
GFI LANguard Network Security Scanner 5

Manual

By GFI Software Ltd.

GFI SOFTWARE Ltd.
<http://www.gfi.com>
E-mail: info@gfi.com

Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of GFI SOFTWARE Ltd.

LANguard is copyright of GFI SOFTWARE Ltd. 2000-2004 GFI SOFTWARE Ltd. All rights reserved.

Version 5.0 – Last updated 01/12/04

Contents

Introduction	5
Introduction to GFI LANguard Network Security Scanner.....	5
Importance of Internal Network Security	5
Key Features	6
GFI LANguard N.S.S. components	6
License Scheme	7
Installing GFI LANguard Network Security Scanner	9
System Requirements	9
Installation Procedure	9
Entering your License key after installation.....	11
Getting Started: Performing an Audit	13
Introduction to Security Audits.....	13
Performing a Scan	13
Analyzing the Scan Results.....	14
IP, Machine name, OS and Service pack Level.....	15
Vulnerabilities Node.....	15
Potential Vulnerabilities Node	16
Shares	16
Password Policy	17
Registry.....	17
Security audit policy.....	17
Open Ports	19
Users & Groups.....	19
Services	19
System Patching status	19
Additional Results.....	20
General Information -?.....	Error! Bookmark n
Trusted Domains - ?	Error! Bookmark n
Computer.....	20
Performing On site and Off site scans.....	20
On Site Scan	20
Off Site Scan	21
Comparison of on site and off site scans	21
Filtering scan results	23
Introduction	23
Selecting the scan results source.....	24
Creating a custom scan filter	24
Configuring Scan Options	27
Introduction to Scan Options	27
Scanning profiles	27
Scanned TCP/UDP ports.....	28
How to add/edit/remove ports	28
Scanned OS data	29

Scanned Vulnerabilities	30
Types of Vulnerabilities	30
Downloading the latest Security Vulnerabilities.....	31
Scanned Patches	31
Scanner options.....	32
Network discovery methods	33
Scheduled Scans.....	34
Parameter files.....	36
Patch Deployment	39
Introduction to patch deployment	39
The patch deployment agent.....	39
Step 1: Perform a scan of your network	39
Step 2: Select on which machines to deploy the patches	40
Step 3: Select which patches to deploy.....	41
Step 4: Download the patch & service pack files	42
Downloading the patches	42
Step 5: Patch file deployment parameters	43
Step 6: Deploy the updates	44
Deploying custom software	45
Step 1: Select the machines on which to install the software/patches	46
Step 2: Specify software to deploy	46
Step 3: Start the deployment process	46
Deployment options.....	47
Results Comparison	49
Why Compare Results?.....	49
Performing a Results Comparison interactively	49
Performing a Comparison with the Scheduled Scans Option	50
Tools	51
Introduction	51
DNS lookup.....	51
Trace Route.....	52
Whois Client.....	53
SNMP Walk	53
SNMP Audit	53
MS SQL Server Audit	54
Enumerate Computers	55
Launching a security scan	55
Deploying Custom patches.....	55
Enabling Auditing Policies	55
Enumerate Users.....	56
Adding vulnerability checks via conditions or scripts	57
Introduction	57
GFI LANguard N.S.S. VBscript language.....	57
Adding a vulnerability check that uses a custom script	57
Step 1 : Create the script.....	57
Step 2: Add the new vulnerability check:.....	58
Adding a CGI vulnerability check	59
Adding other vulnerability checks	60
Troubleshooting	65
Introduction	65
Knowledgebase	65

Request support via e-mail	65
Request support via webchat	66
Request support via phone.....	66
Web Forum	66
Build notifications.....	66

Index	67
--------------	-----------

Introduction

Introduction to GFI LANguard Network Security Scanner

GFI LANguard Network Security Scanner (**GFI LANguard N.S.S.**) is a tool that allows network administrators to quickly and easily perform a network security audit. GFI LANguard N.S.S. creates reports that can be used to fix security issues on a network. It can also perform patch management.

Unlike other security scanners, GFI LANguard N.S.S. will not create a 'barrage' of information, which is virtually impossible to follow up on. Rather, it will help highlight the most important information. It also provides hyperlinks to security sites to find out more about these vulnerabilities.

Using intelligent scanning, GFI LANguard N.S.S. gathers information on machines such as usernames and groups, which may include rogue objects to allow backdoor access, network shares and similar objects found on a Windows Domain.

Apart from this, GFI LANguard N.S.S. also identifies specific vulnerabilities such as configuration problems in FTP servers, exploits in Microsoft IIS and Apache Web Servers or problems in NT security policy configuration, plus many other potential security issues.

Importance of Internal Network Security

Internal Network security is, more often than not, underestimated by its administrators. Very often, such security does not even exist, allowing one user to easily access another user's machine using well-known exploits, trust relationships and default settings. Most of these attacks require little or no skill, putting the integrity of a network at stake.

Most employees do not need and should not have access to each other's machines, administrative functions, network devices and so on. However, because of the amount of flexibility needed for normal operation, internal networks cannot afford maximum security. On the other hand, with no security at all, internal users can be a major threat to many corporate internal networks.

A user within the company already has access to many internal resources and does not need to bypass firewalls or other security mechanisms which prevent non-trusted sources, such as Internet users, to access the internal network. Such internal users, equipped with hacking skills, can successfully penetrate and achieve remote administrative network rights while ensuring that their abuse is hard to identify or even detect.

In fact, 80% of network attacks originate from inside the firewall (ComputerWorld, January 2002).

Poor network security also means that, should an external hacker break into a computer on your network, he/she can then access the rest of the internal network more easily. This would enable a sophisticated attacker to read and possibly leak confidential emails and documents; trash computers, leading to loss of information; and more. Not to mention then use your network and network resources to turn around and start attacking other sites, that when discovered will lead back to you and your company, not the hacker.

Most attacks, against known exploits, could be easily fixed and, therefore, be stopped by administrators if they knew about the vulnerability in the first place. The function of GFI LANguard N.S.S. is to assist administrators in the identification of these vulnerabilities.

Key Features

- Finds rogue services and open TCP and UDP ports
- Detects known CGI, DNS, FTP, Mail, RPC and other vulnerabilities
- Detects Rogue or backdoor users
- Detects Open shares
- Enumeration of users, services, etc.
- Can perform Scheduled Scans
- Automatically updates Security vulnerability checks
- Ability to detect missing hot fixes and service packs for the operating system.
- Ability to detect missing hot fixes and service packs for supported applications.
- Ability to compare scans, to learn about new possible entry points
- Ability to patch OS (English Windows Systems) & Office applications (English, French, German, Italian, Spanish)
- Operating system identification
- Live host detection
- HTML, XSL and XML output
- SNMP & MS SQL auditing
- VBscript compatible scripting language to build custom vulnerability checks

GFI LANguard N.S.S. components

GFI LANguard N.S.S. is built on an enterprise class architecture and has the following components

GFI LANguard Network Security Scanner

This is the main interface to the product. Use this application to view the scanning results real time, configuring scan options, scan profiles, filter reports, use specialized security administration tools and more.

GFI LANguard N.S.S. attendant service

This service runs scheduled network scans, and scheduled patch deployments. It runs in the background.

GFI LANguard N.S.S. Patch agent service

This service is deployed on the target machines on which a patch, service pack or software has to be deployed and takes care of the actual patch, service pack or software installation.

GFI LANguard N.S.S. Script Debugger

Use this module to write/debug custom scripts that you have created.

License Scheme

The GFI LANguard N.S.S. licensing scheme works on the number of machines & devices that you wish to scan. For example, the 100 IP license allows you to scan up to 100 machines or devices from a single workstation/server on your network.

Installing GFI LANguard Network Security Scanner

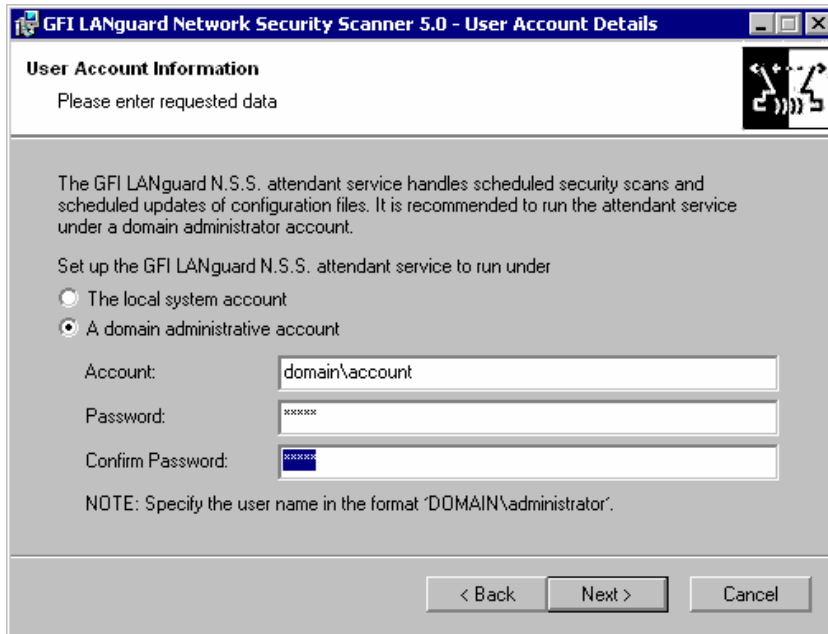
System Requirements

The installation of GFI LANguard Network Security Scanner requires the following:

- Windows 2000/2003 or Windows XP
- Internet Explorer 5.1 or higher
- Client for Microsoft Networks must be installed.
- NO Personal Firewall software or the Windows XP Internet Connection Firewall can be running while doing scans. It can block functionality of GFI LANguard N.S.S.
- To deploy patches on remote machines you need to have administrator privileges

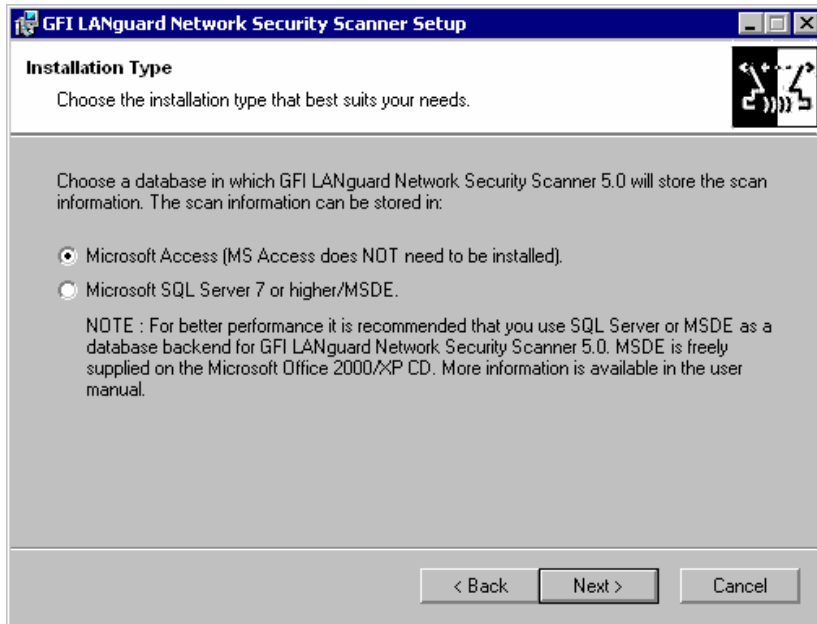
Installation Procedure

1. Run the LANguard Network Security Scanner setup program by double clicking on the lannetscan.exe file. Confirm that you wish to install GFI LANguard N.S.S. The set-up wizard will start. Click **Next**.
2. After reading the License agreement dialog box, click **Yes** to accept the agreement and continue the installation.
3. Setup will ask you for user information and License key



Specify domain administrator credentials or use local system account

4. Setup will ask you for domain administrator credentials which are used by the LANguard N.S.S Attendant service (which runs scheduled scans). Enter the necessary credentials and click **Next**.



Choose database back-end

5. Setup will ask you to choose the database backend for the GFI LANguard N.S.S database. Choose between Microsoft Access or Microsoft SQL Server\MSDE and click **Next**.

NOTE : SQL Server/MSDE must be installed in mixed mode or SQL server authentication mode. NT authentication mode only is not supported.

6. If you selected Microsoft SQL Server/MSDE as a database backend, you will be asked for the SQL credentials to use to log on to the database. Click **Next** to continue.
7. Setup will ask you for an administrator email address and your mail server name. These settings will be used for sending administrative alerts.
8. Choose the destination location for GFI LANguard N.S.S. and click **Next**. GFI LANguard N.S.S. will need approximately 40 MB of free hard disk space.
9. After GFI LANguard N.S.S. has been installed, you can run GFI LANguard Network Security Scanner from the start menu.

Entering your License key after installation

If you have purchased GFI LANguard N.S.S., you can enter your License key in the General > Licensing node.

If you are evaluating GFI LANguard N.S.S., it will time out after 60 days (with evaluation key). If you then decide to purchase GFI LANguard N.S.S., you can just enter the License key here without having to re-install.

You must license GFI LANguard N.S.S. for the number of machines that you wish to scan, and for the number of machines that you wish to run it on. If you have 3 administrators using GFI LANguard N.S.S. then you have to buy 3 licenses.

Entering the License key should not be confused with the process of registering your company details on our website. This is important, since it allows us to give you support and notify you of important product news. Register on:

<http://www.gfi.com/pages/regfrm.htm>

Note: To find out how to buy GFI LANguard N.S.S., follow the General > How to purchase node.

Getting Started: Performing an Audit

Introduction to Security Audits

An audit of network resources enables the administrator to identify possible risks within a network. Doing this manually requires a lot of time, because of the repetitive tasks and procedures, which have to be applied to each machine on the network. GFI LANguard N.S.S. automates the process of a security audit & easily identifies common vulnerabilities within your network in a short time.

Note: If your company runs any type of Intrusion Detection Software (IDS) then be aware that the use of LANguard Network Security Scanner will set off almost every bell and whistle in it. If you are not the one in charge of the IDS system, make sure that the administrator of that box or boxes is aware of the scan that is about to be run.

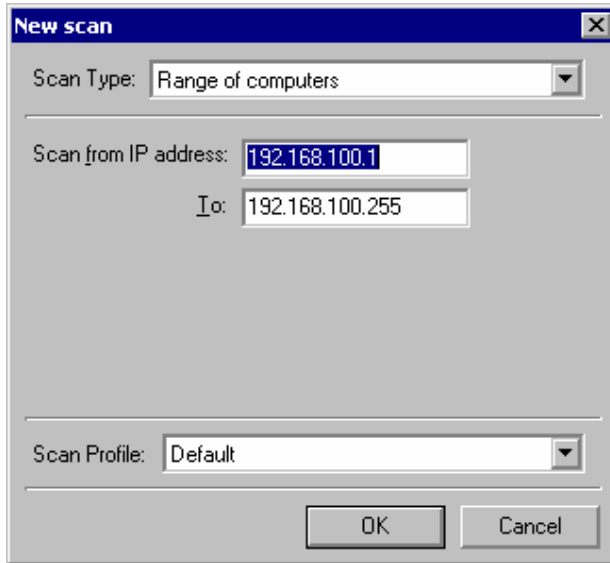
Along with the warning of IDS software be aware that a lot of the scans will show up in log files across the board. Unix logs, web servers, etc. will all show the attempt from the machine running LANguard Network Security Scanner. If you are not the sole administrator at your site make sure that the other administrators are aware of the scans you are about to run.

Performing a Scan

The first step in beginning an audit of a network is to perform a scan of current network machines and devices.

To begin a new network scan:

1. Click on **File > New**.
2. Select what to scan. You can select the following:
 - a. Scan one Computer - This will scan a single machine.
 - b. Scan Range of Computers – This will scan a specific range of IP's
 - c. Scan List of Computers – This scans a custom list of computers. Computers can be added to the list by selecting them from a list of enumerated computers, by entering them one by one, or by importing the list from a text file.
 - d. Scan a Domain – This scans an entire windows domain.
3. Depending on what you want to scan input the starting and ending range of the network to be scanned.
4. Select **Start Scan**.



