GFI LANguard 9.0 ReportPack

Manual

By GFI Software Ltd.

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

Version 9.0 – Last updated November 18, 2008

Contents

Introduction

About GFI ReportCenter

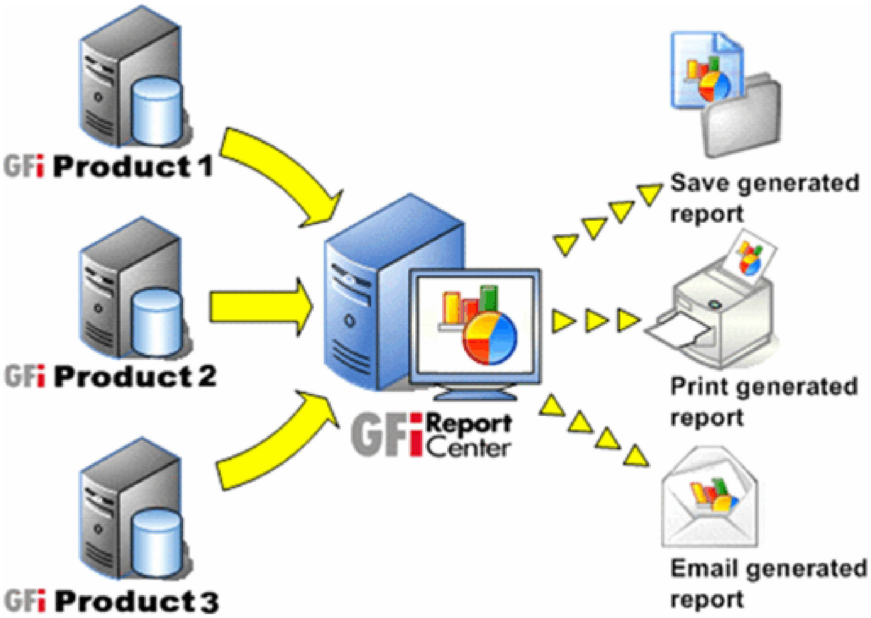


Figure 1 - Centralized reporting framework

GFI ReportCenter is a centralized reporting framework that allows you to generate various reports using data collected by different GFI products. GFI releases specialized reports for each of its products, referred to as a ReportPack; for example, the GFI LANguard ReportPack. A ReportPack can be purchased as an add-on to the GFI product.

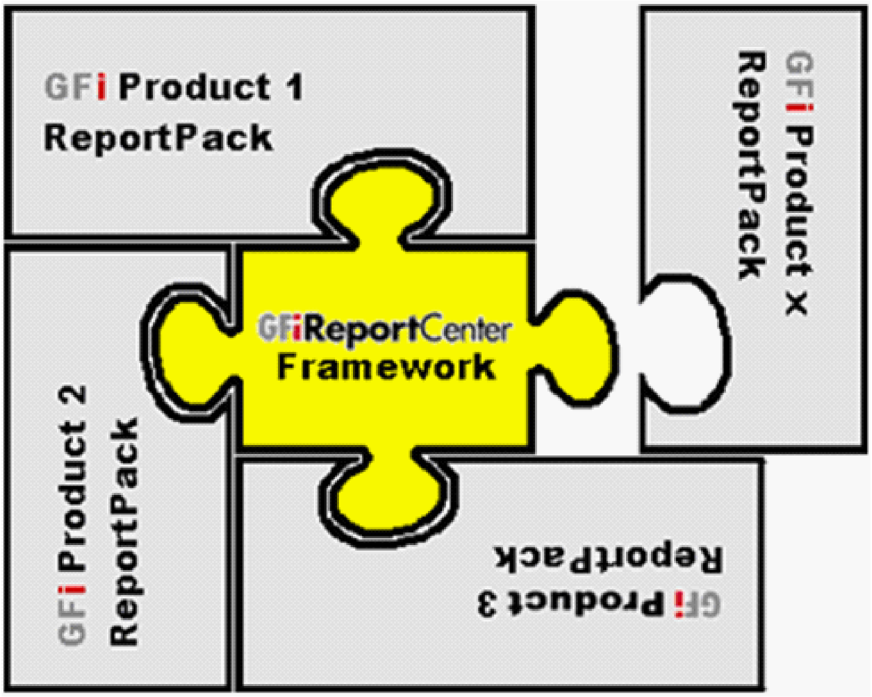


Figure 2 – Several ReportPacks plugged into the GFI ReportCenter framework

A ReportPack plugs into the GFI ReportCenter framework; allowing you to generate, analyze, export and print the information generated through these reports.

About the GFI LANguard 9.0 ReportPack

The GFI LANguard ReportPack is a full-fledged reporting companion to GFI LANguard (GFI LANguard). It allows you to generate graphical IT-level, technical and management reports based on the network security audits carried out by GFI LANguard

From trend reports for management (ROI) to daily drill-down reports for technical staff; the GFI LANguard ReportPack provides you with the easy-to-view information required, to fully identify any vulnerability on your corporate network.

The GFI LANguard ReportPack allows for the creation of various graphical and text based reports related to:

- Vulnerability assessment reports
- Network and software auditing reports
- Results comparison reports.

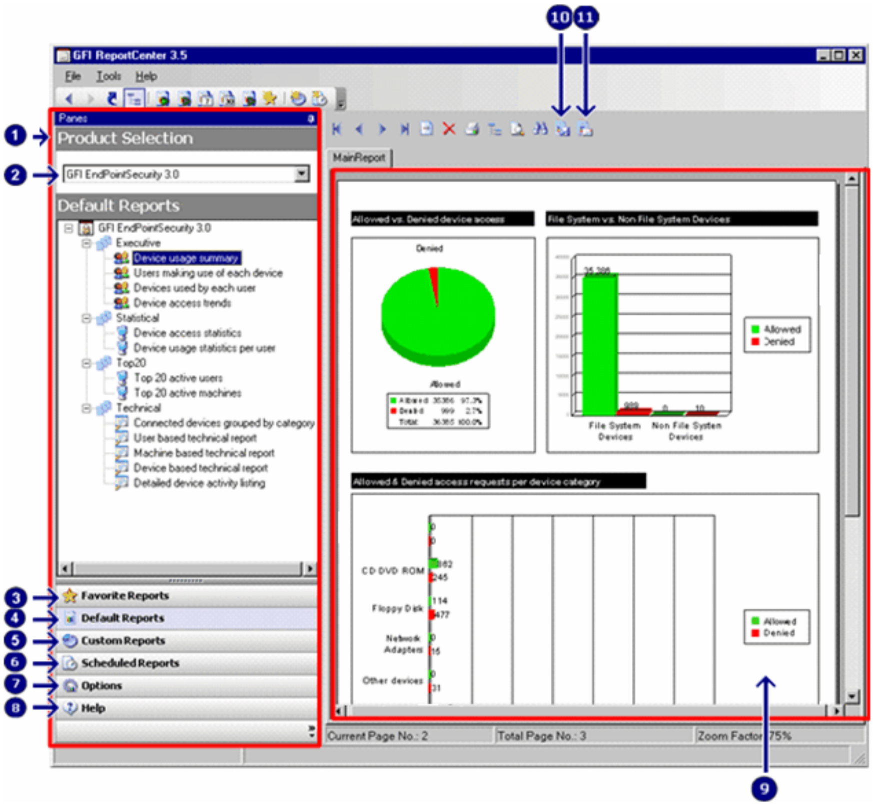
Components of the GFI LANguard 9.0 ReportPack

When you install the GFI LANguard 9.0 ReportPack, the following components are installed:

- GFI ReportCenter framework
- GFI LANguard 9.0 default reports
- Report scheduling service.

GFI ReportCenter framework

The GFI ReportCenter framework is the management console through which you can generate the specialized product reports which are shipped with a product ReportPack. The GFI ReportCenter framework offers a common application interface through which you can navigate, generate, customize and schedule reports.



Screenshot 1 – The GFI ReportCenter management console

The GFI ReportCenter management console is organized as follows:

1	**Navigation Pane** – Use this pane to access the navigation buttons/configuration options provided with GFI ReportCenter.
2	**Product Selection drop-down list** – Use this drop-down list to select the GFI product for which to generate reports. The Product Selection drop-down list displays all the products for which you have installed a ReportPack.
3	**Favorite Reports** – Use this navigation button to access your favorite/most used reports. For more information on how to add reports to this list refer to the 'Adding default reports to the list of favorite reports' and 'Adding custom reports to the list of favorite reports' sections in this manual.
4	**Default Reports** – Use this navigation button to access the default list of reports which can be generated for the selected product. For more information on default reports refer to the 'GFI LANguard default reports' section in this manual.
5	**Custom Reports** – Use this navigation button to access the list of customized reports which can be generated for the selected product. For more information on how to create custom reports

	refer to the ‘Custom reports’ chapter in this manual.
❻	**Scheduled Reports** – Use this navigation button to access the list of scheduled reports for automatic generation and distribution. For more information on how to create scheduled reports refer to the ‘Scheduling reports’ chapter in this manual.
❼	**Options** – Use this navigation button to access the general configuration settings for the GFI product selected in the Product Selection drop down list.
❽	**Help** – Use this navigation button to show this Quick Reference Guide in the Report Pane of the GFI ReportCenter management console.
❾	**Report Pane** - Use this multi-functional pane to: • View and analyze generated reports • Maintain the scheduled reports list • Explore samples and descriptions of default reports.
❿	**Export** – Use this button to export generated reports to various formats including HTML, Adobe Acrobat (PDF), Excel (XLS), Word (DOC), and Rich Text Format (RTF).
⓫	**Send email** – Use this button to instantly distribute the last generated report via email.

GFI LANguard 9.0 default reports

The GFI LANguard 9.0 default reports are a collection of specialized pre-configured reports which plug into the GFI ReportCenter framework. These reports present the results of network security scans performed by GFI LANguard and allow for the generation of both graphical and tabular IT-Level, technical and management reports. Default reports can also serve as the base template for the creation of customized reports which fit specific network-reporting requirements.

Report scheduling service

The report scheduling service controls the scheduling and automatic distribution of reports by email. Reports generated by this service can also be saved to a specific hard disk location in a variety of formats which include DOC, PDF, RTF and HTML.

Key features

Centralized reporting

GFI ReportCenter is a one-stop, centralized reporting framework which enables the generation and customization of graphical and tabular reports for a wide array of GFI products.

Wizard assisted configuration

Wizards are provided to assist you in the configuration, scheduling and customization of reports.

Report scheduling

With GFI ReportCenter you can schedule reports to be generated on a pre-defined schedule as well as at specified intervals. For example, you can schedule lengthy reports to be generated after office hours. This allows you to maximize the availability of your system resources during working hours and avoid any possible disruptions to workflow.

Distribution of reports via email

GFI ReportCenter allows you to automatically distribute generated reports via email. In scheduled reports, this can be achieved automatically after the successful generation of a scheduled report.

Report export to various formats

By default, GFI ReportCenter allows you to export reports to various formats. Supported formats include HTML, PDF, XLS, DOC and RTF. When scheduling reports, you can optionally configure the preferred report output format. Different scheduled reports can also be configured to output generated reports to different file formats.

Default reports

The GFI LANguard ReportPack ships with a default set of graphical and tabular reports. These reports can be generated without any further configuration effort immediately after the installation. The default reports in this ReportPack are organized into four different report-type categories:

- Vulnerability assessment reports
- Network and software auditing reports
- Results comparison reports.

Report customization

The default reports that ship with every ReportPack can serve as the base template for the creation of customized reports. Report customization is achieved by building up custom data filters which will analyze the data source and filter the information that matches specific criteria. In this way, you create reports tailored to your reporting requirements.

Favorites

GFI ReportCenter allows you to create bookmarks to your most frequently used reports – both default and custom.

Printing

By default, all reports generated by GFI ReportCenter are printer friendly and can be printed through the windows printing services provided by the system where GFI ReportCenter is installed.

Installation

System requirements

Install the GFI LANguard ReportPack on a computer that meets the following requirements:

- Windows 2000 (SP4), XP (SP2/SP3), 2003, 2008, VISTA (SP1), operating system.
- Internet Explorer 5.1 or higher
- .NET Framework version 1.1.

