GFI LANguard Network Security Scanner 3.3

Manual

By GFI Software Ltd.

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

Version 3.31 – Last updated October 22 2003

Contents

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. combines the functions of a port scanner and a security scanner. It also creates reports that can be used to fix security issues on a network.

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.

Furthermore, GFI LANguard N.S.S. is freeware for non-commercial usage.

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.

Patch management

GFI LANguard N.S.S. is a complete patch management solution. After it has scanned your network and determined missing patches and service packs - both in the operating system (OS) and in the applications - you can use GFI LANguard N.S.S. to deploy those service packs and patches network-wide.

At present, GFI LANguard N.S.S. supports patching of the following applications:

1. Office XP
2. Office 2000 Developer
3. Office 2000 Premium
4. Office 2000 Small Business
5. Office 2000 Standard
6. Office 2000 with Multilanguage Pack
7. SQL Server 7 (english only)
8. SQL Server 2000 (english only)
9. Microsoft ISA Server (english only)
10. Microsoft Exchange 2000 Standard (english only)
11. Microsoft Exchange 2000 Enterprise (english only)
12. Microsoft Exchange 5.5 (english only)

You can use GFI LANguard N.S.S. for operating system patching, however we recommend using Microsoft SUS. For foreign language operating system patching you have to use Microsoft SUS.

Key Features

Enumeration of Possible Entry Points

- Rogue services and open TCP and UDP ports
- SNMP holes
- CGI holes
- Rogue or backdoor users
- Trojan horses or backdoor software
- Open shares
- Weak network passwords
- Enumeration of users, services, etc.

Methods

- Information gathering
- Operating system identification
- Known security issues in software packages
- Live host detection

Alerts

- Well known security issues are immediately recognized
- Intelligent scanning
- List of missing Hot fixes and Service Packs on NT/2000/XP machines

Presentable Output

- HTML, XSL and XML output
- Ability to customize the output through XSL

Extra Features

- Exploitation of NETBIOS vulnerability in Windows 95/98/ME
- SNMP auditing
- MS SQL auditing
- Trace route
- DNS lookup
- WhoIs client
- Remote machine shutdown
- Sending spoofed messages (social engineering techniques used in hacking)
- LANS – scripting language to help build new alerts
- Check to see if Auditing is Enabled

Features of registered/commercial version

- Scheduled Scan option
- Updating of Security Alerts
- Ability to add hot fixes and service packs to remote machines
- Ability to compare scans, to learn about new possible entry points
- Query XML file for specific information

New Features in LANguard Network Security Scanner 3.3

Welcome to GFI LANguard Network Security Scanner 3.3 (LANSS). There have been many improvements compared to version 3.1. The most important are listed below:

- **Added support for Non-English operating systems service packs** detection and deployment. Languages supported include Italian, French, and German.

- **Added support for Non-English Microsoft Office 2000 / XP suites**, missing patches / service packs detection and deployment. Languages supported include Italian, French and German.
- **Added a new report –** List shares on computers.
- **Added support for new products** including SQL Server, Microsoft ISA Server, Microsoft Exchange Server and Microsoft Office.
- **New Alerts** – e.g. Sendmail bug support, new FTP Alerts.
- **Support for undetectable patches** – Some Patches Lack the necessary information required to determine whether a patch needs to be installed or not. GFI LANguard N.S.S. will report these patches listing them under a new node called: “Patches which cannot be detected”.
- **More User Friendly** – Prior to patch deployment you are presented with information such as which patches will need user intervention to install and also what steps need to be taken for successful installation of these patches.
- **Added a missing patch ignore list** to which you can add the IDs of patches which you are not interested in being notified about. Patches which you know do not need to be installed and also do not want to be reported in the scan results can be added to this list via a simple menu option.
- **Automatic download of latest security patches detection updates from a GFI server** – GFI is now maintaining its own version of the mssecure.xml ensuring that the data inside this file contains the latest, correct and verified information.
- **Scheduled scans** are now handled by a service which does not require the GFI LANguard N.S.S. UI to be loaded for the scans to take place.

In addition to what is listed above, there have been a number of bug fixes and minor additions to the program.

For more information on bug fixes and additions click on **Help > What’s New** and view the change log for the program since version 3.1

Registering GFI LANguard N.S.S.

Certain functions of GFI LANguard N.S.S. 3.3 will only work with the registered version. The 30-day trial version of GFI LANguard N.S.S. will help introduce you to the full functionality of GFI LANguard N.S.S..Registered Only Features are:

- Scheduled Scans.
- Report Generator.
- Results Comparison
- Ability to Deploy missing Hot Fixes to Windows machines.
- Ability to Update Security Alerts and Fingerprint files over the Internet.

You can find the current pricing for GFI LANguard N.S.S. at

http://www.gfi.com/pricing/pricelist.asp?product=lanss

This includes prices for new users and those who want to upgrade from version 2.0.

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 can be running while doing scans. It can block functionality of GFI LANguard N.S.S.

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. Choose the destination location for GFI LANguard N.S.S. and click **Next**.

Note: GFI LANguard N.S.S. will need approximately 8-10 MB of free hard disk space.

4. After GFI LANguard N.S.S. has been installed, you can run GFI LANguard Network Security Scanner from the start menu.

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.

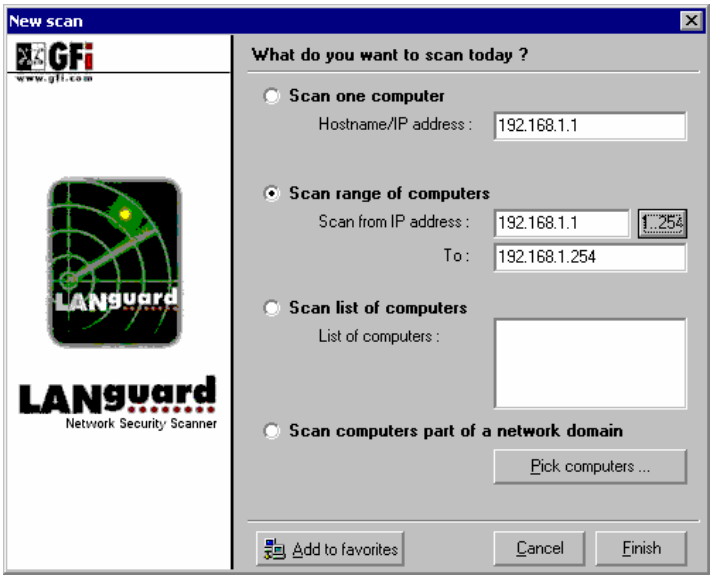
A tool such as GFI's GFI LANguard N.S.S. will help identify common vulnerabilities within your network in a very short time. Using intelligent scanning, GFI LANguard N.S.S. minimizes the time it takes to gather information on machines within the scanning perimeter. Such information normally includes usernames and groups, which may include rogue objects to allow backdoor access, enumeration of network shares and similar objects found on a NT or Windows 2000 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 a number of other potential issues.

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 **Scan a range of computers**.
3. Input the starting and ending range of the network to be scanned.
4. Select **Finish**.
5. Select the Play button [Start Scanning]  from the main GFI LANguard N.S.S. window.



Performing a scan

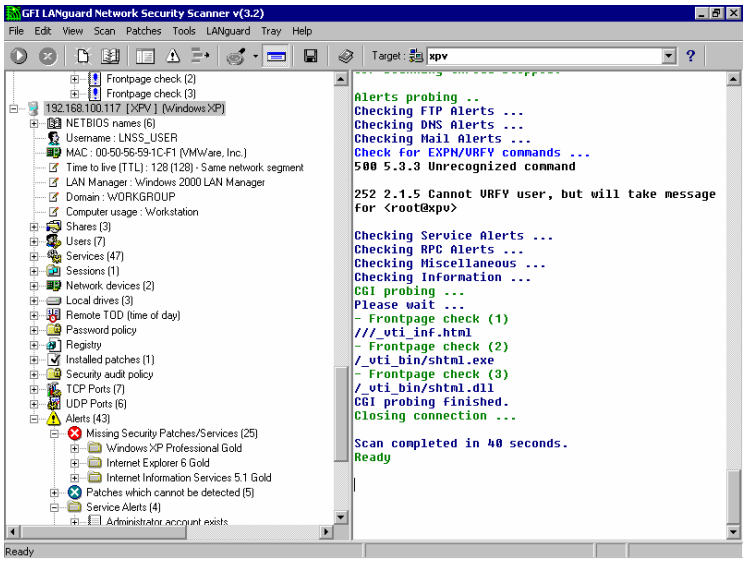
LANguard Network Security Scanner will now do a scan of the entire range entered. It will first detect which hosts/computers are on, and only scan those. This is done using NETBIOS probes, ICMP ping and SNMP queries.

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. If you would like GFI LANguard N.S.S. to scan all devices, even those that don't respond to these queries, look under the scan options section of the manual at ***"Configuring Scan options, Scanning, Adding non-responsive computers"***. But make sure you take notice of the warning, in that section, about time issues before doing this.

Scans can also be done in the following manner:

1. Scan one Computer
    - This will scan only one computer.
2. Scan List of Computers
    - Computers can be added to the list either one at a time, or you can import them from a text file. To add them right click in the window and use the menu that pops up.
3. Scan Computers that are part of a Network Domain
    - If you click on the 'Pick Computers' option you will be presented with a list of all of the Workgroups and Domains that GFI LANguard N.S.S. found on the network. Check the box next to the Workgroup or Domain that you want to scan and GFI LANguard N.S.S. will scan all computers found in that Workgroup/Domain. You can also select individual computers within that Workgroup/Domain.

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.

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 well GFI LANguard N.S.S. can identify it and what information it can retrieve.

Once GFI LANguard N.S.S. has finished its scan of the network a screen like the *'Analyzing the results'* screen shot above will appear.

Depending on the device found different information would be available. However, for explanation purposes we will assume that the network device found is a Windows machine for most of the information to come.

Network Device IP and Name

First the IP address of the device we are working on will appear. Next to that the Netbios Name or DNS name depending on the type of device. Finally GFI LANguard N.S.S. will report what OS is running on the device and if it is NT/2000/XP GFI LANguard N.S.S. will report what Service Pack is on the machine.

Netbios Names

The first node under the device lists Netbios information, such as services, current user logged on, etc. (You can find more information in the section called ***"Additional Results"*** in the next section.)

Trusted Domains

If the computer is part of a Domain, it will show one or more trusted Domains. Ensure that the trust relationships are setup correctly and this machine actually should trust all Domains listed.

Shares

Open shares, if not secured, are a threat to network integrity. Administrators should make sure that:

- No user is sharing his/her whole drive with other users.
- Anonymous/unauthenticated access to shares is not allowed. GFI LANguard N.S.S. now has an option to check for these unpassworded shares and will let you know when it finds them.
- 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.

Users & Groups

The next 2 nodes show the local groups and the local users available on the computer. Check this area to ensure that there are no extra user accounts, and verify that the Guest account is disabled. Rogue users and groups can allow users backdoor access!

Some backdoor programs will reenable the Guest account and grant it Administrative rights, so expand 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 & Processes

All running 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, this automatically reduces the security risks on that machine.

General Information

Network devices, drives and remote time of day shows general information about the computer.

Note: For more information on these see the ***"Additional Results"*** in the next section.

Password Policy

The next node is an important one. Check to see that 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 GPO (Group Policy Objects) in Active Directory.

Registry

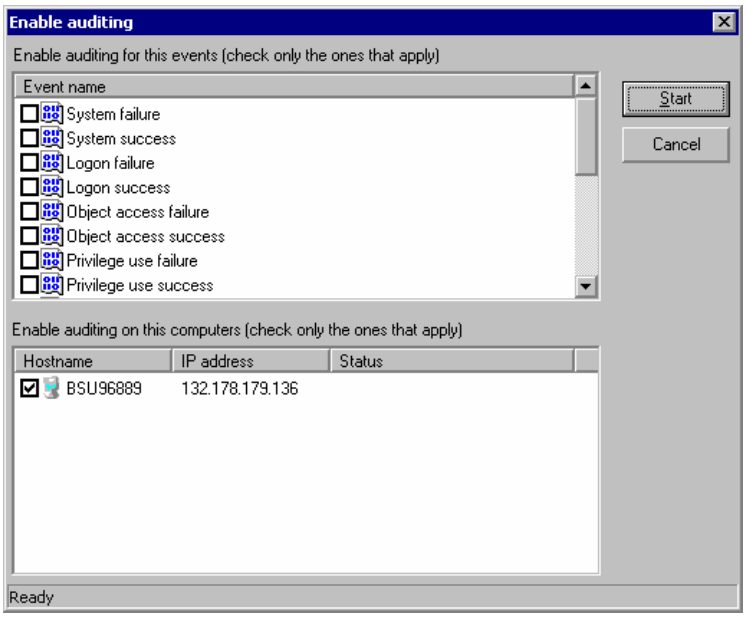
This node gives vital information about the remote registry.

Click on the Run node to check what programs automatically launch at startup.

Check that the programs that automatically launch 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.

Auditing

If the target machine runs Windows NT/2000/XP, GFI LANguard N.S.S. will check if auditing is turned on. It is recommended to turn on auditing on Windows machines. This is an important security feature of Windows that is disabled by default. Turning on auditing will allow you to detect security breaches and check how it occurred.



GFI LANguard N.S.S. provides a way to turn auditing on, assuming you have administrator rights to the machine, once a machine is scanned.

To enable auditing on a machine right click, goto **Enabling Auditing on > This Machine**. You can will then see a screen such as the above one. Check the boxes next to the events you want audited on the machine.

Installed Hot Fixes

The hot fixes node shows what hot fixes are installed. Ensure that your machines have the latest Hot Fixes and Service Packs installed.

Unfortunately, in the windows world there seems to be no greater security risk than not being up to date on the latest hot fixes and service packs. So make sure you always have the latest patches installed.

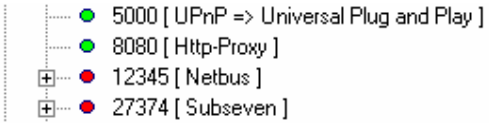
Open Ports

The open ports node lists all open ports found on the machine. (This is called a port scan). LANguard Network Security Scanner does a selective port scan. It does not scan all 65535 TCP and 65535 UDP ports, just the ports it is asked to. To learn more on how to change what ports GFI LANguard N.S.S. is set to scan, look in the manual at ***"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 likely to be open. Hopefully, your Internet firewall is blocking these ports from the outside world.

GFI LANguard N.S.S. will list all open ports it finds that are setup to be scanned for. 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:



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 box. Some valid programs will open ports that are the same as some known Trojan ports. One antivirus program uses the same known port as NetBus Backdoor. So always check the banner information provided and run other checks on these machines.

Alerts Node

The alerts node displays known security issues and informs you how to fix them. These threats can include HTTP issues, NETBIOS alerts, configuration problems and so on.

Alerts are broken down into the following sections: Missing Patches, CGI Abuses, FTP Alerts, DNS Alerts, Mail Alerts, RPC Alerts, Service Alerts, Registry Alerts, Miscellaneous Alerts and Information Alerts.

Missing Patches show up on Windows NT/2000/XP machines if there are any missing Hot Fixes or Service Packs. GFI LANguard N.S.S.

will provide a link to the Microsoft page where you can download that individual patch.

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

FTP Alerts, DNS Alerts, Mail Alerts, RPC Alerts, and Miscellaneous Alerts 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 Alerts 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 Alerts 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 Alerts 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.

Additional Results

GFI LANguard Network Security Scanner also displays some general information about each machine:

NETBIOS Information

NETBIOS names - These are the names of the Services, Users Logged on and Machine Name.

Username

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

MAC

This is the Network card MAC address.

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.

LAN Manager

Gives the LAN Manager in use (and OS).

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.

Computer Usage

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

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.

How Best to Use LANguard Network Security Scanner

Introduction

Below is a recommendation on how to use GFI LANguard N.S.S. for the first time and how to get the most out of those first scans. Before running GFI LANguard N.S.S. it is recommended that you read the ***"Warnings"*** section of the Manual.

On Site Scan

Setup a machine with LANguard Network Security Scanner installed on it. Do a scan of your network with a 'NULL session' (**Scan > Options > Sessions Tab > NULL session**).

Once this first scan is done, save it and go back in to setup a scan with either **Existing credentials** (if you have administrative rights to your domain), or as a **specific user** that does 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 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.

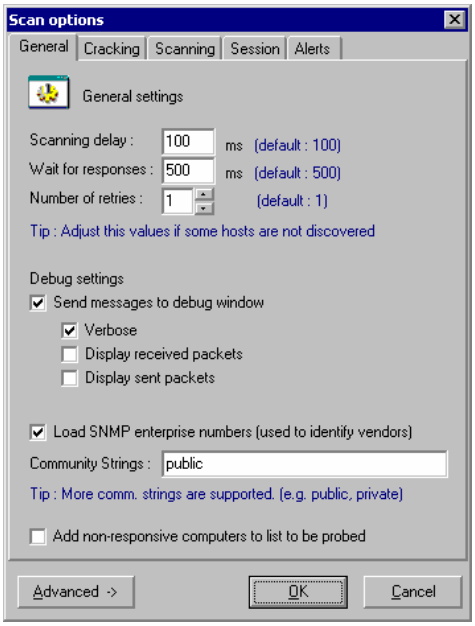
Make sure you run security scans from time to time. This isn't something you can do once and then forget about it. Something new is always out there, and once again, just because you were safe and secure today, you never know what tomorrow's hacker will come up with.