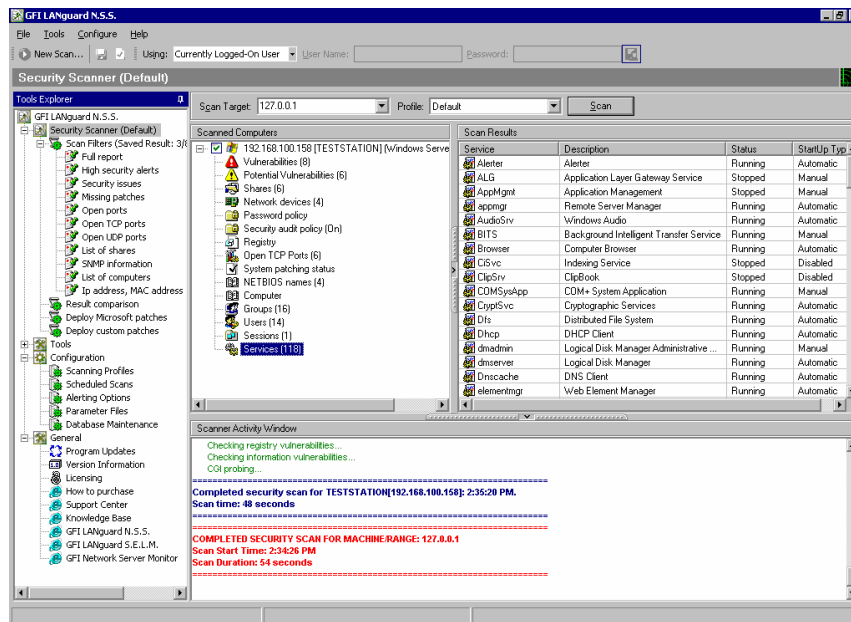
Performing a scan

LANguard Network Security Scanner will now perform a scan. It will first detect which hosts/computers are on, and only scan those. This is done using NETBIOS probes, ICMP ping and SNMP queries.

If a device does not answer to one of these GFI LANguard N.S.S. will assume, for now, that the device either does not exist at a specific IP address or that it is currently turned off.

Note: If you want to force a scan on lmps that do not respond, see the chapter 'Configuring scan options' for information how to configure this.

Analyzing the Scan Results



Analyzing the results

After a scan, nodes will appear under each machine that GFI LANguard N.S.S. finds. The left pane will list all the machines and network devices. Expanding one of these will list a series of nodes with the information found for that machine or network device. Clicking on a particular node will display the scanned information in the right pane.

GFI LANguard N.S.S. will find any network device that is currently turned on when doing a network probe. Depending on the type of device and what type of queries it responds to will determine how GFI LANguard N.S.S. identifies it and what information it can retrieve.

Once GFI LANguard N.S.S. has finished its scan of the machine/device/network it will display the following information.

IP, Machine name, OS and Service pack Level

The IP address of the machine/device will be shown. Then the NetBIOS DNS name will be shown, depending on the type of device. GFI LANguard N.S.S. will report what OS is running on the device and if it is a Windows NT/2000/XP/2003 OS, it will show the service pack level.

Vulnerabilities Node

The vulnerabilities node displays detected security issues and informs you how to fix them. These threats can include missing patches and service packs, HTTP issues, NETBIOS alerts, configuration problems and so on.

Vulnerabilities are broken down into the following sections: Missing Service Packs, Missing Patches, High security vulnerabilities, Medium security vulnerabilities and Low security vulnerabilities.

Under each of the High / Medium / Low vulnerabilities sections you can find further categorization of the issues detected using the following grouping: CGI Abuses, FTP Vulnerabilities, DNS Vulnerabilities, Mail Vulnerabilities, RPC Vulnerabilities, Service Vulnerabilities, Registry Vulnerabilities and Miscellaneous Vulnerabilities.

Missing patches GFI LANguard N.S.S. checks for missing patches by comparing installed patches with the available patches for a particular product. If the machine is missing any patches you should see something like this:



First it tells you what product the patch is for. If you expand that, it will tell you the specific patch that is missing and give you a link to where you can download that specific patch.

CGI Abuses describe issues related to Apache, Netscape, IIS and other web servers.

FTP vulnerabilities, DNS vulnerabilities, Mail vulnerabilities, RPC vulnerabilities, and Miscellaneous vulnerabilities provide links to Bugtraq or other security sites so that you can lookup more information about the problem GFI LANguard N.S.S. found.

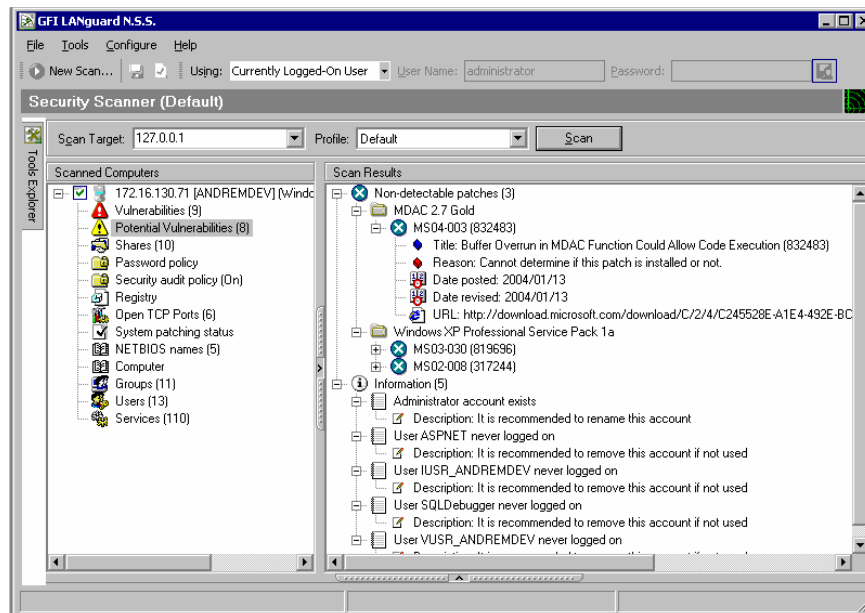
Service vulnerabilities can be a number of things. Anything from actual services running on the device in question to accounts listed on a machine that have never been used.

Registry vulnerabilities cover information pulled from a Windows machine when GFI LANguard N.S.S. does its initial scan. It will provide a link to Microsoft's site or other security related sites that explain why these registry settings should be changed.

Information vulnerabilities are alerts added to the database that are issues important enough to be brought to the administrators' attention, but not always damaging to leave open.

Potential Vulnerabilities Node

The potential vulnerabilities node displays potential security issues, important information, as well as certain checks that could not be performed. For example if it could not be determined that a particular patch is installed, it will be listed under the Non-detectable patches node. These potential vulnerabilities need to be reviewed by the administrator.



Potential vulnerabilities node

Shares

The shares node lists all shares on a machine and who has access to a share. All network shares must be properly secured. Administrators should make sure that:

1. No user is sharing his/her whole drive with other users.
2. Anonymous/unauthenticated access to shares is not allowed.
3. Startup folders or similar system files are not shared. This could allow less privileged users to execute code on target machines.

The above is very important for all machines, but especially for machines that are critical to system integrity, such as the Public Domain Controller. Imagine an administrator sharing the startup folder (or a folder containing the startup folder) on the PDC to all users. Given the right permissions, users can then easily copy executables into the startup folder, which will be executed upon the next interactive logon by the administrator.

Note: If you are running the scan logged in as an administrator, you will also see the administrative shares, for example "C\$ - default share". These shares will not be available to normal users.

With the way Klez and other new viruses are starting to spread, through the use of open shares, all unneeded shares should be turned off, and all needed shares should have a password on them.

Password Policy

This node allows you to check if the password policy is secure. For example enable a maximum password age and password history. Minimum password length should be something practical, such as 8 characters. If you have Windows 2000, you can enable a secure password policy, network wide, using a GPO (Group Policy Objects) in Active Directory.

Registry

This node gives vital information about the remote registry. Click on the Run node to check what programs automatically launch at startup.

Check that the programs that automatically launched are not Trojans or even valid programs that provide remote access into a machine if such software is not allowed on your network. Any type of Remote Access software can end up being a backdoor that a potential hacker can use to gain entrance.

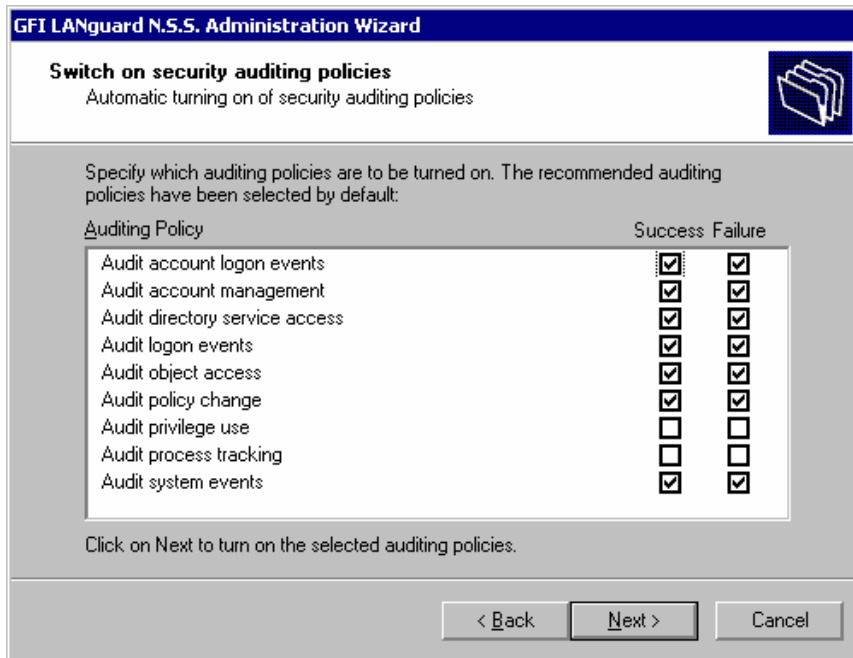
Security audit policy

This node shows which security auditing policies are enabled on the remote machine. The following auditing policies are recommended:

Auditing Policy	Success	Failure
Account logon events	Yes	Yes
Account management	Yes	Yes
Directory service access	Yes	Yes
Logon events	Yes	Yes
Object access	Yes	Yes
Policy change	Yes	Yes
Privilege use	No	No
Process tracking	No	No
System events	Yes	Yes

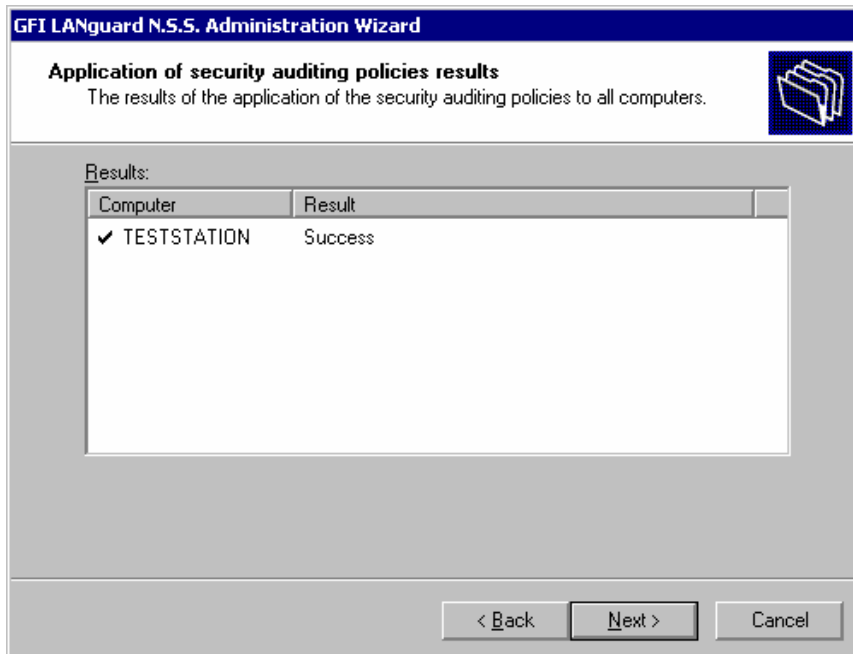
You can enable auditing directly from GFI LANguard N.S.S. Right click on one of the computers in the left pane and select "Enable auditing". This will bring up a the auditing policy administration wizard.

Specify which auditing policies to turn on. There are 7 security auditing policies in Windows NT and 9 security auditing policies in windows 2000. Enable the desired auditing policies on the computers to be monitored. Click on Next to turn on the auditing policies.



Enabling Audit Policies on remote machines.

If no errors are encountered, the finish page will be displayed. If an error has occurred then another page will be displayed indicating the computers on which the application of the policies failed.



Results dialog in audit policy wizard

Open Ports

The open ports node lists all open ports found on the machine. (This is called a port scan). GFI LANguard N.S.S. does a selective port scan, meaning it does not by default scan all 65535 TCP and 65535 UDP ports, just the ports it is configured to scan for. You can configure the ports it should scan for from Scan options. For more information see the chapter *“Configuring Scan Options, Configuring Ports to Scan”*.

Each open port represents a service/application; if one of these services can be 'exploited', the hacker could gain access to that machine. Therefore, it's important to close any port that is not needed.

Note: On Windows Networks, ports 135, 139 & 445 are always open.

GFI LANguard N.S.S. will show open ports, and if the port is considered a known Trojan port, GFI LANguard N.S.S. will display it in RED, otherwise the port will show up in GREEN. You can see this in the following screen shot:

```

+-----+
| 5000 [ UPnP => Universal Plug and Play ]
| 8080 [ Http-Proxy ]
| 12345 [ Netbus ]
| 27374 [ Subseven ]
+-----+
```

Note: Even if a port shows up in RED as a possible Trojan port, that does not mean that that a backdoor program is actually installed on the machine. Some valid programs will use the same ports as some known Trojans. One antivirus program uses the same known port as the NetBus Backdoor. So always check the banner information provided and run checks on these machines.

Users & Groups

These nodes show the local groups and the local users available on the computer. Check for extra user accounts, and verify that the Guest account is disabled. Rogue users and groups can allow backdoor access!

Some backdoor programs will re-enable the Guest account and grant it Administrative rights, so check the details of the users node to see the activity of all the accounts and the rights they have.

Ideally the user should not be using a local account to logon, but should be logging into a Domain or an Active Directory account.

The last main thing to check is to ensure that the password is not too old.

Services

All the services on the machine are listed. Verify that the services running need to be and disable all services that are not required. Be aware that each service can potentially be a security risk and a hole into the system. By closing or switching off services that are not needed security risks are automatically reduced.

System Patching status

This node shows what patches are installed and registered on the remote machine.

Additional Results

This section list additional nodes and results, which you can look at after you have reviewed the more important scan results above.

NETBIOS names

In this node you will find details about the services installed on the machine.

Computer

MAC - This is the Network card MAC address.

Username - This is the username of the currently logged on user, or the machine username.

TTL - The value of Time To Live (TTL) is specific to each device. Main values are 32, 64, 128, and 255. Based on these values and the actual TTL on the packet it gives you an idea of the distance (number of router hops) between the GFI LANguard N.S.S. machine and the target machine that was just scanned.

Computer Usage - Tells you whether the target machine is a Workstation or a Server.

Domain - If the target machine is part of a domain, this will give you a list of the trusted Domain(s).

If it is not part of a Domain it will display the Workgroup the machine is part of.

LAN manager - Gives the LAN Manager in use (and OS).

Sessions

Displays the IP address of machines that were connected to the target machine at the time of the scan. In most cases, this will just be the machine that is running GFI LANguard N.S.S. and has recently made connections.

Note: Due to the constant changing of this value, this information is not saved to the report, but is here for informational purposes only.

Network Devices

Provides a list of network devices available on the target machine.

Remote TOD

Remote Time of the Day. This is the network time on the target machine, which is usually set by the Domain Controller.

Performing On site and Off site scans

We recommend that you run GFI LANguard N.S.S. in 2 ways, the so called On site scans and off site scans.

On Site Scan

Setup a machine with LANguard Network Security Scanner installed on it. Do a scan of your network with a 'NULL session' (Select **Null Session** from the using drop down box).

Once this first scan is done change the using drop down box value to **Currently logged on user** (if you have administrative rights to your domain), or as **Alternative credentials** that have administrative rights to the Domain or to Active Directory.

Save this second scan for comparison later on.

With the 'NULL session' you can see what any user making a connection to your network via a Null connection would be able to see. The scan that has administrative rights, will help show you all of the hot fixes and patches that are missing on the machine.