NOTE 1: 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:

http://kbase.gfi.com/showarticle.asp?id=KBID003100

NOTE 2: The GFI LANguard ReportPack only allows you to generate reports for data contained in scan results databases which were created and maintained by GFI LANguard

Installation procedure

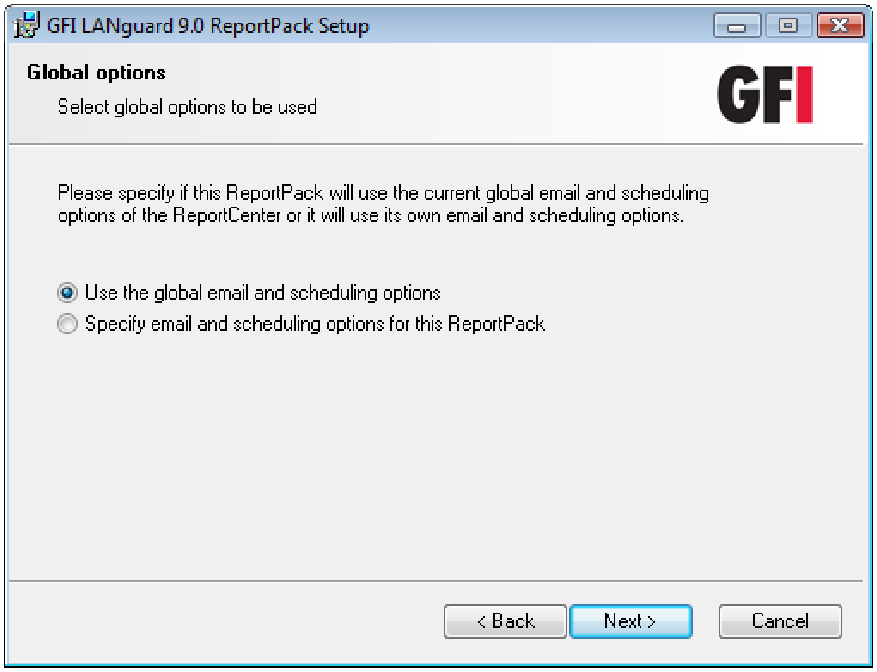
The GFI LANguard ReportPack includes an installation wizard which will assist you through the installation process. During the installation process this wizard will:

- Verify that you are running the latest version of the GFI ReportCenter framework; if you are installing the framework for the first time or the currently installed framework version is outdated, the installation wizard will automatically download the latest one for you.
- Automatically install all the required components distributed including the GFI ReportCenter framework, the GFI LANguard default reports and the Report Scheduling service.

To start the installation:

1. Double-click **languardnss9rp.exe**. As soon as the welcome dialog is displayed, click **Next** to start the installation.

2. If the current version of your GFI ReportCenter framework is not compatible with the GFI LANguard ReportPack, you will be prompted to download and install an updated version. To automatically achieve this, leave the dialog options as default and click on the **Next** button.



Global options

Select global options to be used

Please specify if this ReportPack will use the current global email and scheduling options of the ReportCenter or it will use its own email and scheduling options.

● Use the global email and scheduling options

○ Specify email and scheduling options for this ReportPack

Screenshot 2 – Select global email and scheduling options

3. Choose whether you want this ReportPack to use the global email and scheduling options of the ReportCenter or if it will have its own, customized, email and scheduling options.

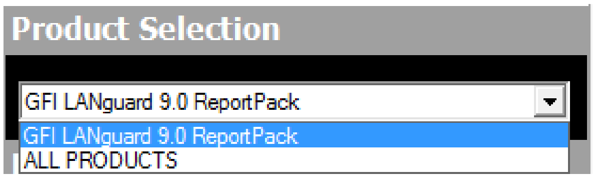
4. Specify the product installation path. The installation wizard is now ready to copy the required files and finalize the installation. To proceed click on the **Next** button.

Launching the GFI LANguard reports for GFI ReportCenter

Following the installation, launch the GFI LANguard Reports for GFI ReportCenter from **Start ▸ Programs ▸ GFI ReportCenter ▸ LANguard 9 ReportPack.**

Selecting a product

When more than one product ReportPack is installed, use the **Product Selection** drop down list to select the GFI product ReportPack to be used.



Screenshot 3 – Product Selection drop down list

For example, to run the reports provided in the GFI LANguard ReportPack:

1. Launch GFI ReportCenter from **Start ▸ Program Files ▸ GFI ReportCenter.**

2. Select ‘GFI LANguard 9.0’ from the **Product Selection** drop down list.

NOTE: Select the ‘ALL PRODUCTS’ option to display and navigate all the ReportPacks that are currently installed in GFI ReportCenter.

Getting started: Default reports

Introduction

After installing the GFI LANguard ReportPack, a number of specialized pre-configured reports can immediately be generated on the data stored in the database backend of GFI LANguard These default reports are organized into the following categories:

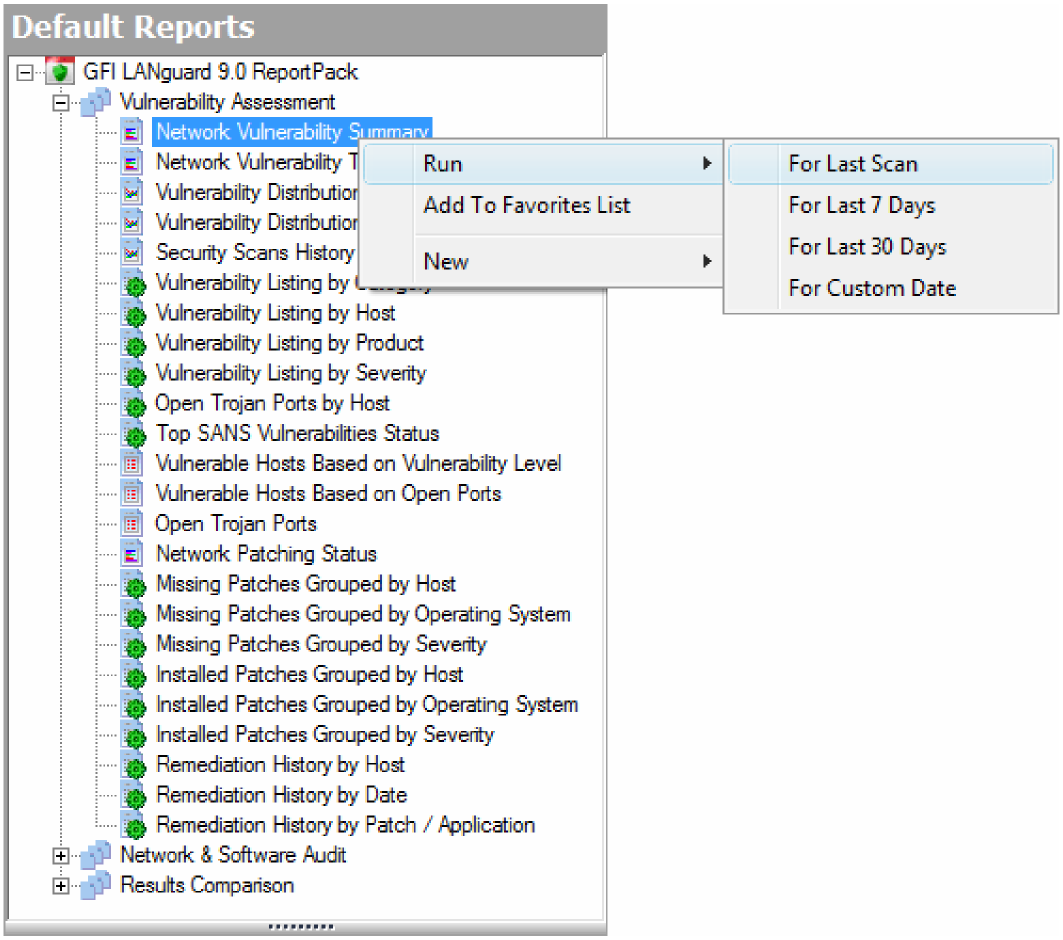
- **Vulnerabilities Assessment reports:** Use the reports in this category to identify vulnerabilities detected on the network as well information on network patches and service packs installed or awaiting deployment.. The reports include vulnerability details such as host machines, operating systems affected and severity.
- **Network and software audit reports:** Use the reports in this category to display detailed information on hardware and software present on the network. These reports help management in analyzing conformance with corporate security policy.
- **Results comparison reports:** Use the reports in this category to compare results of consecutive network scans that have a common profile and target, and of computer scans against a computer used as benchmark.

GFI LANguard default reports are accessed by clicking on the **Default Reports** navigation button provided in the navigation pane.

Generating a default report

To generate a default report:

1. Click on the **Default Reports** navigation button to bring up the list of default reports available.


Default Reports
GFI LANguard 9.0 ReportPack
Vulnerability Assessment
Network Vulnerability Summary
Network Vulnerability T
Vulnerability Distribution
Vulnerability Distribution
Security Scans History
Vulnerability Listing by Category
Vulnerability Listing by Host
Vulnerability Listing by Product
Vulnerability Listing by Severity
Open Trojan Ports by Host
Top SANS Vulnerabilities Status
Vulnerable Hosts Based on Vulnerability Level
Vulnerable Hosts Based on Open Ports
Open Trojan Ports
Network Patching Status
Missing Patches Grouped by Host
Missing Patches Grouped by Operating System
Missing Patches Grouped by Severity
Installed Patches Grouped by Host
Installed Patches Grouped by Operating System
Installed Patches Grouped by Severity
Remediation History by Host
Remediation History by Date
Remediation History by Patch / Application
Network & Software Audit
Results Comparison
Run
Add To Favorites List
New
For Last Scan
For Last 7 Days
For Last 30 Days
For Custom Date

Screenshot 4 – Selecting the data set

2. Right-click on the report to be generated, select **Run** and specify the scan date/time period that will be covered by the report.

Example 1: Generating a "Network Vulnerability Summary" report based on the last scan.

This example demonstrates how to generate a network vulnerability summary report based on the last network security scan carried out:

1. Click on the **Default Reports** navigation button to bring up the list of available reports.

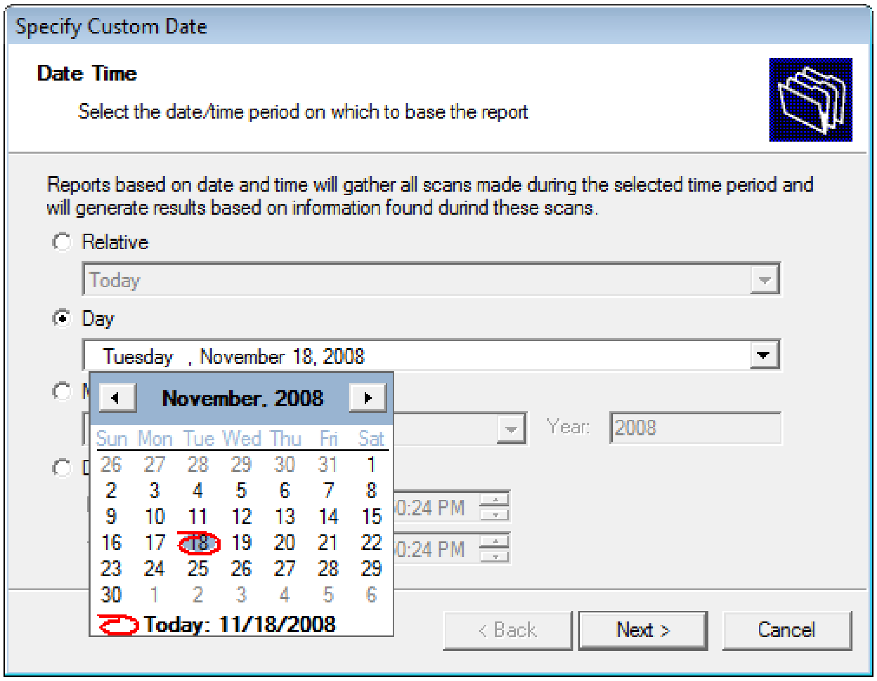
2. Right-click on **Network Vulnerability Summary** and select **Run ▸ For Last Scan**.

Example 2: Generating a "Network Vulnerability Summary" report based on scans made on a particular day.

This example demonstrates how to generate a network vulnerability summary report based on the scan performed on November 18, 2008.

1. Click on the **Default Reports** navigation button to bring up the list of available reports.

2. Right-click on Network Vulnerability Summary and select **Run ▸ For Custom Date**.



Specify Custom Date

Date Time

Select the date/time period on which to base the report

Reports based on date and time will gather all scans made during the selected time period and will generate results based on information found durind these scans.

