GFI LANguard 9

Manual

By GFI Software Ltd.



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

GFI LANguard is copyright of GFI SOFTWARE LTD. 2000-2009 GFI SOFTWARE LTD. All rights reserved.

Last updated: 4TH September 2009 Version: LANSS-ACM-EN-01.00.00

Contents

1.	Introd	uction	1
	1.1 1.2 1.3	Introduction to GFI LANguard GFI LANguard components Vulnerability management strategy	1 1 2
2.	Step 1	: Performing an audit	3
	2.1 2.2 2.3 2.4 2.5 2.6	Introduction Network Scanning options Quick Scan Full Scan Custom scan Setting up a scheduled scan	3 4 5 6 7 10
3.	Step 2	: Analyzing the security scan results	17
	3.1 3.2 3.3 3.4 3.5 3.6 3.7 3.8 3.9 3.10 3.11	Introduction Scan summary Vulnerability level rating Detailed scan results Detailed scan results: Vulnerability assessment Detailed scan results: Network & Software Audit Displaying and sorting scan categories Saving scan results Scan filters Results comparison Reporting	17 17 18 19 21 28 30 31 37 40
4.	Step 3	: Fixing vulnerabilities	43
	4.1 4.2 4.3 4.4 4.5 4.6 4.7	Introduction Patch management Deploying missing updates Deploying custom software Uninstall applications Remote remediation Automatic Remediation	43 45 46 51 54 55 56
5.	GFI LA	ANguard dashboard	59
	5.1 5.2 5.3	Introduction Viewing the global security threat level Monitoring scheduled activity	59 59 60
6.	Config	guring GFI LANguard	63
	6.1 6.2 6.3 6.4 6.5 6.6	Introduction Scheduled Scans Computer profiles Applications inventory Application auto-uninstall Configuring Microsoft updates	63 63 65 67 69 71

	6.7 6.8 6.9	Configuring alerting options Database maintenance options Importing and Exporting Settings	75 75 81
	6.10	Program updates	82
7.	Scann	ing Profiles	87
	7.1 7.2 7.3 7.4 7.5 7.6 7.7 7.8 7.9 7.10 7.11 7.12	Introduction Scanning profile description Creating a new scanning profile Configuring vulnerabilities Configuring patches Configuring TCP port scanning options Configuring UDP port scanning options Configuring system information retrieval options Configuring the attached devices scanning options Scanning for USB devices Configuring applications scanning options Configuring the security scanning options	87 87 92 93 100 102 103 104 105 108 109 113
8.	Utilitie	S	115
	8.1 8.2 8.3 8.4 8.5 8.6 8.7 8.8 8.9	Introduction DNS lookup Traceroute Whois Enumerate computers Enumerate users SNMP Auditing SNMP Walk SQL Server Audit	115 115 117 118 119 121 122 123 123
9.	Using	GFI LANguard from the command line	125
	9.1 9.2 9.3 9.4	Introduction Using 'Insscmd.exe' - the command line scanning tool Using 'deploycmd.exe' - the command line patch deployment tool Using 'impex.exe' - the command line import and export tool	125 125 127 128
10	Adding	g vulnerability checks via custom conditions or scripts	131
	10.1 10.2 10.3 10.4	Introduction GFI LANguard VBscript language GFI LANguard SSH Module Python scripting	131 131 134 136
11.	Miscel	laneous	139
	11.1 11.2 11.3 highe 11.4	Introduction Enabling NetBIOS on a network computer Installing the Client for Microsoft Networks component on Windows 20 er140 Configuring Password Policy Settings in an Active Directory-Based Do	139 139 00 or main 142
	11.5	Viewing the Password Policy Settings of an Active Directory-Based Do	main 147
12	12.1		149
	12.1 12.2 12.3	About OVAL About CVE	149 149 150
13	Troubl	eshooting	153
	13.1 13.2	Introduction The Troubleshooting wizard	153 153

13.3	Knowledge Base	155
13.4	Web Forum	155
13.5	Request technical support	155
13.6	Build notifications	156

Index

1. Introduction

1.1 Introduction to GFI LANguard

GFI LANguard is a security scanning, network auditing and remediation application that enables you to scan and protect your network through:

- Identification of system and network weaknesses using a comprehensive vulnerability check database, which includes tests, based on OVAL, CVE and SANS Top 20 vulnerability assessment guidelines.
- Auditing of all hardware and software assets of your network, enabling you to create a detailed inventory of assets. This goes as far as enumerating installed applications as well as USB devices connected on your network.
- Enabling automatic download and remote installation of service packs and patches for Microsoft operating systems and third party products as well as automatic un-installation of unauthorized software.

1.2 GFI LANguard components

GFI LANguard is built on an architecture that allows for high reliability and scalability, which caters for both medium to larger sized networks.

GFI LANguard consists of the following components:

GFI LANguard management console

The management console is the GUI through which all GFI LANguard administration and functionality is accessed including:

- Triggering of network security scans, patch deployment and vulnerability remediation sessions.
- Viewing of saved and real time security scan results.
- Configuration of scan options, scan profiles and report filters.
- Use of specialized network security administration tools.

GFI LANguard attendant service

GFI LANguard attendant, is the background service that manages all scheduled operations including scheduled network security scans, patch deployment and remediation operations.

GFI LANguard patch agent service

GFI LANguard patch agent is the background service that handles the deployment of patches, service packs and software updates on target computers.

GFI LANguard Script Debugger

The GFI LANguard Script Debugger is the module that allows you to write and debug custom scripts using a VBScript-compatible language.



Screenshot 1 - GFI LANguard script debugger

Use this module to create scripts for custom vulnerability checks through which you can custom-scan network targets for specific vulnerabilities.

GFI LANguard script debugger is accessible from **Start** ► **Programs** ► **GFI LANguard 9.0** ► **GFI LANguard Script Debugger**.

1.3 Vulnerability management strategy

It is recommended to use the following sequence for an effective vulnerability management strategy:

1. Scan: For more information, refer to the <u>Step 1: Performing an</u> <u>audit</u> section in this manual.

2. Analyze: For more information refer to the <u>Step 2: Analyzing the</u> <u>security scan results</u> section in this manual.

3. Remediate: For more information, refer to the <u>Step 3: Fixing</u> <u>vulnerabilities</u> section in this manual.

2. Step 1: Performing an audit

2.1 Introduction

Security scans/audits enable you to identify and assess possible risks within a network. Auditing operations imply any type of checking performed during a network security audit. This includes open port checks, missing Microsoft patches and vulnerabilities, service information, user or process information and more.

Overview of the scanning process

The automated scanning process has three distinct stages.

Stage 1	
Determine availability	Determining whether target computers, is
of target computer	reachable and available for vulnerability scanning.
	This is determined through connection requests,
	sent in the form of NETBIOS queries, SNMP
	queries and/or ICMP pings.
Stage 2	
Establish connection	Establish a direct connection with the target
with target device	computer, by remotely logging on to it. To execute
	a scan, GFI LANguard must logon target
	computers with administrator privileges.
Stage 3	
Execute vulnerability	Execute the vulnerability checks configured within
checks	the selected scanning profile and identify present
	security weaknesses.

2.2 Network Scanning options

GFI LANguard includes default configuration settings that allow you to run immediate scans soon after the installation is complete.



Screenshot 2 – Scan Options

GFI LANguard ships with preconfigured scanning options. These options are located in the **Network Audit** tab, which opens by default every time that the GFI LANguard management console is launched.

Parameters preconfigured in these default-scanning options include the scan profile. Scan profiles are a collection of vulnerability checks that determine what vulnerabilities will be identified and which information will be retrieved from scanned targets.

The default scanning options provide quick access to the following scanning modes:

- Quick scan: Scanning mode set to audit target computers for system information and high security vulnerabilities only (including missing Microsoft updates). The scanning profile used in this scanning option is by default set to 'High Security Vulnerabilities'.
- **Full scan:** Scanning mode set to audit target computers for system information and all possible security vulnerabilities. The scanning profile used in this scanning option is by default set to 'High Security Vulnerabilities'.
- Launch a custom scan: Scanning mode, which allows you to configure (on the fly) the parameters to be used during a scan. Configuration is wizard assisted and configurable parameters

include scanning profile. For more information on how to execute a custom scan, refer to the <u>Custom scans</u> section in this manual.

• Set up a scheduled scan: Scanning mode, which allows you to audit target computers at configurable time intervals. For more information on how to set scheduled scans, refer to <u>Scheduled</u> <u>scans</u> section in this manual.

Important notes

1. If Intrusion Detection Software (IDS) is running during scans, GFI LANguard will set off a multitude of IDS warnings and intrusion alerts in these applications. If you are not responsible for the IDS system, make sure to inform the person in charge about any planned security scans.

2. In most cases, vulnerability scans will generate different event log entries across diverse systems e.g. UNIX logs and web servers logs will all detect GFI LANguard scans as intrusion attempts triggered from the computer running GFI LANguard.

3. To successfully execute a scan, GFI LANguard must remotely logon to target computers with administrator privileges.

4. For large network environments, a Microsoft SQL Server/MSDE database backend is recommended instead of the Microsoft Access database.

5. When submitting a list of target computers from file, ensure that file contains only one target computer name per line.

2.3 Quick Scan

During a quick scan, GFI LANguard will analyze target computers and retrieve setup information and missing updates including:

- Missing Microsoft Office patches
- Missing Microsoft Windows service packs
- System information (Software) including OS details and settings, open ports and open shares.
- System information (Hardware) including Network card details (e.g. MAC address) and any USB devices connected.

Quick Scans have relatively short scan duration times compared to the Full Scan – mainly because only a subset of the entire vulnerability checks database is performed. It is recommended to run a Quick Scan at least once a week.

When to use Quick Scans?

It is recommended to use Quick scans:

- When performing a first time scan since these provide in a very timely fashion, a sample of the information that GFI LANguard can extract from target computers.
- To run daily network audits of multiple network machines since it is non-intrusive and does not overload network infrastructure/bandwidth.
- To retrieve system information and to scan only for high security vulnerabilities.

2.3.1 How to launch a Quick Scan

To run a quick scan:

1. Launch the GFI LANguard management console from **Start** ► **Programs** ► **GFI LANguard 9.0** ► **GFI LANguard**.

2. From the **Network Audit** ► **Scan** tab which opens by default, click on the **Quick Scan** option.

3. Specify the target computer to be scanned by selecting one of the following options:

- Scan this computer Use this option to scan local host.
- Scan another computer Use this option to scan a specific computer. Parameters required are target computer name or IP.
- Scan entire domain/workgroup Use this option to scan the domain/workgroup to which your local host is joined.

4. Click Next.

5. Specify the credentials that GFI LANguard will use to logon to target computers. GFI LANguard must logon to target computers with administrator privileges.

6. Click **Scan** to start the process.

2.4 Full Scan

During a full scan, GFI LANguard will scan target computers to retrieve setup information and identify all security vulnerabilities including:

- Missing Microsoft updates
- System information (Software) including unauthorized applications, incorrect anti-virus settings and outdated signatures.
- System information (Hardware) including modems and USB devices connected.

Due to the large amount of information retrieved from scanned targets, Full Scans tend to often be lengthy. It is recommended to run a Full Scan at least once every 2 weeks.

When to use Full Scans?

It is recommended to launch Full Scans:

- At least once every 2 weeks to run network audits on multiple network machines.
- To retrieve system information and to scan targets for all vulnerabilities.
- Whenever new threats emerge.
- Whenever suspicious activity is noticed.

2.4.1 How to launch a Full Scan

1. Launch the GFI LANguard management console from **Start** ► **Programs** ► **GFI LANguard** 9.0 ► **GFI LANguard**

2. From the **Network Audit** ► **Scan** tab which opens by default, click on the **Full Scan** option.

3. Specify the target computer to be scanned by selecting one of the following options:

- Scan this computer Use this option to scan local host
- Scan another computer Use this option to scan a specific computer. Parameters required are target computer name or IP.
- Scan entire domain/workgroup Use this option to scan the domain/workgroup to which your local host is joined.
- 4. Click Next.

5. Specify the credentials that GFI LANguard will use to logon to target computers. GFI LANguard must logon to target computers with administrator privileges.

6. Click **Scan** to start the process.

2.5 Custom scan

A custom scan is a network audit based on parameters, which you configure on the fly before launching the scanning process. Various parameters can be customized during this type of scan including:

- Type of scanning profile to use (i.e. the type of checks to execute/type of data to retrieve).
- Scan targets
- Logon credentials

In custom scans, scan profiles are organized under 3 profile groups:

- Vulnerability assessment: This group contains profiles that scan target computers for network threats based on guidelines provided by OVAL/CVE and SANS TOP20 bulletins.
- Network & Software audit: This group contains profiles that scan target computers for system information such as OS information, installed applications and USB devices connected.
- Complete/Combination scans: This group contains Full Scan profiles that audit target computers for a wide-array of threats and system information.

When to use Custom Scans?

It is recommended to use custom scans:

- When performing a onetime scan with particular scanning parameters/profiles.
- When performing a scan for particular network threats and/or system information.
- To perform a target computer scan using a specific scan profile.

2.5.1 How to launch a Custom Scan

To perform a custom scan:

1. Launch the GFI LANguard management console from **Start** ► **Programs** ► **GFI LANguard 9.0** ► **GFI LANguard**.

2. From the **Network Audit** ► **Scan** tab which opens by default, click on the **Launch a Custom Scan** option.

Custom scan wizard	x
Step 1 of 5: Select scan job type Select the type of data to collect from scan targets	
Scan job operation	
 Vulnerability Assessment Scan for network threats (e.g. missing Microsoft updates) using built-in vulnerability checks based on OVAL, CVE and SANS TOP 20 vulnerabilities. Network & Software Audit Collect system information such as installed applications (i.e. identify malware/unauthorized software), open network shares (i.e. potential intrusion point) and USB devices connected (i.e. extential data that?) 	
© Complete/Combination Scans Combine vulnerability assessment and network inventory in a single scanning session. NOTE: These scans can be time consuming.	
Current configuration settings < Badk Next > Cancel	

Screenshot 3 – Scan profile groups

3. Select the scan profile group, applicable to the type of information to be retrieved from targets, and click **Next**. E.g. to audit targets for USB devices connected, select the **Network & Software Audit** option.

Custom scan wizard	.
Step 2 of 5: Select scan profile Select parameters to use for scan job	8
Scan profiles	Description
 Full Vulnerability Assessment Full Scan Full Scan (Slow Networks) 	Scan your network for all supported vulnerabilities including open TCP/UDP ports, missing patches and service packs, USB devices and more. This scanning profile is also used to retrieve system information. NOTE: The vulnerability check timeouts in this profile are preconfigured to suit the network traffic and transmission delays usually associated with LAN environments.
NOTE: Scan profiles contain pre-set parameters used by the scanner for the job type selected.	
Current configuration settings	< Back Next > Cancel

Screenshot 4 - Custom Scan Wizard Scan type

4. Select the profile to use during this scan and click Next.

Custom scan wizard	X
Step 3 of 5: Define target type Select the type of targets to be scanned.	10
Scan type	Description
 Scan a single computer 	Choose the local computer or specify the
Scan a range of computers	computer.
Scan a list of computers	
Scan computers in text file	
Scan a domain or workgroup	
Current configuration settings	< Back Next > Cancel

Screenshot 5 - Target computer categories

5. Select one of the following options and click Next:

- Scan a single computer Select this option to scan local host or one specific computer
- Scan a range of computers Select this option to scan a number of computers defined through an IP range. For more information, refer to http://kbase.gfi.com/showarticle.asp?id=KBID002749.
- Scan a list of computers Select this option to import list of targets from file or to select targets from network list.
- Scan computers in text file Select this option to scan targets enumerated in a specific text file.
- Scan a domain or workgroup Select this option to scan all targets connected to a domain/workgroup.
- 6. Specify the respective target computer(s) details and click Next.

Custom scan wizard Step 5 of 5: Remote logon credentials Specify credentials to use to log on to remote targets.	
Credentials	Description
Currently logged on user Alternative credentials	Perform the scan in the security context of the currently logged on user
User name:	
 a NULL session SSH Private Key 	
User_name:	
✓ Use data from computer profiles (Tell me more)	
Current configuration settings	< Back Scan Cancel

Screenshot 6 - Specify the scan job credentials

- 7. Specify the authentication details to use during this scan.
- 8. Click **Scan** to start the audit process.

2.6 Setting up a scheduled scan

A scheduled scan is a network audit, which is scheduled to run automatically on a specific date/time and at a specific frequency. Scheduled scans can be set to execute once or periodically. Scheduled scan status can be monitored via **Dashboard** ► **Scheduled Operations** tab.

Scheduled scans can also be configured to:

- Automatically download and deploy missing Microsoft updates detected during the scheduled audit
- Trigger Email notifications on detection of network threats
- Generate consecutive-scan comparison reports and distribute these automatically via email.
- Automatically uninstall unauthorized applications.

When to use Scheduled Scans?

It is recommended to use scheduled scans:

- To automatically perform periodical/regular network vulnerability scans using same scanning profiles and parameters
- To automatically trigger scans after office hours and generate alerts and auto-distribution of scan results via email.
- To automatically trigger auto-remediation options, (e.g. Auto download and deploy missing updates).

NOTE: For more information on auto-remediation options refer to the <u>Automatic remediation</u>

NOTE: To enable routine scanning of network targets as part of an established network auditing program such as auditing for legal compliance. Ensure that the GFI LANguard Attendant service is running otherwise scheduled operations will fail to start.

2.6.1 How to setup a Scheduled Scan

To perform a scheduled scan:

1. Launch the GFI LANguard management console from **Start** ► **Programs** ► **GFI LANguard** 9.0 ► **GFI LANguard**

2. From the **Network Audit** ► **Scan** tab which opens by default, click on the **Set Up a Scheduled Scan** option.

New scheduled scan	×
Step 1 of 7: Define target type Select the type of targets to be scanned and describe this scan.	
Scan type	Description
Scan a single computer	Scan a single computer.
Scan a range of computers	Choose the local computer or specify the
Scan a list of computers	computer.
Scan computers in text file	
Scan a domain or workgroup	
Scan job description:	
<u> Tell me more </u>	< Back Next > Cancel

Screenshot 7 - New Scheduled Scan dialog

3. Select one of the following options and click Next:

- Scan a single computer Select this option to scan local host or one specific computer
- Scan a range of computers Select this option to scan a number of computers defined through an IP range. For more information refer to: <u>http://kbase.gfi.com/showarticle.asp?id=KBID002749</u>
- Scan a list of computers Select this option to manually create a list of targets, import targets from file or select targets from network list.
- Scan computers in text file Select this option to scan targets enumerated in a specific text file.
- Scan a domain or workgroup Select this option to scan all targets connected to a domain/workgroup.
- 4. Specify the respective target computer(s) details and click Next.

lew scheduled scan	.
Step 3 of 7: Set the triggering time Set the triggering time for this scheduled scan job	
Triggering time	Description
Trigger scan: One time only Every: 1 Days	Set the triggering time for this scheduled scan job
Ne <u>x</u> t scan: 4/30/2009	
Tell me more < Back	Next > Cancel

Screenshot 8 - Scan frequency

- 5. Specify date/time/frequency of scheduled scan and click Next.
- 6. Specify the scan profile to be used in the scan.
- 7. Click Next.
- 8. Specify logon credentials and click Next

ep 6 of 7: Specify auto-remediation options Please configure automatic remediation options.	V
Auto remediation	Description
 Automatically download and deploy missing patches Automatically download and deploy missing service packs Automatically uninstall unauthorized applications <u>Configure auto-remediation options</u> <u>View applications which this scan will uninstall</u> There are Microsoft updates that are not approved for auto-deployment. 	Auto-Remediation options enable LANguard automatically download and install missing patches and service packs, and uninstall unauthorized applications on the scanned computers.
It is recommended to have System Restore on for the system drive on the target computers.	
2	

Screenshot 9 - Scheduled scan auto-remediation options

9. (Optional) Select **Automatically uninstall unauthorized applications** so that all applications validated as unauthorized, will be uninstalled from the scanned computer (unauthorized applications are

defined in **Application Inventory**). For more details see <u>Application</u> <u>auto-uninstall</u>

10. (Optional) Click **View applications which this scan will uninstall**. To launch the **Applications which will be uninstalled** dialog. This will list all the applications that will be uninstalled when the scheduled scan is finished.

11. (Optional) Click **Configure auto-remediation** option to configure the processes that must be triggered before and after a deployment of an application. For more information, refer to <u>Deployment options</u>.

12. Click Next.

ew scheduled scan		
Step 7 of 7: Review sch	eduled scan job	
Please review the sett	ings for this scheduled scan job	5
Scheduled scan sur	nmary	
Target	localhost	
Triggering time	Every 1 day(s) at 4:35:36 PM, starting on 4/30/2009	
Scanning profile	High Security Vulnerabilities	
Credentials	Alternative credentials	
Auto-remediation	Automatically download and deploy missing patches	
Warning	Alerting options are not configured (email reports will not be sent).	-
	g options	
Configure schedu	led scaps reporting options	
<u>Tell me more</u>	< Back Finish Cancel	

Screenshot 10 - Review scheduled scan job

13. (Optional) Click on **Configuring alerting options...** and specify sender/recipient details.

Scheduled Scans Reporting options	x	
Result Saving Results Notification		
Specify where to save scan results to XML or HTML reports.		
For result comparison operations, GFI LANguard saves all scan results to the database backend.		
You can configure GFI LANguard to output the scheduled scan results also to XN or HTML report files in a directory on the hard drive.	1L	
Save as XML files WARNING: Saving scheduled scan results to XML can take several minutes for large scans and can cause performance degradation.	r	
C:\Program Files\GFI\LANguard 9.0\Data\Reports		
Save as HTML reports Generate and save scan result html reports to: C:\Program Files\GFI\LANguard 9.0\Data\Reports Save HTML reports as .MHT (Web Archive, single file)		

Screenshot 11 - Scheduled Scans Reporting options

14. (Optional) Click on **Configure scheduled scan reporting options...** to configure scheduled scans reporting.

- a. Specify whether scan results are saved as HTML or XML
- b. Click on Results Notification tab and select:
- Full Scan to include all data collected during the scheduled scan.
- Results Comparison to create a report which lists only the differences (if any) identified between the last scheduled scan results and the preceding one.
- 15. Click **OK** to finalize your settings.
- 16. Click **Finish** to finalize your configuration.

17. All new scheduled scans are by default disabled. To enable select **Configuration** \blacktriangleright **Scheduled Scans** and click on the **G**.

NOTE: For more information on **Scheduled Scans** refer to the <u>Scheduled Scans</u> section in this manual.

			C 1
Target	Profile	Start Time	Status
Target	Profile Full Vulnerability Assessment	5/4/2009 8:49:23 AM	complete

Screenshot 12 - Scheduled scan status

18. Confirm that the new scheduled scan has been successfully set by clicking on **Dashboard** ► **Scheduled Operations**. New scheduled scan should be listed in the queue.

For more information on how scheduled scans can be monitored please, refer to <u>Monitoring scheduled activity</u>

3. Step 2: Analyzing the security scan results

3.1 Introduction

The most important thing following a network security scan is identifying which areas and systems require your immediate attention. This is achieved by analyzing and correctly interpreting the information collected and generated during a network security scan.

3.2 Scan summary

Upon completing a scan, GFI LANguard immediately displays a scan summary that graphically displays the vulnerability level of the scanned computer or a combined interpretation of the scan results obtained following a network scan.

💽 GFI LANguard		
File Tools Configure Help)	Discuss this version
Network Audit Dashboard	Configuration Utilities Ge	eneral
🐁 Scan 🐁 Analyze 🐁 Remediat	e	
Common tasks Load scan results from database Load scan results from XML Save scan results to XML file	Scan complete Summary of scan res	d! sults generated during this network audit.
Export computers to file Modify default settings	Scan Properties	
Actions Go to: Analyze Go to: Remediate	Scan type: Profile: Duration: Computers audited:	Local computer scan High Security Vulnerabilities 3 minutes, 44 seconds ≡ 1
	Results	
Help: <u>Performing an audit</u> <u>What audit operations mean?</u> <u>FAQ</u>	Audit operations: Network vulnerability level: Missing security updates: Other vulnerabilities: Installed security updates: Installed applications: Open ports:	898 audit operations processed High 15 (15 Critical/High) n/a 25 n/a n/a
	Next Steps	
	•	• ·

Screenshot 13 - Scan summary

3.3 Vulnerability level rating

The vulnerability level is a rating given by GFI LANguard to each computer after it has been scanned. This rating indicates the vulnerability level of a computer/network, depending on the number and type of vulnerabilities and/or missing patches found.

Screenshot 14 - Vulnerability level meter

A high vulnerability level is a result of vulnerabilities and/or missing patches whose average severity is categorized as high.

When a number of computers are scanned in a single audit session, a measurement of the global vulnerability level is based on a weighted sum of the vulnerabilities detected on the computers scanned.

Vulnerability level is indicated using color-coded graphical bar. A red color-code indicates a high vulnerability level, whilst a green color-code indicates a low vulnerability level.

3.4 Detailed scan results

Click on the **Analyze** tab to access a more detailed list of vulnerabilities.



Screenshot 15 - Detailed scan results

Informa	ation in result pane
1	Scan target node: Displays information related to scan targets in
•	terms of, scan range and whether scan result was retrieved from
	database.
2	Scan computer node: Displays information related to the scanned
	computer. Indicates if scan was successful and shows OS details.



Expand the **Scanned computers** node to access the results retrieved during the scan. Security scan results are organized in 2 sub-nodes tagged as:

- Vulnerability Assessment
- Network & Software Audit

3.5 Detailed scan results: Vulnerability assessment



Screenshot 16 - The Vulnerability Assessment node

Click on any **Vulnerability Assessment** node to view the security vulnerabilities identified on the target computer grouped by type and severity as follows:

- High Security Vulnerabilities
- Low Security Vulnerabilities
- Potential vulnerabilities
- Missing Service Packs
- Missing Patches

3.5.1 High/Med/Low Security vulnerabilities

Click on the **High Security Vulnerabilities** or **Low Security Vulnerabilities** sub-nodes for a list of weaknesses discovered while probing a target device. These vulnerabilities are organized into the following groups:

Group	Description
Mail, FTP, RPC,	Lists vulnerabilities discovered on FTP servers, DNS servers, and
DNS and	SMTP/POP3/IMAP mail servers. Links to Microsoft Knowledge
Miscellaneous	Base articles or other support documentation are provided.
Web	Lists vulnerabilities discovered on web servers (such as
	misconfiguration issues). Supported web servers include Apache,
	Netscape, and Microsoft I.I.S.

Services	Lists vulnerabilities discovered in active services as well as the list of unused accounts that are still active and accessible on scanned targets.
Registry	Lists vulnerabilities discovered in the registry settings of a scanned network device. Links to support documentation and short vulnerability descriptions are provided.
Software	Lists vulnerabilities found in software installed on the scanned network device(s). Links to supporting documentation and short vulnerability descriptions are provided.
Rootkit	Lists vulnerabilities discovered because of having a rootkit installed on the scanned network device(s). Links to supporting documentation and short vulnerability descriptions are provided.

3.5.2 Potential vulnerabilities

Click on the **Potential vulnerabilities** sub-node to view scan result items that were classified as possible network weaknesses. Although not classified as vulnerabilities, these scan result entries still require meticulous attention since malicious users can exploit them during malicious activity.

E.g. during vulnerability scanning GFI LANguard will enumerate all of the modems that are installed and configured on the target computer. If unused these modems are of no threat to your network, however if connected to a telephone line these modems can be used to gain unauthorized and unmonitored access to the Internet. This means that users can bypass corporate perimeter security including firewalls, antivirus, website rating and web content blocking exposing the corporate IT infrastructure to a multitude of threats including hacker attacks. GFI LANguard considers installed modems as possible threats and enumerates them in the **Potential Vulnerabilities** sub-node.