Off Site Scan

If you have an outside dialup account, or high speed internet access that is not tied to your company you will now want to turn around and scan your network from the outside world.

Do a 'NULL session' scan of your network. This will let you see what anyone from the Internet would be able to see if/when they scan your network. Things that may effect this are any firewalls your company or ISP may have setup, or any rules at a router along the way that may drop specific types of packets.

Save this scan for later comparison.

Comparison of on site and off site scans

Now it is time to start looking at the information generated by LANguard Network Security Scanner.

If the NULL session scan from your internal network looks identical to that of your external scan be aware that it appears there is no firewall or filtering device on your network. This is probably one of the first things that you should look into.

Then, check to see what any user from the outside world can really see. Can they see your Domain Controllers and get a list of all computer accounts?

What about Web servers, FTP, etc...?

At this point, you are on your own. You may need to start checking for patches for Web Servers, FTP Servers, etc. You may also need to verify and change settings on SMTP servers. Every network is different. GFI LANguard N.S.S. tries to help you pinpoint problems and security concerns and lead you to sites that will help you fix the holes it finds.

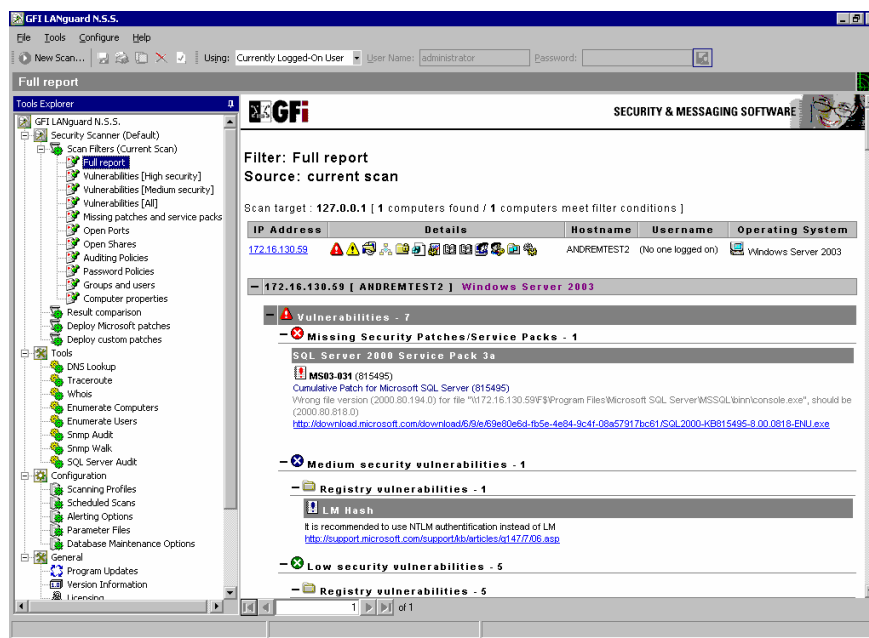
If you find services running that are not needed, make sure you turn them off. Every service is a potential security risk that may allow someone unauthorized into your network. There are new buffer overflows and exploits being released daily and even though your network may look and be secure today, that may not be the case tomorrow.

Make sure you run security scans from time to time. This isn't something you can do once and then forget about it. Something new is always out there, and once again, just because you were safe and secure today, you never know what tomorrow's hacker will come up with.

Filtering scan results

Introduction

After GFI LANguard N.S.S. has performed a scan, it will show the results in the 'Scan results' pane. If you have scanned a large number of machines, you might want to filter that data from the Scan filters node. Clicking on this node and selecting an existing filter will show the scan results based on what filter you selected. GFI LANguard N.S.S. ships with a number of default scan filters. In addition you can make your own custom scan filters.



Scan filters

The following scan filters are included by default:

Full report: Shows all security related data collected in a scan.

Vulnerabilities [High Security]: Shows issues which require immediate attention – missing service packs, missing patches, high security vulnerabilities and open ports.

Vulnerabilities [Medium Security]: Shows issues which may need to be addressed by the administrator – medium security vulnerabilities, patches which cannot be detected.

Vulnerabilities[All]: Shows all vulnerabilities detected – missing patches, missing service packs, potential information checks, patches which could not be detected, low & high security vulnerabilities.

Missing patches and service packs: lists all missing service packs and patch files on the machines scanned.

Open Ports: lists all open TCP and UDP ports.

Open Shares: lists all open shares and who has access to them.

Auditing Policies: lists the auditing policy settings on each of the scanned computers.

Password Policies: lists the active password policies on each of the scanned computers.

Groups and users: lists the users and groups detected on each of the scanned computers.

Computer properties: Shows the properties of each computer

Selecting the scan results source

By default, the filters will work on the current scan data. However it is possible to select a different 'scan results' data source file and apply the filters to this saved scan results data source file (which is actually an XML file). To do this:

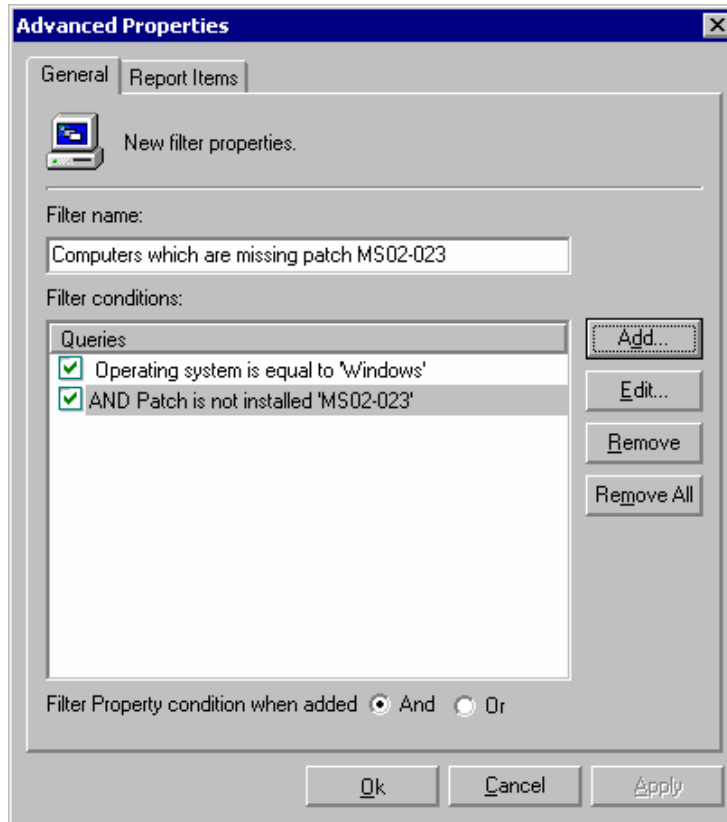
1. Go to the Scan filters node in the GFI LANguard N.S.S. security scanner program
2. Right click and select 'Filter saved scan results XML file...'
3. Select the XML file containing the scan results data.
4. All filters will now show data from this scan results file. Next to the Scan Filters node the scan data source will be shown: Either current scan data or the file name of the scan results you are filtering from.

NOTE: If the data source for the scan filters is set to "Current Scan", there will be no results shown until a scan is made.

Creating a custom scan filter

To create a custom scan filter:

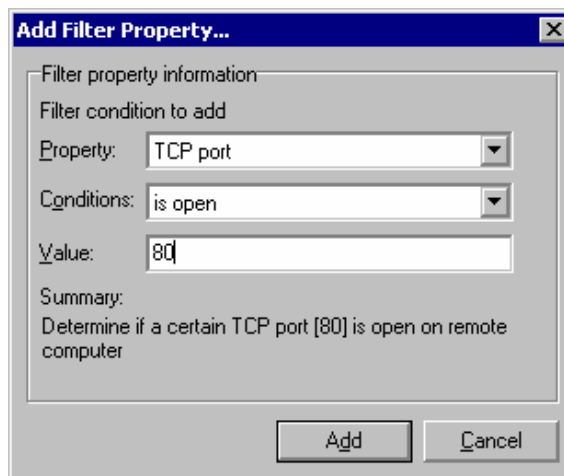
1. Right click on the GFI LANguard N.S.S. > Security scanner > Scan Filters node and select New > Filter...
2. This will bring up the Scan Filter Properties dialog.



Scan Filters – General page

3. Give the scan filter a name

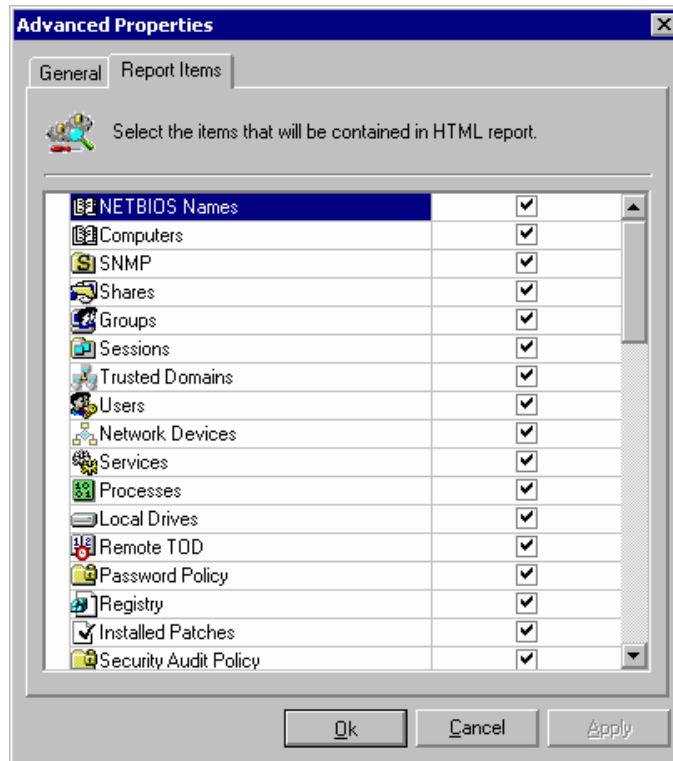
4. Add any conditions that you want to filter to apply to the scan results data using the Add... button. You can create multiple conditions for the filter. For each condition you must specify the property, the condition and the value. Available properties are Operating System, hostname, logged on user, domain, service pack, share etc.).



Conditions dialog

5. Select which categories of information you want to see in the filter from the 'Report Items' page.

6. Click on ok to create the filter.



Scan Filters - Report items page

This procedure will create a new permanent node under the Scan Filters node.

NOTE : You can delete/customize any filter under the Scan Filters node by right clicking on the filter and selecting Delete.../Properties depending on the operation you want to perform.

Example 1 – Find computers with a particular missing patch

You want to find all Windows computers missing MS03-026 patch. (this is the famous blaster virus patch)

Define the filter as follows:

1. Condition 1: Operating system includes **Windows**
2. Condition 2: Hot fix (patch) is not installed **MS03-026**

Example 2 – List all Sun stations with a web server

To list all Sun stations running a web server on port 80 define the following queries:

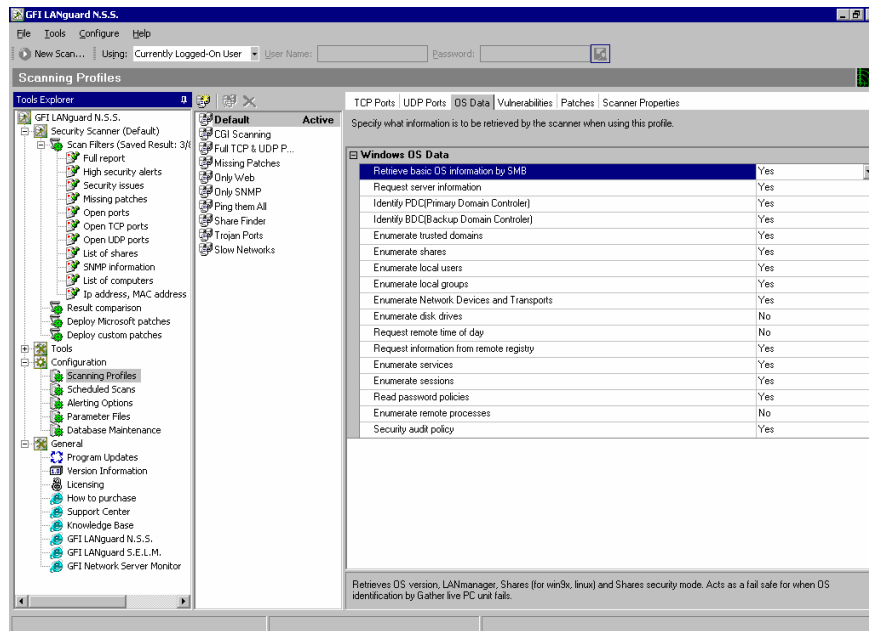
1. Operating system includes **SunOS**
2. TCP port is open **80**

Configuring GFI LANguard N.S.S.

Introduction to configuring GFI LANguard N.S.S.

You can configure GFI LANguard N.S.S. from the configuration node. Here you can configure scan options, scanning profiles with different scanning options, scheduled scans, alerting options and more.

Scanning profiles



Scanning profiles

Using scanning profiles, you can configure different types of scans, and use these different scans to focus on particular types of information that you want to check for.

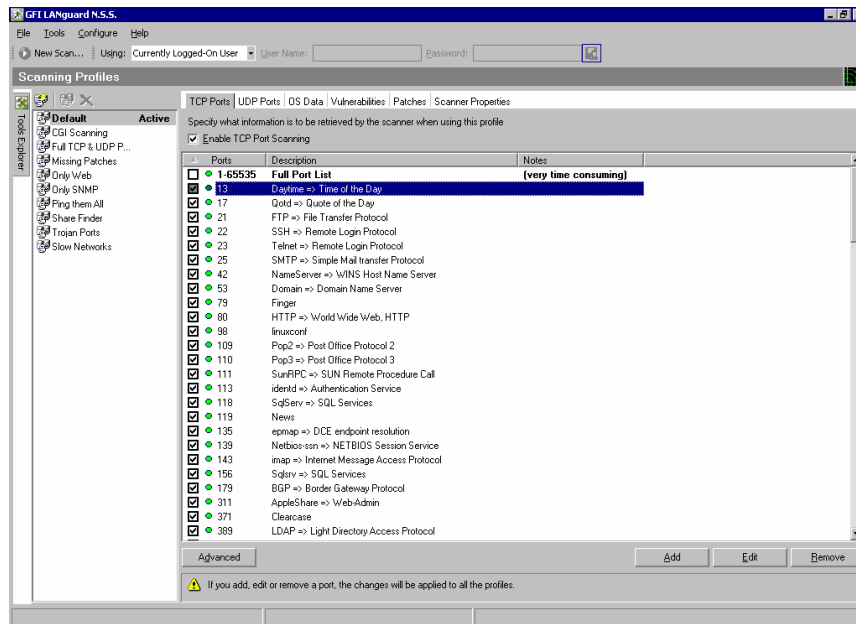
A scan profile is created by going to the Configuration > Scanning profiles node right-clicking and selecting New > Scan Profile...

You can configure the following options for each profile:

1. Scanned TCP ports
2. Scanned UDP ports
3. Scanned OS data
4. Scanned Vulnerabilities
5. Scanned Patches
6. Scanner properties

Scanned TCP/UDP ports

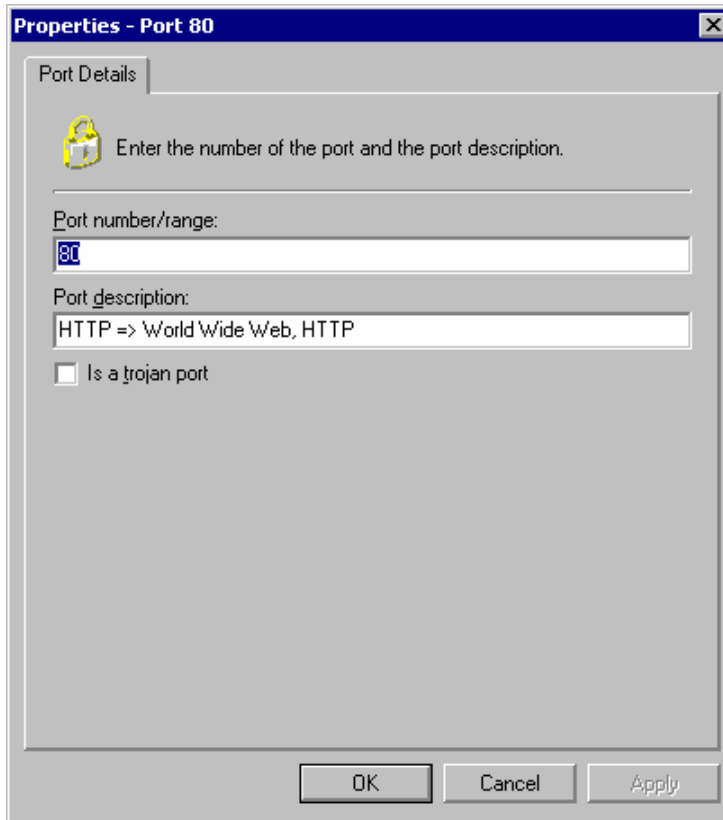
The scanned TCP/UDP ports tabs allow you to specify which TCP and UDP ports you wish to scan. To enable a port simply click on the tick box next to the port.