Configuring Scan Options

Introduction to Scan Options

After you have performed the first security audit, and familiarized yourself with LANguard Network Security Scanner, the first thing you'll want to do, is configure the GFI LANguard N.S.S. scan options. To do this, go to **Scan > Options**. The options dialog will appear.

General - Options



General - Options

Delay & Retries

Scanning Delay is the time LANguard Network Security Scanner waits between 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 to 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 need 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.

Debug Settings

This section allows you to configure the verbosity of the debug window. It is recommend leaving the debug window enabled. It shows you, some of, what GFI LANguard N.S.S. is actually doing. Also, some information, such as return information from LANS, is only displayed in the debug window, and is not copied into the output window and therefore not saved in the reports.

If you would like to see more of what GFI LANguard N.S.S. is sending and receiving you can enable the options: **Display received packets** and **Display sent packets**. During normal usage of the product these options are not enabled and don't need to be. If you start having problems and think there is a bug or problem then you can enable these options and use them to help track more of what GFI LANguard N.S.S. is doing.

To save the debug information, right click in the debug window and go to **Save debug info**.

SNMP

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, or trying to increase the load time of GFI LANguard N.S.S. it is recommended to leave this option enabled.

By default most SNMP enabled devices have a read community name of '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'.

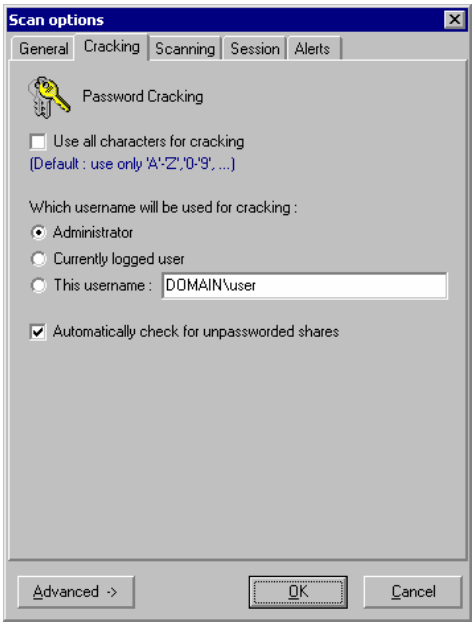
Adding Non-Responsive Computers

Because of the possibility of a personal firewall on a machine that blocks NETBIOS, SNMP, and ICMP packets there is now an option to add all non-responsive computers to the list of machines to be port scanned.

Note: This will greatly increase your network scan times, because LANguard Network Security Scanner will need to TCP and UDP port scan each non-responsive host and wait for the timeout to occur on each and every port scanned. Unless you know that there are quite a

few machines on your network, setup to be non-responsive to NETBIOS, SNMP, and ICMP packets, it is not recommend using this. GFI LANguard N.S.S. already has a few other checks it does to try to determine if a machine is actually blocking these packets.

Cracking - Options



Cracking - Options

This tab allows you to configure the password testing options in order to identify weak passwords.

You can perform brute force cracking with the option **Use all characters for cracking**. This will of course increase the time for a network audit using GFI LANguard N.S.S.. It might also cause various alerts on intrusion detection systems!

Username used for Cracking

This is the username that GFI LANguard N.S.S. will use to attempt to break into shares.

On Microsoft NT/2000/XP machines the administrator account cannot be locked out due to too many incorrect login attempts. That is why the default account name here is Administrator. If the Administrator username has been changed, you can select **This username:** and set it there.

GFI LANguard N.S.S. can be set to try using the **Currently Logged on user** when it tries to crack the password on a share, but if policies have been setup for account lockout, this will eventually lock the currently logged on users account. Therefore, this is not recommended.

Note: On a NT/2000/XP box you can do a number of things to thwart an attack such as this. There are many articles and books on this, but two easy things to do are: rename the administrator account and remove it from the administrator group. (Before doing this ensure that other accounts have administrative access.) Also, modifying the Local

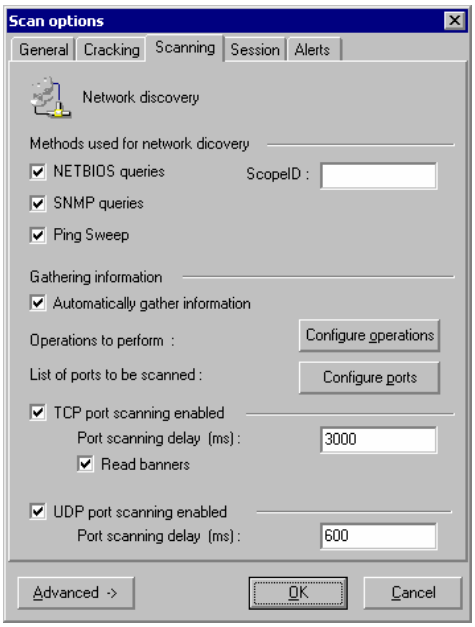
Security Policy to log Failed Login attempts to the Event Log. (This will not keep the attack from happening, but at least you will be able to see that someone was trying to login to the box and failed.)

Unpassworded Shares

If checked, LANguard Network Security Scanner will check machine shares for a password and let you know if any are found without one.

One reason that Unpassworded Shares are dangerous is because of the way some of today's viruses are spreading. Viruses such as Klez spread through open shares; once a machine is infected it will look for shares it has access to and try to infect them. It only takes one person in a company to quickly infect many machines if shares are left open.

Scanning - Options



Scanning - Options

Methods for Network Discovery

Here is where you can specify the method(s) used to discover which computers are on. Some devices will not be running NETBIOS or SNMP, but all machines will usually respond to ping.

The **NETBIOS queries** option allows Netbios or SMB queries to be sent out. 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.

There is the ability to add ScopeID information to the Netbios Query. In most cases this should not be set. However, in special cases some systems might have been set with 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 compare that to a local database while determining what that device is.

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

Each of the above query types can be turned off, but GFI LANguard N.S.S. uses all 3 types of queries to help it 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. will still attempt to identify the device and the OS on it. (GFI LANguard N.S.S. may not be as reliable if it is not doing a full scan.)

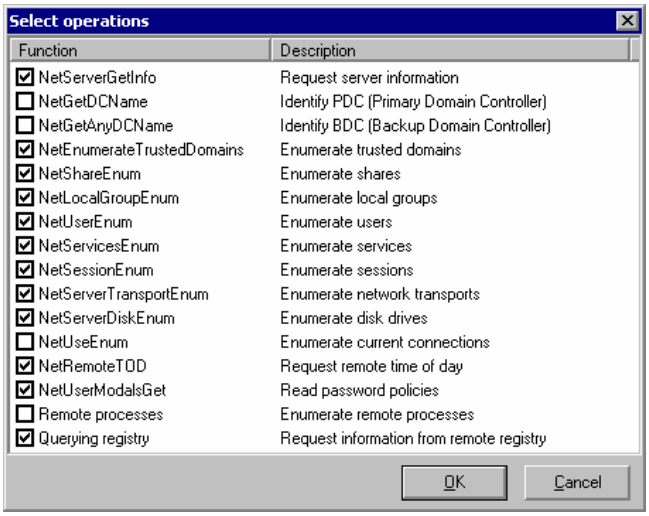
Note: Some personal firewalls will block a machine from even sending out an ICMP echo, but in most cases you will probably not see this on your corporate network. If you feel that quite a few devices on your network are running personal firewalls, look at enabling the option called ***"Adding non-responsive computers"*** to the list to be probed which is described elsewhere in the documentation.

Gathering Information

This section effectively allows you to configure what GFI LANguard Network Security Scanner should scan for. You can configure the exact information that GFI LANguard N.S.S. should request as well as the ports that it should scan.

It is recommend that you leave the option to **automatically gather information** enabled. If this is disabled then GFI LANguard N.S.S. will not do a port scan of the device and will not try to make any of the secondary Netbios connections.

Configure the Netbios Information to Scan



Configuring info to scan

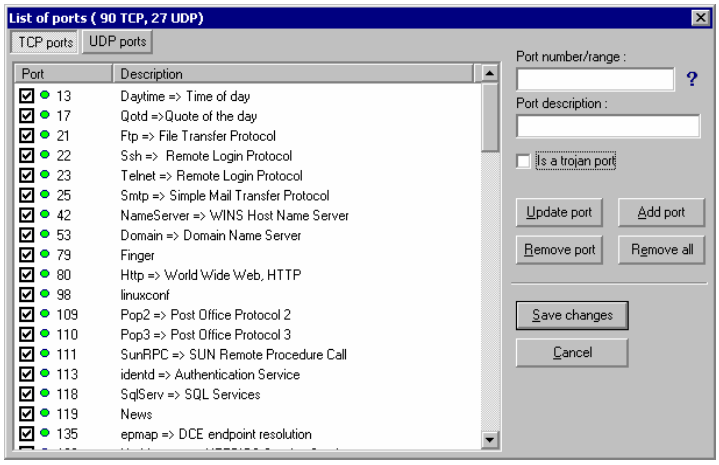
You can configure the information that LANguard Network Security Scanner should scan for from the **Scan > Configure Operations**.

Each function provides a description of what information it is going to try to gather. Notice that not all options are turned on by default.

Ones that provide the most info and seem to be supported on all OS's are on by default.

Note: Some of these connections are only supported if connecting as a user with rights. In other words, if you are trying to gather information connected as a NULL connection, you will see errors in the debug screen telling you that you don't have rights to make that type of connection.

Configuring Ports to Scan



Configuring ports to scan

You can configure the ports that LANguard Network Security Scanner should scan for from the **Scan > Configure Ports**. (Either TCP or UDP ports)

How to Add a Port

Input the port number(s) you want to scan (i.e. 21 or 1-21), put in a description for these port numbers, and if it is a Trojan/backdoor port check the **Is a Trojan**. Then Click on **Add Port**.

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

How to Update a Port

If you have created a port already and find that it, or one of the default ports is mislabeled you can update that information.

To do this, highlight the port you want to update, change the Port Number, Description, or check boxes, and then click **Update**.

How to Remove a Port

If you find that you don't want LANguard Network Security Scanner scanning a specific port anymore, you will want to remove that port from the List of Ports it is set to scan.

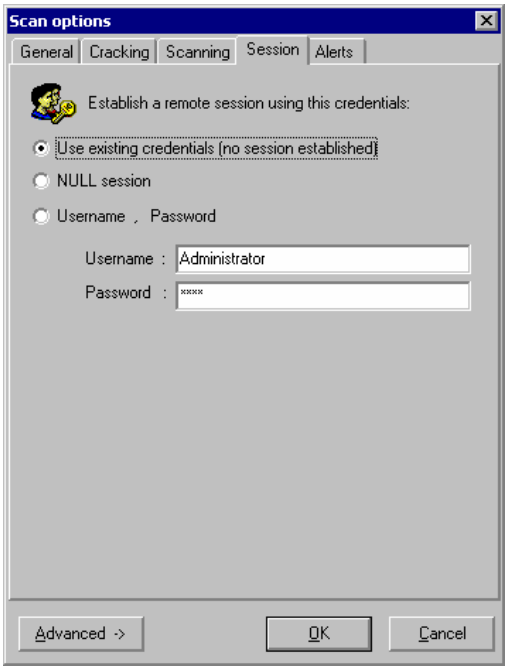
To do this, highlight the port you want to remove from the list and click **Remove**.

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

If you don't want GFI LANguard N.S.S. to scan a specific port, but you do not want to remove it permanently just uncheck the box next to the port number.

Note: This is different than in version 2.0. The check box no longer tells GFI LANguard N.S.S. to read the banner information provided by the port, GFI LANguard N.S.S. does that automatically. The check box next to the port now tells GFI LANguard N.S.S. to scan that port!

Session - Options



Session - Options

In this tab you can specify which user credentials to use for running NETBIOS queries.

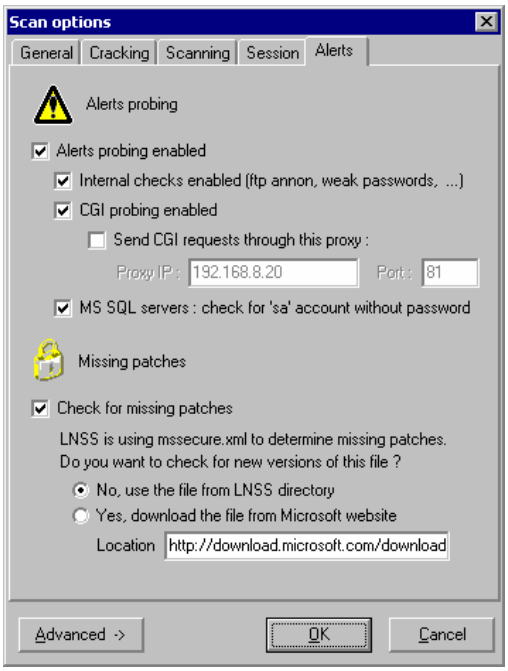
Use existing credentials will make use of your current privileges. If you don't have access to the network, little or no information will be obtained.

In that case, you should choose **NULL session**, which means you will log on as an anonymous user.

Optionally, you can specify a **Username and Password** of a particular user. This will allow you to get an idea what information that user would be able to see if they ran a NETBIOS scan.

Note: if you are going to use a specific username/password of a domain or Active Directory account you will want to put in the username in the form of Domain\username.

Alerts - Options



Alerts - Options

Alerts are security holes found by GFI LANguard Network Security Scanner.

By default, GFI LANguard N.S.S. will scan for alerts. You can change this from the Alerts tab.

Internal checks are alerts that you have no control over but are built into GFI LANguard N.S.S. (such as checking to see if SNMP is enabled on a device).

CGI probes are sent against web servers, you have the ability to turn them off here and if you are running the audit from behind a proxy server, you can tell GFI LANguard N.S.S. to run CGI probes through that proxy.

Recently, the MS SQL 'sa' account issue has come to light. Here you can configure GFI LANguard N.S.S. to check for **MS SQL 'sa' accounts with no passwords**.

Note: this menu option is different from alerts in the Scan menu at **Scan > Alerts**. This section specifies which types of alerts (internal, CGI, MS SQL, etc) to run. The **Scan > Alerts** enables the exact alerts to run, such as Unicode Exploit against IIS.

Missing Patches

LANguard Network Security Scanner, by default will check each Windows NT/2000/XP machine for missing Hot Fixes and patches.

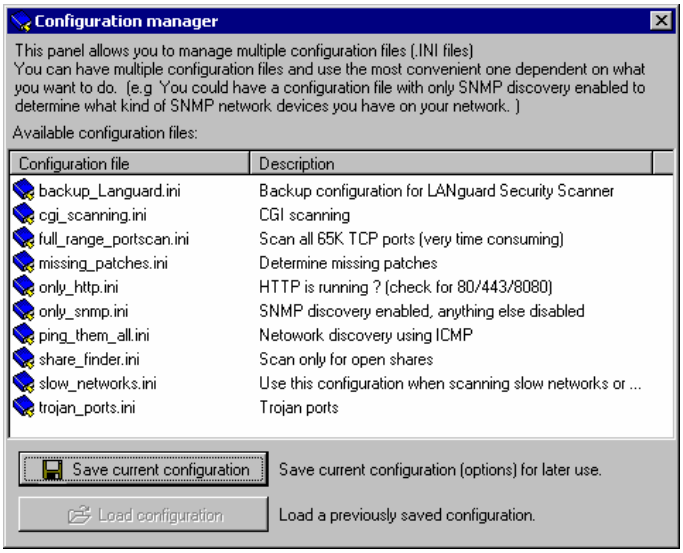
This version of LANGUARD N.S.S. will automatically download lnssprms.cab when needed each time you start LANGUARD N.S.S. (This file will be uncompressed into mssecure.xml

and products.xml). This procedure will make sure you will always be scanning for the latest security patches and service packs.

For more information on this see the ***"Deploying Patches to Microsoft Machines"*** elsewhere in the manual.

Configuration Manager

If you click on the **Advanced ->** button you will you will see a window like this:



Configuration Manager Window

If you do lots of different types of scans on your network, the ability to save your settings through this utility will save you a lot of time. In the past you had to manually set these options every time you wanted to change the way the program worked. But now, with the ability to save configuration files with the port scan options and all other settings you will be able to save time.

Saving Configurations

Once you have GFI LANguard N.S.S. configured the way you want, you can click on **Advanced > Save Current Configuration** and then save all of the settings you have currently configured.

Loading Configurations

When you want to load one of the other configuration files you can just highlight them and click **Load Configuration**. This will load all of the settings for that initialization file. (Ports to scan, types of scans, etc.)

Alerts

Introduction to Alerts

Alerts are warnings about potential security issues on your network. The Alerts chapter covers 4 areas:

1. Updated Alerts
2. Types of Alerts
3. Configuring Alerts
4. LANS – a scripting language

Updated Alerts

This feature is only available in the registered version of GFI LANguard Network Security Scanner!

New in GFI LANguard N.S.S. 3.1 is the ability to Update the Alerts over the Internet that GFI LANguard N.S.S. scans for.

To update your Security Alerts, Click on **Help > Check for security update > Begin Updates**

Note: The security update feature will also update the fingerprint files used to determine what OS is on a device and may update other behind the scene files.

Types of Alerts

This was mentioned in an early section, but is presented again here as a reminder of the types of alerts that GFI LANguard N.S.S. provides.