3.5.3 Missing Service Packs/Patches

Click on the **Missing Service Packs** or **Missing Patches** subnode respectively to check which Microsoft software updates or patches are missing.

NOTE: GFI LANguard can identify missing service packs and patches on various Microsoft products. For a complete list of supported products visit: <u>http://kbase.gfi.com/showarticle.asp?id=KBID002573</u>

Bulletin information

To access bulletin information, right-click on the respective service pack and select **More details** ► **Bulletin Info**.

Bulletin Info							—
Bulletin							
Bulletin ID:	MS09-007	QNumber:	960225	Date:	2009-03-10	Severity:	Important
Title:	Security Update	for Windows	Vista (KB96022	5)			
Description:	A security issue behavior witho from Microsoft to you and lice	e has been ide ut the knowled After you ins nsed under th	ntified that cou dge of the user tall this update e Windows Vist	Ild allow an a You can he , you may ha a License Te	attacker to misrepr Ip protect your sy ave to restart your rms.	esent a system stem by installir r system. This u	n action or ng this update update is provided
Applies To:	Windows Vista						
URL:	http://go.micros	oft.com/fwlink	?LinkID=1398</th <th>54</th> <th></th> <th></th> <th></th>	54			
File							
File Name:	Windows6.0-KB	960225-x86.ca	ab				
File Size:	205 KB						
File URL:	http://download	windowsupda	ate.com/msdow	inload/updat	e/software/secu/2	2009/01/windov	ws6.0-kb96022
							Close

Screenshot 17 - Missing Service pack: Bulletin info dialog

3.6 Detailed scan results: Network & Software Audit

Scan Results Overview	
🖃 🛐 Scan target: localhost	
🖮 🔽 🔮 192.168.3.85 [ESM_DEMO] (Windows Vista Service Pack 1)	
🕀 🐴 Vulnerability Assessment	
🚊 📷 Network & Software Audit	
🕀 👋 System Patching Status	
🕀 📲 Ports	
🕀 🍂 Hardware	
🕀 🧃 Software	
🗄 🖏 System Information	

Screenshot 18 - The network and software audit node

Expand the **Network & Software Audit** node to view security vulnerabilities identified on scanned targets. Here, vulnerabilities are grouped by type and severity as follows:

- System Patching Status
- Ports
- Hardware
- Software
- System Information

Category	Information	
? 12	Fast response	
? 27	Medium Response	
	Slow response	

NOTE: The first icon indicates that the scan is queued, while the second icon indicates that the scan is in progress.

3.6.1 🛯 🖉 System patching status

Expand System Patching Status sub-node to access Information on:

- Missing Patches List of missing Microsoft Patches
- Missing Service Packs List of missing Microsoft Service Packs
- Installed Patches List of installed Microsoft Patches
- Installed Service Packs List of installed Microsoft Service Packs.

3.6.2 💐 Ports

Expand the **Ports** sub-node to view all TCP and UDP ports detected during a scan. When a commonly exploited port is found open, GFI LANguard will mark it in red. Care is to be taken, as even if a port shows up in red, it does not mean that it is 100% a backdoor program. Nowadays with the array of software being released, it is becoming more common that a valid program uses the same ports as some known Trojans.

Further to detecting if, the port is open or not, GFI LANguard uses service fingerprint technology to analyze the service(s) that are running behind the detected open port(s). Through service fingerprinting you can ensure that no hijack operation has taken place on that port. For example, you can verify that behind port 21 of a particular target computer there is an FTP server running and not an HTTP server.

3.6.3 📥 Hardware

Expand the **Hardware** sub-node to view a hardware audit categorized as follows:

Category	Information provided
🐓 Network Devices	MAC address
(Physical, Virtual, Wireless,	IP address
Software enumerated devices)	Device type
	Vendor
	Hostname
	DHCP Set
	DNS Server
	Status
🖶 USB Devices	Device name
	Description
	Manufacturer
> Local Drives	Drive letter
	Total disk space
	Available disk space
Processors	Vendor
	Processor speed

🎾 Motherboard	Product name
	Manufacturer
	Version
	BIOS name
	BIOS vendor
	BIOS version
	BIOS release date
	BIOS Serial Number
💺 Memory details	Physical memory
	Free physical memory
	Virtual memory
	Free virtual memory
Storage details	Description
	Manufacturer
	Interface type
	Media type
	Partitions
	• Size
	• Drive(s)
舉 Display adapters	Manufacturer
	Monitor
	Current video mode
🤝 Other devices	• HID
	System devices
	Keyboard
	Ports (COM & LPT ports)
	Floppy disk controllers
	Mouse
	Multimedia
	Hard disk controllers
	Computer
	Storage volumes
	SCSI and RAID controllers

3.6.4 a Software

Expand the **Software** sub-node to access software audit categories:

Category	Information provided
🔩 General Applications	Application name
	Version
	Publisher
🔩 Antivirus Applications	Application name
	Real-time protection
	Up-to-date
	Last update
	Version
	Publisher

3.6.5 😽 System Information

Expand the System Information s	sub-node to	access (DS information
grouped as follows:			

Category	Information Provided	neips to identify
Shares	 Share name Share remark (extra details on the share) Folder which is being shared on the target computer Share permissions and access rights NTFS permissions and access rights. 	Users sharing entire hard-drives, shares that have weak or incorrectly configured access permissions. Startup folders, and similar system files, that are accessible by unauthorized users, or through user accounts, that do not have administrator privileges, but are allowed to execute code on target computers. Unnecessary or unused shares.
Policy	 Maximum password length Maximum password 	lockout control
	length	Password strength
	Minimum password age	enforcement policies
	Force logoff	
60 0 1 1 1 1	Password history	O a surit a balance an
Audit Boliev	Audit account logon	Security holes or
Addit Policy	Audit account	Diedches
	management	
	Audit directory service	
	access	
	Audit logon events	
	And more	
💇 Registry	Registered owner	Hardware and software
	Registered organization Broduct name	settings such as which
	Current build number	will be automatically
		launched at system startup
S NETBIOS	Workstation service	Rogue computers and
Names	Domain name	Wrong configurations
	Domain controllers	
	File server service	

Somputer 🕌	 MAC address Time to live (TIL) Network role Domain 	Rogue computers and Wrong configurations
3 Groups	 Account operators Administrators Backup operations Guests 	Wrong configurations and security flaws due to rogue or obsolete user groups
🐇 Users	Full namePrivilegeFlagsLogin	Rogue, obsolete or default user accounts
Logged On Users	List of logged on users	Authorized and unauthorized users currently logged on computers
Sessions	 Lists hosts remotely connected to the target computer during scanning, 	Authorized and unauthorized remote connections
Services 😽	List of active services	Rogue or malicious processes; redundant services
👹 Processes	List of active processes	Rogue or malicious processes
Remote TOD (time of day)	Time of remote workstation, server or laptop.	Time inconsistencies and regional settings Wrong configurations



An important part of any security plan is the ability to monitor and audit events happening on your network. These event logs are frequently referenced in order to identify security holes or breaches. Identifying attempts and preventing them from becoming successful breaches of your system security is critical. In Windows, you can use 'Group Policies' to set up an audit policy that can track user activities or system events in specific logs.

In order to help you keep track of your system's auditing policy GFI LANguard collects the security audit policy settings from scanned target computers and includes in the scan results. This information is accessed by click on the **Security Audit Policy** sub-node.

Apart from gaining knowledge on the current audit policy settings, you can also use GFI LANguard to access and modify the audit policy settings of your target computers. To achieve this:

1. From the Scanned Computers (middle) pane, right-click on the respective target computer and select **Enable auditing on** ► **This computer/Selected computers/All computers**.

GFI LANguard Administration Wizard				×
Switch on security auditing policies Automatic turning on of security auditing policies				
Specify which auditing policies are to be turned on. The recomm have been selected by default:	ended aud	diting poli	cies	
Auditing Policy	Success	Failure		
Audit account logon events		~	*	
Audit account management	✓	✓		
Audit directory service access	✓	✓	=	
Audit logon events	✓	✓		
Audit object access	✓	✓		
Audit policy change	✓	✓		
Audit privilege use			-	
Select Next to turn on the selected auditing policies.				
< Back	Next >		Cance	el 📄

Screenshot 19 - The audit policy administration wizard

2. Select/unselect auditing policies accordingly, and click **Next** to deploy the audit policy configuration settings, on the target computer(s).

Computer	Result

Screenshot 20 - Results dialog in audit policy wizard

3. At this stage, a dialog will show whether the deployment of audit policy settings was successful or not. You can choose to re-deploy settings on failed computers by clicking on the **Back** button. To proceed to the next stage click **Next**.

4. Click **Finish** to finalize your configuration.

👫 Groups/users

Rogue, obsolete or default user accounts can be exploited by malicious or unauthorized users to gain access to restricted areas of your IT infrastructure. The 'Guest' account for example is just one example of commonly exploited accounts – reason being that more often than not, this account is left configured within a system and even worse without changing the default password settings. Malicious users have developed applications, which can automatically re-enable the 'Guest' account and grant it administrative rights; Empowering users to gain access to sensitive areas of the corporate IT infrastructure.

GFI LANguard collects information on all user accounts and user groups currently enabled on scanned targets. This information is organized in the scan results under two separated nodes. To access the list of user accounts identified during on a target computer, click on the **Susers** sub-node. Use the information enumerated in this sub-node to inspect the access privileges assigned to each user account. To gain access to the list of user-groups configured on a target computer, click on the **Susers** sub-node.

NOTE: Users should not use local accounts to log on to a network computer. For better security, users should log on to network computers using a 'Domain' or an 'Active Directory' account.



Click on the **Sessions** sub-node to access the list of hosts that were remotely connected to the target computer during scanning.

NOTE: The information enumerated in this sub-node also includes the remote connection details of the scanning session just performed by GFI LANguard i.e. the IP of the computer that is running GFI LANguard, the logon credentials, etc.



Active services can be a potential security weak spot in your network system. Any of these services can be a Trojan, a viruses or another type of malware, which can seriously affect your system in a dangerous way. Furthermore, unnecessary applications and services that are left running on a system consume valuable system resources.

During the scanning process, GFI LANguard enumerates all services running on a target computer for you to analyze. This way you can identify which services must be stopped. Further to the freeing up of resources, this exercise automatically hardens your network by reducing the entry points through which an attacker can penetrate into your system. To access the list of services enumerated during a scan, click on the **Services** sub-node.



Processes

Click on the **W Processes** sub-node to access the list of processes that were running on the target computer during a scan.



Remote time of day

Click on the Remote TOD (time of the day) sub-node to view the network time that was read from the target computer during the scan. This time is generally set on network computers by the respective domain controller.

3.7 Displaying and sorting scan categories

GFI LANguard provides you with the ability to hone down and sort available scan categories and scanned computers. This allows you to focus on specific data that might require your attention in more detail without getting lost in other data that might not be relevant at that point in time.

Customize scan results view	X
View Sorting	
Select which information categories you want to show/hide insi the scan result window.	de
Item to show/hide	
🕼 🚣 High Security Vulnerabilities	
🔽 🔔 Medium Security Vulnerabilities	
🔽 🦲 Low Security Vulnerabilities	=
🔽 🔔 Potential Vulnerabilities	
📝 🕐 Missing Service Packs	
📝 🕐 Missing Patches	
📝 🥩 Installed Service Packs	
📝 🥩 Installed Patches	
📝 👒 Open TCP Ports	
V to Open UDP Ports	
🗹 🐓 Network Devices	
USB Devices	
Local drives	
V M Processors	
🗹 🌺 Motherboard	
🔽 💺 Memory Details	Ŧ
OK Cancel Ap	ply

Screenshot 21- Customize view

To customize and sort the list of scan results:

1. Under **Common Tasks** in the left panel, click on **Customize scan results view...**

2. From the **View** tab select which scan categories you want to show or hide. Click **Apply** to save setting.

3. Click on the **Sorting** tab and set your sorting preferences. Click **OK** to finalize your configuration.



3.7.1 Loading saved scan results from database

Screenshot 22 - Reloaded scan results

By default, saved scan results are stored in a database. GFI LANguard stores the results data of the last 10 scans performed per scanning profile.

NOTE: You can configure the number of scan results that are stored in a database file. For more information, refer to the <u>Database</u> <u>maintenance options</u> section in this manual.

To load saved scan results from the database backend or from an XML files:

1. Click on the **Analyze** ► **Scan Results**.

2. Under **Common Tasks** in the left pane, click **Load scan results** from database.

3.8 Saving scan results

Scan results are an invaluable source of information for systems administrators. GFI LANguard results are stored in a MS-SQL Server or an MS-Access database. In addition, scan results can also be exported to XML.

3.8.1 Saving scan results to XML file

To save scan results to XML file:

1. Go to **Network Audit** ► **Analyze**.

2. Launch a new scan or click on **load the saved scan result from database** to load the results you want to export to XML.

3. Click on **Save scan results to XML file...** and specify XML file where results will be saved.

4. Click **Save** to finalize your configuration.
3.8.2 Loading saved scan results from XML

To load saved scan results from an XML file:

1. Click on the Analyze ► Scan Results.

2. Under Common Tasks in the left pane, click Load saved scan results from XML.

3. Locate the scan results to load and click OK.

3.9 Scan filters

Scan results typically present a substantial amount of information. You might however at times require only specific information to achieve a particular targets - such as for example, identifying only which patches are missing in your system.



Screenshot 23 - Scan filter nodes

GFI LANguard ships with a default set of scan result filters that allow you to sift scan results data and display only the relevant information. Scan filters are organized in three categories:

- Complete Scans
- Vulnerability Assessment
- Network & Software Audit

Scan result filter	Description
Full report	Displays all the information that was collected during a network vulnerability scan including system OS information, outdated anti-virus signatures, and missing patches and service packs.
Vulnerabilities [All]	Displays all Critical, High and Medium severity vulnerabilities discovered during a network security scan.
Vulnerabilities [High security]	Displays only severe vulnerabilities such as missing critical security patches and service packs.
Vulnerabilities [medium security]	Displays only moderate severity vulnerabilities, which may need to be addressed by the administrator. Such as average threats and medium vulnerability patches.
Auto-remediation	Displays auto-remediation actions triggered.
High vulnerability level computers	Use this filter to access list of computers and vulnerability details for which vulnerability level is high.
Missing patches and service packs	Use this filter to access list of missing patches and service packs discovered on scanned target computer(s).
Missing service packs	Use this scan filter to display a list of all computers and computer details of computers, which have a missing service pack.
Missing critical patches	Displays all missing patches marked as critical.
Open ports	Shows all open TCP and UDP ports discovered on the scanned target computer(s).
Open shares	Shows all open shares and the respective access rights.
Groups and users	Shows the users and groups detected on the scanned target computer(s).
Computer properties	Shows the properties of each target computer.
Hardware audit	Displays information about the hardware configuration of the scanned computer(s).
Important devices - USB	Shows all the USB devices attached to the scanned target computer(s).
Important devices - Wireless	Shows all the wireless network cards, (both PCI and USB) attached to the scanned target computer(s).
Installed Applications	Shows all the installed applications (including security software) discovered during target computer scanning.
Non-Updated security software	Shows only the installed security applications (i.e. anti-virus/anti-spyware software) that have missing updates and outdated signature definition files.
Virtual machines	Shows a list of non-updated security software on the scanned target computer(s).

The filters, which ship with GFI LANguard, are:

3.9.1 Filtering scan results

To apply a scan result filter on security scan results:

1. Launch and complete a security scan of your network or load the scan results of past scans from your database or XML file.



Screenshot 24 - Scan filters: Full report

2. Click Network Audit ► Analyze.

3. Select the **Results Filtering** node and expand the **Complete Scans** node.

4. Select the scan filter to apply against scan results.

3.9.2 Creating a custom scan filter

Apart the scan filters that ship by default; you can create custom filters based on your requirements and network infrastructure. To create a custom scan filter:

1. Click Network Audit Analyze

2. Right click on the scan filter category where the new filter will be added and select **Create new results filter...**

Advanced Properties	—
General Report Items	
Scan Filter Properties	
Eilter name:	
Filter conditions:	
Queries	Add
 ✓ High vulnerabilities Exists ✓ AND Missing patches Exists 	Edit Remove Remove All
Logical operator for the selected condition:	
OK Cancel	I Apply

Screenshot 25 - The new Scan filter properties dialog: General tab-page

3. In the **General** tab, specify the name of the new scan filter.



Screenshot 26 - Filter properties dialog

4. Click **Add...** and select the required filter property from the provided list. This defines what type of information is extracted from the scan results (i.e. the area of interest of the scan filter). Click **Next** to continue.

Add Filter Prope	erties	X
Filter Co	ondition Properties	
Filter Property I	nformation	
Filter condition	to add	
Property:	Missing patches	
Conditions:	Does not exist	•
<u>V</u> alue:		
Summary: Determine if mi computer	ssing patches are NOT found on the remote	
	K Back Add Cance	ł

Screenshot 27 - Filter condition properties dialog

5. Select the required filter condition from the drop down provided.

6. Specify the filter value. This is the reference string with the specified condition to filter information from scan results. Click **Add** to continue.

NOTE: You can create multiple filter conditions for every scan filter. This allows you to create powerful filters that more accurately isolate the scan results information that you may want to analyze.

Advanced Properties	×
General Report Items	
Select the items that will be contained in HTM	L report.
Show Summary Table	
🔒 Vulnerability Level	
y Automatic Remediation Details	
🛛 🐻 Scan Errors	
Vulnerability Assessment	
🔒 Missing Service Packs	
🛨 🕐 Missing Patches	
🛨 📤 High Security Vulnerabilities	
🛨 🔔 Medium Security Vulnerabilities	
🛨 庄 Low Security Vulnerabilities	✓
Potential Vulnerabilities	
Information	
Network & Software Audit	
Installed Patches & Service Packs	
🖃 🔩 Ports	
TCP Ports	
Sector Contemports	✓ ▼
ОК	Cancel Apply

Screenshot 28 - The new Scan-Filter properties dialog: Report Items tab-page

7. Click **Report Items** tab and select the information categories/subnodes to display. Click **OK** to save and create the new filter.

The new filter will be added as a new permanent sub-node under the **Results Filtering** node.

NOTE: To delete or customize a scan filter, right-click target filter and select **Delete filter** or **Edit filter properties**.

3.10 Results comparison

GFI LANguard enables you to compare saved scan results and generate a list of network changes discovered.

3.10.1 Configuring what scan results changes will be reported

The result comparison tool can report various information discovered during the comparison of two saved scan results. To configure what changes will be included in a comparison report:



Screenshot 29 - Results comparison configuration options

1. Click on **Network Audit** ► **Analyze**.

2. Right click **Result comparison** node and select **Edit comparison options...**

Options 💽
General
Result comparison options
Display the following items:
Vew items.
Removed items.
Changed items.
Options:
Show vulnerability changes.
Show only hotfix changes.
UK

Screenshot 30 - Edit comparison options

3. Select the information item(s) to be reported.

atabase Source				-
General				
Select the scan i	result to use for the	e required operation.		
Target	Profile	∇ Date	Completed	-
🔲 localhost	Full scan	5/4/2009 13:39:08	Yes	
🗐 file:Cache\200905	High Security	5/4/2009 12:58:21	Yes	
🔲 domain:Primary do	Full Scan	5/4/2009 12:54:43	No	
192.168.3.20	Full scan	5/4/2009 10:42:09	Yes	
192.168.3.20	Full scan	5/4/2009 10:36:57	Yes	
📒 localhost	Full Vulnerabi	5/4/2009 10:18:16	Yes	=
📒 localhost	Top SANS 2	5/4/2009 10:15:59	Yes	
📒 localhost	Full Vulnerabi	5/4/2009 10:15:18	No	
📒 localhost	High Security	5/4/2009 10:09:52	No	
📒 localhost	Full scan	5/4/2009 09:42:51	Yes	
📒 localhost	High Security	5/4/2009 09:08:53	Yes	
192.168.3.20	High Security	5/4/2009 09:06:24	Yes	
192.168.3.20	Full Vulnerabi	5/4/2009 08:49:23	Yes	
🔲 localhost	High Security	5/4/2009 08:46:01	Yes	
🔲 localhost	High Security	4/30/2009 17:22:49	Yes	+
f an		4100100004740.00		
		ОК	Can	cel

3.10.2 Generating a results comparison report

Screenshot 31 - Comparing scan results

To generate a scan results comparison report:

- 1. Click on **Network Audit** ► **Analyze**.
- 2. Click on the **Result comparison** node.

3. Click search file \nearrow button and select files to compare select the scan result files that you wish to compare.

NOTE: You can only compare results of the same type i.e. you cannot compare a result stored in XML with one stored in database.

4. Click **Compare** to start the results comparison process.

🗑 GFI LANguard		x
File Tools Configur	e Help Discuss this version	n
Network Audit Dash	board Configuration Utilities General	
🇞 Scan 🐁 Analyze 🍇	Remediate	
 Scan Analyze Analyze Analyze: Scan Results Results Filtering Results Filtering Results Comparison Results Comparison results Save comparison results Edit comparison options Help: Comparing the results 	Remediate Scan result 1: localhost - Full Scan - 5/4/2009 13:33:08 Compare Dptions Scan result 2: localhost - Full Vulnerability Assessment - 5/4 P Results Comparison The Results Comparison option enables the identification of network security changes which occurred over a period of time which spans two network security scans. ESM_DEMO 192.168.3.85 Image: Ima	
]	-

3.10.3 The Results Comparison Report

Screenshot 32 - Results Comparison Report

On completion, the results comparison report is displayed in the right pane of the management console.

3.11 Reporting

NOTE: On Microsoft Windows Vista computers, an error message might be displayed during the automatic installation of the Microsoft .NET framework 1.1. For more information on how to resolve this issue, refer to <u>http://kbase.gfi.com/showarticle.asp?id=KBID003100</u>.

3.11.1 Access/download/install reporting

GFI LANguard ships with a powerful reporting companion that is ideal to generate management and technical reports.

To access reporting:

- 1. Click on **Network Audit** ► **Analyze**.
- 2. Select the Reporting node.



Screenshot 33 – GFI LANguard ReportPack not installed

3. If the GFI LANguard ReportPack is not installed, you will be prompted to auto-download and install the reporting package. Click on the Download and Install ReportPack button to proceed.

File Total Configure Help Discuss this version Network Audit Dashoard Configuration Ublities General Scan * Analyze * Remediate Network Audit Discuss this version Markation * Remediate Network Audit Scan reference : domain Primary domain Scan reference : : domain Primary domain Scan reference : domain Primary domain Scan reference : : : 14-Hor-2008 18:42 Vehrench Faching States Network Audit Scan reference : : : Scan reference : : : : : : Vehrench Faching States : : : : : Scan reference : : : : : : : Scan reference : : <td< th=""><th>GFI LANguard</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th>, .</th></td<>	GFI LANguard									, .
Network Audit Dathboard Configuration Utilitie General Scan Analyze Remediate Soan Reads Renges Remediate Network Vulnerability Summary Report Sean Reads Renges Remediate Network Vulnerability Summary Report Weinschleft Scan reference : domain:Primary domain Sean Roads Software Audit Operation Scan reference : domain:Primary domain Sean Roads Software Audit Operation Status Scan reference : domain:Primary domain Sean reference : domain:Primary domain Scan reference : domain:Primary domain Sean reference : domain:Primary domain Scan reference : domain:Primary domain Sean reference : domain Primary domain Scan reference : domain Primary domain Sean reference : domain Primary domain Scan reference : domain Primary domain Sean reference : domain Primary domain Scan reference : domain Primary domain Sean reference : domain Primary domain Scan reference : domain Primary domain Sean reference : domain Primary domain Scan reference : domain Primary domain	File Tools Configure Help								Discuss ti	is versio
San Ruda San Ruda Ruda Compation Executive Reports: Network Ydnorobity Summary Winnels House Based on Vulnerability Level Distribution Winnels House Based on Vulnerability Level Distribution House House Hous	Network Audit Dashboard Configuration	Utilities Gene	eral							
Analysis Service Reading Results	🖁 Scan 🐁 Analyze 🧚 Remediate									
Span Paula Paula Filtering Span Paula Paula Congaton Paula Congaton	Analyze:									
Preduz Terrosoviti Picture Valueobing Value Properties Scan reference : domain Primary domain Sc	🖉 Scan Results	Network V	ulnerabi	lity Summary	Report					
Scan reference : domain:Primary domain Scan date & time : 34-Nov-2008 18:42 Scan date	Results Filtering			inty outilities,	Report					
Scan date & time : 14-Nov-2008 18:42 Scan date & time : 14-Nov-2008 18:42 Hosts Severity Level Distribution Table of GP1 Measure RecomPack. Scan date & time : 14-Nov-2008 18:42 Hosts Severity Level Distribution Scan date & time : 14-Nov-2008 18:42 Hosts Severity Level Distribution Scan date & time : 14-Nov-2008 18:42 Hosts Severity Level Distribution Scan date & time : 14-Nov-2008 18:42 Hosts Severity Level Distribution Scan date & time : 14-Nov-2008 18:42 Hosts Severity Level Distribution Scan date & time : 14-Nov-2008 18:42 Hosts Severity Level Distribution High data date & time : 14-Nov-2008 18:42 Hosts Severity Level Distribution High data date & time : 14-Nov-2008 18:42 Hosts Severity Level Distribution High data date & time : 14-Nov-2008 18:42 Hosts Severity Level Distribution High data date & time : 14-Nov-2008 18:42 Hosts Valnerability Level Distribution	Reporting	Scan reference		domain:	Primary domain					
Metrody Munerability Sumary Weinsch Rading Status Metrody Munerability Lavel Deparating Systems and Sancios Pack Distribution	xecutive Reports:	Scan date & tir	ne :	14-Nov-	2008 18:42					
I Method Patching Status Software Aud. Software Aud. Developerating System and Service Pack Distribution Image: Construction of SPI LNRsamt RecordPack. Image: Construction of SPI LNRsamt RecordP	Network Vulnerability Summary Vulnerable Hosts Based on Vulnerability Level									
Voltage Voltage <t< td=""><td>Network Patching Status</td><td>Hosts Seve</td><td>rity Leve</td><td>l Distribution</td><td>Top 10 Vulner</td><td>able Hosts (by Seve</td><td>erity)</td><td></td><td></td><td></td></t<>	Network Patching Status	Hosts Seve	rity Leve	l Distribution	Top 10 Vulner	able Hosts (by Seve	erity)			
With common Tasks: With Tasks: With Medium Medium Not Figh Medium Not Figh Figh Figh Figh Figh Figh Figh Figh	Operating System and Service Pack Distribution				IP Address	Host Name		Severity		
Sine moot Prix moot Larsch GPI LANauel ReportPack Vuln Vuln Yuln		Low					High	Med.	Low	
Save mod 192.168.3.4 ANDREMUSCAT-PC 20 2 6 Userch GPI L/Nexaed BenotPlack 192.168.3.26 SBORG 0 0 7 Waln Yuln Yuln 102.168.2.35 JASON 1 0 2 Waln Yuln Yuln 102.168.3.35 JASON 1 0 2 High 89 75 102.168.3.141 MIROS 0 0 1 Hosts Vulnerability Level Distribution 192.168.3.141 MIROS 0 0 1	ommon Tasks:				192.168.3.27	RICHARD	67	13	9	
Virtimont 192:168.3.26 SBORG 0 0 2 Laarch GFI L/Hound ReportPack. 102:168.3.36 JSON 1 0 2 Virin- Severity Count High 96 75 1 0 1 192:168.3.30 TMLASON_XP 1 0 1 Walne- Nedium 5 4 1 0 1 Hosts Vulnerability Level Distribution Vulnerability Level Distribution Vulnerability Level Most 0 1	Save moot	Medium-			192.168.3.4	ANDREMUSCAT-PC	20	2	6	
Vuln: Vuln: <th< td=""><td>Print report</td><td></td><td></td><td></td><td>192.168.3.26</td><td>SBORG</td><td>0</td><td>0</td><td>7</td><td></td></th<>	Print report				192.168.3.26	SBORG	0	0	7	
Vuln. 102 103 100 2 192 168 3.30 TMLASON_XP 1 0 1 192 168 3.141 MROS 0 0 1	Launch GFI LANguard ReportPack			1	192.168.0.15	TREEBEARD	0	0	2	
Vuln. Vuln. <th< td=""><td></td><td></td><td></td><td>Lingh</td><td>192.168.3.36</td><td>JASON</td><td>1</td><td>0</td><td>2</td><td></td></th<>				Lingh	192.168.3.36	JASON	1	0	2	
Vulner Severity Count % High 80 75 Medium 5 4 Low 255 21 Hosts Vulnerability Level Distribution High 2 High 2 Migh 2 Migh 2					192.168.3.30	TMJASON_XP	1	0	1	
High 80 75 Medium 5 4 Low 25 21 Hosts Vulnerability Level Distribution High 2 Medium 0		Vuln. Severity	Vuln. Count	%	192.168.3.141	MIROS	0	0	1	
Holium 5 4 Low 25 21 Hosts Vulnerability Level Distribution High 2 Medium 0		High	89	75						
Hosts Vulnerability Level Distribution Vulnerability Level Most High 2 High 2 Medium 0		Medium	5	4						
High 2 Medium 0		Hosts Vulne	erability L	evel Distributi	on	ulnerability Level	Host Count]		
Medium 0		_			1	High	2			
▲						Medium	0			
]	•	_				_	_	_	-

Screenshot 34 - GFI LANguard with installed ReportPack

4. From the left pane select the reports you run.

NOTE: For more information on the reports in GFI LANguard, refer to the GFI LANguard ReportPack manual available from: http://www.gfi.com/lannetscan/ LANguard9rpmanual.pdf

4. Step 3: Fixing vulnerabilities

4.1 Introduction

Following a scan, GFI LANguard enables you to automatically fix some of the issues identified during your network audit. This is achieved through the built-in tools that ship with the product. Available remediation actions include:

- Auto-patch management This remediation feature automatically downloads missing Microsoft updates and deploys them network-wide.
- Applications auto-uninstall This remediation action enables the auto-uninstall of applications that support silent uninstall. The process involves a test phase (called validation) during which an application is uninstalled automatically to identify if silent uninstall is supported by target application. If it is, all the other instances on the network will be automatically uninstalled during scheduled scans.