Configuring the ports to scan in a profile

How to add/edit/remove ports

If you want to add custom TCP/UDP ports, click the add button. The Add port dialog will appear.



Screenshot 1 - Adding a port

Simply enter a port number or a port range and enter a description of the program which is supposed to run on that port. If the program associated with this port is a Trojan, click on the 'Is a Trojan port' check box.

If you specify it is a Trojan port, the green / red circle next to the port will be red

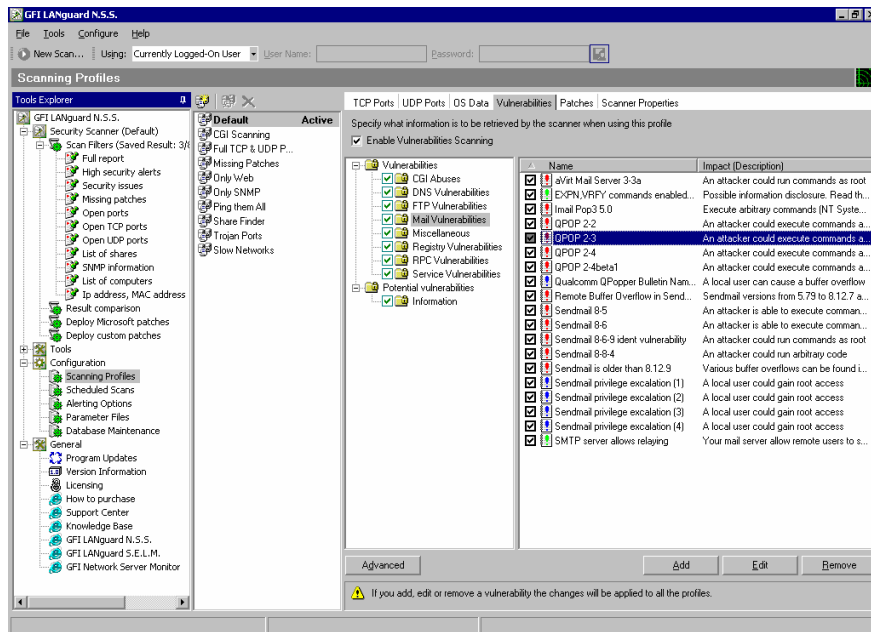
Note: Make sure you are inputting this port in the correct Protocol Window, either TCP or UDP.

You can edit or remove ports by clicking on the Edit or remove buttons

Scanned OS data

The Scanned OS data tab specifies the kind of information you want GFI LANguard N.S.S. to collect from the operating system during the scan. Currently only Windows OS data is supported, however UNIX scan data is under development.

Scanned Vulnerabilities



Configuring the Vulnerabilities to scan

The scanned vulnerabilities tab lists all vulnerabilities that GFI LANguard N.S.S. can scan for. You can disable checking for all vulnerabilities by de-selecting the 'Check for vulnerabilities' check box.

By default, GFI LANguard N.S.S. will scan for all vulnerabilities it knows. You can change this by removing the check box next to a particular vulnerability.

From the right pane, you can change the options of a specific vulnerability by double clicking on it. You can change the security level of a particular vulnerability check from the "Security Level" option.

Types of Vulnerabilities

Vulnerabilities are broken down into the following sections: Missing Patches, Patches which cannot be detected, CGI Abuses, FTP Vulnerabilities, DNS Vulnerabilities, Mail Vulnerabilities, RPC Vulnerabilities, Service Vulnerabilities, Registry Vulnerabilities, and Miscellaneous Vulnerabilities.

Vulnerability checks advanced options

Click on the advanced button to bring up these options.

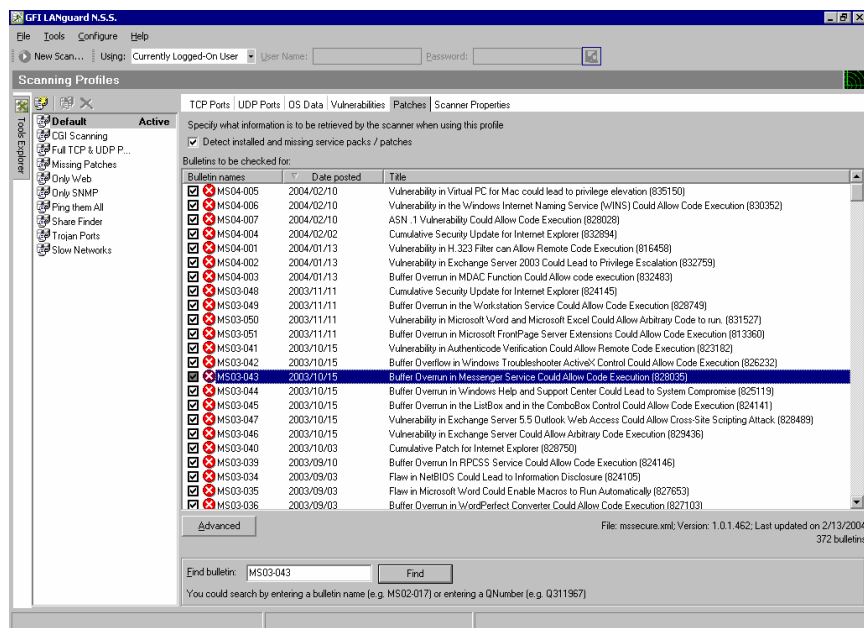
- **Internal Checks** - These include ftp anonymous password checks, weak password check etc..
- **CGI Probing** - Switch on CGI probing if you are running web servers that use CGI. You can optionally specify a proxy server if you are located behind a proxy server.
- **New vulnerabilities are enabled by default** – Enables/Disables newly added vulnerabilities to be included in the scans of all other profiles.

Downloading the latest Security Vulnerabilities

To update your Security Vulnerabilities, select Help > Check for updates from the GFI LANguard N.S.S. scanner program. This will download the latest security vulnerabilities from the GFI website. This will also update the fingerprint files used to determine what OS is on a device.

NOTE : On startup GFI LANguard N.S.S. can automatically download new vulnerability checks from the GFI website. You can configure this from the GFI LANguard N.S.S. > General > Product Updates node.

Scanned Patches

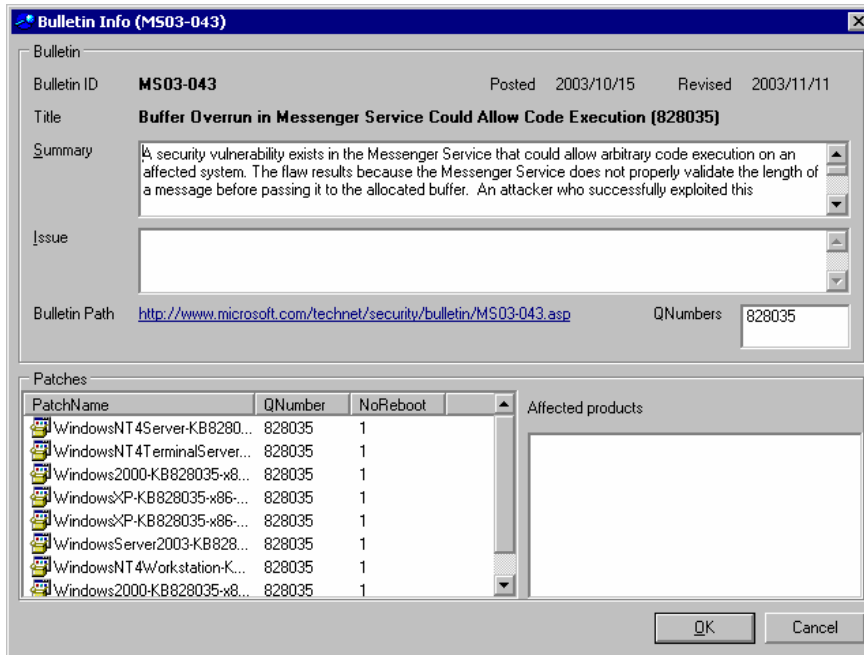


Configure which patches to check for when scanning with a particular profile.

The scanned patches tab allows you to configure whether this particular scan profile should check for missing patches and/or service packs.

The tab lists all the patches that GFI LANguard N.S.S. checks for. You can disable checking for particular patches for this profile by unchecking the tick box next to the patch bulletin.

The list of patches is obtained by downloading the latest patch list from the GFI website, which in turn is obtained from Microsoft (mssecure.xml). GFI obtains the list of patches of Microsoft and checks it for correctness, since sometimes it contains errors.

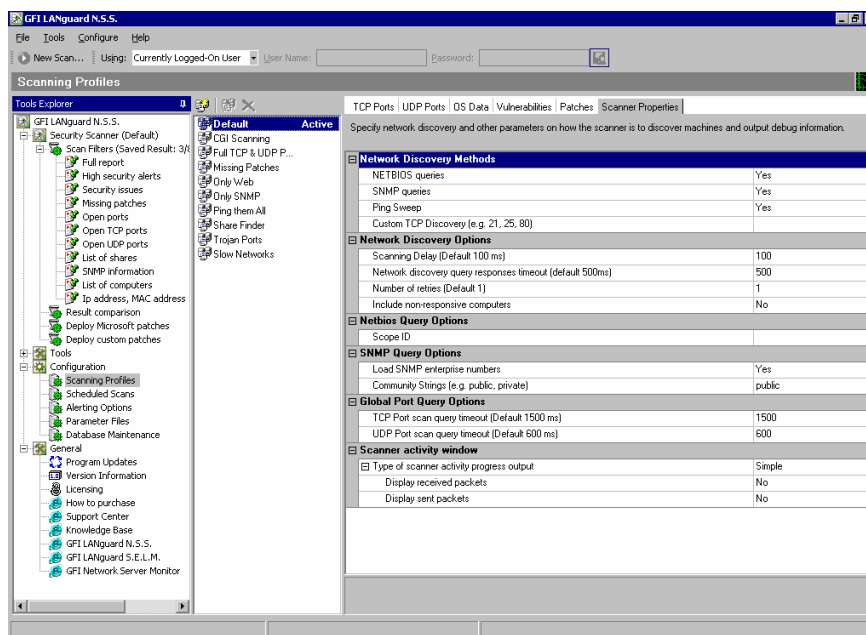


Extended bulletin information

For more information on a particular bulletin, double click on an the bulletin or right click on it and select Properties. You will be presented with more details on what the bulletin checks for and what it addresses.

Scanner options

In this tab you can configure options relating to how GFI LANguard N.S.S. should perform a scan.



Security Scanner properties

Network discovery methods

This section addresses which methods GFI LANguard N.S.S. is to use to discover machines over the network.

The **NETBIOS queries** option allows NetBIOS or SMB queries to be used. If the Client for Microsoft Networks is installed on the Windows Machine, or if Samba Services are installed on a Unix machine, then those machines will answer the NetBIOS type query.

You can add a ScopeID to the NetBIOS Query. This is only required in some cases, in which systems have a ScopeID. If your organization has a ScopeID set on NetBIOS, input it here.

The **SNMP queries** option will allow SNMP packets to be sent out with the Community String that was set in the General tab. If the device responds to this query, GFI LANguard N.S.S. will request the Object Identifier from the device and compares that to a database to determine what that device is.

Ping Sweep does an ICMP ping of each network device. (See **Note:** below)

Custom TCP Port Discovery checks for a particular open port on the target machines.

Note: Each of the above query types can be turned off, but GFI LANguard N.S.S. depends on all these queries to determine the type of device and the OS running on it. If you choose to turn any one of these off, GFI LANguard N.S.S. may not be as reliable in its identification.

Note: Some personal firewalls block a machine from even sending out an ICMP echo and will therefore not be detected by GFI LANguard N.S.S. If you think there are many machines with personal firewalls on your network, consider forcing a scan of each IP on your network.

Network discovery options

The network discovery parameters allow you to tweak machine detection, so that you have the most reliable machine detection in the least time possible. Adjustable parameters include

- **Scanning Delay** is the time LANguard N.S.S. waits between TCP/UDP packets it sends out. The default is 100 ms. Depending on your network connection and the type of network you are on (LAN/WAN/MAN) you may need to adjust these settings. If it is set too low you may find your network congested with packets from GFI LANguard N.S.S. If you set it too high a lot of time will be wasted that is not needed.
- **Wait for Responses** is the time GFI LANguard N.S.S. will actually wait for a response from the device. If you are running on a slow or busy network you may need to increase this timeout feature from 500 ms to something higher.
- **Number of retries** is the number of times that GFI LANguard N.S.S. will do each type of scan. During normal circumstances this setting should not be changed. Be aware, however, that if you do change this setting, it will run through each type of scan (NETBIOS, SNMP, and ICMP) that number of times.

- **Include non-responsive computers** is an option which instructs the GFI LANguard N.S.S. security scanner to try to scan a machine which has not replied to any network discovery method.

NetBIOS Query Options

The effect of using a NetBIOS Scope ID is to isolate a group of computers on the network that can communicate only with other computers that are configured with the identical NetBIOS Scope ID.

NetBIOS programs started on a computer using NetBIOS Scope ID cannot "see" (receive or send messages) to NetBIOS programs started by a process on a computer configured with a different NetBIOS Scope ID.

LNSS is supporting NETBIOS Scope ID in order to be able to scan this isolated computers that otherwise would be inaccessible.

SNMP Query Options

The option to **Load SNMP enterprise numbers** will allow GFI LANguard N.S.S. to extend support in SNMP scanning. If this is disabled, devices discovered by SNMP that are unknown to GFI LANguard N.S.S. will not report who the vendor is supposed to be. Unless you are running into problems, it is recommended to leave this option enabled.

By default most SNMP enabled devices use the default community string 'public', but for security reasons most administrators will change this to something else. If you have changed the default SNMP community name, on your network devices, you will want to add it to the list GFI LANguard N.S.S. uses.

Note: You can add more than one SNMP community name here. For each additional community name you add, the SNMP part of the scan will have to run another time. If you have 'public' and 'private' set in the community name string, the SNMP scan will run through the whole IP range you give it twice. It will go through it once with the string of 'public', and then again with the string of 'private'.

Scanner activity windows options

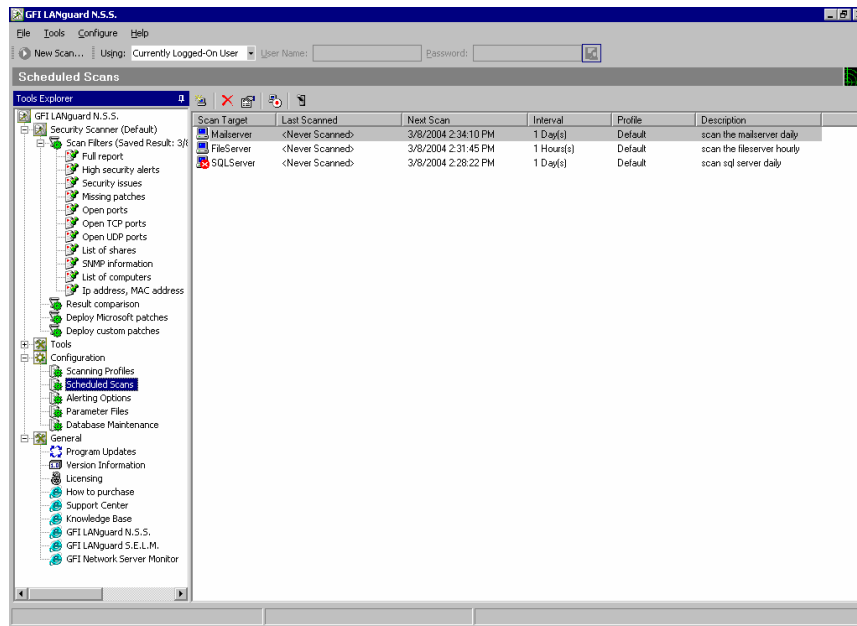
The output options allow you to configure what information will be displayed in the scanner activity pane. It is useful to enable it, however only enable 'Verbose' or the 'Display packets' for exceptional debugging purposes.