Alerts are broken down into the following sections: Missing Patches, CGI Abuses, FTP Alerts, DNS Alerts, Mail Alerts, RPC Alerts, Service Alerts, Registry Alerts, Miscellaneous Alerts and Information Alerts.

Missing Patches show up on Windows NT/2000/XP machines if there are any missing Hot Fixes or Service Packs. GFI LANguard N.S.S. will provide a link to the Microsoft page where you can download that individual patch.

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

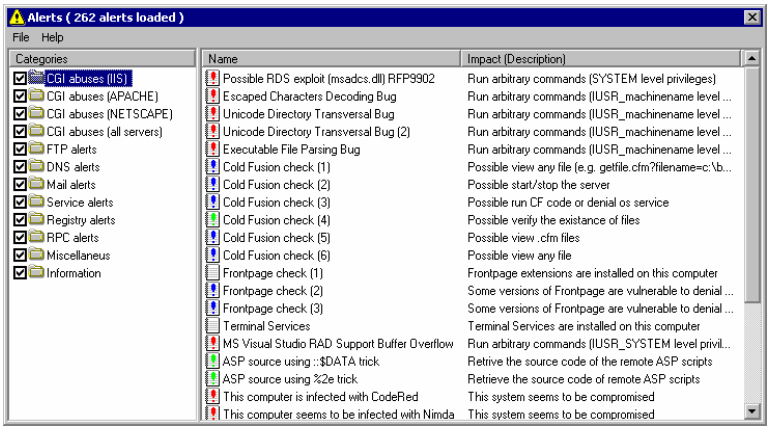
FTP Alerts, DNS Alerts, Mail Alerts, RPC Alerts, and Miscellaneous Alerts provide links to Bugtraq or other security sites so that you can lookup more information about the problem GFI LANguard N.S.S. found.

Service Alerts 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 Alerts 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 Alerts 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.

Configuring Alerts to Scan for



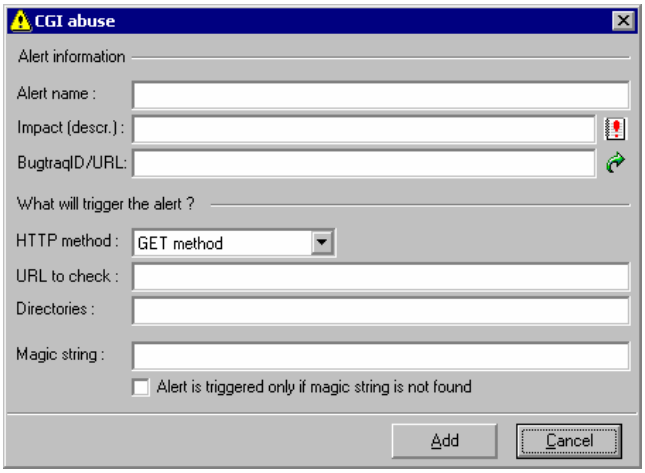
Configuring the alerts to scan

GFI LANguard Network Security Scanner includes a database of alerts that it will scan for. You can view these alerts from the **Scan > Alerts** menu. This will bring up a dialog in which you can configure the alerts.

You can specify which alert types are run by selecting or de-selecting them from the left pane. From the right pane, you can change a specific alert by double clicking on it. Each Protocol has it's own Format. You can specify the level of the alert by clicking on the  button.

Note: Only Expert Users should create new alerts, as mis-configuring alerts will give false positives or provide no alert information at all.

Format of the CGI Alerts



Creating a new CGI alert

Alert name: is the name you want GFI LANguard N.S.S. to display in the alerts section of its output, and what you want to call it.

Impact: is a description of what problems this CGI abuse will cause if not fixed. You can also change the icon on the side that indicates how severe this vulnerability is. (High - Red, Medium - Blue, Low - Green, or Informational – pure white)

BugtraqID/URL: is the web address where more information can be found on this bug/hole.

HTTP method: the 2 methods GFI LANguard N.S.S. supports in its CGI abuse section are GET and HEAD.

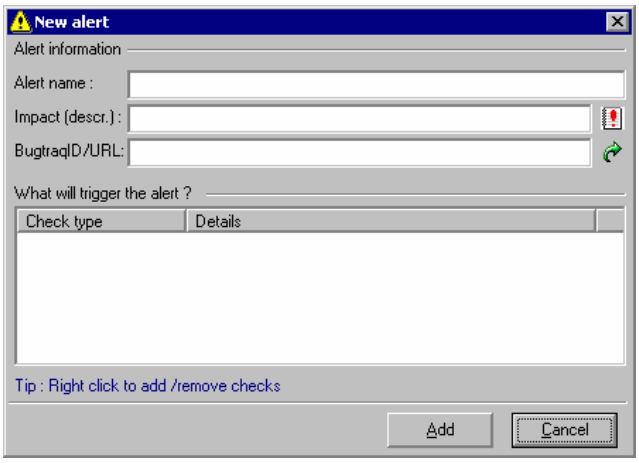
URL to check: is the URL that GFI LANguard N.S.S. should ask the machine for.

Magic String: is what GFI LANguard N.S.S. should look for in the returned information to see if the machine is vulnerable to this attack.

If the Magic String not being returned should trigger this alert, then check the box **Alert is triggered only if magic string is not found**.

Format of the other Alerts

The rest of the alerts all use the same basic format to create them.



Alert name: is the name you want GFI LANguard N.S.S. to display in the alerts section of its output, and what you want to call it.

Impact: is a description of what problems this type of vulnerability will cause if not fixed. You can also change the icon on the side that indicates how severe this vulnerability is. (High, Medium, Low, or just Informational)

BugtraqID/URL: is the web address where more information can be found on this bug/hole.

At this point each type of alert must be carefully thought out and designed. To add something to check for, right click in the window **What will trigger the alert?** and add a new check.

You can specify all of the following things to base an alert 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
- 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.
- LANS Script
  - Returns True (1)
  - Returns False (0)

Each option above has its own set of criteria, as you can see, that the alert can be based on. If you are too general when creating an alert you will get more false reports about a bug or hole in a service. So if you decide to create your own alerts 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 an alert; it could be that you have it set to do the following:

- 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 alert be triggered.

Note: Building expressions will let you do an alert 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.

Examples

If you would like to see a sample/walkthrough on creating a new alert with a LANS script in it, look at the ***“LANS – Scripting, First LANS script”*** part of the manual. There is a walkthrough on creating a script, describing exactly what the script does and how the alert works.

Lets look at some simple examples of expressions first:

[09-] matches '0', '9' and '-'

[-90] matches '-', '9' and '0'

[0-9] matches all ten characters from '0' to '9'

Now lets look at a little more difficult ones:

First we will work with the [^ which means to match characters not in the list.

1[^1-8]2 matches 102 and 192, but not 112, 122, 132 … 172

Next we will work with the | character, which means OR

1[^1-8](2|3) matches 102, 103, 192, 193

More examples can be found at the author of TregExpr at: http://anso.virtualave.net/RegExpE/tregexpr_syntax.htm

The author is given credit in the ***"LANS – LANguard Scripting"*** section of the manual.

LANS

There is a whole chapter on LANS later in the documentation. Look for it at ***"LANS – LANguard Scripting"*** elsewhere in the manual.

LANguard scripting allows you to extend the functionality of the Alerts that you can create. Like the Alerts, this should only be used by Expert Users.

Saving GFI LANguard N.S.S. Scan Results

Introduction to Saving Scan Results

When you save information from GFI LANguard N.S.S. it is saved in 3 formats:

- HTML
- XML
- XSL

You don't have to choose between the 3, it automatically saves in all 3 and uses each one for specific purposes.

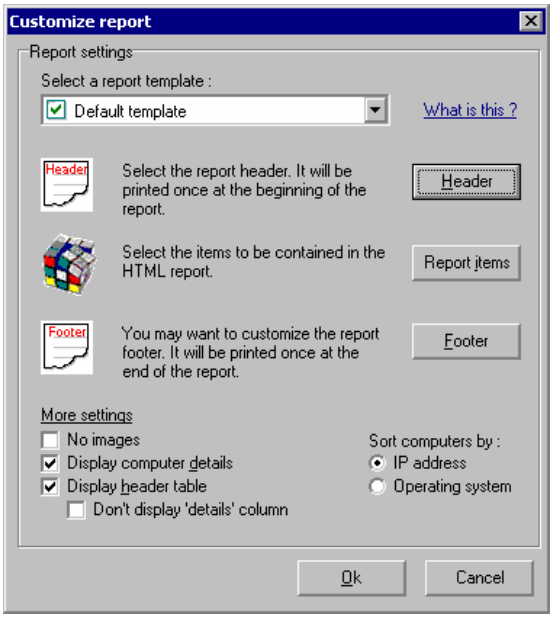
Generating Reports

When you click on **File > Generate Report** you will be prompted with a window that looks like this:

Generating a GFI LANguard N.S.S. report

Customize the Output

Through the use of XSL files you have the ability to only save specific pieces of information from GFI LANguard N.S.S.. If you click on the customize button you will see a window like this:



Customizing a GFI LANguard N.S.S. report

If you don't like the default header that GFI LANguard N.S.S. uses you can modify it, to do so though, you'll need to know a little HTML. To modify it click **Header**.

To keep certain things from showing up in the report you can modify what is saved. You can do this by modifying it in the **Report items** button.

Again, if you don't like the default footer that GFI LANguard N.S.S. uses you can modify it, to do so though, you'll need to know a little HTML. To modify it click **Footer**.

You can change the XSL stylesheet used to save the report. You may want to play with each one to see how the output looks. You can also modify those files if you like so that GFI LANguard N.S.S. saves information differently. For more information on each, look at ***"Saving to Predefined Reports"*** which is the next section of the manual.

Filtering Scan Results

GFI LANguard N.S.S. provides 8 predefined reports.

Default Template

This is the default report format if you don't try customization. It includes all information generated by GFI LANguard N.S.S. in an easy to read format.

The next 7 reports can either be found through customization of a report on saving, or under the **File > Filer Scan Reports for** Option.

High Security Alerts

This report includes:

- all open ports
- missing service packs
- high security alerts (red exclamation mark)

Security Alerts

This report includes:

- all open ports
- all missing hot fixes
- medium security alerts (blue exclamation mark)

Missing Hot Fixes

This report includes:

- missing service packs
- missing hot fixes/patches

Open Ports

This report includes:

- all open ports (TCP and UDP)

Open TCP Ports

This report includes:

- all open TCP ports

SNMP Information

This report includes:

- SNMP information (system oid)

List of Computers

This report includes:

- detailed information for every computer (columnar)

Creating your own Reports

If you want to modify or create new reports you can create new XSL files in the Config\XSL directory under the directory you installed GFI LANguard N.S.S. to.

Any files added to that directory will be listed in **Customize report, Report, Report Stylesheet** – option through the customize option on saving reports. (Look at the picture '*Customizing a GFI LANguard N.S.S. report*' at the beginning of this section.

Once you have created your own report XSL file, you may want to modify the 'custom_reports.xml' file. By adding the entry into that file your new report will be displayed in the **File > Generate Custom Reports** menu entry the next time you startup GFI LANguard N.S.S..

Formatting of the XSL file

GFI LANguard N.S.S. automatically adds these lines to the begin of every XSL file:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<xsl:stylesheet version="1.0"
xmlns:xsl="http://www.w3.org/1999/XSL/Transform">
```

(so you won't have to)

Your custom XSL should start with the template definition: <xsl:template match="/">

To better understand the way GFI LANguard N.S.S. uses the XSL files you can study the existing ones.

Sample Report

The following report will generate a list from your generic save file of just the alerts gathered from your machines and any backdoor Trojan ports found open. In some places sections have been cut out to keep it from running to long. But except for minor changes this is the same basic script as can be found in the Config\xsl directory. It is a modification of the high_security_alerts.xsl file.

all_security_alerts.xsl

```
<xsl:template match="/">
 <body>
  <font face="Verdana, Arial, Helvetica, sans-serif" size="2">
  Scan target :
  <b><xsl:value-of select="hosts/@scan_target"/></b> [
  <b><xsl:value-of select="count(hosts/host)"/></b>
  computers found ]
  </font>
  <hr/>
```

(Note: The above code produces the following output.

Scan target : 192.168.192.1-192.168.199.254 [67 computers found])

```
  <font face="Verdana, Arial, Helvetica, sans-serif" size="3"
color="Black">
  <b>All security alerts report</b><br/></font>
  <font face="Verdana, Arial, Helvetica, sans-serif" size="2"
color="Black">
  This report includes : <br/>
  <ul>
   <li>Just security alerts</li>
  </ul>
  </font>
  <br/>
```

(Note: The above code produces the following output.

All security alerts report
This report includes:

- **Just security alerts)**

```
  <xsl:if test="$show_table=1">
   <!--table begin-->
   <table border="0">
    <tr>
     <th align="middle" bgColor="#3366cc"><font color="#ffffff"
size="2">IP Address</font></th>
     <th align="middle" bgColor="#3366cc"><font color="#ffffff"
size="2">Hostname</font></th>
     <th align="middle" bgColor="#3366cc"><font color="#ffffff"
```

```
size="2">Username</font></th>
      <th align="middle" bgColor="#3366cc"><font color="#ffffff"
size="2">Operating System</font></th>
    </tr>
    <!--each host-->
    <xsl:for-each select="hosts/host">
    <xsl:sort data-type="text" select="os"/>
    <xsl:if test="1">
    <tr>
      <td bgColor="#f0f0f0"><a href="#{ip}"><xsl:value-of
select="ip"/></a></td>
      <td bgColor="#f0f0f0"><xsl:value-of select="hostname"/></td>
      <td bgColor="#f0f0f0"><xsl:value-of select="username"/></td>
      <td bgColor="#f0f0f0">
       <xsl:if test="$show_images=1">
        <img src="{os_image_path}"/>
        <xsl:text disable-output-escaping="yes"> &amp;nbsp;</xsl:text>
       </xsl:if>
      <xsl:value-of select="os"/>
      </td>
    </tr>
    </xsl:if>
    <!--end each host-->
    </xsl:for-each>
  </table>
  <!--table end-->
 </xsl:if>
```

(**Note:** The above code produces the initial table that has IP Address, Hostname, Username, and Operating System and links to the appropriate section in the table below.

Using normal web color codes you can change the background and the font color.)

```
    <!--start details-->
    <xsl:if test="$show_details=1">
    <br/>
    <xsl:for-each select="hosts/host">
    <xsl:sort data-type="text" select="os"/>
    <!--conditional 1=true, 0=false -->
    <xsl:if test="1">
      <A name="{ip}"/>
      <table border="1" cellspacing="0" cellpadding="0"
      style="border-collapse:collapse; mso-border-alt:solid windowtext
.9pt;mso-padding-alt:0in 1.4pt 0in 1.4pt">
      <tr><td width="738" valign="top"
      style="width:7.10in;border:none windowtext
.9pt;background:#3366cc;padding:0in 5.4pt 0in 4.4pt">
      <font color="white">
        <b><xsl:value-of select="ip"/>
        [ <xsl:value-of select="hostname"/> ]
```

```
<font color="yellow">
<xsl:text disable-output-escaping="yes">&amp;amp;nbsp;</xsl:text>
<xsl:value-of select="os"/>
</font>
</b>
</font>
</td></tr>
<td>
<!--alerts title-->
<xsl:if test="$show_alerts = 1">
<xsl:if test="count(alerts/*) > 0">
<A name="{ip}alerts"/>
<br/>
<xsl:for-each select="alerts">
<!--backdoors-->
[cut exact format can be found in high_security_alerts.xsl file]
<!--end backdoors-->
<!--CGI abuses-->
<xsl:for-each select="cgi_abuses/cgi_abuse">
<xsl:if test="level=0 or level=1 or level=2">
```

(**Note:** The above line is the first line that has really been modified between this code and the high_security_alerts.xsl file. We have modified it so that if any alert: 0 – high, 1 – medium, or 2 – informational, is found in the file, it will be saved to the new output.)

