

DECLARATION OF NATHANIEL E FRANK-WHITE

1. I am a Records Request Processor at the Internet Archive. I make this declaration of my own personal knowledge.

2. The Internet Archive is a website that provides access to a digital library of Internet sites and other cultural artifacts in digital form. Like a paper library, we provide free access to researchers, historians, scholars, and the general public. The Internet Archive has partnered with and receives support from various institutions, including the Library of Congress.

3. The Internet Archive has created a service known as the Wayback Machine. The Wayback Machine makes it possible to browse more than 450 billion pages stored in the Internet Archive's web archive. Visitors to the Wayback Machine can search archives by URL (i.e., a website address). If archived records for a URL are available, the visitor will be presented with a display of available dates. The visitor may select one of those dates, and begin browsing an archived version of the Web. Links on archived files in the Wayback Machine point to other archived files (whether HTML pages or other file types), if any are found for the URL indicated by a given link. For instance, the Wayback Machine is designed such that when a visitor clicks on a hyperlink on an archived page that points to another URL, the visitor will be served the archived file found for the hyperlink's URL with the closest available date to the initial file containing the hyperlink.

4. The archived data made viewable and browseable by the Wayback Machine is obtained by use of web archiving software that automatically stores copies of files available via the Internet, each file preserved as it existed at a particular point in time.

5. The Internet Archive assigns a URL on its site to the archived files in the format http://web.archive.org/web/[Year in yyyy][Month in mm][Day in dd][Time code in hh:mm:ss]/[Archived URL] aka an "extended URL". Thus, the extended URL http://web.archive.org/web/19970126045828/http://www.archive.org/ would be the URL for the record of the Internet Archive home page HTML file (http://www.archive.org/) archived on January 26, 1997 at 4:58 a.m. and 28 seconds (1997/01/26 at 04:58:28). The date indicated by an extended URL applies to a preserved instance of a file for a given URL, but not necessarily to any other files linked therein. Thus, in the case of a page constituted by a primary HTML file and other separate files (e.g., files with images, audio, multimedia, design elements, or other embedded content) linked within that primary HTML file, the primary HTML file and the other files will each have their own respective extended URLs and may not have been archived on the same dates.

6. Attached hereto as Exhibit A are true and accurate copies of browser screenshots of the Internet Archive's records of the archived files for the URLs and the dates specified in the attached coversheet of each printout.

INTERNET ARCHIVE
archive.org

7. Attached hereto as Exhibit B are true and accurate copies of printouts of the Internet Archive's records of the archived files for the URLs and the dates specified in the attached coversheet of each printout.

8. I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

DATE: July 19, 2024

Nathaniel E Frank-White

Nathaniel E Frank-White

EXHIBIT A

https://web.archive.org/web/20070503023514/http://www.symantec.com/security_response/writeup.jsp?docid=2003-081113-0229-99&tabid=2

INTERNET ARCHIVE WayBackMachine
http://www.symantec.com/security_response/writeup.jsp?docid=2003-081113-0229-99&tabid=2
Go
32 captures
3 May 2007 - 20 May 2(
APR MAY JUL
2006 03 2007 2008
About this capture

W32.Blaster.Worm

Risk Level 2: Low

Printer Friendly Page

SUMMARY | TECHNICAL DETAILS

Discovered: August 11, 2003
Updated: December 9, 2003 11:50:19 PM
Type: Worm
Systems Affected: Windows 2000, Windows XP

W32.Blaster.Worm is a worm that propagates by exploiting the Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability (BID 8205).

The worm connects on TCP port 135 and sends a large amount of data sufficient to overrun the buffer. This results in critical memory being overwritten allowing the remote system to gain a shell on TCP port 4444 with Local System privileges. This shell is then used to invoke 'tftp.exe' to transfer the worm's main executable, 'msblast.exe', from the host that compromised the system. This makes stopping the worm's propagation more difficult than shutting down a hardcoded list of IP addresses.

The worm also creates the following registry entry so that it is launched every time Windows starts:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\windows auto update = msblast.exe

The worm causes the system to reboot in order to launch 'msblast.exe' immediately. It creates a mutex named 'BILLY' so that only a single instance of the worm is running on the system at a time. The compromised host will then listen on UDP port 69 for tftp connections from newly compromised systems.

The following strings are visible in the worm's code:
msblast.exe
I just want to say LOVE YOU SAN!!
billy gates why do you make this possible ? Stop making money and fix your software!!
windowsupdate.com
start %s
tftp -i %s GET %s
%d.%d.%d.%d
%i.%i.%i.%i
BILLY
windows auto update
SOFTWARE\Microsoft\Windows\CurrentVersion\Run

If the system date is after August 15th and before December 31st, the worm will cause compromised systems to initiate a denial of service attack against windowsupdate.com. This attack will also occur after the 15th day of each month not in the above date range. One of the following conditions must be met in order for the denial of service attack to occur:
The worm runs on a Windows XP computer that was either infected or rebooted during the payload period.

The worm runs on a Windows 2000 computer that was infected during the payload period and has not been restarted since it was infected.

The worm runs on a Windows 2000 computer that has been restarted since it was infected, during the payload period, and the currently logged in user is Administrator.

The denial of service attack traffic will have the following characteristics:
SYN flood with a destination port of 80.
50 HTTP packets per second.
Packets are 40 bytes in length.
If it is unable to locate a DNS entry for windowsupdate.com it will use a destination address of 255.255.255.255. It is important to note that Microsoft has removed DNS records for windowsupdate.com.

The packets will also have the following characteristics:
IP identification = 256
Time to Live = 128
Source IP address = a.b.x.y, where a.b are from the host ip and x.y are random. In some cases a.b are random.
Destination IP address = dns resolution of "windowsupdate.com"
TCP Source port is between 1000 and 1999
TCP Destination port = 80
TCP Sequence number always has the two low bytes set to 0; the 2 high bytes are random.
TCP Window size = 16384

The worm's code appears to contain the correct offsets to exploit Windows 2000 and Windows XP regardless of service pack levels. The worm has an 20% chance of using the Windows 2000 offset against a target and a 80% chance of using the Windows XP offset.

To perform its scanning routine, the worm calculates a random IP address of A.B.C.0, where A, B, and C are random values between 0 and 254. There is a 40% chance that if C is greater than 20, it will subtract a random value less than 20 from C. Once the random address is calculated, the worm begins scanning from A.B.C.0 and incrementing the last octet to scan the entire subnet.

** August 13, 2003 - A new variant of this worm has been reported in the wild. The variant uses a file named 'penis32.exe'. Analysis of this variant is currently underway and a new record will be generated when further details are available.

** August 13, 2003 - A possible third version of this worm may be in the wild. This variant is reportedly identical in functionality to the original version but uses the filename 'teekids.exe'. The executable has reportedly had some strings changed and been repacked to avoid detection with current antivirus definitions.

PRINT THIS PAGE
[+] RATE THIS PAGE

TOP THINGS TO DO
- See all Viruses & Risks
- Secure your email
- Browse the web safely
- Read the Security Response Weblogs
- Scan your computer for malware

Search Threats
Search by name
Example: W32.Beagle.AG@mm





** August 27, 2003 - HP has reported that W32.Blaster.Worm will cause a denial of service on HP OpenView DCE daemons. Other DCE implementations are likely vulnerable to this denial of service.

Multiple vendors have reported that W32.Blaster.Worm, will cause a denial of service on DCE daemons. This issue is described in BID 8371.

Recommendations

Symantec Security Response encourages all users and administrators to adhere to the following basic security "best practices":

- Turn off and remove unneeded services. By default, many operating systems install auxiliary services that are not critical, such as an FTP server, telnet, and a Web server. These services are avenues of attack. If they are removed, blended threats have less avenues of attack and you have fewer services to maintain through patch updates.
- If a blended threat exploits one or more network services, disable, or block access to, those services until a patch is applied.
- Always keep your patch levels up-to-date, especially on computers that host public services and are accessible through the firewall, such as HTTP, FTP, mail, and DNS services (for example, all Windows-based computers should have the current Service Pack installed.). Additionally, please apply any security updates that are mentioned in this writeup, in trusted Security Bulletins, or on vendor Web sites.
- Enforce a password policy. Complex passwords make it difficult to crack password files on compromised computers. This helps to prevent or limit damage when a computer is compromised.
- Configure your email server to block or remove email that contains file attachments that are commonly used to spread viruses, such as .vbs, .bat, .exe, .pif and .scr files.
- Isolate infected computers quickly to prevent further compromising your organization. Perform a forensic analysis and restore the computers using trusted media.
- Train employees not to open attachments unless they are expecting them. Also, do not execute software that is downloaded from the Internet unless it has been scanned for viruses. Simply visiting a compromised Web site can cause infection if certain browser vulnerabilities are not patched.

Writeup By: Douglas Knowles, Frederic Perriott

‹ *Summary*

Site Map · Legal Notices · Privacy Policy · Site Feedback · Contact Us · Global Sites · License Agreements
©1995 - 2007 Symantec Corporation

https://web.archive.org/web/20061020202310/http://www.securityfocus.com/infocus/1759

INTERNET ARCHIVE
WayBackMachine
http://www.securityfocus.com/infocus/1759
Go
APR OCT JUL
20
2005 2006 2008
13 captures
12 Apr 2006 - 8 Jun 202
About this capture

News
Infocus
- Foundations
- Microsoft
- Unix
- IDS
- Incidents
- Virus
- Pen-Test
- Firewalls

Columnists
Mailing Lists
- Newsletters
- Bugtraq
- Focus on IDS
- Focus on Linux
- Focus on Microsoft
- Forensics
- Pen-test
- Security Basics
- Vuln Dev

Vulnerabilities
Jobs
- Job Opportunities
- Resumes
- Job Seekers
- Employers

Tools
RSS
- News
- Vulns

Nessus, Part 3: Analysing Reports

Harry Anderson 2004-02-03

1.0 Introduction

This article, the last in the series about Nessus, will endeavor to explain a Nessus report and how to analyze it. Nessus is a vulnerability scanner, a program that looks for security bugs in software. The first article explained how to install Nessus and a basic overview of features. The second article gave general rules of thumb for various scanning situations. It is suggested that you review the first two articles before reading this one.

Understanding how and why vulnerabilities exist in software is important to being able to analyze the final scan report, and this article uses a number of examples to illustrate various important concepts. In some cases these may be older, more common examples instead of the "latest" day zero vulnerabilities. There are several reasons for this. First, I don't currently know of any awe inspiring "zero day" vulnerabilities to wow the reader with. Second, the stated examples typically have a large body of information available for the reader to do further research, and I will list a few sites providing a good start for such research. Third, although some of these examples may be older, they are still quite common and unfortunately most readers will still encounter them when scanning.

2.0 Report generation

In the last article we covered the scan process. Once the scan has been completed the results need to be analyzed. These results can be directly viewed within a report generated with the client, either Nessus GUI (Unix) or NessusWx (Windows), or by having the data exported for analysis in an external program. If viewed from within a Nessus client, the results are arranged in a hierarchical fashion by the host. In NessusWX the scan results can be obtained by selecting the session and choosing Session | Manage Results. The results can then be viewed using the VIEW command, or written into a plain text (.txt), HTML, or Adobe Acrobat (.pdf) report. In the Unix GUI the results are automatically displayed upon completion of the scan, as shown below in Figure 1. In NessusWX, sample results are shown in Figure 2.

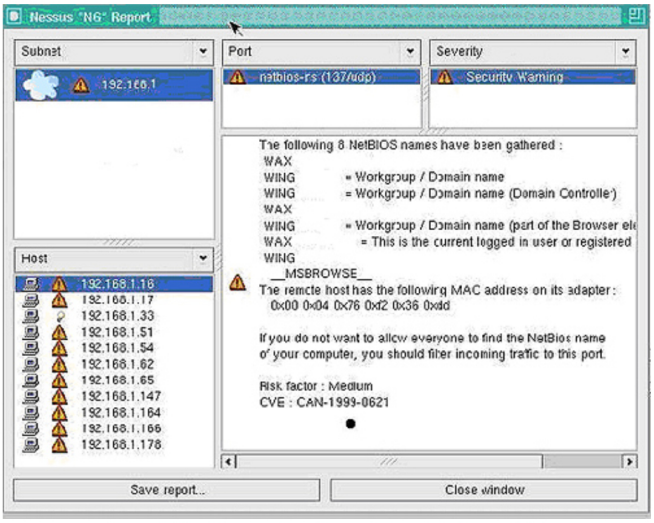


Figure 1: Results are automatically displayed in Nessus GUI.