Scheduled Scans

The scheduled scan feature allows you to configure scans which will be run automatically at a specific date / time. Scheduled scans can also be run periodically. This allows you to run a particular scan at night or early in the morning and can be used in conjunction with the results comparison feature, allowing you to receive a 'change report' automatically in your mailbox.

By default all scheduled scans are stored in the database. Optionally you can save all scheduled scan results to an XML file (one per scheduled scan). This can be done by right clicking on the Scheduled

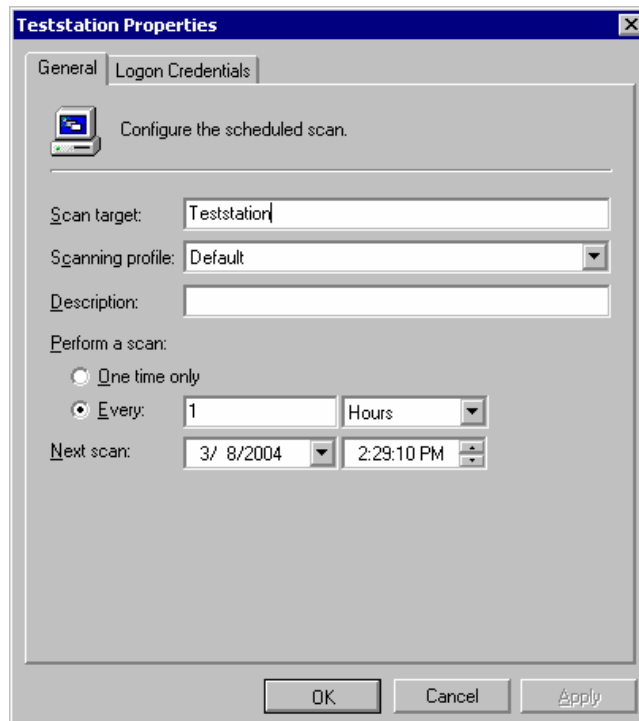
Scan node, selecting properties, enabling the Save Scheduled Scan option and specifying a path for the XML files.



Configuring a scheduled scan

To create a scheduled scan

1. In the GFI LANguard N.S.S. security scanner program, right-click on the Configuration > Scheduled scans > New > Scheduled scan...
2. This brings up the New Scheduled Scan dialog



Creating a new Scheduled Scan

In the New scheduled scan dialog you can configure:

1. Scan target: Specify the computer names or IP range that you wish to scan. You can specify the scan target as follows
 - i. Host name – e.g. ANDREMDEV
 - ii. IP address – e.g. 192.168.100.9
 - iii. Range of IP's – e.g. 192.168.100.1 – 192.168.100.255
 - iv. A text file with a list of computers - e.g. file:c:\test.txt (complete path to the file) Each line contained in the file can take any of the formats or targets specified in (1), (2) or (3).
 2. Scanning Profile : Select the scanning profile to be used for this scheduled scan.
 3. Next scan: Specify at what date and time you wish the scan to start
 4. Perform a scan every: Specify if you wish the scan to be run once or periodically.
 5. Description: This will show up in the scheduled scan list
- Click OK to create the scheduled scan.

To analyze/view the scan results of a scheduled scan, you must specify the scan results XML file of that scheduled scan in the scan filters node. To do this:

1. Right click on the “Scan Filters” main node and select “Filter saved scan results XML file...”
2. Specify the Scan results XML file of the scheduled scan.
3. The filter nodes will now display data from the scheduled scan results file.

Parameter files

The parameter files node provides a direct interface to edit various text based parameter files that GFI LANguard N.S.S. uses. Only advanced users should modify these files. If these files are edited wrongly, it will affect the reliability of GFI LANguard N.S.S. when determining the type of device it has found.

- Ethercodes.txt - this file contains a list of mac addresses and the associated vendor which has been assigned that particular range.
- ftp.txt – this file contains a list of ftp server banners that are used internally by LNSS to help identify what OS is running on that particular machine based on the ftp server running there.
- Identd.txt – this file contains identd banners that are also used internally by LNSS to identify the OS using banner information.
- Object_ids.txt – this file has SNMP object_ids and to which vendor and product they belong. When GFI LANguard N.S.S. finds a device that responds to SNMP queries it compares the Object ID information on the device to that stored in this file.
- Passwords.txt – this file has a list of passwords which are used to assert password weaknesses..
- Rpc.txt – this file contains a map between the service numbers returned by the rpc protocol and the service name associated with

that particular service number. When RPC services are found running on a machine (normally Unix or Linux) the information received back is compared to this file.

- Sntp.txt – contains a list of banners and the associated OS. As with the ftp and ident files, these banners are used internally by LNSS to identify the OS running on the target machine.
- Snmp-pass.txt – this file contains a list of community strings that LNSS uses to identify if they are available on the target SNMP server. If available, these community strings will be reported by the SNMP scanning tool.
- telnet.txt – Again, a file containing various telnet server banners used by LNSS to identify the OS running on the target machine.
- www.txt – A file contain web server banners used to identify what OS is running on the target machine.
- Enterprise_numbers.txt – list of OID (Object Identifier) to enterprise (vendor/university) relation codes. If GFI LANguard N.S.S. doesn't have the specific information on a device when it finds it (information provided by the object_ids.txt file), it will look at the vendor specific information returned and at least provide who the vendor is for the product it found. This information is based on SMI Network Management Private Enterprise Codes, which can be found at: <http://www.iana.org/assignments/enterprise-numbers>

Using GFI LANguard N.S.S. from the command line

It is possible to invoke the scanning process from the command line. This allows you to call the scanner from another application or simply on a scheduled basis with your own custom options.

Usage:

```
Insscmd <Target> [/profile=profileName] [/report=reportPath]
[/output=pathToXmlFile] [/user=username /password=password]
[/email=emailAddress] [/DontShowStatus] [/?]
```

Legend:

/Profile Optional : Profile to use for scanning. If not specified, the current active profile will be used.

/Output Optional : Full path (including filename) where to output the scan result xml file.

/Report Optional : Full path (including filename) where to generate the output scan report html file.

/User Optional : Scan the specified target using the alternative credentials specified in the /User and /Password parameters.

/Password Optional : Scan the specified target using the alternative credentials specified in the /User and /Password parameters.

/Email Optional : Send the resulting report to this alternative email address. The mailserver specified in the LNSS\Configuration\Alerting Options node will be used.

/DontShowStatus Optional : Do not show scan progress details.

NOTE : For full paths, and profile names, enclose the name in inverted commas e.g. "Default", "c:\temp\test.xml".

Example:

```
Insscmd.exe 127.0.0.1 /Profile="Default" /Output="c:\out.xml"  
/Report="c:\result.html" /email="Inss@127.0.0.1"
```

The above will make the command line scanner perform a security scan on the machine 127.0.0.1, output the xml file to c:\out.xml, once the scan is complete generate the html report in c:\result.html and send the report to the email address Inss@127.0.0.1

Patch Deployment

Introduction to patch deployment

Use the patch deployment tool to keep your Windows NT, 2000, XP and 2003 machines up to date with the latest security patches and service packs. To deploy patches and services packs, you need to follow these steps

Step 1: Perform a scan of your network

Step 2: Select on which machines to deploy the patches

Step 3: Select which patches to deploy

Step 4: Download the patch & service pack files

Step 5: Patch file deployment parameters

Step 6: Deploy the updates

To deploy patches, you must have

- Administrative rights on the machine you are scanning.
- NETBIOS must be enabled on the remote machine.

The patch deployment agent

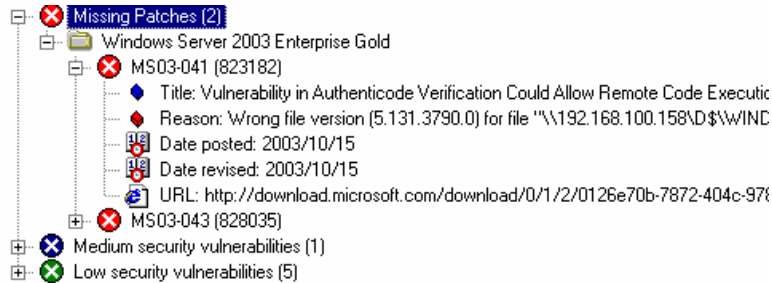
GFI LANguard N.S.S. 5 uses a patch deployment agent, which is installed silently on the remote machine, to deploy patches, services packs and custom software. The patch deployment agent consists of a service which will run the installation at a scheduled time depending on the deployment parameters indicated. This architecture is much more reliable than without using a patch deployment agent. The patch deployment agent is installed automatically without administrator intervention.

Note: It is not uncommon that Microsoft retires patch files. When this happens, the information of that patch remains in the mssecure.xml file, since the patch was available at some point. When this happens, GFI LANguard NSS will report the patch as missing, even though it can not be installed. If you do not want to be informed about these missing patches, you will need to disable checking for that particular bulletin from GFI LANguard N.S.S. > Configuration > Scanning Profiles > Patches.

Step 1: Perform a scan of your network

GFI LANguard N.S.S. discovers missing patches and service packs as part of the security scan. It does this by comparing registry settings, file date/time stamps, and version information on the remote machine. using information provided by Microsoft in the mssecure.xml file.

First GFI LANguard N.S.S. detects which products for which it has patch information are installed on the target machine (for example Microsoft Office). After it has done that, it checks what patches and service packs are available for that product and posts the missing patch information in the Missing patches node of the high security vulnerabilities node.

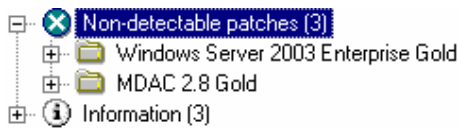


Missing patch sample output in scan results tree

For each missing service pack / patch GFI LANguard N.S.S. reports a link from where you can download the patch file as well as other information related to that bulletin.

Patches which are definitely missing are reported in the “Missing patches and service packs nodes” of the scan results.

Patches which cannot be confirmed whether they are installed or not due to lack of detection information are reported in the “Potential vulnerabilities node” of the scan results.



Non-detectable patches sample output in scan results tree

Step 2: Select on which machines to deploy the patches

After scanning the network, the list of missing service packs & patches will be listed in the scan results window. To deploy the missing updates you have to select which computers you want to update. Patches can be deployed on one machine, all machines, or on selected machines.

To deploy missing patches on one computer:

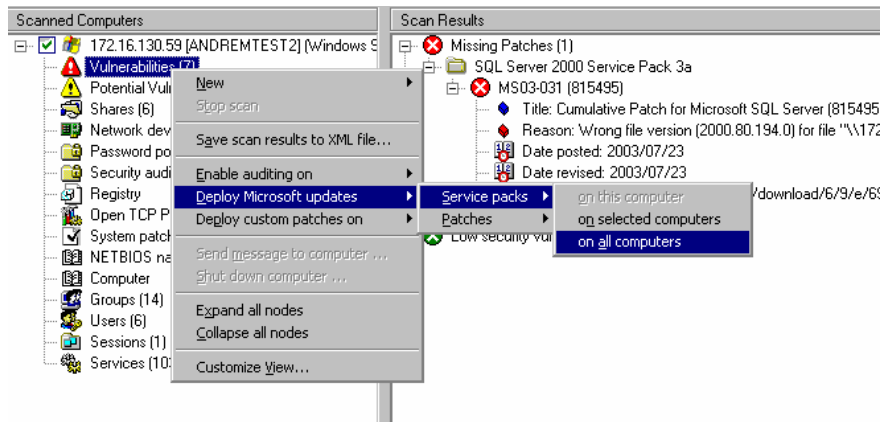
Right click on the computer you want to update > Deploy Microsoft updates > [type of update] > This computer.

To deploy missing patches on all computers:

Right click on any computer in the result tree > Deploy Microsoft updates > [type of update] > All computers.

To deploy missing patches on selected machines

Use the check boxes on the left hand side of the scan results to select which machines you want to update. Right click on any computer in the result tree > Deploy Microsoft updates > [type of update] > Selected Computers.



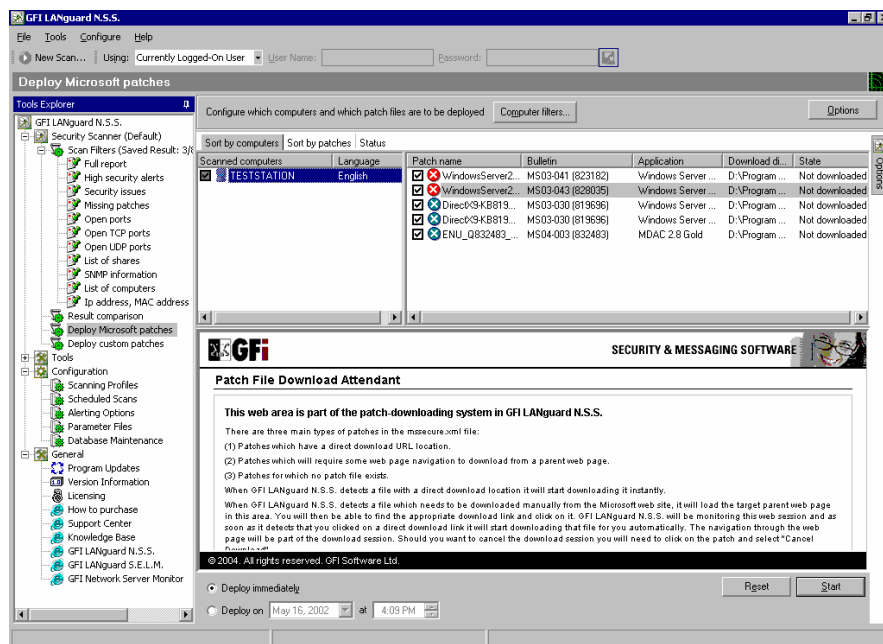
Indicate which machines you want to deploy the required updates on.

Step 3: Select which patches to deploy

Once you have selected the target computers to deploy Microsoft patches on, you will be taken to the Deploy Microsoft patches node. This node shows the details of the selected computers and which patches/service packs need to be deployed to those computers.

You have two views in which you can manage the deployment options.

- (1) Sort by computers: Select a computer and see which patches / updates need to be deployed to it
- (2) Sort by patches: Select a patch and see which computers are missing that update.







Deploy Microsoft patches node

By default all patches will be selected for deployment. If you want certain patches not to be deployed, de-select them by clicking on the tick box next to the patch.





Step 4: Download the patch & service pack files

After you have selected the patches/service packs to be deployed, the appropriate files containing the patches to be deployed need to be downloaded. This is done largely automatically by GFI LANguard N.S.S. and it also places them in the correct directories depending on the product and the language of the product being updated.