```
<table border="0" cellspacing="0" cellpadding="0"
style="border-collapse:collapse; mso-border-alt:solid windowtext
.9pt;mso-padding-alt:3in 1.4pt 0in 1.4pt">
<tr><td width="20"></td>
<td width="200" valign="top"
style="width: 6.70in ;border:none windowtext
.9pt;background:#6f6f6f;padding:0in 5.4pt 0in 4.4pt">
<xsl:if test="$show_images=1">
<xsl:choose>
<xsl:when test="level = 0">
<img src="images/high.bmp"/>
</xsl:when>
<xsl:when test="level = 1">
<img src="images/med.bmp"/>
</xsl:when>
<xsl:when test="level = 2">
<img src="images/low.bmp"/>
</xsl:when>
<xsl:otherwise>
<img src="images/information.bmp"/>
</xsl:otherwise>
</xsl:choose>
<xsl:text disable-output-escaping="yes">
&amp;amp;nbsp;</xsl:text>
</xsl:if>
<font color = "white">
<b>
<xsl:value-of select="name"/><br/>
```

```
</b>
</font>
</td>
</tr>
<tr><td></td>
<td width="738" valign="top"
style="width:4.90in;border:none windowtext
.9pt;background:#f5f5f5; padding:0in 5.4pt 0in 4.4pt">
<xsl:value-of select="impact"/><br/>
<a href="{bugtraq}"><xsl:value-of select="bugtraq"/></a><br/>
</td>
</tr>
</table>
<br/>
</xsl:if>
</xsl:for-each>
<!--end CGI abuses-->
<!--FTP alerts-->
[cut same basic format as the CGI abuses]
<!--end FTP alerts-->
<!--DNS alerts-->
[cut same basic format as the CGI abuses]
<!--end DNS alerts-->
<!--mail alerts-->
[cut same basic format as the CGI abuses]
<!--end mail alerts-->
<!--service alerts-->
[cut same basic format as the CGI abuses]
<!--end service alerts-->
<!--RPC alerts-->
[cut same basic format as the CGI abuses]
<!--end RPC alerts-->
<!--Registry alerts-->
[cut same basic format as the CGI abuses]
<!--end Registry alerts-->
<!--Misc alerts-->
[cut same basic format as the CGI abuses]
<!--end Misc alerts-->
</xsl:for-each>
</xsl:if>
</xsl:if>
<!--end alerts-->
<!--end computer details-->
</td>
</table>
<br/>
</xsl:if>
<!--end each details-->
</xsl:for-each>
</xsl:if>
```

