distribute license keys. Demo newt Pro license keys will normally expire in seven days.

To replace or upgrade a NeWT Pro key, stop and exit NeWT if it is currently running.



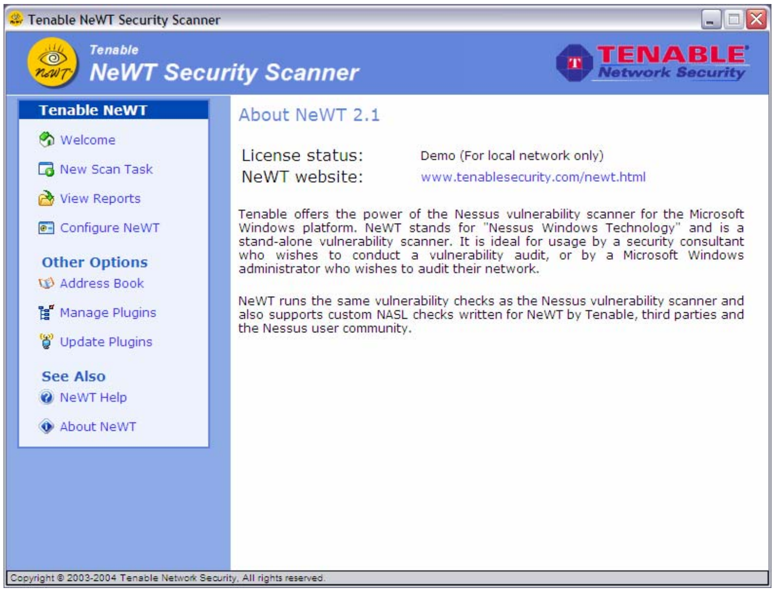
Name	Size	Type	Date Modified
msvcp71d.dll	748 KB	Application Extension	3/18/2003 10:04 PM
msvcr70.dll	336 KB	Application Extension	1/5/2002 3:37 AM
msvcr71.dll	340 KB	Application Extension	2/21/2003 4:42 AM
msvcr71d.dll	532 KB	Application Extension	3/18/2003 10:03 PM
nasl	200 KB	Application	11/13/2003 10:22 AM
newt	2 KB	Registration Entries	11/25/2003 10:12 AM
NeWT	34 KB	Application	11/7/2003 3:14 PM
NeWT	15 KB	Icon	10/23/2003 9:54 AM
NeWT.dll	188 KB	Application Extension	11/21/2003 10:04 AM
NeWTCli.dll	80 KB	Application Extension	11/22/2003 8:24 PM
newtd	2 KB	CONF File	11/24/2003 4:21 PM
newtd	37 KB	Application	11/24/2003 6:12 PM
newtd	115 KB	Palm Database File	11/24/2003 6:13 PM

The demo key provided by Tenable will be named of the format "tenable-##-##.key" such as *tenable-08-22.key* or *tenable-55-12.key*.

This key should be copied to the NeWT installation directory which is normally in:

C:\Program Files\Tenable\NeWT

Move the key provided by Tenable into this directory, and then rename the key to *newt.key*. Once a new key is installed, NeWT may be restarted. To verify that the new key is working properly, check the 'About NeWT' link on the start page. This page should indicate the current license level as shown below:



About NeWT 2.1

License status: Demo (For local network only)
NeWT website: www.tenablesecurity.com/newt.html

Tenable offers the power of the Nessus vulnerability scanner for the Microsoft Windows platform. NeWT stands for "Nessus Windows Technology" and is a stand-alone vulnerability scanner. It is ideal for usage by a security consultant who wishes to conduct a vulnerability audit, or by a Microsoft Windows administrator who wishes to audit their network.

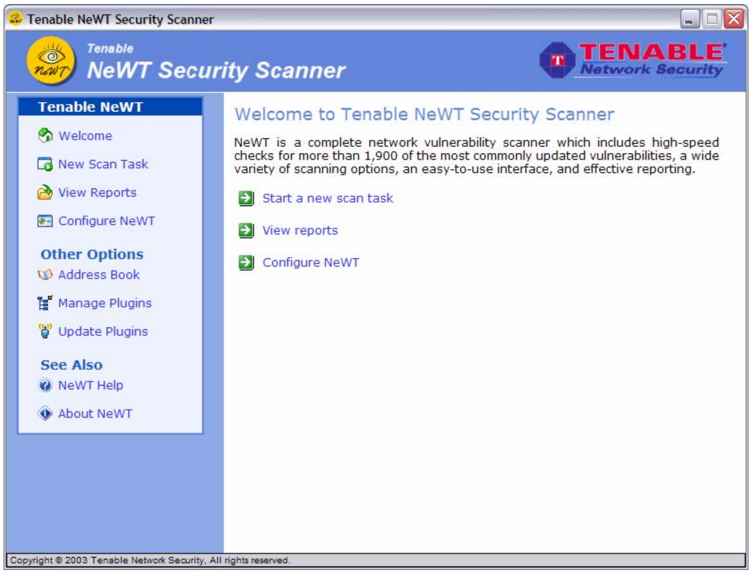
NeWT runs the same vulnerability checks as the Nessus vulnerability scanner and also supports custom NASL checks written for NeWT by Tenable, third parties and the Nessus user community.

Copyright © 2003-2004 Tenable Network Security. All rights reserved.

Quick Start Strategies

Starting

Start NeWT from the "Desktop" or "Start" menu.   The following welcome screen should appear:



Welcome to Tenable NeWT Security Scanner

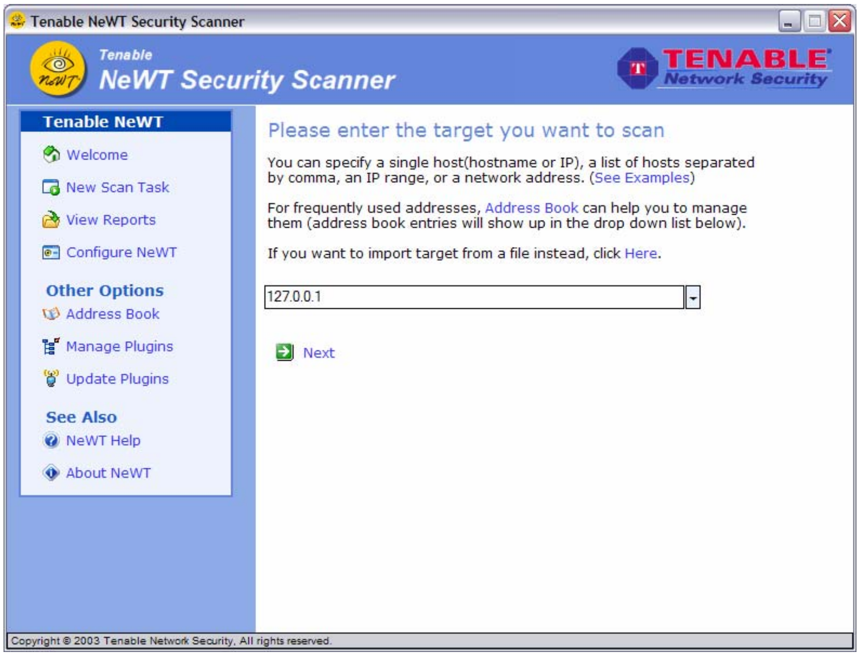
NeWT is a complete network vulnerability scanner which includes high-speed checks for more than 1,900 of the most commonly updated vulnerabilities, a wide variety of scanning options, an easy-to-use interface, and effective reporting.

Copyright © 2003 Tenable Network Security. All rights reserved.

Launching a Vulnerability Scan

To launch a scan simply select the first option, "Start a New Scan" on the NeWT welcome page. The next screen will prompt you for an IP address or range of IP addresses. The IP address can be entered in CIDR format or with the network mask following the address. A host name is also a valid entry as long as it is resolvable on the server or the fully qualified domain name is used such as newt.tenable.com.

To scan the machine running NeWT, enter the internal IP address 127.0.0.1.



Please enter the target you want to scan

You can specify a single host(hostname or IP), a list of hosts separated by comma, an IP range, or a network address. (See Examples)

For frequently used addresses, Address Book can help you to manage them (address book entries will show up in the drop down list below).

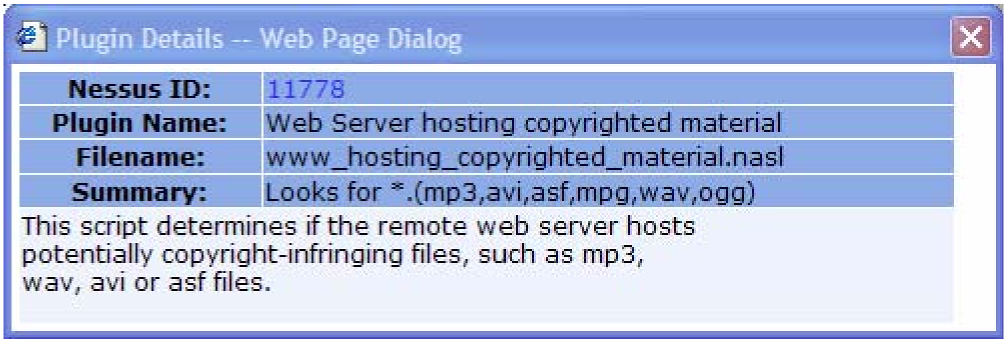
If you want to import target from a file instead, click Here.

127.0.0.1

NeWT can also make use of an 'Address Book' which contains multiple network target addresses. By clicking on the 'Address Book' link, the user will be presented with a list of current network targets and can add, edit and delete them. These targets can also be used to select the desired network(s) for scanning by NeWT.

If you've clicked on the 'Address Book' section, let's continue by clicking on the 'New Scan Task' link and entering in the localhost address 127.0.0.1 as shown above. Once this is done, click on the 'Next' link.