Patch name	Bulletin	Application	Download directory	State
<input checked="" type="checkbox"/>  SQL2000-KB815495-8.00.0818-ENU.exe	MS03-031 (815495)	SQL Server 2000 S...	F:\Inss\Repository...	Not downloaded
<input checked="" type="checkbox"/>  DirectX9-KB819696-x86-ENU.exe	MS03-030 (819696)	Windows Server 20...	F:\Inss\Repository...	Not downloaded
<input checked="" type="checkbox"/>  DirectX9-KB819696-x86-ENU.exe	MS03-030 (819696)	Windows Server 20...	F:\Inss\Repository...	Not downloaded
<input checked="" type="checkbox"/>  ENU_0832483_MDAC_x86.exe	MS04-003 (832483)	MDAC 2.8 Gold	F:\Inss\Repository...	Downloaded

GFI LANguard NSS shows which patch files need to be downloaded

GFI LANguard N.S.S. will show which files need to be downloaded in the patches to be deployed list. Each patch file required will be listed and will be in one of the following states, indicated by an icon in the missing patch list:

-  Downloaded
-  Currently being downloaded
-  Waiting for user to navigate to the web page to click on the link to download the file.
-  Not downloaded

Downloading the patches

Microsoft patches, listed in the mssecure.xml file, can be categorized in three main types:

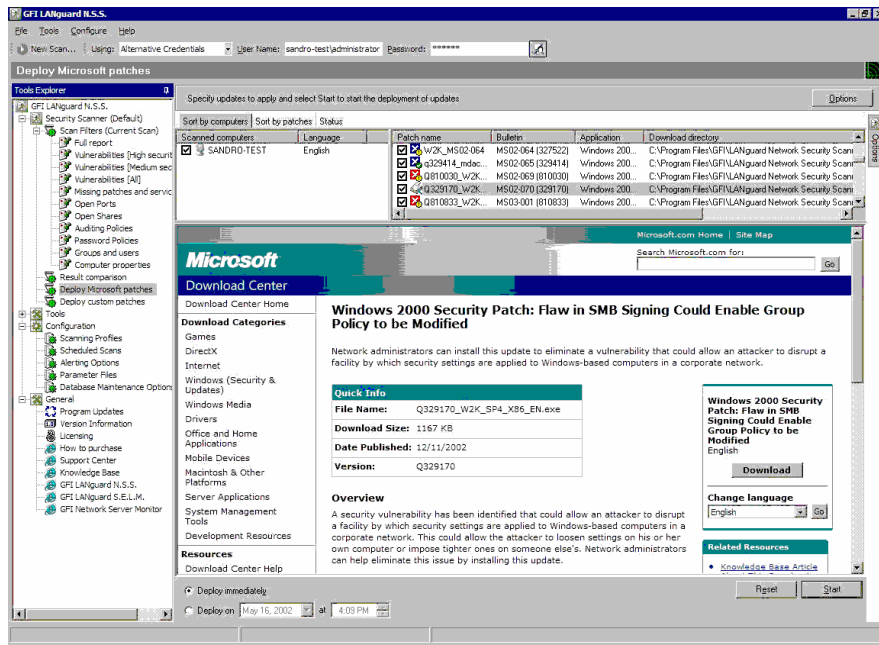
- (1) Patches which have a direct download URL location.
- (2) Patches which will require some web page navigation to download the file.
- (3) Patches for which no patch file exists.

To download patches for which there is a direct link:

For patches for which there is a direct download link, right click on the patch file and select "Download File". The download will start and when completed, the file will be placed in the correct directory for you.

To download patches for which there is no download link but only a source web page.

When GFI LANguard N.S.S. detects a file which needs to be downloaded manually from the Microsoft web site, it will load the target parent web page in the bottom area of the deployment tool. You will then be able to find the appropriate download link and click on it. GFI LANguard N.S.S. will be monitoring this web session and as soon as it detects that you clicked on a direct download link it will start downloading that file for you automatically. The navigation through the web page will be part of the download session. Should you want to cancel the download session you will need to click on the patch and select "Cancel Download". Once the download completes, the file will be placed in the correct directory for you.



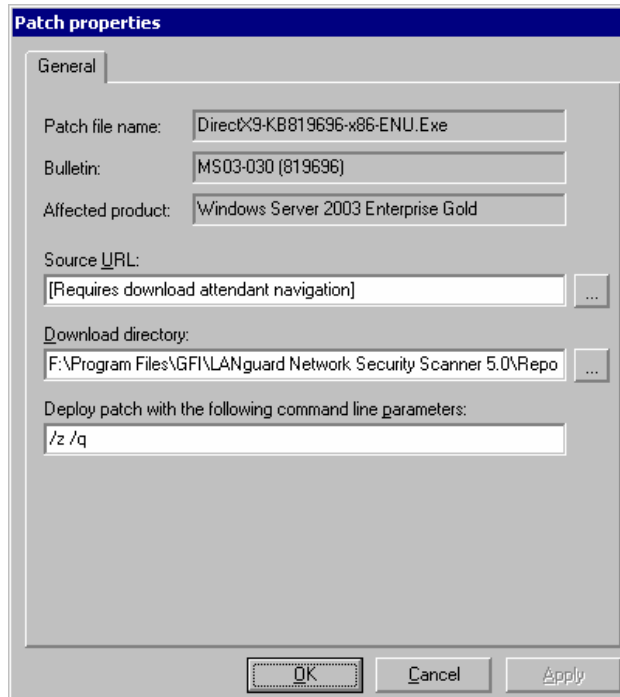
Downloading a patch from a web page with the download assistant.

Step 5: Patch file deployment parameters

Optionally, you can configure alternative deployment parameters on a patch by patch basis. To do this:

1. Right click on the patch file and select “Properties”.
2. Optionally specify an alternative download source URL
3. Optionally specify command line parameters to use during deployment

You can check to which bulletin a patch applies by right-clicking on the patch file and selecting “Bulletin Info...”

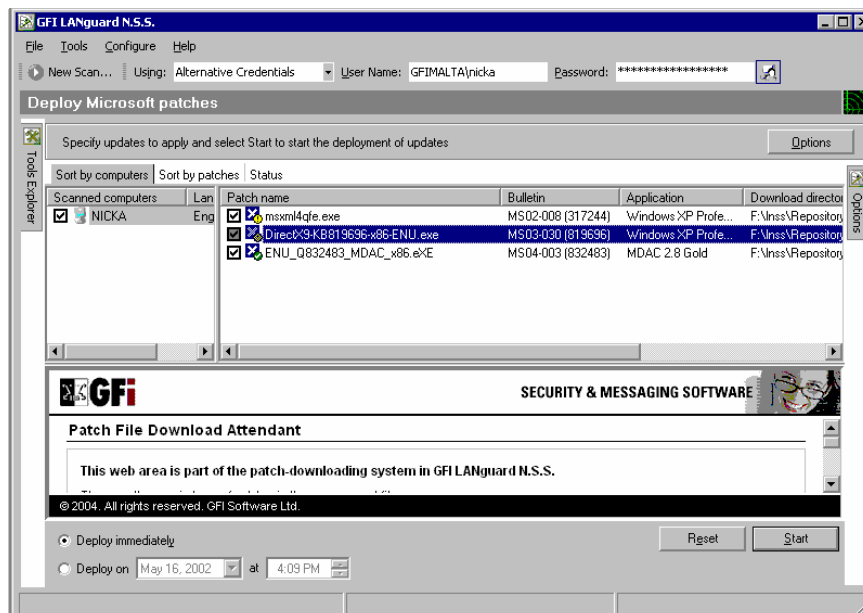


Patch file properties

Step 6: Deploy the updates

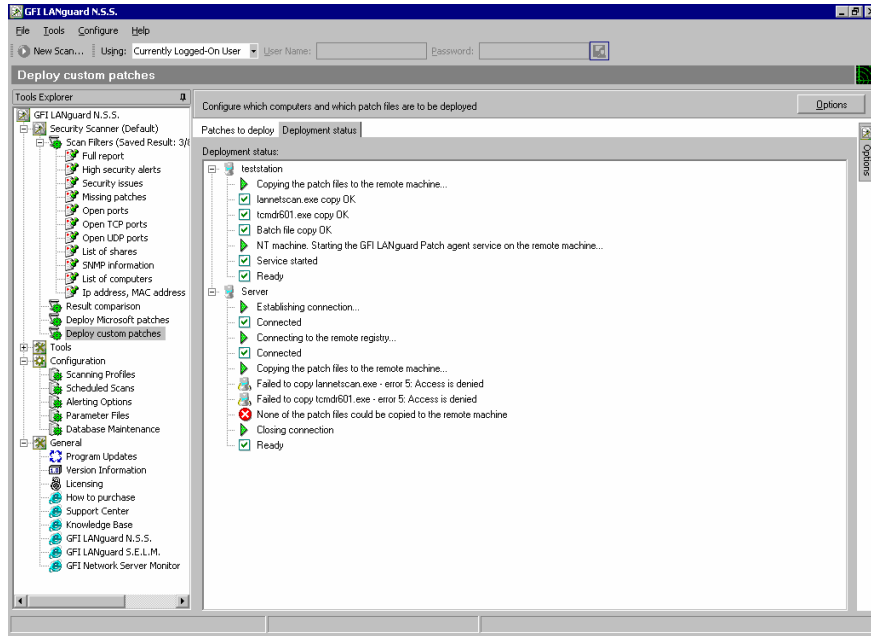
After you have selected the computers to deploy the patches on and downloaded the patches, you are ready for deployment!

Click Start at the bottom right to start deployment.



Initiating patch deployment by clicking on start.

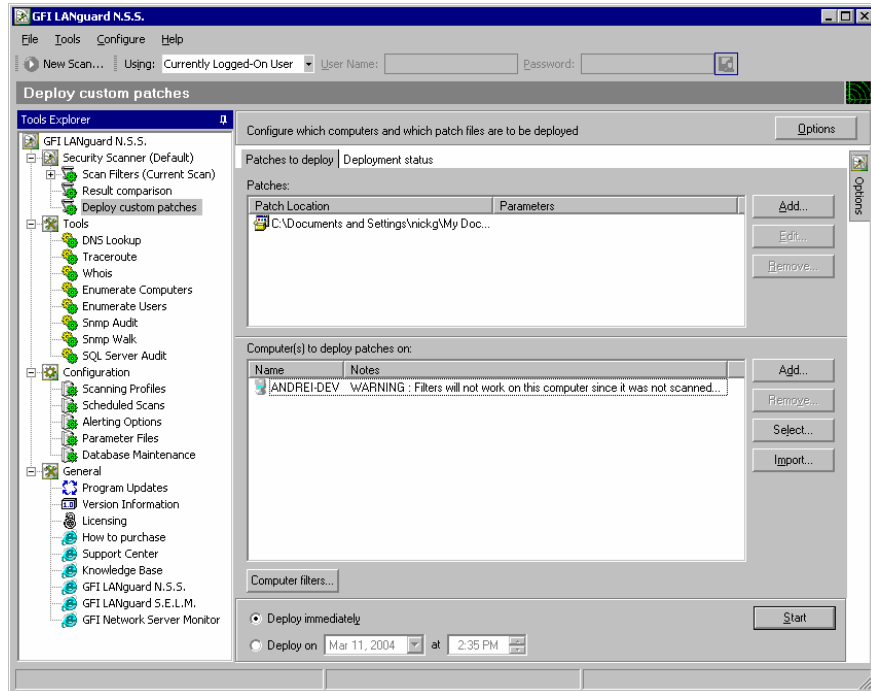
Deployment of the patches will now start. You can monitor the patch deployment status from the deployment status tab



Monitoring the download process.

Deploying custom software

The custom software deployment tool is very handy to quickly deploy custom patches for software network wide, or even to install software network wide. The custom software deployment tool is also frequently used to deploy virus signature updates network-wide. The process of deploying custom software is very similar to the process of patching a machine.



Deploying customer software

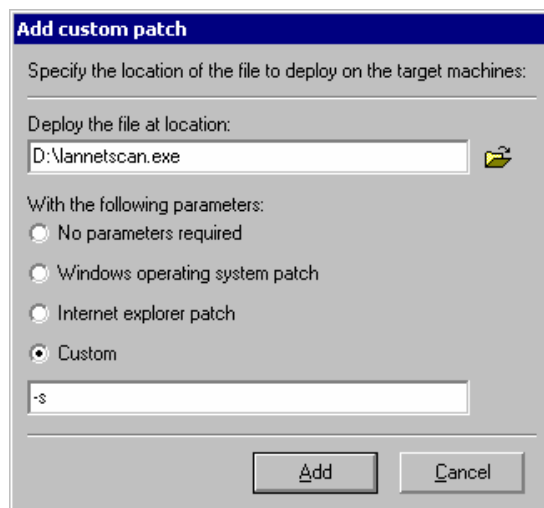
Step 1: Select the machines on which to install the software/patches

1. Go to Deploy custom software node in the tools node.
2. Click on the Add button to add a single computer, or click on the select button to select a range of computers on which to deploy the custom software.

Note: You can also select which machines to deploy custom software on from Security Scanner node and the Tools > Enumerate Computers node.

Step 2: Specify software to deploy

Click on the Add... button in the "Patches:" section to specify the source location of the file and specify any command line parameters which need to be used for deployment of the file.

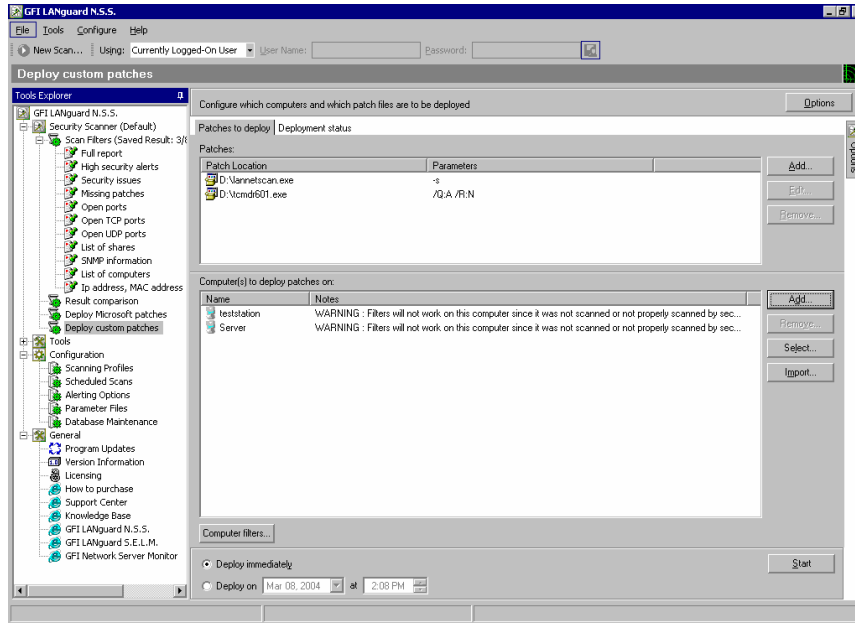


Specifying the software to deploy

Optionally you can schedule a time when the deployment should take place

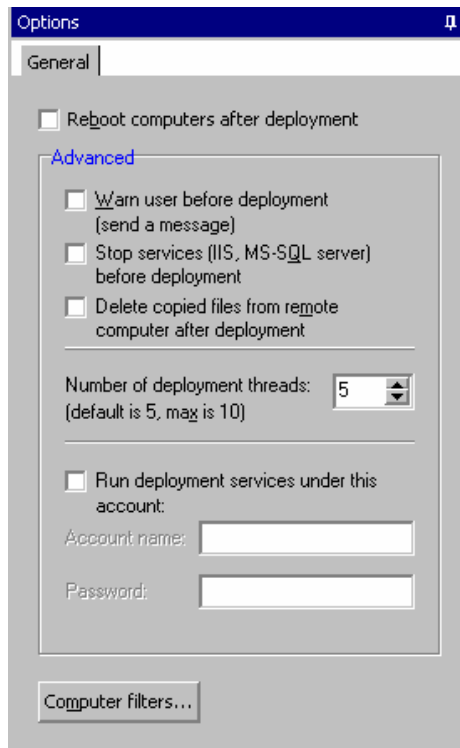
Step 3: Start the deployment process

Once you have specified the software to be deployed and the computers to which it is to be deployed, you can start the deployment process by clicking on the Start button.



Deploy custom patches indicating which patch files to deploy on which computers.

Deployment options



Deployment options

You can configure deployment options by hovering over the options button, located at the right side of the screen, with the mouse. Here you can:

- Configure the deployment agent service to run under alternative credentials.

- Reboot target computer after deployment. Some patches require a reboot after installing. Tick this tick box if one or more patches you want to deploy need a reboot.
- Warn user before deployment: will send a message to the target machine before deploying the updates.
- Stop services before deployment: This option stops the ISS & MS SQL Server services before deployment.
- Delete copied files on the remote machines after deployment.
- Configure the number of patch deployment threads to use
- Configure particular filtering conditions to which to deploy the patch to (computer filters)

NOTE : In the Deploy custom patches tool, the Computer filters will not apply to computers which have not been scanned by the security scanner tool.

Results Comparison

Why Compare Results?

By performing audits regularly and comparing results from previous scans you will get an idea of what security holes continually pop up or are reopened by users. This creates a more secure network.

GFI LANguard Network Security Scanner helps you do this by allowing you to compare results between scans. GFI LANguard N.S.S. will report the differences and allow you to take action. You can compare results manually or through scheduled scans.