4.1.1 Deployment options

The general deployment options allow you to configure the actions and processes that must be triggered pre/post deployment of the selected file. Supported actions include:

- Send notification/deployment request to the currently logged on user.
- Automated reboot of target computer following deployment operation.

To edit the general deployment options:

1. Under **Common Tasks** in the left pane click **Deployment** options...

Deployment Options
General Advanced
Before deployment:
✓ Warn user (send a message)
Wait for user's approval
Stop services before deployment
Services
Copy software to deploy to target computer via:
Administrative shares
Custom share:
After deployment:
O not reboot/shut down the computer(s)
Reboot the target computer(s)
Let the user decide when to reboot
Shut down the target computer(s)
Delete copied files from remote computer(s) after deployment
Computer filters
Remember settings

Screenshot 35 - General deployment options

2. Configure the **Before deployment** options.

3. Configure the **Copy software to deploy to target computer via:** option by selecting between administrative or a custom shares.

4. Configure the After deployment options.

Deployment Options
General Advanced
Number of deployment threads: 5 (max 10) WARNING: Deploying with more than 5 threads may render the UI unresponsive until the deployment operation is complete.
Deployment timeout (seconds):
Deploy patches under the following administrative account (domain\user or user@FQDN format)
Account name:
Password:
Note: Only select this option if you want to run the installation packages on the target computers under an account other than the Local System account. If you need to select this option, make sure that the specified account has the Log on as service privilege on the target computers.
Deploy patches with their original names
Remember settings

Screenshot 36 - Advanced deployment options

5. Click **Advanced** tab to configure advanced deployment options including:

- the number of patch deployment threads that will be used
- deployment timeout
- authentication credentials for the deployment agent service.

4.2 Patch management

Apart from automatically downloading Microsoft patches and service packs, GFI LANguard can also deploy these updates network-wide as well as recall any patches that have already been deployed. Patches are generally recalled due to newly discovered vulnerabilities or problems caused by the installation of these updates such as conflict issues with present software or hardware. Examples of updates recalled by the manufacturer include patches MS03-045 and MS03-047 for Exchange that was released by Microsoft on October 15, 2006.

Both patch deployment and patch rollback operations are managed by an agent service, which handles all file transfers between GFI LANguard and the remote targets. This service is installed automatically on the remote target computer during patch deployment process.

Important notes

1. To successfully deploy missing patches ensure that GFI LANguard is running under an account that has administrative privileges.

2. Ensure that the NetBIOS service is enabled on the remote target computer. For more information on how to enable NetBIOS, refer to the <u>Enabling NetBIOS on a network computer</u> section in this manual.

3. A complete list of Microsoft products for which GFI LANguard can download and deploy patches is available at http://kbase.gfi.com/showarticle.asp?id=KBID001820.

4. GFI LANguard can be set to automatically download missing patches and service packs discovered during a network security scan. For more information, refer to the <u>Configuring Microsoft updates</u> section in this manual.

4.3 Deploying missing updates

💽 GFI LANguard						
File Tools Configure Help					Discuss this	version
Network Audit Dashboard Co	nfigu	ration Utilities General				
Scan Analyze Remediate	-					
Scall Service Filenceaute						
Patch Management:	1	Deploy Micros	oft Pate	hes		
Deploy Microsoft Patches	-	Specify undates to apply	and select St.	art to start the deployme	ent of undates	
Uninstall Microsoft Patches						
Uninstall Microsoft Service Packs	Sor	t by computers Sort by pat	ches Deplo	yment status		
Application Management:		Specify the target com	outers whe	re to deploy patcl	hes	
Deploy Custom Software						
		Computer name	Language	Notes		
Other Options:		V 👹 ESM_DEMO	English			
Semote Desktop Connections						
Credentials						
Authenticate using:						
		4				Þ
Password:	0	Specify which patches	to deploy t	o which compute	rs	
	9	specify which patenes	to acpicy t	o which compute	15	
Remember credentials		Update file name		State	Bulletin	Applica
Use computer profiles		🔽 🌺 Windows6.0-KB951072-	v2-x86.cab	Downloaded	Not Available (951072)	Windo
(Edit)		Windows6.0-KB953733-	x86.cab	Downloaded	MS08-047 (953733)	Windo
Common Tasks		Windows6.0-KB951698-	x86.cab	Downloaded	MS08-033 (951698)	Windo
		Windows6.0-KB951376-	x86.cab	Downloaded	MS08-030 (951376) MC00.033 (040001)	Windo
Deployment options			X06.CaD /96.ov/0	Not downloaded	MS00-023 (340001) MS07.040 (929729)	Windo
Go to: Patch auto-download options		MDF1.1sp1•Kb323/23/	oo.exe	NUL UUWHIUAUEU	M307-040 (323723)	WINUU
Edit proxy settings		•		III		F.
Ø Help:						
Deploying Microsoft updates	3	Launch deployment				
Deploying Microsoft updates automatic		 			Pearl	Chard
		 Deploy immediately 			neset	Juait
		Deploy on 5/ 5/200	9 🔲 🕆 at	8:45:30 AN		
		1				

Screenshot 37 - Deploying missing service packs and patches

To deploy missing patches and service packs on specific computers:

1. Launch a scan or load saved scan results from **Network Audit** ► **Scan**.

2. Once the scan results are loaded, click on the **Network Audit** ► **Remediate** tab.

3. Click on Go to: Deploy Microsoft Patches or Go to: Deploy Microsoft Service Packs accordingly.

	Specify the target computers where to deploy patches					
Language	Notes					
English						
	Language English					

Screenshot 38 - Deploying missing patches on selected computers

4. From list of target computers (labeled as '1'), select the target computers on which patches/service packs will be deployed. Right click on list to access **Select/Unselect all** options.

Update file name	State	Bulletin	Applicati
📝 🍢 Windows6.0-KB951072-v2-x86.cab	Downloaded	Not Available (951072)	Windows
📝 塔 Windows6.0-KB953733-x86.cab	Downloaded	MS08-047 (953733)	Windows
📝 塔 Windows6.0-KB951698-x86.cab	Downloaded	MS08-033 (951698)	Windows
📝 塔 Windows6.0-KB951376-x86.cab	Downloaded	MS08-030 (951376)	Windows
📝 塔 Windows6.0-KB948881-x86.cab	Downloaded	MS08-023 (948881)	Windows
📝 🋂 NDP1.1sp1-KB929729-X86.exe	Not downloaded	MS07-040 (929729)	Windows

Screenshot 39 – Select the updates to deploy

5. From the list of missing patches/service packs (labeled as '2'), select the updates to be downloaded and deployed. Right click on the list to access **Select/Unselect all** options.

3 Launch depl	loyment	
Oeploy immedia	ately	Reset Start
🔘 Deploy on	5/ 5/2009 , at 8:45:30 A ►	

Screenshot 40 – Deploy patches

6. Select the preferred launch deployment option.

- To schedule patch/service pack deployment to a later date/time choose the **Deploy on** option and specify date/time.
- To start the deployment immediately, select **Deploy immediately** and click **Start**.
- 7. Follow on screen instructions (if applicable)

Update file name	State	Bulletin	Application
📝 塔 Windows6.0-KB951072-v2-x86.cab	Downloaded	Not Available (951072)	Windows
📝 塔 Windows6.0-KB953733-x86.cab	Downloaded	MS08-047 (953733)	Windows
📝 塔 Windows6.0-KB951698-x86.cab	Downloaded	MS08-033 (951698)	Windows
📝 塔 Windows6.0-KB951376-x86.cab	Downloaded	MS08-030 (951376)	Windows
📝 塔 Windows6.0-KB948881-x86.cab	Downloaded	MS08-023 (948881)	Windows
📝 🋂 NDP1.1sp1-KB929729-X86.exe	Not downloaded	MS07-040 (929729)	Windows
•			•

4.3.1 Identifying the download queue status

Screenshot 41 - Identifying the download queue status

The icons next to each update file as well as the 'State' column show the current download status. These icons indicate the following states:

- Bownloaded
- **O** Currently being downloaded
- 🌯 Not downloaded.

4.3.2 Monitor the patch deployment process

💽 GFI LANguard	
File Tools Configure Help	Discuss this version
Network Audit Dashboard	Configuration Utilities General
🇞 Scan 🐁 Analyze 🍇 Remediat	te
Patch Management: Deploy Microsoft Patches Deploy Microsoft Service Packs Uninstall Microsoft Patches Uninstall Microsoft Patches Management:	Deploy Microsoft Patches Specify updates to apply and select Start to start the deployment of updates Sort by computers Sort by patches Deployment status ESM_DEMO Preparing to copy 5 files
🍓 Deploy Custom Software	Copying process started
🄩 Uninstall Applications	Copying 4eDBVBG1EBeQZnnsjujwmw4Vd+4=_Windows6.0-KB951072-v2-x86.cab (750.8 KB)
Other Options: Credentials:	 Copying #KViofZn3yWB0GZQmhYQ+L_kVvg=_Windows6.0+KB953733-x86.cab (287.6 KB) Copying N49dL3hnxRzcVdoJXq0Cm+0xwc=_Windows6.0+KB951698-x86.cab (668.1 KB) Copying JIsYARR32n7dfB00DIbkQQQfq0nE=_Viindows6.0+KB951376-x86.cab (243.8 KB) Copying Let +jvrK78dg182EP_17g280uv8k=_Windows6.0+KB948881-x86.cab (44.2 KB) Copying process completed
Authenticate using:	Batch file copy OK
Currently logged on user	NT machine. Starting the GFI LANguard Patch agent service on the remote machine
Usemanie.	 Service is not installed. Installing the service
Password:	Copying the files needed
	· V Service installed
Remember credentials	Service started
Use computer profiles	Deploying pkgmgr /ip /norestart /quiet /s:temp /m:4eubvbG1EBeQ2nnsjujwmw4vd+4=_windows6.0-kBs
<u>(Edit)</u>	
Common Tasks:	
Deployment options Go to: Patch auto-download options Edit proxy settings	
Ø Help:	Reset Start
Deploying Microsoft updates Deploying Microsoft updates autom	*

Screenshot 42 - Monitoring the deployment process

To view the patch deployment activity in progress, click the **Deployment Status** tab located at the top of the right pane.





Screenshot 43 - Stopping active downloads

To stop an active patch-download, right-click on the respective patches and select **Cancel Download**.

Patch properties		×
General		
Patch file name:	NDP1.1sp1-KB929729-X86.exe	
Bulletin:	MS07-040 (929729)	
Affected product:	Windows	
Source URL:		
http://www.download	.windowsupdate.com/msdownload/update/software/s	
Download directory:		
C:\Program Files\GFI	LANguard 9.0\Repository\English	
Deploy patch with the	following command line parameters:	
-q		
	OK Cancel App	ly

4.3.4 (Optional) Configure alternative patch-file deployment parameters

Screenshot 44 - Patch file properties dialog

You can optionally configure alternative patch deployment parameters on a patch-by-patch basis. Parameters that can be configured include:

- Download URL
- Destination path of the downloaded patch file.

To change the deployment and download settings of a missing patch:

1. Right click on the respective patch file and select **Properties**.

2. Make the required changes and click **OK** to finalize your configuration.

4.3.5 Uninstall patches already deployed on targets

To roll back deployed patches and service packs:

1. Go to **Network Audit** ► **Scan** and launch a scan on the computer(s) from which you need to roll back patches.

2. From the scan results, right click on listed computers and select **Remediate ► Uninstall Microsoft patches**

3. Select the target computer.

File Tools Configure Help			Discuss this version
Network Audit Dashboard Cont	figuration Utilities General		
👫 Scan 🐁 Analyze 🍇 Remediate			
Patch Management: Palpoy Microsoft Patches Deploy Microsoft Service Packs Uninstall Microsoft Patches Uninstall Microsoft Patches Uninstall Microsoft Patches Deploy Custom Software Uninstall Applications Options:	Uninstall Mic Specify updates to un Sort by computers Sort by p Specify the target con Computer name Computer name	rosoft Patc nstall and select St atches Uninstal nputers where Language English	hes ant to start the uninstall of updates I status to uninstall patches from Notes
Semote Desktop Connections			
Cradentiale			
Authenticate using:			
	4		II •
Password:	Specify which patche	s to uninstall f	rom which computers
Remember credentials	Bulletin	Application	Title
Use computer profiles	📝 🔇 MS09-014 (963027)	Windows	Cumulative Security Update for Internet Explorer ; 😑
(Edit)	📝 🔮 MS09-013 (960803)	Windows	Security Update for Windows Vista (KB960803)
Common Tasks:	MS09-012 (952004)	Windows	Security Update for Windows Vista (KB952004)
	MS03-012 (336572)	Windows	Security Update for Windows Vista (KB9585972)
Deployment options	MS09-007 (960225)	Windows	Security Update for Windows Vista (KB960225)
	🔲 🙆 Not Available (960715) Windows	Update Rollup for ActiveX Killbits for Windows Vis
W Help:		A Constanting	C
Uninstalling Microsoft updates			0
	Launch deployment		
			Posst Start
	Uninstall immediately		ineset Statt
	O Uninstall on 5/5/2	009 🤍 🛛 at	9:20:25 AF
			.:

Screenshot 45 – Uninstalling a patch

4. Select the patches or service packs to be uninstalled from selected targets.

5. Click Start to initiate the uninstall process.

4.3.6 Monitoring the patch uninstall process

To view the patch rollback progress, click on the Uninstallation Status tab.

4.4 Deploying custom software

In addition to Microsoft security updates (i.e. patches, etc.), GFI LANguard also allows you to remotely deploy third party or custom software network-wide. Software that can be remotely deployed via this engine includes:

- Security applications such as complete anti-virus/anti-spyware solutions, software firewalls and more
- Third party software updates and patches such as anti-virus/antispyware signature file updates
- Custom code such as scripts and batch-files
- Desktop applications such as MS Office 2007 and more.

File Tools Configure Help				Discuss this version
Network Audit Dashboard Co	onfigurati	on Utilities Gen	eral	
Scan 👫 Analyze 🍇 Remediate				
Patch Management:	-	Deploy Cu	stom Software	
Leploy Microsoft Service Packs		Specify the custon	n software (e.g. custom scripts) which will be dep	ployed to target computers
Uninstall Microsoft Patches	Den	lovment Configuration	Deployment Status	
	Dep	loyment configuration	Deployment Status	
Application Management:		Specify the softwa	re to be deployed	
Deploy Custom Software Uninstall Applications			. ,	
		Software Location	Parameters	Add
Other Options:	-			Edit
Tenole Desktop Connections				Remove
Credentials:	-			
Authenticate using:		Specify the target	computers where to deploy softwar	
Credentials: Authenticate using: Currently logged on user	2	Specify the target	computers where to deploy software	e
Credentials: Authenticate using: Currently logged on user	2	Specify the target	computers where to deploy softwar	e Add
Credentials: Authenticate using: Currently logged on user	2	Specify the target	computers where to deploy softwar	e Add Remove
Credentials: Authenticate using: Currently logged on user Usemame: Password:	2	Specify the target	computers where to deploy software	e Add Remove Select
Credentials: Authenticate using: Currently logged on user Usemame: Password: Remember credentials	2	Specify the target	Notes	e Add Remove Select
Credentials: Authenticate using: Currently logged on user Usemame: Password: Remember credentials Use computer profiles (For a)	2	Specify the target	computers where to deploy softwar	e Add Remove Select Import
Credentials: Authenticate using: Currently logged on user Usemame: Password: Password: Buse computer profiles (Edit) Common Tasks:	2	Specify the target	computers where to deploy softwar	e Add Remove Select Import
Credentials: Authenticate using: Currently logged on user Usemame: Usemame: Password: Remember credentials Use computer profiles (Edit) Common Tasks: Edit deelement entime	2	Specify the target	computers where to deploy softwar	e Add Remove Select Import
Credentials: Authenticate using: Currently logged on user Usemame: Usemame: Password: Remember credentials V Use computer profiles (Edt) Common Tasks: Edt deployment options	2	Specify the target	Notes	e Add Remove Select Import
Credentials: Authenticate using: Currently logged on user Usemame: Password: Remember credentials Use computer profiles (Edit) Common Tasks: Edit deployment options Whelp:	2	Specify the target Computer Name	computers where to deploy software Notes	e Add Remove Select Import
Credentials: Authenticate using: Currently logged on user Usemame: Password: Remember credentials Use computer profiles (Edit) Common Tasks: Edit deployment options Whelp: Deploying custom software	2 2 3	Specify the target Computer Name	computers where to deploy softwar	e Add Remove Select Import Reset Deploy

4.4.1 Enumerating the software to be deployed

Screenshot 46 - Deploy custom software

To specify which software to deploy:

- 1. Click on **Network Audit** tab ► **Remediate**.
- 2. Click Deploy Custom Software.

Specify the software to be depl	oyed
Software Location	Parameters
C:\Program Files\GFI\LANguard 9.0 C:\Program Files\GFI\LANguard 9.0 C:\Program Files\GFI\LANguard 9.0	-z -m -q

Screenshot 47- List of software to be deployed

3. From list of software to be deployed (labeled as '1'), click **Add...** and specify the path to the application to be deployed.

4. Specify any additional parameters needed by the application and click **OK**.

Computer Name	Notes
 192.168.3.20	WARNING : Filters will not work on this comp

Screenshot 48 - Target computers for software deployment

5. From list of target computers (labeled as '2'), click **Add...** to specify the target computers on which the software will be deployed.

3 Launch so	ftware deployment			
Oeploy imme	diately		Reset	Deploy
Deploy on	5/ 5/2009 🔲 🔻 at	9:15:48 AN		

Screenshot 49 - Launch deployment options

6. Select the preferred launch deployment option.

- To schedule patch/service pack deployment to a later date/time choose the **Deploy on** option and specify date/time.
- To start the deployment immediately, select **Deploy immediately** and click **Start**.

7. Repeat the process described above for every file/software to deploy.

8. Follow on screen instructions (if applicable) and switch to the **Deployment Status** tab to view the progress of the installation.



Screenshot 50 - Software deployment status

4.5 Uninstall applications

Through application uninstallation, you can control which applications are installed, on which computers, and uninstall any unauthorized applications present on network computers.

To uninstall applications:

1. Select **Network Audit** tab ► **Remediate** tab and click **Uninstall Applications**.

GFI LANguard			
File Tools Configure Help			Discuss this version
Network Audit Dashboard Conf	iguration Utilities General		
Scan 🔊 Analyze 🌺 Remediate	·		
Scan Analyze Remediate Patch Management: Deploy Microsoft Patches Deploy Microsoft Patches Deploy Microsoft Patches Uninstall Microsoft Service Packs Application Management: Deploy Custom Software Uninstall Applications Other Options: Remote Desktop Connections Credentials: Authenticate using: Usemame:	Uninstall Unauthoriz Specify applications to uninstall ar Sort by computers Sort by applications Specify the target computers w Computer name Computer name Computer name Computer name	zed Applications nd select Start to start the uninstall of ap Uninstall Status where to uninstall application	plications s from
Password:	Specify which applications to	uninstall from which compute	ers
Remember credentials	Application name	Version Publisher	Uninstall string 🔦
Use computer profiles (Edt) Common Tasks: Deployment options	Microsoft SQL Server Setup Su MSXML 4.0 SP2 (KB954430) SQLXML4 SQLXML4 Microsoft Office 2003 Web Com Microsoft SQL Server 2005 Bac	9.00.1399 Microsoft Corporation 4.20.9870.0 Microsoft Corporation 9.00.1399 Microsoft Corporation 11.0.6558.0 Microsoft Corporation 8.05.1054 Microsoft Corporation	MsiExec.exe ↓ MsiExec.exe ↓ MsiExec.exe ↓ MsiExec.exe ↓ MsiExec.exe ↓
Help: <u>Uninstalling applications</u> <u>Removing unauthorized software automati</u>	GFI Report Center Framework GFI Report Center Framework TH GO Uninstall Uninstall immediately Uninstall on 5/ 5/2009	3.5.113 GFI Software Ltd Re 3.5.113 GFI Software Ltd Re	MsiExec.exe , *
			.:

Screenshot 51 - Uninstall applications

2. From the **Uninstall Unauthorized Applications** screen, select either the **Sort by computers** tab (view list of computers and the relative applications to uninstall) or the **Sort by applications** tab (list of applications and relative computers to uninstall from).

3. Select the applications/computer combination to uninstall.

NOTE: The list of applications displayed relies on the unauthorized applications set up for the scanning profile in use. For more information on how to set up and validate applications to uninstall, refer to the <u>Applications inventory</u> and <u>Application auto-uninstall</u> <u>validation</u> sections in this manual.

4. Select **Uninstall immediately** to immediately uninstall any applications selected or provide a date/time combination in the **Uninstall on** field.

5. Click **Start** to uninstall applications based on your configuration. Review the status of any uninstallation from the **Uninstallation status** tab.

4.6 Remote remediation

Through remote remediation, you can control remote computers using Terminal Services and Remote Desktop Protocol. Remote remediation enables you to install missing patches, service packs and custom software through a remote connection.

To create a new remote connection:

1. Select **Network Audit** ► **Remediate** ► **Remote Desktop Connections** ► **New Connection.**

New Remote Desktop Con	nection 💽
Open Remote Desktop	
New Remote Desktop	o Connection
Machine Name	PC1
Domain	vexch2k31.local
User Name	administrator
Password	
Color Depth	TrueColor 🗸
	Share Printers
	Share Disk Drives
	Connect Cancel

Screenshot 52 – Creating a remote connection

2. Specify the credentials required to connect to the remote machine.

3. Click **Connect** to open a remote connection with the target machine.

4.7 Automatic Remediation

Through scheduled scans, you can launch automatic remediation actions. This enables you to automatically download and deploy missing patches as well as to automatically uninstall unauthorized applications during scheduled operations.

To uninstall software, a 3-stage process is required in order to identify whether the selected application supports silent uninstall:

Stage 1 – Select the application to be auto-uninstalled

Stage 2 – Ensure that application supports silent uninstall by trying to remotely uninstall the application. This is called the validation process.

Stage 3 – Setup a scheduled scan, which will successfully uninstall all instances of that application from targets during a scheduled scan.

NOTE: Auto-remediation option of scheduled scans and application un-authorization only work for scanning profiles which perform Missing patches detection and/or Installed application detection

Important notes

1. Always test patches in a test environment before deployment.

2. By default Microsoft updates are not enabled for automatic deployment. Manually approve each patch (as it is tested) or set all Microsoft updates as approved.

4.7.1 Automatically deploy missing Microsoft updates

To automatically deploy missing patches follow the instructions below before setting up a scan with auto-remediation options.

Step 1: Approve the patches to deploy automatically.

1. From the **Configuration** tab, navigate to **Microsoft Updates** ► **Patch Auto-Deployment**.

2. Select the patches to approve for auto-deployment. Optionally, set the automatic patch approval options by selecting the **To automatically approve patches and/or service packs, click here** option. For more information, refer to the <u>Auto-deployment settings</u> section in this manual.

Step 2: Set up a scheduled scan.

Set up a scheduled scan that will have the option to automatically deploy all approved missing Microsoft updates. Within the scheduled scan, define what computers will be scanned for missing Microsoft updates and the frequency.

Step 3: Review scheduled scan status

Select **Dashboard** ► **Scheduled Operations** to review the status of scheduled scans and auto-remediation operations

4.7.2 Automatically uninstall unauthorized applications

To automatically uninstall unauthorized applications follow the instructions below before setting up a scan with auto-remediation options.

Step 1: Define unauthorized applications list.

1. From the **Configuration** tab, select **Applications inventory** subnode.

2. In the right pane, click the application to unauthorized under the heading **unauthorized on** column.

3. Select a scanning profile to mark the application as unauthorized for that profile. Click **Next** to continue.

4. Review the currently affected applications screen and click **Finish** to finalize settings.

Refer to the <u>Applications inventory</u> section in this manual for further on defining unauthorized applications.

Step 2: Validate the applications to remotely uninstall.

1. From the **Configuration** tab, select **Applications inventory** ► **Auto-Uninstall Validation** sub-node.

2. In the right pane, select an application to validate click **Validate...** button.

3. In the **Application auto-uninstall validation** wizard click **Next** in the Welcome screen and select the computer on which to test the application auto-uninstall. Click **Next** to continue.

4. Provide the authentication details for the validation operation and click **Next** to continue.

5. Review the **Auto-uninstall validation wizard** information and click **Start** to validate application auto-uninstall.

For more information on auto-uninstall validation refer to <u>Application</u> <u>auto-uninstall validation</u> in this manual.

Step 3: Set up a scheduled scan.

Define a scheduled scan that will have the option to automatically uninstall all unauthorized applications, which are validated. Within the scheduled scan, define what computers are scanned, the frequency and which the unauthorized applications are.

Step 4: Review scheduled scan status

Select **Dashboard** ► **Scheduled Operations** to review the status of scheduled scans and auto-remediation operations.

5. GFI LANguard dashboard

5.1 Introduction

GFI LANguard provides you with a dashboard, which graphically indicates the status of various operations that might be currently active, or are scheduled.

Access the GFI LANguard dashboard from the **Dashboard** tab.

5.2 Viewing the global security threat level



Screenshot 53 - Status Monitor: Statistics tab

The **Security Status** tab provides you with extensive security information based on data acquired during scans. This enables you to determine at a glance the current network vulnerability level, the top most vulnerable computers, the number of computers in the database. It also provides you with a breakdown of the vulnerable computers according to their vulnerability level.