The next screen will prompt the reader to enter the plugin options. NeWT organizes its vulnerability checks by 'plugin' and 'plugin family'. A particular vulnerability may be checked by one or more plugins. All plugins have a unique "Nessus ID" and some short description information. Here is an example, plugin shown below:



Nessus ID:	11778
Plugin Name:	Web Server hosting copyrighted material
Filename:	www_hosting_copyrighted_material.nasl
Summary:	Looks for *.(mp3,avi,asf,mpg,wav,ogg)

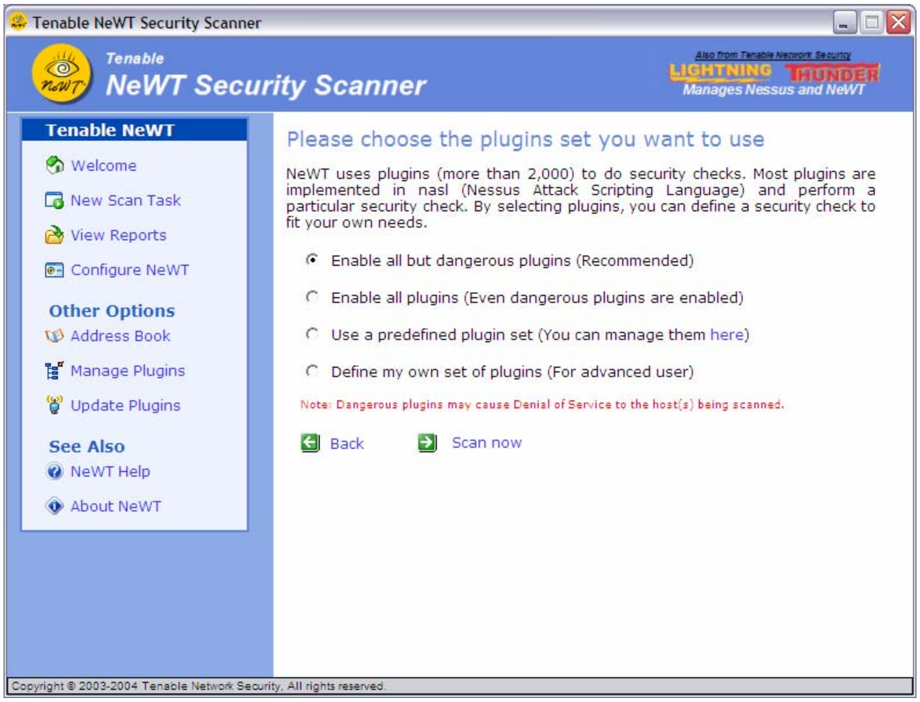
This script determines if the remote web server hosts potentially copyright-infringing files, such as mp3, wav, avi or asf files.

All plugins check for the presence of information. Some checks are pure audits, such as finding an open port, and other checks are for exploitable holes. NeWT labels these pieces of security data as informational, warnings and holes.

Tenable also maintains an online archive of plugin descriptions, user feedback and additional vulnerability mitigation information. To view this, simply click on the Nessus ID value, and this will bring the reader to the portion of the Nessus web site, which tracks user feedback.

There are more than 4000 available plugins. Each plugins checks for one or more unique vulnerabilities. To help organize these security checks, Tenable places each of these plugins into "Families". One of these families is the "Denial of Service attacks" family.

Choosing the first option, "Enable all but dangerous plugins", will allow all the security checks to be performed, except the Denial of Service attacks. The second option includes the Denial of Service attacks and could cause an interruption of service to the hosts being tested.



Please choose the plugins set you want to use

NeWT uses plugins (more than 2,000) to do security checks. Most plugins are implemented in nasl (Nessus Attack Scripting Language) and perform a particular security check. By selecting plugins, you can define a security check to fit your own needs.

● Enable all but dangerous plugins (Recommended)

○ Enable all plugins (Even dangerous plugins are enabled)

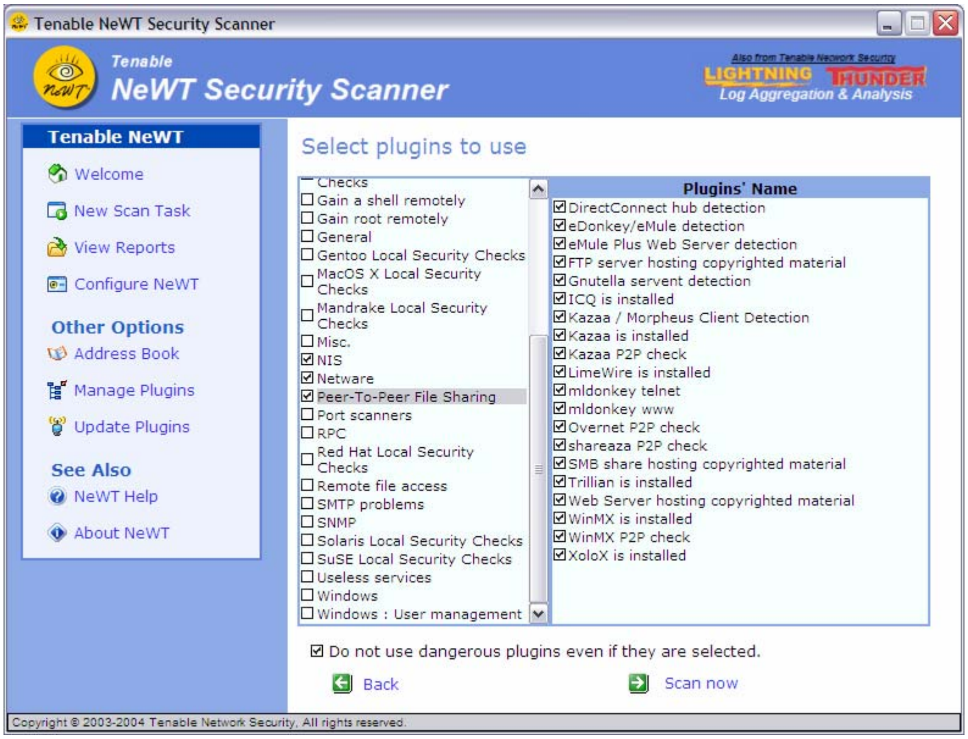
○ Use a predefined plugin set (You can manage them here)

○ Define my own set of plugins (For advanced user)

Note: Dangerous plugins may cause Denial of Service to the host(s) being scanned.

The third option allows the advanced user to individually select security checks by "family", a group of related security checks, or specific individual checks. One or more point tests can also be selected individually by first clicking on the "family" name and then selecting specific checks.

When selecting the third option, NeWT will display a split menu list of all available families and the individual plugins that comprise that family. If a family is turned on or off completely, all of the plugins within that family are enabled or disabled. If individual plugins are enabled or disabled, the family plugin checkbox will become grayed out.



Select plugins to use

- Checks
- □ Gain a shell remotely
- □ Gain root remotely
- □ General
- □ Gentoo Local Security Checks
- □ MacOS X Local Security Checks
- □ Mandrake Local Security Checks
- □ Misc.
- ☑ NIS
- ☑ Netware
- ☑ Peer-To-Peer File Sharing
- □ Port scanners
- □ RPC
- □ Red Hat Local Security Checks
- □ Remote file access
- □ SMTP problems
- □ SNMP
- □ Solaris Local Security Checks
- □ SuSE Local Security Checks
- □ Useless services
- □ Windows
- □ Windows : User management

Plugins' Name

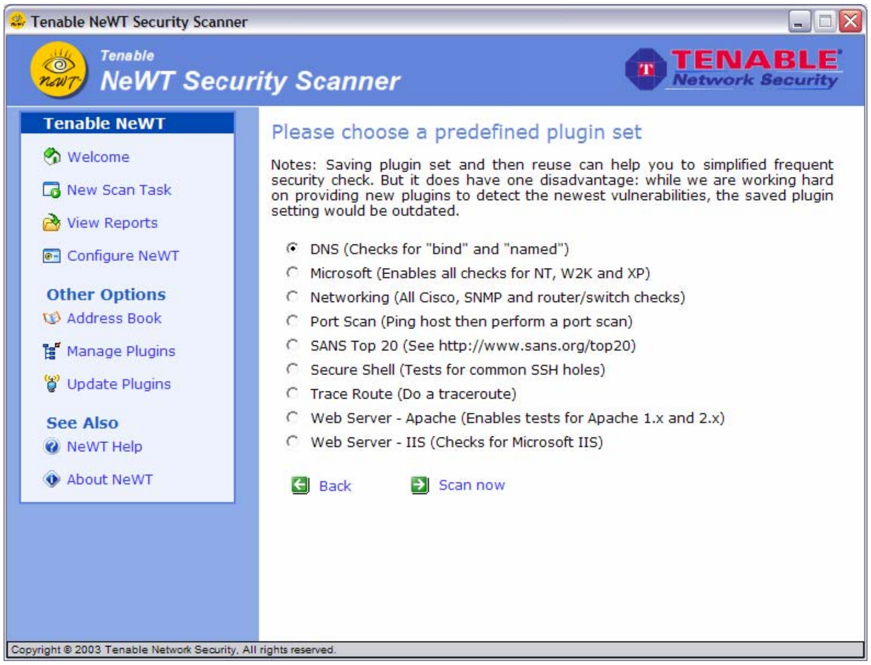
- ☑ DirectConnect hub detection
- ☑ eDonkey/eMule detection
- ☑ eMule Plus Web Server detection
- ☑ FTP server hosting copyrighted material
- ☑ Gnutella servent detection
- ☑ ICQ is installed
- ☑ Kazaa / Morpheus Client Detection
- ☑ Kazaa is installed
- ☑ Kazaa P2P check
- ☑ LimeWire is installed
- ☑ mldonkey telnet
- ☑ mldonkey www
- ☑ Overnet P2P check
- ☑ shareaza P2P check
- ☑ SMB share hosting copyrighted material
- ☑ Trillian is installed
- ☑ Web Server hosting copyrighted material
- ☑ WinMX is installed
- ☑ WinMX P2P check
- ☑ XoloX is installed

☑ Do not use dangerous plugins even if they are selected.