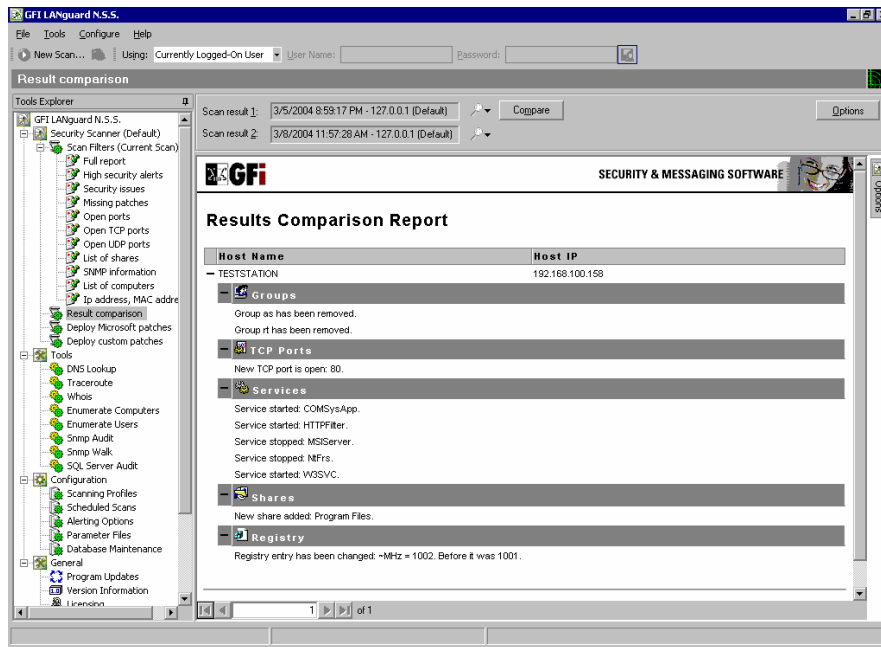
Performing a Results Comparison interactively

Whenever GFI LANguard N.S.S. performs a scheduled scan it saves the scan results XML file in the Data\Reports directory in the GFI LANguard N.S.S. installation directory.

You can also save the current scan results to an xml file by right clicking on the security scanner node and selecting 'Save scan results to XML file...'.

To compare two scan result XML files:

1. Go to the result comparison tool under 'GFI LANguard N.S.S. > Security Scanner > Result comparison'.
2. Select two scan result files, performed with the same options and on the same set of computers, but performed at different times, and click 'Compare'.



Comparing results

The result will be something similar to the above screenshot. It tells you what has been enabled or disabled and any network changes since the last scan.

- New items will show you anything new that occurred after the first scan.
- Removed items will show any devices/issues that were removed since the first scan.
- Changed items will display anything that has changed, such as a service being enabled or disabled between scans.

Performing a Comparison with the Scheduled Scans Option

Instead of manually scanning your network each day, week, or month, you can setup a scheduled scan. A Scheduled Scans will run automatically at a certain time and will emailing the differences between scheduled scans to the administrator. For example: the administrator can configure the Scheduled Scan feature to perform a scan every night at 23:00. The GFI LANguard N.S.S. attendant service will launch a security scan on the selected target computer(s) and save the results to the central database. Then, it will compare the current results with the results from the night before and report the differences, if any.

NOTE: If this is the first time that a scheduled scan is performed or if there are no differences detected with the previous scan, then GFI LANguard N.S.S. will not email you a report. *You will only receive a report if something has changed.*

Tools

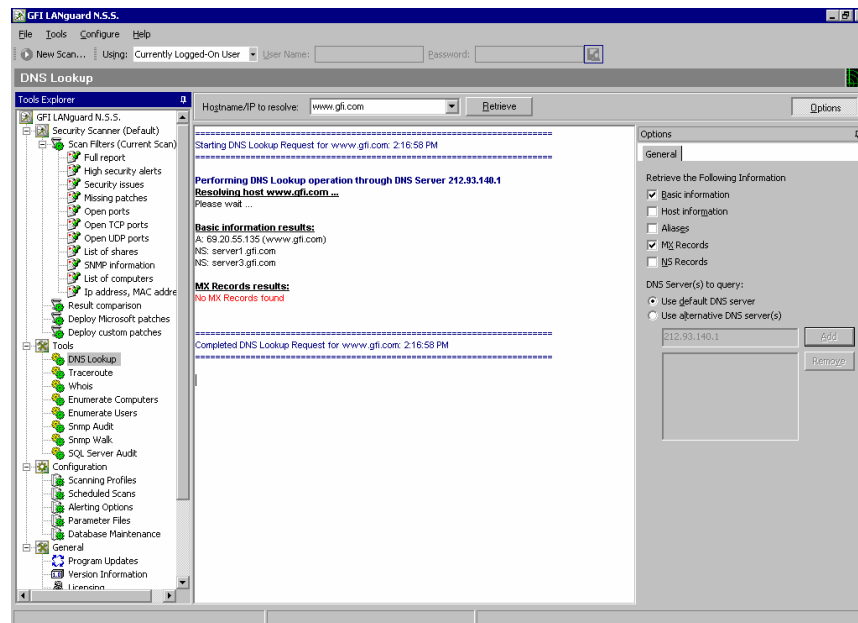
Introduction

The following Tools can be found under the Tools Menu

- DNS Lookup
- Whois Client
- Trace Route
- SNMP Walk
- SNMP Audit
- MS SQL Server Audit
- Enumerate Computers

DNS lookup

This tool resolves the Domain Name to a corresponding IP address and in addition provides information about the domain name, such as whether it has an MX record etc..



DNS Lookup tool

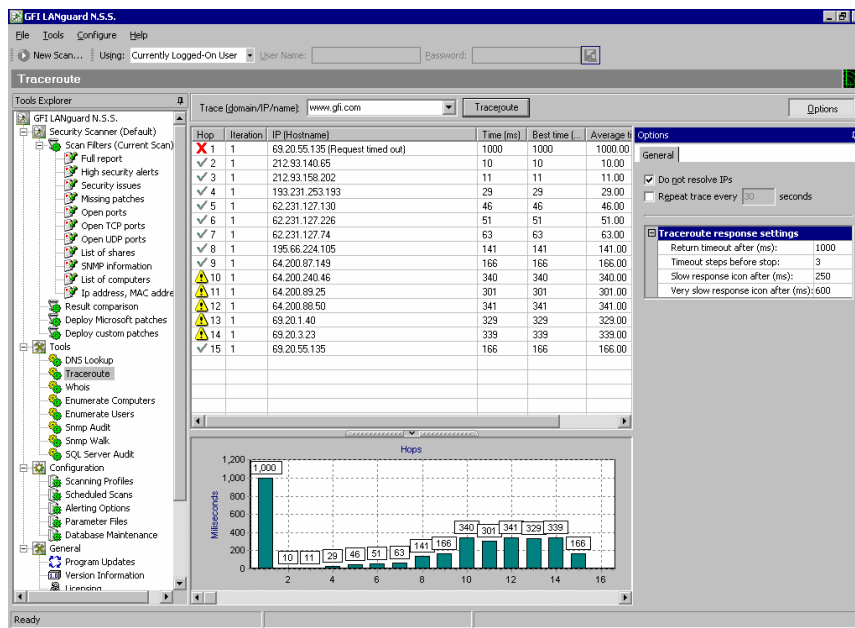
To obtain information about a domain name:

1. Go to the Tools > DNS lookup node.
2. Specify the hostname to resolve
3. Specify the information to retrieve:

- **Basic Information** – I.e. host name and to what ip this resolves
- **Host Information** - Known technically as the HINFO, and usually includes information such as hardware and what OS runs on the specified domain (most DNS entries do not contain this information for security reasons.)
- **Aliases** - returns information on what A Records the Domain might have.
- **MX Records** known also as Mail exchangers records, shows which mail server(s) and in what order are responsible for this domain.
- **NS Records** indicate which name servers are responsible for this domain.

In addition it is possible to specify an alternative DNS server .

Trace Route

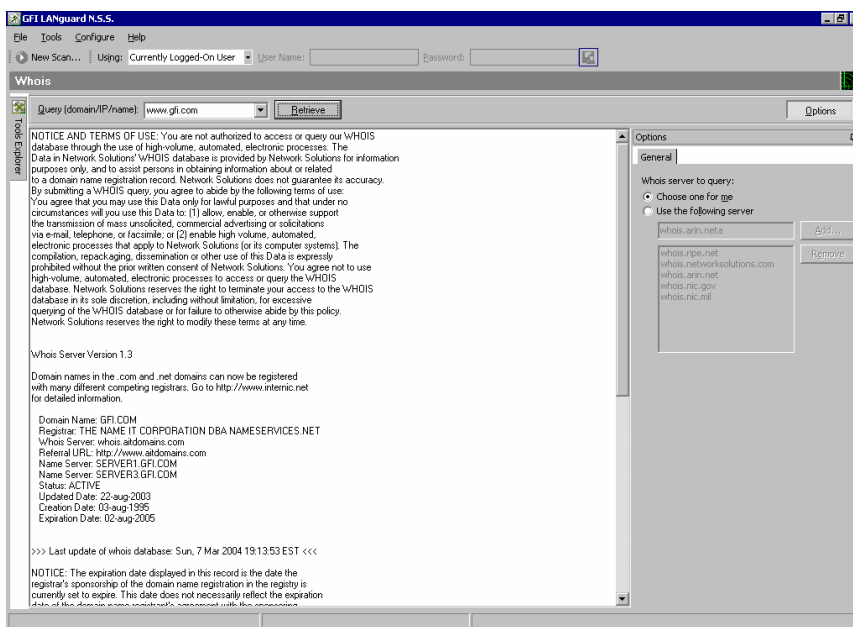


Trace route tool

This tool shows the network path that GFI LANguard N.S.S. followed to reach the target machine. When you perform a trace route, each hop has an icon next to it:

- ✓ Indicates a successful hop taken within normal parameters
- ⚠ Indicates a successful hop, but time required was quite long.
- ⚠ Indicates a successful hop, but the time required was too long
- X Indicates that the hop timed out. (i.e it took longer then 1000ms)

Whois Client



Whois tool

This tool will lookup information on a domain or IP address. You can select a specific Whois Server from the options area, or you can use the 'Default' option which will select a server for you

SNMP Walk

SNMP walk allows you to gather SNMP information. The right pane contains a list of names symbolizing specific Object ID's on the device. To find out more about the information provided by the SNMP walk, you will have to check with the vendor. Some vendors provide great details on what each piece of information means, others, though their devices support SNMP, provide no documentation on it at all.

To use the utility, click on **Tools > SNMP walk**. Enter the IP address of a machine or device which you wish to scan/'walk'.

Note: In most cases SNMP should be blocked at the router/firewall so that Internet users cannot SNMP scan your network.

It is possible to provide alternative community strings.

Note: SNMP will help malicious users learn a lot about your system, making password guessing and similar attacks much easier. Unless this service is required it is highly recommended that SNMP is turned off.

SNMP Audit

The SNMP Audit tool, allows you to perform an SNMP audit on a device and audit for weak community strings.

Some network devices will have alternative or non-default community strings. The dictionary file contains a list of popular community strings to check for. The default file it uses for the dictionary attack is called

snmp-pass.txt. You can either add new community names to this file, or direct the SNMP audit to use another file altogether.

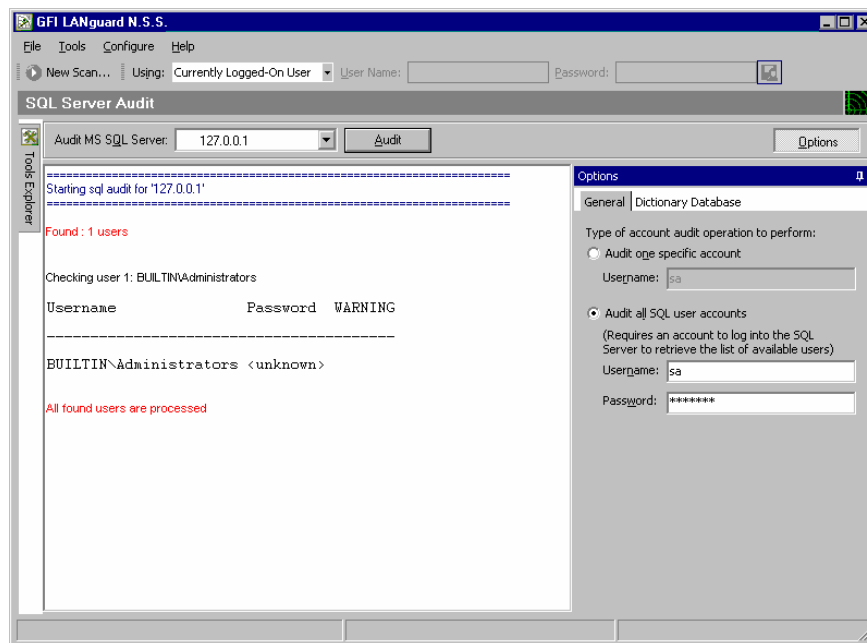
To use the utility, input the IP address of a machine running SNMP and click Retrieve.

MS SQL Server Audit

This tool allows you to perform an audit on a Microsoft SQL server installation. You can audit both the SA account, as well as all SQL accounts

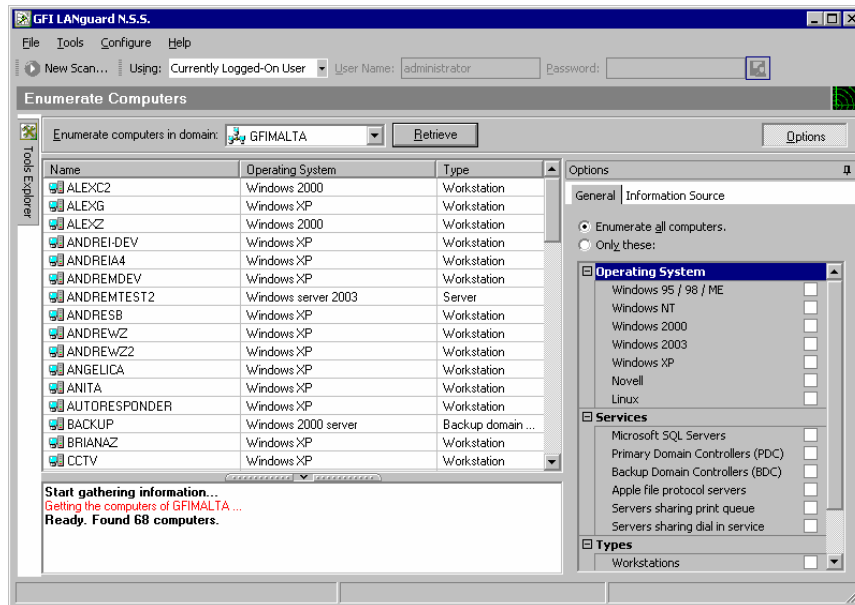
By default it will use the dictionary file called passwords.txt. You can either add new passwords to this file, or direct the utility to another password file.

To run a SQL server audit, input the IP address of the machine running MS SQL. If you want to password guess all SQL accounts, you have to enter a user name and password to login to SQL to retrieve all user accounts.



SQL Accounts audit tool

Enumerate Computers



Enumerate computers tool

This utility will search your network for Domains and/or Workgroups on it. Once it has found that, you will have the ability to scan those Domains for a list of computers in them. Once it has performed its scan it will list whatever OS is installed on that machine, and any comments that might be listed through NETBIOS.

Computers can be enumerated using one of the following methods

- From Active Directory – This method is much faster and will also enumerate computers that are currently switched off
- Using the Windows Explorer interface – This method is slower and will not enumerate computers that are switched off.

You can specify which method to use from the 'Information Source' tab. Note that you will need to perform the scan using an account that has access rights to Active Directory.

Launching a security scan

Once the computers in the domain are enumerated you can launch a scan on selected machines by right-clicking on any of the enumerated computers and selecting 'Scan'.

If you want to launch the scan but continue to use the Enumerate computers tool, select "Scan in background"

Deploying Custom patches

Select which machines you want to deploy updates on > Right click on any selected machine > Deploy Custom Patches.

Enabling Auditing Policies

Select which machines you want to enable auditing policies on > Right click on any selected machine > Enable Auditing Policies....

Enumerate Users

The Enumerate users function connects to Active Directory and retrieves all users and contacts in Active Directory.

Adding vulnerability checks via conditions or scripts

Introduction

GFI LANguard N.S.S. allows you to quickly add custom vulnerability checks. This can be done in 2 ways: By writing a script, or by using a set of conditions. Whichever method you use, you will have to add the vulnerability via the Security scanner interface and specify either the script name or the conditions which must be applied.