NOTE: The data displayed in the **Security Status** tab is dynamically worked out by GFI LANguard based on previous scans.

5.3 Monitoring scheduled activity

Scheduled Activity is all the GFI LANguard operations that have been set up to trigger at a later date and time. Through the **Scheduled Operations** tab in the Dashboard tab, you can monitor these operations and stop operations in progress or remove finished operations details.

💽 GFI LANguard					- • •	
File Tools Configure Help				Discu	iss this version	
Network Audit Dashboard Cont	figuration Utilitie	es General				
🜒 Security Status 🕘 Scheduled Opera	tions					
Scheduled Activity:						
Scheduled Security Scans Microsoft Updates Download Remediation Operations Konsoft Updates Download Konsoft Updates Download						
Product Updates Activity	Target	Profile	Start Time	Status	Remaining Ti	
Common Tasks: Filter scheduled scans Go to: Scheduled scans Actions: Stop selected scan(s) View remediation details View scan results details We scan results details	192.168.3.66 192.168.3.66	Full Vulnerability Assessm Full Vulnerability Assessm	5/5/2009 10:56:08 AM 5/5/2009 10:55:46 AM	running (0/1) running (0/1)	2 minutes 2 minutes	
Monitoring scheduled operations Scheduled scans	•	m				

Screenshot 54 - Dashboard: Scheduled Operations tab

To view scheduled operations in progress:

1. Select the **Dashboard > Scheduled Operations** tab.

2. Under Scheduled Activity in the left panel, select Security Scans, Patch Downloads, Remediation Options or Updates History and trigger any of the operations from the left panel as required. The Scheduled activity options are described below:

Scheduled Security Scans

The scheduled security scans screen enables monitoring of all the scheduled security scans, which are currently in progress, which have been successfully, or unsuccessfully completed. A scheduled scan can be stopped, by right clicking the security scan, and selecting **Stop selected scan(s)** option.

For more information on how to set up a new scheduled scan, refer to <u>Setting up a scheduled scan</u> section in this manual.

Microsoft Updates Downloads

The Microsoft Updates Downloads screen enables you to monitor, pause, cancel or change priority all the scheduled patch downloads. For more information on how to configure scheduled patch downloads refer to <u>Auto-download settings</u> section in this manual.

Remediation Operations

The remediation operations screen enables you to monitor as well as cancel all the scheduled remediation features within GFI LANguard. For more information on how to set up scheduled remediation operations, refer to <u>Automatic Remediation</u> section in this manual.

Product Updates Activity

The Product updates activity screen enables you to monitor or edit GFI LANguard scheduled or manual updates. For more information on how to set up scheduled or manual updates, refer to <u>Program updates</u> section in this manual.

6. Configuring GFI LANguard

6.1 Introduction

GFI LANguard allows you to run vulnerability scans straight out of the box – using the default settings configured prior to shipping. However, if required you can also customize these settings to suit any particular vulnerability management requirements that your organization might need. You can customize and configure various aspects of GFI LANguard including scan schedules, vulnerability checks, scan filters and scan profiles.

6.2 Scheduled Scans

Scheduled scans enable you to automate the process of performing regular scans, auditing and remediation procedures.

6.2.1 Reviewing, editing or deleting scan schedules

Scan schedules can be reviewed, edited, or deleted from the **Configuration ► Scheduled Scans** node.

🌯 🛸 🛼 🍢 🇠 O

Screenshot 55 - Scheduled scan toolbar

All the scans are listed in the review page together with the relevant information. Use the scheduled scan toolbar to:

Complete/C	Lombination Scans Scanning Profiles	
*5	Add new scan button – Use this button to display the New	
	scheduled scan wizard and create a new scheduled scan.	
	Reporting options button - Use this button to display the	
<u>8</u>	Scheduled Scans Reporting Options dialog for the selected	
	scheduled scan. For more information on how to set up	
	reporting options, refer to the How to setup a Scheduled Scan	
	section in this manual.	
.	Delete button – Use this button to delete the selected	
	scheduled scan.	
15	Properties button – Use this button to review and edit the	
	properties of the selected scan.	
~~	Enable/Disable button – Use these buttons to toggle the status	
	of the selected scan between enabled and disabled. This	
	enables you to activate/suspend a scanning schedule without	
	deleting the scheduled scan.	
	Scan now button – Use this button to trigger the selected	
Ø	scheduled scan. This button overrides the scheduled scan	
	date/time settings and executes an immediate scan.	

6.2.2 Scheduled scan properties

The scheduled scan properties page enables you to configure all the parameters of the scheduled scans.

To use the scheduled scan properties tab:

1. Go to **Configuration** tab ► **Scheduled Scans**

2. Select the scheduled scan and click the Scheduled Scan **Properties** button.

192.168.3.66 Proper	ties		×			
General Logon C	redentials Advance	d Auto Remediation				
Configure the scheduled scan						
Scan target:	192.168.3.66] [
Scanning profile:	Scanning profile: Full Vulnerability Assessment					
Description:						
Perform a scan:						
One time or	ly					
every:	1	Days 🔻				
<u>N</u> ext scan:	5/ 6/2009 🔲 🔻	10:55:57 AM 🚔				
	ОК	Cancel Appl	y)			

Screenshot 56 - Scheduled Scan properties - General tab

3. Edit the properties as required and click \mathbf{OK} to finalize your configuration:

- **General** tab Use this tab to make changes to scan target setting, type of scanning profile to use description and scan frequency.
- Logon Credentials tab Use this tab to specify logon credentials to be used when scanning the specified target.
- Advanced tab Use this tab to specify whether GFI LANguard should wait for offline computers to connect to the network. This enables GFI LANguard to postpone the scan on these machines and keep track of targets pending a scan e.g. laptops or other mobile devices, which are not connected to the network. As soon as these devices are connected back to the network, scanning will take place.
- Auto Remediation tab Use this tab to configure the remediation options applicable to the scan being configured. This includes

downloading and installing missing patches and service packs and unauthorized software un-installation.

6.3 Computer profiles

When working in both large and smaller-sized networks, you will inevitably have to log in with different sets of credentials on different computers. Systems such as Linux-based systems often make use of special authentication methods such as public key authentication. Such authentication methods generally require special/custom logon credentials such as private key files instead of the conventional password strings.

Through computer profiles, you can specify a different set of logon credentials for every target computer. The scanning engine can then refer to the logon credentials stored in these computer profiles when authenticating to target computers. This way you will not need to specify a default set of logon credentials prior to starting a network scan. It also makes it possible to scan target computers that require different logon credentials and authentication methods in the same (single) session. For example, you can run vulnerability checks on Windows targets which require username/password credential strings and Linux based targets which require username/SSH private key files, in a single scanning session.

6.3.1 About SSH private key authentication

GFI LANguard connects to Linux-based target computers through SSH connections. In public key cryptography, two keys (in the form of text files) are used to verify the authenticity of an SSH connection request. These keys are identified as the **SSH private key** and **SSH public key**.

The SSH key pair (i.e. public and private keys) are manually generated using a third party tool such as SSH-KeyGen (generally included by default in the Linux SSH package).

The SSH private key is the half of the key pair that the scanning engine will use to authenticate to a remote Linux based target. This means that the SSH private key is used instead of the conventional password string and hence must be stored on the computer which is running GFI LANguard

The SSH public key is the part which the remote target computer will use to challenge the authentication of GFI LANguard and is stored on the remote target computer(s).

All new computer profiles are disabled by default. For information on how to enable newly created computer profiles, refer to the Enabling/Disabling Profiles section in this manual.

6.3.2 Creating a new computer profile

- 1. Select Configuration
 Computer Profiles
- 2. Under Common Tasks, click on New computer(s) profile...
- 3. In the **General** tab, specify the target computer name.

Computer(s) profile					
General Logon Credentials					
Specify credentials to use to log on to target computer(s).					
Logon to target computer(s) using:					
Security context of the account under which the security scan is being made.					
O Alternative credentials:					
User Name:					
Password:					
SSH private key authentication (Linux/Unix logons):					
User Name:					
Key file:					
NOTE: To scan Windows computers use the scan security context (currently logged on user/service user) or alternative logon credentials. To scan non-Windows computers such as Linux machines you need to specify alternative credentials or a SSH private key file.					
OK Cancel					

Screenshot 57 - Computer profile properties dialog

4. Click on the **Logon Credentials** tab and specify credentials accordingly.

5. Click ${\bf OK}$ to finalize configuration.
| r | | | , |
|------------------------------------|------|-----------------------------|----------------------|
| 💽 GFI LANguard | | | |
| File Tools Configure Help | | | Discuss this version |
| Network Audit Dashboard | Conf | iguration Utilities General | |
| Configurations: | Â. | * 🐼 🐮 🕷 | |
| | | Computer(s) Logon method | Username |
| Scheduled Scans | | Alternative credentials | administrator |
| Applications Inventory | | New P | |
| Auto-Uninstall Validation | | 🍓 Enable | |
| Patch Auto-Deployment | | 🗊 Delete | |
| Patch Auto-Download | | Properties | |
| Alerting Options | | | |
| Program Updates | | | |
| | | | |
| | = | | |
| ۰ III ۲ | | | |
| Common Tasks: | | | |
| New computer(s) profile | | | |
| | | | |
| Actions: | | | |
| Edit computer profile's properties | | | |
| Delete computer profile | | | |
| Enable selected profiles | | | |
| Disable selected profiles | | | |
| Ø Help: | | | |
| Computer profiles | Ŧ | · | 4 |
| | | | .:: |

6.3.3 Configuring computer profile parameters

Screenshot 58 - List of existing computer profiles

To configure/change the parameters of an existing computer profile:

1. Click Configuration Computer Profiles.

2. Right-click the computer profile to configure and select **Properties**.

3. Configure the required parameters and click \mathbf{OK} to finalize your configuration.

6.3.4 Enabling/Disabling Profiles

By default all, the newly created computer profiles are disabled. GFI LANguard will therefore not use these profiles during vulnerability scans unless you enable them.

To enable (or disable) profiles:

1. Click **Configuration** ► **Computer Profiles** and select one or more profiles to be enabled/disable.

2. Right-click on these profiles and select **enable G** / **disable G** accordingly.

6.4 Applications inventory

GFI LANguard applications inventory provides a list of all applications detected during past scans. This list is used to specify which applications are unauthorized. You can also manually add applications to the list. You can do this by specifying the entire name as well as a partial name specify generic names or part of an application name.

Automatically, GFI LANguard scans the list of applications and detects partial names.

To indicate an application as unauthorized:

1. Click on **Configuration** > **Applications inventory** sub-node.

2. From the list of applications detected, locate the application to set to unauthorized by clicking in the **Unauthorized on** column entry.

Configure application wizard					
Step 1 of 2: Mark application as unauthorized Select the profiles under which the application will be unauthorized					
Configure application: Microsoft SQL Server Setup Support Files (English) (Version: 9.00.1399.06, Publisher: Microsoft Corporation) Unauthorized applications are classified in scan results as 'High Security Vulnerability' To mark this application as unauthorized select the scanning profile(s) which will classify this software as 'High Security Vulnerability'					
this software as 'High Security Vulnerability' Scanning profiles: Full Scan Full Scan (Slow Networks) Software Audit System Information					
Cancel Sack Next > Cancel					

Screenshot 59 - Unauthorized application - scanning profile

3. Select the scanning profile for which this application will be set as unauthorized and click **Next**.

4. GFI LANguard can associate partial names with entries already in the list. As a result, the system will prompt you to confirm whether to apply the same changes also to applications partially have the same name.

5. Click **Finish** to finalize settings.

Adding a new unauthorized application

To manually add a new application without selecting an application from the applications inventory:

1. Click on **Configuration** tab > **Applications inventory** sub-node.

2. Under Common Tasks, click on Add a new application...

3. The **Add unauthorized application wizard** is launched. In the welcome, screen click **Next** to proceed.

Add unauthorized application	n wizard
Step 1 of 4: Specify applic Specify a generic applica version	cation details ation name and optional details such as publisher and
Specify a complete or pa Application name	artial application name by which this application can be identified:
Note: Partial appli	cation names are accepted.
Optionally you can provi	de the following details:
Version Number	1.0
Publisher	My Application Software Inc.
(2) <u>Tell me more</u>	< Back Next > Cancel

Screenshot 60 – Applications inventory wizard

4. Specify application name. Optionally you can also specify version number and publisher. Click **Next** to continue.

5. Select the scanning profiles on which you would like the unauthorized application (e.g. Full Scan) and click **Next** to continue.

6. Specify whether changes made will effect applications, which have partial/full name match. Click **Next** to continue.

7. Review **Add application wizard** information and click **Finish** to finalize configuration.

6.5 Application auto-uninstall

Application auto-uninstall entails that applications marked as unauthorized for specific scanning profiles are first validated for a successful uninstall on a test machine. Subsequently a scheduled scan base on the scanning profile for which the application is marked as unauthorized is configured to auto-uninstall applications.

For more information on how to set a scheduled scan, refer to the <u>Setting up a scheduled scan</u> section in this manual.



6.5.1 Application auto-uninstall validation

Screenshot 61 – Application auto-uninstall validation

Application auto-uninstall validation enables you to validate the uninstallation procedure for the applications which are to be automatically uninstalled by GFI LANguard. This is a requirement prior to the actual uninstallation process and no applications are uninstalled during scans unless verified.

NOTE: For more information on how to mark applications as unauthorized and therefore enable their uninstallation, refer to the <u>Applications inventory</u> section in this manual.

1. Click on **Configuration ► Applications Inventory ► Auto-Uninstall Validation**

2. In the right pane select an application to validate click **Validate...** button

3. In the **Application auto-uninstall validation** wizard click **Next** in the Welcome screen and select the computer on which to test the application auto-uninstall. Click **Next** to continue.

4. Provide the authentication details for the validation operation and click **Next** to continue.

5. Review the **Auto-uninstall validation wizard** information and click **Start** to validate application auto-uninstall.

6.5.2 Managing scheduled scans

The **Manage applicable scheduled scans** button enables you to review or edit scheduled scans, which will perform the validated applications auto install. To manage a scheduled scan:

1. From the Auto-Uninstall validation pane, click **Manage applicable** scheduled scans... button.

anage applicable sche	dule scans		
Manage applicable s This is a list of all s create a new sche	chedule scans cheduled scans that ma duled scan.	ay uninstall at least an application validated	for auto-uninstall or
 Scan target 	Profile	Will uninstall	Scan description
Cia	<< There k on 'Create a new sche	are no applicable scheduled scans! >> eduled scan'to configure an applicable sc	heduled scan
	Edit selected scan	Create a new scheduled scan	View all scheduled scans
How can a scheduled sc	an appear in this list?		Close

Screenshot 62 - Manage applicable schedule scans

2. From the Manage applicable schedule scans dialog, perform the following tasks:

a. Edit existing scheduled scans by selecting an existing scan and clicking **Edit selected Scan...** This will take you to the scan properties of the scheduled scan. For more information on how to edit an existing scheduled scan, refer to <u>Scheduled Scans</u> section in this manual.

b. Create a new scheduled scan by clicking on **Create a new scheduled scan...** button. This will display the new scheduled scan wizard where you can create a new scheduled scan, which will automatically uninstall applications. For more information on how to set up a new scheduled scan, refer to <u>Setting up a</u> <u>scheduled scan</u> section in this manual.

c. Review all scheduled scans by clicking **View all scheduled scans** button. This will display the Scheduled scan screen where you will be able to add new, edit or delete scheduled scans. For more information on how to edit an existing scheduled scan, refer to <u>Scheduled Scans</u> section in this manual.

6.6 Configuring Microsoft updates

6.6.1 Auto-deployment settings

GFI LANguard ships with a patch auto-deployment feature, which allows you to automatically deploy missing Microsoft patches and service packs in all 38 languages supported by Microsoft products.

To configure patch auto-deployment:

1. Click on the **Configuration** ► **Microsoft updates** ► **Patch Auto-Deployment**

2. In the right pane, select the patches that you would like to autodeploy. **NOTE:** If patches and service packs are automatically approved for auto-deployment a message, advising you of such status is displayed. To manually approve patches/service packs click the link that enables you to change the status manually approve patches/service packs.

T GFI LANguard							
File Lools Configure Help						Discuss this	version
Network Audit Dashboard Con	nfiguratio	n Utilities Gen	eral				
Configurations:	^	Dotob A		mont			
 		The Patches A for automatic	Auto-Deployment patch deployment	option enables t.	you to select w	which patches are app	roved
Applications Inventory Auto-Uninstall Validation Microsoft Updates		Approve Microso Only approve patch	ft patches and es that were previo	service pactors ously tested and	ks for auto-de d do not cause a	eployment any issues.	
Patch Auto-Deployment		Patch language filter:	English	•			
Alerting Options Database Maintenance Options		To automatically a	pprove patches a	nd/or service p	backs click <u>her</u>	<u>e</u> .	
🛶 Program Updates	_	Approval	Bulletin ID	Severity	QNumber	 Date posted 	Title 🔺
	=	Not Approved	8 MS09-011	Critical	961373	2009-04-14	Secur
		Not Approved	🕴 MS09-011	Critical	961373	2009-04-14	Secur
		Not Approved	🕴 MS09-011	Critical	961373	2009-04-14	Secur
		Not Approved	😵 MS09-011	Critical	961373	2009-04-14	Secur
Common Tasks:		Not Approved	🥹 MS09-013	Critical	960803	2009-04-14	Secur
Advanced options		Not Approved	MS09-013	Critical	960803	2009-04-14	Secur
		Not Approved	MS09-013	Critical	960803	2009-04-14	Secur
		Not Approved	8 MS09-013	Critical	960803	2009-04-14	Secur 👻
Actions		•			1		•
Approve colocted extenses		Find patch:			Find	Show Bullet	tin ID
Remove approval for selected patches	- 6	Define new or re	view existing s	cheduled sca	ans that will p	erform approved p	atche
Show Bulletin ID		Configure scheduled	scans that trigger	r auto-deployme	ent of patches a	nd service packs	
Help: Declaving Microsoft undates automatically	-				Manage	applicable scheduled s	scans
Constitute Processor updates automaticain							

Screenshot 63 - Patch auto-deployment

NOTE: For more information on how to enable patch auto deployment during scheduled scans refer to the <u>Creating a scheduled scan</u> section in this manual.

6.6.2 Advanced Options

From the **Common Tasks** ► **Advanced options** configure the patch approval for auto-remediation advanced options.

A	dvanced	Options 💽	
	General		
	!	Configure patch approval for auto remediation advanced options	
	Ser	nd mail when new patches or service packs are available	
	Enable	patches and service packs auto approval:	
	A	utomatically approve all patches	
	A	utomatically approve all service packs	
	•	By enabling patches and service packs auto approval, all missing patches and service packs will automatically be deployed to target computers after scheduled scans.	

Screenshot 64 - Patch Auto-Deployment Advanced Options

1. Click Advanced Options... to view advanced options dialog.

2. Select the notification and approval options by clicking the appropriate checkboxes and click **OK** to save changes.

6.6.3 Manage applicable scheduled scans

The **Manage applicable scheduled scan...** option enables you to configure scheduled scans that trigger auto-deployment of patches and service packs. For more information on how to use the **Manage applicable scheduled scan** feature refer to <u>Managing scheduled scans</u> section in this manual.

6.6.4 Auto-download settings

GFI LANguard ships with a patch auto-download feature, which enables you to automatically download missing Microsoft patches and service packs in all 38 languages supported by Microsoft products. In addition, you can also schedule patch auto-download by specifying the timeframe within which the download of patches is performed.

To configure patch auto-download:

1. Click on **Configuration** ► **Microsoft updates** ► **Patch Auto-Download** ► Click on link in the right pane.

I	Patch Auto-download Properties					
	General Patch Repository Timeframe					
	Configure patches auto-download options.					
	Enable patch auto-download					
	Select patches to download:					
	All patches NOTE: Download all patches for deployment					
	Only needed patches NOTE: Download only required patches as determined by previous scans					
	Number of download threads: 5					
	OK Cancel Apply					

Screenshot 65- Configuring Patch Auto-download Properties

2. In the General tab, select All patches or Only needed patches.

NOTE: Selecting **All patches** downloads all patches issued by Microsoft, regardless of whether these are required for deployment. The **Only needed patches** option downloads only the patches required for deployment.

3. To change the location where the downloaded patches are stored click the **Patch Repository** tab and specify the required details.

4. To change the timeframe during which patch downloads are performed click on the **Timeframe** tab and specify the required details.

NOTE: GFI LANguard can use patch files downloaded by Microsoft WSUS when deploying missing patches and service packs on target computers. To enable use of Microsoft WSUS downloaded files select the **Use files downloaded by Microsoft WSUS when available** option and specify the path from where the Microsoft WSUS downloaded patches are retrieved.

5. Click **OK** to finalize your settings.

6.7 Configuring alerting options

To configure mail server settings or administrator email address:

- 1. Click Configurations
 Alerting options
- 2. Click the link in the right pane

Alerting Options	Alerting Options Properties				
General					
Specif after	fy SMTP server and email address details for email notifications each scheduled scan.				
<u>T</u> o:	johndoe@vexch2k31.local				
<u>C</u> C:	manager@vexch2k31.local				
Erom:	languard@mailserver.vexch2k31.local				
Server:	localhost				
Port:	25				
SMTP Serve	er requires login				
Pass <u>w</u> ord:		5			
	Verify Settings				
	OK Cancel App	ly 🛛			

Screenshot 66 - Configuring Alerting Options

3. Configure the parameters: To, CC, From, Server, Port, Username and Password as required.

- 4. Click on the Verify Settings button to verify email settings.
- 5. Click **OK** to finalize your settings.

6.8 Database maintenance options

GFI LANguard ships with a set of database maintenance options through which you can maintain your scan results database backend in good shape. For example, you can improve product performance and prevent your scan results database backend from getting excessively voluminous by automatically deleting scan results that are older than a specific number of months.

If you are using a Microsoft Access database backend, you can also schedule database compaction. Compaction allows you to repair any corrupted data and to delete database records marked for deletion in your database backend; hence ensure the integrity of your scan results database.

6.8.1 Selecting a database backend

GFI LANguard 9 supports both Microsoft Access and Microsoft SQL Server (2000 or higher) based database backend.

6.8.2 Storing scan results in a MS Access database backend

To store scan results in a Microsoft Access database:

1. Click on **Configuration** ► **Database Maintenance Options** ► **Database backend settings**...

Properties	
Change Database Saved	Scan Results Scanned Computers Advanced
Current GFI LANguard da	tabase backend settings
Database type:	MS Access
File path:	C:\Program Files\GFI\LANguard 9.0\Data\scanrest
New GFI LANguard data	pase backend settings
Indicate below the new to	upe of database backend to use:
MS Access (MS SQL Server
Please specify the path	where the new database backend is to be located:
C:\Program Files\GFI\LA	Nguard 9.0\Data\scanresults.mdb Browse
	OK Cancel Apply

Screenshot 67 - The database maintenance properties dialog

2. Select the **MS Access** option and specify the full path (including the file name) of your Microsoft Access database backend.

NOTE 1: If the specified database file does not exist, it will be created. **NOTE 2:** if the specified database file already exists and belongs to a previous version of GFI LANguard, you will be asked whether you want to over-write the existing information.

3. Click **OK** to finalize your settings.

6.8.3 Storing scan results in an MS SQL Server database

To store scan results in a Microsoft SQL Server database:

1. Click on **Configuration** ► **Database Maintenance Options** ► **Database backend settings**...

Properties 💽
Change Database Saved Scan Results Scanned Computers Advanced
Current GFI LANguard database backend settings
Database type: MS Access
File path: C:\Program Files\GFI\LANguard 9.0\Data\scanresu
New GFI LANguard database backend settings Indicate below the new type of database backend to use: MS Access MS SQL Server
Please specify the name or IP of the machine containing the SQL Server / MSDE database to use:
Server: win2k8EntServ -
Use NT authority credentials Use the below SQL/MSDE credentials to log into the database backend:
User name: johnDoe
Password:
OK Cancel Apply

Screenshot 68 - Microsoft SQL Server database backend options

2. Select the **MS SQL Server** option and choose the SQL Server that will be hosting the database from the provided list of servers discovered on your network.

3. Specify the SQL Server credentials or select the **Use NT authority credentials** option to authenticate to the SQL server using windows account details.

4. Click on **OK** to finalize your settings.

NOTE 1: If the specified server and credentials are correct, GFI LANguard will automatically log on to your SQL Server and create the necessary database tables. If the database tables already exist, it will re-use them.

NOTE 2: When using NT authority credentials, make sure that GFI LANguard services are running under an account that has both access and administrative privileges on the SQL Server databases.

6.8.4 Database maintenance: Managing saved scan results

Use the **Saved Scan Results** tab to maintain your database backend and delete saved scan results that are no longer required. Deletion of non-required saved scan results can be achieved manually as well as automatically through scheduled database maintenance. During scheduled database maintenance, GFI LANguard automatically deletes saved scan results that are older than a specific number of days/weeks or months. You can also configure automated database maintenance to retain only a specific number of recent scan results for every scan target and scan profile.

roperties						
Change Database	Saved Sc	an Results	Scanned Computers	Advanced		
-Saved scap resi	" ults in databa	e backend				
Treat		-61-	E Data	Com		
	Fi	orile	\ Date	Lom		
📃 localhost	Hi	gh Securit	5/15/2009 10:35:42	Yes		
📃 📃 localhost	Hi	gh Securit	5/14/2009 09:49:05	Yes	=	
📃 📃 localhost	My	y Profile	5/13/2009 13:45:45	Yes	-	
📃 📃 localhost	My	y Profile	5/12/2009 13:45:41	Yes		
80.143.32.1	1/24 Fu	ıll Scan	10/30/2008 14:07:54	Yes		
80.143.32.1	1/24 Fu	ıll Scan	10/28/2008 14:07:54	Yes		
80.143.32.1	1724 Fu	ıll Scan	10/27/2008 14:07:54	Yes		
80.143.32.1	1/24 Pir	ng them All	10/26/2008 14:07:54	Yes	Ψ.	
De	elete scan(s)		Mark scan(s) as rea	d only		
Scan results rete Retain: Scans ge (© scans pe	Scan results retention policy Retain: scans generated during the last 30 days scans per scan target per profile in number of					
[10					
NOTE: Scan results marked as read only will not be removed by the database results cleanup operations.						
OK Cancel Apply						

Screenshot 69 - Database maintenance properties: Managed saved scan results tab

To manage saved scan results:

1. Click on the **Configuration** ► **Manage saved scan results...**

2. To manually delete saved scan results, select the particular result(s) and click on **Delete Scan(s)** button.

3. To let GFI LANguard manage database maintenance for you, select **Scans generated during the last** to automatically delete scan results which are older than a specific number of days/weeks or months or **Scans per scan target per profile in number of** to retain only a specific number of recent scan results.

6.8.5 Database maintenance: List of scanned computers

GFI LANguard incorporates a mechanism where a global list of scanned computers is maintained for licensing purposes. This enables GFI LANguard to enforce its licensing details, where a larger range of scanned computers than what is specified in the licensing information will not be scanned. GFI LANguard enables systems administrators to delete previously scanned computers (nodes) so that node licenses taken by computers that are no longer present on the network, or which should no longer be scanned, can be reutilized.