For example, it is possible to determine whether Kazaa is running on any systems in the network by selecting the" Peer-To-Peer File Sharing" family and select only the Kazaa options.

The “Denial of Service” family should not be unleashed on any enterprise network. It has the potential to crash, reboot or freeze a wide variety of networking, server, application and desktop installations.

The fourth option, “Use a predefined plugin set” will allow the user to select a policy of certain checks for scanning. NeWT ships with several different policy checks which are shown below:



Please choose a predefined plugin set

Notes: Saving plugin set and then reuse can help you to simplified frequent security check. But it does have one disadvantage: while we are working hard on providing new plugins to detect the newest vulnerabilities, the saved plugin setting would be outdated.

● DNS (Checks for "bind" and "named")
○ Microsoft (Enables all checks for NT, W2K and XP)
○ Networking (All Cisco, SNMP and router/switch checks)
○ Port Scan (Ping host then perform a port scan)
○ SANS Top 20 (See http://www.sans.org/top20)
○ Secure Shell (Tests for common SSH holes)
○ Trace Route (Do a traceroute)
○ Web Server - Apache (Enables tests for Apache 1.x and 2.x)
○ Web Server - IIS (Checks for Microsoft IIS)

The ‘Manage Plugins’ link on the left menu can be used to edit, add and delete new predefined plugin sets.

Launching the Scan

To launch the scan, click on the ‘Scan now’ link. There will be a short pause and then the target host(s) will begin being probed.

Watching the Scan’s Progress

When a scan is launched, NeWT will display the total progress and a summary of the rolling results. While the scan is progressing, the NeWT application can be minimized. When the scan is finished, NeWT will launch a new instance of the Internet Explorer to view the scan results.

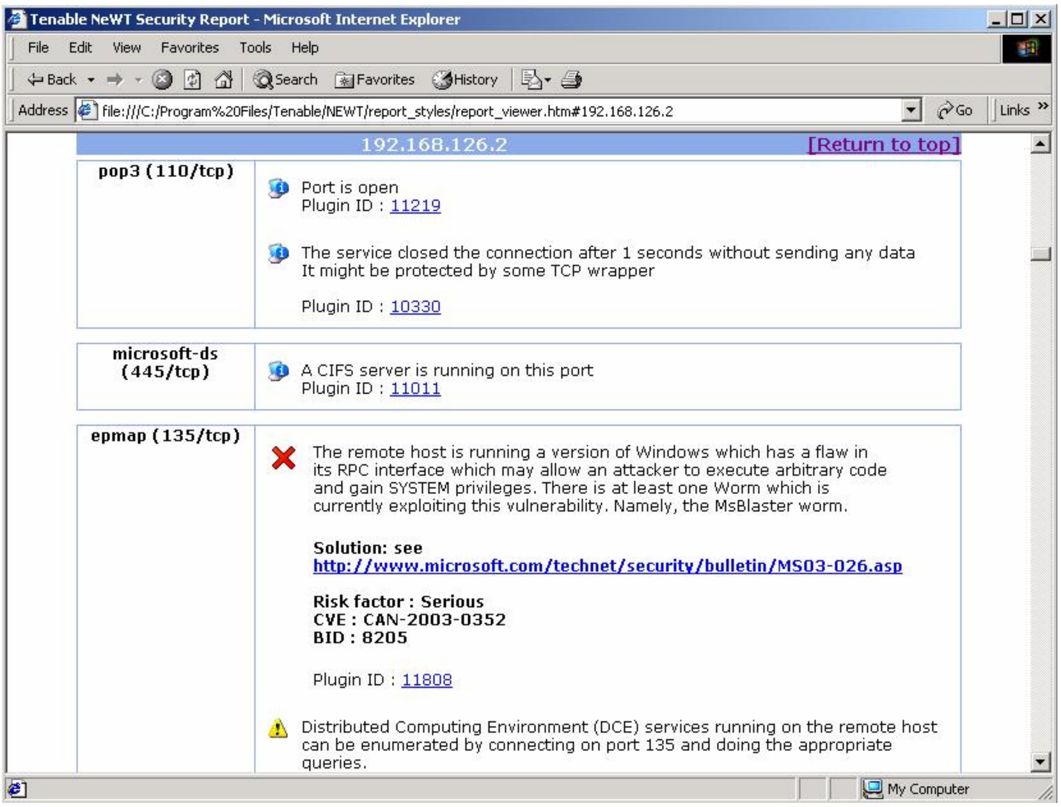
While a scan is in progress, the current list of IP addresses being scanned will be indicated. A progress bar which tracks the entire scanning process is also provided and will automatically refresh to indicate how close a scan is to completion.

Stopping a Scan

While a scan is in progress, it can be paused or stopped. When a scan is stopped, the current results are saved by NeWT and are immediately viewable. When a scan is paused, it can be resumed when desired.

Viewing the Results

The NeWT security reports will automatically pop up as a new instance of Microsoft Explorer. All reports are archived and available for viewing and printing. Below is an example scan report:


Tenable NeWT Security Report - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
History
Address
file:///C:/Program%20Files/Tenable/NEWT/report_styles/report_viewer.htm#192.168.126.2
Go
Links
My Computer

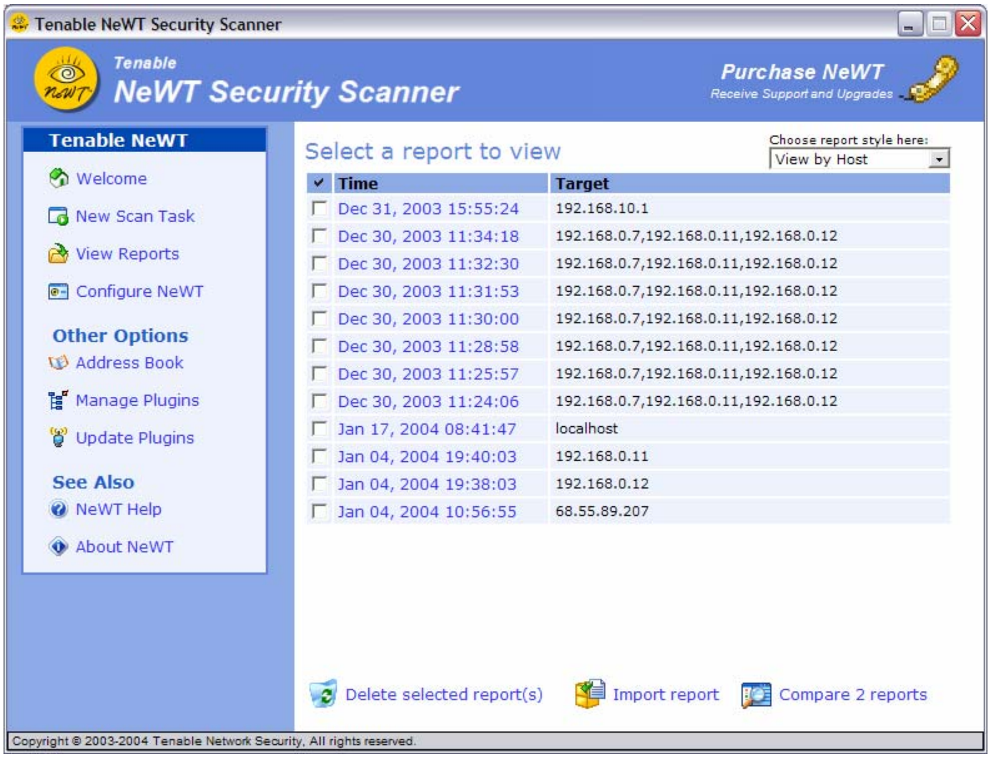
192.168.126.2 [Return to top]

pop3 (110/tcp)	Port is open Plugin ID : 11219 The service closed the connection after 1 seconds without sending any data It might be protected by some TCP wrapper Plugin ID : 10330
microsoft-ds (445/tcp)	A CIFS server is running on this port Plugin ID : 11011
epmap (135/tcp)	The remote host is running a version of Windows which has a flaw in its RPC interface which may allow an attacker to execute arbitrary code and gain SYSTEM privileges. There is at least one Worm which is currently exploiting this vulnerability. Namely, the MsBlaster worm. **Solution: see http://www.microsoft.com/technet/security/bulletin/MS03-026.asp** **Risk factor : Serious** **CVE : CAN-2003-0352** **BID : 8205** Plugin ID : 11808 Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

To access the archived reports, select the “View Saved Reports” option from the welcome menu. Reports can be viewed in multiple formats.

Report Templates

NeWT saves all of its vulnerability data in an XML format. When selecting the ‘View Reports’ option, a list of all available reports will be provided. These reports can be viewed several different ways. Their results can be viewed “by Host”, “by Port” and “by Vulnerability”. This allows a user to easily see the results of their scan. In the next section, we will discuss adding your own XSLT report templates.



Select a report to view

Choose report style here: View by Host

☑	Time	Target
☐	Dec 31, 2003 15:55:24	192.168.10.1
☐	Dec 30, 2003 11:34:18	192.168.0.7,192.168.0.11,192.168.0.12
☐	Dec 30, 2003 11:32:30	192.168.0.7,192.168.0.11,192.168.0.12
☐	Dec 30, 2003 11:31:53	192.168.0.7,192.168.0.11,192.168.0.12
☐	Dec 30, 2003 11:30:00	192.168.0.7,192.168.0.11,192.168.0.12
☐	Dec 30, 2003 11:28:58	192.168.0.7,192.168.0.11,192.168.0.12
☐	Dec 30, 2003 11:25:57	192.168.0.7,192.168.0.11,192.168.0.12
☐	Dec 30, 2003 11:24:06	192.168.0.7,192.168.0.11,192.168.0.12
☐	Jan 17, 2004 08:41:47	localhost
☐	Jan 04, 2004 19:40:03	192.168.0.11
☐	Jan 04, 2004 19:38:03	192.168.0.12
☐	Jan 04, 2004 10:56:55	68.55.89.207

Creating Report Differentials

NeWT can also create a differential report based on any two existing reports. This is extremely useful when determining what has changed on a network. It's extremely powerful to see not only which vulnerabilities have been fixed, but also which vulnerabilities are new.