○ Relative

Today

● Day

Tuesday , November 18, 2008

Year: 2008

November, 2008

Sun	Mon	Tue	Wed	Thu	Fri	Sat
26	27	28	29	30	31	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	1	2	3	4	5	6

Today: 11/18/2008

Screenshot 5 - Configuring custom date/time period

3. Select the ‘Day’ option and expand the provided drop down. This will bring up the date selection calendar.

4. Navigate to the required month (i.e. January) and select the required day (i.e. 14).

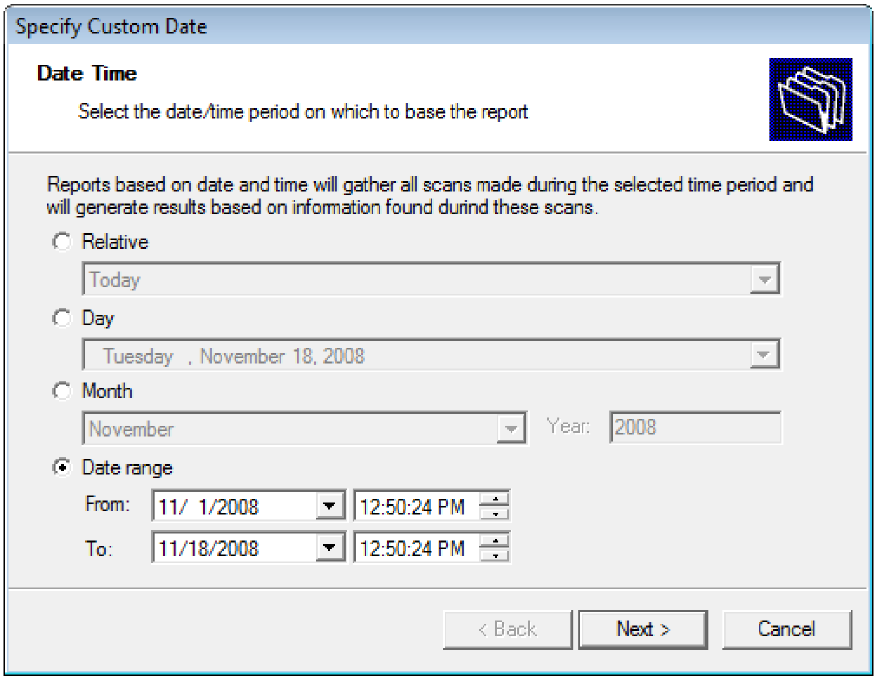
5. Click **Finish** to generate the report.

Example 3: Generating a “Network Vulnerability Summary” report based on data collected over a specific date/time period.

This example demonstrates how to generate a network vulnerability summary report based on network security scans carried out between November 1, 2008 and November 18, 2008.

1. Click on the **Default Reports** navigation button to bring up the list of available reports.

2. Right-click on **Network Vulnerability Summary** and select **Run ▸ For Custom Date**.



Specify Custom Date

Date Time

Select the date/time period on which to base the report

Reports based on date and time will gather all scans made during the selected time period and will generate results based on information found durind these scans.

○ Relative

Today

○ Day

Tuesday , November 18, 2008

○ Month

November Year: 2008

● Date range

From: 11/ 1/2008 12:50:24 PM

To: 11/18/2008 12:50:24 PM

Screenshot 6 - Configuring custom date/time period

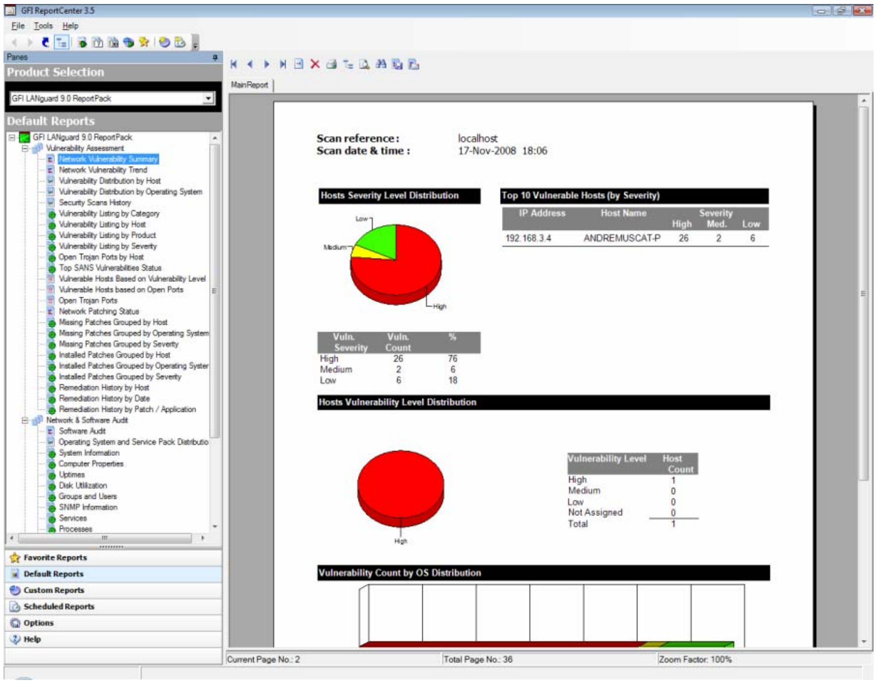
3. Select the ‘Date range’ option and specify the required parameters:

- ‘From’ – 01/14/2007 0:00:00.
- ‘To’ – 01/22/2007 23:59:59.

NOTE: Date and time format are based on the regional settings configured on your computer.

4. Click **Finish** to generate the report.

Analyzing the generated report


GFI ReportCenter 3.5
File
Tools
Help
Panes
Product Selection
GFI LANguard 9.0 ReportPack
Default Reports
GFI LANguard 9.0 ReportPack
Vulnerability Assessment
Network Vulnerability Summary
Network Vulnerability Trend
Vulnerability Distribution by Host
Vulnerability Distribution by Operating System
Security Scans History
Vulnerability Listing by Category
Vulnerability Listing by Host
Vulnerability Listing by Product
Vulnerability Listing by Severity
Open Trojan Ports by Host
Top SANS Vulnerabilities Status
Vulnerable Hosts Based on Vulnerability Level
Vulnerable Hosts based on Open Ports
Open Trojan Ports
Network Patching Status
Missing Patches Grouped by Host
Missing Patches Grouped by Operating System
Missing Patches Grouped by Severity
Installed Patches Grouped by Host
Installed Patches Grouped by Operating Syster
Installed Patches Grouped by Severity
Remediation History by Host
Remediation History by Date
Remediation History by Patch / Application
Network & Software Audit
Software Audit
Operating System and Service Pack Distributio
System Information
Computer Properties
Uptimes
Disk Utilization
Groups and Users
SNMP Information
Services
Processes
Favorite Reports
Default Reports
Custom Reports
Scheduled Reports
Options
Help
MainReport
Low
Medium
High
High

Scan reference : localhost
Scan date & time : 17-Nov-2008 18:06

Hosts Severity Level Distribution

Vuln. Severity	Vuln. Count	%
High	26	76
Medium	2	6
Low	6	18

Top 10 Vulnerable Hosts (by Severity)

IP Address	Host Name	Severity		
		High	Med.	Low
192.168.3.4	ANDREMUSCAT-P	26	2	6

Hosts Vulnerability Level Distribution

Vulnerability Level	Host Count
High	1
Medium	0
Low	0
Not Assigned	0
Total	1

Vulnerability Count by OS Distribution

Current Page No.: 2 Total Page No.: 36 Zoom Factor: 100%

Screenshot 7 – Generated reports are displayed in the right pane of the management console

Generated reports are shown in the right pane of the GFI ReportCenter. Use the toolbar at the top of the report pane to access common report related functions:

Report browsing options

Browse the generated report page by page.

Zoom in/Zoom out.

Search the report for particular text or characters.

Go directly to a specific page.

Breakdown the report into a group tree (e.g. by date/time).

Print report.

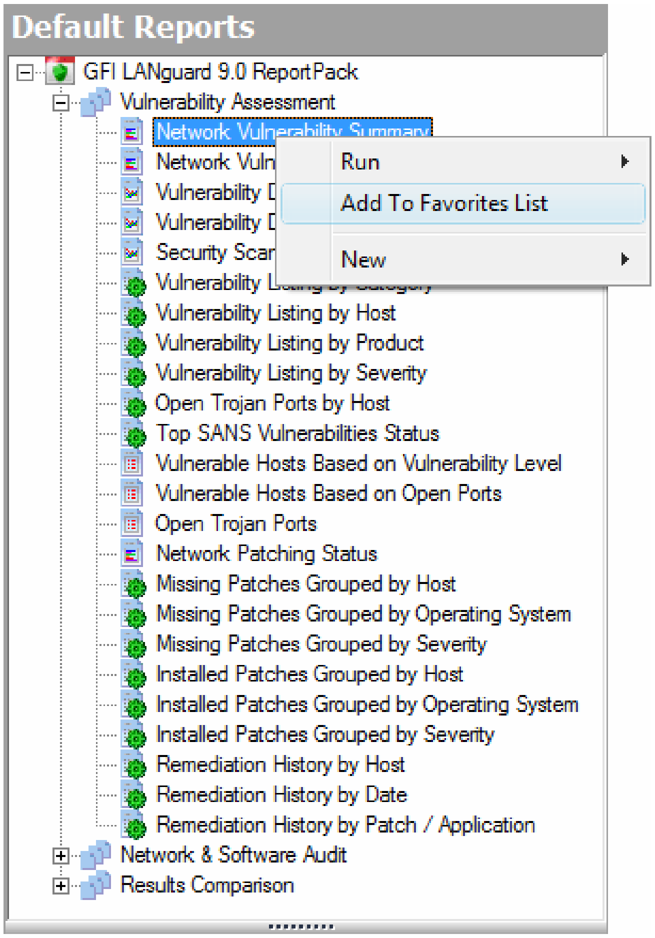
Report storage and distribution options

Export the generated report to a specific file format.

Distribute the generated report via email.

NOTE: For information on how to configure report storage and distribution options refer to the ‘Configuring Advanced Settings’ section in this manual.

Adding default reports to the list of favorite reports


Default Reports
GFI LANguard 9.0 ReportPack
Vulnerability Assessment
Network Vulnerability Summary
Network Vuln
Vulnerability D
Vulnerability D
Security Scan
Vulnerability Listing by Category
Vulnerability Listing by Host
Vulnerability Listing by Product
Vulnerability Listing by Severity
Open Trojan Ports by Host
Top SANS Vulnerabilities Status
Vulnerable Hosts Based on Vulnerability Level
Vulnerable Hosts Based on Open Ports
Open Trojan Ports
Network Patching Status
Missing Patches Grouped by Host
Missing Patches Grouped by Operating System
Missing Patches Grouped by Severity
Installed Patches Grouped by Host
Installed Patches Grouped by Operating System
Installed Patches Grouped by Severity
Remediation History by Host
Remediation History by Date
Remediation History by Patch / Application
Network & Software Audit
Results Comparison
Run
Add To Favorites List
New

Screenshot 8 – Favorite Reports navigation button

You can group and access frequently used reports through the **Favorite Reports** navigation button. To add a default report to the list of favorite reports:

1. Click on the **Default Reports** navigation button to bring up the list of available reports.

2. Right-click on the default report that you to be added to favorites and select **Add to favorites list**.

3. Click **Yes** to confirm.

Custom reports

Introduction

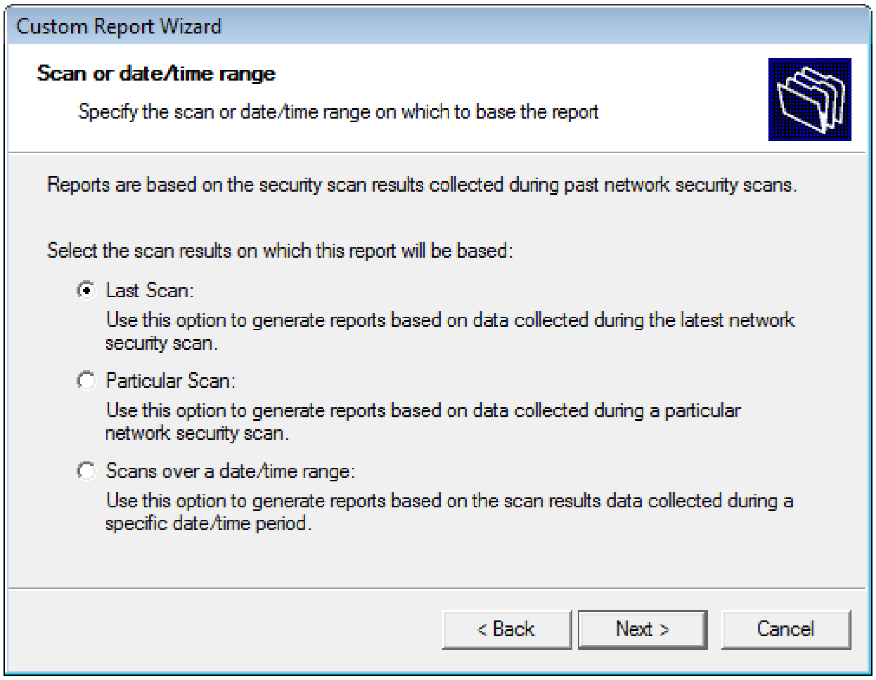
GFI ReportCenter allows you to create custom reports which are tailored to your reporting requirements. This is achieved by building up custom data filters which will analyze the data source and filter out the information that matches the specified criteria.