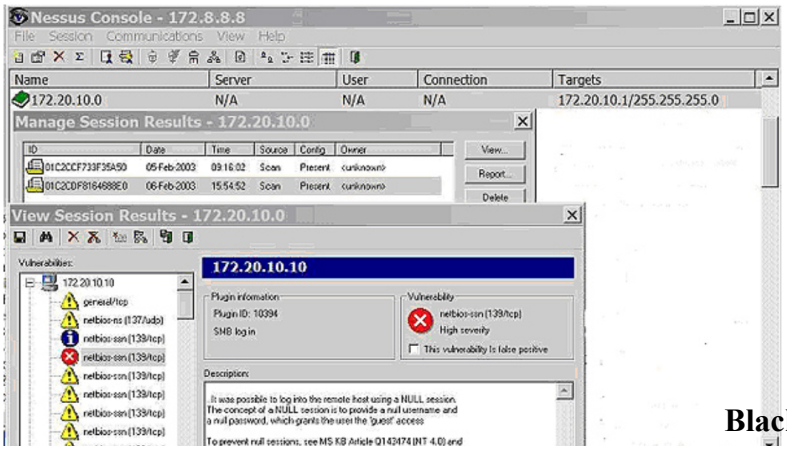




Figure2: Viewing results in NessusWX.

If a large number of hosts are being dealt with, the export functions can be very convenient. In NessusWX, results can be exported to CSV for importation to a spreadsheet, extended NSR, NSR and NBE for re-importation by any Nessus client, or into SQL files for importation into a SQL database (including MySQL). Each line item found will be exported as a single record. By importing the data into a spreadsheet or database, sorting and queries against various fields can be easily done. This gives one the ability to sort or group items by vulnerability, thus allowing one to deal with a single vulnerability at a time across many hosts. In NessusWX the scan results can be obtained by selecting the session and choosing Session | Export. In the Unix GUI, from the automatically displayed results screen, Save Report is chosen to export the data. The Unix GUI can save the data in a few more formats then NessusWX. The GUI saves in the depreciated NSR format (equivalent of the NSR format in NessusWX), as well as XML, HTML, NBE (equivalent to the extended NSR format in NessusWX), HTML, LaTeX, ASCII (similar to plain text in NessusWX) and HTML with Pies and Graphs. One difference to note between NessusWX and the Unix GUI is that NessusWX automatically saves the results when finished. The Unix GUI does not and the results will be lost upon exit if not saved.

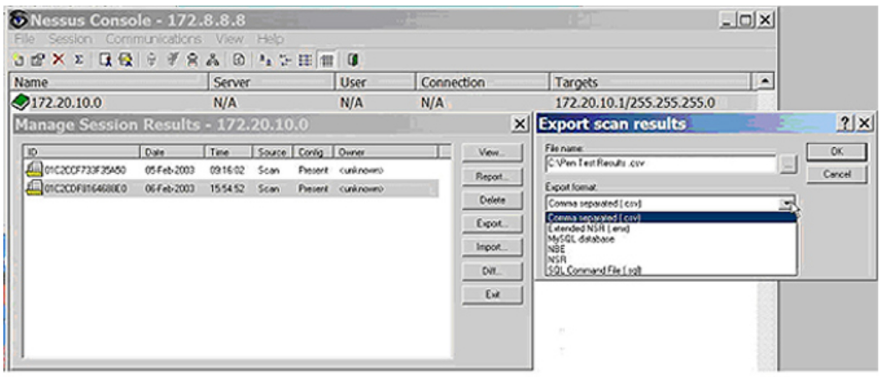


Figure 3: Image of exporting results in NessusWX.

3.0 Identifying false positives

Once the results are in a format you are prepared to deal with, the real work begins: analyzing the results and proposing solutions. In a perfect world this would be simple but due to the myriad combinations of software and configurations, remote black box vulnerability scanning is difficult and an inexact science.

One problem is that sometimes Nessus just gets it wrong. This is the case not very often but it does happen. If appropriate techniques are used (many of which are discussed in the second article of this series) the accuracy can be increased, but for the foreseeable future a human will still need to pass final judgment. Sometimes vulnerability reports can be confusing due to the many possible combinations of software and configurations involved. Although every possible way that Nessus may throw a false positive or confuse the reader can't be enumerated, many of the reasons why these things happen and the signs to look for can be discussed. Nessus typically gives you a false positive due to one of two reasons: either the plug-in is only testing for a software version number or the results are unexpected but still valid.

Testing for a given piece of software's version number only may be desirable but can also create issues that must be reviewed. Nessus has a safe-check option which changes any dangerous (but safe-check enabled) plug-ins to just check for the version number. This is a good compromise for safety, but with the current state of software configuration management, the safe check option sometimes raises false positives. There are several causes for this. First, the software may be reporting the version number of a vulnerable version but a patch or workaround has been applied. This is frequently the case with various Linux systems. The major distributions or manufacturers such as Red Hat, IBM, etc., may patch the code and not change the version number.

Version number checking may also be misleading if the vulnerability is present but not accessible due to a workaround or best practice. A good example of a best practice bypassing a vulnerability is the IIS Unicode (MS00-078, BID 1806) vulnerability. This vulnerability will execute system commands through specially formatted URLs. By following a commonly applied best practice of placing the OS and application software on separate disk partitions, this vulnerability is rendered useless. The IIS software itself would still be a vulnerable version and ideally should be patched, but the system itself would not be vulnerable to the hole. Note that this example is not affected by the safe-check option in Nessus.

All safe-check enabled items bear a warning that they may give a false positive due to the fact that only version numbers are being checked. When this warning is displayed, often a bit of research is required to determine if the system is actually vulnerable. One approach is to check the manufacturer's release notes to see if they have fixed the problem in that version of software release. Possibly by researching the vulnerability it can be determined if the vulnerability is or isn't present on a particular OS version. In the end it simply may not be possible to conclusively determine if a system is vulnerable without access to the system, or by using a non-safe check enabled Nessus scan.

Sometimes false positives also occur due to unexpected but otherwise valid results being sent back. Nessus takes into account many possible responses but it is impossible to delineate all of them. A common example of this is the large number of web vulnerabilities (usually port 80) that are sometimes falsely reported when scanning a web-server. The issue here is that Nessus isn't receiving what it expects to receive. A plug-in testing a web vulnerability will typically expect to receive an "HTTP 404" error response if the requested page isn't found. However, although it is technically against the HTTP standard, it is becoming increasingly common

for webmasters to use "custom 404 pages". These "custom 404 pages" aren't really "HTTP 404" error messages but typically a "pretty" page stating that the desired data was not found. Plug-in 10386, the "No 404 check" goes a long way to filter out these false positives by looking for common responses to page requests and correlating responses that are "custom 404s". Typically this works well. However if the web-server returns a custom page containing random or changing data, Nessus can not recognize these as a "custom 404". A telltale sign of such an issue is the large number of web-server vulnerabilities for both IIS and Apache (if the plug-ins for both web servers are being used). Verifying these is time-consuming but easy. Simply browse to the page reported to be a problem. You may have to reconstruct the problem URL from the vulnerability report. If a 404 type of custom page is displayed, it is a false positive. Otherwise the stated problem most likely does, in fact, exist.

Printers, UPSes and other hardware based devices occasionally flag a number of semi-false positives on any report. Stripped down versions of Unix/Linux and Apache are usually used for these devices and are often burned onto the device's read only memory (ROM). Of course these versions will still have whatever vulnerabilities that are later found in the software. However, since there is often little accessible memory and available resources, typically these vulnerabilities are unusable. Even if the vulnerability is exploitable, the risk may be low. Practically, how much damage can an intruder do compromising the typical printer? Printers can be identified by examining the OS discovery line item in the report.

4.0 Suspicious signs

Now that we know some of the reasons false positives may be generated, how do we recognize them? One suspicious sign is inconsistent results, especially with the reporting of a vulnerability for a software package that doesn't seem to reside on the target. Suppose a target is a identified as Windows based and yet an apparent Unix based vulnerability is found. This should raise suspicions, however the item should not be immediately written off. There could be three possible explanations: the item is false, the OS and software detection is wrong, or the problem software has been unexpectedly ported to this operating system.

While the OS and software detection in Nessus isn't perfect, it does quite well with common OSes. However, Nessus sometimes misses it when there is a variation from what is expected or when it finds an odd device. In addition, sometimes system administrators purposely change parameters specifically to confuse OS detection software. In today's computing environment more and more cross-platform development is being done, and many of today's software packages have been ported to a different OS or are used as part of other programs. Sometimes it is surprising how vulnerabilities can show up in ports across different platforms, so don't be hasty about writing off an item in Nessus' report without proper research. One example of such a surprising port is the recent system compromising OpenSSL vulnerability (BID 8732). Although usually referred to as a Unix based vulnerability, this software resides at such a low level in most packages it can also show up on Windows and Cisco environments as well. All that is required is a port of a program that uses the right version of OpenSSL.

5.0 Areas of potential confusion

False positives aren't the only issues to deal with in the report, as sometimes the correct results themselves are confusing. Confusion may stem from the result of similar vulnerability notifications. In one instance, plug-in 11424 advises against using the IIS WebDav component. This isn't a vulnerability but simply a suggested best practice. Plug-in 11412 tests for the much more famous and more dangerous, system compromising WebDav Overflow (MS03-007, BID 7116). Ironically this vulnerability has little to do with IIS and doesn't even require WebDav. WebDav was just the first of several delivery mechanisms discovered for the hole. These two items exist totally independent of each other, however in a quick reading they may be confused with each other as similar.

Another area of potential confusion is when the same named vulnerability produces different results in different environments. The Apache chunked encoding vulnerability (BID 5033) is a good example. Apache chunked encoding is actually two separate, highly related vulnerabilities. One is a DOS and one is a system compromise. The ancillary software on the target determines the result. If safe-checks are disabled, Nessus tests for this hole by sending enough junk to the server to trigger the problem. If the connection drops there is a problem. If the system compromise aspect is present, the server will start executing the uploaded data which overloaded the buffer. If the DOS aspect is present the web-server thread, which was overflowed, will crash. Nessus assumes that if the server stops responding that the vulnerability is present but it does not report if the DOS or system compromise aspect is active. If safe-checks are enabled, only the version of apache is checked.

One other area of confusion worth mentioning is the set of a few vulnerabilities to which no exploit, patch or workaround exists. These can be identified by the Nessus solution that states, "Contact your vendor for a patch." Although these vulnerabilities truly exist they are general in nature and the risk factor is low. Also, since these vulnerabilities are generally not acknowledged by the software manufacturer there is normally little that can be done to conclusively solve them

6.0 Informational items

Nessus also generates a number of informational items in its reports. Typically a report will include at least two General/TCP informational messages per host. One will document the current traceroute information to a host, and the second will make an educated guess as to the OS of the remote host. By comparing the target's fingerprint of various network-oriented parameters against a library of known values, this determination is accurate, especially for common OSes. For less common OSes usually it identifies at least the manufacturer correctly. If the fingerprint gathered does not exist in the library and the user knows the OS, the program requests the user to submit the signature and OS type to os-signatures@nessus.org. These submissions help to improve Nessus's OS detection facility for future use.

7.0 Evaluating risk

Evaluating the risk that a vulnerability might occur is another matter. Since the risk level typically determines the attention given to a problem, risk level is a important quality in the report. Nessus classifies each vulnerability as a Note, a Warning or a Hole. The risk is further identified in the plug-in summary as none, low, medium, High, Serious and Critical. Unfortunately, these classifications aren't well defined and have been subjectively applied over the years; therefore the definitions are somewhat inconsistent. There is a website available that lists some in depth statistics on Nessus's risk classifications.

If you are fixing the problems yourself, the built in classifications and risk level is probably sufficient. However, if you are passing the results on for correction by others a better defined scheme would be helpful.

Unfortunately, unlike many other industries there are no accepted computer security definitions for rating risk. The closest is the suggested definitions in the Open Source testing manual OSSTM (PDF document).