When creating this new report, three options exist to tailor the output.

The first option allows either a "by unique Nessus ID" or "full text" diff. If the differential test occurs by Nessus ID, then the report will only show when a specific IP address has either a missing ID or a new ID. If this 'by ID' check is not used, then a comparison of the full text of the plugin will be accomplished. This may be useful to find out if versions of specific services have changed. However, it may also provide misleading 'new' information because certain fields of banners, such as time stamps, change all of the time.

The second option for differential report is to ignore the "host is dead" messages. This can dramatically clean up the report when large numbers of hosts have changed. Without this option, it would also be difficult to compare two scan results in which one report did log the fact that a host was dead and the other did not.

And finally, the third option for differential reporting is to specify the analysis of just the hosts which are common to both reports.

New XML Style Sheets

NeWT saves all vulnerability data in a flat XML data file. It uses "style sheets" to dynamically render interesting and useful reports in the Internet Explorer web browser. Tenable includes several style sheets with NeWT and is developing more reporting functionality, but it is useful to know how to add new style sheets for custom reporting.

It is easy to create new style sheets to change the look and format of the reports. Once you have created a new report format, you can add it as an option in the report drop down menu by taking the following steps:

1) Copy the new style sheet into the report styles directory , by default –
   `C:\Program Files\Tenable\NEWT\report_styles`

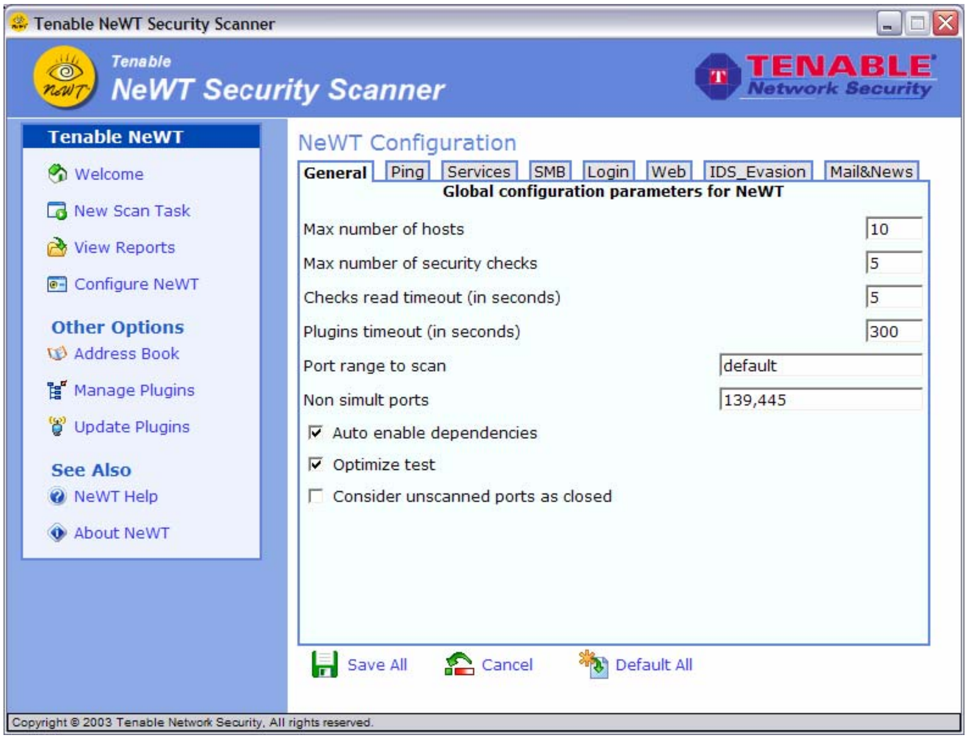
2) Add the following lines to the end of the *report_styles.xml* file. This file is in the report styles directory listed above -

```
<style>
     <name>Your Style</name>
     <xsl_file>yourstyle.xsl</xsl_file>
</style>
```

Replace "Your Style" with the title of the new report. Replace "yourstyle.xsl" with the new file name. You will see a template to add additional reports commented out at the end of the *report_styles.xml* file. The new report format will be available in the drop-down menu in the "View Reports" tool.

Configuring NeWT

NeWT can be configured by selecting the "Configure NeWT" option at the welcome screen. There are several hundred configuration options. Specific scan options can be saved as the 'default' scan or the original defaults can be loaded. The configuration screen will appear as below:



NeWT Configuration

Global configuration parameters for NeWT

Max number of hosts	10
Max number of security checks	5
Checks read timeout (in seconds)	5
Plugins timeout (in seconds)	300
Port range to scan	default
Non simult ports	139,445

☑ Auto enable dependencies

☑ Optimize test

☐ Consider unscanned ports as closed

There are eight configuration tabs that allow very granular configuration of NeWT: General, Services, Login, Web, SMB, IDS Evasion, Ping, and Miscellaneous.

General

The configuration options in this screen allow you to set global parameters for the plugins being run by NeWT. The first option sets the maximum number of hosts that will be scanned simultaneously. The next option sets the maximum number of security plugins that will be run on each host. Some hosts can become disabled, either temporarily or permanently, if too many plugins are launched at the same time.

Thus the total number of running processes will be equivalent to the Max number of hosts times the Max number of security checks. In the example above there will be 160 processes running simultaneously. It is important to balance the two options so the network is not overwhelmed.

Ping

The ping protocol is used by NeWT to check if hosts and specific ports are alive. There are setting for ICMP ping and TCP ping. If both ICMP ping and TCP ping are selected, NeWT will attempt to connect to hosts using both protocols.

Services

This tab defines parameters for the services related plugins. These plugins determine what services are running behind specified ports. A few of these setting are options that will override the global parameters that were set for NeWT in the general screen for only the Services plugin**s**. This provides a way to minimize the impact of security scans on printers or other devices that cannot support multiple open ports simultaneously.

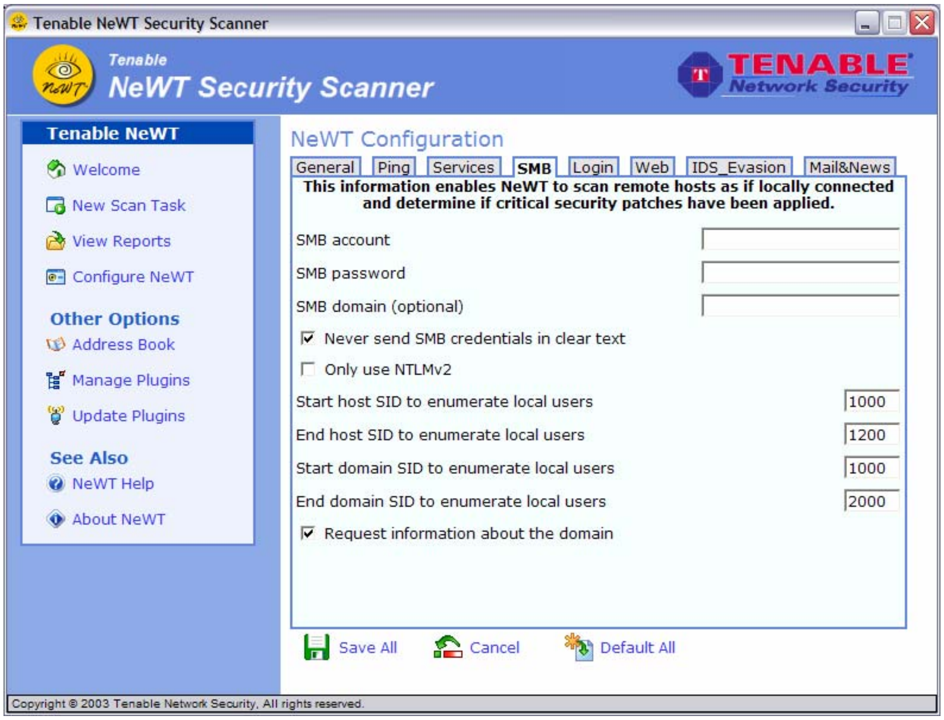
Login

The options in this tab allow you to provide site specific information such as account names and passwords to NeWT. This information will be used by the plugins to provide more thorough testing of the enterprise. All requested login information is optional, meaning that it is not needed for proper NeWT operation.

Tenable highly recommends that the SNMP community string be configured if it is known. If NeWT can guess it during a scan, it will be applied to subsequent checks, but if it can be pre-configured, a very detailed audit can be performed. For example, there are approximately twenty Cisco router checks which determine the vulnerabilities present by simply considering the version string returned via SNMP. Without the SNMP community string, these audits could not occur.

SMB

Server Message Block or SMB is a file sharing protocol that allows computers to share information transparently across the network. The SMB tab has options to provide NeWT with information such as SMB account name, password and domain name. Providing this information to NeWT will allow it find local information from a remote Windows host such as whether important security patches have been applied. Only expert security personnel should modify other SMB parameters from default settings.



This information enables NeWT to scan remote hosts as if locally connected and determine if critical security patches have been applied.

SMB account	
SMB password	
SMB domain (optional)	
☑ Never send SMB credentials in clear text	
□ Only use NTLMv2	
Start host SID to enumerate local users	1000
End host SID to enumerate local users	1200
Start domain SID to enumerate local users	1000
End domain SID to enumerate local users	2000
☑ Request information about the domain	

If a maintenance SMB account is created with limited administrator privileges, NeWT can easily and securely scan multiple domains. Detailed configuration instructions are available at:

http://www.nessus.org/doc/nessus_domain_whitepaper.pdf

Tenable recommends that network administrators consider creating specific domain accounts to facilitate testing. NeWT includes a variety of security checks for Windows NT, 2000 and XP which are more accurate if a domain account is provided. NeWT does attempt to try several checks in most cases if no account is provided.