Creating a new custom report

To create a custom report:

1. Click on the **Default Reports** navigation button.

2. Right-click on the default report to be used as template and select **New ▶ Custom Report**. This will bring up the 'Custom Report Wizard'.



Custom Report Wizard

Scan or date/time range

Specify the scan or date/time range on which to base the report

Reports are based on the security scan results collected during past network security scans.

Select the scan results on which this report will be based:

● Last Scan:
Use this option to generate reports based on data collected during the latest network security scan.

○ Particular Scan:
Use this option to generate reports based on data collected during a particular network security scan.

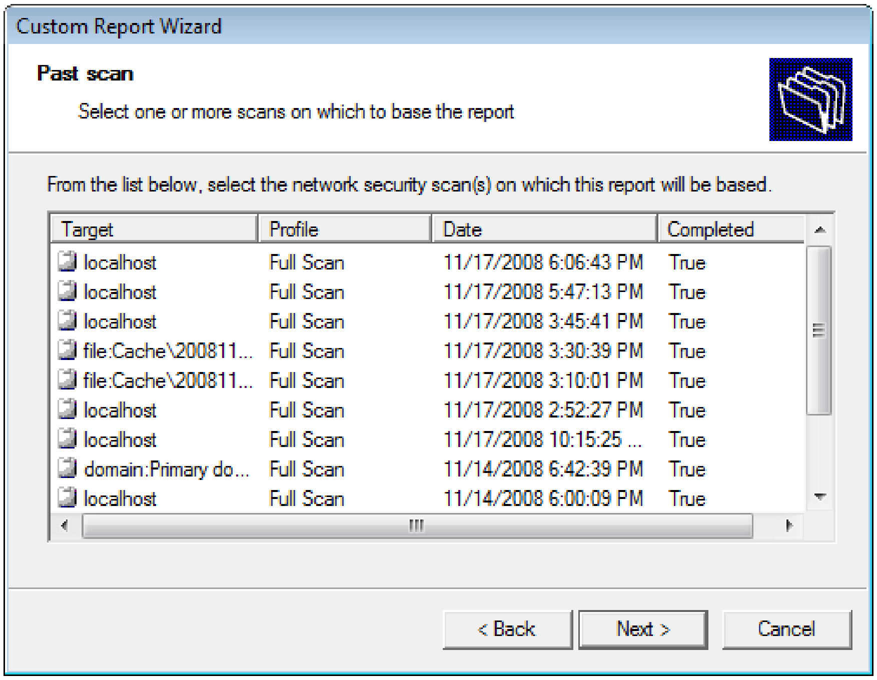
○ Scans over a date/time range:
Use this option to generate reports based on the scan results data collected during a specific date/time period.

Screenshot 9 - Selecting the scan data source to use

3. Specify the data source option that will be used to generate the custom report. This data source refers to scan results from:

- the last scan
- particular scan(s)
- scans carried out over a specific date/time period.

Click on **Next** to continue.



Past scan

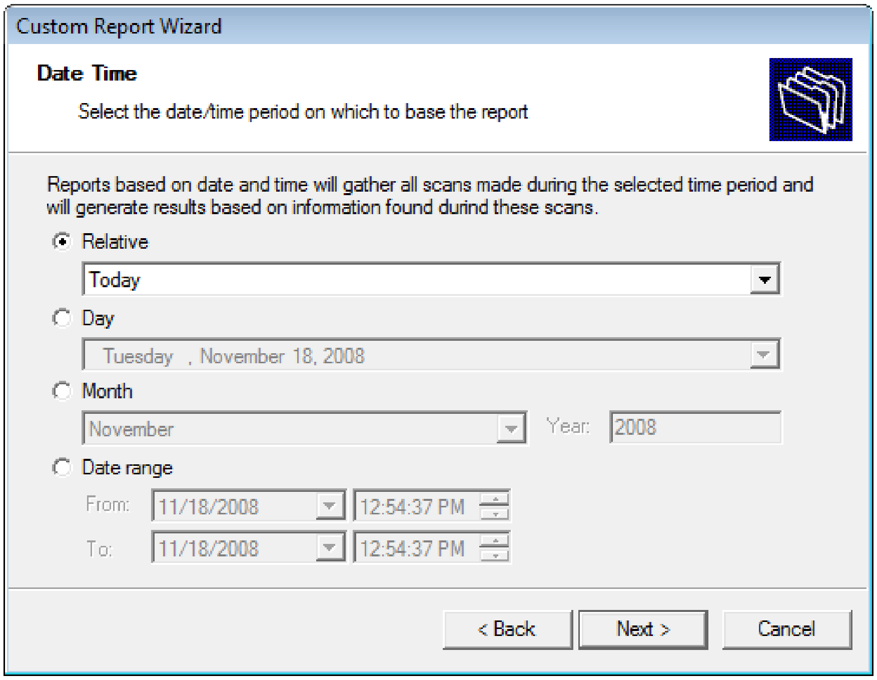
Select one or more scans on which to base the report

From the list below, select the network security scan(s) on which this report will be based.

Target	Profile	Date	Completed
localhost	Full Scan	11/17/2008 6:06:43 PM	True
localhost	Full Scan	11/17/2008 5:47:13 PM	True
localhost	Full Scan	11/17/2008 3:45:41 PM	True
file:Cache\200811...	Full Scan	11/17/2008 3:30:39 PM	True
file:Cache\200811...	Full Scan	11/17/2008 3:10:01 PM	True
localhost	Full Scan	11/17/2008 2:52:27 PM	True
localhost	Full Scan	11/17/2008 10:15:25 ...	True
domain:Primary do...	Full Scan	11/14/2008 6:42:39 PM	True
localhost	Full Scan	11/14/2008 6:00:09 PM	True

Screenshot 10 – Selecting the scan data source to use

4. If using the ‘Particular Scan’ option, select the required scan(s) from the list of network security scans carried out on the corporate network. Click on **Next** to continue.



Date Time

Select the date/time period on which to base the report

Reports based on date and time will gather all scans made during the selected time period and will generate results based on information found durind these scans.

● Relative

Today

○ Day

Tuesday , November 18, 2008

○ Month

November Year: 2008

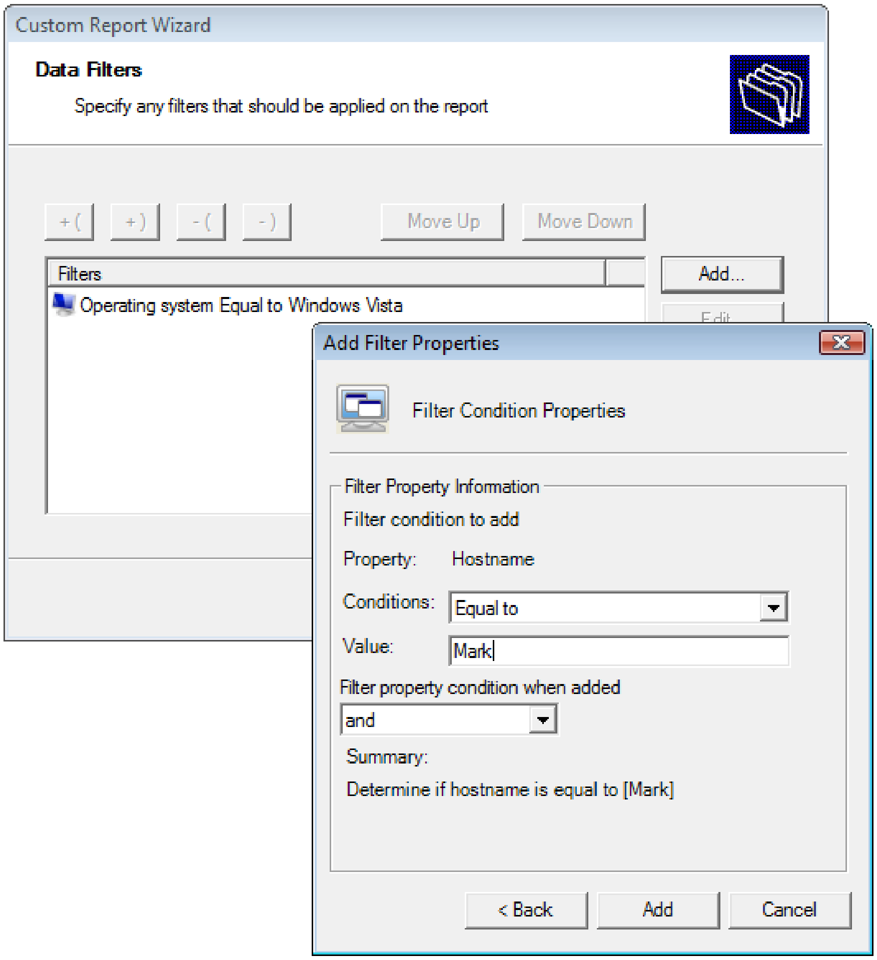
○ Date range

From: 11/18/2008 12:54:37 PM

To: 11/18/2008 12:54:37 PM

Screenshot 11 - Configuring custom date/time period

5. If using the ‘Scans over a date/time range’ option, select the date/time period from which network security scan results will be gathered. Click on **Next** to continue.



Operating system Equal to Windows Vista

Filter condition to add

Property: Hostname

Conditions: Equal to

Value: Mark

Filter property condition when added: and

Summary:

Determine if hostname is equal to [Mark]

Screenshot 12 – Specifying data filter conditions

6. Configure the data filter conditions that will be applied against the selected data source. Click on **Next** to continue.

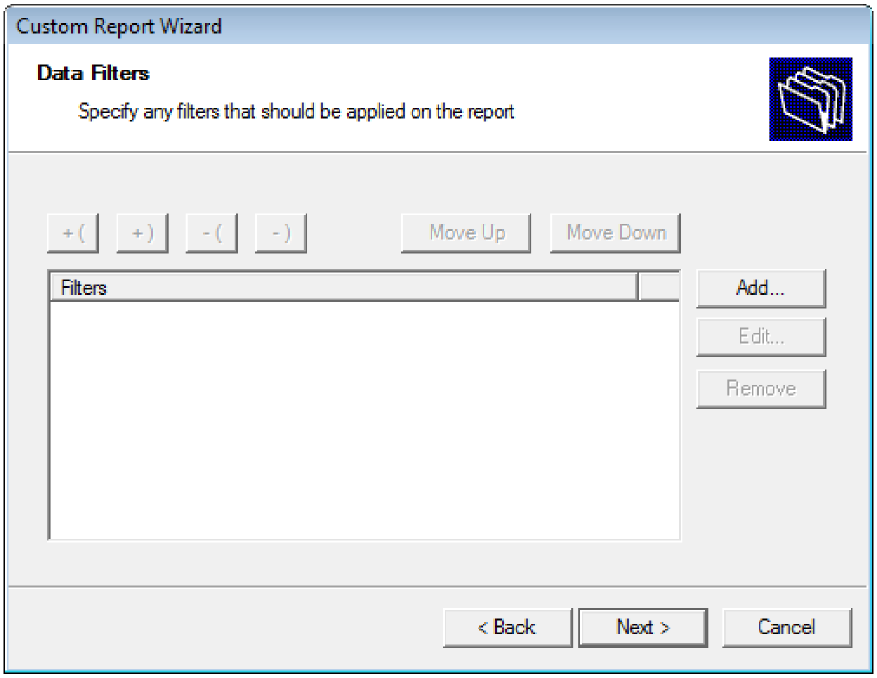
NOTE: For more information on how to configure filter conditions, refer to the section ‘Configuring data filter conditions’ in this manual.