```
   <xsl:element name="HR"/>
   <font face="Verdana, Arial, Helvetica, sans-serif"
size="2"><xsl:value-of select="hosts/@created_on"/></font><br/>
  </body>
</xsl:template>
</xsl:stylesheet>
```

This is a quick modification of an existing XSL file. One main line was modified to get it to check for Alerts 0-2, instead of only one specific alert number. The open ports section was also removed.

There are a number of good books and sites on the Internet to help you better understand and create your own XSL files. And by so doing get GFI LANguard N.S.S. to save output in the format you desire.

As a reminder, once you have created a new xsl file you will also want to modify the custom_reports.xml file in the Config\xsl directory. That way, the next time you restart GFI LANguard N.S.S. you will be able to save directly to your new format through the **File > Generate custom report** menu option.

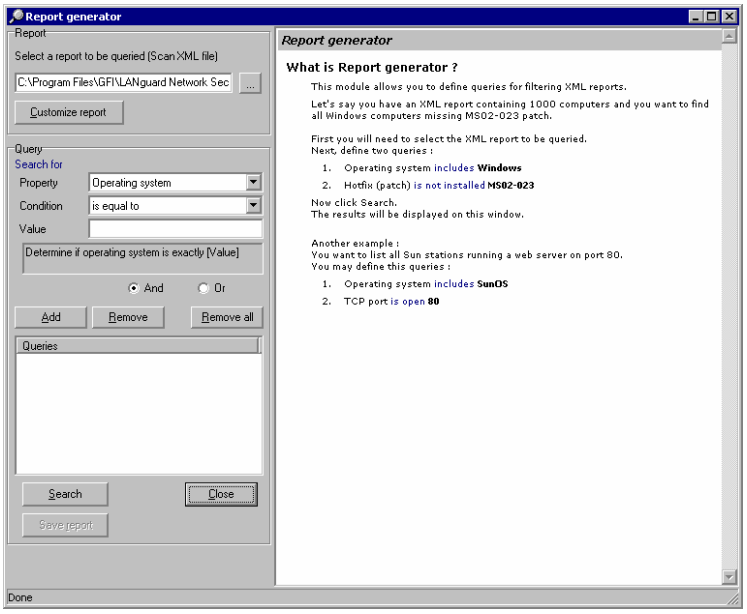
Report Generator

What is the Report Generator

This feature is only available in the registered version of GFI LANguard Network Security Scanner!

This module allows you to define queries for filtering XML reports.

If you click on **File > Query Generator** you will see a window that looks like this:



Example 1

Let's assume you have an XML report containing 1000 computers and you want to find all Windows computers missing MS02-023 patch.

First, select the XML report to be queried.

Next, define two queries:

1. Operating system includes **Windows**
2. Hot fix (patch) is not installed **MS02-023**

Now click **Search**.

The results will be displayed in the window.

Example 2

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**

Now click **Search**.

The results will be displayed in the window.

Example 3

To list all computers that have open ports (Open ports being one of the available templates you can use to generate and save reports for scan results). For this example it will be assumed that the scan results where saved using the generic.xsl (Default template), which saves all information.

1. Select the file you originally saved.
2. Click on customize report.
3. Under 'Report Stylesheet' change that from generic.xsl (Default template) to open_ports.xsl (Open Ports) and click on **Ok** and get sent back to the previous window.
4. Click on **Search** to generate the report.

Conclusion

Example 3 helps to show that you do not need to add specific query information to the report. You can use the predefined XSL files to parse information.

Note: Queries are case sensitive. So if you search for SunOS, that is different than searching for SunOs or SUNOS.

Deploying Patches to Microsoft Machines

Introduction to Deploying Patches

This feature is only available in the registered version of GFI LANguard Network Security Scanner!

The deploy patches feature is a powerful tool to allow you to keep your Windows NT, 2000 and XP machines (including applications) up to date with the latest security patches. This chapter deals with the following:

- Finding out what Hot Fixes and patches are on a machine
- Pushing Hot Fixes and patches that the machine is missing
- Pushing OS Specific Service Packs
- Pushing Custom Patches

For any of these to work, you must have administrative rights to the machine you are scanning. If you don't have the correct rights you will not be able to make a remote connection to the registry, you will not be able to scan for file information and you will not be able to install the patches.

Microsoft SUS & GFI LANguard N.S.S.

Microsoft SUS is a good solution for pushing out operating system patches. However, Microsoft SUS does not have the following features that LANguard N.S.S. does have:

- GFI LANguard N.S.S. can deploy service packs
- GFI LANguard N.S.S. can deploy patches to machines running Windows NT
- GFI LANguard N.S.S. 3.3 can deploy Microsoft application patches and service packs for Microsoft Office, Microsoft SQL Server & Microsoft Exchange Server.
- GFI LANguard N.S.S. can deploy third party software (Example: How to deploy GFI FAXmaker client to many workstations using GFI LANguard N.S.S.)

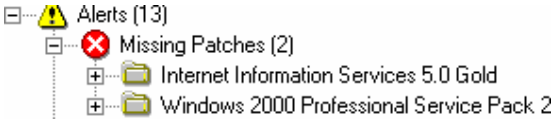
Microsoft SUS has no plans to make SUS support these features. Microsoft's alternative is Microsoft SMS, which is more expensive and quite difficult to use. Therefore, we recommend using Microsoft SUS to keep Windows 2000/XP/.NET machines up to date, and use GFI LANguard N.S.S. for service packs, microsoft application patches & service packs and third party software deployment.

Determining what Hot Fixes or Service Packs are Missing

Before GFI LANguard N.S.S. can determine what Hot Fixes or Service Packs are missing, on a machine, it first must know what Hot Fixes or Service Packs are installed on a machine. GFI LANguard N.S.S. does this by comparing registry settings, file date/time stamps, and version information on the machine, to information provided by Microsoft in their mssecure.xml file.

Once GFI LANguard N.S.S. has compared what products are on the machine it will check for Hot Fixes and Service Packs that are available for that product. Any found missing will be added to the list, and the output generated by GFI LANguard N.S.S..

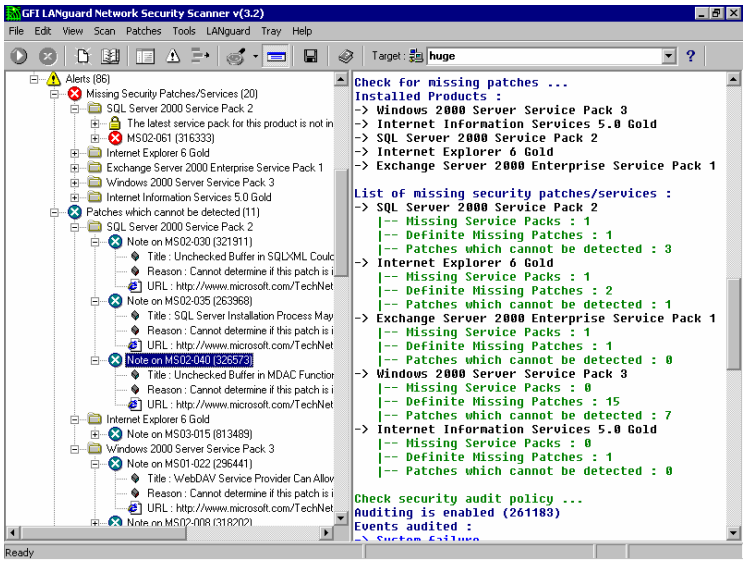
If the machine is missing any patches you should see something like this:



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.

Unidentifiable patches

In some cases, LANguard N.S.S. cannot identify whether a particular patch is installed or not. These particular patches will be reported under a node under alerts called “Patches which cannot be detected”.



Products supported for patching

Products that GFI LANguard N.S.S. will currently look for patches for are:

- Windows NT 4.0
- Windows NT 4.0 Server
- Windows NT 4.0 Enterprise Edition

- Windows 2000 Professional
- Windows 2000 Server
- Windows 2000 Advanced Server
- Windows 2000 Datacenter Server
- Windows XP Home Edition
- Windows XP Professional
- Internet Information Server 3.1
- Internet Information Server 4.0
- Internet Information Server 5.0
- Internet Information Server 5.1
- SQL Server 7.0
- SQL Server 2000
- Internet Explorer 4.0
- Internet Explorer 4.1
- Internet Explorer 5.0
- Internet Explorer 5.01
- Internet Explorer 5.5
- Internet Explorer 6.0
- SQL Server 7
- SQL Server 2000
- Microsoft ISA Server
- Microsoft Exchange 2000 Standard
- Microsoft Exchange 2000 Enterprise
- Microsoft Exchange 5.5
- Office XP
- Office 2000 Developer
- Office 2000 Premium
- Office 2000 Small Business
- Office 2000 Standard
- Office 2000 with Multilanguage Pack

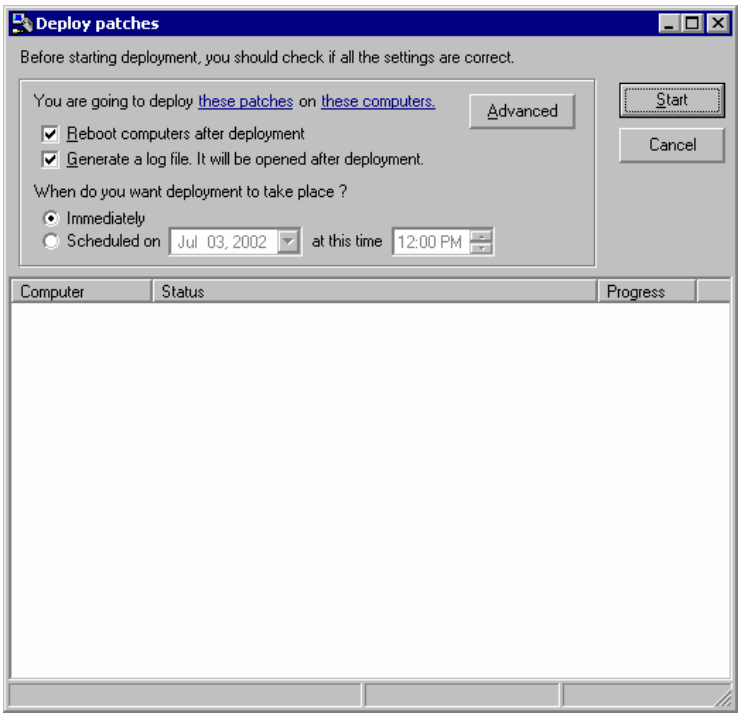
Some of these GFI LANguard N.S.S. can push both Hot Fixes and SP's to, others it can only push Hot Fixes to. This all depends on how Microsoft has packaged their update files. If it is an all inclusive file that can be installed silently GFI LANguard N.S.S. can push it and install it. But if it is a utility that queries the system, asks for user input, and downloads files from the internet, GFI LANguard N.S.S. most likely will not be able to install it (Check the Custom Patch section below).

Installing Hot Fixes on Machines

Note: GFI LANguard N.S.S. can at this point only deploy patches for English windows!

How to Start Deploying Hot Fixes

Once you have a list of Hot Fixes that are missing, you will want to patch these machines. If you right click on a machine that is missing some Hot Fixes and tell it to **Deploy patches to this machine** you will see a window like this:



Deploying patches to a Windows Machine

If you click on the **these patches,** you can modify which patches GFI LANguard N.S.S. pushes to this machine. By default it will push all detectable patches missing to the machine, but there may be reasons for you to only send specific patches to the machine. If that is the case, unselect patches you don't want to install.

If you told GFI LANguard N.S.S. to **Deploy patches to all machines** you can click on **these computers** and see what machines are listed. If there is a machine that you do not want to push patches to you can unselect it there.

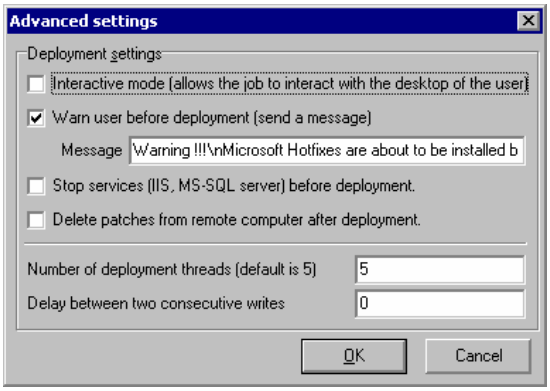
If you want the machines to automatically reboot after you have installed the patches on them, check the box **Reboot computers after deployment**.

In most cases you will want a report generated so you know what GFI LANguard N.S.S. did. If not you can unselect the **Generate a log file…** option.

In some cases you may not want to have these patches install immediately. If you want GFI LANguard N.S.S. to schedule a time on these machines to install and reboot the machines you can specific that information in the scheduling section.

Advanced Options

The advanced button will provide you with a window like this:



Advanced Settings on Patching Windows Machines

In some cases you may not want the patch to automatically install, you may want it to ask the end user at that machine questions. If this is the case you can select the **Interactive mode…** setting here.

Note: Some patches will prompt the user for information, others will install automatically regardless of this setting due to the way the patch was created.

In most cases you will want to warn end users that patches to their machine are about to be pushed and that their machine will reboot. The **Warn user before deployment** option let's you do just that. The default message will tell them that Hot Fixes are about to be installed and that user XYZ on machine ABC is who initiated this. (The username will be whoever is currently logged onto the machine that GFI LANguard N.S.S. is running from.) You can change this message to whatever you want.

Note: This just pops up a message notifying the end user that this is about to happen, this does not give them the opportunity to cancel the patches.

If you are pushing IIS or SQL patches, you should first stop the service before pushing them. The patch may stop the service for you, but it may not. If services are running on the machine that you want to stop, enable the **Stop services** option here.

If hard drive space on the end user machine is an issue, you may want to remove the patch files from the system after it has installed them. If you don't, the original Q files and patches will be left on the end users' machine.

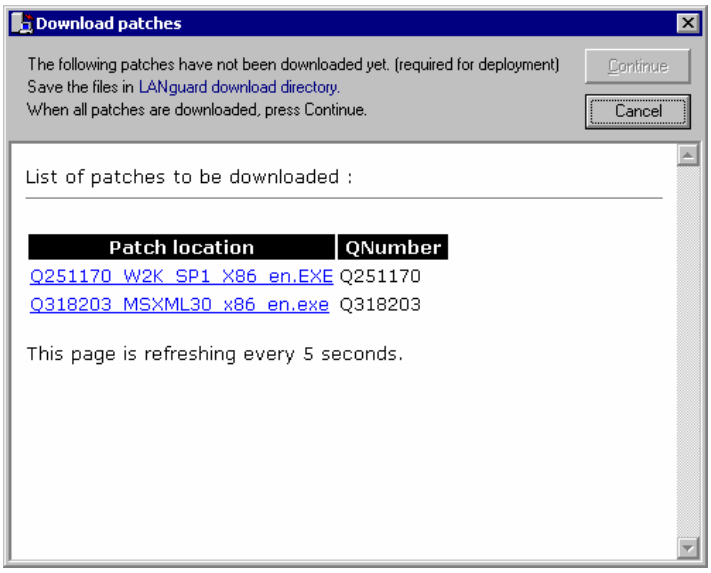
The next two options, the **Number of deployment threads** and **Delay between two consecutive writes** are described below:

- **Number of deployment threads** – This is how many threads are used for deployment. (The more threads you use the faster computers are patched at the same time. But for every additional thread, even though it will increase the speed of patching, it will also increase the network load.)
- **Delay between two consecutive writes** – This is how fast the patches are copied to remote computers. (Ultimately, how long to wait between patches being sent. A small delay will give your network a chance to do other things besides just try to send this patch.)

Both parameters will help in network load issues. It is recommended to leave these set at the default, unless you have a slow network and/or you are seeing problems with the speed of patches being sent out over your network.

Starting the Patch Process

Once you have all of the settings the way you want, you can click **Start**, you will see a window such as this:



Patches still needed to be downloaded

Before you can actually patch the machines you will have to download the patches from Microsoft. GFI LANguard N.S.S. will provide you with a direct link to the file to download when possible, in other cases it will provide you with a link to the main download page for that patch, but you will have to either provide information, or select languages, etc.

Note: Make sure you download the patches to the correct directory. If you change the directory that GFI LANguard N.S.S. is trying to save to, GFI LANguard N.S.S. will not know where the patch is and prompt you to download it again. The patches should be saved into the \download directory under the GFI LANguard N.S.S. installation. **In the case of non-English service packs/patches, you may be indicated to save the files in alternative directories**. It is important that files are placed in the correct directory, otherwise you will not be able to deploy that service pack / patch for non-english operating systems.

Once all patches have been downloaded, click on the **Continue** button. It will start the copy process from your machine to the machines that are to be patched.

Note: You can start the patch process without downloading all of the patches. So make sure that you have downloaded all patches that you want to install on your machines before clicking on the **Continue** button.

GFI LANguard N.S.S. will show you the percentage done on each file that it is copying over to the machine, and then inform you that it is

currently patching the system. Once it is done copying the files and has verified that the patch process has started, it will provide you with a report that shows what it did.

Note: At the time of the report popping up, the patching of the selected machine(s) is probably not complete. Depending on the number of patches, the size of them, and the speed of your network and computers the patching process could be done in as little as a minute or two, or it could last as long as an hour.

Once you believe all machines have been patched and rebooted you should rescan them to verify that the patches were actually installed and registered correctly.

Installing Service Packs on Machines

How to Start Deploying missing Service Packs

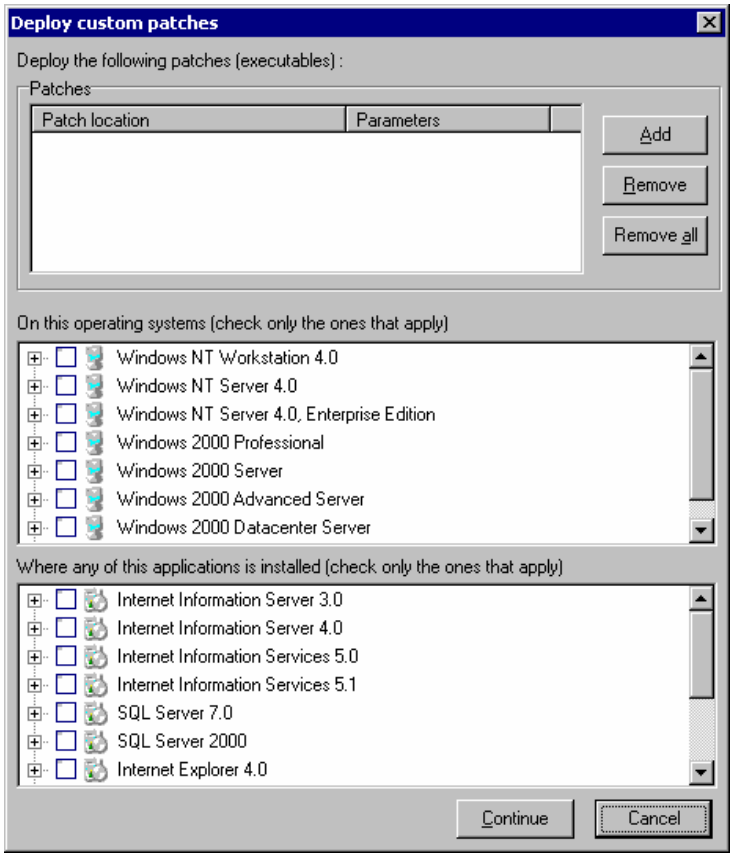
Installing missing Service Packs is just like installing Hot Fixes in the section above. If you right click on a machine that is missing a Service Pack and tell it to **Deploy Service Packs to this machine** it will run you through the exact same windows and prompts as the Hot Fix section, except this time it will only prompt you to download the correct Service Pack for the Machine(s) listed.

Note: You will want to make sure that you have GFI LANguard N.S.S. set to reboot the machine when the Service Pack is done installing. If you do not have GFI LANguard N.S.S. set to reboot the machine, and the machine is patched, and rescanned, it will still show that it is at a previous SP level and that you need Hot Fixes for the previous SP. If you push these Hot Fixes on top of the workstation, you may cause serious issues. So it is recommened to always set the workstation to reboot after a successful push of any type of patche.

Installing Custom Patches on Machines

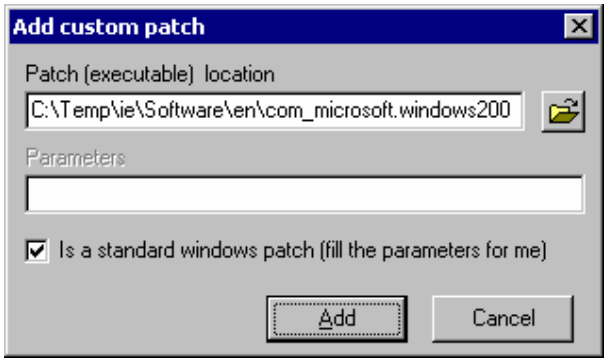
How to Start Deploying Custom Patches

Installing Custom Patches is **NOT SUPPORTED**, but is added for your convenience. The reason it is not supported is that through this utility you can push any type of patch to machines. All Hot Fixes and Service Packs that GFI LANguard N.S.S. officially supports can be pushed through the other features, but it could be that your company requires certain patches be pushed and that this utility will work for you in those cases. For this utility to work, the patch you are pushing, must be able to be run in a silent, or an unattended mode. If you right click on a machine that you want to test this on and tell it to **Deploy Custom Patches to all machines** you will see a window like this:



Note: If you tell it to push to 'this machine' the OS and application options above will be greyed out, this is because GFI LANguard N.S.S. already knows what machine it is pushing to and does not have to try to determine this from any of these options.

The first thing you will need to do is to add the executable you want to push. You can do this by clicking on the add button. Once you do you will see a window like this:



If the patch is a normal windows patch, you can leave the 'Is a standard Windows Patch' option checked and GFI LANguard N.S.S. will supply the parameters for you. If this is a custom patch, or a Microsoft patch that does not conform to their normal standards, you can uncheck this option and provide the needed parameters.

Note: You should be able to push any program that can be installed in silent mode. It does not have to be a Microsoft program, but could be any program that can be installed without operator interaction.

Once you have the patches added to the list that you want to push, you will have to specify the criteria that is used to determine if this patch should be installed. You can do this by checking either the OS or the products that this push of custom patches should apply to.

Example 1: - Installing Windows Media Player 7.1 to all Windows 2000 Professional machines.

Do the initial scan, right click on a machine, and select deploy custom patches to all machines.

Click on Add, locate the Windows Media Player 7.1 installable file (**Note:** This file and any other patches you may wish to install through the custom patch feature, must be located and downloaded without the help of GFI LANguard N.S.S..)

Check the box that says 'Windows 2000 Professional'

Click Continue.

At this point the patching process menus are the same as in Hot Fix and Service Pack patching.

Example 2: - Installing Office 97 SP1 to all Windows 2000 Professional machines.

This is the same as in example one, but is brought up because Office SP's, in certain cases, can be pushed out to workstations. One issue with this arises if you were to try to push SP2 for Office 97. In SP2, MS added a feature to request the Serial Number before it would allow the installation of the patch, because of this, SP2 for Office 97 can not be pushed (unless there is an undocumented way to supply that on a command line interface).

The custom patch feature can be very useful in certain cases, but may not work in others.

Note: If you are going to push a custom patch make sure you test it in multiple circumstances. If the patch fails to install, also try to install the patch in 'interactive mode' which is under advanced options on the Deploy Patches page. Some patches will install in interactive mode that will not install in complete silent mode.

Warning on Patching

Any type of patching should be tested first!

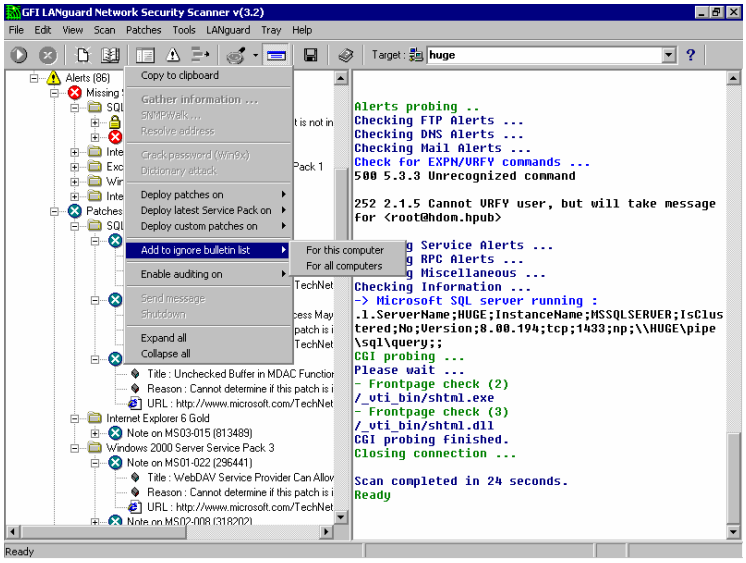
Everyone's environment is different, every computer setup is slightly different and because of this Service Packs and Hot Fixes may not always work as advertised, or may cause other unforeseen problems.

GFI LANguard N.S.S. provides a way to get these patches to the end machine, but as with any patching system, before doing wide spread pushes you should see how vendor specific patches work in your environment. GFI LANguard N.S.S. can help save you time on getting these patches out, but testing these patches on your own can save you even more.

Ignoring patches

It is possible to add patches to an ignore list. This useful in case you do not wish to deploy a certain patch, or because a patch already installed is not detectable or silently installable. It avoids the patch being listed in the patches to be installed node.

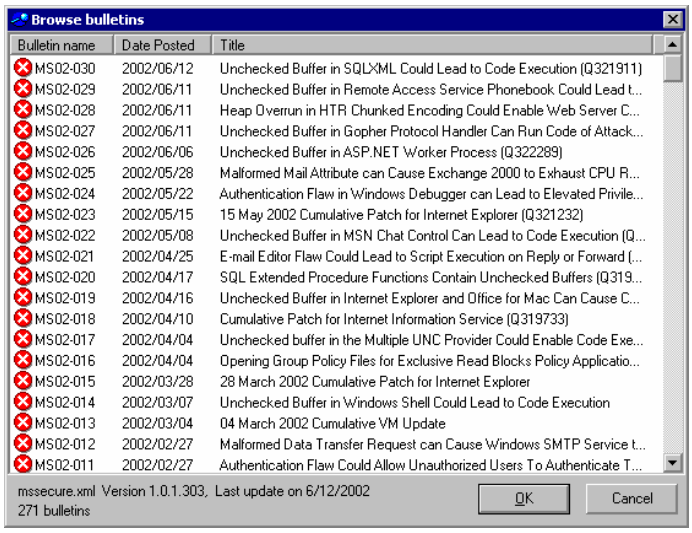
This feature can be accessed by simply right-clicking on the patch in question and selecting add to ignore list as shown in the screenshot below:



Adding a patch to an ignore list

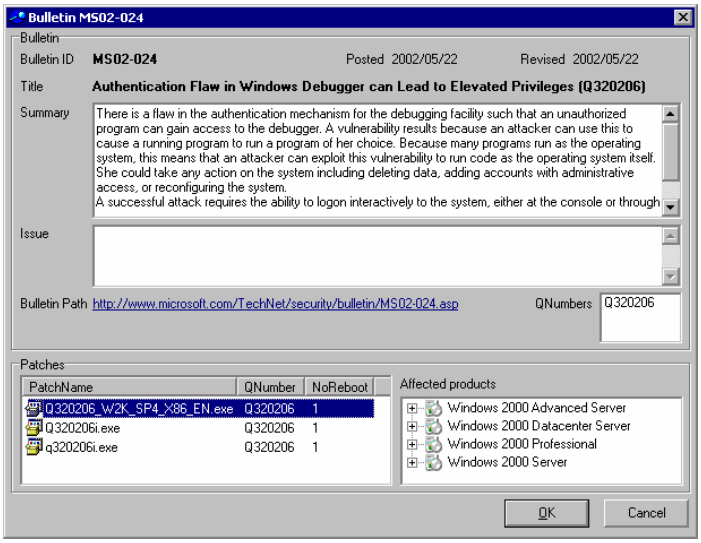
Browsing MS Bulletins

If you would like to find out more about the patches GFI LANguard N.S.S. is going to check for on machines it scans click on **Patches > Browse Bulletins**. This will bring up a window that looks like this:



MS Bulletin Browser

By double clicking on a bulletin you will get a window to popup that tells you about the problem, and what files are needed to patch it. Along with that, you will also be given a path to the web page on Microsoft's site and the original bulletin. It will look something like this:



Specific MS Bulletin

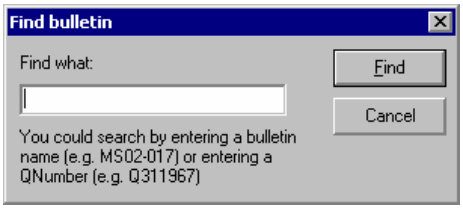
By highlighting a specific patch, GFI LANguard N.S.S. will inform you what products that patch is for. An example of this is q320206_w2k_sp4_x86_en.exe above. It affects Windows 2000 Advanced Server, Data center Server, Professional, and Server.

Note: You can download the patch through this utility. If you double click on the patch (in this case q320206_w2k_sp4_x86_en.exe) it will connect to Microsoft's site and start downloading the Hot Fix.

Finding a specific MS Bulletin

If you need to find information on a specific bulletin you may want to use the Find Bulletin option. It can be found under **Patches > Find Bulletin**.

You will see something like this:



Finding a specific MS bulletin

If you enter the bulletin name, or the Qnumber, GFI LANguard N.S.S. will look this information up for you.

Results Comparison

Why Compare Results?

The Results Comparison, both Interactively and through Scheduled Scans are only available in the registered version of GFI LANguard Network Security Scanner!

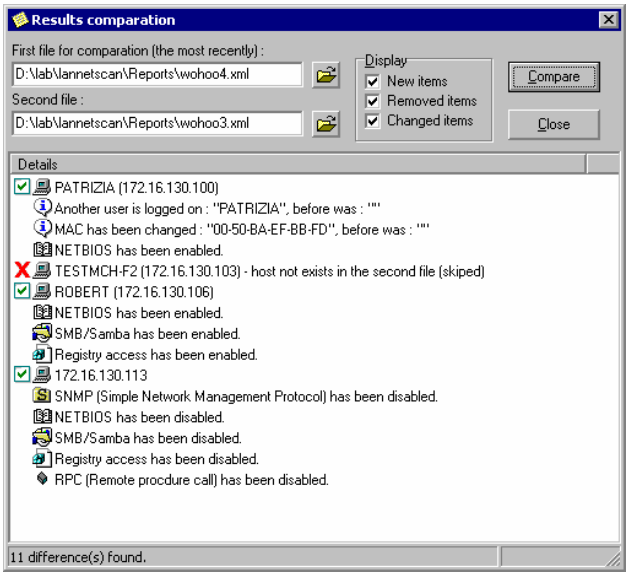
By performing audits regularly and comparing results from previous scans you will get an idea of what security holes continually pop up or are reopened by users. This creates a more secure network.

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, both will be discussed shortly.

Performing a Results Comparison Interactively

When GFI LANguard Network Security Scanner saves the Reports as HTML output, it also saves an XML file that is used in the Results comparison module.

To compare two reports, select **File > Results comparison**. A window will open. Select two files consisting of the same scan at different times, and choose **compare**.



Comparing results

The result should 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 between the two scans.
- Removed items will show any devices that were removed between the two scans.
- Changed items will display anything that has changed, such as a service being enabled or disabled, or new ports being open.
- Alert changes will display any of the alerts that have changed between the scans.

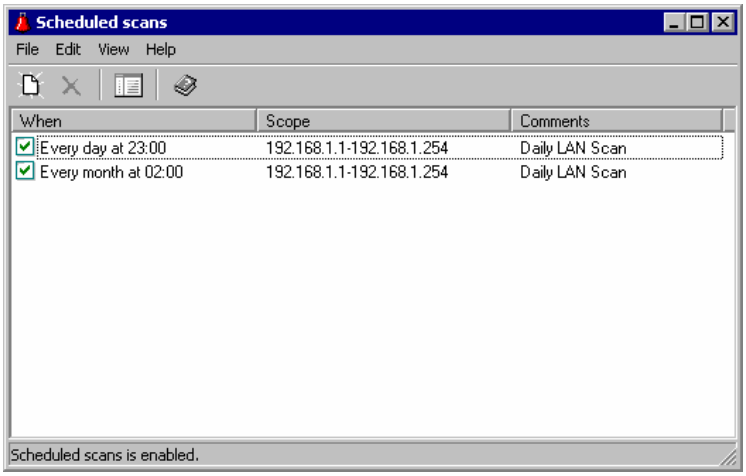
Performing a Comparison with the Scheduled Scans Option

Instead of manually scanning your network each day, week, or month, you can setup a scheduled scan.

Scheduled Scans is a tool for performing scheduled scans and emailing the differences to the administrator. For example: the administrator can instruct Scheduled Scans to perform a scan every night at 23:00. When the time comes, Scheduled Scans will start LANguard Network Security Scanner, scan the selected computer(s) and save the results. Then, it will compare the current results with the results from the night before. Any differences will be emailed to the administrator.

How to Setup a Scheduled Scan

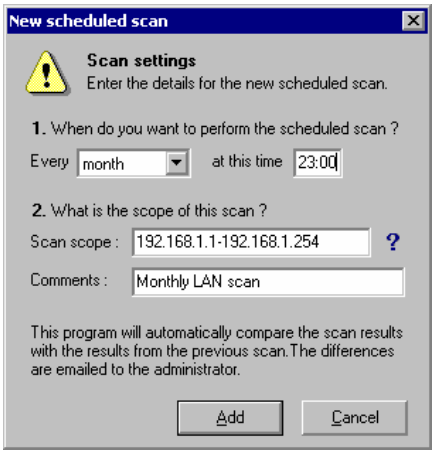
To setup a new Scheduled Scan, from within GFI LANguard N.S.S. click on **Scan > Scheduled Scan** and you will see a window like this:



Scheduled Scan Window

How to Add a New Scan

To add a new scheduled scan click on **File > New** and you will see a window such as:



Adding a new scan to the schedule

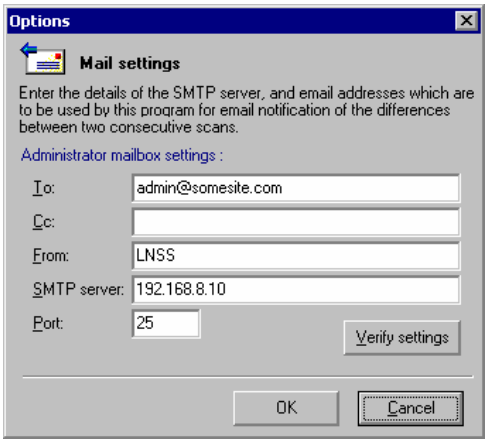
How to Delete a Scheduled Scan

If you decide you no longer want Scheduled Scan to run a specific query you can easily remove the scan by highlighting it, click on **Edit > Remove** (or right click on it, and Remove Scheduled Scan).

How to Modify a Scheduled Scan

If you need to modify a scan all you need to do is highlight it, click on **Edit > Modify** (or right click on it, and Edit Scheduled Scan).

Setting up Mail Configuration Options



Mail configuration settings

You will want to make sure you change the default mail options. To do this:

1. Click on File > Options.
2. A window will open where you can specify the SMTP server address, port to connect to (normally 25), email address to send the information to, and what you want to set as the subject line.
3. In order to verify the settings, you should click Verify settings. If everything is setup correctly you should have a test email message within a few minutes.

Note: Some SMTP gateways will not allow you to leave the from field as just a name, you will need to specify a complete email address such as GFI LANguard N.S.S.@scanner.local Even though this is a fake address it is needed in some cases for SMTP gateways to send the message on. You will have to test your gateway to see how it is configured.

What will happen when it Performs the Scan

When the time comes for a scheduled scan to start GFI LANguard N.S.S. will start performing the scan in the background as configured.

Once it is done it will save the scan information to the Reports\RC directory, under the directory GFI LANguard N.S.S. was installed to. Then it will run a compare on the current scan and the previous scan.

If this is the first time that this has run and there are no other scans to compare it to, or there are no differences between this scan and the previous, GFI LANguard N.S.S. and Scheduled Scan will not email you a notice, because there is nothing that has changed to report to you. *You will only receive a report if something has changed.*

OS Identification

How GFI LANguard N.S.S. determines the OS running on a device

GFI LANguard N.S.S. sends out 3 main types of packets/queries: NETBIOS, SNMP, and ICMP.

First you have how devices respond to SMB packets. Windows and some flavors of Unix will respond to these packets. Windows machines that have File and Print sharing installed on it will give up more info that other machines, so you can normally get a better idea of what the machine is there.

Then you have SNMP, on devices that it is running, in most cases it is a quite reliable source of what the device is. There are a few exceptions where the vendor doesn't do individual ID's for each of its devices and in these cases the OID of the device will pretty much just give you the vendor. But in most cases SNMP can be used to find the type of hardware/OS that is running on the device.

Next you have ICMP packets. This is broken up into 2 main categories.

The first is how the device responds with/to: TTL, Address Mask Request, and Time Stamp Request packets. Based on TTL you can break devices down a bit (128 is normally Windows, 255 usually Unix of some flavor), codes in the reply etc also help in the determination, but OS identification by these methods isn't as reliable because some of these can be changed within the OS, such as TTL.

The 2nd part of the ICMP packets would be on banner grabbing as you connect to a port. In some cases this is very informative about what OS is running, and in other cases no info is provided at all. The problem with this method is that the banner that the OS sends, in most cases, can be changed, so that it either does not give up the information about the OS, or gives out false information.

GFI LANguard N.S.S. does identify quite a few flavors of *nix. The problem with almost all Unix type OS's is that the IP stacks of most of them are the same at least with the tests GFI LANguard N.S.S. does (TTL, Address Mask Reply, Info Request Reply, Time Stamp Reply). There are some minor differences, but that only lets you break them down into groups. Even the Macintosh falls into the same IP stack issues. Therefore, identification of these types of OS's has to be done via SMB, SNMP or banner grabbing. Depending on what ports are open and what has been put into the fingerprinting files (which is discussed in the next section) the information to identify the OS might be in there, but it might not.

So GFI LANguard N.S.S. uses all of this, plus a few other tricks, to determine what OS is running on a device. In most cases the OS that

GFI LANguard N.S.S. determines is correct, but there is always a possibility of error.

Fingerprinting Files

This section will deal with the text files used by GFI LANguard N.S.S. to help it determine the type of device it finds.

All of the files listed below are located in the Fingerprint directory under the installation directory of GFI LANguard N.S.S.. You can modify them if you want, but be aware that mis-configured information entered there will affect the reliability of GFI LANguard N.S.S. when determining the type of device it has found.

RPC Services

When RCP services are found running on a machine (normally Unix or Linux) the information received back is compared to the file rpc.txt, which can be found and modified under **View > RPC.txt**.

SNMP Object ID Information

When LANguard Network Security Scanner finds a device that responds to SNMP queries it compares the Object ID information on the device to that stored in GFI LANguard N.S.S.. This information can be updated and/or viewed by going to **View > Object_ids.txt**.

SNMP Enterprise Numbers

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

The name of the file used here is enterprises.txt.

Banner Information

GFI LANguard N.S.S. also bases OS identification off of the banners it retrieves from devices when it connects to certain ports. Those Ports/Services are:

- FTP (ftp.txt)
- Indentd (indentd.txt)
- SMTP (smtp.txt)
- Telnet (telnet.txt)
- HTTP (www.txt)

If, when connecting to these ports, a banner is displayed, GFI LANguard N.S.S. compares that to its own list and will use this information to determine the OS or type of device it has found.

LANS: LANguard Scripting

What is LANS?

LANS is a scripting language for LANguard Network Security Scanner. It has been designed for writing security checks to be used in the Alerts module. It includes an editor with syntax highlighting capabilities and a debugger.

IMPORTANT NOTE: GFI cannot offer any support in the analysis of scripts that you have created that are not working. Therefore the LANguard scripting feature is unsupported.

LANS Syntax

Comments:

Comments are prefixed with # character. Anything after # is ignored by the interpreter.