Web

The options in this tab allow you to provide site-specific information about the web services in the network being scanned. Filling out these parameters will enable NeWT to perform tests against Web services in the network. All requested information is optional, meaning it is not needed for proper NeWT operation.

One of the options used in this page is a username and password. When auditing a web site protected by a username or password, adding that information to NeWT allows for vulnerability testing of the privileged access. For example, a NeWT server scanning a vulnerable, but password protected Apache web server application, would not report on any vulnerability if it cannot log onto the system. By configuring NeWT with the username and password to the web server, all of the Apache server's vulnerabilities could be exploited. These vulnerabilities would only be exploitable by valid users, but could still pose a large threat.

IDS evasion

The IDS (intrusion detection systems) evasion tab contains a variety of tests that are available to check the effectiveness of network IDS system. Many network IDS solutions use different checks to process network packets and sessions. Variations in these checks can lead to situations which allow an attacker to launch an attack without being detected by a network IDS.

Running these tests should set off alarms in the IDS system. If an event has been logged by the IDS system, you will know that the IDS is effectively detecting hacking attempts. If there is no entry in the IDS log, then the IDS evasion attempt was successful. More specific information about IDS evasion techniques are available at:

“Using Nessus’s NIDS Evasion Techniques” by Michel Arboi and Renaud Deraison on the Nessus web site at http://www.nessus.org/doc/nids.html.

"Anti-IDS Tools and Tactics" by Steve Martin on the SANs web site at http://www.sans.org/rr/paper.php?id=339.

Mail and News

The options in this tab determine if mail and news servers can be used to relay spam. NeWT will attempt to post a news message to the news server. There are options to test whether it is possible to post a message to upstream news servers as well.

The SMTP tests will run on all devices within the scanned domain that are running SMTP services. NeWT will attempt to send spam through each SMTP device to the address listed in the “third party domain” parameter.

If the SMTP and Mail Servers receive error messages that the news or mail messages could not be delivered, then the hosts have been protected and cannot be used to relay spam. If the messages are sent without any errors, the spam attempt was successful   All requested information in the Mail and News tab is optional, meaning it is not required for proper NeWT operation.

Enabling local security checks with NeWT

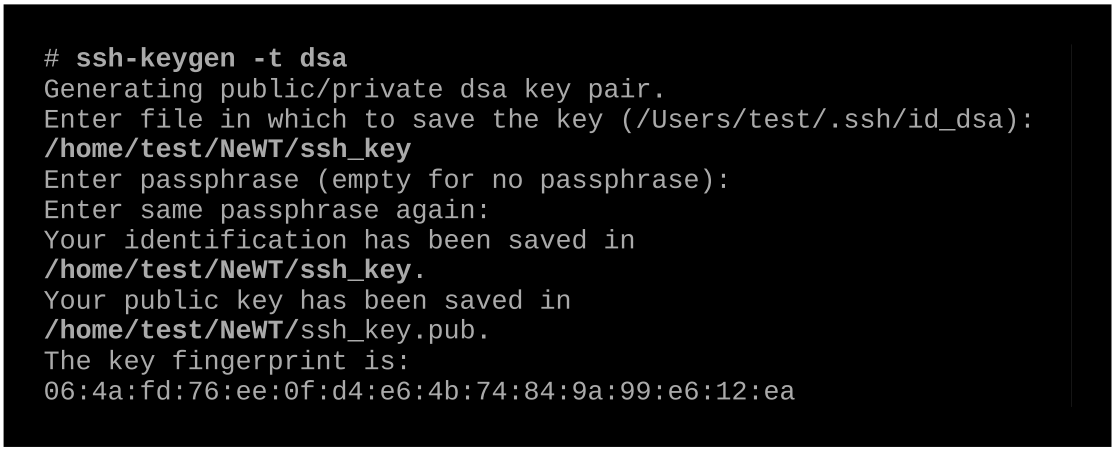
The process detailed below will allow you to perform local security checks on UNIX and Linux systems. Local security checks on Windows-based systems will be configured from the SMB tab of the NeWT Configuration screen.

To enable local security checks, the idea is to:

- Create a SSH private/public key pair for NeWT to use
- Create a user account on every system for which you want to perform a local scan
- Copy the SSH public key that NeWT will use in the directory of the new user
- Tell NeWT to use this SSH private and public keys and perform the scan

<u>Generating a SSH public key & private key</u>

The first step is to generate a private/public key pair for the NeWT system to use. This key pair can be generated from any of your Unix/Linux systems, using any user account. To generate the key pair, use *ssh-keygen* and save the key in a safe place. (the following example the keys are generated on a Red Hat ES 3 install)



```
# ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/Users/test/.ssh/id_dsa):
/home/test/NeWT/ssh_key
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in
/home/test/NeWT/ssh_key.
Your public key has been saved in
/home/test/NeWT/ssh_key.pub.
The key fingerprint is:
06:4a:fd:76:ee:0f:d4:e6:4b:74:84:9a:99:e6:12:ea
```

As seen in the example above, two files created:

`/home/test/NeWT/ssh_key` is the **private** SSH key. Do not transfer this file to any system other than the one running your NeWT client.

`/home/test/NeWT/``ssh_key.pub` is the **public** SSH key. This file will be distributed to every system you want to perform local security check scans on using NeWT.

When *ssh-keygen* asks you for a passphrase, you may want to enter return twice (i.e.: do not set any passphrase). For this example, we will not use a passphrase.

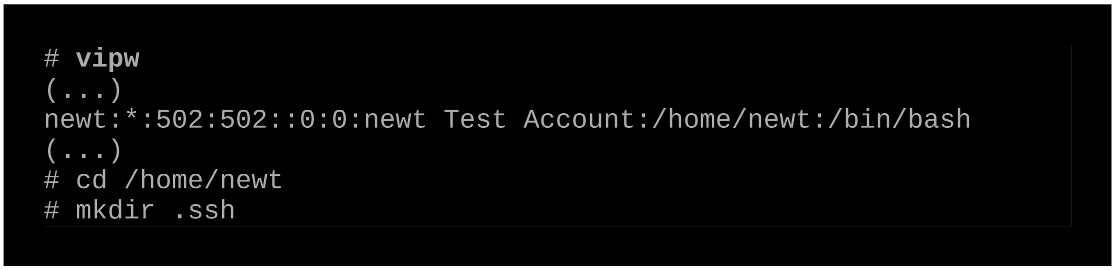
In order to more easily manage the public and private key files, you may wish to copy both of them to the main NeWT application directory on the system running NeWT (\Program Files\Tenable\NeWT by default), and then copy the public key to the target systems as needed.

Creating a user account and setting up the SSH key

On every target system to be scanned using local security checks, create a new user account dedicated to NeWT. This user account must have exactly the same name on all systems. For the purposes of this document, we will call this user newt, but you can use any name.

Once the account is created for the user (using adduser or any utility that the system provides you with), make sure that the account has no valid password set (you will have to edit /etc/passwd with ‘vi’ or 'vipw' and change the password entry to an asterix (*).

You must also create the directory under this new account’s home directory to hold the public key. For this exercise, the directory will be /home/newt/.ssh. Example is provided below:



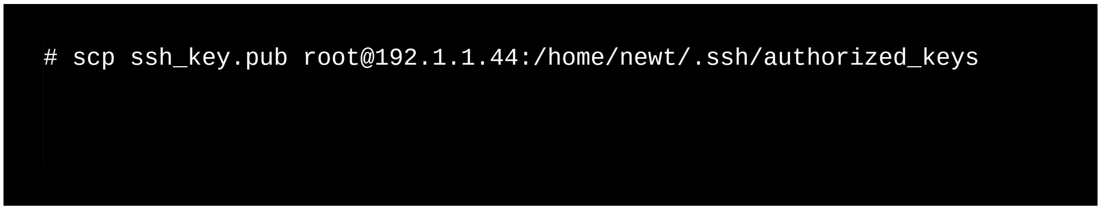
```
# vipw
(...)
newt:*:502:502::0:0:newt Test Account:/home/newt:/bin/bash
(...)
# cd /home/newt
# mkdir .ssh
```

Now that the user account is created, you must transfer the key to the system and place it in the appropriate directory. Finally, you must set the correct permissions:

Example:

From the system containing the keys, secure copy the public key to system that will be scanned for host checks:

# scp ssh_key.pubroot@192.1.1.44:/home/newt/.ssh/authorized_keys (192.1.1.44 is the example remote system that will be tested with the host based checks)

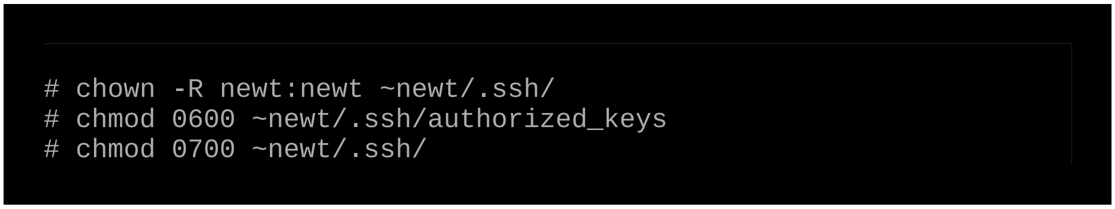


```
# scp ssh_key.pub root@192.1.1.44:/home/newt/.ssh/authorized_keys
```

You can also copy the file from the system on which NeWT is installed. Note that the file on the target system must be named ‘authorized_keys’

Return to the system housing the public key.

Set the permissions on both the /home/newt/.ssh directory, as well as the authorized_keys file.