Another classification scheme that bears mention is the FBI/SAN's list of "The Twenty Most Critical Internet Security Vulnerabilities". This specification is valuable because it is fairly well known and can sometimes bring needed attention to a languishing problem. However, the list is fairly broad and it actually lists around 100 "Top" vulnerabilities and some of these are not as serious as ones which have been left off.

Most risk rating systems for vulnerabilities are based on risk relative to a target's operation and not the operation of the business. This simplifies the determining of risk but may be misleading to non-technical users since it is divorced from risk to business processes, which business types tend to better understand.

8.0 Finding a solution

Once there is a good list of found vulnerabilities, solving them is the ultimate goal. The person generating the audit report may also be the one in charge of remediation of problems, however this isn't always the case. Remediation is often passed off to others. Irregardless it is important for someone to know how to solve the problems that have been found. Some vulnerabilities are simple and obvious to solve, and the Nessus report will often include a link to a patch or a reference to a patch or workaround.

Sometimes a solution is a bit more elusive and doing some research becomes necessary. When available, Nessus provides some useful reference numbers. Chief among these are the Bugtraq ID (BID) and Common Vulnerability Exposure (CVE) numbers. The BID number is a reference number generated upon submission of a vulnerability to the Bugtraq security list. These are also the reference numbers in the searchable SecurityFocus vulnerability database. This database lists discussions on why various vulnerabilities work, lists published exploits, vulnerable versions and solutions as well as a host of other data on specific vulnerabilities. This database is arguably the most complete collection of vulnerability data available.

The CVE number provides the key to the Common Vulnerability database run by Mitre. Although some vulnerability info is stored in the CVE database, its primary purpose is to differentiate and identify vulnerabilities. This is similar to a large vulnerability Rosetta stone, providing connection between various vulnerability databases. Although the CVE database is very useful, sometimes it is a bit frustrating. Many of the vulnerabilities are still in the Candidate stage, which means that their data isn't completely verified, even though they have been around for quite a while.

Once a solution has been found and applied, good practice dictates that the target be scanned again. Unfortunately sometimes patches do not update properly, workarounds do not work or open up other holes. Thus, a follow-up scan, although sometimes not possible, is certainly a good conclusion, verifying that the target is no longer vulnerable.

9.0 Conclusion

Analysis is always the tough part of any exercise. Pressing the buttons to start a scan is easy, but understanding the result is hard. Hopefully, now you understand some of the complexities of the scanning process and can start to be able to spot the significant problems out of the tangle of information Nessus can present. This the final article in the series of Nessus articles. Hopefully they have equipped you well for those long nights of scanning ahead. Happy scanning!

SecurityFocus accepts Infocus article submissions from members of the security community. Articles are published based on outstanding merit and level of technical detail. Full submission guidelines can be found at http://www.securityfocus.com/static/submissions.html.

PRINT EMAIL

Comments Mode: Threaded Go

Expand all | Post comment

ONLINE CLASSIFIEDS

Barracuda Spam and Spyware Firewall
Reclaim your Network. Stop Spam, Spyware and Viruses at the gateway. The leading solution.

Lock Down Windows Desktops - Without the Hassle
Remove admin rights and you're busy handling exceptions. Try a simpler approach. Free webinar with featured industry analyst.

Want to know your CIS security score?
The CIS has developed detailed IT security benchmarks which will help make your computer more secure. Click here to download the Belarc Advisor which will automatically show you how secure your system is compared to the CIS benchmark configurations.

Policy Management vs Vulnerability Scanning
Which is right for you? Vulnerability scanning products test for known vulnerabilities. Policy management products are pro-active by locking the doors in advance of a possible attack. Click to request our white paper.

Find IT Consulting Jobs
Access Pre-Qualified Projects from Top Businesses. Register Now!

Buy a link Now

Privacy Statement
Copyright 2005, SecurityFocus

https://web.archive.org/web/20070219213924/http://www.nessus.org/documentation/

INTERNET ARCHIVE WayBackMachine
http://www.nessus.org/documentation/ Go JAN FEB MAR
319 captures 10 Dec 2004 - 17 Jul 20
2006 19 2007 2008
About this capture

DOCUMENTATION
QUICK LINKS

REGISTER
Register your Nessus installation to obtain the complete archive of Nessus Security Checks.

NEW PLUGINS
See the list of the newest security checks

DOWNLOAD
Download Nessus 3.0.5 now

BUY NOW
Buy a Nessus-related product today

DIRECT FEED SUPPORT
Log in to the Tenable Support Portal (Nessus Direct Feed Customers only)

BLOG
The official blog of Tenable and Nessus

WEBINARS
Register for a free webinar from Tenable Network Security, Inc.

Documentation

Nessus 3 Material

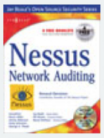
- Why Upgrade to Nessus 3 ? This page, intended for Nessus 2 users, explains the benefits of upgrading to Nessus 3
- The Nessus 3 FAQ covers various questions with regards to the Nessus 3 licensing and the licensing of its plugins
- The Policy Compliance FAQ covers various questions with regards to the policy compliance checks in Nessus 3
- Nessus 3.0 Installation Guide
- Nessus 3.0 Advanced User Guide
- Nessus 3.0 Client User Guide

Nessus 2.x material :

• Installation instructions
Learn to install the Nessus 2.x source code

• Configuring cron to fetch new plugins daily
Learn to how to configure your Unix systems to have it retrieve the newest Nessus plugins every night. **Note that this is not relevant in Nessus 3**

Books and articles about Nessus

- 

"Nessus Network Auditing" is a comprehensive manual for the Nessus scanner. Go to Syngress.com for more information.
Table of Contents Sample Chapter
- 

"Nessus, Snort and Ethereal Power Tools" is an advanced manual which explains how to configure Nessus, Snort and Ethereal to better suit your needs. Go to Syngress.com for more information.
Table of Contents Sample Chapter
- 
"Nessus 2.x kompakt" is a short (120 pages) book written in German which can be used as a quick introduction to Nessus and its related projects.. Go to http://www.bomots.de/Nessus for more information. The first three chapters are available on-line.

- **Introduction to Nessus** by Harry Anderson [Part 1] [Part 2] [Part 3]
Harry wrote three very good articles on Nessus at SecurityFocus.com. If you know nothing about Nessus, you should probably start here.
- Nessus Technical Guide by Mike Chapple
Mike Chapple at Search Security wrote a very comprehensive Nessus Technical Guide which is a good introduction to the program.

Scanning With Credentials :

- Blended security assessments
Tenable Network Security is uniquely positioned to offer enterprise management of host-based, network-based and passive vulnerability assessment technologies. This paper discusses the advantages and limitations of each technology. The challenges of performing enterprise network vulnerability assessments and how they can be overcome with Tenable Security Center and Nessus. July 2004. 10 pages
- Nessus Credentials Checks for UNIX and Windows
Nessus can not only perform remote security checks of Unix hosts and Windows hosts, but it can also log into them (provided you give it the proper credentials) to enumerate the list of missing patches. This document explains how to configure your network and Nessus to perform a complete vulnerability scan.

Online help :

- The Nessus Knowledge Base
Edgeos organized a very nice knowledge base about every configuration option in the Nessus client and the Nessus daemon. If you want to know which option means what, you should definitely look at this page !
- The Nessus Mailing Lists

Misc.

- Using Nmap from within Nessus
Nessus has the ability to launch nmap or to import its results when doing a page. This is done thru a plugin called 'nmap.nasl'. Before downloading this plugin, read this document.

© Copyright 2002 - 2007 Tenable Network Security(R). All Rights Reserved.

https://web.archive.org/web/20070222091638/http://www.nessus.org/plugins/index.php?view=single&id=11329

INTERNET ARCHIVE WayBackMachine
http://www.nessus.org/plugins/index.php?view=single&id=11329
Go
15 captures
9 Feb 2005 - 8 Mar 201
SEP FEB SEP
2005 22 2007 2010
About this capture

PLUGINS

Direct Plugin Feed
Information on how to obtain the newest Nessus plugin feed.

Newest plugins
See the list of the newest security checks

All plugins
See the whole list of security checks performed by Nessus

Search plugins
Search the Nessus plugins

Nessus Licensing FAQ
Frequently asked questions about the licensing of Nessus and its plugins

QUICK LINKS

REGISTER
Register your Nessus installation to obtain the complete archive of Nessus Security Checks.

NEW PLUGINS
See the list of the newest security checks

DOWNLOAD
Download Nessus 3.0.5 now

BUY NOW
Buy a Nessus-related product today

DIRECT FEED SUPPORT
Log in to the Tenable Support Portal (Nessus Direct Feed Customers only)

BLOG
The official blog of Tenable and Nessus

WEBINARS
Register for a free webinar from Tenable Network Security, Inc.

Plugins

The remote host is infected by a virus

This script is Copyright (C) 2005 Tenable Network Security
View the source code of this plugin here

Family	Windows
Nessus Plugin ID	11329
Bugtraq ID	
CVE ID	

Description:

This script checks for the presence of different virii on the remote host, by using the SMB credentials you provide Nessus with.

- W32/Badtrans-B
- JS_GIGGER.A@mm
- W32/Vote-A
- W32/Vote-B
- CodeRed
- W32.Sircam.Worm@mm
- W32.HLLW.Fizzer@mm
- W32.Sobig.B@mm
- W32.Sobig.E@mm
- W32.Sobig.F@mm
- W32.Sobig.C@mm
- W32.Yaha.J@mm
- W32.mimail.a@mm
- W32.mimail.c@mm
- W32.mimail.e@mm
- W32.mimail.l@mm
- W32.mimail.p@mm
- W32.Welchia.Worm
- W32.Randex.Worm
- W32.Beagle.A
- W32.Novarg.A
- Vesser
- NetSky.C
- Doomran.a
- Beagle.m
- Beagle.j
- Agobot.FO
- NetSky.W
- Sasser
- W32.Wallon.A
- W32.MyDoom.M
- W32.MyDoom.AI
- W32.MyDoom.AX
- W32.Aimdes.B
- W32.Aimdes.C
- W32.ahker.D
- Hackarmy.i
- W32.Erkez.D/Zafi.d
- Winser-A
- Berbew.K
- Hotword.b
- W32.Backdoor.Ginwui.B
- W32.Wargbot
- W32.Randex.GEL
- W32.Fujacks.B

Risk factor : High
Solution : See the URLs which will appear in the report

© Copyright 2002 - 2007 Tenable Network Security(R). All Rights Reserved.

https://web.archive.org/web/20060924205758/http://www.nessus.org/plugins/index.php?view=single&id=11818

INTERNET ARCHIVE WayBackMachine
http://www.nessus.org/plugins/index.php?view=single&id=11818
Go MAR SEP OCT
4 captures 24
28 Dec 2004 - 24 Sep 2 2005 2006 2007
About this capture

PLUGINS

Direct Plugin Feed
Information on how to obtain the newest Nessus plugin feed.

Newest plugins
See the list of the newest security checks

All plugins
See the whole list of security checks performed by Nessus

Search plugins
Search the Nessus plugins

Nessus Licensing FAQ
Frequently asked questions about the licensing of Nessus and its plugins

QUICK LINKS

REGISTER
Register your Nessus installation to obtain the complete archive of Nessus Security Checks.

NEW PLUGINS
See the list of the newest security checks

DOWNLOAD
Download Nessus 3.0.3 now

BUY NOW
Buy a Nessus-related product today

BLOG
The official blog of Tenable and Nessus

Plugins

The remote host is infected by msblast.exe

This script is Copyright (C) 2003 Tenable Network Security
View the source code of this plugin here

Family	Windows
Nessus Plugin ID	11818
Bugtraq ID	
CVE ID	

Description:

Synopsis :

The remote host is infected by a virus.

Description :

The remote host seems to be infected by the MS Blaster worm,
or the Nachi worm, and may make this host attack random hosts on the internet.

Solution :

- http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.worm.html
- http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.b.worm.html
- http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.c.worm.html
- http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.d.worm.html
- http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.e.worm.html
- http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.f.worm.html
- http://www.symantec.com/avcenter/venc/data/w32.welchia.worm.html
- http://www.microsoft.com/technet/security/bulletin/ms03-039.mspx

Risk factor :

Critical / CVSS Base Score : 10
(AV:R/AC:L/Au:NR/C:C/A:C/I:C/B:N)

© Copyright 2005 Tenable Network SecurityTM. All Rights Reserved.