7. Specify a name and description for the customized report. Click on **Next** to continue.

8. Click on **Finish** to finalize your configuration settings.

Configuring data filter conditions

Use data filter conditions to specify which network security scan data/results will be included in the report. Only scans which match the specified criteria will be processed and presented within the report.

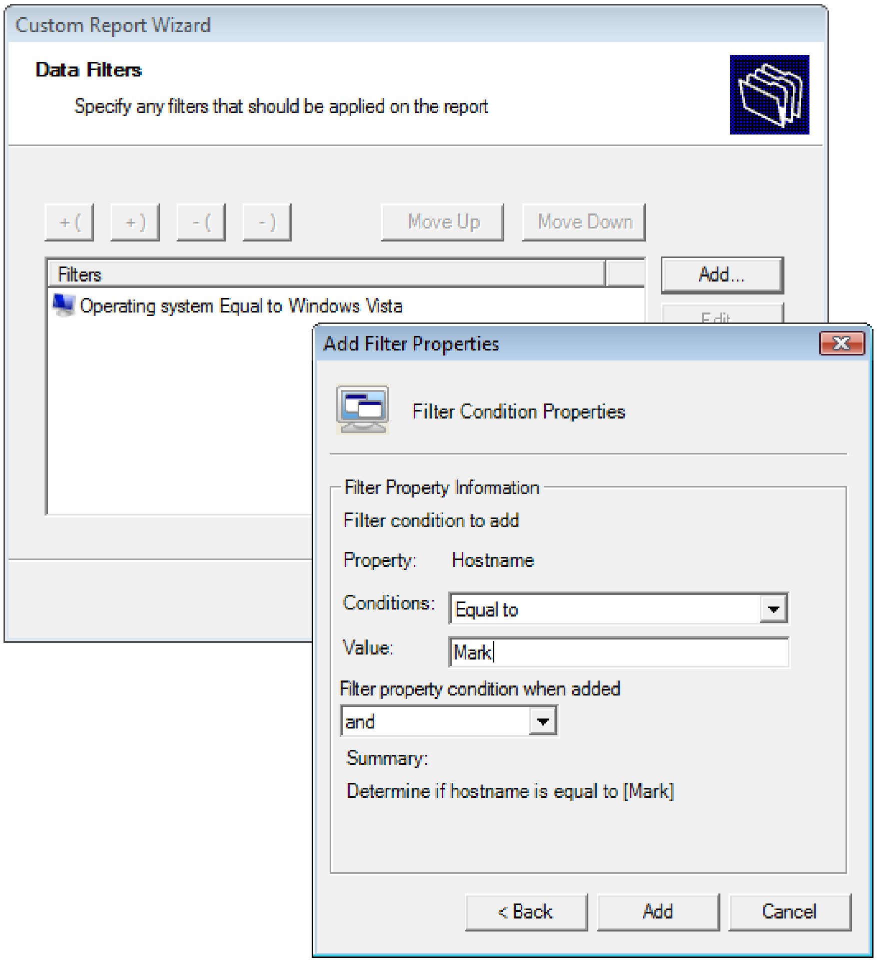


Screenshot 13 - Custom Report Wizard: Filters dialog

Click on the **Add…** button to bring up the 'Edit filter properties' dialog and configure the following conditions:

- '*Filter condition*' – Specify the data source area on which the filter will focus (for example, select 'Operating System' to filter the events data related to a specific operating system).
- '*Condition*' – Specify the condition comparison parameter.
- '*Value*' – Specify the string to which source data will be compared.

For example to generate a report which contains only information related to Windows XP, configure your filter parameters as shown below:



Custom Report Wizard
Data Filters
Specify any filters that should be applied on the report
+ (
+)
- (
-)
Move Up
Move Down
Filters
Operating system Equal to Windows Vista
Add...
Edit
Add Filter Properties
Filter Condition Properties
Filter Property Information
< Back
Add
Cancel

Filter condition to add

Property: Hostname

Conditions: Equal to

Value: Mark

Filter property condition when added: and

Summary:

Determine if hostname is equal to [Mark]

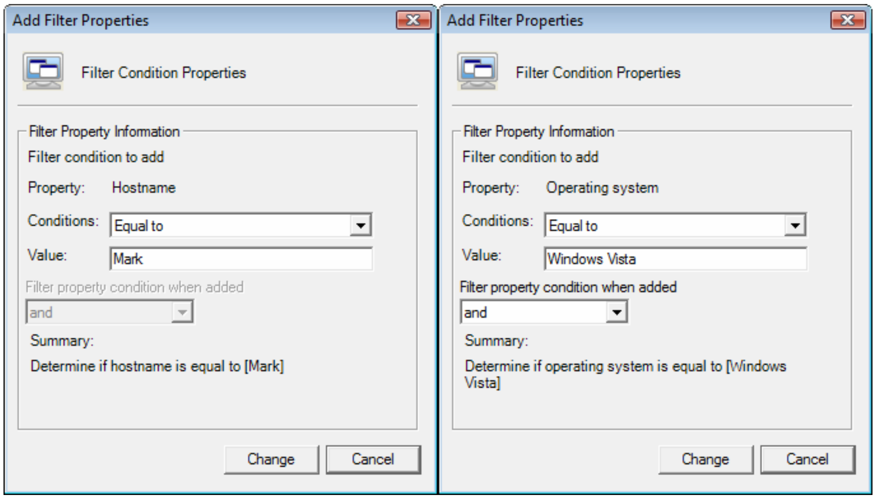
Screenshot 14 - Filter conditions configuration dialog

For more specific reports, you can limit the range of information to be displayed by tightening your conditions/search criteria. This is achieved by configuring and applying multiple data filters against the selected data source. When more than one filter is used, specify how these filters will be logically linked. This is achieved by selecting a logical grouping condition from ‘Filter property condition…’ drop down list.

- Select **And** to include ALL the scan data information that satisfies ALL of the conditions specified in the filters.
- Select **Or** to include ALL the scan data information that matches at least one of the specified filter conditions.

Example: Using multiple filters

Consider the situation where a custom report has 2 filters configured as follows:



Filter condition to add

Property: Hostname

Conditions: Equal to

Value: Mark

Filter property condition when added: and

Summary:

Determine if hostname is equal to [Mark]

Filter condition to add

Property: Operating system

Conditions: Equal to

Value: Windows Vista

Filter property condition when added: and

Summary:

Determine if operating system is equal to [Windows Vista]

Screenshot 15 - Using multiple filters

Parameters	Filter 1	Filter 2
Filter condition	Hostname	Operating System
Logical relation	Is equal to	Is equal to
Value	'Mark'	'Windows XP'

The data which will be included in this custom report will vary according to how these filters will be applied against your data. This is defined through the 'Filter property condition…' drop-down.

Filters applied			Data output
Filter 1	and	Filter 2	The report will show: • All scan data which is related to a host called 'Mark' which runs on 'Windows XP'.
Filter 1	or	Filter 2	The report will show: • All scan data related to 'Windows XP' – (no matter which host it belongs to) AND • All scan data related to a host called 'Mark' – (no matter which operating system it has installed).

Example: Creating a custom report based on network security scans performed during a particular month

This example demonstrates how to generate a network vulnerabilities summary report called 'Network vulnerabilities summary on hostname Mark for January 2007'. This report will be based on scans:

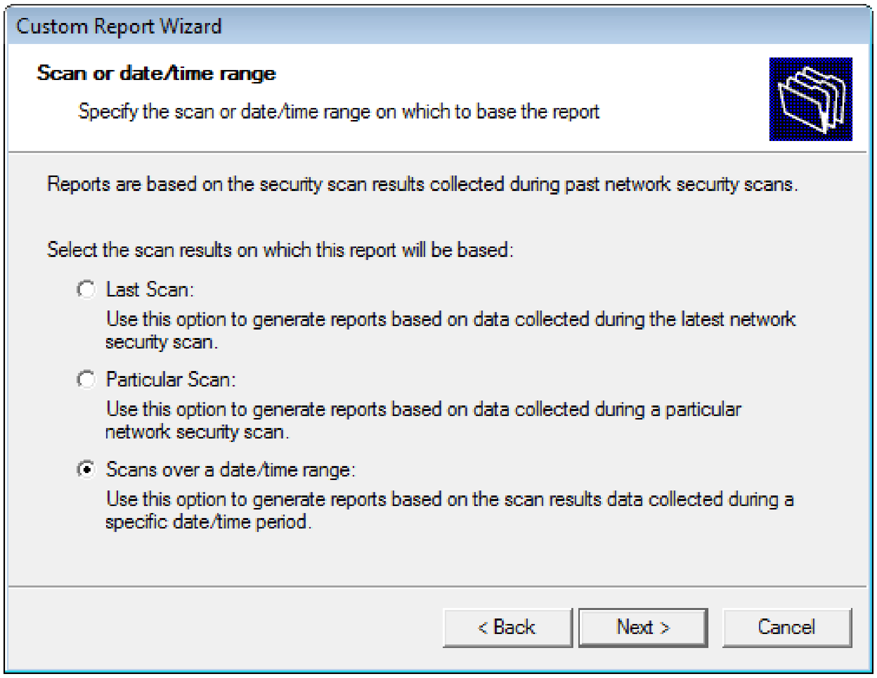
- Related to a host named 'Mark'
- Corresponding to operating system 'Windows XP'
- Performed during the month of 'November 2008'.

To create this report:

1. Click on the **Default Reports** navigation button.

2. Right-click on the report to be customized and select **New ▸ Custom Report**. This will bring up the 'Custom Reports Wizard'.

3. As soon as the welcome dialog is displayed, click **Next**.



Scan or date/time range

Specify the scan or date/time range on which to base the report

Reports are based on the security scan results collected during past network security scans.

Select the scan results on which this report will be based:

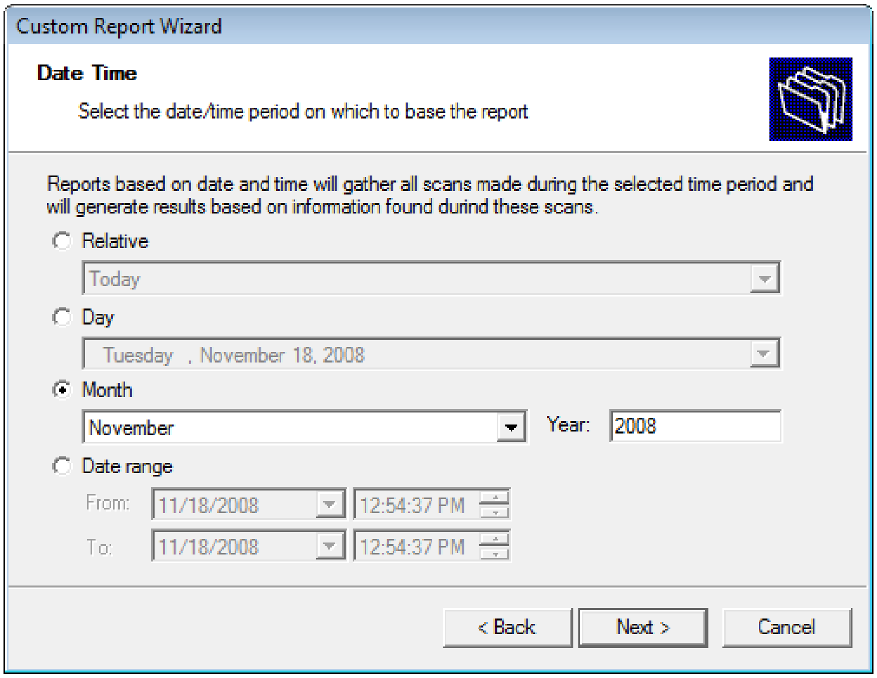
○ Last Scan:
Use this option to generate reports based on data collected during the latest network security scan.

○ Particular Scan:
Use this option to generate reports based on data collected during a particular network security scan.

● Scans over a date/time range:
Use this option to generate reports based on the scan results data collected during a specific date/time period.

Screenshot 16 – Selecting the data source to use

4. Select the *'Scans over a date/month range'* option and click Next.



Date Time

Select the date/time period on which to base the report

Reports based on date and time will gather all scans made during the selected time period and will generate results based on information found durind these scans.