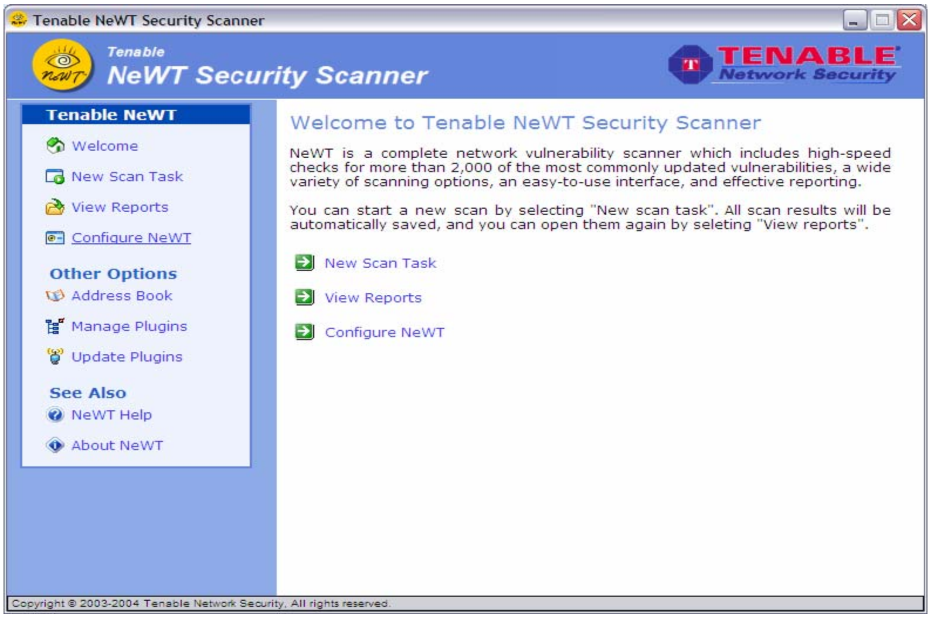


```
# chown -R newt:newt ~newt/.ssh/
# chmod 0600 ~newt/.ssh/authorized_keys
# chmod 0700 ~newt/.ssh/
```

Repeat this process on all systems that will be tested for SSH checks (starting at “Creating a user account and setting up the SSH key” above).

Configuring NeWT for SSH Checks

If you have not already done so, secure copy the private and public key files to the system that NeWT installed.

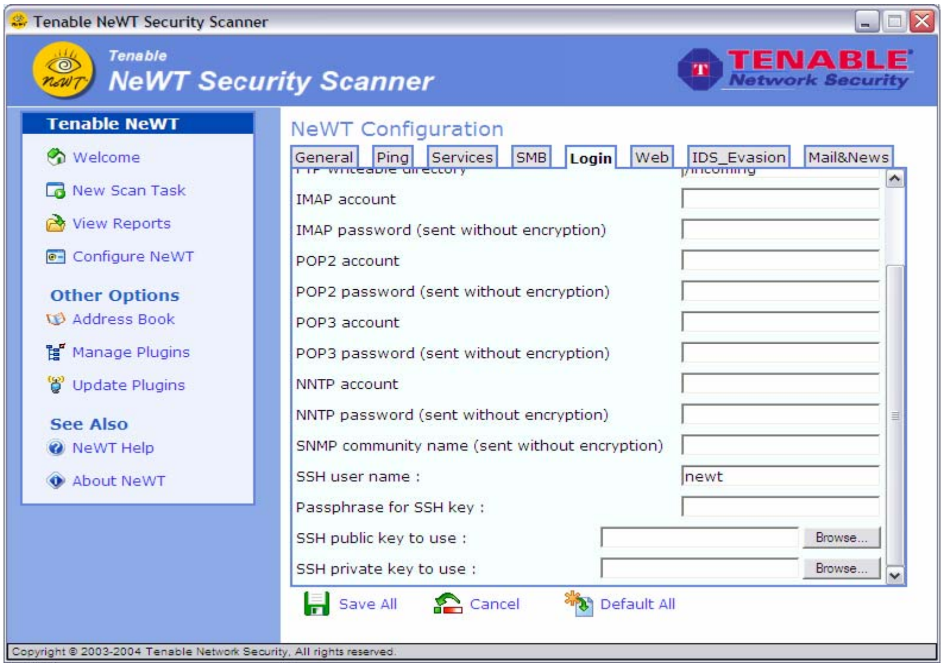


NeWT is a complete network vulnerability scanner which includes high-speed checks for more than 2,000 of the most commonly updated vulnerabilities, a wide variety of scanning options, an easy-to-use interface, and effective reporting.

You can start a new scan by selecting "New scan task". All scan results will be automatically saved, and you can open them again by seleting "View reports".

New Scan Task
View Reports
Configure NeWT
Copyright © 2003-2004 Tenable Network Security, All rights reserved.

Open NeWT as seen above and select Configure NeWT.

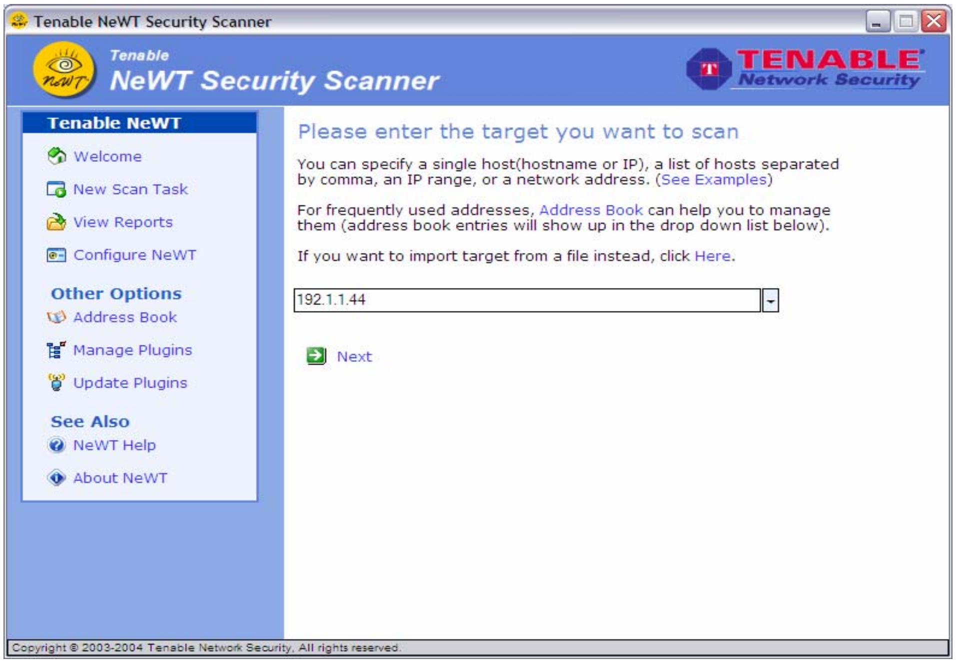


FTP writeable directory /incoming
IMAP account
IMAP password (sent without encryption)
POP2 account
POP2 password (sent without encryption)
POP3 account
POP3 password (sent without encryption)
NNTP account
NNTP password (sent without encryption)
SNMP community name (sent without encryption)
SSH user name : newt
Passphrase for SSH key :
SSH public key to use :
SSH private key to use :

From the NeWT Configuration screen, select the Login tab.

- For the item “Add the SSH user name:” enter the name of the account that is dedicated to NeWT on each of the scan target systems.
- For the item “Add the SSH public key to user:” click on the Browse… button and locate the public key file on the local system.
- For the item “Add the SSH private key to user:” click on the Browse… button and locate the private key file on the local system.

At this point, click on Save All at the bottom of the window and configuration should be complete.



Please enter the target you want to scan

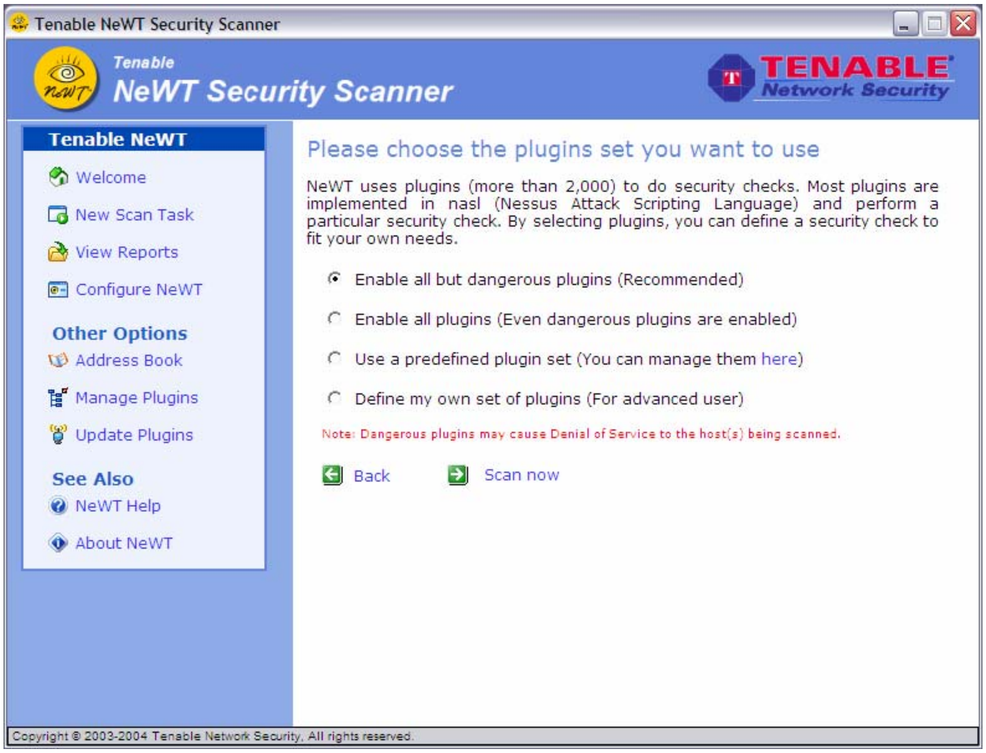
You can specify a single host(hostname or IP), a list of hosts separated by comma, an IP range, or a network address. (See Examples)

For frequently used addresses, Address Book can help you to manage them (address book entries will show up in the drop down list below).