EXHIBIT B

https://web.archive.org/web/20070312175637/http://nessus.org:80/documentation/nessus_3.0_client_guide.pdf

TENABLE
Network Security®

Nessus 3.0
Client Guide

March 6, 2007
(Revision 19)

The newest version of this document is available at the following URL:
http://www.nessus.org/documentation/nessus_3.0_client_guide.pdf

Table of Contents

TABLE OF CONTENTS **2**

INTRODUCTION **3**

NESSUS WINDOWS **3**

- INSTALLATION 3
- QUICK START STRATEGIES 3
- CREATING A POLICY 8
- REPORTS 13
- COMMAND LINE MODE 15

NESSUSWX **16**

- INSTALLATION 16
- QUICK START STRATEGIES 17
- CONFIGURING NESSUSWX 22

NESSUS GTK CLIENT **23**

UNIX COMMAND LINE OPERATION **24**

FOR FURTHER INFORMATION **25**

ABOUT TENABLE NETWORK SECURITY **26**

APPENDIX 1: CONFIGURING NESSUS SERVERS FOR CLIENT CONTROL **27**

- NESSUS UNIX SERVERS 27
- NESSUS WINDOWS SERVERS 27

APPENDIX 2: NESSUS WINDOWS TROUBLESHOOTING **30**

- INSTALLATION ISSUES 30
- SCANNING ISSUES 30

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**

Copyright 2004-2007, Tenable Network Security, Inc.
Proprietary Information of Tenable Network Security, Inc.

Black Kite Ex. 1013, Page 22 of 52

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. Tenable Network Security, Inc. is the author and manager of the Nessus Security Scanner. In addition to constantly improving the Nessus engine, Tenable is in charge of writing most of the plugins available to the scanner.

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

Standards and Conventions

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

Command line options and keywords are 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 are highlighted with this symbol and grey text boxes.

Nessus Windows

Installation

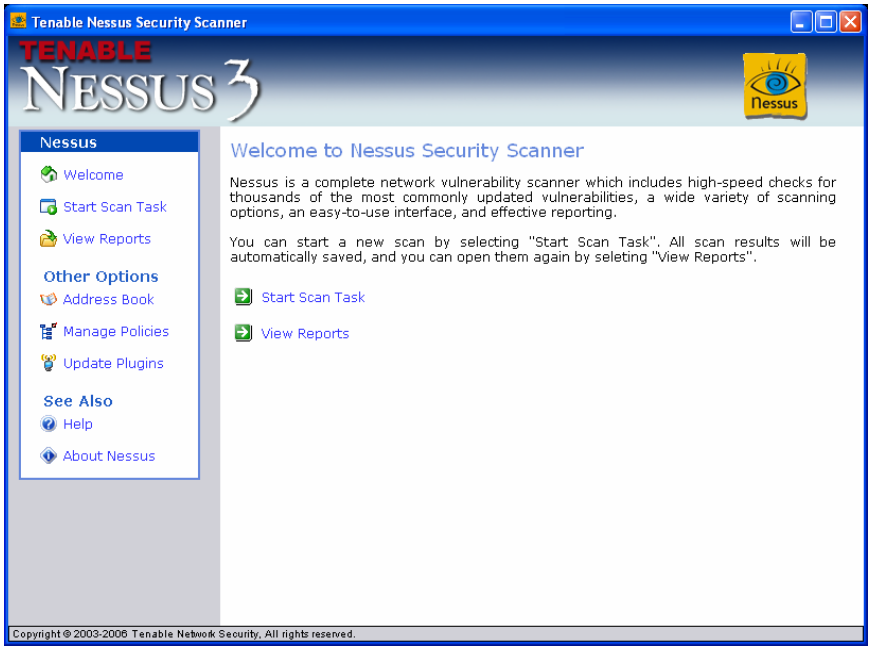
Instructions for installation are included in the "Nessus Installation Guide". These instructions will install both the server and the client for Nessus Windows.

Quick Start Strategies

Starting Nessus

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

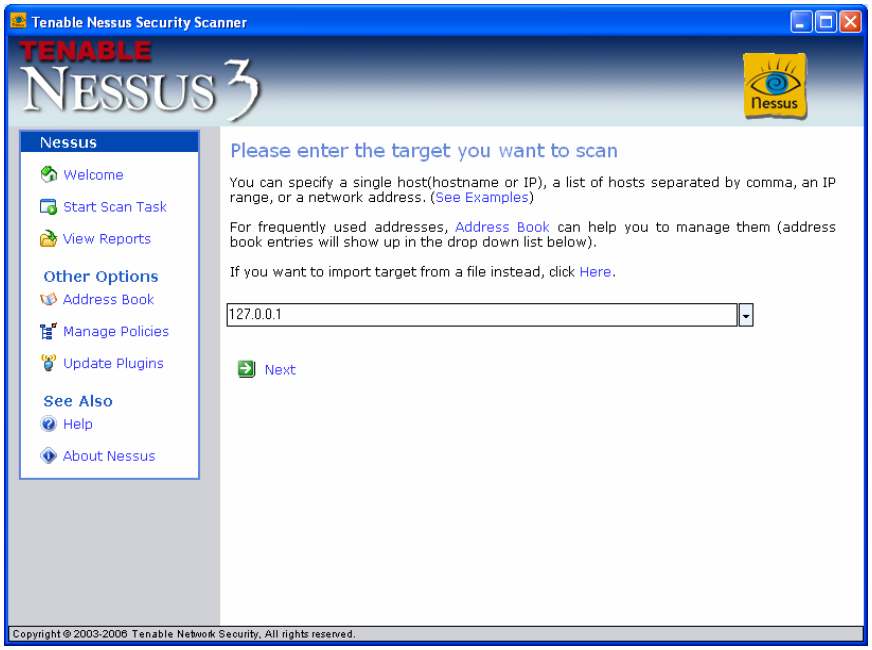
Copyright 2004-2007, Tenable Network Security, Inc.
Proprietary Information of Tenable Network Security, Inc.



Launching a Vulnerability Scan

To launch a scan simply select the first option, “Start Scan Task”, on the Nessus 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 nessus.tenable.com.

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

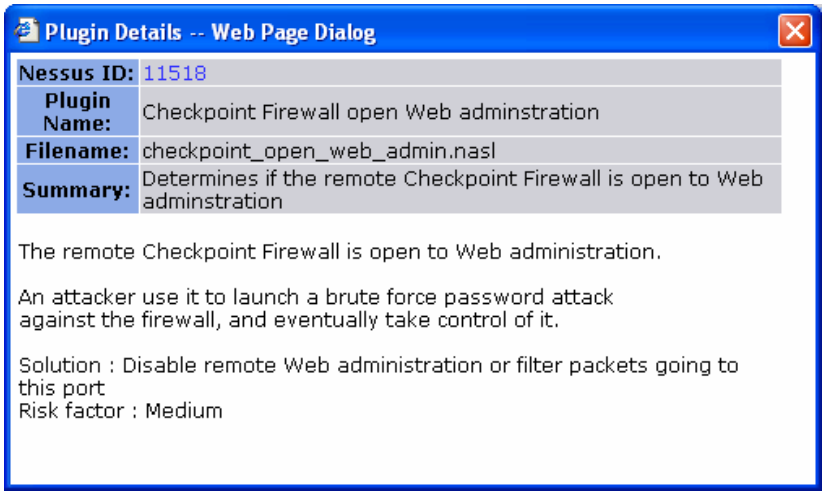


Copyright 2004-2007, Tenable Network Security, Inc.
Proprietary Information of Tenable Network Security, Inc.

Nessus 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 Nessus.

If you have clicked on the “Address Book” section, let us 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. Nessus 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 a short description. Here is an example plugin shown below:

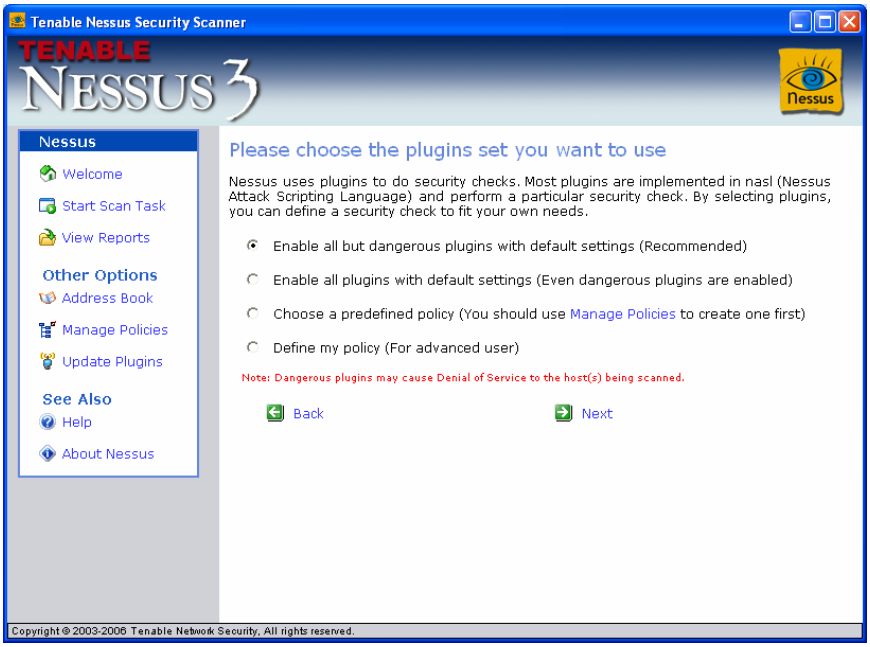


All plugins check for the presence of information. Some checks are pure audits, such as finding an open port and other checks are for exploitable holes. Nessus labels these pieces of security data as informational, warnings, and holes.

There are more than 10,000 available plugins. Each plugin 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 with default settings”, will allow all the security checks to be performed, except the Denial of Service attacks, using the default configuration settings. The second option includes the Denial of Service attacks with the default configuration settings and could cause an interruption of service to the hosts being tested.

Copyright 2004-2007, Tenable Network Security, Inc.
Proprietary Information of Tenable Network Security, Inc.



The third option allows the user to select a predefined policy that was created. A user creating a policy is able to first select specific configurations settings, and then select security checks by "family" or individual checks, and save it for future use. Then, a scan can be run using the predefined policy.

The fourth option, "Define my policy", will allow the user to create a policy with certain configuration options and checks for scanning. First the user will be able to choose the specific configuration settings to be used for the policy. Then, they can select the security checks by "family" or specific individual checks. The configuration settings are discussed in more detail in the section below entitled "Creating a Policy".

Select the Nessus Server

The next screen prompts the user to select the Nessus server that will perform the scan. Since Nessus has a client/server architecture, it is possible to use a remote Nessus server to scan a target. This can be a Nessus 3.x server on any OS that Tenable supplies a package for. Previous versions and user-compiled versions of Nessus are not supported.

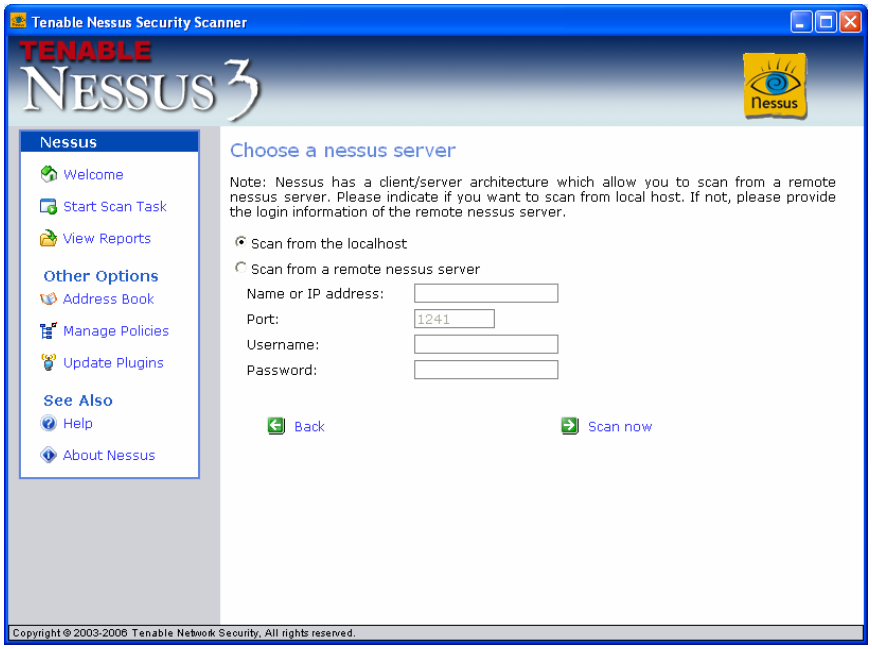
The client and server for Nessus Windows are not entirely separate at this time. The client can control any Nessus server with regard to performing a scan, but it will not push plugins to or poll plugins from any other server other than the Nessus Windows server that is installed along with the client. This means that if Nessus Windows has the Direct Feed and the remote server only has the Registered Feed, then you will be able to configure your scan to include compliance checks and the most recent plugins (less than 7 days old), but the remote server will not be able to perform these checks.