Note: Only Expert Users should create new Vulnerabilities, as misconfiguring Vulnerabilities will give false positives or provide no Vulnerabilities information at all.

GFI LANguard N.S.S. VBscript language

GFI LANguard N.S.S. includes a VBscript compatible scripting language. This language has been created to allow you to easily add custom checks. It also allows GFI to quickly add new vulnerability checks and make them available for download. GFI LANguard N.S.S. includes an editor with syntax highlighting capabilities and a debugger.

For further information on how to write scripts please refer to help file 'Scripting documentation', accessible from the GFI LANguard N.S.S. program group.

IMPORTANT NOTE: GFI cannot offer any support in the creation of scripts that are not working. You can post any queries you may have about GFI LANguard N.S.S. scripting on the GFI LANguard forums at <http://forums.languard.com> where you will be able to share scripts and ideas together with other GFI LANguard N.S.S. users.

Adding a vulnerability check that uses a custom script

You can add vulnerability checks that use a custom script. You can create these custom scripts using the GFI LANguard NSS editor/debugger. To do this:

Step 1 : Create the script

1. Launch the GFI LANguard N.S.S. Script Debugger from Start > Programs > GFI LANguard Network Security Scanner > Script Debugger
2. File > New...
3. Create a script. As an example, you can use the following dummy script and enter it in the debugger:

```
Function Main
echo "Script has run successfully"
Main = true
End Function
4. Save the file, e.g. "c:\myscript.vbs"
```

Step 2: Add the new vulnerability check:

1. Go to the GFI LANguard N.S.S. Main Program > Configuration > Scanning Profiles node.
2. Go to the Scanned Vulnerabilities tab, and select the category under which the new vulnerability will fall. Now click on the Add button. This brings up the new vulnerability check dialog.

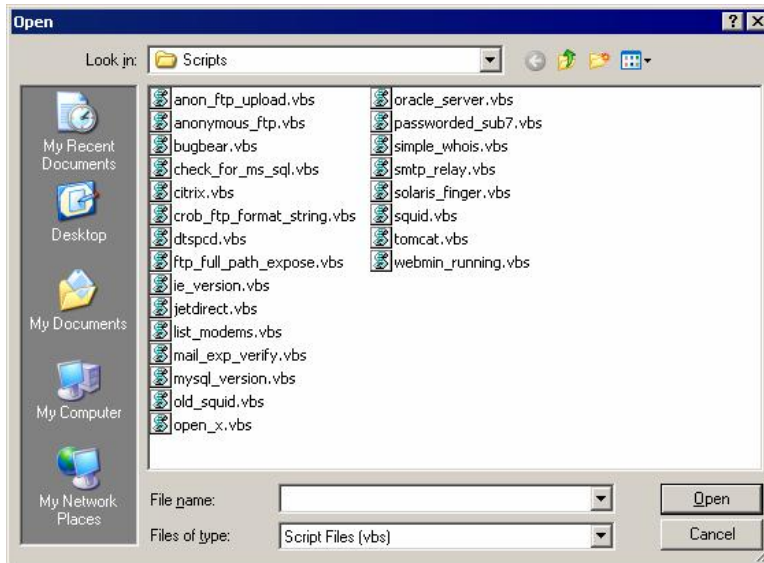
The screenshot shows the 'Add Vulnerability' dialog box. It has a title bar with 'Add Vulnerability' and a close button. The dialog is divided into two tabs: 'General' and 'Description'. The 'General' tab is active. It contains the following fields:

- Vulnerability Name: [Text input field]
- Short Description: [Text input field]
- Security Level: [Dropdown menu with 'Low Security' selected]
- BugtraqID/URL: [Text input field with a refresh icon]
- Time consumption: [Dropdown menu with 'Quick to execute' selected]

Below these fields is a 'Trigger condition' section. It contains a table with two columns: 'Check type' and 'Details'. The table is currently empty. At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Apply'. A tip at the bottom left reads: 'Tip: Right Click to add/remove checks'.

Add new vulnerability check

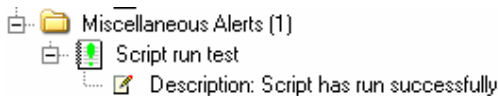
3. Now enter the basic details such as the name, short description, security level, URL (if applicable). You can also specify how long it takes to execute this check.
4. Now right click in the Trigger condition list and select "Add check"
5. Now select 'Script' from the Check type list.



Select script containing the vulnerability checking code

6. Specify the location of the script "c:\myscript.vbs". Click 'Add' to add vulnerability. It will be run next time a computer is scanned for vulnerabilities.

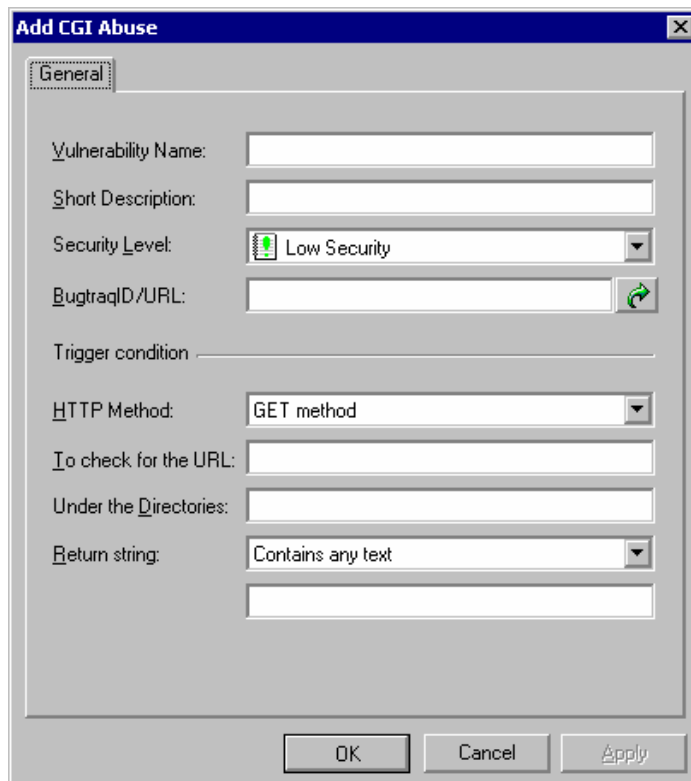
7. To test it out, simply scan your local host machine and you should see the vulnerability warning under the miscellaneous section of the vulnerabilities node of the scan results.



Adding a CGI vulnerability check

You can also add vulnerabilities without writing scripts. For example a CGI vulnerability check. To do this:

1. Go to the GFI LANguard N.S.S. Main Program > Configuration > Scanning Profiles node.
2. Go to the Scanned Vulnerabilities tab, and select the CGI vulnerabilities node. Now click on the Add button. This brings up the new CGI vulnerability check dialog.



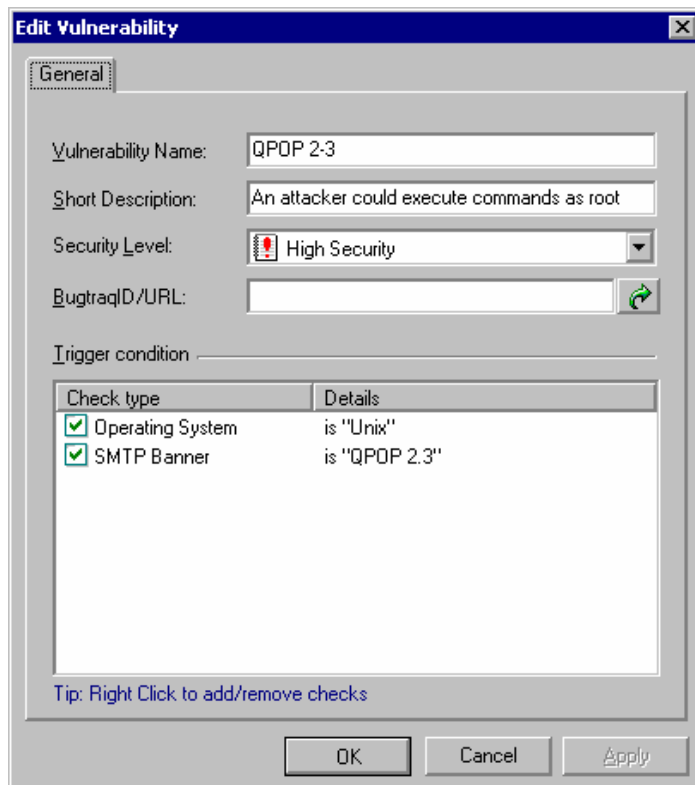
Creating a new CGI Vulnerabilities

3. Enter the basic details such as the name, short description, security level, URL (if applicable). You can also specify how long it takes to execute this check.
4. Specify **HTTP method**: the 2 methods GFI LANguard N.S.S. supports in its CGI abuse section are GET and HEAD.
5. Specify **URL to check**: This is the URL that GFI LANguard N.S.S. should query.
- 6: Specify the **Return String**: This is what GFI LANguard N.S.S. should look for in the returned information to see if the machine is vulnerable to this attack.

Adding other vulnerability checks

You can also add other vulnerabilities without writing scripts. They use the same basic format as the CGI vulnerability check, however you can set more complex conditions. To do this:

1. Go to the GFI LANguard N.S.S. Main Program > Configuration > Scanning Profiles node.
2. Go to the Scanned Vulnerabilities tab, and select the type of vulnerability you wish to add by clicking on the category under which the new vulnerability will fall. Now click on the Add button. This brings up the new vulnerability check dialog.



Creating a new Vulnerability

3. Enter the basic details such as the name, short description, security level, URL (if applicable). You can also specify how long it takes to execute this check.

4. Now you must specify what the to check for. To add something to check for, right click in the window **Trigger condition** and add a new check.

5. You can specify any of the following things to base a vulnerabilities check off of:

- Operating System
 - Is
 - Is Not
- Registry Key
 - Exists
 - Not Exists

Note: Only works under HKEY_LOCAL_MACHINE
- Registry Path
 - Exists
 - Not Exists

Note: Only works under HKEY_LOCAL_MACHINE
- Registry Value
 - Is Equal With
 - Is Not Equal With
 - Is Less Than

- Is Greater Than
- Note:** Only works under HKEY_LOCAL_MACHINE
- Service Pack
 - Is
 - Is Not
 - Is Lower Than
 - Is Higher Than
- Hot fix
 - Is Installed
 - Is Not Installed
- IIS
 - Is Installed
 - Is Not Installed
- IIS Version
 - Is
 - Is Not
 - Is Lower Than
 - Is Higher Than
- RPC Service
 - Is Installed
 - Is Not Installed
- NT Service
 - Is Installed
 - Is Not Installed
- NT Service running
 - Is running
 - Is not running
- NT Service startup type
 - Automatic
 - Manual
 - Disabled
- Port (TCP)
 - Is Open
 - Is Closed
- UDP Port
 - Is Open
 - Is Closed
- FTP banner
 - Is
 - Is Not

Note: You can build expressions that check for Version 1.0 through 1.4, and Version 2.0 through 2.2, but not Version 1.5 through 1.9. See the examples below.

- HTTP banner

- Is
- Is Not

Note: You can build expressions that check for Version 1.0 through 1.4, and Version 2.0 through 2.2, but not Version 1.5 through 1.9. See the examples below.

- SMTP banner

- Is
- Is Not

Note: You can build expressions that check for Version 1.0 through 1.4, and Version 2.0 through 2.2, but not Version 1.5 through 1.9. See the examples below.

- POP3 banner

- Is
- Is Not

Note: You can build expressions that check for Version 1.0 through 1.4, and Version 2.0 through 2.2, but not Version 1.5 through 1.9. See the examples below.

- DNS banner

- Is
- Is Not

Note: You can build expressions that check for Version 1.0 through 1.4, and Version 2.0 through 2.2, but not Version 1.5 through 1.9. See the examples below.

- SSH banner

- Is
- Is Not

Note: You can build expressions that check for Version 1.0 through 1.4, and Version 2.0 through 2.2, but not Version 1.5 through 1.9. See the examples below.

- Telnet banner

- Is
- Is Not

Note: You can build expressions that check for Version 1.0 through 1.4, and Version 2.0 through 2.2, but not Version 1.5 through 1.9. See the examples below.

- Script

- Returns True (1)
- Returns False (0)

6. Each option above has its own set of criteria, as you can see, that the vulnerability check can be based on. If you are too general when creating a vulnerability check you will get too many false reports. So if you decide to create your own vulnerability checks make sure you

design them very specifically and put a lot of thought and planning into them.

You are not limited to just one of the above things to trigger a vulnerability check; it could be that you have it set to check for multiple conditions, for example:

- Check OS
- Port XYZ
- Banner “ABC”
- LANS script QRS run and checks for the vulnerability

If all of the criteria above are met, then and only then, will the vulnerability check be triggered.

Note: Building expressions will let you do a vulnerability check such as this one that is used to check the version of Apache running on a machine: `~.*Apache/(1\.([0-2]\.[0-9])3\.[0-9][^0-9][0-1][0-9])2[0-5])|2\.0\.([0-9][^0-9][0-2][0-9])3[0-8])`.

For those experienced in C or Perl the above format is much the same as what you can do in those languages. There are many help pages on the Internet on how to use this. In the examples below we will try to walk through and explain it, but if you need more help on it, see the end of this section for a hyperlink.

If you would like to see a sample/walkthrough on creating a new Vulnerability with a script in it, look at the “***GFI LANguard N.S.S. scripting documentation***”.

Troubleshooting

Introduction

The troubleshooting chapter explains how you should go about resolving issues you have. The main sources of information available to users are:

1. The manual – most issues can be solved by reading the manual.
2. The GFI knowledgebase – <http://kbase.gfi.com>.
3. The GFI support site – <http://support.gfi.com>
4. Contacting the GFI support department by email at support@gfi.com
5. Contacting the GFI support department using our live support service at <http://support.gfi.com/livesupport.asp>
6. Contacting our support department by telephone.

Knowledgebase

GFI maintains a knowledgebase, which includes answers to most common problems. If you have a problem, please consult the knowledgebase first. The knowledgebase always has the most up-to-date listing of support questions and patches.

The knowledgebase can be found on <http://kbase.gfi.com>

Request support via e-mail

If, after using the knowledgebase and this manual, you have any problems that you cannot solve, you can contact the GFI support department. The best way to do this is via e-mail, since you can include vital information as an attachment that will enable us to solve the issues you have more quickly.

The **Troubleshooter**, included in the program group, automatically generates a number of files needed for GFI to give you technical support. The files would include the configuration settings etc. To generate these files, start the troubleshooter and follow the instructions in the application.

In addition to collecting all the information, it also asks you a number of questions. Please take your time to answer these questions accurately. Without the proper information it will not be possible to diagnose your problem.

Then go to the support directory, located under the main program directory, **ZIP the files**, and send the generated files to support@gfi.com.

Ensure that you have registered your product on our website first, at <http://www.gfi.com/pages/regfrm.htm>!

We will answer your query within 24 hours or less, depending on your time zone.

Request support via web chat

You may also request support via Live support (web chat). You can contact the GFI support department using our live support service at <http://support.gfi.com/livesupport.asp>

Ensure that you have registered your product on our website first, at <http://www.gfi.com/pages/regfrm.htm>!

Request support via phone

You can also contact GFI by phone for technical support. Please check our support website for the correct numbers to call, depending on where you are located, and for our opening times.

Support website:

<http://support.gfi.com>

Ensure that you have registered your product on our website first, at <http://www.gfi.com/pages/regfrm.htm>!

Web Forum

User to user support is available via the web forum. The forum can be found at:

<http://forums.gfi.com/>

Build notifications

We strongly suggest that you subscribe to our build notifications list. This way, you will be immediately notified about new product builds. To subscribe to our build notifications, go to:

<http://support.gfi.com>

X

XML 6

Index

D

DNS lookup 51, 53, 54, 55,
56

G

groups 5, 19

H

Hot fixes 19
HTML 6

L

License 7

O

Open ports 6
Operating System 6

P

Password policy 17
Passwords 6

R

Registry 17

S

security policy 5
Services 6
Shares 5, 6, 16
SNMP 14, 53
SNMP audit 53
System requirements 9

T

Traceroute 52
Trusted domains 20

U

Users 5–6, 5–6, 19–20, 19–
20, 57