If you want to import target from a file instead, click Here.

192.1.1.44

Select New Scan Task & add IP of system to scan. When IP is entered, select, Next.



Please choose the plugins set you want to use

NeWT uses plugins (more than 2,000) to do security checks. Most plugins are implemented in nasl (Nessus Attack Scripting Language) and perform a particular security check. By selecting plugins, you can define a security check to fit your own needs.

● Enable all but dangerous plugins (Recommended)

○ Enable all plugins (Even dangerous plugins are enabled)

○ Use a predefined plugin set (You can manage them here)

○ Define my own set of plugins (For advanced user)

Note: Dangerous plugins may cause Denial of Service to the host(s) being scanned.

Select “Enable all but dangerous plugins (Recommended). & select Scan now.

SSH checks are also included in Enable all but dangerous plugins (Recommended), Enable all plugins (Even dangerous plugins are enabled.) & Define my own set of plugins (for advanced user)

Update Plugins

NeWT has thousands of plugins (or scripts) that test for network and host vulnerabilities. New vulnerabilities are regularly being discovered and new plugins are developed to detect these vulnerabilities. NeWT has an update wizard that will automatically retrieve the latest computer vulnerability plugins with one simple step.

To view the most recent plugin checks produced by Tenable and the Nessus community, please visit the web at:

http://www.nessus.org/scripts.php

As a general rule, you should update your vulnerability plugins each time you perform a scan.

Upgrading NeWT with New Releases

As newer versions of NeWT are released by Tenable, upgrading is accomplished with a full re-installation. To upgrade, the older version of NeWT must be completely un-installed. All previous vulnerability scan reports will be saved and will not be deleted. After the new version of NeWT is installed, they will still be available for viewing.

Importing Scan Data

NeWT can be used to import vulnerability data from existing Nessus, NeWT or Lightning Console scans. To import a scan, while viewing reports, choose the ‘Import Report’ function as shown below:

This will present the user with an opportunity to import a text file formatted for either NeWT’s *.xml* or Nessus’s *.nbe* or *.nsr* formats. The form also asks the user to provide a name to describe the imported data. Once the data has been imported, it will be available to perform differential scan reports, as well as to be viewed as if it were conducted by the NeWT scanner.

Using Custom Vulnerability Checks

NeWT can make use of any custom NASL vulnerability scripts that have been written independently of the Nessus project. Tenable encourages NeWT users to submit their plugin checks to the project. Tenable will make every effort to either maintain the author’s original copyright, or hide the author’s identity. While writing custom plugins, Tenable also urges the users of NeWT to comply with the NASL language and can refer to the “NASL 2 Reference Manual” (http://www.nessus.org/doc/nasl2_reference.pdf) for examples of the API in action.

To install custom NASL scripts into NeWT, simply copy the desired script(s) to the *\users\admin\plugins\* directory within the NeWT program directory. Once the plugins are located there, the user can either attempt to manually update the plugins from the NeWT interface, or at the command line, run the *build.exe* program. To verify that the new plugins have been imported to NeWT, choose to launch a new scan task, select to define your own set of plugins, and then locate your new plugin(s) in the specific family they are located in.

Sharing NeWT Reports with other Users

It may be very useful to save a specific NeWT report and email it to a customer, administrator or supervisor.

Web Archives

An easy way to do this is to save a report as a Microsoft Web Archive *.mht* file. While viewing a report, which has been rendered in HTML, the Internet Explorer browser can save all of the text, layout and images in a single file known as a “web archive”. This archive can be easily emailed, shared and viewed on other Windows systems. Web archives can be opened by many web browsers and also by recent versions of Microsoft Word and PowerPoint.

Raw HTML

While viewing a report, the direct HTML and images can be saved. This format is not idea though as the data is spread between a *.html* file and a sub-directory named based on the saved file name and that contains the images and content style sheets for the report.

Printing to PDF

Although not directly supported by NeWT, if the system which has NeWT installed on it also has a PDF print server, the actual report can be ‘printed’ to a PDF file. This file can then be shared across any operating system which has a PDF viewer installed.

XML Output

Each NeWT report is available in raw XML form. This can be imported into Microsoft Office 2003 Excel and newer releases for manipulation and analysis.

Working with the Lightning Console

What is the Lightning Console?

Tenable Network Security offers an enterprise vulnerability and security management tool named the ‘Lightning Console”. This tool allows multiple NeWT, NeWT Pro or Nessus vulnerability scanners to be used in conjunction to scan small and large networks on a periodic basis.

The Console allows for multiple users and administrators with different security levels to share vulnerability information, prioritize vulnerabilities, show which network assets have critical security issues, make recommendations to system administrators for fixing these security issues and to track when the vulnerabilities are mitigated. Lightning also receives data from many leading intrusion detection systems such as Snort and ISS.

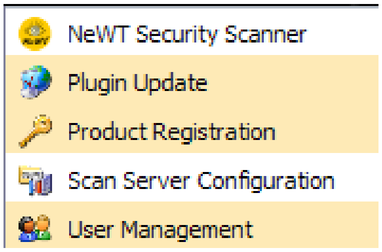
Lightning can also receive passive vulnerability information from Tenable’s NeVO vulnerability monitor such that end users can discover new hosts, applications, vulnerabilities and intrusions without the need for active scanning with Nessus or NeWT.

Configuring NeWT Pro to listen as a Network Daemon

Both NeWT and NeWT Pro can be configured to communicate with the Lightning Console. To do this, we need to complete two tasks. We need to add an account for the Lightning Console to log into NeWT with, and then we need to enable NeWT to listen to inbound network connections from the Console as well. By default, NeWT only listens to localhost connections and we need to configure it to be bound to a specific network interface.

Adding User Accounts

To manage the user accounts for NeWT, invoke the ‘User Management’ tool which is accessible from the Start button by following the Start / All Programs / Tenable Network Security / Tenable NeWT series of options as shown below:

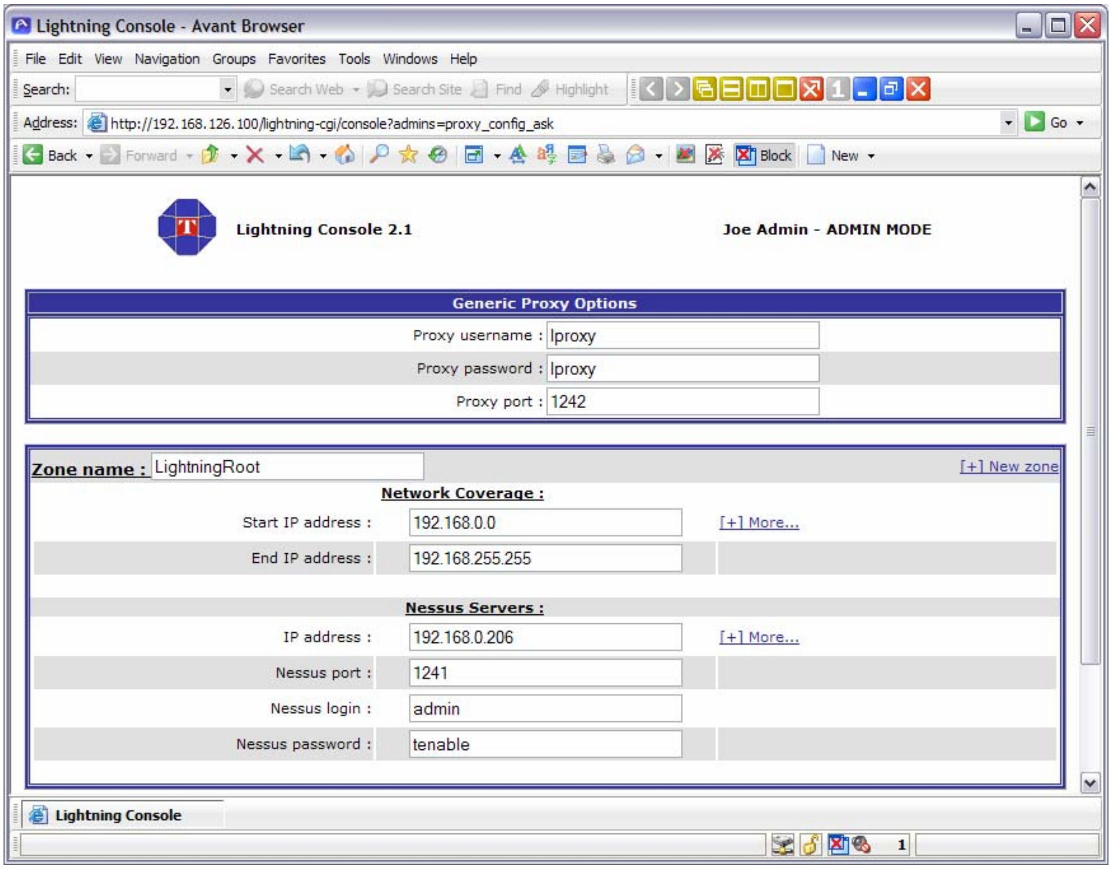


Please note that user accounts for NeWT refer to a specific username and password to be used by the Lightning Console to log in remotely to launch scans and retrieve vulnerability data.

Choose a unique username and password to be used by the Lightning Console and keep it handy when adding this NeWT to it.

Configuring the Lightning Console

At the Lightning Console, a “Nessus Server” can be added through the administration interface. Within this interface, the IP address of the NeWT scanner and the associated network range(s) are specified. An example screen shot of the Lightning interface is shown below:


Lightning Console - Avant Browser
File Edit View Navigation Groups Favorites Tools Windows Help
Search: Search Web Search Site Find Highlight
Go
Back Forward Block New
Lightning Console 2.1
Joe Admin - ADMIN MODE
[+] New zone
[+] More...
[+] More...
Lightning Console

Address: http://192.168.126.100/lightning-cgi/console?admins=proxy_config_ask

Generic Proxy Options

Proxy username :	lproxy
Proxy password :	lproxy
Proxy port :	1242

Zone name : LightningRoot

Network Coverage :

Start IP address :	192.168.0.0
End IP address :	192.168.255.255

Nessus Servers :

IP address :	192.168.0.206
Nessus port :	1241
Nessus login :	admin
Nessus password :	tenable

The Lightning Console will refer to the NeWT scanner as a ‘Nessus Server’. When working with the Lightning Console, NeWT and Nessus are compatible and should be treated as the same type of scanner.