Properties			×
Change Database Saved Scan Results	Scanned Computers	Advanced	
Your current GFI LANguard licen: number of different target IP addr	se enables you to sca esses/computers.	n an unlimited	_
Number of different computers/IP addresse	es scanned to date:3.		
Computer	Last scanned	Scans	
ESM_DEMO (192.168.131.65)	5/5/2009	2	
RBORG (192.168.3.48)	5/5/2009	1	
VXPPRO (192.168.3.66)	5/5/2009	4	
	Delete sele	cted computer(s	;
	UK Cano	cel Ap	ply

Screenshot 70 - Database maintenance properties: Scanned Computers tab

To delete computers previously scanned:

1. Click on Configuration
Manage list of scanned computers...

2. Select the computers to delete by holding the control key and clicking on the computers.

3. Click on **Delete selected computer(s)** button to delete scanned computer data.

NOTE 1: Deleting computers from the database is a one-way operation that will also delete all computer related data from the database. **Once deleted, this data is no longer recoverable.**

NOTE 2: While this is a very efficient mechanism for freeing up licenses previously occupied by unused nodes, note that this affects the long-term security reporting capabilities of GFI LANguard Where long term security reporting must be ascertained, or in environments where security databases must be intact, it is highly advisable to not delete any data whatsoever. In such scenarios, it is advisable that more licenses are acquired to cater for network growth or expansion.

6.8.6 Database maintenance: Advanced options

To improve the performance of your Microsoft Access based database backend you must regularly repair and compact it; two functions that GFI LANguard allows you to automate.

During compaction, the database files are reorganized and records that have been marked for deletion are removed. In this way, you can regain precious storage space. During this process, GFI LANguard also repairs corrupted database backend files. Corruption may occur for various reasons. In most cases, a Microsoft Access database is corrupted when the database is unexpectedly closed before records are saved (for example, due to a power failure, hung up processes, forced reboots, etc.).

Properties			×
Change Database Saved S	Scan Results Scanner	d Computers Advanced	
Please configure the database compaction options.			
The below option is only available when using Microsoft Access as a database backend. When using SQL Server / MSDE as a database a backend you need to manually set maintenance plans according to your company policies.			
Compact Now]		
Database compact and repa	ir frequency		_
One time only			
O Every:	1	weeks 🔻	
<u>N</u> ext operation	5/12/2009 🔲 🔻	11:53:34 AM 🚔	
	ОК	Cancel Apply	

Screenshot 71 - Database Maintenance properties: Advanced tab

To compact and repair a Microsoft Access based database backend:

1. Click on Configuration Database maintenance plan...

2. To manually launch a repair and compact process on a Microsoft Access database backend, click on the **Compact Now** button.

3. To automate the repair and compact process on an Microsoft Access database backend select **One time only** to schedule a onetime Microsoft Access database repair and compact or **Every** to execute a repair and compact process on a regular schedule. Specify the date, time and frequency in days/weeks or months at which the compact and repair operations will be executed on your database backend.

6.9 Importing and Exporting Settings

GFI LANguard allows configurations, import and export, through **Import and Export Configurations...** in the **File** menu. Configurations that can be Imported/Exported include:

- Scanning Profiles
- Vulnerability Assessment
- Ports (TCP/UDP)
- Results Filtering Reports
- Auto-Remediate Settings (Auto-Uninstall and Patch settings)
- Options (Database Backend, Alerting, Schedule scan and Internal Settings)

6.9.1 Exporting Configurations

To export the configurations:

1. From the main menu, click **File ► Import and Export** Configurations...

2. Select Export the desired configuration to a file and click Next.

3. Specify the path were to save the exported configuration, and click **Next**.

4. Wait for the configuration tree to load and select the configurations to export. Click **Next** to start export.

- 5. A notify dialog will confirm that exporting is completed.
- 6. Click **OK** to finish.

6.9.2 Importing Configurations

To import saved configurations:

1. From the main menu, click on **File** ► **Import and Export** Configurations...

2. Select **Import the desired configuration from a file** and click **Next**.

3. Specify the path from where to load configuration, and click Next.

4. Wait for the configuration tree to load and select the configurations to import. Click **Next** to start import.

5. Confirm the override dialog box; by clicking, **Yes** or **No** as required.

- 6. A notify dialog will confirm that exporting is completed
- 7. Click **OK** to finish.

NOTE: To import configurations from an existing installation of GFI LANguard, select **Importing Configurations from another instance**.

6.10 Program updates

💽 GFI LANguard					
File Tools Configure Help					Discuss this version
Network Audit Dashboard Conf	figuration Utilitie	s Gene	eral		
Configurations: Scanning Profiles Scheduled Scans Computer Profiles Auto-Uninstall Validation GFI LANguard updates GFI LANguard updates				maintain outstanding	
Patch Auto-Deployment	Auto-download	Type	Last Undate Check	Last Download	Last Undate Version
Patch Auto-Download		type	Never	Last Download	20090430
Alerting Options		🇞 G	5/4/2009 5:05:44 PM	5/4/2009 5:17:13 PM	12
Database Maintenance Options Program Lindates		诃 Vu	5/4/2009 5:05:44 PM	Never	1
Togram opulates		🍓 Pa	5/4/2009 5:05:44 PM	5/4/2009 5:06:13 PM	3
		🎯 Att	5/4/2009 5:05:44 PM	Never	1
		🎯 Sc	5/4/2009 5:05:44 PM	5/4/2009 5:06:22 PM	2
۰ III ا		т 🥑	5/4/2009 5:05:44 PM	5/4/2009 5:06:24 PM	1
Common Tasks:		🥑 Ру	5/4/2009 5:05:44 PM	5/4/2009 5:06:27 PM	1
Check for updates Edit program updates options Edit proxy settings	Oreck for updates Edit program updates options Edit program updates options Edit proxy settings Wicrosoft patches and service packs Auto-download Microsoft updates in selected language packs for network-wide				de
Program updates	<< Automatically downloaded by GFI LANguard. >>				
				<u>_</u> h	eck For Updates
					.:!

Screenshot 72 – Program updates

Out of the box, GFI LANguard supports multilingual patch management for all Unicode compliant languages. Through multilingual patch management, you can download and deploy missing Microsoft product updates, discovered during a security scan, in a variety of different languages.

The security-scanning engine identifies missing Microsoft patches and service packs by referencing the 'Microsoft Software Update files'. These files contain the latest (complete) list of product updates currently provided by Microsoft and are available in all languages supported by Microsoft products.

Use the GFI LANguard **Program Update** tool (in the Configuration tab), to download the latest Microsoft Software Update files in all languages currently in use on your network. This would allow the security-scanning engine to discover and report both English as well as non-English missing patches and service packs. Based on this information, you can then use the patch deployment engine to download and install the missing update files in their respective languages network wide.

The Automatically download the required Microsoft Language packs option enables you to automatically download language packs for a wide range of languages which includes (but is not limited to) English, German, French, Italian, Spanish, Arabic, Danish, Czech, Finnish, Hebrew, Hungarian, Japanese, Korean, Dutch, Norwegian, Polish, Portuguese, Portuguese/Brazilian, Russian, Swedish, Chinese, Chinese (Taiwan), Greek, and Turkish.

Information on how to manually download and deploy multilingual 'Microsoft Update Files' is provided further on in this chapter.

NOTE: Manual updates are required only if GFI LANguard is not configured to automatically download the required Microsoft Language packs.

6.10.1 GFI LANguard updates

The program updates tool, will allow the user to download and customize the GFI LANguard updates. The user can configure GFI LANguard, to auto download updates released by GFI to improve functionalities in GFI LANguard. These updates include also checking GFI web site for a newer build. Updates can be disabled by removing the mark from the checkbox in the **Auto-download** column.

6.10.2 Configure GFI LANguard Proxy settings

To manually configure proxy server settings for internet updates:

1. Click on Edit proxy settings... under common tasks

LANguard 9.0 Proxy Settings				
General				
Use this option to manually provide your proxy server settings.				
✓ Override automatic proxy detection				
C Connect directly to the Internet				
© Connect via a proxy server				
Server: <pre><server>:<port></port></server></pre>				
Proxy server requires <u>a</u> uthentication:				
User name:				
Password:				
Note: Patch file download, scheduled updates and some operations performed during the scanning process need to open Internet connections.				
OK Cancel Apply				

Screenshot 73 - Configuring proxy server settings

3. Select **Override automatic proxy detection**, and, chose one of the following options:

• **Connect directly to the Internet** – Select this option when a direct internet connection is available.

- **Connect via a proxy server** Select this option when internet access is through a proxy server.
 - Update the Server name and port number using this format <server>:<port>
 - If applicable, select **Proxy server requires authentication** and update the **User name** and **Password** respectively.

6.10.3 Enable/Disable GFI LANguard auto updates on startup

GFI LANguard can check for the availability of software updates at every program startup. To disable/enable this feature

1. Click on the Edit program updates options...

2. In the builds updates section, select/unselect the **Check for updates at application startup** option accordingly.

3. Click **OK** to finalize your configuration.

6.10.4 Enable GFI scheduled updates

GFI LANguard scheduled updates are enabled by default. To disable/enable this feature

1. Click on the Edit program updates options...

2. Optionally: In the builds updates section, unselect the **Check for updates at application startup** option.

3. Click Enable scheduled updates.

4. Specify auto-updates frequency

6.10.5 Starting program updates manually

To manually start GFI LANguard program updates:

1. Click on **Check for Updates...**

🥃 Update LANguard 9.0	23
Choose which action to do in the next step You can choose to update the application files or to download all the update files to a specific path used further as an alternative update location.	4
 Update application files from the following location Location GFI web site Alternative location: 	
Download all update files from GFI web site to this path: Browse]
< Badk Next >	ancel

Screenshot 74 - The Check for Updates wizard: Stage 1

2. Specify the location from where the required update files will be downloaded.

3. Optionally: Change the default download path, select **Download all update files... to this path** option will allow the user to provide an alternate download path to store all GFI LANguard updates.

4. Click Next to proceed with the update.

🔄 Update LANguard 9.0	—
Choose which packages to update Disabled items represents packages already updated that you can also update by checking "Update ALL files" or packages without update.	Q
Packages:	
 Microsoft Software Updates - English Version Microsoft Software Updates - German Version Microsoft Software Updates - French Version Microsoft Software Updates - Italian Version Microsoft Software Updates - Spanish Version Microsoft Software Updates - Arabic Version Microsoft Software Updates - Arabic Version Microsoft Software Updates - Czech Version Microsoft Software Updates - Czech Version 	11 ×
Microsoft Software Updates - Finnish Version Microsoft Software Updates - Hebrew Version Microsoft Software Updates - Hungarian Version	
Checked packages details:	
Size: 23139134 bytes lanss_9_patchmngmt_de.cab - Version 16 - Tuesday, June 09th, 2009 Added New Patches lanss_9_patchmngmt_fr.cab - Version 16 - Tuesday, June 09th, 2009 Added New Patches	4 III +
Update ALL files (including the ones already updated)	
< Back Next >	Cancel

Screenshot 75 - The Check for updates Wizard: Stage 2

- 5. Select the updates to be downloaded and click Next.
- 6. Click Start to initiate the update process.

6.10.6 Product Updates Activity

GFI LANguard 9.0 maintains a comprehensive log of all updates activity. This information can be reviewed by open **Dashboard** tab ► **Scheduled Operations** ► **Product Updates Activity** node. This enables you to keep track of which updates were completed successfully or not.

7. Scanning Profiles

7.1 Introduction

GFI LANguard enables you to scan your IT infrastructure for particular vulnerabilities using pre-configured sets of checks known as 'scanning profiles'. Scanning profiles enable you to scan your network targets and enumerate only specific information. For example, you may want to use a scanning profile that is set to be used when scanning the computers in your DMZ as opposed to your internal network.

In practice, scanning profiles allow you to focus your vulnerability scanning efforts on to a specific area of your IT infrastructure such as identifying only missing security updates. The benefit is that this way you have less scan results data to analyze; tightening up the scope of your investigation and quickly locate the information that you require more easily.

With multiple scanning profiles, you can perform various network security audits without having to go through a reconfiguration process for every type of security scan required.

7.2 Scanning profile description

Out of the box, GFI LANguard includes an extensive list of scanning profiles as described below.

7.2.1 Complete/Combination scans

Complete/Combination scanning profiles

Full	Use this scanning profile to enumerate particular network		
Vulnerability	vulnerabilities such as open TCP/UDP ports commonly		
Assessment	exploited by Trojans as well as missing patches and		
	service packs. The list of vulnerabilities enumerated by		
	this profile can be customized through the Vulnerabilities		
	tab. Installed USB devices and applications are not		
	enumerated by this profile. This profile will scan for all		
	vulnerabilities. This includes vulnerabilities which have an		
	associated Microsoft patch to them and which are		
	considered missing patches.		
Full Scan	considered missing patches. Use this scanning profile to retrieve system information		
Full Scan (Active)	considered missing patches. Use this scanning profile to retrieve system information as well as scan your network for all supported		
Full Scan (Active)	considered missing patches. Use this scanning profile to retrieve system information as well as scan your network for all supported vulnerabilities including open TCP/UDP ports, missing		
Full Scan (Active)	considered missing patches. Use this scanning profile to retrieve system information as well as scan your network for all supported vulnerabilities including open TCP/UDP ports, missing patches and service packs, USB devices connected and		
Full Scan (Active)	considered missing patches. Use this scanning profile to retrieve system information as well as scan your network for all supported vulnerabilities including open TCP/UDP ports, missing patches and service packs, USB devices connected and more. The vulnerability check timeouts in this profile are		
Full Scan (Active)	considered missing patches. Use this scanning profile to retrieve system information as well as scan your network for all supported vulnerabilities including open TCP/UDP ports, missing patches and service packs, USB devices connected and more. The vulnerability check timeouts in this profile are specifically preconfigured to suite the network traffic and		
Full Scan (Active)	considered missing patches. Use this scanning profile to retrieve system information as well as scan your network for all supported vulnerabilities including open TCP/UDP ports, missing patches and service packs, USB devices connected and more. The vulnerability check timeouts in this profile are specifically preconfigured to suite the network traffic and transmission delays usually associated with LAN		

Full Scan	Use this scanning profile to retrieve system information
(Slow	as well as scan your network for all supported
Networks)	vulnerabilities including open TCP/UDP ports, missing
	patches and service packs, USB devices connected and
	more The vulnerability check timeouts in this profile are
	specifically preconfigured to suite the network traffic and
	transmission delays usually associated with WAN
	environments.

7.2.2 Vulnerability Assessment

Vulnerability asso	essment scanning profiles
Top SANS 20	Use this scanning profile to enumerate all
Vulnerabilities	vulnerabilities reported in the SANS top 20 list.
High Security	Use this scanning profile to enumerate open
Vulnerabilities	TCP/UDP ports and high security vulnerabilities. The
	list of TCP/UDP ports and high security vulnerabilities
	that will be enumerated by this profile can be
	customized through the TCP/UDP Ports tabs and the
	Vulnerabilities tab respectively.
Last Year's	Use this scanning profile to enumerate network
Vulnerabilities	vulnerabilities that emerged during the last 12
	months.
Only Web	Use this scanning profile to identify web-server
	specific vulnerabilities. This includes scanning and
	enumerating open TCP ports that are most
	commonly used by web-servers such as port 80.
	Only TCP ports commonly used by web-servers are
	scanned by this profile. Network auditing operations
	as well as enumeration of vulnerabilities and missing
	patches are not performed using this profile.
Missing Patches	Use this scanning profile to enumerate missing
	Microsoft patches. The list of missing patches that
	will be enumerated by this profile can be customized
	through the Patches tab.
Critical Patches	Use this scanning profile to enumerate only missing
	Microsoft patches that are tagged as critical. The list
	of critical patches that will be enumerated by this
	profile can be customized through the Patches tab.
Last Month's	Use this scanning profile to enumerate only missing
Patches	Microsoft patches that were released last month. The
	list of missing patches that will be enumerated by this
Only Convice	Les this scenning profile to contracts missing
Only Service	Use this scanning profile to enumerate missing
Facks	will be onumerated by this profile can be sustarized
	will be enumerated by this profile can be customized
	through the Patches tab.

Protection from	Use this scanning profile to check if GFI	
Portable Storage	EndPointSecurity is installed or if GFI	
	EndPointSecurity's security agent is deployed on	
	scan targets.	
	You can customize this profile to enumerate only	
	unauthorized/blacklisted software or vice-versa. For	
	more information on GFI EndPointSecurity refer to	
	the user manual available at:	
	http://www.gfi.com/endpointsecurity/esec4manual.pdf	

Network and Son	wate Audit scanning promes
Trojan Ports	Use this scanning profile to enumerate open TCP/UDP ports that are commonly exploited by known Trojans. The list of TCP/UDP ports to be scanned can be customized through the TCP Ports and UDP Ports tabs respectively. Only the TCP/UDP ports commonly exploited by known Trojans are scanned by this profile. Network auditing operations as well as enumeration of other open TCP/UDP ports and missing patches are not performed by this profile.
Port Scanner	Use this scanning profile to enumerate open TCP/UDP ports including those most commonly exploited by Trojans. The list of ports that will be enumerated by this profile can be customized through the TCP/UDP ports tab.
Software Audit	Use this scanning profile to enumerate all software applications installed on scan targets. This includes security software such as anti-virus and anti- spyware.
Full TCP & UDP	Use this scanning profile to audit your network and
Scan Only SNMP	Use this scanning profile to perform network discovery and retrieve information regarding hardware devices (routers, switches, printers, etc.) that have SNMP enabled. This enables you to monitor network-attached devices for conditions that require administrative attention.
Ping Them All	Use this scanning profile to audit your network and enumerate all computers that are currently connected and running.
Share Finder	Use this scanning profile to audit your network and enumerate all open shares either hidden or visible. No vulnerability checks are performed by this profile.
Uptimes	Use this scanning profile to audit your network and identify how long each computer has been running since the last reboot.
Disks Space Usage	Use this scanning profile to audit your network and retrieve system information on available storage space.
System Information	Use this scanning profile to retrieve system information such as operating system details, wireless/virtual/physical network devices connected, USB devices connected, installed applications and more.

7.2.3 Network & Software Audit

Hardware Audit	Use this scanning profile to audit your network and
	enumerate all hardware devices currently connected
	to your network computers.

7.2.4 Which scanning profile shall I use?

Select the scanning profile based on the:

1. The scope of your vulnerability analysis i.e. what you want to achieve out of your vulnerability scan. Based on these factors, you can determine the type of vulnerability checks to be performed and the information that you want to retrieve from your scan targets.

2. Time you have at your disposal for target vulnerability scanning. The more vulnerability checks you run the longer it will take the scan process to complete.

7.3 Creating a new scanning profile

To create a new scanning profile:

1. Click **Configuration** tab ► **Scanning Profiles** and go to **Scanning profiles management.**

8 GFI LANguard Scanning Profiles Editor		_ 0 🔀
File		
Scanning Profiles		
Profile categories: Complete/Combination Scans Vulnerability Assessment Network & Software Audit	Vulnerability Assessment (Vulnerabilities Ratches Choose scan profile conditions. Enable vulnerability scanning	Dptions Network & Softw.
Frones. Full Vulnerability Assessment Full Scan Full Scan (Slow Networks)	Group by: Type Group by: Type	Name A V (1) Abyss Web server Bufferov A V (1) AFS-Kerberos Support in Op V (1) AFS-Kerberos Support in Op V (1) Alservers: (e)shop Online- V (1) All Servers: Alstats (a1dis; V (1) All Servers: Adorder - build. V (1) All Servers: Addimose
Common Tasks: <u>New scanning profile</u> <u>Set Active</u> <u>Rename</u> <u>Delete</u> W Help:		 All Servers: AHG's 'search.c All Servers: AHG's 'search.c All Servers: Alex Heiphetz C All Servers: Alex Heiphetz C All Servers: Auktion.cgi All Servers: Brian Stanback All Servers: Brian Stanback All Servers: Commerce.cgi All Servers: COWS CGI Onli
Scanning Profiles LANguard Scripting	۲ اس کې د او	Image: Construction of the second
	Find vulnerability: by Name	• erabilities from the above list applies the o
		.:

Screenshot 76 - The Scanning Profile Editor

2. In the Scanning Profiles Editor click New scanning profile...

3. Specify the name of the new profile and select **Copy all settings from an existing profile** to clone settings from an existing profile.

4. Click **OK** to save settings. The new scanning profile is added under **Profiles** in the left pane.

7.4 Configuring vulnerabilities



Screenshot 77 - Scanning Profiles properties: Vulnerabilities tab options

The scanning profiles that ship with GFI LANguard 9 are already preconfigured to run a number of vulnerability checks on selected target. You can however disable vulnerability scanning as well as customize the list of vulnerability checks executed during a scan.

7.4.1 Enabling/disabling vulnerability scanning

To enable vulnerability scanning:

1. From the **Vulnerability Assessment Options** tab, click **Vulnerabilities** sub-tab.

2. Select the scanning profile to customize from the left pane under **Profiles**.

3. In the right pane, select **Enable Vulnerability Scanning** option.

NOTE: Vulnerability scanning is configurable on a scan profile by scan profile basis. If in a particular profile this option is not selected, no vulnerability tests will be performed in the security audits carried out by this scanning profile.

7.4.2 Customizing the list of vulnerabilities to be scanned

To specify which vulnerabilities will be enumerated and processed by a scanning profile during a security audit: 1. From the **Vulnerability Assessment Options** tab, select the scanning profile to customize from the left pane under **Profiles**.

Vulnerability Assessment (Options Retwork & Software Audit Options	💐 Scanner O, 🛄
Choose scan profile conditions.		
Enable vulnerability scanning		
Group by: Type 🔻	Name 🔺 0	OVAL ID CVE
🖃 🔽 🦰 Vulnerabilities	Abyss Web server Bufferoverflow	*
📝 🎴 DNS	AFS-Kerberos Support in OpenSSH Pos	
📝 🎴 FTP	Alerter service enabled	
🔽 🙀 Mail	📝 🕕 All Servers: (e)shop Online-Shop System	
🔽 🙀 Miscellaneous	📝 🕕 All Servers: A 1Stats (a 1disp)	
🔽 🍓 Registry	📝 🕕 All Servers: Abe Timmerman zml.cgi File	
🗹 闷 Rootkit	📝 🕕 All Servers: Adcycle - build.cgi	
🗹 🍓 RPC	🔽 🚺 All Servers: Aglimpse	
🗹 🍖 Services	🔽 🗓 All Servers: AHG's 'search.cgi' Search E	
🗹 🍖 Software	📝 🗓 All Servers: Alex Heiphetz Group EZSho	
🗹 🍖 Web	🔽 🚺 All Servers: Arts Store.cgi	
🗄 🗹 闷 Potential Vulnerabilities	🔽 🚺 All Servers: Auktion.cgi	
	🔽 則 All Servers: Brian Stanback bsguest.cgi	
	🔽 則 All Servers: Brian Stanback bslist.cgi	
	All Servers: Commerce.cgi	
	🔽 🚺 All Servers: COWS CGI Online Worldwe	
	All Servers: DCShon vulnerability	· ·
		,
	2557 vulnerabilities	
Advanced	Add Edit	Remove
Find vulnerability: by Name	Find	Find next
Adding, editing or removing vulnedited vulnerabilities are selected	erabilities from the above list applies the changes to all d.	the profiles where the

Screenshot 78 - Select the vulnerability checks to be run by this scanning profile

2. In the right pane, select the vulnerability checks that you wish to execute through this scanning profile.

7.4.3 Customizing the properties of vulnerability checks

All the checks listed in the **Vulnerabilities** tab have specific properties that determine when the check is triggered and what details will be enumerated during a scan.

E	dit vulnerability		×
	General Conditions	Description References	
	<u>N</u> ame:	All Servers: (e)shop Online-Shop System]
	<u>Т</u> уре:	Miscellaneous 🔻)
	OS <u>F</u> amily:	windows 🗸]
	OS Version:		
	Product:]
	Timestamp:	9/15/2001]
	S <u>e</u> verity:	🚺 High 🗸	
l			
		OK Cancel Apply	

Screenshot 79 - Vulnerability properties dialog: General tab

To change the properties of a vulnerability check:

1. Right click on the vulnerability to customize and select Properties.

2. Customize the selected vulnerability check through the following tabs:

• **General** - Use this tab to customize the general details of a vulnerability check including vulnerability check name, vulnerability type, OS family, OS version, Product, Timestamp and Severity.

• **Conditions**: Use this tab to configure the operational parameters of this vulnerability check. These parameters will define whether a vulnerability check is successful or not. For information on how to configure vulnerability, check conditions refer to the <u>Vulnerability</u> check conditions setup section in this manual.

• **Description:** Use this tab to customize the vulnerability check description.

• **References:** Use this tab to customize references and links that lead to relevant information in the OVAL, CVE, MS Security, Security Focus and SANS TOP 20 reports.

3. Click on **OK** to save your settings.

7.4.4 Vulnerability check conditions setup

The **Conditions** tab enables you to add or customize conditions, which define whether the computer or network being scanned is vulnerable, or not. It is therefore of paramount importance that any custom checks defined in this section are set-up by qualified personnel that are aware of the ramifications of their actions.

Edit vulnerability
General Conditions Description References
This vulnerability will be triggered when the below conditions are met.
AND V Not +()+ -()-
 Independent CGI Abuse Test AND Windows Group Test
Description:
Enables different users belonging to specific groups to be tested.
Add Edit Delete Clear 🔶
OK Cancel Apply

Screenshot 80 - Vulnerability conditions setup tab

To add a vulnerability check condition:

1. Click Add.

Check properties	×
Step 1 of 3: Select the type of check Specify what do you want to check from the list below	\checkmark
Check type:	
Independent Family Test Independent FTP Banner Test Independent HTTP Banner Test Independent POP3 Banner Test Independent Port Open Test Independent SMTP Banner Test Independent SMTP Banner Test Independent SMTP Banner Test Independent SMTP Banner Test Independent TCP Banner Test Independent TELNET Banner Test Independent TELNET Banner Test Independent TELNET Banner Test Independent TELNET Banner Test Independent Text File Content Test Independent Text File Content Test Independent VB Script Test	E
Check description:	
Executes a VB script and returns a boolean value.	*
< Back Next >	Cancel

Screenshot 81 - Check properties wizard

2. Select the type of check to be configured and click **Next**.

3. Define the object to examine and click Next.

4. Set attributes/desired parameters and click $\ensuremath{\textit{Finish}}$ to finalize your settings.

Edit vulnerability
General Conditions Description References
This vulnerability will be triggered when the below conditions are met.
AND V Not +()+ -()-
Independent CGI Abuse Test AND Windows Group Test AND
Independent VB Script Test Independent VB Script
Description:
Executes a VB script and returns a boolean value.
Add Edit Delete Clear 🛧 🕈
OK Cancel Apply

Screenshot 82 - Edit vulnerability

5. If more than one condition is set up, define conditional operators and click ${\bf OK}$ to finalize your configuration settings.

Vulnerability checks - advanced options

Use the **Advanced...** included in the **Vulnerabilities** tab to bring up the advanced vulnerabilities scanning options.

ŀ	٩dva	ance	d Vulnerabilities Properties		X
	Ge	eneral	7		
			Specify advanced vulnerabilities options.		
		- v	ulnerability Scan Options		
		-	Internal checks		
			Weak passwords		
			FTP anonymous access allowed	\checkmark	
			Administrator account exists	\checkmark	
			Users that never logged on		
			New vulnerabilities are enabled by default	Yes	
			Show vulnerabilities with errors during evaluatio	No	
		- 0	GI Probing Settings		
		=	Send CGI request through proxy	No	
			Proxy IP address		
			Proxy port		
	L				
			ОК	Cancel Apply	

Screenshot 83 - Advanced vulnerability scanning dialogs

Use these options to:

- Configure extended vulnerability scanning features that check your target computers for weak passwords, anonymous FTP access, and unused user accounts.
- Configure how GFI LANguard will handle newly created vulnerability checks.
- Configure GFI LANguard to send CGI requests through a specific proxy server. This is mandatory when CGI requests will be sent from a computer that is behind a firewall to a target web server that is 'outside' the firewall (for example, Web servers that are on a DMZ). The firewall will generally block all the CGI requests that are directly sent by GFI LANguard to a target computer that is in front of the firewall. To avoid this, set the Send CGI requests through proxy option to 'Yes' and specify the name/IP address of your proxy server and the communication port which will be used to convey the CGI request to the target.