○ Relative
Today

○ Day
Tuesday , November 18, 2008

● Month
November Year: 2008

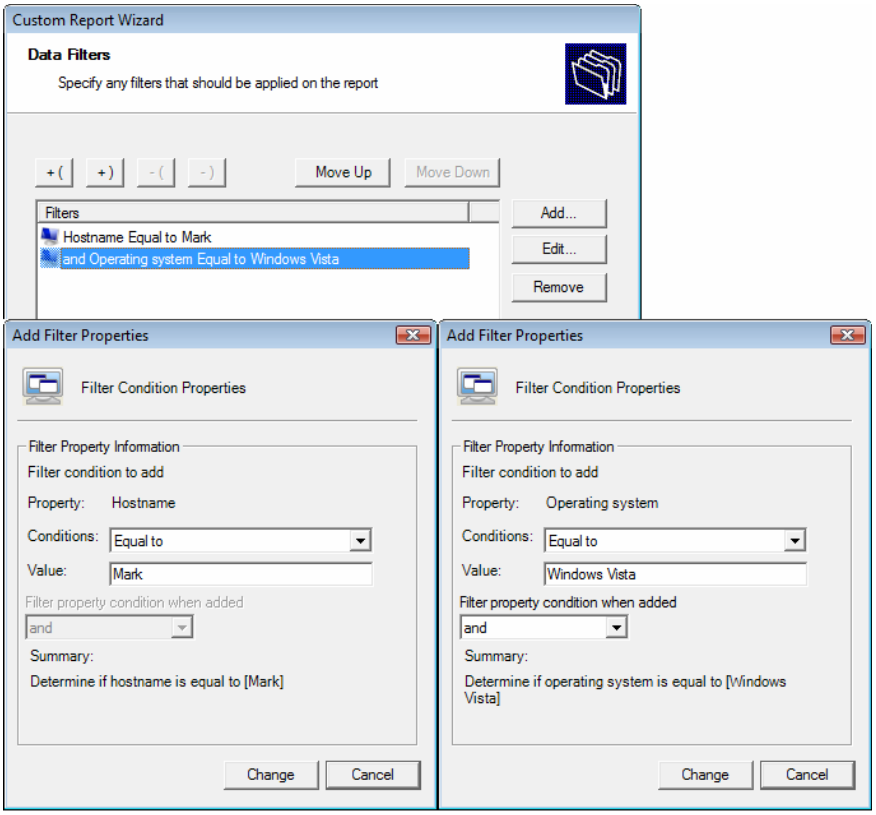
○ Date range
From: 11/18/2008 12:54:37 PM
To: 11/18/2008 12:54:37 PM

Screenshot 17 – Selecting the date/time period

5. Select the *'Month'* option and specify the following parameters:

- **Month**: '*November*'.
- **Year**: '*2008*'.

6. Click on **Next** to proceed to the data filters dialog.



Custom Report Wizard

Data Filters

Specify any filters that should be applied on the report

Filters

- Hostname Equal to Mark
- and Operating system Equal to Windows Vista

Add Filter Properties

Filter Condition Properties

Filter Property Information

Filter condition to add

Property: Hostname

Conditions: Equal to

Value: Mark

Filter property condition when added: and

Summary:

Determine if hostname is equal to [Mark]

Add Filter Properties

Filter Condition Properties

Filter Property Information

Filter condition to add

Property: Operating system

Conditions: Equal to

Value: Windows Vista

Filter property condition when added: and

Summary:

Determine if operating system is equal to [Windows Vista]

Screenshot 18 - Filter conditions dialog(s)

6. Click on the **Add…** button and configure the parameters of filter 1 as follows:

- ***Filter condition***: *'Hostname'*
- **Condition**: *'Equal to'*
- **Value**: *'Mark'.*

7. Click **OK** to finalize your filter configuration settings.

8. Click again on the **Add…** button and configure the parameters of filter 2 as follows:

- **Filter condition:** *'Operating system'*
- **Condition:** *'is equal to'*
- **Value:** *'Windows Vista'*
- **Filter Property condition…:** *'and'.*

9. Click **OK** to finalize your filter configuration settings.

10. Click **Next** and specify the following parameters:

- **Report Name**: *'Network Vulnerability summary for November 2008'*
- **Report Title:** *'Network security scans of hostname Mark'*
- **Report Description***: 'This report shows a summary of vulnerabilities found on hostname Mark during November 2008.'*

11. Click **Next** to proceed to the final dialog.

12. Click **Finish** to finalize your custom report configuration settings.

Run a custom report

To run a custom report:

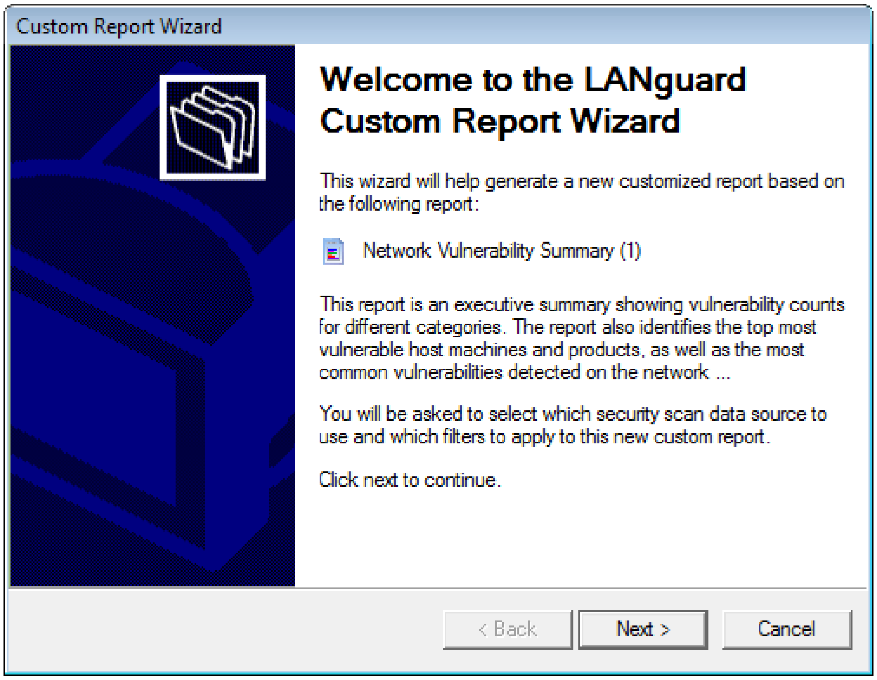
1. Click on the **Custom Reports** navigation button.

2. Right-click on the custom report to be generated and select **Generate**.

Editing a custom report

To edit the configuration settings of a custom report:

1. Click on the **Custom Reports** navigation button.



Custom Report Wizard

Welcome to the LANguard Custom Report Wizard

This wizard will help generate a new customized report based on the following report:

Network Vulnerability Summary (1)

This report is an executive summary showing vulnerability counts for different categories. The report also identifies the top most vulnerable host machines and products, as well as the most common vulnerabilities detected on the network ...

You will be asked to select which security scan data source to use and which filters to apply to this new custom report.

Click next to continue.

Screenshot 19 - Custom Report Wizard: Welcome dialog

2. Right-click on the custom report to be modified and select **Edit**. This will bring up the 'Custom Reports Wizard' through which you can make the required changes.

NOTE: For more information on how to configure the parameters of a custom report refer to the 'Creating a custom report' section in this chapter.

Deleting a custom report

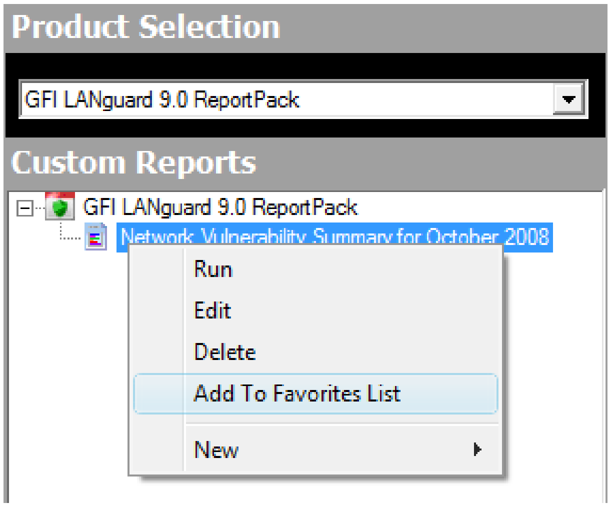
To delete a custom report:

1. Click on the **Custom Reports** navigation button.

2. Right-click on the custom report to be permanently removed from the list and select **Delete**.

3. Click **Yes** to confirm.

Adding custom reports to the list of favorite reports


Product Selection
GFI LANguard 9.0 ReportPack
Custom Reports
GFI LANguard 9.0 ReportPack
Network Vulnerability Summary for October 2008
Run
Edit
Delete
Add To Favorites List
New

Screenshot 20 - Favorite reports navigation button

You can group and access frequently used reports through the **Favorite Reports** navigation button. To add a custom report to the list of favorite reports:

1. Click on the **Custom Reports** navigation button to bring up the list of available reports.

2. Right-click on the custom report to be added to favorites and select **Add to Favorites List**.

3. Click Yes to confirm.

Scheduling reports

Introduction

GFI ReportCenter allows you to generate reports on a pre-defined schedule as well as at specified intervals. This way you can automate the generation of reports that are required on regular basis/ periodically.

Further to this, GFI ReportCenter can also be configured to automatically distribute scheduled reports via email. For every scheduled report, you can configure custom emailing parameters including the list of report recipients and the file format (e.g. PDF) in which the report will be attached to the email.

Use the report scheduling feature to automate your report generation requirements. For example, you can schedule lengthy reports after office working hours and automatically email them to the intended recipients. This way, you maximize the availability of your system resources during working hours and avoid any possible disruptions to workflow.

Both default and custom reports can be scheduled for automatic generation.

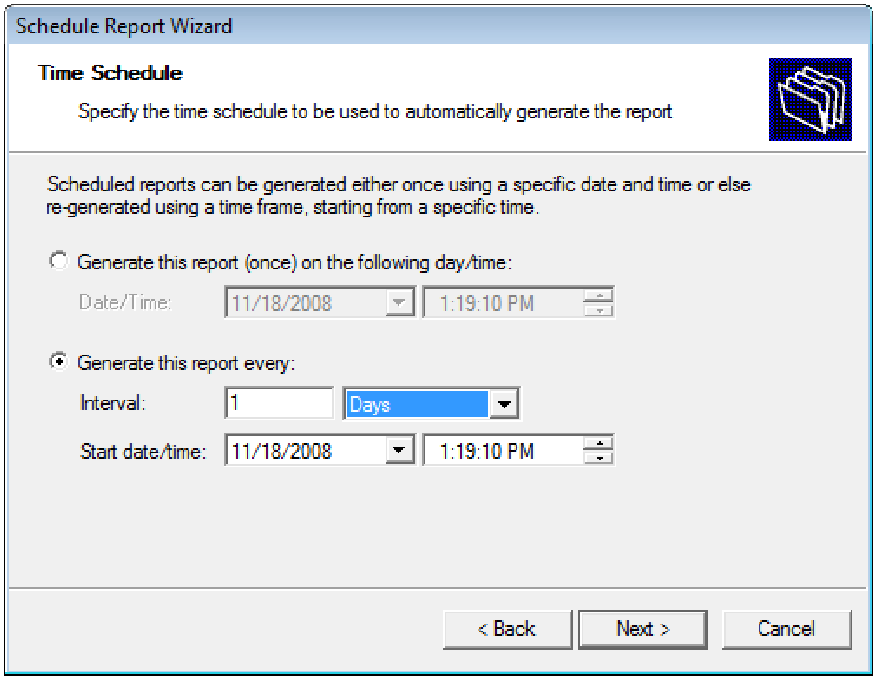
Scheduling a report

To schedule a report:

1. Click on the **Default/Custom Reports** option pane.

2. Right-click on the report to be scheduled and select **New ▸ Scheduled report**. This will bring up the 'Scheduled Report Wizard'. Click on **Next** to continue.

3. Select the network security scan(s) data to be covered by this report.



Schedule Report Wizard

Time Schedule

Specify the time schedule to be used to automatically generate the report

Scheduled reports can be generated either once using a specific date and time or else re-generated using a time frame, starting from a specific time.