Conversely, if Nessus Windows has the Registered Feed and the remote server has the Direct Feed, then you will not be able to set up a compliance scan or a regular scan using the most recent plugins (less than 7 days old). Therefore, if you would like to use the Nessus Windows client with a remote server, you must update the plugins on both Nessus installations and you must also have the same type of plugin feed (Direct or Registered) on both scanners.

Copyright 2004-2007, Tenable Network Security, Inc.
Proprietary Information of Tenable Network Security, Inc.

To scan from a remote server you must provide its login information. Enter the name or IP address, username, and password for the remote server. Otherwise, choose the option to scan from the localhost.

For more information on configuring your Nessus servers to accept a scan job remotely from a Nessus client, please see "Appendix 1: Configuring Nessus Servers for Client Control" later in this document.



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

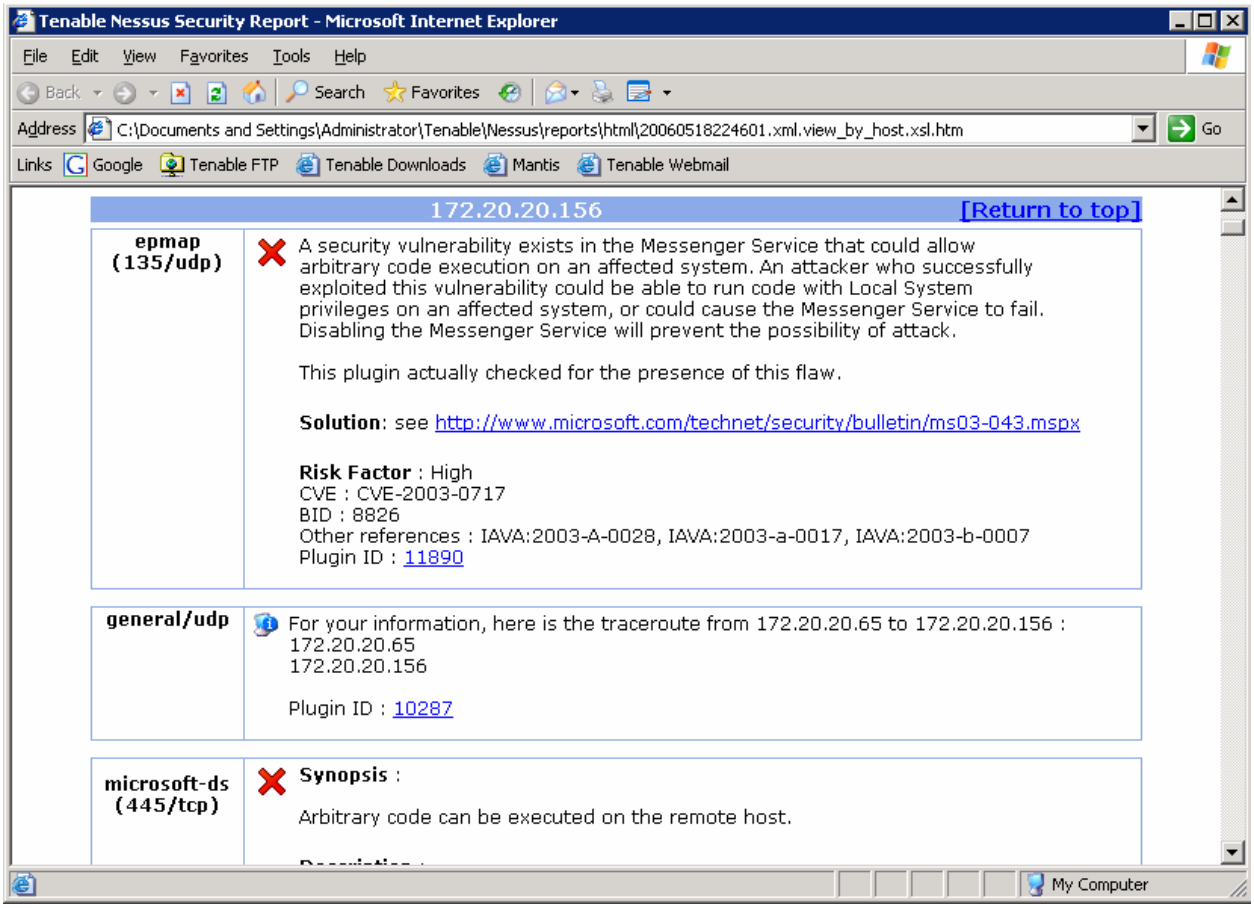
Stopping a Scan

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

Viewing the Results

The Nessus security reports will automatically pop up as a new instance of Microsoft Explorer. All reports are archived and available for viewing and printing. There is more information on reports in the "Reports" section. Below is an example scan report:

Copyright 2004-2007, Tenable Network Security, Inc.
Proprietary Information of Tenable Network Security, Inc.



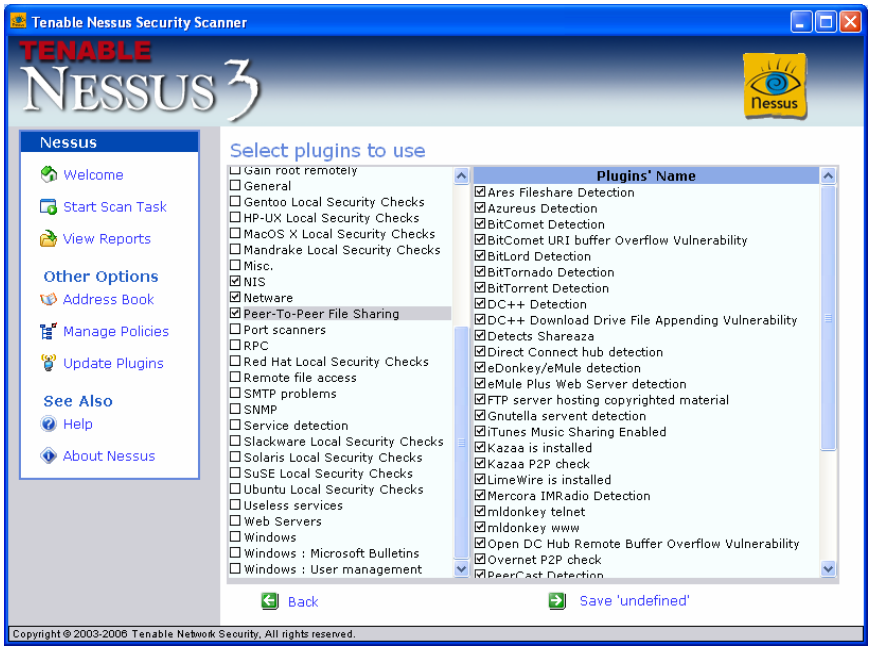
Creating a Policy

A scan policy for Nessus can be created by selecting the “Manage Policies” option. The user can either create a new policy or edit an existing policy. Once a new policy is created, click on “Edit Plugins”.

Edit Plugins

Here the user can choose specific security checks by “family” or individual checks. When selecting specific plugins, Nessus 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 within a family are enabled or disabled, the family plugin checkbox will become grayed out.

Copyright 2004-2007, Tenable Network Security, Inc.
Proprietary Information of Tenable Network Security, Inc.



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

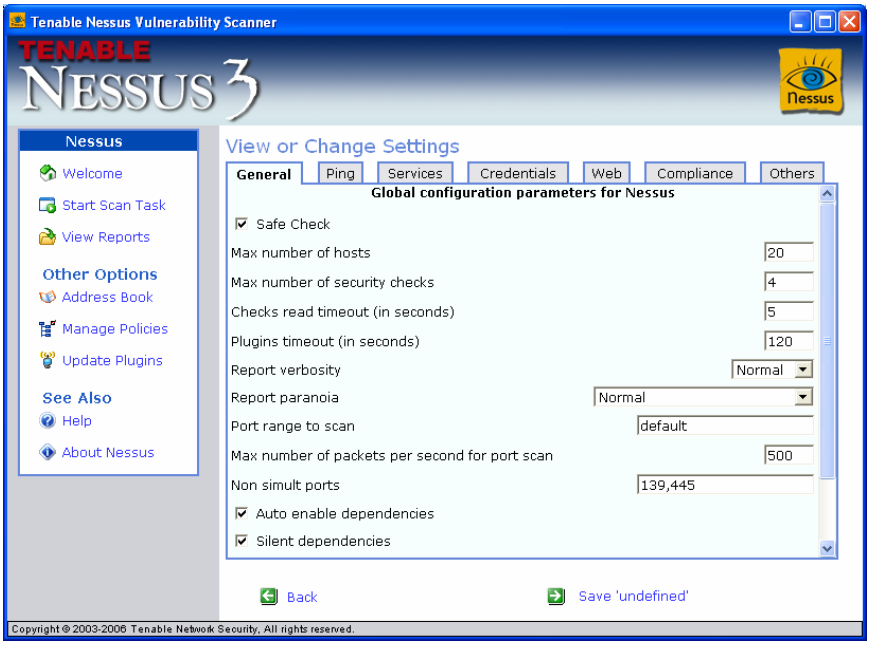


The “Denial of Service” family should not be unleashed on any enterprise network. It has the potential to crash, reboot, or freeze a wide variety of networking, server, application, and desktop installations.

Edit Settings

Next, click on “Edit Settings” to change the configuration settings. There are several hundred configuration settings. Clicking on the configuration description will produce a window with the details pertaining to that particular setting. The configuration screen will appear as below:

Copyright 2004-2007, Tenable Network Security, Inc.
Proprietary Information of Tenable Network Security, Inc.



There are seven configuration tabs that allow very granular configuration of Nessus: General, Ping, Services, Credentials, Web, Compliance, and Others. These are discussed in more detail in the next sections. Once the configuration settings are chosen, click on "Save <policy name>".

General

The configuration settings in "General" allow you to set global parameters for the plugins being run by Nessus. The first setting disables dangerous plugins that can cause Denial of Service attacks to the host(s) being scanned. The next setting sets the maximum number of hosts that will be scanned simultaneously. The third setting sets the maximum number of security plugins that will be run on each host simultaneously. 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 50 processes running simultaneously. It is important to balance the two settings so the network is not overwhelmed. Also, checking the "Thorough tests" setting causes some plugins to perform addition testing, which will produce addition results but can slow down scan time.

There are a couple settings that control the reports that are generated. "Report verbosity" controls the amount of information that the plugins will generate for the reports. "Report paranoia" changes the sensitivity of some plugins to report potential vulnerabilities.

In addition, there are settings for advanced port scanning control. The "Port range to scan" option specifies which ports to scan. Also, "Max number of packets per second for port scan" can be reduced to improve port scan accuracy. Throttling back on this number may prevent network thrashing or other problems. Finally, you can list ports that should not have two plugins running simultaneously with the "No simult ports" option.

Copyright 2004-2007, Tenable Network Security, Inc.
Proprietary Information of Tenable Network Security, Inc.