7.5 Configuring patches

🔋 GFI LANguard Scanning Profiles Edit	tor				- • 💌
File					
Scanning Profiles	3				
Profile categories:	🍋 Vulnerability Assessment (Options 🍓 Network 8	k Software Audit Op	otions 🛛 💐 S	canner O,
Complete/Combination Scans Vulnerability Assessment Network & Software Audit Profiles:	Vulnerabilities Ratches Choose scan profile conditions. Returns Detect installed and missing serviv	e packs / patches			
Numerability Assessment	Patch language filter: English	•			
Sull Scan	NOTE: Configure supported language	es in LANguard -> Configura	tion -> Program Up	dates.	
Hull Scan (Slow Networks)	Bulletins to be checked for:				
To my scanning prome	Group by: Severity 🔻	Bulletin names	Severity	QNumber	Date poster
	🖃 📝 👩 All Patches	👿 🥹 MS09-009	Important	959988	2009-04 🔺
	🔤 📝 🧓 Critical	👿 🥸 MS09-009	Important	959993	2009-04
	- 🗹 🔯 Important	📝 🔯 MS09-009	Important	959995	2009-04
	🗹 둱 Moderate	👿 🔯 MS09-009	Important	959997	2009-04
	🔽 🕞 Low	👿 🔯 MS09-009	Important	960000	2009-04
Common Taska		👿 🔯 MS09-009	Important	960003	2009-04
Common Tasks.		👿 😻 MS09-010	Important	923561	2009-04
New scanning profile		🛛 🤯 MS09-010	Important	923561	2009-04
Set Active		🛛 🔯 MS09-010	Important	923561	2009-04
Rename		MS09-010	Important	923561	2009-04
Delete		MS09-010	Important	923561	2009-04
		MS09-010	Important	923561	2009-04
🕑 Help:		W 8 MS09-010	Important	933399	2009-04
Scanning Profiles		W V MS09-010	Important	960476	2009-04
LANguard Scripting	۰ III ا	MS09-011	Critical	961373	2009-02
	File: lans Find bulletin: Search by bulletin name (e.g. MS02-0	017) or QNumber (e.g. Q311	/ersion: 10; Last up I Find n 967).	dated on: 5/4/2 ext	009 5:12:00 PM 2161 patches
					.::

Screenshot 84 - Scanning Profiles properties: Patches tab options

Use the **Patches** tab to specify which security updates are checked during vulnerability scanning. The patches to be checked are selected from the complete list of supported software updates that is included by default in this tab. This list is automatically updated whenever GFI releases a new GFI LANguard missing patch definition file.

7.5.1 Enabling/disabling missing patch detection checks

To enable missing patch detection checks in a particular scanning profile,

1. From the **Vulnerability Assessment Options** tab, click **Patches** sub-tab.

2. Select the scanning profile that you wish to customize from the left pane under **Profiles**.

3. In the right pane, select **Detect installed and missing service** packs/patches option.

NOTE: Missing patch scanning parameters are configurable on a scan profile by scan profile basis. Make sure to enable missing patch scanning in all profiles where missing patch scanning is required.

7.5.2 Customizing the list of software patches to be scanned

To specify which missing security updates will be enumerated and processed by a scanning profile:

1. From the Vulnerability Assessment Options tab, click Patches sub-tab

Bulletin names	Severity	QNumber	Date posted 💌	Title
📝 🔯 MS09-009	Important	959988	2009-04-14	Security Update for Microsoft Excel 2002 (KB
📝 🔯 MS09-009	Important	959993	2009-04-14	Security Update for Microsoft Office Excel Vie
📝 🔯 MS09-009	Important	959995	2009-04-14	Security Update for Microsoft Office Excel 20
📝 🔯 MS09-009	Important	959997	2009-04-14	Security Update for Microsoft Office Excel 20
📝 🔯 MS09-009	Important	960000	2009-04-14	Security Update for Microsoft Office Excel Vie
📝 🔯 MS09-009	Important	960003	2009-04-14	Security Update for 2007 Microsoft Office Sy:
📝 🔯 MS09-010	Important	923561	2009-04-14	Security Update for Windows 2000 (KB92356
📝 🔯 MS09-010	Important	923561	2009-04-14	Security Update for Windows Server 2003 (Ki
📝 🔯 MS09-010	Important	923561	2009-04-14	Security Update for Windows Server 2003 for
📝 🔯 MS09-010	Important	923561	2009-04-14	Security Update for Windows Server 2003 x6
📝 🔯 MS09-010	Important	923561	2009-04-14	Security Update for Windows XP (KB923561)
📝 🔯 MS09-010	Important	923561	2009-04-14	Security Update for Windows XP x64 Edition (
📝 🔯 MS09-010	Important	933399	2009-04-14	Security Update for Office XP (KB933399)
🔽 🔯 MS09-010	Important	960476	2009-04-14	Security Update for Microsoft Office File Conv
🔽 😰 MS09-011	Critical	961373	2009-04-14	Security Update for DirectX 8 for Windows 20
•				+

2. Select the scanning profile to customize from the left pane under **Profiles**.

Screenshot 85 - Selecting the missing patches to be enumerated

3. In the right pane, select/unselect which missing patches are enumerated by this scanning profile.

7.5.3 Searching for bulletin information

Find <u>b</u> ulletin:		Find	Find next
Search by bulletin nam	ne (e.g. MS02-017) or QNumber	(e.g. Q311967).	

Screenshot 86 - Searching for bulletin information

To search for a particular bulletin:

1. Specify the bulletin name (for example, MS02-017) or QNumber (for example, Q311987) in the search tool entry box included at the bottom of the right pane.

2. Click Find to start searching for your entry.

Bulletin Info								×
Bulletin								
Bulletin ID:	MS09-009	QNumber:	959995	Date:	2009-04-14	Severity:	Important	
Title:	Security Update for	r Microsoft Of	ffice Excel 2003 (I	KB959995)				
Description:	A security vulnera when a maliciously	bility exists ir / modified file	n Microsoft Office is opened. This u	Excel 2003 Ipdate reso	3 that could al olves that vuln	low arbitrary coo erability.	de to run	
Applies To:	Office 2003							
URL:	http://www.micros	oft.com/dowr	nloads/details.asp	x?FamilyIc	I=D9DBFA63-	COCB-4C84-9B8	A-6E52568045	<u>B08</u>
File								
File Name:	EXCEL.CAB							
File Size:	4,984 KB							
File URL:	http://download.wi	indowsupdate	e.com/msdownloa	d/update/s	software/secu	/2009/03/excel	be1ae3c1c6fe	<u>:714</u>
							Close	

Screenshot 87 - Extended bulletin information

7.6 Configuring TCP port scanning options

Scanning Profiles	
Profile categories:	Vulnerability Assessment Options 🏹 Network & Softwar
Complete/Combination Scans Vulnerability Assessment	TCP Ports UDP Ports System Information Devices Application
🔉 Network & Software Audit	Choose scan profile conditions.
Profiles:	Enable TCP Port Scanning
No. Full Vulnerability Assessment	Ports 🔺 Description
🍇 Full Scan	TCP Port Service Multiplexer
Networks) 😽 😽	🛛 💮 2 Compressnet Management Utility, If this service is n
🍇 My Scanning profile	Compressnet Compression Process
	🛛 😑 5 Remote Job Entry, If this service is not installed bew
	🛛 💽 7 Echo
	🛛 📀 11 Active Users, If this service is not installed beware o
	🛛 💭 😑 13 DAYTIME - (RFC 867)
	🛛 💽 😑 17 Quote of the Day
	🛛 🕙 🔵 18 Message Send Protocol, If this service is not installed
Common Tasks:	🛛 💽 😑 19 Character Generator
New scapping profile	20 FTP - data, If this service is not installed beware cou
Set Active	🛛 💽 21 FTP - control (command)
Rename	📝 🔵 22 Secure Shell (SSH)
Delete	23 Telnet protocol - unencrypted text communications
	🖉 🔵 25 Simple Mail Transfer Protocol (SMTP)
(i) Help:	🛛 💽 35 Any private printer server protocol
	TIME protocol, If this service is not installed beware
Scanning Profiles	9 Resource Location Protocol (RLP), If this service is n
Eninguard Scripting	Graphics, If this service is not installed beware could
	42 nameserver, ARPA Host Name Server Protocol
	• III •
	Advanced Add Edit Remove
	If you add, edit or remove a port, the changes will be applied to all the

Screenshot 88 - Scanning Profiles properties: TCP Ports tab options

7.6.1 Enabling/disabling TCP Port scanning

To enable TCP Port Scanning in a particular scanning profile,

1. From the **Network & Security Audit Options** tab, click **TCP Ports** sub-tab.

2. Select the scanning profile that you wish to customize from the left pane under **Profiles**.

3. Select Enable TCP Port Scanning option.

7.6.2 Configuring the list of TCP ports to be scanned

To configure which TCP ports will be processed by a scanning profile during vulnerability scanning select the required ports:

1. From **Network & Security Audit Options** tab, click **TCP Ports** sub-tab.

2. Select scanning profile to customize from the left pane under **Profiles**.

3. Select TCP ports analyze with this scanning profile.
7.6.3 Customizing the list TCP ports

1. From the **Network & Security Audit Options** tab, click **TCP Ports** sub-tab.

2. Select the scanning profile that you wish to customize from the left pane under **Profiles**.

3. Customize the list of TCP Ports through **Add**, **Edit** or **Remove**. **NOTE:** The list of supported TCP/UDP Ports is common for all profiles. Deleting a port from the list will make it unavailable for all scanning profiles.

7.7 Configuring UDP port scanning options

🙎 GFI LANguard Scanning Profiles Editor		
File		
Scanning Profiles		
Profile categories:	Vulnerability Assessment Options 🍡 Network & Software Audit Options	ptions 🄍 斗 .
Vulnerability Assessment	TCP Ports UDP Ports System Information Devices Applications	
🚺 Network & Software Audit	Choose scan profile conditions.	
	Fnable LIDP Port Scanning	
Profiles:		
Full Vulnerability Assessment	Ports Description	Notes
Full Scan Full Scan Full Scan	2 Compressnet Management Utility	<u>^</u>
My Scanning profile	Compression Process	
a hij oodining plano	M 5 Remote Job Entry	
	Active Users Active Users	
	IS DATINE - (KFC 807)	
	V V Qubite of the Day	
	Character Generator	
Common Tasks:		
	Any private printer server protocol	
New scanning profile	37 TIME protocol	
Set Active	Resource Location Protocol (RLP)	
Rename	Graphics	
Delete	42 nameserver, ARPA Host Name Server Protocol	
	V 43 whois	
Инир:	TACACS Login Host protocol	
Scanning Profiles	🗑 🍝 52 XNS (Xerox Network Services) Time Protocol	
LANguard Scripting	🕼 🦳 53 Domain Name System (DNS)	
	🔽 🍧 54 XNS (Xerox Network Services) Clearinghouse	-
		•
	Advanced Add Edit	Remove
	() If you add, edit or remove a port, the changes will be applied to all the profile	es.

Screenshot 89 - Scanning Profiles properties: UDP Ports tab options

7.7.1 Enabling/disabling UDP Port scanning

To enable UDP Port Scanning in a particular scanning profile,

1. From the **Network & Security Audit Options** tab, click **UDP Ports** sub-tab.

2. Select scanning profile to customize from the left pane under **Profiles**.

3. Select Enable UDP Port Scanning option.

7.7.2 Configuring the list of UDP ports to be scanned

To configure which UDP ports will be processed by a scanning profile during vulnerability scanning select the required ports:

1. From the **Network & Security Audit Options** tab, click **UDP Ports** sub-tab.

2. Select the scanning profile to customize from the left pane under **Profiles**.

3. Select the UDP ports that will be analyzed by this scanning profile.

7.7.3 Customizing the list UDP ports

1. From the **Network & Security Audit Options** tab, click **UDP Ports** sub-tab.

2. Select the scanning profile to customize from the left pane under **Profiles**.

3. Customize the list of UDP Ports through **Add**, **Edit** or **Remove**. **NOTE:** The list of supported UDP Ports is common for all profiles. Deleting a port from the list will make it unavailable for all scanning profiles.

7.8 Configuring system information retrieval options

Scanning Profiles		
Profile categories:	Vulnerability Assessment Options 💦 Network & Software Audit Options	
 Complete/Combination Scans Vulnerability Assessment Network & Software Audit 	TCP Ports UDP Ports System Information Devices Applications Choose scan profile conditions.	
Profiles:		
Full Vulnerability Assessment	Windows System Information	
Full Scan	Retrieve basic OS information by SMB Yes	
😽 Full Scan (Slow Networks)	Request server information Yes	
😽 My Scanning profile	Identify PDC (Primary Domain Controller) No	
	Identify BDC (Backup Domain Controller) No	
	Enumerate trusted domains No	
	Enumerate shares No	
	Display admin shares Yes	
	Display hidden shares Yes	
	Enumerate local users No	
Common Tasks:	Enumerate local groups No	
	Enumerate logged on users No	
New scanning profile	Enumerate users logged on locally Yes	
Set Active	Enumerate users logged on remotely Yes	
Rename	Enumerate disk drives No	
Delete	Request remote time of day No	
	Request information from remote registry Yes	
9 Help:	Enumerate services No	
Scanning Profiles	Enumerate sessions No	
LANguard Scripting	Read password policies No	
	Enumerate remote processes No	
	Security audit policy No	
	Identify virtualization technology No	
	- Linux System Information	
	List all user groups present on the target machine.	

Screenshot 90 - Scanning Profiles properties: System Information tab options

To specify what System Information is enumerated by a particular scanning profile during vulnerability scanning:

1. From the **Network & Security Audit Options** tab, click **System Information** sub-tab.

2. Select the scanning profile that you wish to customize from the left pane under **Profiles**.

3. From the right pane, expand the **Windows System Information** group or **Linux System Information** group accordingly.

4. Select which Windows/Linux OS information will be retrieved by the security scanner from scanned targets.

For example, to enumerate administrative shares in scan results, expand the **Enumerate shares** option and set the **Display admin shares** option to 'Yes'.

7.9 Configuring the attached devices scanning options

Use the **Devices** tab to enumerate network devices.

8 GFI LANguard Scanning Profiles Editor	- 8	×
File		
Scanning Profiles		
Profile categories:	🍋 Vulnerability Assessment Options 🛛 💫 Network & Software Audit Options	4 <u>+</u>
Complete/Combination Scans Vulnerability Assessment Network & Software Audit	TCP Ports UDP Ports System Information Devices Applications Choose scan profile conditions. Image: Condition of the product of the produ	_
 Full Vulnerability Assessment Full Scan Full Scan (Slow Networks) My Scanning profile 	Network Devices USB Devices Configure which Network devices you want to mark as dangerous and which you want to have ignored in your scan results. Devices which will be marked as dangerous will have a high security vulnerability notification in the scan results. Devices which are on the ignore list will not be listed or saved to the database. Create a high security vulnerability for network devices which name contains:	
Common Tasks: New scanning profile Set Active		*
Rename Delete	Ignore (Do not list/save to db) devices which name contains:	
Belp: Scarning Profiles LANguard Scripting		*
	Advanced	4
	12	

Screenshot 91 - The network devices configuration page

Together with device enumeration, you can further configure GFI LANguard to generate high security vulnerability alerts whenever particular USB and network hardware is detected. This is achieved by compiling a list of unauthorized/blacklisted network and USB devices that you want to be alerted.

You can also configure GFI LANguard to exclude from the scanning process particular USB devices that you consider as 'safe' such as USB keyboards. This is achieved by compiling a safe/whitelist of USB devices to be ignored during scanning.

Similarly you can create a separate scanning profile that enumerates only Bluetooth dongles and wireless NIC cards connected to your target computers In this case however, you must specify 'Bluetooth' and 'Wireless' or 'WiFi' in the unauthorized network and USB lists of your scanning profile.

All the device scanning configuration options are accessible through the two sub-tabs contained in the devices configuration page. These are the **Network Devices** tab and the **USB Devices** tab.

• Use the **Network Devices** sub-tab to configure the attached network devices scanning options and blacklisted (unauthorized)/whitelisted (safe) devices lists.

• Use the **USB Devices** sub-tab to configure the attached USB devices scanning options and unauthorized/safe devices lists.

7.9.1 Enabling/disabling checks for all installed network devices

To enable network device (including USB device) scanning in a particular scanning profile:

1. From the **Network & Security Audit Options** tab, click **Devices** sub-tab

2. Click **Network Devices** tab

3. Select the scanning profile to customize from the left pane under **Profiles**.

4. From the right pane, select **Enable scanning for hardware devices on target computer(s)**.

NOTE: Network device scanning is configurable on a scan profile by scan profile basis. Make sure to enable network device scanning in all profiles where this is required.

7.9.2 Scanning for network devices

Compiling a network device blacklist/whitelist

To compile a network device blacklist/whitelist for a scanning profile:

1. From the **Network & Security Audit Options** tab, click **Devices** sub-tab.

2. Click Network Devices tab.

3. Select the scanning profile to customize from the left pane under **Profiles**.

4. In the right pane: to create a network device blacklist, specify which devices you want to classify as high security vulnerabilities in the space provided under **Create a high security vulnerability for network devices which name contains**.

For example, if you enter the word 'wireless' you will be notified through a high security vulnerability alert when a device whose name contains the word 'wireless' is detected. To create a network device whitelist, specify which devices you want to ignore during network vulnerability scanning in the space provided under **Ignore (Do not list/save to db) devices which name contains**.

NOTE: Only include one network device name per line.

Advanc	ed Network Devices Properties		×
Gener	al		
	Specify advanced network devices options.		
	Enumerate Network Devices		
	Enumerate wired network devices	Yes	
	Enumerate wireless network devices	Yes	
	Enumerate software enumerated network devices	Yes	
	Enumerate virtual network devices	Yes	_
	OK Canc	el Appl	у

7.9.3 Configuring advanced network device scanning options

Screenshot 92 - Advanced network devices configuration dialog

From the **Network Devices** tab, you can also specify the type of network devices checked by this scanning profile and reported in the scan results. These include 'wired network devices', 'wireless network devices', 'software enumerated network devices' and 'virtual network devices'.

To specify which network devices to enumerate in the scan results:

1. From the **Network & Security Audit Options** tab, click **Devices** sub-tab.

2. Click on the **Network Devices** tab (opens by default).

3. Select the scanning profile that you wish to customize from the left pane under **Profiles**.

4. Click **Advanced** at the bottom of the page.

5. Set the required options to **Yes** and on completion click **OK** to finalize your settings.

7.10 Scanning for USB devices



Screenshot 93 - The Devices configuration page: USB Devices tab options

7.10.1 Compiling a USB devices blacklist/whitelist

To compile a list of unauthorized/dangerous USB devices:

1. From the **Network & Security Audit Options** tab, click the **Devices** sub-tab.

2. Click **USB Devices** tab.

3. Select the scanning profile that you wish to customize from the left pane under **Profiles**.

4. In the right pane to create a USB device blacklist, specify which devices you want to classify as high security vulnerabilities in the space provided under **Create high security vulnerability for USB devices that name contains.** For example, if you enter the word 'iPod' you will be notified through a high security vulnerability alert when a USB device whose name contains the word 'iPod' is detected. To create a USB device whitelist, specify which USB devices you want to ignore during network vulnerability scanning in the space provided under **Ignore (Do not list/save to db) devices which name contains**.

NOTE: Only include only one network device name per line.

7.11 Configuring applications scanning options

Use the **Applications** tab to specify which installed applications will be investigated by a scanning profile during a target computer scan.

8 GFI LANguard Scanning Profiles Editor					
File					
Scanning Profiles					
Profile categories: Complete/Combination Scans Vulnerability Assessment Network & Software Audit Profiles:	Wilnerability Assessment Options Network & Software Audit Options Scanner Options TCP Ports UDP Ports System Information Devices Applications Choose scan profile conditions. Image: Computer (s) Image: Computer (s) Image: Computer (s)				
 Full Vulnerability Assessment Full Scan Full Scan (Slow Networks) My Scanning profile 	Installed Applications Security Applications Specify which installed applications are authorized/un-authorized and which you do not need to be notified about. NOTE: When an application is not authorized a high security vulnerability warning will be generated. Specify which applications are authorized to be installed: Only the applications in the list below Image: All applications except the ones in the list below				
Common Tasks: New scanning profile Set Active Rename Delete @ Help: Scanning Profiles	Application name Version Publisher				
LANguard Scripting	Application name Version Publisher				

Screenshot 94 - The applications configuration page

Through this tab, you can also configure GFI LANguard to detect and report unauthorized software installed on scanned targets and to generate high security vulnerability alerts whenever such software is discovered.

7.11.1 Scanning installed applications



Screenshot 95 - List of supported anti-virus and anti-spyware applications

By default, GFI LANguard also supports integration with particular security applications. These include various anti-virus and anti-spyware software. During security scanning, GFI LANguard will check if the supported virus scanner(s) or anti-spyware software is correctly configured and that the respective definition files are up to date.

Application scanning is configurable on a scan profile by scan profile basis and all the configuration options are accessible through the two sub-tabs contained in the applications configuration page. These are the **Installed Applications** sub-tab and the **Security Applications** sub-tab.

8 GFI LANguard Scanning Profiles Editor	
File	
Scanning Profiles	
Profile categories:	🍋 Vulnerability Assessment Options 🛛 🔒 Network & Software Audit Options 🔍 Scanner Options
Complete/Combination Scans Vulnerability Assessment Network & Software Audit	TCP Ports UDP Ports System Information Devices Applications Choose scan profile conditions. Image: Computer (s) Image: Computer (s) Image: Computer (s)
Null Vulnerability Assessment	Installed Applications Security Applications
 Full Scan Full Scan (Slow Networks) My Scanning profile 	Specify which installed applications are authorized/un-authorized and which you do not need to be notified about. NOTE: When an application is not authorized a high security vulnerability warning will be generated.
	Specify which applications are authorized to be installed: Only the applications in the list below All applications except the ones in the list below
	Application name A Version Publisher
Common Tasks:	i) ares
New scanning profile	👸 yahoo
Set Active	
Rename	< >
<pre>@ Help:</pre>	Add Edit Remove
Scanning Profiles	Ignore (Do not list/save to db) applications in the list below:
LANguard Scripting	Application name 🔺 Version Publisher
	< Mdd Edit Remove

Enabling/disabling checks for installed applications

Screenshot 96 - The Applications tab: Installed Applications tab options

To enable installed applications scanning in a particular scanning profile:

1. From the **Network & Security Audit Options** tab, click on the **Applications** sub-tab.

2. Click on the Installed Applications tab.

3. Select the scanning profile that you wish to customize from the left pane under **Profiles**.

4. Select the **Enable scanning for installed applications on target computers** option.

NOTE: Installed applications scanning are configurable on a scan profile by scan profile basis. Make sure to enable installed applications scanning in all profiles where this is required.

Compiling installed applications blacklist/whitelist

To compile installed applications blacklist/whitelist:

1. From the **Network & Security Audit Options** tab, click **Applications** sub-tab.

2. Click on the Installed Applications tab.

3. Select the scanning profile that you wish to customize from the left pane under **Profiles**.

4. In the right pane, select **Enable scanning for installed** applications on target computer(s) option.

5. Select either **Only applications in the list below:** or **All applications except the ones in the list below** and click add button to add applications that will either be listed or blacklisted.

6. In the **Ignore (Do not list/save to db) applications from the list below:** options key in applications by clicking Add. Any application listed is whitelisted.

NOTE: Include only one application name per line.

7.11.2 Scanning security applications

🙎 GFI LANguard Scanning Profiles Editor	
File	
Scanning Profiles	
Profile categories:	🍋 Vulnerability Assessment Options 🛛 💫 Network & Software Audit Options
Complete/Combination Scans Vulnerability Assessment Network & Software Audit	TCP Ports UDP Ports System Information Devices Applications Choose scan profile conditions. Image: Computer (s) Image: Computer (s) Image: Computer (s)
 Full Vulnerability Assessment Full Scan Full Scan (Slow Networks) My Scanning profile 	Installed Applications Security Applications Use GFI LANguard to detect installed security software and ensure that they are using the latest definition files. Where applicable GFI LANguard will also check that important settings are enabled (e.g. real time scanning)
Common Tasks: New scarning profile Set Active Rename Delete Ø Help: Scarning Profiles LANguard Scripting	Advanced

Screenshot 97 - The Applications configuration page: Security Applications tab options

GFI LANguard ships with a default list of anti-virus and anti-spyware applications that can be checked during security scanning.

Enabling/disabling checks for security applications

To enable checks for installed security applications in a particular scanning profile:

1. From the **Network & Security Audit Options** tab, click on the **Applications** sub-tab.

2. Click on the Security Applications tab.

3. Select the scanning profile that you wish to customize from the left pane under **Profiles**.

4. Select the **Detect and process installed antivirus/antispyware software on target computer(s)** option.

NOTE: Security applications scanning are configurable on a scan profile by scan profile basis. Make sure to enable security applications scanning in all profiles where this is required.

Customizing the list of security application for scanning

To specify which security applications will be scanned during an audit:

1. From the **Network & Security Audit Options** tab, click on the **Applications** sub-tab.

2. Click on the Security Applications tab.

3. Select the scanning profile that you wish to customize from the left pane under **Profiles**.

4. Select the security applications that you wish investigate.

Configuring security applications - advanced options

Use the **Advanced** button included in the **Security Applications** configuration page to configure extended security product checks that generate high security vulnerability alerts when:

- The anti-virus or anti-spyware product definitions files are out of date.
- The 'Realtime Protection' feature of a particular anti-virus or antispyware application is found disabled.
- None of the selected anti-virus or anti-spyware software is currently installed on the scanned target computer.

7.12 Configuring the security scanning options

Use the **Scanner Options** tab to configure the operational parameters of the security-scanning engine. These parameters are configurable on a scan profile by scan profile basis and define how the scanning engine will perform target discovery and OS Data querying.

File				
Scanning Profiles				
Profile categories:	Vulnerability Assessmen	nt Options 🛛 💦 Network & Soft	ware Audit Options	Scanner Options
Complete/Combination Scans Vulnerability Assessment Network & Software Audit	Specify network discovery an information.	d other parameters on how the sc	anner is to discover m	nachines and output debug
	 Network Discovery Me 	thods		
Profiles:	NetBIOS queries		Yes	
🍇 Full Vulnerability Assessment	SNMP queries		Yes	
😽 Full Scan	Ping sweep		Yes	
Full Scan (Slow Networks)	Custom TCP discovery	(e.g. 21, 25, 80)		
My scanning profile	 Network Discovery Opt 	tions		
	Scanning delay (default	t 100 ms)	100	
	Network discovery quer	ry responses timeout (default 500 i	m 500	
	Number of retries (defa	ault 1)	1	
	Include non-responsive	computers	No	
	 Network Scanner Option 	ons		
	Scanning threads count	t	3	
Common Tasks:	NetBIOS Query Options	5		
New scanning profile	Scope ID			
Set Active	 SNMP Query Options 			
Rename	Load SNMP enterprise n	numbers	Yes	
Delete	Community strings (e.g.	. public, private)	public	
	Global Port Query Optic	ons		
) Help:	TCP port scan query tim	neout (default 1500 ms)	1500	
C	UDP port scan query tin	meout (default 600 ms)	600	
Scanning Profiles	 WMI Options 			
	WMI timeout (default 2	0000 ms)	20000	
	SSH Options			
	SSH Timeout (default 1	5000 ms)	15000	
	 Scanner activity windo 	w.		
	- Type of compart activity	o accharat	Cimple	

Screenshot 98 - Scanning Profiles properties: Scanner Options tab

Configurable options include timeouts, types of queries to run during target discovery, number of scanning threads count, SNMP scopes for queries and more.