```
i = 1 # this is a comment
# another comment
```

Variables:

Variables must be declared before use. Currently, LANS has two variable types: **string** and **integer**. Multiple variables can be declared on a single line.

```
string   str1,                                    str2
integer          i1,i2,j
```

Warning: Variables cannot be initialized when they are declared. The following is incorrect:

```
string   str1 = "test"  !!! incorrect
```

Numbers can be specified in decimal or hexadecimal base. Hexadecimal numbers must be prefixed with **$**. (C like hexadecimal declaration (0x) is not supported.)

```
integer          i1,i2,j
i1 = 100
i2 = $3f
j = 0x3f  !!! incorrect
```

String variables must be double quoted.

```
string   str1, bad
str1 = "a sample string"
bad = 'some string'  !!! incorrect
```

String variables can also be initialized with the notation:

```
stringVar = {hexnumber1, hexnumber2, hexnumber3, ... }
```

an example of this is:

```
string stringVar

stringVar = {$41, $42, $43} # "ABC"
# you could also do this:
stringVar = stringVar + "DEF" + {$13, $10} # "ABCDEF" + end_of_line
```

String variables can also be indexed. Therefore, stringVar[1] returns the first character from the string variable stringVar.

```
string stringVar

stringVar = "ABC"
echo(stringVar[1])
```

Output:

```
A
```

Lines

Long expressions can be split on several lines using this operator: ****

```
string get_names

get_names = \
{$01, $f8, $00, $10, $00, $01, $00, $00, $00, $00,\
 $00, $00, $20, $43, $4B, $41, $41, $41, $41, $41,\
 $41, $41, $41, $41, $41, $41, $41, $41, $41, $41,\
 $41, $41, $41, $41, $41, $41, $41, $41, $41, $41,\
 $41, $41, $41, $41, $41, $00, $00, $21, $00, $01}
```

Operators

The following operators are supported under LANS:

Arithmetic and Boolean operators

Operator	Operation	Operand types
+	addition	integer, string
-	subtraction	integer
*	multiplication	integer
/	division	integer
&	and	integer
|	or	integer
^	xor	integer
>>	shr - shift right	integer
<<	shl - shift left	integer

Relational operators

Operator	Operation	Operand types
=	equal	integer, string
>	greater than	integer
<	less than	integer

>=	greater than or equal	integer
<=	less than or equal	integer
<>	not equal	integer, string

If Statements

Format**:**

if *expression*
  statement1
  statement2
 ...
[**else** *expression*
  statement1
  statement2
  ...]
end if

```
if size > 0
  echo("size is greater than 0")
else
  echo("size equal with 0")
else if
```

While Statements

Format**:**

while *expression*
  statement1
  statement2
 ...
end while

```
i = 1
while i < 10
  i = i + 1
end while
```

Using LANS Scripts with the Alerts Module

When a LANS script gets executed from LANguard Network Security Scanner an important string variable _**ip** is set with the IP address of the currently scanned computer. Another important variable is the integer variable _**return**. The _**return** value should be set before the end of the script. The value of this variable determines if the check was successful or not. (1=success. 0=failure)

For a detailed example, check the First LAN Script Example at the beginning of the next section.

Default Variables

Important variables

Variable	Description
_ip	Contains the IP address of the currently scanned computer
_return	Should be set to 1 if the check is successful, 0 otherwise

Less important variables

Variable	Description
_eol	End of line. Equal to CR+LF.
_hostname	Contains the hostname of the currently scanned computer

First LANS Script

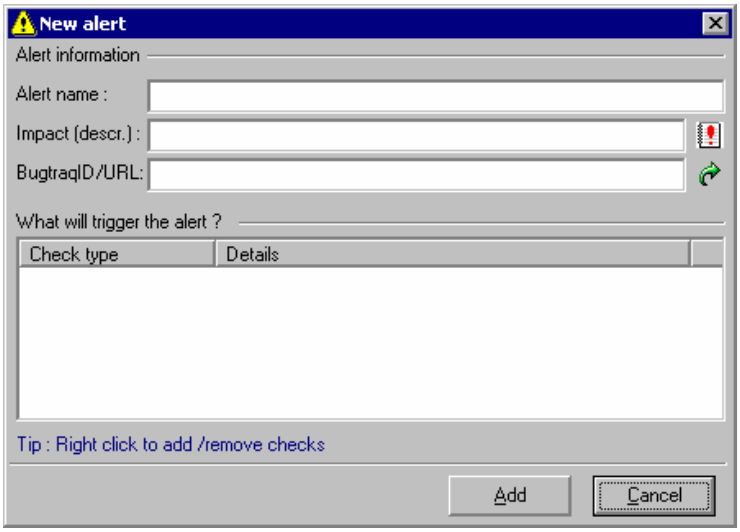
Defining a New Alert

This tutorial will demonstrate how to write a simple security check using LANS. We will create a security alert for checking the following bug: "Solaris Fingerd Discloses Complete User List" There is a bug in the finger service, which will make it display the list of accounts, when this request is issued:

finger "a b c d e f g h"@solaris_host

First we need to create a new alert. Let's click **Configure Alerts** button from the toolbar.

Next, we must select the category where the alert will be located. Select **Miscellaneous** and the list of alerts from this category will be displayed. We need to create a new alert here. Select **New alert** from the file menu. The following window should be displayed:



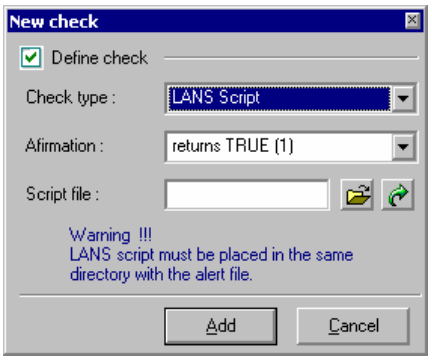
New Alert Window

Now fill in the following fields.

1. **Alert name:** Solaris Fingerd Discloses Complete User List (sample)
2. **Impact:** Sensitive information disclosure
3. **BugtraqID/URL:** http://www.securiteam.com/unixfocus/6B00M0U2UW.html (this URL contains more information regarding this bug)
4. **Checks:** We will add three checks:

- Operating system is Solaris, SunOS
- TCP port 79 (finger) is open
- A LANS script for checking the bug

We will concentrate on the third check. (**LANS script**)



New check alert

Provide a name for the script (in this case solaris_finger.lans)

Click **Open script in LANS** to start writing the code. The LANS editor will open up. This is what we want to do**:**

The Script

```
1.# Solaris finger bug '@a b c d e f g h'
2.string          request, data, fdata
3.integer         sock
4.#_ip = "192.168.8.10"
5._return = 0
6.echo("ip= " +_ip,_color_green)
7.request = "a b c d e f g h" + _eol
8.sock = open_tcp(_ip, 79)
9. if sock > 0
10.   send(sock, request)
11.   fdata = ""
12.   data = "1"
13.   while length(data) > 0
14.    data = recv(sock, 256)
15.    fdata = fdata + data
16.   end while
17.   echo(fdata)
18.   if pos("nobody", fdata) > 0
19.    _return = 1
20.   end if
21. end if
```

Note: Line numbers are added for clarity and descriptive purposes only. They would not exist in the actual script.

How this Script Works?

Explanation of how this script works:

```
1.# Solaris finger bug '@a b c d e f g h'
```

This line describes what the scripts purpose is. Observe the # character prefixing the actual text. This character is used for adding comments or remarks.

```
2.string    request, data, fdata
3.integer   sock
```

The next two lines are used for declaring variables to be used in the script. We declare three string variables: request, data, fdata and one integer variable sock.

- **request** will contain the finger request data to be sent
- **data** will be used as a temporary buffer
- **fdata** will contain the response from server
- **sock** will contain the socket handle

```
4.#_ip = "192.168.8.10"
```

Default variable _**ip** is initialized with a custom value “192.168.8.10”. This line is commented out in the actual script, but it is useful to force a connection to a specific machine during script development and testing. So for testing purposes you would want to change this variable to a machine running this vulnerability and uncomment it.

```
5._return = 0
```

Default variable _**return** is initialized with 0 (or false for now). The _**return** variable will contain the check result when it leaves the script. (**True** – the check was successful or **false** – the check failed).

```
6.echo("ip= " +_ip,_color_green)
```

This is added for testing. It will display the current IP address in the color green.

```
7.request = "a b c d e f g h" + _eol
```

This is the initialization of the string variable _**request**. Observe the _**eol** (end of line) variable, it is used as a replacement for the following:

```
_eol = chr(13) + chr(10)
```

```
8.sock = open_tcp(_ip, 79)
```

This initializes a TCP connection on port 79 (finger). It returns a handler to the recently created socket, or zero if the connection could not be established.

At this point we have two different possible situations:

1. The connection is established
2. The connection could not be established

Therefore, we must use a conditional statement, in this case “**if**”. We are only interested in the first case where the connection is established. So we write:

```
9. if sock > 0
   ...
21. end if
```

We check to see if we have a valid socket handle. If we do:

```
10.send(sock, request)
```

This will send our request to the finger service.

```
11. fdata = ""
12. data = "1"
13. while length(data) > 0
14.   data = recv(sock, 256)
```

```
15.  fdata = fdata + data
16. end while
```

Now we read the response from the finger service. We use a temporary buffer to hold the data. (We read 256 characters at once). We keep reading until the **data** variable is empty and there is nothing left to read. The complete response will be contained in the **fdata** variable.

```
17. echo(fdata)
```

This will display the response in the debug window. It should contain some interesting information.