Ping

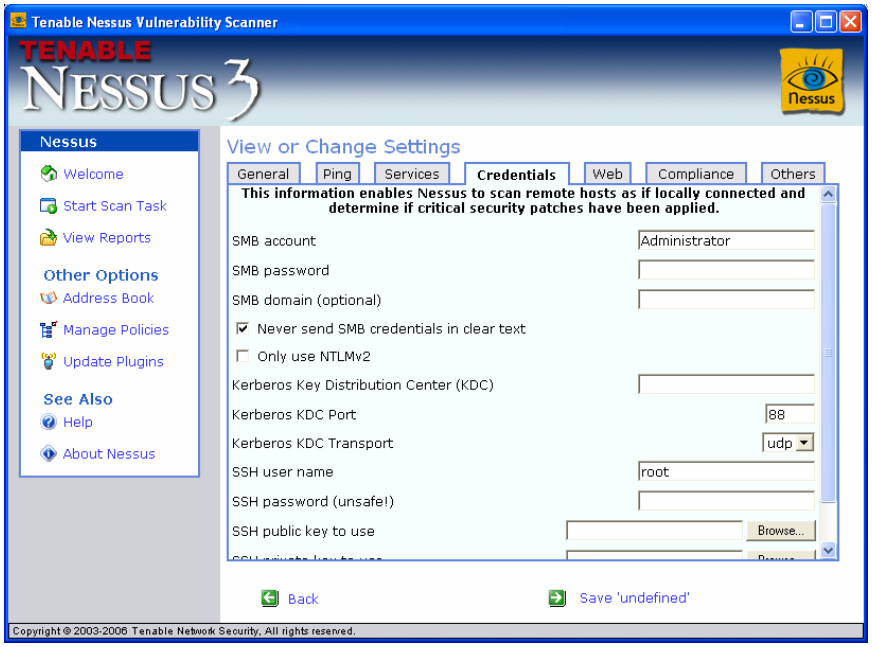
The ping protocol is used by Nessus to check if hosts and specific ports are alive. There are settings for ARP ping, ICMP ping, and TCP ping. If both ICMP ping and TCP ping are selected, Nessus will attempt to connect to hosts using both protocols.

Services

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

Credentials

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



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

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

Tenable recommends that network administrators consider creating specific domain accounts to facilitate testing. Nessus includes a variety of security checks for Windows NT,

Copyright 2004-2007, Tenable Network Security, Inc.
Proprietary Information of Tenable Network Security, Inc.

2000, Server 2003, and XP which are more accurate if a domain account is provided. Nessus does attempt to try several checks in most cases if no account is provided.

Web

The settings 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 Nessus to perform tests against Web services in the network. All requested information is optional, meaning it is not needed for proper Nessus operation.

One of the settings used in this page is a username and password. When auditing a web site protected by a username or password, adding that information to Nessus allows for vulnerability testing of the privileged access. For example, a Nessus 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 Nessus 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.

Compliance



The phrases "Policy Compliance" and "Compliance Checks" are used interchangeably within this document.

This tab enables you to submit specific policy files (*.audit*) to check your systems for compliance with various standards. You can have up to 10 different policies to compare your systems against. There are 5 for Windows and 5 for UNIX/Linux. Simply click on the "Browse…" button and select the *.audit* file to assign to the policy and click "Open". You will see the path and filename listed in the text box.



Ensure you choose the plugin family "Policy Compliance" in order to use this policy file.



Compliance checks are only enabled for customers of the Nessus Direct Feed. To gain access to this, contact your local Tenable sales representative or contact licensing@tenablesecurity.com.

Others

This tab contains additional settings. There are some settings that determine if mail and news servers can be used to relay spam. Nessus will attempt to post a news message to the news server. There are settings 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. Nessus 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.

Copyright 2004-2007, Tenable Network Security, Inc.
Proprietary Information of Tenable Network Security, Inc.

There are settings in this tab that allow you to provide site specific information, such as account names and passwords, to Nessus. 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 Nessus operation.

Tenable highly recommends that the SNMP community string be configured if it is known. If Nessus 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.

Reports

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

Report Templates

Nessus 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", "by Vulnerability", as "Plain XML", and as "Plain Text (NSR)". This allows a user to easily see the results of their scan.



Creating Report Differentials

Nessus 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 is extremely powerful to see not only which vulnerabilities have been fixed, but also which vulnerabilities are new.

Copyright 2004-2007, Tenable Network Security, Inc.
Proprietary Information of Tenable Network Security, Inc.

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" differential. 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

Nessus 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 Nessus 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\Nessus\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.

Importing Scan Data

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

Copyright 2004-2007, Tenable Network Security, Inc.
Proprietary Information of Tenable Network Security, Inc.



This will present the user with an opportunity to import a text file formatted for either Nessus's *.xml*, *.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 Nessus scanner.

Sharing Nessus Reports with Other Users

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

There are several ways to accomplish this, which are listed below:

- Web archives

  An easy way to share reports is to save the 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 ideal because, the data is spread between an *.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 Nessus, if the system which has Nessus 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.

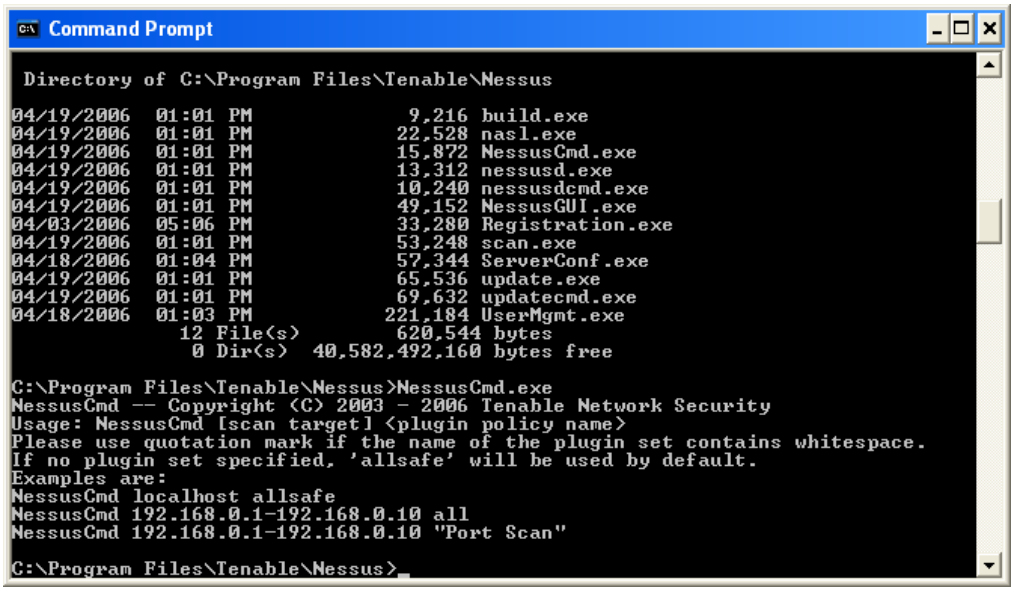
- XML Output

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

Command Line Mode

Nessus can be launched from the DOS command line mode. To do this, simply execute the *NessusCmd.exe* file from the directory *C:\Program Files\Tenable\Nessus* as shown below:

Copyright 2004-2007, Tenable Network Security, Inc.
Proprietary Information of Tenable Network Security, Inc.



This will cause a scan to be executed, but will not invoke the *nessusd.exe* file. The Nessus 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 Nessus.

After a scan has completed, the report will be located in the following directory:

C:\Documents and Settings\<admin_username>\Tenable\Nessus\reports

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.

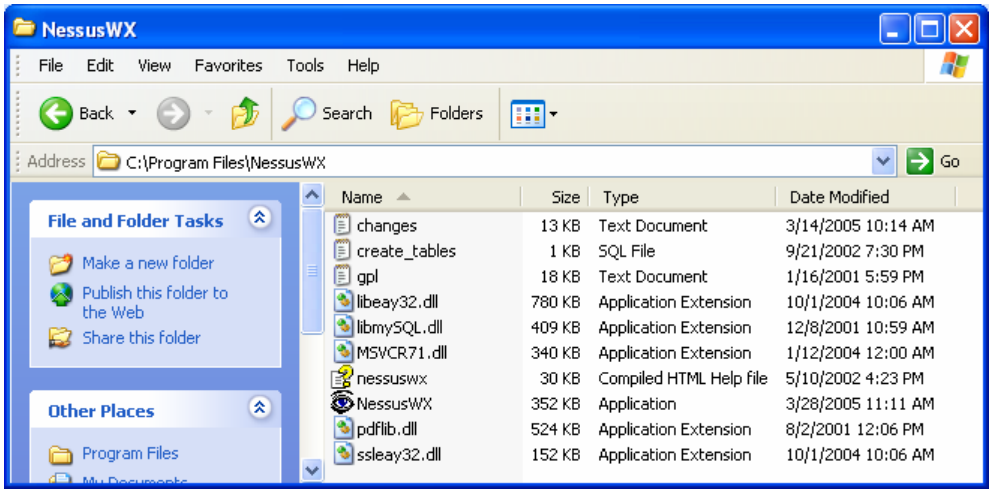
Installation

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

Copyright 2004-2007, Tenable Network Security, Inc.
Proprietary Information of Tenable Network Security, Inc.

http://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 http://www.nessus.org/download/.

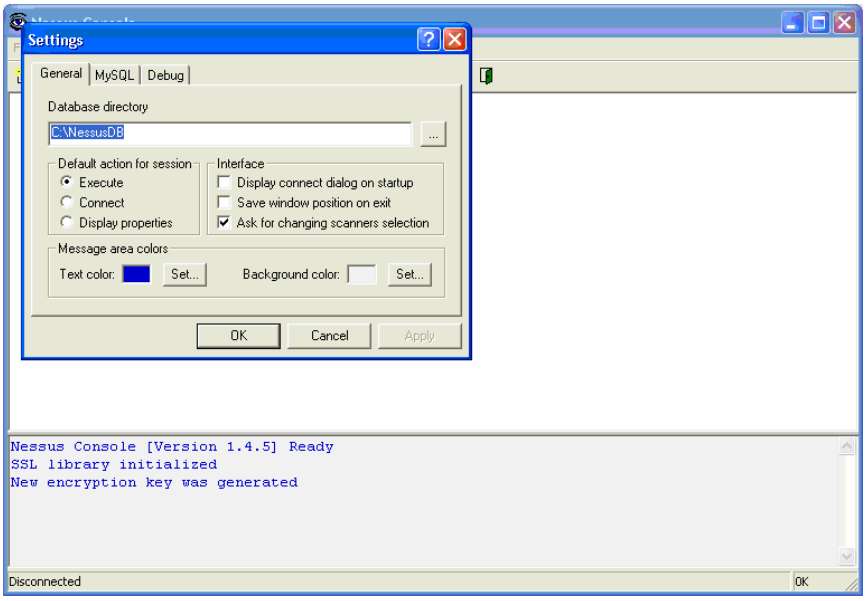
The NessusWX client will download as a zip file. Unzip its entire contents, *dll*, *exe*, and other miscellaneous files and copy them into the same directory where NessusWX is currently located (should be in C:\Program Files\NessusWX), overwriting the existing files. The database for Nessus is in a different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

Quick Start Strategies

Start 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”.

Copyright 2004-2007, Tenable Network Security, Inc.
Proprietary Information of Tenable Network Security, Inc.



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

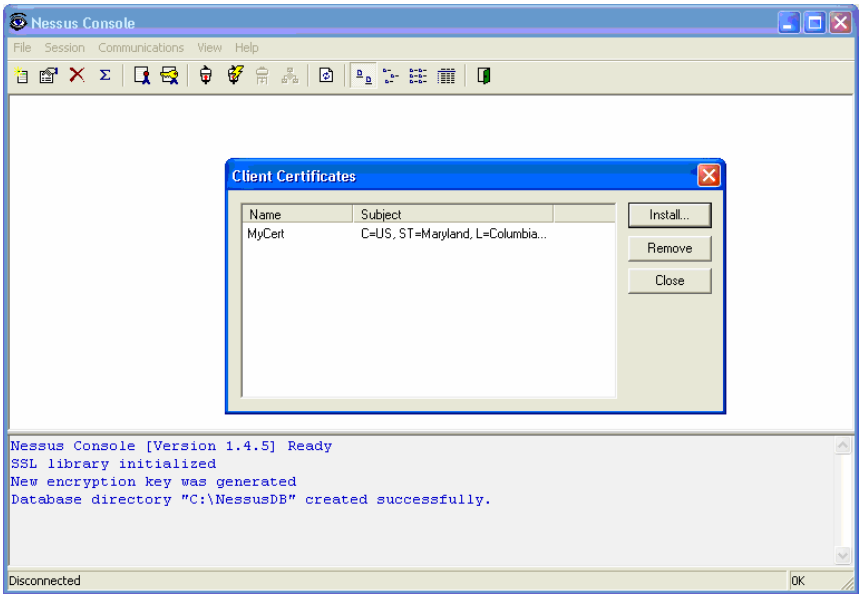
Trace complete.