NOTE: Configure these parameters with extreme care! An incorrect configuration can affect the security scanning performance of GFI LANguard.

8. Utilities

8.1 Introduction

Use the **Utilities** tab to access the following list of default network tools:

- DNS Lookup
- Traceroute
- Whois
- Enumerate Computers
- Enumerate Users
- SNMP Audit
- SNMP Walk
- SQL Server Audit

8.2 DNS lookup

DNS lookup resolves domain names into the corresponding IP address and retrieves particular information from the target domain (for example, MX record, etc.).

💽 GFI LANguard	
File Tools Configure Help	Discuss this version
Network Audit Dashboard Configura	tion Utilities General
Tools:	Hostname/IP to resolve: www.microsoft.com
DNS Lookup Traceroute Whois Enumerate Computers SNMP Audt SNMP Walk SQL Server Audt	Starting DNS Lookup Request for www.microsoft.com: 1:40.02 PM Performing DNS Lookup operation through DNS Server 192.168.3.254 Resolving host www.microsoft.com Please wal Basic information results: No A Records found
Authenticate using: Currently logged on user Usemame: administrator	MX Records results: ENAME: toggle www.ms.akadns.net ENAME: g.www.ms.akadns.net ENAME: Ib1.www.ms.akadns.net
Password:	Completed DNS Lookup Request for www.microsoft.com: 1:40:11 PM
Remember credentials Use computer profiles (Edit)	
Common Tasks:	
Edit DNS lookup options	
DNS lookup	

Screenshot 99 - The DNS Lookup tool

To resolve a domain/host name:

1. Click on the **Utilities** tab and select **DNS Lookup** in the left pane under **Tools**.

2. Specify the hostname to resolve in the **Hostname/IP to resolve** textbox.

DNS Lookup Options	3
General	
Specify DNS Lookup information to be retrieved and the DNS server to be used	
Retrieve the following information:	
Basic information Host information Aliases	
MX Records NS Records	
DNS Server(s) to query: Use default DNS server Use alternative DNS server(s) Add Remove	
OK Cancel Apply	

Screenshot 100 - The DNS Lookup tool

3. Under **Common Tasks** in the left pane, click on **Edit DNS Lookup options...** or **Options** button on the right pane and specify the information that you wish to retrieve:

- **Basic Information** Select this option to retrieve the host name and the relative IP address.
- Host Information Select this option to retrieve HINFO details. The host information (known as HINFO) generally includes target computer information such as hardware specifications and OS details.

NOTE: Most DNS entries do not contain this information for security reasons.

- Aliases Select this option to retrieve information on the 'A Records' configured on the target domain.
- **MX Records** Select this option to enumerate all the mail servers and the order (i.e. priority) in which they receive and process emails for the target domain.
- **NS Records** Select this option to specify the 'name-servers' that are authoritative for a particular domain or sub domain.

4. Specify (if required) the alternative DNS server that will be queried by the DNS Lookup tool or leave as default to use the default DNS server.

5. Click on the **Retrieve** button to start the process.

8.3 Traceroute

Traceroute identifies the path that GFI LANguard followed to reach a target computer.

💽 GFI LANguard									
File Tools Configure Help								Discuss th	is version
Network Audit Dashboard Config	uratio	on 📋	Utilities	General					
Tools:		Trace	(domain/ll	P address/name):	192.168.3.66		 Trace 	route 0	ptions
DNS Lookup Traceroute	-	Нор	Itera	IP Address (Hos	tname)		Time (ms)	Best time	Average
Whois Enumerate Computers		√ 1	1	192.168.3.66 (V	XPPRO)		39	39	39.00
SNMP Audit SNMP Walk									
SQL Server Audit									
Credentials:									
Authenticate using:									
Currently logged on user -									
Usemame:	=								
administrator								_	
Password:					(🗸	·			
*****					Hop	os			
Remember credentials			45			39			
Use computer profiles			35						
(Edit)		월	30						
Common Tasks:		l Diag	25						
Edit traceroute options		Millis	15 10						
🕑 Help:			°			1			
Traceroute	-	•							
leady									

Screenshot 101 - Trace route tool

To use this tool:

1. Click on the **Utilities** tab and select **Traceroute** in the left pane under **Tools**.

2. In the **Trace (domain/IP/name)** dropdown, specify the name/IP or domain to reach.

3. Under **Common Tasks** in the left pane, click on **Edit Traceroute options...** or **Options** button on the right pane to change the default options.

4. Click on the **Traceroute** button to start the tracing process.

Traceroute will break down, the path taken to a target computer into 'hops'. A hop indicates a stage and represents a computer that was traversed during the process. The information enumerated by this tool includes the IP of traversed computers, the number of times that a computer was traversed and the time taken to reach the respective computer. An icon is also included next to each hop. This icon indicates the state of that particular hop. The icons used in this tool include:

- ✓ Indicates a successful hop taken within normal parameters.
- ▲ Indicates a successful hop, but time required was quite long.
- Indicates a successful hop, but the time required was too long.
- X Indicates that the hop was timed out (> 1000ms).

8.4 Whois

Whois looks up information on a particular domain or IP address.

💽 GFI LANguard		
File Tools Configure Help		Discuss this version
Network Audit Dashboard Configurat	ion Utilities General	
Tools:	Query (domain/IP address/name):	Retrieve Options
DNS Lookup Traceroute Whois Enumerate Computers SNMP Audt SNMP Walk SQL Server Audt Credentials: Authenticate using: Currently logged on user Usemame: administrator Password: ***** Ø Remember credentials Ø Use computer profiles (Edt) Common Tasks:		
Edit whois options		
elp:		
Whois		

Screenshot 102 - Whois tool

1. Click on the **Utilities** tab and select **Whois** in the left pane under **Tools**.

2. In the **Query (domain/IP/name)** dropdown, specify the name/IP or domain to reach.

3. Under **Common Tasks** in the left pane, click on **Edit Whois options...** or **Options** button on the right pane to change the default options.

4. Click on the **Retrieve** button to start the process.

8.5 Enumerate computers

💽 GFI LANguard		
File Tools Configure Help		Discuss this version
Network Audit Dashboard Configura	ion Utilities General	
Tools:	Enumerate computers in domain:	Retrieve Options
INS Lookup	Name Operating System	т Туре
Whois Enumerate Computers For more to Lloom		*
SNMP Audit		
SQL Server Audit		
Credentials:		
Authenticate using:		
Currently logged on user -		
Usemame:		
administrator		
Password:		

Remember credentials		
Use computer profiles		
(Edit)		
Common Tasks:		
Edit enumerate computers options		
🜒 Help:		v
Enumerate computers		4

Screenshot 103 - Enumerate Computers tool

The enumerate computers utility identifies domains and workgroups on a network. During execution, this tool will also scan each domain/workgroup discovered so to enumerate their respective computers. The information enumerated by this tool includes:

- the domain or workgroup name.
- the list of domain/workgroup computers.
- the operating system installed on the discovered computers.
- any additional details that might be collected through NetBIOS.

Computers can be enumerated using one of the following methods:

- From the Active Directory This method is much faster and will include computers that are currently switched off.
- Using the Windows Explorer interface This method enumerates computers through a real-time network scan and therefore it is slower and will not include computers that are switched off.

To enumerate computers:

1. Click on the **Utilities** tab and select **Enumerate Computers** in the left pane under **Tools**.

2. In the **Enumerate computers in domain** dropdown, select the desired domain.

3. Under **Common Tasks** in the left pane, click on **Edit Enumerate Computers options...** to change the default options or **Options** button on the right pane.

4. Click on the **Retrieve** button to start the process.

NOTE: For an Active Directory scan, you will need to run the tool (i.e. GFI LANguard) under an account that has access rights to the Active Directory.

8.5.1 Starting a security scan

The 'Enumerate Computers' tool scans your entire network and identifies domains and workgroups as well as their respective computers. After enumerating the computers in a domain or workgroup, you can use this tool to launch a security scan on the listed computers. To start a security scan directly from the 'Enumerate Computers' tool, right click on any of the enumerated computers and select **Scan**.

You can also launch a security scan and at the same time continue using the **Enumerate Computers** tool. This is achieved by right clicking on any of the enumerated computers and selecting **Scan in background**.

8.5.2 Deploying custom patches

You can use the **Enumerate Computers** tool to deploy custom patches and third party software on the enumerated computers. To launch a deployment process directly from this tool:

1. Select the computers that require deployment.

2. Right click on any of the selected computers and select **Deploy Custom Patches**.

8.5.3 Enabling auditing policies

The **Enumerate Computers** tool also allows you to configure auditing policies on particular computers. This is done as follows:

1. Select the computers on which you want to enable auditing policies.

2. Right click on any of the selected computers and select **Enable Auditing Policies...**. This will launch the **Auditing Policies configuration Wizard** that will guide you through the configuration process.

8.6 Enumerate users

💽 GFI LANguard		
File Tools Configure Help		Discuss this version
Network Audit Dashboard Configura	ion Utilities General	
Tools:	Enumerate users in domain:	Retrieve Options
Tracemute	User name Full name Desc	ription
Whois		
Sector Enumerate Computers		
🐳 Enumerate Users		
SNMP Audit		
SNMP Walk		
SQL Server Audit		
Credentials:		
Authenticate using:		
Currently logged on user		
Usemame:		
administrator		
Password:		

Remember credentials		
Use computer profiles		
(Edit)		
Common Tasks		
Edit enumerate users options		-
	•	•
🕐 Help:	· · · · · · · · · · · · · · · · · · ·	
Enumerate users		
	2	

Screenshot 104 - The Enumerate Users tool dialog

To scan the Active Directory and retrieve the list of all users and contacts included in this database:

1. Click on the **Utilities** tab and select **Enumerate Users** in the left pane under **Tools**.

2. In the **Enumerate users in domain** dropdown, select the desired domain.

3. Under **Common Tasks** in the left pane, click on **Edit Enumerate Users options...** or **Options** button on the right pane to filter the information to be extracted and display only the users or contacts details. In addition, you can optionally configure this tool to highlight disabled or locked accounts.

4. Click on the **Retrieve** button to start the process.

From this tool, you can also enable or disable any user account that has been enumerated. This is achieved by right clicking on the account and selecting **Enable/Disable account** accordingly.

8.7 SNMP Auditing

💽 GFI LANguard												ı x
File Tools Configure Help										Discu	iss this ve	rsion
Network Audit Dashboard Configuration Utilities General												
Tools:	IP address or range of IP addresses for computer(s) running SNMP: 192.168.3.100 Betrieve											
DNS Lookup Traceroute	P Address	Comp	public	private	all pri	router	cisco	admin	DIOXV	write	access	root
Whois	192.168.3.100								P9			
Enumerate Users												
SNMP Audit SNMP Walk												
SQL Server Audit												
Credentiais:												
Authenticate using: Currently logged on user												
administrator Password:												
Remember credentials Use computer profiles												
(Edit)												
Common Tasks:												
Edit SNMP audit options												
Welp:												
SNMP audit 🚽 🗸				III	1		1	1				Þ
1009	%											

Screenshot 105 - SNMP Audit tool

This tool identifies and reports weak SNMP community strings by performing a dictionary attack using the values stored in its default dictionary file (snmp-pass.txt). You can add new community strings to the default dictionary file by using a text editor (for example, notepad.exe).

You can also direct the **SNMP Audit** tool to use other dictionary files. To achieve this, specify the path to the dictionary file that you want to from the tool options at the right of the management console.

To perform SNMP audits on network targets and identify weak community strings:

1. Click on the **Utilities** tab and select **SNMP Audit** in the left pane under **Tools**.

2. In the **IP of computer running SNMP** dropdown, specify the IP to reach.

3. Under **Common Tasks** in the left pane, click on **Edit SNMP Audit options...** or **Options** button on the right pane to edit the default options.

4. Click on the **Retrieve** button to start the process.

8.8 SNMP Walk

💽 GFI LANguard			- • •
File Tools Configure Help		Discu	ss this version
Network Audit Dashboard Configurat	ion Utilities General		
Network Audit Dashboard Configurat Tools:	ion Utilities General IP address: 127.0.0.1 Description: iso.org.dod.internet.secur iso org org org org org org org org	D: 1.3.6.1.5 <u>Retrieve</u>	Value
Edit SNMP walk options			
🕖 Help:			
SNMP walk		<) •
			.4

Screenshot 106 - SNMP Walk

To probe your network nodes and retrieve SNMP information (for example, OID's):

1. Click on the **Utilities** tab and select **SNMP Walk** in the left pane under **Tools**.

2. In the **IP address** dropdown, specify the IP address of the computer that you wish to scan for SNMP information.

3. Under **Common Tasks** in the left pane, click on **Edit SNMP Walk options...** or **Options** button on the right pane to edit the default options such as providing alternative community strings.

4. Click on the **Retrieve** button to start the process.

NOTE: SNMP activity is often blocked at the router/firewall so that Internet users cannot SNMP scan your network. The information enumerated through SNMP can be used by malicious users to attack your system. Unless this service is required, it is highly recommended to turn off SNMP.

8.9 SQL Server Audit

This tool allows you to test the password vulnerability of the 'sa' account (i.e. root administrator), and any other SQL user accounts configured on the SQL Server. During the audit process, this tool will perform dictionary attacks on the SQL server accounts using the credentials specified in the 'passwords.txt' dictionary file. However, you can also direct the **SQL Server Audit** tool to use other dictionary files. You can also customize your dictionary file by adding new passwords to the default list.

To perform a security audit on a particular Microsoft SQL server installation:



1. Click on the **Utilities** tab and select **SQL Server Audit** in the left pane under **Tools**.

Screenshot 107 -SQL Server Audit

2. In the **Audit MS SQL Server** dropdown, specify the IP address of the SQL Server that you wish to audit.

3. Under **Common Tasks** in the left pane, click on **Edit SQL Server Audit options...** or **Options** button on the right pane to edit the default options such as performing dictionary attacks on all the other SQL user accounts.

4. Click on the **Audit** button to start the process.

9. Using GFI LANguard from the command line

9.1 Introduction

In this chapter you will discover how to use the three command line tools bundled with GFI LANguard; 'Insscmd.exe', 'deploycmd.exe' and 'impex.exe' These command line tools allow you to launch network vulnerability scans and patch deployment sessions as well as importing and exporting profiles and vulnerabilities without loading up the GFI LANguard management console.

Configured through a set of command line switches, the complete list of supported switches together with a description of the respective function is provided below.

9.2 Using 'Insscmd.exe' - the command line scanning tool

The 'Insscmd.exe' command line target-scanning tool allows you to run vulnerability checks against network targets directly from the command line, or through third party applications, batch files and scripts. The 'Insscmd.exe' command line tool supports the following switches:

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

Switch	Description
Target	Specify the IP / range of IPs or host name(s) to be
	scanned.
/Profile	(Optional) Specify the scanning profile that will be
	used during a security scan. If this parameter is not
	specified, the scanning profile that is currently active
	in the GFI LANguard will be used.
	NOTE: In the management console, the default (i.e.
	currently active) scanning profile is denoted by the
	word (Active) next to its name. To view which profile
	is active expand the Configuration Scanning
	Profiles node.
/Output	(Optional) Specify the full path (including filename) of
	the XML file where the scan results will be saved.
/Report	(Optional) Specify the full path (including filename) of
	the HTML file where the scan results HTML report
	will be output/saved.

Switches:

/User and	(Optional) Specify the alternative credentials that the
/Password	scanning engine will use to authenticate to a target
	computer during security scanning. Alternatively you
	can use the /UseComputerProfiles switch to use the
	authentication credentials already configured in the
	Computer Profiles (Configuration > Computer
	Profiles node).
/Email	(Optional) Specify the email address on which the
	resulting report(s) will be sent at the end of this scan.
	Reports will be emailed to destination through the
	mail server currently configured in the Configuration
	Alerting Options node (of the management
	console).
/DontShowStatus	(Optional) Include this switch if you want to perform
	silent scanning. In this way, the scan progress details
	will not be shown.
/?	(Optional) Use this switch to show the command line
	tool usage instructions.

NOTE: Always enclose full paths, and profile names within double quotes (i.e. '[path or profile name]') for example, 'Default', 'c:\temp\test.xml'.

The command line target-scanning tool allows you to pass parameters through specific variables. These variables will be automatically replaced with their respective value during execution. Supported variables include:

Supported variable	Description
%INSTALLDIR%	During scanning, this variable will be replaced with the path to the GFI LANguard installation directory.
%TARGET%	During scanning this variable will be replaced with the name of the target computer.
%SCANDATE%	During scanning this variable will be replaced with the date of scan.
%SCANTIME%	During scanning this variable will be replaced with the time of scan.

Example: How to launch target computer scanning from the command line tool.

For this example, we will be assuming that a scan with the following parameters is required:

1. Perform a security scan on a target computer having IP address '130.16.130.1'.

- 2. Output the scan results to 'c:\out.xml' (i.e. XML file).
- 3. Generate an HTML report and save it in 'c:\result.html'.

4. Send the HTML report via email to 'lanss@127.0.0.1'

The command line tool instruction for this particular security scan is:

9.3 Using 'deploycmd.exe' - the command line patch deployment tool

The 'deploycmd.exe' command line patch deployment tool allows you to deploy Microsoft patches and third party software on remote targets directly from the command line, or through third party applications, batch files or scripts. The 'deploycmd.exe' command line tool supports the following switches:

deploycmd [target] [/file=FileName] [/username=UserName /password=Password] [/UseComputerProfiles] [/warnuser] [/useraproval] [/stopservices] [/customshare=CustomShareName] [/reboot] [/rebootuserdecides] [/shutdown] [/deletefiles] [/timeout=Timeout(sec)] [/?]

Switch	Description
Target	Specify the name(s), IP or range of IPs of the target
	computer(s) on which the patch(es) will be deployed.
/File	Specify the file that you wish to deploy on the
	specified target(s).
/User and	(Optional) Specify the alternative credentials that the
/Password	scanning engine will use to authenticate to a target
	computer during patch deployment. Alternatively you
	can use the /UseComputerProfiles switch to use the
	authentication credentials already configured in the
	Computer Profiles (Configuration Computer
	Profiles node).
/warnuser	(Optional) Include this switch if you want to inform the
	target computer user that a file/patch installation is in
	progress. Users will be informed through a message
	dialog that will be shown on screen immediately
	before the deployment session is started.
/useraproval	(Optional) Include this switch to request the user's
	approval before starting the file/patch installation
	process. This allows users to postpone the file/patch
	installation process for later (for example, until an
	already running process is completed on the target
	computer).
/stopservice	(Optional) Include this switch if you want to stop
	specific services on the target computer before
	installing the file/patch.
	NOTE : You cannot specify the services that will be
	stopped directly from the command line tool.
	Services can only be added or removed through the
	management console.
/customshare	(Optional) Specify the target share where you wish to
	transfer the file before it is installed.

Switches:

/reboot	(Optional Parameter) Include this switch if you want to reboot the target computer after file/patch deployment.
/rebootuserdecides	(Optional Parameter) Include this switch to allow the current target computer user to decide when to reboot his computer (after patch installation).
/shutdown	(Optional Parameter) Include this switch if you want to shutdown the target computer after the file/patch is installed.
/deletefiles	(Optional Parameter) Include this switch if you want to delete the source file after it has been successfully installed.
/timeout	(Optional Parameter) Specify the deployment operation timeout. This value defines the time that a deployment process will be allowed to run before the file/patch installation is interrupted.
/?	(Optional) Use this switch to show the command line tool's usage instructions.

Example: How to launch a patch deployment process from the command line tool.

For this example, we will be assuming that a patch deployment session with the following parameters is required:

- 1. Deploy a file called 'patchA001002.XXX'.
- 2. On target computer 'TMJohnDoe'.
- 3. Reboot the target computer after successful deployment of the file.

The command line tool instruction for this particular patch deployment session is:

deploycmd TMJohnDoe /file="patchA001002.XXX" /reboot

9.4 Using 'impex.exe' - the command line import and export tool

The Impex tool is a command line tool which can be used to Import and Export profiles and vulnerabilities from GFI LANguard Network Security Scanner. The parameters supported by this tool are the following:

impex [[/H] | [/?]] | [/XML:xmlfile [/DB:dbfile] [[/EX] [/MERGE]] | [/IM [/ONLYNEWER]]

[/PROFILES | /VULNS | /PORTS | /PROFILE:name |

/VULNCAT:cat [/VULN:name]

/PORTTYPE:type [/PORT:number]]

[/SKIP | /OVERWRITE | /RENAME:value]]

Options:

Option	Description
H, /?, running without	Displays help information.
parameters	

/XML: <xmlfile></xmlfile>	This parameter specifies the name of the imported or exported XML file. <xmlfile> needs to be replaced with the name of the file the profile is being exported to. NOTE: This parameter is mandatory to import or export alerts.</xmlfile>
/DB: <dbfile></dbfile>	Where <dbfile> is the database file to be used during the import/export operation. If this is not specified the default "operationsprofiles.mdb" file will be used.</dbfile>
/EX	Exports data from database to XML file (Default option)
/MERGE	If this is specified when the target XML for export already exists, the file will be opened and data will be merged; otherwise the XML file is first deleted.
/IM	Imports data from XML file to database
/ONLYNEWER	When specified only vulnerabilities newer than the newest vulnerability in the database will be imported.
/PROFILES	Exports/Imports all scanning profiles.
/VULNS	Exports/Imports all vulnerabilities.
/PORTS	Exports/Imports all ports
/PROFILE: <name></name>	Exports/Imports the specified scanning profile.
/VULNCAT: <category></category>	Exports/Imports all vulnerabilities of the specified category.
/VULN: <name></name>	Exports/Imports the specified vulnerability (/VULNCAT must be specified).
/PORTTYPE: <type></type>	Exports/Imports all ports of the specified type.
/PORT: <number></number>	Exports/Imports the specified port (/PORTTYPE must be specified).
/SKIP	If an item already exists in the target XML/database, that item will be skipped
/OVERWRITE	If an item already exists in the target XML/database, that item will be overwritten.
/RENAME: <value></value>	If an item already exists in the target XML/database, that item will be renamed to <value>. If /PROFILE or /VULN was specified, port information merged with that item is a port or renamed by prefixing its name with <value> in any other case.</value></value>

Example: To export a specific alert:

impex /xml:regcheck.xml /vuln:"Blaster Worm" /vulncat:"Registry Vulnerabilities"

Example: To import a whole XML file:

impex /xml:regcheck.xml /im

NOTE 1: The Impex executable can be located in the GFI LANguard 9.0 installation folder.

NOTE 2: It is highly recommended not to use the Impex tool if GFI LANguard application (languard.exe) or LANguard scanning profiles (scanprofiles.exe) are running.

NOTE 3: If the specified <xmlfile>, <dbfile>, <name>, <category> or <value> contain any space character, the whole value must be placed between double quotes.

Example: /VULN:"Apache: Apache doc directory"

NOTE 4: It is recommended that if the vulnerabilities are imported into another installation, the other installation have the same build number as where the vulnerabilities database has been exported.

10. Adding vulnerability checks via custom conditions or scripts

10.1 Introduction

Scripts that identify custom vulnerabilities can be created using any VBScript compatible scripting language. By default, GFI LANguard ships with a script editor that you can use to create your custom scripts.

New checks must be included in the list of checks supported by GFI LANguard. Use the **Vulnerability Assessment** tab to add new checks to the default list of vulnerability checks on a scan profile by scan profile basis.

GFI LANguard also supports Python scripting. For more information on GFI LANguard Python scripting refer to the section in this manual.

NOTE: Only expert users should create new vulnerability checks. Scripting errors and wrong configurations in a vulnerability check can result in false positives or provide no vulnerability information at all.

10.2 GFI LANguard VBscript language

GFI LANguard supports and runs scripts written in VBscript compatible languages. Use VBscript compatible languages to create custom scripts that can be run against your network targets.

Security auditing scripts can be developed using the script editor that ships with GFI LANguard. This built-in script editor includes syntax highlighting capabilities as well as debugging features that support you during script development. Open the script editor from **Start** ► **Programs** ► **GFI LANguard 9.0** ► **LANguard Script Debugger**.

NOTE: For more information on how to develop scripts using the builtin script editor, refer to the **Scripting documentation** help file included in **Start** ► **Programs** ► **GFI LANguard 9.0** ► **LANguard Scripting documentation**.

IMPORTANT NOTE: GFI does not support requests related to problems in custom scripts. You can post any queries that you may have about GFI LANguard scripting on the GFI LANguard forums at http://forums.gfi.com/. Through this forum you will be able to share scripts, problems and ideas with other GFI LANguard users.

10.2.1 Adding a vulnerability check that uses a custom VB (.vbs) script

To create new vulnerability checks that use custom VBscripts:

- Step 1 : Create the script.
- Step 2: Add the new vulnerability check.

The following are examples of how this is done.

Step 1 : Create the script

1. Launch the Script Debugger from **Start** ► **Programs** ► **GFI LANguard 9.0** ► **LANguard Script Debugger**.

2. Go on **File ► New...**

3. Create a script. For this example use the following dummy script code.

```
Function Main
echo "Script has run successfully"
Main = true
```

```
End Function
```

4. Save the script in '<LANguard 9.0 installation folder path> \Data\Scripts\myscript.vbs'.

Step 2: Add the new vulnerability check

1. Open the GFI LANguard management console.

2. Click on the **Configuration** tab, and select scanning profiles management,

3. Click on the **Vulnerability Assessment** sub-node and from the middle pane, select the category in which the new vulnerability check will be included (for example, High Security Vulnerabilities).

Add vulnerability		X
General Conditions	Description References	
<u>N</u> ame:		
<u>T</u> ype:	DNS	J
OS <u>F</u> amily:	windows 👻	
OS <u>V</u> ersion:		
Product:		
Timestamp:	5/ 5/2009	
S <u>e</u> verity:	\rm High 👻	
	OK Cancel	

Screenshot 108 - The new vulnerability check dialog

4. In the new window, add a new vulnerability by clicking **Add...** in the middle pane.

5. Go through the **General**, **Description** and **References** tabs while specifying the basic details such as the vulnerability name, short description, security level and OVAL ID (if applicable).

6. Click the **Conditions** tab and click on the **Add...** button. This will bring up the check properties wizard.

Check properties	.
Step 1 of 3: Select the type of check Specify what do you want to check from the list below	\checkmark
Check type:	
Independent Family Test Independent FTP Banner Test Independent HTTP Banner Test Independent POP3 Banner Test Independent Port Open Test Independent Python Script Test Independent SMTP Banner Test Independent SSH Banner Test Independent TCP Banner Test Independent TELNET Banner Test Independent Text File Content Test Independent VB Script Test	
Check description:	
Executes a VB script and returns a boolean value.	*
< Back Next > Car	ncel

Screenshot 109 - The check triggering conditions dialog

7. Select **Independent checks** ► **VBScript** node and click on **Next** button to continue setup.

8. Click on the **Choose file** button and select the custom VBscript file that will be executed by this check (For this example select 'myscript.vbs'). Click on **Next** to proceed.

9. Select the relative condition setup in the wizard to finalize script selection. Click on **Finish** to exit wizard.

10. Click on **OK** to save new vulnerability check.

Testing the vulnerability check/script used in example

Scan your local host computer using the scanning profile where the new check was added.

In **Network Audit** Scan Results, a vulnerability warning will be shown in the **Vulnerability Assessment** node of the scan results.

10.3 GFI LANguard SSH Module

GFI LANguard includes an SSH module which handles the execution of vulnerability scripts on Linux/UNIX based systems.

The SSH module determines the result of vulnerability checks through the console (text) data produced by an executed script. This means that you can create custom Linux/UNIX vulnerability checks using any scripting method that is supported by the target's Linux/UNIX OS and which outputs results to the console in text.