○ Generate this report (once) on the following day/time:

Date/Time: 11/18/2008 1:19:10 PM

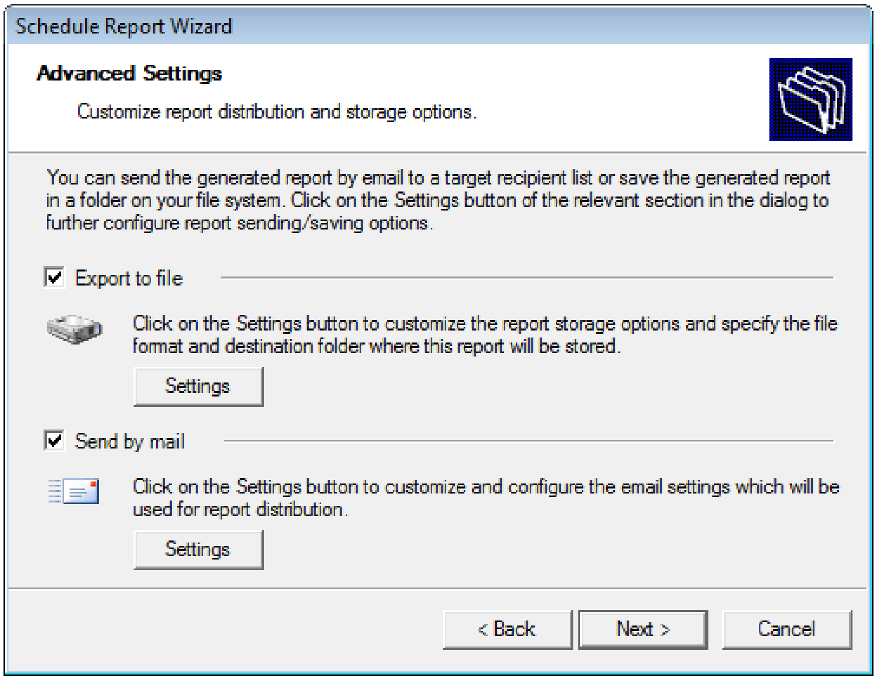
● Generate this report every:

Interval: 1 Days

Start date/time: 11/18/2008 1:19:10 PM

Screenshot 21 – Report Scheduling Wizard: Time schedule dialogue

4. Specify the report scheduling parameters (date/time/frequency). Click on **Next** to continue.



Schedule Report Wizard

Advanced Settings

Customize report distribution and storage options.

You can send the generated report by email to a target recipient list or save the generated report in a folder on your file system. Click on the Settings button of the relevant section in the dialog to further configure report sending/saving options.

☑ Export to file

Click on the Settings button to customize the report storage options and specify the file format and destination folder where this report will be stored.

☑ Send by mail

Click on the Settings button to customize and configure the email settings which will be used for report distribution.

Screenshot 22 – Report Scheduling Wizard: Advanced Settings dialog

5. To export the generated report to file, select the *'Export to file'* option. To customize the report export configuration settings click on the **Settings** button underneath this option.

NOTE: For information on how to configure export-to-file settings refer to the 'Configuring report export to file options' section in this chapter.

6. To automatically distribute generated reports via email, select the *'Send by mail'* option. To customize the email settings used for report distribution click on the **Settings** button underneath this option.

NOTE: For information on how to configure email settings refer to the 'Configuring report emailing options' in this chapter.

7. Specify a name and description for this scheduled report. Click on **Next** to continue.

8. Click on **Finish** to finalize your settings.

Configuring advanced settings

GFI LANguard ReportPack allows you to export scheduled reports to a specific file format as well as to automatically distribute these reports via email. This is achieved using either a set of parameters (e.g. recipient's email addresses) which are specified on the fly during scheduled report configuration or using the default set of report export and distribution parameters configured during the ReportPack installation.

NOTE: The Report Scheduling Wizard is by default configured to use the default set of report export and distribution parameters.

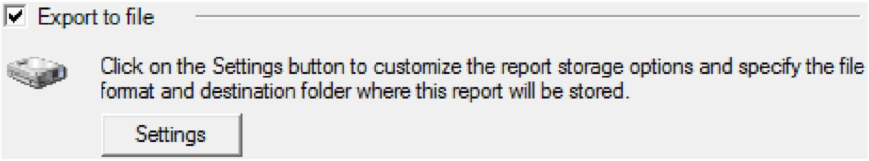
Report export formats

Scheduled reports can be exported in a variety of formats. Supported file formats include:

	Format	Description
1	Adobe Acrobat (.PDF)	Use this format to allow distribution of a report on different systems such as Macintosh and Linux while preserving the layout.
2	MS Excel (.XLS)	Use this format if you want to further process the report and perform more advance calculations using another (external) program such as Microsoft Excel.
3	MS Word (.DOC)	Use this format if you want to access this report using Microsoft Word.
4	Rich text format (.RTF)	Use this format to save the report in a format that is small in size and which allows accessibility through different word processors in different operating systems.

Configuring report export to file options

To configure the report export to file settings of a scheduled report do as follows:

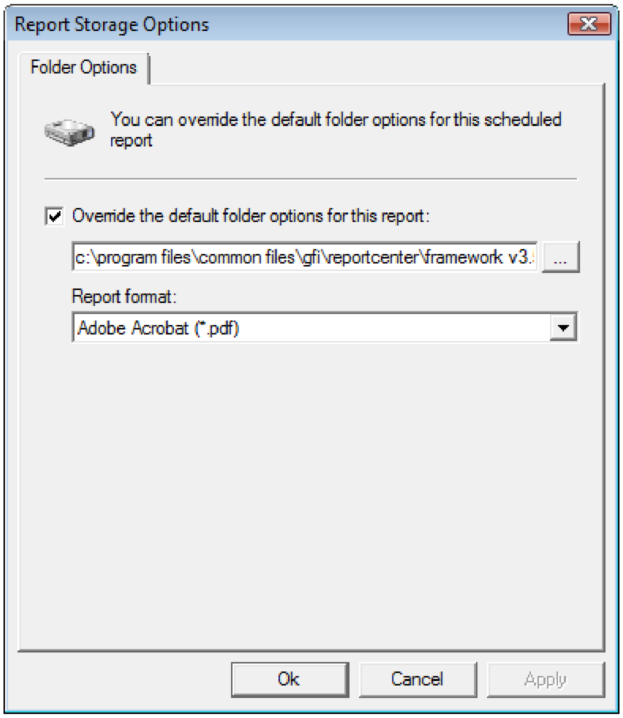


☑ Export to file

Click on the Settings button to customize the report storage options and specify the file format and destination folder where this report will be stored.

Screenshot 23 - Advanced Settings dialog: Export to file settings button

1. From the 'Advanced Settings' dialog, click on the **Settings** button underneath the *'Export to file'* option.


Report Storage Options

Folder Options

You can override the default folder options for this scheduled report

☑ Override the default folder options for this report:

c:\program files\common files\gfi\reportcenter\framework v3.

Report format:

Adobe Acrobat (*.pdf)

Screenshot 24 - Advanced Settings: Export to file options

2. Select the option *'Override the default folder options for this report:'*

3. Specify the complete path where the exported report will be saved.

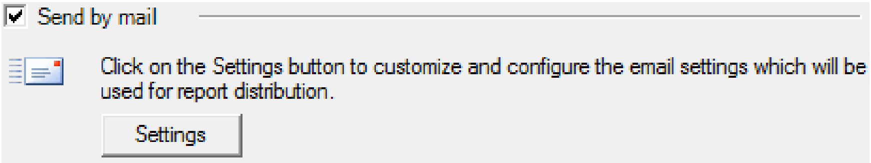
4. Specify the file format in which the exported report will be saved.

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

NOTE: For information on how to configure the default export to file settings refer to the 'Configuring default scheduling options' section in this manual.

Configuring report emailing options

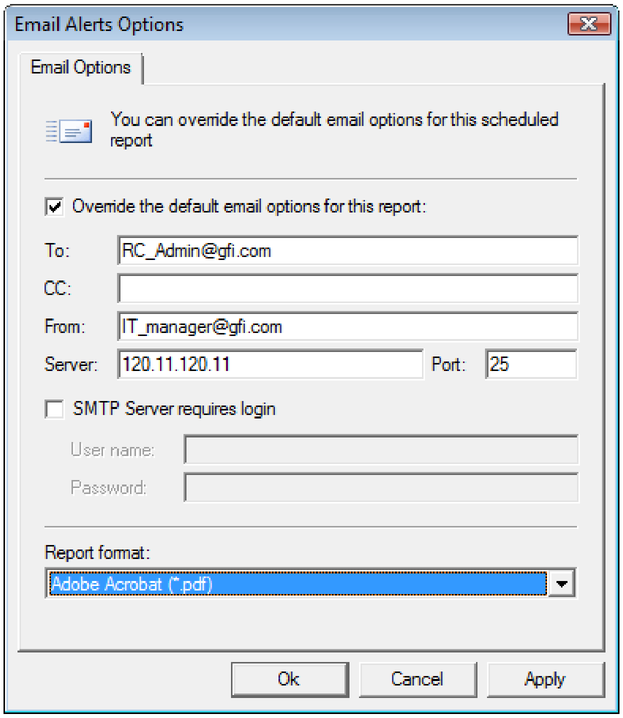
To configure the report emailing options of a scheduled report do as follows:


☑ Send by mail

Click on the Settings button to customize and configure the email settings which will be used for report distribution.

Screenshot 25 - Advanced Settings dialog: Send by email settings button

1. From the 'Advanced Settings' dialog, click on the **Settings** button underneath the *'Send by email'* option.



You can override the default email options for this scheduled report

☑ Override the default email options for this report:

To: RC_Admin@gfi.com

CC:

From: IT_manager@gfi.com

Server: 120.11.120.11

Port: 25

☐ SMTP Server requires login

User name:

Password:

Report format: Adobe Acrobat (*.pdf)

Screenshot 26 - Report distribution options

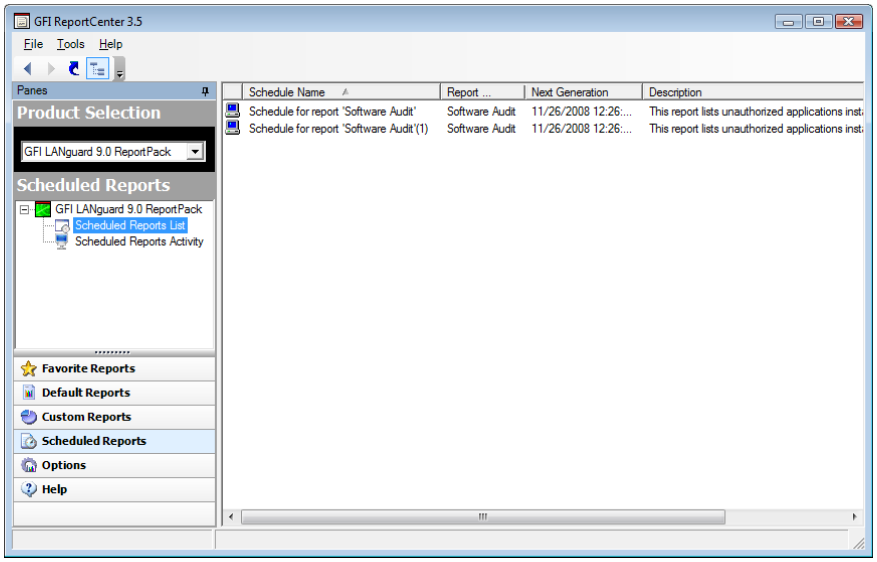
2. Select the option *'Override the default email options for this report:'*

3. Specify the following parameters:

- **To/CC**: Specify the email address(es) where the generated report will be sent.
- **From**: Specify the email account that will be used to send the report.
- **Server**: Specify the name/IP of your SMTP (outbound) email server. If the specified server requires authentication, select the option 'SMTP Server requires login' and specify the logon credentials in the *'User name'* and *'Password'* fields.
- **Report format**: Reports are sent via email as attachments. Select the file format in which to send out your report.