C:\>
```

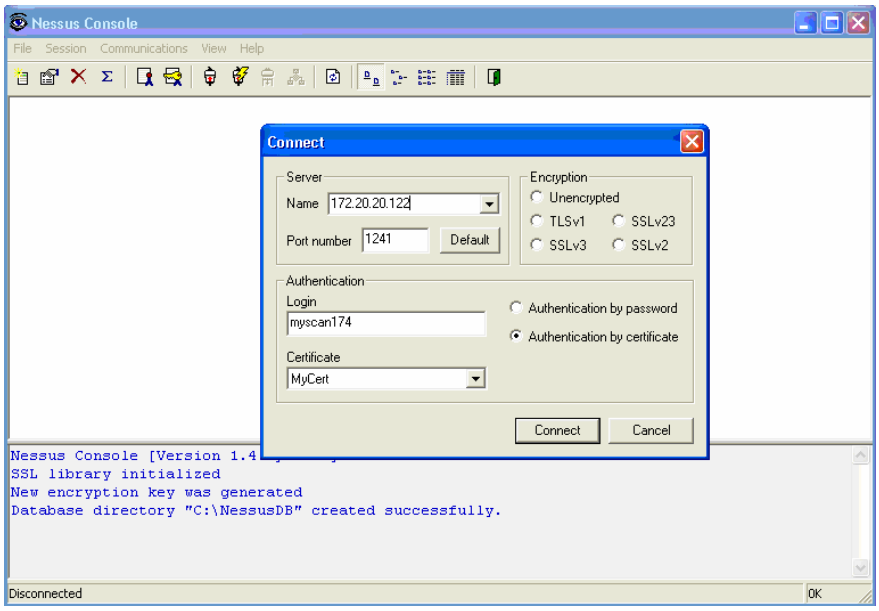
Connect to a Nessus Scanner

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 click on "Client certificate". Here is an example screen shot below:

Copyright 2004-2007, Tenable Network Security, Inc.
Proprietary Information of Tenable Network Security, Inc.

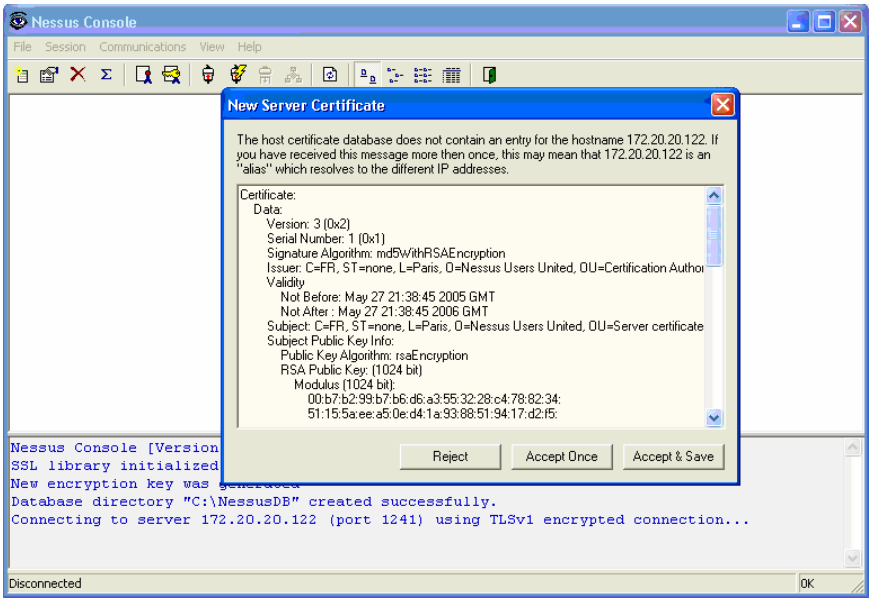


In the NessusWX GUI go to the "Communications" menu and choose "Connect". Enter the Nessus scanner IP and port (1241 is the default port). Enter the Nessus user details which will be used to authenticate the connection to the Nessus scanner. If you are using the certificate based authentication and installed 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.

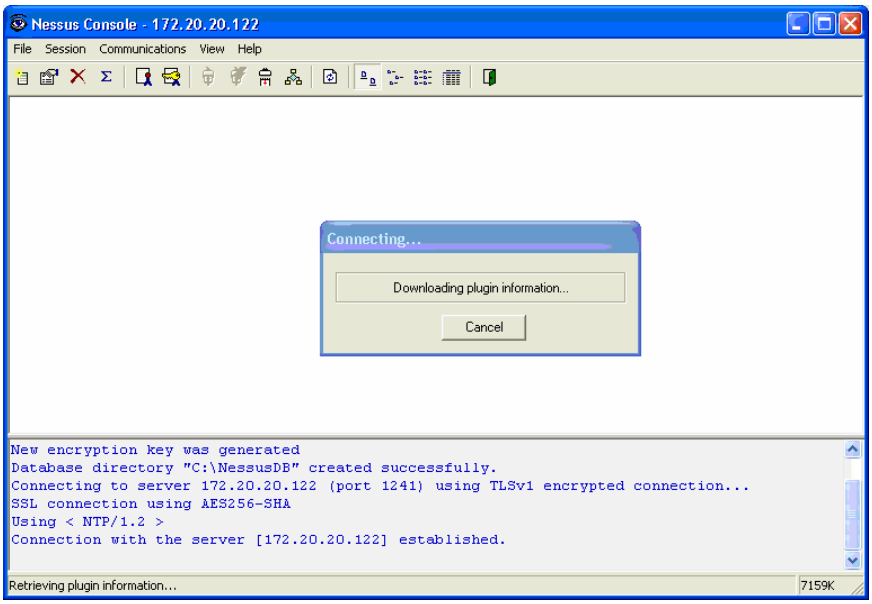


Click "Connect" and NessusWX will attempt to connect to the Nessus scanner. If a successful connection is made you will be prompted to accept the Nessus server certificate, as shown below. Click Accept Once.

Copyright 2004-2007, Tenable Network Security, Inc.
Proprietary Information of Tenable Network Security, Inc.



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.

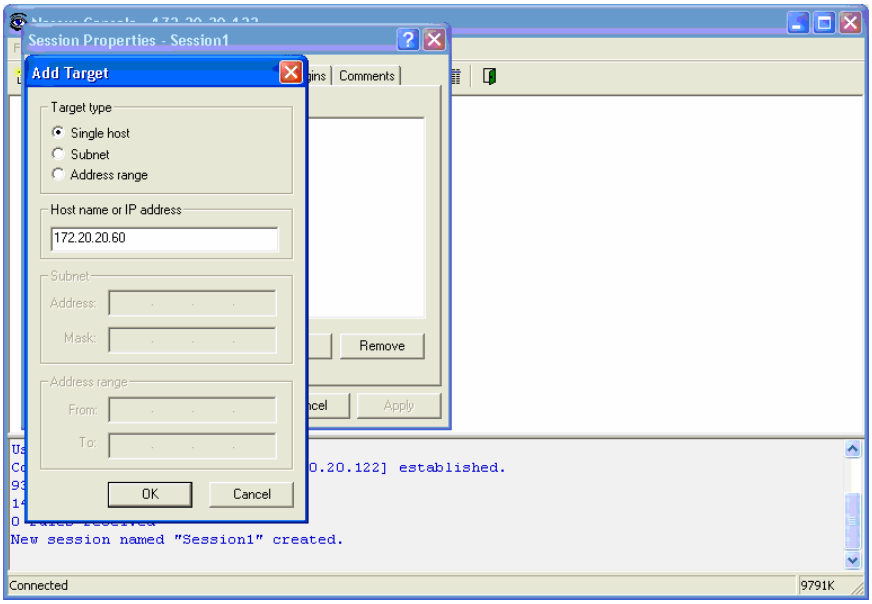
Creating an Initial Test Scan Session

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.

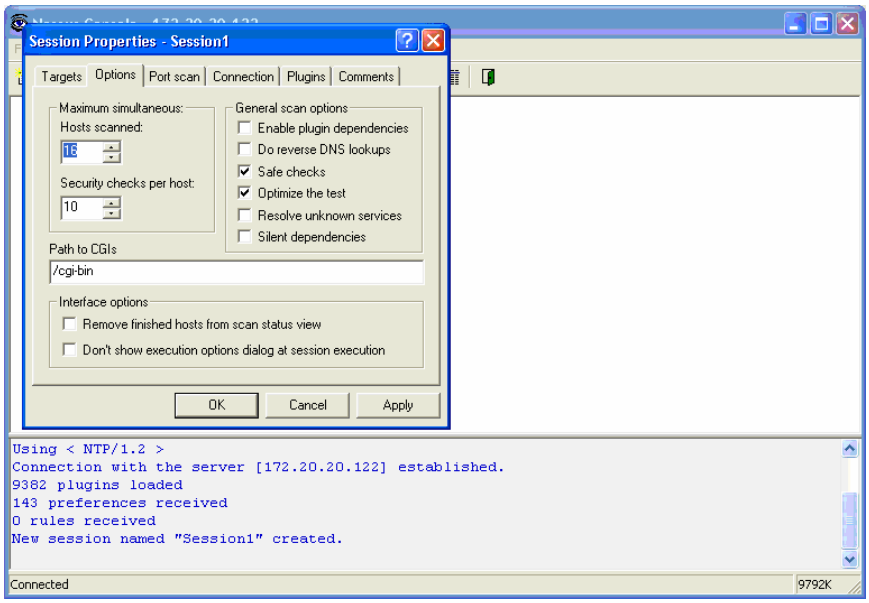
To run a test vulnerability scan, you first create a scan session using the NessusWX client. Go to the "Session" menu and choose "New". Accept the default name and click "Create".

Copyright 2004-2007, Tenable Network Security, Inc.
Proprietary Information of Tenable Network Security, Inc.

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”.

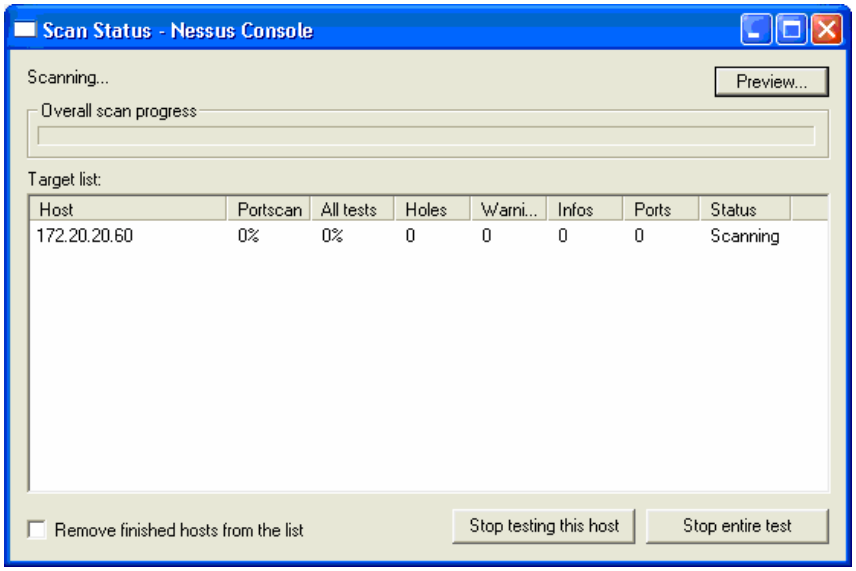
Start a Scan

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

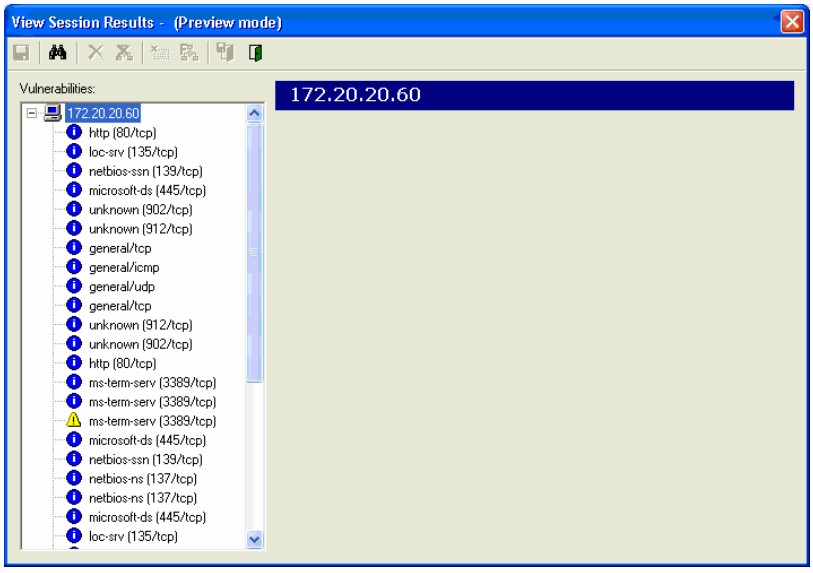
Copyright 2004-2007, Tenable Network Security, Inc.
Proprietary Information of Tenable Network Security, Inc.

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 Session" 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.

Targets

Copyright 2004-2007, Tenable Network Security, Inc.
Proprietary Information of Tenable Network Security, Inc.

The “Targets” tab 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.

Options

In the “Options” tab 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.

Port Scan

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.

Connection

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.

Plugins

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.

Comments

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.

Copyright 2004-2007, Tenable Network Security, Inc.
Proprietary Information of Tenable Network Security, Inc.

You can download NessusClient RPM from http://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.

UNIX 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.

Copyright 2004-2007, Tenable Network Security, Inc.
Proprietary Information of Tenable Network Security, Inc.

`-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
- **Real-Time Compliance Monitoring** – outlines how Tenable’s solutions can be used to assist in meeting many different types of government and financial regulations

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.

Copyright 2004-2007, Tenable Network Security, Inc.
Proprietary Information of Tenable Network Security, Inc.

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 http://www.tenablesecurity.com.

TENABLE Network Security, Inc.
7063 Columbia Gateway Drive
Suite 100
Columbia, MD 21046
TEL: 1-877-448-0489
http://www.tenablesecurity.com

Copyright 2004-2007, Tenable Network Security, Inc.
Proprietary Information of Tenable Network Security, Inc.

Appendix 1: Configuring Nessus Servers for Client Control

Nessus UNIX Servers

To enable any UNIX Nessus scanner for control by a Nessus client, a username and password combination must be created. The user account created for administration when the Nessus server was installed can be used for this purpose.

Also, you may use the `nessus-adduser` utility on the Nessus server to be managed by the client to create the credentials. This utility will be located in the */opt/nessus/sbin/* directory. For example, on Red Hat Linux systems, this utility will be located at */opt/nessus/sbin/nessus-adduser*.

If a Nessus scanner is configured to only scan certain IP ranges, it can still be used by the remote client. However, if an attempt is made to scan outside of those ranges, no vulnerability data will be reported.

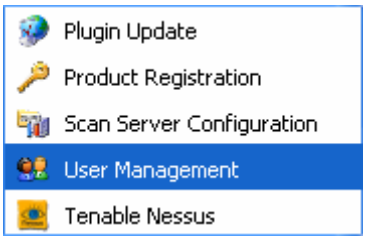
The Nessus scanner must be restarted for these changes to take effect. It can be restarted with the `kill` command as in `kill –HUP <process id of nessusd>`.

Nessus Windows Servers

Nessus Windows can be configured to receive scan job requests from remote clients. To do this, we need to complete two tasks. First, we need to add an account for the remote client to log into Nessus with, and then we need to enable Nessus to listen to inbound network connections. By default, Nessus only listens to localhost connections.

Adding User Accounts

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



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

Choose a unique username and password that will be used when the remote Nessus client requests this server to perform scans.



Please note that Nessus uses an internal administrative account for local communication between the Nessus GUI and the Tenable Nessus Service. This account cannot be used for remote connection from the Security Center.

Copyright 2004-2007, Tenable Network Security, Inc.
Proprietary Information of Tenable Network Security, Inc.

Black Kite Ex. 1013, Page 47 of 52

Enabling Network Connections

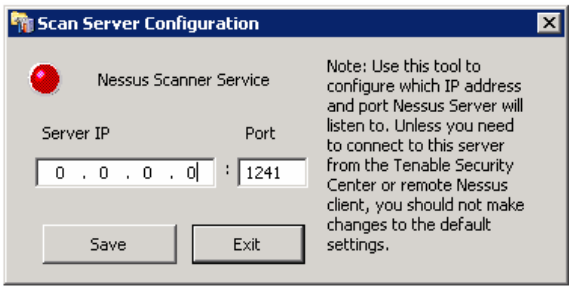
To allow a remote connection to Nessus from remote Nessus clients, run the "Scan Server Configuration" tool. This tool allows the port and bound interface of the Nessus daemon to be configured. By default, the Nessus daemon listens to connections on localhost (127.0.0.1) and port 1241.

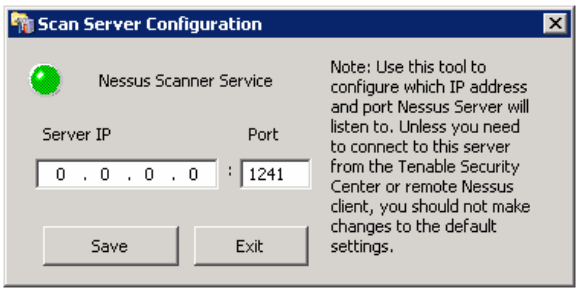
Nessus must be configured to listen for connections either on one network interface, or any interface. Type in the IP address of the Nessus network interface it should be bound to.

- 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 Nessus" service is not running. Clicking on the red button will start the service. If this is attempted, the indicator will turn yellow and then green if successful.

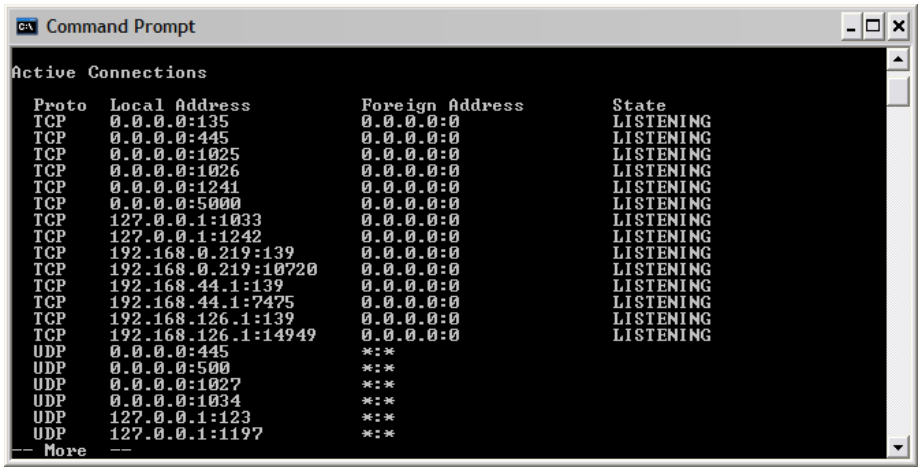




Any change to the information in the dialogue box of the "Scan Server Configuration" tool will also prompt the user to see if they want to restart the "Tenable Nessus" service.

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

Copyright 2004-2007, Tenable Network Security, Inc.
Proprietary Information of Tenable Network Security, Inc.



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 Nessus 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 remote client’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.

Copyright 2004-2007, Tenable Network Security, Inc.
Proprietary Information of Tenable Network Security, Inc.

Appendix 2: Nessus Windows Troubleshooting

Installation Issues

Issue: I am receiving the following error when I try to install Nessus Windows:

"1607: Unable to install InstallShield Scripting Runtime"

Solution: This is a problem between the Microsoft Windows Operating System settings and the InstallShield product that is used for installing and removing Nessus Windows. There are knowledge base articles from both Microsoft and InstallShield which both detail potential causes and the resolution of the issue.

- Microsoft Knowledge Base Article ID 910816: http://support.microsoft.com/?scid=kb;en-us;910816
- InstallShield Knowledge Base Article ID Q108340: http://consumer.installshield.com/kb.asp?id=Q108340

Scanning Issues

Issue: While starting or operating Nessus Windows I receive the following error:

"A Runtime Error Has Occurred. Do you wish to debug?
Line 31: Error: Object doesn't support this property or method"

Clicking on Continue launches the debugger. If you choose not to debug by clicking "No", you are returned to the main Nessus screen.

Attempting subsequent Nessus operations, such as New Scan Task, returns the following error:

"Error: line 154"

Continuing through the above error message returns:

"No scan control"

Solution: COM registration for Nessus has failed on the system during installation. Since the installer can not fix the problem, please perform the following steps:

1. From Start menu, click on "All Programs", then "Accessories".
2. Right click on "Command Prompt" and select "Run as Administrator".
3. Type "cd c:\Program File\Tenable\Nessus".
4. Type "regsvr32 scan.dll".

The steps above will install the COM component manually. Nessus should now start and operate without issue.

Copyright 2004-2007, Tenable Network Security, Inc.
Proprietary Information of Tenable Network Security, Inc.

Issue: When attempting to perform a scan using Nessus Windows I receive the following error message:

"Error: Automation server can't create object"

Or

"Error 1935. An error occurred during the installation of assembly "Microsoft.MSXML..."

Solution: This is an issue with the XML Parser on the system Nessus Windows is installed on. Either it is not up to date or it may need to be re-installed.

If the system is up to date, please refer to the following Microsoft knowledge base article for more information regarding the msxml.dll parser:

http://support.microsoft.com/kb/269238/

To re-install the MS XML Parser on the system, access a command prompt and execute the following command:

```
regsvr32 %windir%\system32\msxml4.dll
```

Issue: I cannot scan over my PPP or PPTP connection.

Solution: Currently, this is not supported. Future revisions of Nessus Windows will include this functionality.

Issue: A virus-scan of my system reports a large number of viruses in Nessus Windows.

Solution: Certain anti-virus applications may show some of the Nessus plugins as viruses. You should exclude the plugins directory from virus scans. There are no executable programs in this directory.

Issue: I am scanning an unusual device, such as a RAID controller, and the scan is aborted because it because Nessus has detected it as a printer.

Solution: Disable "Safe Checks" in the scan policy before scanning the device. A scan of a printer will usually result in the printer needing to be restarted therefore when "Safe Checks" is set devices detected as printers are not scanned.

Issue: I am not able to use Nmap to conduct port scans as with previous versions of Nessus.

Solution: Please see the following URL:

http://www.nessus.org/documentation/index.php?doc=nmap-usage

Issue: I am not able to conduct a TCP Connect scan using Nessus Windows.

Solution: Because of the limitations of the Windows TCP/IP stack, Nessus Windows cannot perform TCP Connect scans.

Copyright 2004-2007, Tenable Network Security, Inc.
Proprietary Information of Tenable Network Security, Inc.

Issue: SYN scans do not appear to wait for the port connection to be established in Nessus Windows.

Solution: This is correct in that the SYN scan does not establish a full TCP connect, however it does not change the scan results.

Issue: When performing a scan, what factors affect false negative results when running Nessus Windows on a Windows XP system?

Solution: Microsoft has added changes to Windows XP Service Pack 2 (Home & Pro) that can impact the performance of Nessus Windows and cause false negatives. The TCP/IP stack now limits the number of simultaneous incomplete outbound TCP connection attempts. After the limit has been reached, subsequent connection attempts are put in a queue and will be resolved at a fixed rate (10 per second). If too many enter the queue, they may be dropped. See the following Microsoft TechNet page for more information:

http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/sp2netwk.mspx

This has the effect of causing a Nessus scan on Windows XP to potentially have false negatives as XP only allows for 10 new connections per second that are incomplete (in a SYN state). For better accuracy it is recommended that Nessus on a Windows XP system have its port scan throttle setting down to the following which is found in the individual scan configuration for each scan policy:

Max number of hosts: 10
Max number of security checks: 4
Max number of packets per second for a port scan: 50

For increased performance and scan reliability it is highly recommended that Nessus Windows be installed on a server product from the Microsoft Windows family like Windows Server 2003.

Copyright 2004-2007, Tenable Network Security, Inc.
Proprietary Information of Tenable Network Security, Inc.

Black Kite Ex. 1013, Page 52 of 52