10.3.1 Keywords

The SSH module can run security scanning scripts through its terminal window. When a security scan is launched on Linux/UNIX based target computers, vulnerability checking scripts are copied through an SSH connection to the respective target computer and run locally.

The SSH connection is established using the logon credentials (i.e. username and password/SSH Private Key file) specified prior to the start of a security scan.

The SSH module can determine the status of a vulnerability check through specific keywords present in the text output of the executed script. These keywords are processed by the module and interpreted as instruction for the GFI LANguard. Standard keywords identified by the SSH module include:

- TRUE:
- FALSE:
- AddListItem
- SetDescription
- !!SCRIPT_FINISHED!!

Each of these keywords triggers an associated and specific process in the SSH Module. The function of each keyword is described below:

- **TRUE:** / **FALSE:** These strings indicate the result of the executed vulnerability check/script. When the SSH module detects a TRUE: it means that the check was successful; FALSE: indicates that the vulnerability check has failed.
- AddListItem This string triggers an internal function that adds results to the vulnerability check report (i.e. scan results). These results are shown in the GFI LANguard management console after completion of a scan. This string is formatted as follows:

AddListItem([[[[parent node]]]],[[[[actual string]]]])

- [[[[parent node]]]] Includes the name of the scan results node to which the result will be added.
- [[[[actual string]]]] Includes the value that will be added to the scan results node.

NOTE: Each vulnerability check is bound to an associated scan result node. This means that 'AddListItem' results are by default included under an associated/default vulnerability node. In this way, if the parent node parameter is left empty, the function will add the specified string to the default node.

• **SetDescription** – This string triggers an internal function that will overwrite the default description of a vulnerability check with a new

description. This string is formatted as follows: SetDescription([New description])

!!SCRIPT_FINISHED!! – This string marks the end of every script execution. The SSH module will keep looking for this string until it is found or until a timeout occurs. If a timeout occurs before the '!!SCRIPT_FINISHED!!' string is generated, the SSH module will classify the respective vulnerability check as failed.

NOTE: It is imperative that every custom script outputs the '!!SCRIPT_FINISHED!!' string at the very end of its checking process.

10.3.2 Adding a vulnerability check that uses a custom shell script

In the following example we will create a vulnerability check (for Linux based targets) which uses a script written in Bash. The vulnerability check in this example will test for the presence of a dummy file called 'test.file'

Step 1 : Create the script

1. Launch your favorite text file editor.

2. Create a new script using the following code:

```
#!/bin/bash
if [ -e test.file ]
then
echo "TRUE:"
else
echo "FALSE:"
fi
echo "!!SCRIPT_FINISHED!!"
```

3. Save the file in ' <GFI LANguard 9.0 installation folder path> ..\Data\Scripts\myscript.sh"

Step 2: Add the new vulnerability check

1. Open the GFI LANguard management console.

2. Click on the **Configuration** tab, expand the **Scanning Profiles** and click on the **Vulnerability Assessment** sub-node.

3. From the middle pane, select the category in which the new vulnerability check will be included (for example, High Security Vulnerabilities...).

4. In the new window, add a new vulnerability by clicking **Add...** in the middle pane.

5. Go through the General, Description and Reference tabs while specifying the basic details such as the vulnerability name, short description, security level and OVAL ID (if applicable).

6. Choose the **Conditions** tab and click on the **Add...** button. This will bring up the check properties wizard.

Check properties
Step 1 of 3: Select the type of check Specify what do you want to check from the list below
Check type:
Windows Checks Unix Checks Unix File Test Unix Process Test Unix RPC Service Test Unix SSH Script Test Unix Uname Test Solaris Checks Independent Checks
Check description:
Executes a SSH script on the target computer and returns a boolean value or a string.
< Back Next > Cancel

Screenshot 110 - The check triggering conditions dialog

7. Select **Unix checks** ► **SSH Script Test** node and click on Next button to continue setup.

8. Click on the **Choose file** button and select the custom SSH Script file that will be executed by this check (For this example select 'myscript.sh'). Click on **Next** to proceed.

9. Select the relative condition setup in the wizard to finalize script selection. Click on **Finish** to exit wizard.

10. Click on **OK** to save new vulnerability check.

Testing the vulnerability check/script used in our example

Scan your local host computer using the scanning profile where the new check was added.

1. Log on to a Linux target computer and create a file called 'test.file'. This check will generate a vulnerability alert if a file called 'test.file' is found.

2. Launch a scan on the Linux target where you created the file.

3. Check you scan results.

10.4 Python scripting

GFI LANguard also supports a new type of vulnerability checks -Python Script Test. This type of check is available under the Independent Checks type.

Check properties	×
Step 1 of 3: Select the type of check Specify what do you want to check from the list below	\checkmark
Check type:	
 Linux Checks Independent Checks Independent CGI Abuse Test Independent DNS Banner Test Independent Family Test Independent FTP Banner Test Independent POP3 Banner Test Independent Port Open Test Independent SMTP Banner Test Independent SSH Banner Test Independent TCP Banner Test 	
Check description:	
Executes a Python script and returns a boolean value.	*
< Back Next > Cance	el

Screenshot 111 - Independent checks: Python Script Test

For more information on Python scripting refer to the GFI LANguard scripting documentation located in **Start menu** ► **Programs** ► **GFI LANguard 9.0**.
11. Miscellaneous

11.1 Introduction

In this section you will find information on:

- How to enable NetBIOS on a network computer.
- Installing the Client for Microsoft Networks component on Windows 2000 or higher.
- Configuring Password Policy Settings in an Active Directory-Based Domain.
- Viewing the Password Policy Settings of an Active Directory-Based Domain.

11.2 Enabling NetBIOS on a network computer

1. Log on to the target computer with administrative rights

2. Navigate to **Control Panel** and access **Networking options** or **Network or Sharing Centre**.

3. Right click on **Local Area Connection** icon of the NIC card that you wish to configure and select **Properties**.

- 4. Click on Internet Protocol (TCP/IP) and select Properties.
- 5. Click on the **Advanced** button.
- 6. Click on the **WINS** tab.

Advanced TCP/IP Settings	? ×	
IP Settings DNS WINS Options		
WINS addresses, in order of use:		
	÷	
<u>A</u> dd <u>E</u> dit	Remoye	
If LMHOSTS lookup is enabled, it applies to all o TCP/IP is enabled.	connections for which	
Enable LMHOSTS lookup Import LMHOSTS		
NetBIOS setting Default: Use NetBIOS setting from the DHCP server. If static IP address is used or the DHCP server does not provide NetBIOS setting, enable NetBIOS over TCP/IP.		
C Enable NetBIOS over TCP/IP		
Disable NetBIOS over TCP/IP		
	OK Cancel	

Screenshot 112 - Local Areas Connection properties: WINS tab

7. Select the **Default** option from the **NetBIOS Setting** area.

NOTE: If static IP is being used or the DHCP server does not provide NetBIOS setting, select the **Enable NetBIOS over TCP/IP** option instead.

8. Click on **OK** and exit the Local Area Properties dialog(s).

11.3 Installing the Client for Microsoft Networks component on Windows 2000 or higher

The Client for Microsoft Networks is an essential networking software component for the Microsoft Windows family of operating systems. A Windows computer must run the Client for Microsoft Networks to remotely access files, printers and other shared network resources. These step-by-step instructions explain how to verify that the client is present and, if not, how to install it.

1. Navigate to **Control Panel** and access **Networking options** or **Network or Sharing Centre**.

2. Right click on the **Local Area Connection** item and select **Properties**.

NOTE: If the computer runs any older version of Windows, like Windows 95 or Windows 98, locate and right click on **Network Neighborhood**, then choose **Properties**. Alternatively, navigate to **Control Panel** and open the **Network** item.

🚣 Local Area Connection Properties 🛛 📍 🗙
General Authentication Advanced
Connect using:
Intel 21140-Based PCI Fast Ethernet
This connection uses the following items:
 Client for Microsoft Networks Network Load Balancing File and Printer Sharing for Microsoft Networks Tornet Protocol (TCP/IP)
I <u>n</u> stall <u>U</u> ninstall <u>Properties</u>
Allows your computer to access resources on a Microsoft network.
 Show icon in notification area when connected Notify me when this connection has limited or no connectivity
OK Cancel

Screenshot 113 - Local Area Connection Properties dialog

3. From the **General** tab, select the checkbox next to **Client for Microsoft Networks** and click on **Install...** to begin the installation process.

NOTE 1: If **Client for Microsoft Windows** checkbox is already selected, then the component is already installed.

NOTE 2: If the network is currently active, you may not see any checkboxes in the window. In this case, click the **Properties** button one more time to reach the full **General** tab.

NOTE 3: If the computer runs any older version of Windows, view the **Configuration** tab and verify if **Client for Microsoft Windows** is present in the displayed list. If not, install the component by clicking on the **Add...** button.

4. From the new dialog on display, select **Client** and click on **Add...** to continue.

5. From the list of manufacturers at the right of the active window choose **Microsoft**. Then, choose **Client for Microsoft Windows** from the list of network clients on the right side of the window. Click **OK** button to continue.

6. To finalize the installation, click on the **OK** button and reboot the computer. After the computer has restarted, **Client for Microsoft Windows** will be automatically installed.

11.4 Configuring Password Policy Settings in an Active Directory-Based Domain

NOTE: You must be logged on as a member of the Domain Admin group.

To implement password policies on network computers belonging to an Active Directory domain:

1. Navigate to the **Control Panel** and open the **Administrative Tools**.

📁 Active Directory Users and Compute	ers		
실 Eile Action <u>V</u> iew <u>W</u> indow <u>H</u> elp			_ B ×
←→ 📧 🗗 🔂 😫 🦉	🎽 🖓 🍝 🗑 👘		
Active Directory Users and Computers [v	2 Active Directory Us	ers and Computers [v	/2k3Exch1.ve
En Saved Queries	Name	Туре	Description
Delegate Control	Queries	Dennis	Folder to store
Find	\$31.10	Domain	
Connect to Domain	otroller		
Raise Domain Function	al Level		
Operations <u>M</u> asters			
New	•		
All Tas <u>k</u> s	•		
New <u>W</u> indow from Here	•		
P <u>r</u> operties			
Help			
			Þ
Opens property sheet for the current selection	n. 🛛		

Screenshot 114 - Active Directory Users and Computers configuration dialog

2. Open **Active Directory Users and Computers**. Right click on the root container of the domain and select **Properties**.

vexch2k31.local Properties		? ×
General Managed By Group Policy		
To improve Group Policy management, upgrade to the Group Policy Management Console (GPMC).		
Current Group Policy Object Links fo	r vexch2k31	
Group Policy Object Links	No Override	Disabled
S Domain Policy Company Policy		
Group Policy Objects higher in the list have the h	ighest priority.	
This list obtained from: v2k3Exch1.vexch2k31.lo	cal	
<u>New</u> <u>Add</u> <u>Edit</u>		<u>Шр</u>
Options Delete Properties		Do <u>w</u> n
□ <u>B</u> lock Policy inheritance		
Close	Cancel	Apply

Screenshot 115 - Configuring a new Group Policy Object (GPO)

3. In the properties dialog, click on the **Group Policy** tab. Then click on **New** to create a new Group Policy Object (GPO) in the root container.

4. Specify the name of the new group policy (for example, 'Domain Policy') and then click on **Close**.

NOTE: Microsoft recommends that you create a new Group Policy Object rather than editing the default policy (called 'Default Domain Policy'). This makes it much easier to recover from serious problems with security settings. If the new security settings create problems, you can temporarily disable the new Group Policy Object until you isolate the settings that caused the problems.

5. Right click on the root container of your domain and select **Properties**. This will bring up again the Domain Properties dialog.

6. Click on the **Group Policy** tab, and select the new Group Policy Object Link that you have just created (example, 'Domain Policy').

7. Click on **Up** to move the new GPO to the top of the list, and then click on **Edit** to open the **Group Policy Object Editor**.

Screenshot 116 - The Group Policy Object Editor

8. Expand the **Computer Configuration** node and navigate to **Windows Settings** ► **Security Settings** ► **Account Policies** ► **Password Policy** folder.

Enforce password history Properties	
Security Policy Setting	
Enforce password history	
Define this policy setting	
Keep password history for: 24	
OK Cancel Ap	oly

Screenshot 117 - Configure the GPO password history

9. From the right pane, double-click on the **Enforce password history** policy. Then select the **Define this policy setting** option, and set the **Keep password history** value to '24'.

10. Click **OK** button to close the dialog.

Maximum password age Properties	? ×
Security Policy Setting	
Maximum password age	
Define this policy setting	
Password will expire in:	
42 days	
,	
OK Cancel	Apply

Screenshot 118 - Configuring GPO password expiry

11. From the right pane, double-click on the **Maximum password age** policy. Select the **Define this policy setting** option and set the **Password will expire in** value to 42 days.

12. Click on **OK** to close the properties dialog.

Minimum password age Properties	? ×
Security Policy Setting	
Minimum password age	
Define this policy setting	
Password can be changed after:	
OK Cancel A	3bblà

Screenshot 119 - Configuring the minimum password age

13. From the right pane, double-click on the **Minimum password age** policy. Then select the **Define this policy setting** option and set the **Password can be changed after:** value to '2'.

14. Click on the **OK** button to close the dialog.

Minimum password length Properties	? ×
Security Policy Setting	
Minimum password length	
Define this policy setting	
Password must be at least:	
OK Cancel A	pply

Screenshot 120 - Configuring the minimum number of characters in a password

15. From the right pane, double-click on the **Minimum password length** policy. Select the **Define this policy setting** option and set the value of the **Password must be at least:** entry field to '8'.

16. Click on the **OK** button to close the dialog.

Password must meet complexity requirements Properties 👘 😤 🗙
Security Policy Setting
Password must meet complexity requirements
Define this policy setting:
• Enabled
○ Di <u>s</u> abled
OK Cancel Apply

Screenshot 121 - Enforcing password complexity

17. From the right pane, double-click on the **Password must meet** complexity requirements policy. Then enable the **Define this policy** setting in the template option, and select **Enabled**.

18. Click on the **OK** button to close the dialog.

19. At this stage the password policy settings of the new GPO have been configured. Close all dialogs and exit the **Active Directory Users and Computers** configuration dialog.

11.5 Viewing the Password Policy Settings of an Active Directory-Based Domain

NOTE: You must be logged on as a member of the Domain Admin group.

Use the following procedure to verify that the appropriate password policy settings are applied and effective in the Domain Policy GPO. Verifying the settings and their operation ensures that the correct password policies will be applied to all users in the domain.

To verify password policy settings for an Active Directory domain

1. Navigate to the Control Panel and open the Administrative Tools.

2. Open **Active Directory Users and Computers**. Right click on the root container of the domain and select **Properties**.

3. Click on the **Group Policy** tab. Select the GPO to be checked (for example, Domain Policy GPO) and click on **Edit** to open the **Group Policy Object Editor**.

4. Expand the **Computer Configuration** node and navigate to **Windows Settings** ► **Security Settings** ► **Account Policies** ► **Password Policy** folder.



Screenshot 122 - Verifying the GPO settings

The password policy configuration settings, are displayed in the right pane of the GPO editor. The password policy of your GPO shall be set as follows:

- Enforce password history: 24 passwords remembered
- Maximum password age: 42 days
- Minimum password age: 2 days

- Minimum password length: 8 characters
- Password must meet complexity requirements: Enabled

12. GFI LANguard certifications

12.1 Introduction

GFI LANguard is OVAL and CVE certified.

12.2 About OVAL

Open Vulnerability and Assessment Language (OVAL[™]) is an international, information security, community standard to promote open and publicly available security content, and to standardize the transfer of this information across the entire spectrum of security tools and services. OVAL includes a language used to encode system details, and an assortment of content repositories held throughout the OVAL community. The language standardizes the three main steps of the assessment process:

- Representing configuration information of systems for testing
- Analyzing the system for the presence of the specified machine state (vulnerability, configuration, patch state, etc.)
- Reporting the results of this assessment.

The repositories are collections of publicly available and open content that utilize the language.

The OVAL community has developed three XML schemas to serve as the framework and vocabulary of the OVAL Language. These schemas correspond to the three steps of the assessment process:

- An OVAL System Characteristics schema for representing system information
- An OVAL Definition schema for expressing a specific machine state
- An OVAL Results schema for reporting the results of an assessment

Content written in OVAL Language is located in one of .the many repositories found within the community. One such repository, known as the OVAL Repository, is hosted by MITRE Corporation. It is the central meeting place for the OVAL Community to discuss, analyze, store, and disseminate OVAL Definitions. Each definition in the OVAL Repository determines whether a specified software vulnerability, configuration issue, program, or patch is present on a system.

The information security community contributes to the development of OVAL by participating in the creation of the OVAL Language on the OVAL Developers Forum and by writing definitions for the OVAL Repository through the OVAL Community Forum. An OVAL Board consisting of representatives from a broad spectrum of industry, academia, and government organizations from around the world oversees and approves the OVAL Language and monitors the posting of the definitions hosted on the OVAL Web site. This means that the

OVAL, which is funded by US-CERT at the U.S. Department of Homeland Security for the benefit of the community, reflects the insights and combined expertise of the broadest possible collection of security and system administration professionals worldwide.

12.2.1 GFI LANguard 9.0 OVAL Support

GFI LANguard 9.0 supports all checks defined in the XML file issued by OVAL, with the exception of HP-UX checks.

GFI LANguard 9.0 does not support HP-UX based machines and therefore it is beyond the scope of this product to include these checks within its check definition database.

12.2.2 About OVAL Compatibility

OVAL Compatibility is a program established to develop consistency within the security community regarding the use and implementation of OVAL. The main goal of the compatibility program is to create a set of guidelines that will help enforce a standard implementation. An offshoot of this is that users are able to distinguish between, and have confidence in, compatible products knowing that the implementation of OVAL coincides with the standard set forth.

For a product or service to gain official OVAL Compatibility, it must adhere to the **Requirements and Recommendations for OVAL Compatibility** and complete the formal OVAL Compatibility Process.

OVAL Compatibility means that GFI LANguard incorporates OVAL in a pre-defined, standard way and uses OVAL for communicating details of vulnerabilities, patches, security configuration settings, and other machine states.

12.2.3 Submitting OVAL listing error reports

Any issues with the GFI LANguard or the listing of the OVAL checks included with GFI LANguard should be reported to GFI through its official support lines. Refer to the <u>Troubleshooting</u> section within this manual for more information regarding email, phone or web forum support channels.

GFI Software Ltd will endeavor to look into any issues reported and if any inconsistency or error is ascertained, it will issue updates to fix such issues. Vulnerability check updates are usually released on monthly basis.

12.3 About CVE

CVE (Common Vulnerabilities and Exposures) is a list of standardized names for vulnerabilities and other information security exposures. Its aim is to standardize the names for all publicly known vulnerabilities and security exposures.

CVE is a dictionary which aim is to facilitate data distribution across separate vulnerability databases and security tools. CVE makes searching for information in other databases easier and should not be considered as a vulnerability database by itself.

CVE is a maintained through a community-wide collaborative effort known as the CVE Editorial Board. The Editorial Board includes representatives from numerous security-related organizations such as security tool vendors, academic institutions, and governments as well as other prominent security experts. The MITRE Corporation maintains CVE and moderates editorial board discussions.

12.3.1 About CVE Compatibility

"CVE-compatible" means that a tool, Web site, database, or service uses CVE names in a way that allows it to cross-link with other repositories that use CVE names. CVE-compatible products and services must meet the four requirements:

- CVE Searchable: A user must be able to search for vulnerabilities and related information using the CVE name.
- CVE Output: Information provided must include the related CVE name(s).
- Mapping: The repository owner must provide a mapping relative to a specific version of CVE, and must make a good faith effort to ensure accuracy of that mapping.
- Documentation: The organization's standard documentation must include a description of CVE, CVE compatibility, and the details of how its customers can use the CVE-related functionality of its product or service.

NOTE: For an in-depth understanding of CVE compatibility refer to the complete list of CVE requirements available at:

http://cve.mitre.org/compatible/requirements.html.

12.3.2 About CVE and CAN

CVE names (also called "CVE numbers," "CVE-IDs," and "CVEs") are unique, common identifiers for publicly known information security vulnerabilities. CVE names have "entry" or "candidate" status. Entry status indicates that the CVE name has been accepted to the CVE List while candidate status (also called "candidates," "candidate numbers," or "CANs") indicates that the name is under review for inclusion in the list.

Each CVE name includes the following:

- CVE identifier number (i.e. "CVE-1999-0067").
- Indication of "entry" or "candidate" status.
- Brief description of the security vulnerability or exposure.
- Any pertinent references (i.e., vulnerability reports and advisories or OVAL-ID).

For an in-depth understanding of CVE names and CANs, refer to: <u>http://cve.mitre.org/cve/identifiers/index.html</u>

12.3.3 Searching for CVE entries in GFI LANguard

CVE entries can be searched from the Scanning profiles node within the Configuration tab.

Find <u>b</u> ulletin:		Find	Find next
Search by bulletin nam	ne (e.g. MS02-017) or QNumber	(e.g. Q311967).	

Screenshot 123 – Searching for CVE information

To search for a particular CVE bulletin:

1. Specify the bulletin name (for example, CVE-2005-2126) in the search tool entry box included at the bottom of the right pane.

2. Click on Find to start searching for your entry.

12.3.4 Obtaining CVE names

CVE entry names can be obtained through the GFI LANguard user interface from within the Scanning profiles node within the Configuration tab. By default, the CVE ID is displayed for all the vulnerabilities that have a CVE ID.

12.3.5 Importing and exporting CVE Data

CVE data can be exported through the impex command line tool. For more information on the impex command line tool refer to the <u>Using</u> <u>'impex.exe' – the command line import and export tool</u> section within this manual

13. Troubleshooting

13.1 Introduction

The troubleshooting chapter explains how you should go about resolving any software issues that you might encounter. It explains the use of the GFI LANguard troubleshooting wizard. The main sources of information available to users are:

- The manual most issues can be solved by reading this manual.
- The GFI Knowledge Base <u>http://kbase.gfi.com</u>
- The GFI technical support site <u>http://support.gfi.com</u>
- The GFI Web forum http://forums.gfi.com/
- Contacting the GFI technical support team by email at <u>support@gfi.com</u>
- Contacting the GFI technical support team using our live support service at <u>http://support.gfi.com/livesupport.asp</u>
- Contacting our technical support team by telephone.

13.2 The Troubleshooting wizard

The GFI LANguard troubleshooting wizard is a tool designed to assist you when encountering technical issues related to GFI LANguard's use.

To use the GFI LANguard troubleshooting wizard:

1. Launch the troubleshooting wizard from the **Start** ► **Programs** ► **GFI LANguard 9.0** ► **GFI LANguard Troubleshooter**.

2. Click **Next** in the introduction page.

Troubleshooter Wizard - Welcome
Information Details Please select the information to gather.
The troubleshooter should:
Automatically detect and fix known issues (Recommended)
Gather only application information and logs. Note: Use this option when the problem is already located and only support files are needed.
< Back Next > Cancel

Screenshot 124 - Troubleshooter wizard - Information details

- 3. In the Information details page select one of the following options:
- Automatically detect and fix known issues Use this option to automatically have the troubleshooting wizard detect and fix issues, which already have been notified and fixed by GFI support.

NOTE: This is the recommended option.

- **Gather only application information and logs** Use this option to gather logs to send to GFI support.
- 4. Click **Next** to continue.

Troubleshooter Wizard - Gathering Information	X
Known Issues The troubleshooter will check you installation for common issues.	F
Details:	
Checks if the latest build is installed. Checks if the user LNSS_MONITOR_USR exists on this computer. Checks if the user LNSS_MONITOR_USR has administrator privileges. Checks if the Attendant Service user has administrator privileges. Checks if the LNSSCommunicator COM object can be instantiated. Checks if the RepServer COM object can be instantiated. Checks if the CRMI COM object can be instantiated. Checks if the Attendant Service is installed on this computer. Checks if the Attendant Service is running on this computer. Checks if the Attendant Service is running on this computer. Checks if the Attendant Service is running on this computer.	
Finished all checks.	
< Back Next >	Cancel

Screenshot 125 - Troubleshooter wizard - Gathering information about known issues

4. The troubleshooter wizard will retrieve all the information required to solve common issues. Click **Next** to continue.

Troubleshooter Wizard - Known Issues		X
Known Issues Found Fixing issues.		GF
Done.		
Fixed all of the issues which can be automa Does this solve the problem(s) you were ha	tically solved. ving?	
⊘ Yes Image: No		
	< Back Next >	Cancel

Screenshot 126 - Troubleshooter fixed known issues

5. The troubleshooter will fix any known issues that it encounters. Select **Yes** if your problem was fixed or **No** if your problem is not solved to search the GFI Knowledge base for information.

13.3 Knowledge Base

GFI maintains a Knowledge Base, which includes answers to the most common problems. The Knowledge Base always has the most up-to-date listing of technical support questions and patches. To access the Knowledge Base, visit <u>http://kbase.gfi.com/</u>.

13.4 Web Forum

User to user technical support is available via the web forum. The forum can be found at: <u>http://forums.gfi.com/</u>.

13.5 Request technical support

If you have referred to this manual and our Knowledge Base articles, and you still cannot solve issues with the software, contact the GFI Technical Support team by filling in an online support request form or by phone.

- **Online:** Fill out the support request form on: http://support.gfi.com/supportrequestform.asp. Follow the instructions on the page to submit your support request.
- Phone: To obtain the correct technical support phone number for your region visit: <u>http://www.gfi.com/company/contact.htm</u>. We will answer your query within 24 hours or less depending on your time zone.

NOTE: Before you contact our Technical Support team ensure that you have your Customer ID available. Your Customer ID is the online

account number that is assigned to you when you first register your license keys in our Customer Area at: <u>http://customers.gfi.com</u>.

13.6 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, visit:

http://www.gfi.com/pages/productmailing.htm

Index

A

Alerting Options, 126 Applications, 105, 109, 110, 111, 112 Attendant service, 1

С

command line, 125, 126, 127, 128 command line tools, 125 Computer Profiles, 65, 126, 127 Custom Patches, 120 custom scripts, 2 CVE, 150, 151, 152

D

database backend, 30, 31, 75, 76, 77, 80, 81 Database Maintenance Options, 75 DNS Lookup, 115, 116, 117

Е

Enumerate Computers, 115, 119, 120 Enumerate Users, 115, 121

G

Group Policy Object, 143, 144, 147

I

installation, 123, 126, 127 Intrusion Detection Software, 5

Μ

Microsoft Access, 5, 75, 76, 80 Microsoft SQL Server Audit, 115

Ν

NetBIOS, 139, 140 network devices, 107 network tools, 115

0

OS data, 104 OVAL, 1, 95, 133, 135, 149, 150

Ρ

Patch Autodownload, 71, 73, 74 patch deployment, 1, 45, 48, 50, 127, 128 program updates, 84

R

Registry, 20 Remote Processes, 28 results comparison, 39

S

scan categories, 28 scan results, 1, 30, 31, 33, 36, 39, 76, 77, 78, 94, 125, 126, 133, 134 Scanning Profiles, 87, 93, 100, 102, 103, 113, 125 scanning threads, 113 **Script Debugger**, 1, 2, 131, 132 script editor, 131 Security Audit Policy, 26 services, 20, 77, 127 SNMP Audit, 115, 122 SNMP Walk, 115, 123 SSH, 134, 135 SSH Private Key, 65, 134 Status Monitor, 59, 60

т

target computers. See TCP Ports, 102, 103 Trace Route, 117

U

UNIX, 5, 134 USB devices, 105, 106, 108 Users, 27–28, 27–28, 131 users and groups, 27

V

Vulnerabilities, 19, 20, 94, 98, 132, 135

Whois, 115, 118