Enabling Network Connections

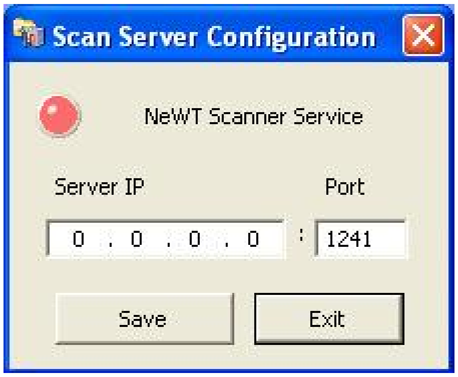
To allow a remote connection to NeWT from the Lightning Console, run the “Scan Server Configuration” tool. This tool allows the port and bound interface of the NeWT daemon to be configured. By default, the NeWT daemon listens to connections on localhost (127.0.0.1) and port 1241.

To enable connectivity from the Lightning Console, NeWT must be configured to listen for connections either on one network interface, or any interface. Type in the IP address of the NeWT network interface it should be bound to.

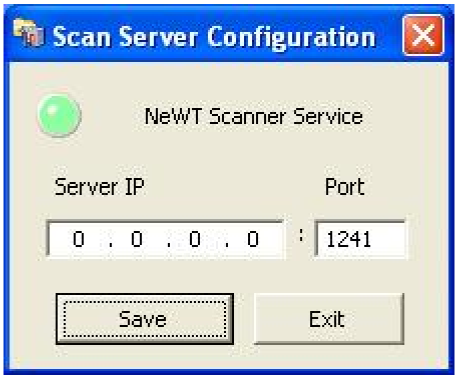
- If your server only has one IP address and network card, then type in that IP address.
- If your server has multiple IP addresses and you only want it to listen for connections on port 1241 on one of those, type in the IP address of that interface.
- If your server has multiple IP addresses and you want it to listen on all interfaces, use an IP address of 0.0.0.0.

Here are two screen shots of the "Scan Server Configuration" tool. They both have been bound to all network cards with an IP address of 0.0.0.0, and they are both listening on port 1241.

The image on the left with the red indicator shows that the "Tenable NeWT" service is not running. Clicking on that button will prompt the use with an option to start the service. If this is attempted, the indicator will turn yellow and then green if successful.



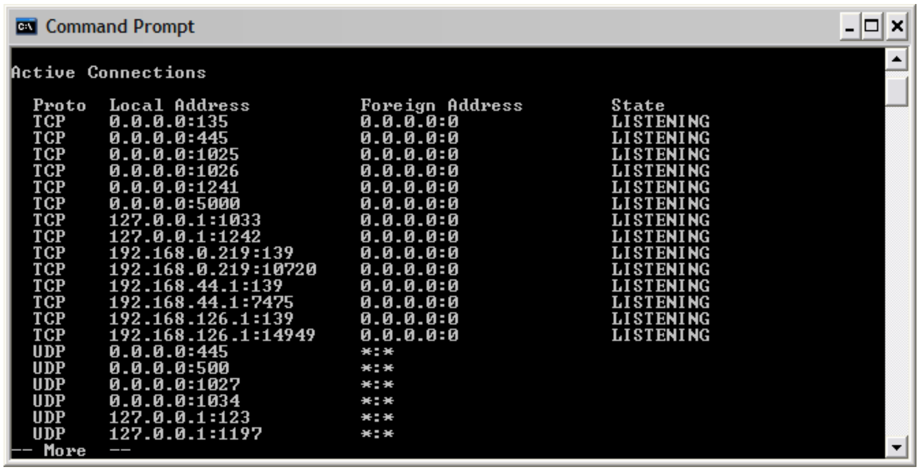
Server IP: 0 . 0 . 0 . 0
Port: 1241



Server IP: 0 . 0 . 0 . 0
Port: 1241

Any change to the information in the dialogue box of the 'Scan Server Configuration" tool will also prompt the user to see if they want to restart the "Tenable NeWT" service.

To verify that NeWT is indeed listening on port 1241, from the Windows command line use the *netstat –an* command as shown below:



```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1241           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5000           0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1033         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1242         0.0.0.0:0              LISTENING
  TCP    192.168.0.219:139      0.0.0.0:0              LISTENING
  TCP    192.168.0.219:10720    0.0.0.0:0              LISTENING
  TCP    192.168.44.1:139       0.0.0.0:0              LISTENING
  TCP    192.168.44.1:7475      0.0.0.0:0              LISTENING
  TCP    192.168.126.1:139      0.0.0.0:0              LISTENING
  TCP    192.168.126.1:14949    0.0.0.0:0              LISTENING
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:1027           *:*
  UDP    0.0.0.0:1034           *:*
  UDP    127.0.0.1:123          *:*
  UDP    127.0.0.1:1197         *:*
-- More  --
```

Notice that the fifth TCP line contains “0.0.0.0:1241” which means a server is listening on that port.

Host-Based Firewalls

If your are NeWT or NeWT Pro server is configured with a local firewall such as Zone Alarm, Sygate, BlackICE, the Windows XP firewall or any other, it is required that connections be opened from the Lightning Console’s IP address.

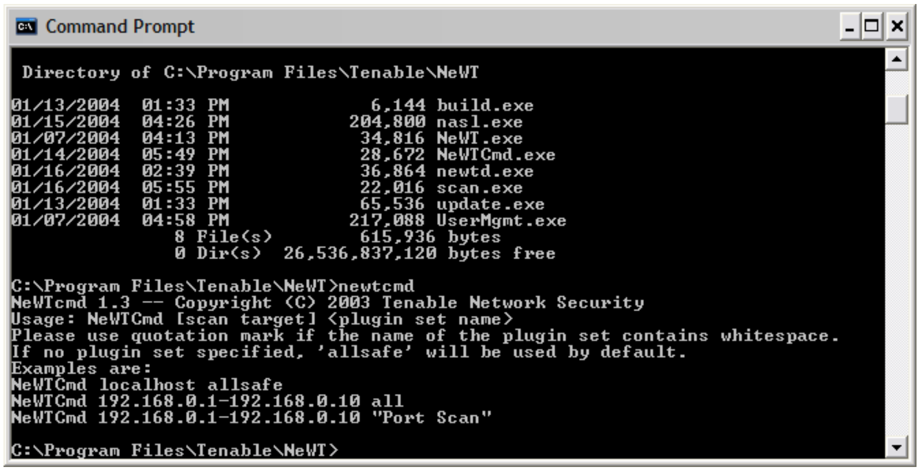
By default, port 1241 is used. On Microsoft XP service pack 2 systems, running the “Security Center” icon available in the Control Panel will present the user with the opportunity to manage the ‘Windows Firewall’ settings. To open up port 1241, choose the ‘Exceptions’ tab, and then add port 1241 to the list.

Using NeWT and NeWT Pro with Lightning

Although NeWT and NeWT Pro scanners can both be connected to the Lightning Console, NeWT licenses will still only be able to scan their local Class C subnet.

Command Line Mode

NeWT can be launched from the DOS command line mode. To do this, simply execute the *NeWTCmd.exe* file as shown below:



```
 Directory of C:\Program Files\Tenable\NeWT

01/13/2004  01:33 PM             6,144 build.exe
01/15/2004  04:26 PM           204,800 nasl.exe
01/07/2004  04:13 PM            34,816 NeWT.exe
01/14/2004  05:49 PM            28,672 NeWTCmd.exe
01/16/2004  02:39 PM            36,864 newtd.exe
01/16/2004  05:55 PM            22,016 scan.exe
01/13/2004  01:33 PM            65,536 update.exe
01/07/2004  04:58 PM           217,088 UserMgmt.exe
               8 File(s)        615,936 bytes
               0 Dir(s)  26,536,837,120 bytes free

C:\Program Files\Tenable\NeWT>newtcmd
NeWTcmd 1.3 -- Copyright (C) 2003 Tenable Network Security
Usage: NeWTCmd [scan target] <plugin set name>
Please use quotation mark if the name of the plugin set contains whitespace.
If no plugin set specified, 'allsafe' will be used by default.
Examples are:
NeWTCmd localhost allsafe
NeWTCmd 192.168.0.1-192.168.0.10 all
NeWTCmd 192.168.0.1-192.168.0.10 "Port Scan"

C:\Program Files\Tenable\NeWT>
```

This will cause a scan to be executed, but will not invoke the *newtd.exe* file. The NeWT daemon must already be running in order for the command line mode to proceed.

In addition, there is an executable named *updatecmd.exe* which can be used to script the downloading and updating of vulnerability checks. Simply running this command will download the latest vulnerability checks and configure them for use by NeWT.

For Further Information

Please feel free to contact either email below, or visit our web site at
http://www.tenablesecurity.com.

sales@tenablesecurity.com

Also From Tenable

- **NeVO Passive Scanner –** 100% passive vulnerability analysis. NeVO “sniffs” your vulnerability and network information directly from network traffic. Available for Windows XP, RedHat Linux and FreeBSD.
- **Lightning Console –** Enterprise security management. Schedule scans, manage distributed Nessus, NeWT and NeVO scanners, and manage vulnerabilities, track security remediation actions, executive reporting, and intrusion detection event correlation. Available for RedHat Linux.
- **Thunder Log Aggregator** – Allows the Lightning Console to aggregate, normalize, analyze and report about firewall, honey-pot, router, server, web access, intrusion detection, operating system and application logs. Available for RedHat Linux.