```
18.  if pos("nobody", fdata) > 0
19.   _return = 1
20.  end if
```

At this time we have the finger response. Now we have to check if it contains valid information. A list of users should contain the **nobody** account. So, we check to see if it is contained inside of the response. We use the pos function for this task. If the magic word is found (nobody), then we have a vulnerable computer and we instruct LANguard Network Security Scanner to mark our check as successful by setting the **_return** variable to 1 (or true).

Save the script in the same directory with the alert file "Alerts\Miscellaneous" and we are done.

Sample output (slightly modified):

```
Login      Name              TTY         Idle   When    Where
root       Super-User        pts/3         hostname1
daemon          ???                      < .  .  .  . >
bin             ???                      < .  .  .  . >
sys             ???                      < .  .  .  . >
adm        Admin             pts/4         hostname2
lp         Line Printer Admin             < .  .  .  . >
uucp       uucp Admin                     < .  .  .  . >
nuucp uucp Admin                          < .  .  .  . >
listen     Network Admin                        < .  .  .  . >
nobody Nobody                             < .  .  .  . >
noaccess No Access User                   < .  .  .  . >
nobody4  SunOS 4.x Nobody                 < .  .  .  . >
smb        SMB guest account              < .  .  .  . >
...
...
```

Other Samples

There are over 20 sample scripts for you to look at and use to help better understand LANS. They can be found in the folder "Sample LANS Scripts" under the directory where GFI LANguard N.S.S. is installed.

Network Functions

Function Open_tcp

Opens a TCP connection with a remote computer.

Usage:

integer open_tcp (**string** ip, **string** port)

Remarks:

This returns a handler to the recently created socket or zero if the connection could not be established.

Example:

```
integer  sock
sock = open_tcp("192.168.8.10", "80")
if sock > 0
  echo("port 80 is open")
else
  echo("port 80 is closed")
end if
```

Output:

port 80 is closed

See Also:

Close, Send, Recv

Function Open_udp

Opens a UDP socket for sending datagrams.

Usage:

integer open_udp ()

Remarks:

This returns a handler to the recently created socket or zero if the connection could not be established.

Example:

```
integer  sock
sock = open_udp()
if sock > 0
  echo("UDP socket is open.")
  close(sock)
end if
```

Output:

UDP socket is open.

See Also:

Close, SendTo, RecvFrom

Function Close

Used to close a socket. Can be used for either TCP or UDP sockets.

Usage:

close (**integer** sock)

Example:

```
integer  sock
sock = open_tcp("192.168.8.10", "80")
if sock > 0
  echo("port 80 is open")
  close(sock)
```

```
else
  echo("port 80 is closed")
end if
```

Output:

port 80 is open

See Also:

Open_tcp, Open_udp

Function Recv

Receives data through a socket. (TCP sockets only)

Usage:

string recv (**integer** socket, **integer** size)

Remarks:

If no data is received through the socket, the function will timeout and return a null string.

Example:

```
integer  sock
string   data

sock = open_tcp("192.168.8.10", "13")
if sock > 0
  echo("port 13 (daytime) is open")
  data = recv(sock, 1024) # receive maximum 1024 bytes
  if length(data) > 0
    echo(inttostr(length(data)) + " bytes received: " + data)
  else
    echo("no data")
  end if
  close(sock)
else
  echo("port 13 (daytime) is closed")
end if
```

Output:

port 13 (daytime) is open
20 bytes received: 8:27:57 PM 1/7/2002

See Also:

Send

Function Send

Sends data through a socket. (TCP sockets only)

Usage:

integer send (**integer** socket, **string** data [, **integer** size])

Remarks:

If the size parameter is not specified, the whole string will be sent.

Example:

```
integer  sock, sent
string data
```

```
data = "some data"
sock = open_tcp("192.168.8.10", "7")
if sock > 0
  echo("port 7 (echo) is open")
  sent = send(sock, data)
  echo(inttostr(sent) + " bytes sent.")
  close(sock)
else
  echo("port 7 (echo) is closed")
end if
```

Output:

port 7 (echo) is open 9 bytes sent.

See Also:

Recv

Function RecvFrom

Receives data through a socket. (UDP sockets only)

Usage:

string recvfrom (**integer** socket, **integer** size)

Remarks:

If no data is received through the socket, the function will timeout and return a null string.

Example:

```
integer  udp_sock
string   data

# open udp socket
udp_sock = open_udp()
if udp_sock > 0
  sendto(udp_sock, "192.168.8.10", "13", "");
  echo("now receiving ...")
  data = recvfrom(udp_sock, 1024) # receive maximum 1024 bytes
  if length(data) > 0
    echo(inttostr(length(data)) + " bytes received: " + data)
  else
    echo("no data")
  end if
  close(udp_sock)
else
  echo("unable to create the udp socket")
end if
```

Output:

now receiving ...
20 bytes received: 8:43:11 PM 1/7/2002

See Also:

SendTo

Function SendTo

Sends data through a socket. (UDP sockets only)

Usage:

integer sendto (**integer** socket, **string** ip, **string** port, string data [, **integer** size])

Remarks:

If the size parameter is not specified, the whole string will be sent.

Example:

```
integer  udp_sock, sent
string   data

data = "some data"
udp_sock = open_udp()
if udp_sock > 0
  echo("sending data through socket")
  sent = sendto(udp_sock, "192.168.8.10", "7", data)
  echo(inttostr(sent) + " bytes sent.")
  close(udp_sock)
else
  echo("unable to create the socket.")
end if
```

Output:

```
sending data through socket
9 bytes sent.
```

See Also:

RecvFrom

Lookup Functions

Function DnsLookup

Resolves a hostname to its corresponding IP address.

Usage:

string dnslookup (**string** hostname)

Remarks:

If the hostname cannot be resolved, a null string is returned.

Example:

```
# DNS functions test
string    hostname, ip

hostname = "trinity" # my desktop computer
ip = dnslookup(hostname)
if ip <> ""
  echo("hostname: " + hostname)
  echo("resolved as: " + ip, _color_blue)
  # now backwards:)
  hostname = ReverseDnsLookup(ip)
  if hostname <> ""
    echo("back to: " + hostname,)
  end if
else
  echo("unable to resolve " + hostname + " !", \
   _color_red)
end if
```

Output:

```
hostname: trinity
resolved as: 192.168.8.10
back to: TRINITY
```

See Also:

ReverseDnsLookup

Function ReverseDnsLookup

Resolves an IP address to its corresponding hostname.

Usage:

string ReverseDnsLookup (**string** ip)

Remarks:

If the IP address cannot be resolved, a null string is returned.

Example:

```
# DNS functions test
string    hostname, ip

hostname = "trinity" # my desktop computer
ip = dnslookup(hostname)
if ip <> ""
   echo("hostname: " + hostname)
   echo("resolved as: " + ip, _color_blue)
   # now backwards:)
   hostname = ReverseDnsLookup(ip)
   if hostname <> ""
      echo("back to: " + hostname,)
   end if
else
   echo("unable to resolve " + hostname + " !", \
    _color_red)
end if
```

Output:

```
hostname: trinity
resolved as: 192.168.8.10
back to: TRINITY
```

See Also:

DnsLookup

Function WhoIs

Performs a WhoIs query.

Usage:

string whois (**string** query, [**string** whois_server, [**string** port]])

Remarks:

If no WhoIs server is specified, LANS will try to find a valid server from your query string. This may or may not work.

Example:

```
# whois function test
string query, server, data

# whois server (my test whois server)
server = "163.342.244.228"
```

```
# query for bogdan
query = "bogdan"
# perform the query
data = whois(query, server)
# display the response (if valid)
if length(data) > 0
  echo(data)
end if
```

Output:

SWHOISD 2.0

Searching for bogdan. Found 1 record(s) matching bogdan.

Person:	(Handle JD1-FOOBAR)
Name:	Bogdan Calin
Email address:	cooly@foobar.com
Address:	6083 Foobar Ave., San Diego, CA 92121
Country:	US
Telephone:	858-853-1212
FAX No:	858-555-1977
Created:	Sat Jun 23 01:57:22 PDT 2001
Last Updated:	Sat Jun 23 01:57:22 PDT 2001

Note:

To single out one record, look it up with "!XXX", where XXX is the handle

See Also:

DnsLookup

SNMP Functions

Function SnmpGet

Wrapper for SNMP get request. Returns the value for a specified OID (object id). For more information, you should consult the sample script **snmp_test.lans**.

Usage:

integer snmpget (**string** ip, **string** oid, **string** community_string, **string** string_variable)

Remarks:

string_variable is the name of the variable that will receive the result. This variable should be specified between parentheses. (see example)

Example:

```
# snmp functions test
string  ip
string  oid,res # object ids, results

ip  = "192.168.8.20"
oid = "1.3.6.1.2.1.1.1.0" # system Description
# perform snmpget
if snmpget(ip, oid, "public", "res") = 1
  # display the information (if valid)
  if length(res) > 0
```

```
    echo(oid + " = " + res)
  end if
end if
```

Output:

1.3.6.1.2.1.1.1.0 = Hardware: x86 Family 6 Model 11 Stepping 1 AT/AT COMPATIBLE - Software: Windows 2000 Version 5.1 (Build 2600 Uniprocessor Free)

See Also:

SnmpGetNext

Function SnmpGetNext

This is a wrapper for SNMP getnext request. Returns the name for the next OID (object id). For more information, you should consult the sample script **snmp_test.lans**.

Usage:

integer snmpgetnext (**string** ip, **string** oid, **string** community_string, **string** string_variable)

Remarks:

string_variable is the name of the variable that will receive the result. This variable should be specified between parentheses. (see example)

Example:

```
# snmp functions test
string  ip
string  oid,res # object ids, results

ip  = "192.168.8.20"
oid = "1.3.6.1.2.1.1.1.0" # system Description
# perform snmpget
if snmpgetnext(ip, oid, "public", "res") = 1
  # display the information (if valid)
  if length(res) > 0
    echo("current oid: " + oid)
    echo("next oid is: " + res)
  end if
end if
```

Output:

current oid: 1.3.6.1.2.1.1.1.0
next oid is: 1.3.6.1.2.1.1.2.0

See Also:

SnmpGet

Function SnmpSet

Wrapper for SNMP set request. Set the value for a specified OID (object id). For more information, you should consult the sample script **snmpset_test.lans**.

Usage:

integer snmpset (**string** ip, **string** oid, **string** community_string, **string** value, **integer** valueType)

Remarks:

value is the value to be set.

valueType is the value type.

Currently you can only use these types:
  _**snmp_string** - for writing string values
  _**snmp_integer** - for writing integer values

Example:

```
# snmp functions test
# snmpset implementation in LANS
string  ip
string  oid, res # object id
string  read_comm, write_comm, value

read_comm  = "public"
write_comm = "private"
value      = "LANS was here"
ip  = dnsLookup("trinity")
# sysContact
oid = "1.3.6.1.2.1.1.4.0"
# let's check the current value
if snmpget(ip, oid, read_comm, "res") = 1
   # display the information (if valid)
   if length(res) > 0
      echo(oid + " = " + res)
   end if
end if
if length(res) > 0
 echo("trying to set ... ", _color_navy)
 # perform snmpset (before set)
 if snmpset(ip, oid, write_comm, value, _snmp_string) = 1
    echo("value was set (OK)", _color_blue)
 else
    echo("unable to set value", _color_red)
 end if
 # let's verify if the value was set
 if snmpget(ip, oid, read_comm, "res") = 1
    # display the information (if valid)
    if length(res) > 0
       echo(oid + " = " + res)
    end if
 end if
else
 echo("unable to read value", _color_red)
end if
```

Output:

```
1.3.6.1.2.1.1.4.0 = blade@trinity
trying to set ...
value was set (OK)
1.3.6.1.2.1.1.4.0 = LANS was here
```

See Also:

SnmpGet

String Functions

Function Length

Returns the number of characters in a string.

Usage:7

integer length (**string** str)

Example:

```
echo(length("Sample string"))
```

Output:

13

See Also:

Left, Right

Function Pos

Returns the position of a substring within a string.

Usage:

integer pos (**string** substring, **string** str)

Remarks:

Returns the index value of the first character from substring or 0 if the substring is not found.

Example:

```
echo(pos("string", "Sample string"))
```

Output:

8

See Also:

RegExp

Function Left

Returns the first **count** number of character(s) from a string.

Usage:

string left (**string** str, **integer** count)

Example:

```
echo(left("Sample string", 6))
```

Output:

Sample

See Also:

Right

Function Right

Returns the last **count** characters from a string.

Usage:

string right (**string** str, **integer** count)

Example:

```
echo(right("Sample string", 6))
```

Output:

string

See Also:

Left

Function Delete

Removes a substring from a string.

Usage:

string delete (**string** str, **integer** index, **integer** count)

Example:

```
string x
x = "how are you ?"
echo(x)
x = delete(x, 5,4)
echo(x, _color_red)
```

Output:

how are you ?
how you ?

See Also:

Pos

Function Uppercase

Returns a copy of a string in uppercase.

Usage:

string uppercase (**string** str)

Example:

```
echo(uppercase("cool"))
```

Output:

COOL

See Also:

Lowercase

Function Lowercase

Returns a copy of a string in lowercase.

Usage:

string lowercase (**string** str)

Example:

```
echo(lowercase("COOL"))
```

Output:

cool

See Also:

Uppercase

Function Ord

Returns the ordinal value for a character.

Usage:

integer ord (**String** char)

Example:

```
echo("ASCII code for 'a': " + inttostr(ord("a")))
```

Output:

ASCII code for 'a': 97

See Also:

Chr

Function Dup

Returns a string equal with **str_or_char** duplicated **n** times.

Usage:

string dup (**string** str_or_char, **integer** n)

Remarks:

This is useful for testing buffer overflows.

Example:

```
string test_dup
test_dup = dup("za", 10)
echo(test_dup)
```

Output:

zazazazazazazazazaza

See Also:

Str

Function Chr

Returns the character for a specified ASCII value.

Usage:

string chr (**integer** value)

Example:

```
string  end_of_line
# compose EOL (end of line)
end_of_line = chr(13) + chr(10)
echo("cool" + end_of_line)
```

Output:

cool

See Also:

Ord

Function Mid

Returns **n** characters from text starting with **p** position.

Usage:

string mid (**string** text, **integer** p, **integer** n)

Example:

```
string  test
test = "welcome"
echo(mid(test, 1, 3))
```

Output:

wel

See Also:

Trim

Function Trim

Trims the leading and trailing spaces and control characters from text.

Usage:

string trim (**string** text)

Example:

```
string  before_trim, after_trim
before_trim = "  test string  "
echo("-" + before_trim + "-")
after_trim = trim(before_trim)
echo("-" + after_trim + "-")
```

Output:

- test string -

-test string-

See Also:

Mid

Conversion Functions

Function StrToInt

Converts a string that represents an integer to a number.

Usage:

integer strtoint (**string** str)

Example:

```
string str
str = "150"
echo(strtoint(str) * 2)
```

Output:

300

See Also:

IntToStr

Function IntToStr

Converts an integer to a string.

Usage:

string inttostr (**integer** value)

Example:

```
integer year

year = 2002
echo("Year: " + inttostr(year))
```

Output:

```
Year: 2002
```

See Also:

StrToInt

Function IntToHex

Returns hexadecimal representation of a number.

Usage:

```
string inttohex (integer number, integer number_of_digits)
```

Example:

```
integer number

number = 255
echo(inttohex(number, 2))
```

Output:

```
FF
```

See Also:

StrToInt

Function Base64Encode

Encode a string into Base64.

Usage:

```
string base64encode (string input)
```

Example:

```
# base64 test
string input

input = "how are you ?"
echo("Original string: " + input)
input = base64encode(input)
echo("Encoded: " + input, _color_red)
input = base64decode(input)
echo("Decoded: " + input)
```

Output:

```
Original string: how are you ?
Encoded: aG93IGFyZSB5b3UgPw==
Decoded: how are you ?
```

See Also:

Base64Decode

Function Base64Decode

Decode a Base64 encoded string.

Usage:

```
string base64decode (string encoded_string)
```

Example:

```
# base64 test
string input

input = "how are you ?"
echo("Original string: " + input)

input = base64encode(input)
echo("Encoded: " + input, _color_red)

input = base64decode(input)
echo("Decoded: " + input)
```

Output:

```
Original string: how are you ?
Encoded: aG93IGFyZSB5b3UgPw==
Decoded: how are you ?
```

See Also:

Base64Encode

Registry Functions

Function RegistryRead

Read the contents of a specified key from the registry. (local or remote)

Usage:

integer registryRead (**string** computer, **string** reg_path, **string** reg_key, **string** string_variable)

Remarks:

computer can be an IP address or a hostname. LANS automatically prefixes the value of this variable with "\\" so you don't have to.

string_variable is the name of the variable that will receive the result. This variable should be specified between parentheses. (see example)

Example:

```
# registry test
# read Internet Explorer version from registry
string    ip, path, key, version

ip   = dnsLookup("freedom")
path = "SOFTWARE\Microsoft\Internet Explorer\Version Vector"
key  = "IE"
if  length(ip) > 0
   if registryRead(ip, path, key, "version") > 0
      echo("Internet Explorer version: " \
      + version, _color_blue)
   end if
end if
```

Output:

```
Internet Explorer version: 6.0000
```

Miscellaneous Functions

Function RegExp

Evaluate a regular expression.

Usage:

integer regexp (**string** regex, **string** text_to_evaluate)

Remarks:

LANS is using the TRegExpr library written by Andrey V. Sorokin. If you want to know more about TRegExpr you should go to http://anso.da.ru.

Example:

```
# will match Solaris ftp servers with this versions:
# 2.6, 2.7, 2.8 and 5.6, 5.7, 5.8
regex = "FTP server \(SunOS (2|5)\.[678]\) ready"
text_to_match  = "220 mars FTP server (SunOS 5.7) ready."
if regexp(regex, text_to_match) = 1
  echo(text_to_match + " matched")
else
  echo(text_to_match + " not matched !")
end if
text_to_match  = "220 mars FTP server (SunOS 5.5) ready."
if regexp(regex, text_to_match) = 1
  echo(text_to_match + " matched")
else
  echo(text_to_match + " not matched !!!")
end if
```

Output:

```
220 mars FTP server (SunOS 5.7) ready. Matched
220 mars FTP server (SunOS 5.5) ready. not matched !!!
```

Function Sleep

Suspend the execution of the current script for some amount of time (in milliseconds).

Usage:

sleep (**integer** time)

Example:

```
echo("wait a minute ...")
sleep(1000)
```

Output:

wait a minute ... (and then a 1000 ms pause will happen)

Function Echo

Display text in the debug window. You can optional use a color.

Usage:

echo (**string** text, [**integer** color])

Remarks:

Color could be one of the following:

- _color_black
- _color_red
- _color_green
- _color_blue
- _color_purple
- _color_silver
- _color_yellow

Or it could be specified as RGB pair: $1F11FF.

Example:

```
string  text

text = "welcome"
# display text
echo(text)
# display text using red color
echo(text, _color_red)
# display text using $1F11FF color
echo(text, $1F11FF)
```

Output:

```
Return value = welcome
Return value = welcome
Return value = welcome
```

See Also:

Mid

Function StatusBar

Display a message on status bar.

Usage:

statusbar (**string** message)

Example:

```
string  text

text = "welcome"
# display text
echo(text)
# display text on status bar
statusbar(text)
```

Output:

```
welcome
```

See Also:

Echo

Procedure WriteToLog

Writes text to LANS log file (lans_log.txt).

Usage:

writetolog (**string** text)

Example:

```
string info
```

```
info = "Some information"
writetolog(info)
```

See Also:

Echo

Future Plans for LANS

- Increase the interaction between LANS and GFI LANguard N.S.S. (e.g. allowing LANS scripts to interact directly with the scanning window such as add/modify/delete fields, status bar,
- Add the capability to forge IP packets and a nice packet editor

Credits

- TSynEdit (http://synedit.sourceforge.net)
- TRegExpr - Author: Andrey V. Sorokin

Additional Tools and Features

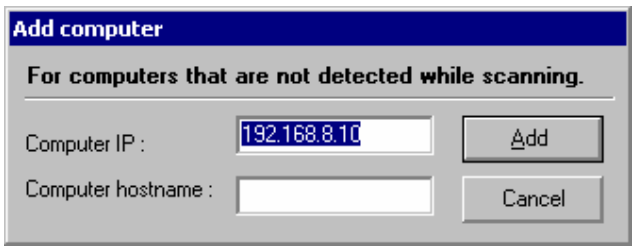
Introduction

This chapter describes additional features that can be found under the Edit Menu

- Add Computer
- Remove Computer
- Find Computer
- Sort Computers
- The following Tools can be found under the Tools Menu
- DNS Lookup
- WhoIs Client
- Trace Route
- SNMP Walk
- SNMP Audit
- MS SQL Server Audit
- Enumerated Computers

Add Computer

If you want to add one specific device to the output window you can do that with the add computer feature.



Adding a computer by hand to be scanned

Once you have added a computer to the list you will need to highlight it and right click on it, then tell LANguard Network Security Scanner to **Gather Information** on this device.

Remove Computer

If you decide that you don't want LANguard Network Security Scanner to gather information from a device, you can remove it by highlighting it and then going to **Edit > Remove Computer**.

Or if you have already scanned it, but do not want it to show up in the reports, you can do the same thing.

Find Computer

Once you have done a scan of your network and want to find a specific device you can use the Find Computer Option.

It will give you the option to find by Hostname, IP Address, MAC Address, or Username.

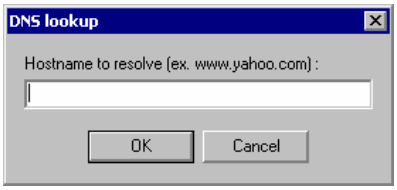
Note: This only scans through information that LANguard Network Security Scanner has in the display. It does not go out on your network looking for this information.

Sort Computers

This option tells LANguard Network Security Scanner how to sort the devices once it has completed its scan. You can sort by IP Address, Hostname, or by Operating System.

DNS lookup

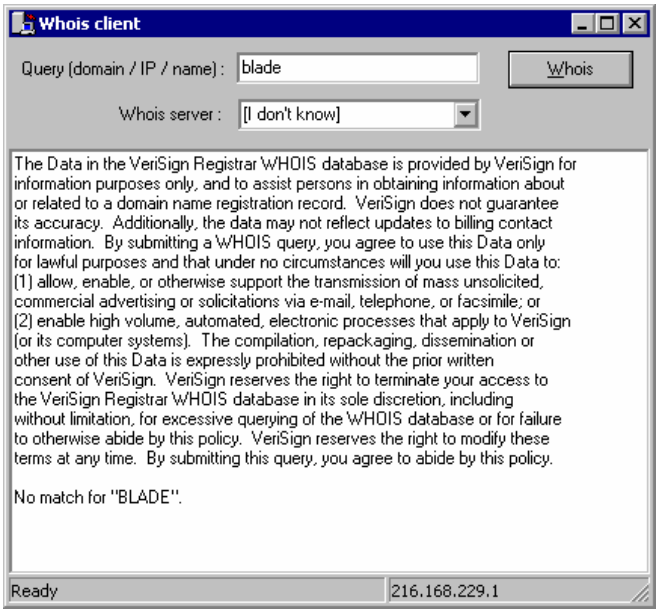
This tool resolves the Domain Name to a corresponding IP address.



Performing a DNS lookup

WhoIs Client

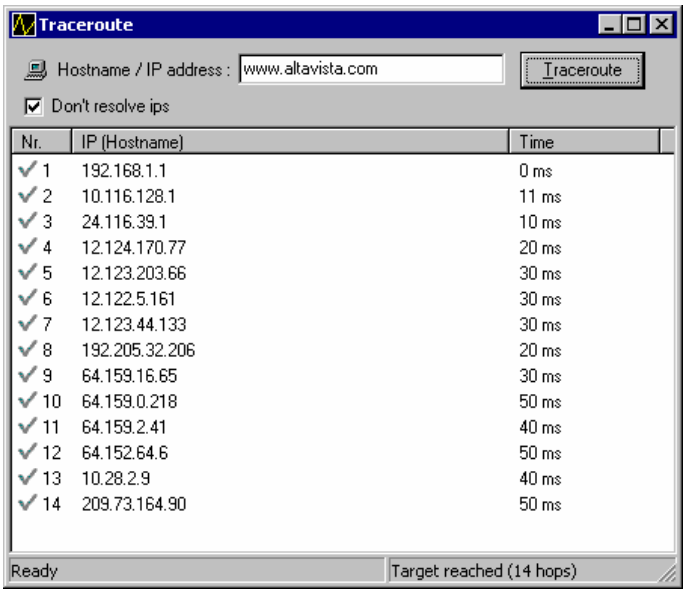
This tool will lookup information on a domain, IP address, or a name. You can select a specific WhoIs Server, or you can use the 'Default' option which will select a server for you



Performing a WhoIs lookup

Trace Route

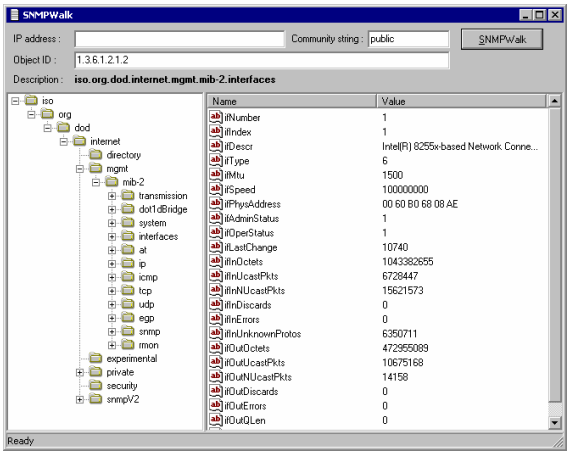
This tool shows the network path that GFI LANguard N.S.S. followed to reach the target machine.



Performing a trace route

SNMP Walk

SNMP will help malicious users to 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 walk

To access this feature, right click on the target computer and select SNMP walk, this will only be available if SNMP is running on the machine. Once you start the SNMP walk, the right pane will contain 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.

If you just want to startup the utility on its own, click on **Tools > SNMP walk**. If you start it in this format you will have to input the IP address on your own.

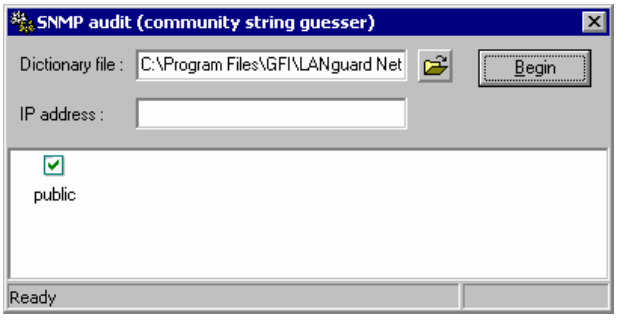
Note: In most cases SNMP should be blocked at the router/firewall so that Internet users cannot SNMP scan your network.

SNMP Audit

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

Some network devices will have alternative or non-default community strings. The dictionary file should contain 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.

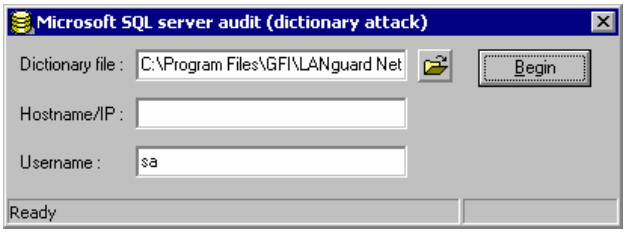


Performing a SNMP audit

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

MS SQL Server Audit

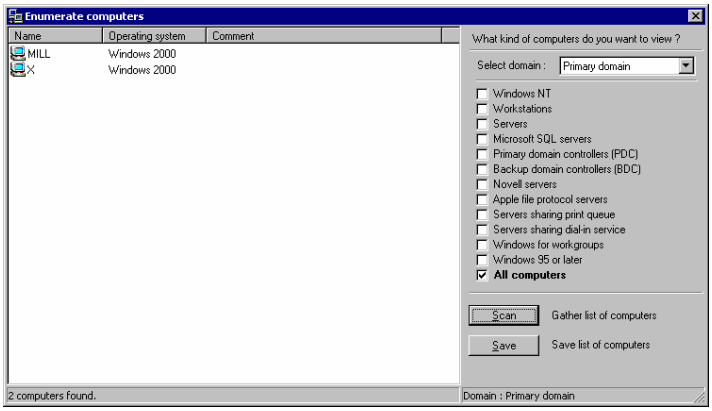
This tool allows you to perform an audit on a machine running MS SQL server. By default it will use the dictionary file called passwords.txt. You can either add new passwords to this file, or direct the utility to another file completely.



Performing a MS SQL audit

To use the utility, input the IP address of a machine running MS SQL, provide the Username you wish to try to get in as, and click begin.

Enumerated Computers



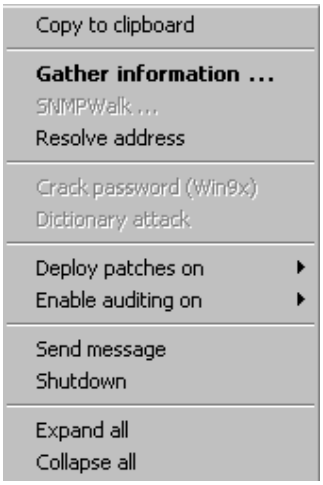
Enumerated Computers

This utility will search your network first for a list of all 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.

Additional Scan Functions

Additional Scan Functions

After you have performed a scan of a network or of a machine, you can right click on the computer to bring up the additional scan functions menu.



Right-click on a computer for additional scan functions

Copy to Clipboard

This option will copy the information selected to the clipboard.

Gather Information

This option allows you to perform more detailed scanning. If the option has been turned off (from the **Scan > Options** dialog), you can gather more information on a per computer basis by right-clicking the target computer and selecting **Gather Information**.

SNMP Walk

This feature is enabled when a host has SNMP running on it. It enables GFI LANguard N.S.S. to "walk through" a SNMP service, which will reveal a lot of information, such as enumeration of open ports, services running, and so on.

It is described in more detail in the ***"Additional Tools"*** section of the manual.

Resolve Address

This option allows you to resolve the address of a computer. If the option has been turned off (from the **Scan > Options** dialog), you can resolve the address on a per computer basis by right-clicking the target computer and selecting **Resolve Address**.

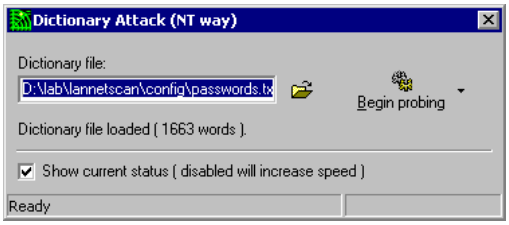
Crack Password (Win9x)

A vulnerability in Windows 95/98/ME NETBIOS allows malicious users to easily and systematically crack passwords. This option will only be available if the target machine is running Windows 95/98/ME. For more information about this problem check out:

http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/Q273/9/91.ASP&NoWebContent=1

Dictionary Attack

To test password strength, right-click on a share and select dictionary attack. This will check a share for weak passwords. The user that is selected to logon can be specified from the **Scan > Options > Cracking tab**. Passwords are specified in a password list. You can add more passwords to the file passwords.txt, or specify a different dictionary file.



Performing a Dictionary attack

If you turn off the **Show current status** it will increase the speed at which this utility works. This is because of the extra time it takes to write to the screen.

This option is tied to the **Scan > Options > Cracking Tab**, **Which username will be used for cracking:** For more information on this look at the ***"Scan Options"*** part of the manual on Cracking.

Configure the Password file

When scanning for weak passwords, GFI LANguard N.S.S. will use passwords included in the passwords.txt file. You can add more passwords to this file by opening it up and adding passwords. You can open the password.txt file from the GFI LANguard N.S.S. directory, or simply from the View menu.

Deploy Patches on ->

This allows you to deploy patches to an individual or all machines.

It is described under the ***"Deployment of Microsoft Patches"*** section of the manual.

It is only available when right clicking on a machine if that machine is a machine that can be patched (I.E. Microsoft NT/2000/XP machine).

Deploy latest Service Pack on ->

This allows you to deploy OS Service Packs to an individual or all machines.

It is described under the ***"Deployment of Microsoft Patches"*** section of the manual.

It is only available when right clicking on a machine if that machine is a machine that can be patched (I.E. Microsoft NT/2000/XP machine).

Deploy Custom Patches on ->

This feature is added for the user, but is NOT supported by GFI. In some cases there may be patches that you want to push, but that GFI LANguard N.S.S. does not officially support. If the patch can be pushed and run in an unattended mode the odds are you should be able to use this feature to install it.

This allows you to deploy any type of patch or SP to an individual or all machines.

It is described under the ***"Deployment of Microsoft Patches"*** section of the manual.

It is only available when right clicking on a machine if that machine is a machine that can be patched (I.E. Microsoft NT/2000/XP machine).

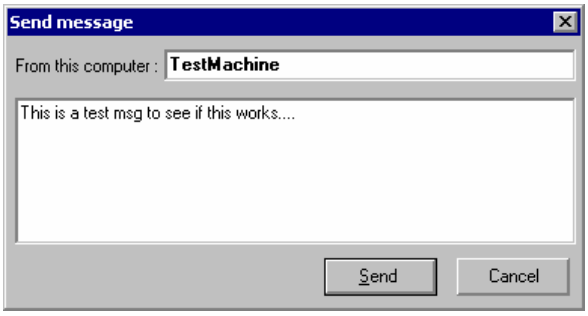
Enable Auditing on ->

Described under the ***"Analyzing Scan Results > Audit"*** section of the manual.

Send Message

This option allows GFI LANguard N.S.S. to send NETBIOS Messenger messages with a spoofed source IP address.

This option could allow social engineering attacks.



Sending a spoofed message

Note: In some cases the sending of messages to workstations will fail. The Microsoft Client not being installed on the machine could cause this, or other utilities used to block messaging. If the message was sent successfully it will tell you that the message was sent.

Shutdown

This does a Remote Shutdown on the machine. This will work if the user running GFI LANguard N.S.S. has the privileges to shutdown the target machine.

Badly configured permissions, either local or network, could allow this operation to succeed on machines that normally should not allow it.

Command Line Syntax

How to use GFI LANguard N.S.S. from the Command Line

For those of you who may want to run GFI LANguard N.S.S. from a script or batch file here is the format of the command line syntax:

languard [custom_ini_file.ini] <target> <output_file> [tray]

- Anything in []'s is optional
- Anything in <>'s is required

You have the ability to specify a specific INI file for GFI LANguard N.S.S. to use. If you don't specify one, the default one will be used.

You also have the ability to cause GFI LANguard N.S.S. to run minimized in the tray with the [tray] option.

The target format is the same as when running GFI LANguard N.S.S. through the GUI. It can be input as a hostname, IP address, IP range, or a list of computers.

Examples:

languard alpha output.html

languard 192.168.8.10 output.html

languard 192.168.8.10-192.168.8.20 output.html

languard file:list_of_computers.txt output.html

languard ping_them_all.ini file:list_of_computers.txt output.html

languard ping_them_all.ini file:list_of_computers.txt output.html tray

The same basic information can be obtained by running languard /? from the command line while in the directory GFI LANguard N.S.S. is installed in.

Warnings

Introduction

When GFI LANguard N.S.S. is run it will, or at least should, alarm any administrators who regularly check their logs that an attack of some sort has happened!

IDS Software

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.

Shared Administration

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.

Security Software

Every effort has been taken to ensure that this product will help you find security holes, missing patches, etc. on your network. But, no Security Software is 100% reliable. New attack methods come out every day, so be aware that even if you appear to be safe today, tomorrow you may not. Scan often and stay up on security alerts!

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 – accessible from the GFI website.
3. The GFI support site.
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, generates automatically a series 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 webchat

You may also request support via Live support (webchat). 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

Index