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

Viewing the list of scheduled reports



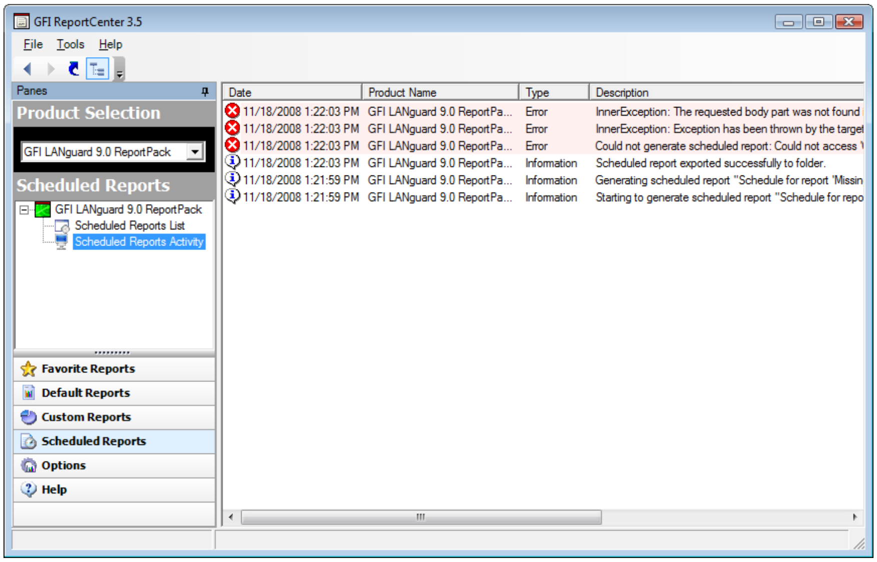
Schedule Name	Report ...	Next Generation	Description
Schedule for report 'Software Audit'	Software Audit	11/26/2008 12:26:...	This report lists unauthorized applications inst:
Schedule for report 'Software Audit'(1)	Software Audit	11/26/2008 12:26:...	This report lists unauthorized applications inst:

Screenshot 27 - List of Scheduled reports

Click on the **Scheduled Reports** navigation button to show the list of scheduled reports which are currently configured for automatic generation. This information is displayed in the right pane of the management console and includes the following details:

- **Schedule Name:** The custom name that was specified during the creation of the new scheduled report.
- **Report Name:** The names of the default or custom report(s) that will be generate.
- **Last Generation***:* Indicates the date/time when the report was last generated.
- **Next Generation:** Indicate the date/time when the report is to be next generated.
- **Description**: The description that you have entered for each schedule.

Viewing the scheduled reports activity



Date	Product Name	Type	Description
11/18/2008 1:22:03 PM	GFI LANguard 9.0 ReportPa...	Error	InnerException: The requested body part was not found
11/18/2008 1:22:03 PM	GFI LANguard 9.0 ReportPa...	Error	InnerException: Exception has been thrown by the target
11/18/2008 1:22:03 PM	GFI LANguard 9.0 ReportPa...	Error	Could not generate scheduled report: Could not access
11/18/2008 1:22:03 PM	GFI LANguard 9.0 ReportPa...	Information	Scheduled report exported successfully to folder.
11/18/2008 1:21:59 PM	GFI LANguard 9.0 ReportPa...	Information	Generating scheduled report "Schedule for report 'Missin
11/18/2008 1:21:59 PM	GFI LANguard 9.0 ReportPa...	Information	Starting to generate scheduled report "Schedule for repo

Screenshot 28 - Schedule activity monitor

GFI ReportCenter also includes a schedule activity monitor through which you can view events related to all scheduled reports that have been executed.

To open the schedule activity monitor, click on the **Scheduled Reports** navigation button and select the **Scheduled Reports Activity** node. This will bring up the activity information in the right pane of the GFI ReportCenter management console.

The activity monitor displays the following events:

ⓘ - **Information**: The scheduled report was successfully executed and sent by email and/or saved to disk.

⚠ - **Warning**: The scheduled report was not executed because product license is invalid or has expired.

⊗ - **Error**: The scheduled report was not executed due to a particular condition/event. Typical conditions include:

- Errors when attempting to save the generated report to a specific folder (for example, out of disk space).
- Errors when attempting to send the generated report via email (for example, the SMTP server configured in the GFI ReportCenter settings is not reachable).

The activity monitor records and enumerates the following information:

- **Date:** The date and time when the scheduled report was executed.
- **Product name**: The name of the GFI product to which the report belongs.
- **Type:** The event classification - error, information, or warning.
- **Description:** Information related to the state of a scheduled report that has been executed. The format and contents of the activity description vary, depending on the event type.

NOTE: The description is often the most useful piece of information, indicating what happened during the execution of a scheduled report or the significance of the event.

Enable/disable a scheduled report

Scheduled reports can be enabled or disabled as required. Use the **Scheduled Reports** navigation button to view the list of scheduled reports as well as to identify their current status. The status of scheduled reports is shown through the icon included on the left hand side of each schedule:

🖥❌ - Indicates that the scheduled report is disabled.

🖥 - Indicates that the scheduled report is enabled/pending.

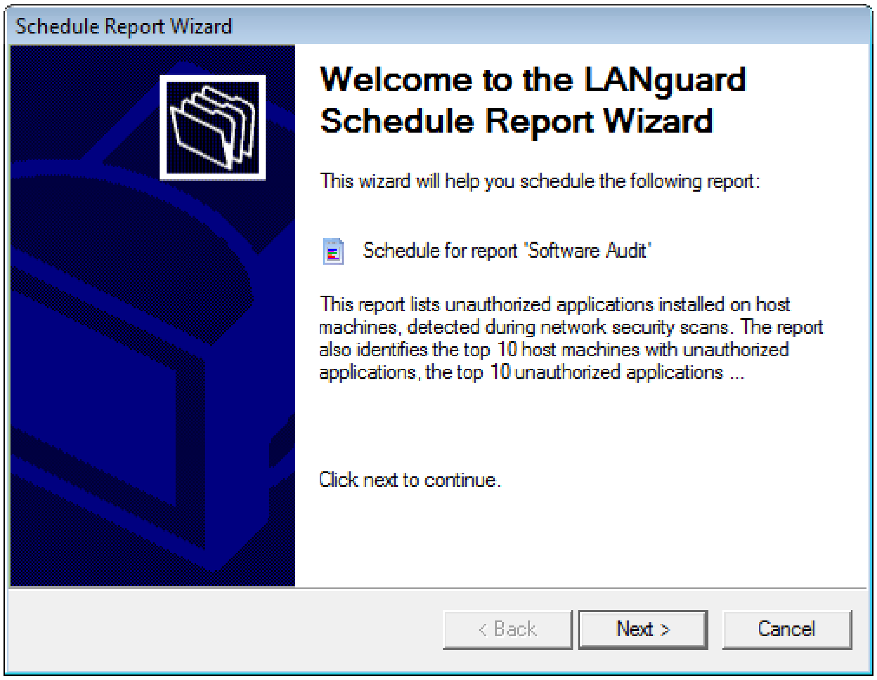
To enable or disable a scheduled report, right-click on the respective report and select **Enable/Disable** accordingly.

Editing a scheduled report

To make changes to the configuration settings of a scheduled report:

1. Click on the **Scheduled Reports** navigation button.

2. Right-click on the scheduled report to be re-configured and select **Properties**. This will bring up the ‘Scheduled Reports Wizard’.



Schedule Report Wizard

Welcome to the LANguard Schedule Report Wizard

This wizard will help you schedule the following report:

Schedule for report 'Software Audit'

This report lists unauthorized applications installed on host machines, detected during network security scans. The report also identifies the top 10 host machines with unauthorized applications, the top 10 unauthorized applications ...

Click next to continue.

Screenshot 29 - Scheduled Reports wizard

3. Click on **Next** and perform the required changes. For information on how to configure the parameters of a scheduled report refer to the ‘Creating a scheduled report’ section in this chapter.

Deleting a scheduled report

To delete a scheduled report:

1. Click on the **Scheduled Reports** navigation button.

2. Right-click on the scheduled report to be permanently removed from the list and select **Delete**.

Example: Scheduling a report

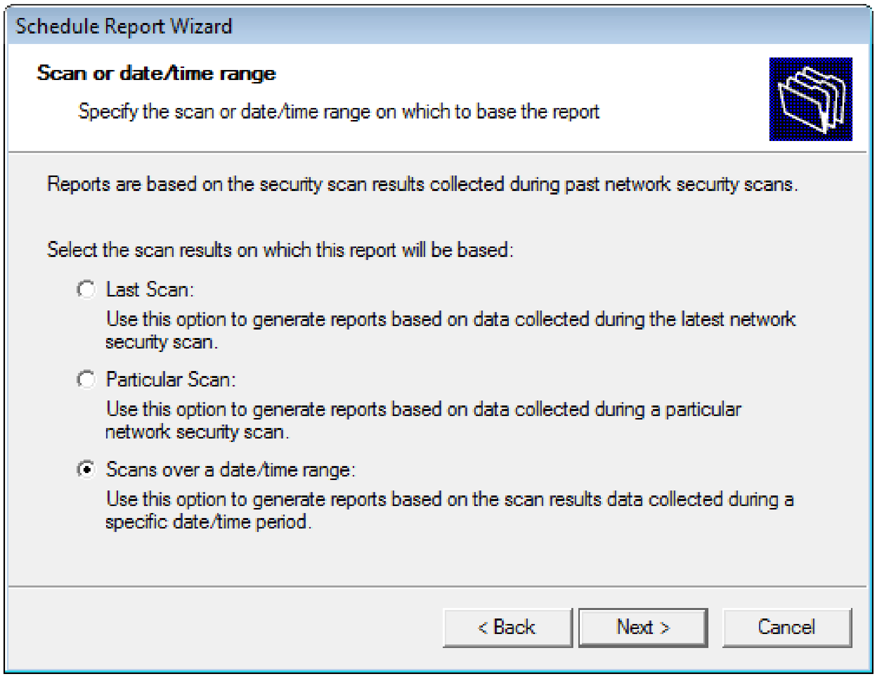
This example demonstrates how to schedule a software audit report which will:

- Generate the first report on 18/11/2008 at 20:00.
- Continue generating the same report on a monthly basis.
- Export the generated report(s) to folder 'C:\Monthly Reports' in PDF format.
- Email the generated report using the following custom parameters:
    - o Send from email account: 'RC_Admin@gfi.com'
    - o Send to email account: 'IT_manager@gfi.com'
    - o SMTP server details: '120.11.120.11.

To create the scheduled report:

1. Click on the **Default Reports** navigation button.

2. Right-click on 'Network Vulnerability Summary' and select **New ▸ Scheduled Report**. As soon as the welcome dialog is displayed click **Next**.



Schedule Report Wizard

Scan or date/time range

Specify the scan or date/time range on which to base the report

Reports are based on the security scan results collected during past network security scans.

Select the scan results on which this report will be based:

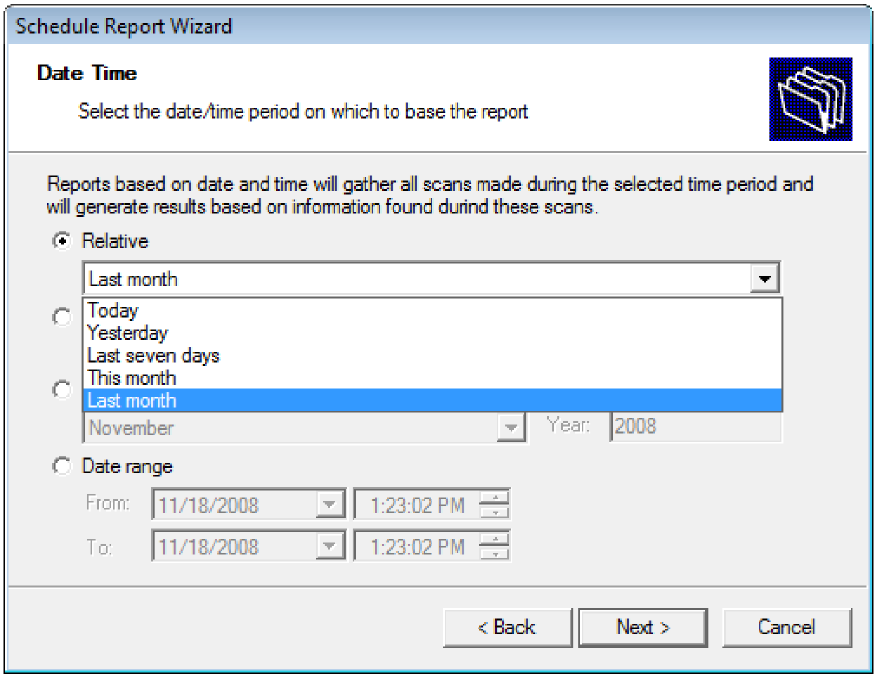
○ Last Scan:
Use this option to generate reports based on data collected during the latest network security scan.

○ Particular Scan:
Use this option to generate reports based on data collected during a particular network security scan.

● Scans over a date/time range:
Use this option to generate reports based on the scan results data collected during a specific date/time period.

Screenshot 30 - Select network security scan(s) data

3. Select the option '***Scans over a date/time range***' for data to be covered by this report and click **Next**.



Schedule Report Wizard

Date Time

Select the date/time period on which to base the report

Reports based on date and time will gather all scans made during the selected time period and will generate results based on information found durind these scans.

● Relative

Last month

- Today
- Yesterday
- Last seven days
- This month
- Last month

○

○ November Year: 2008

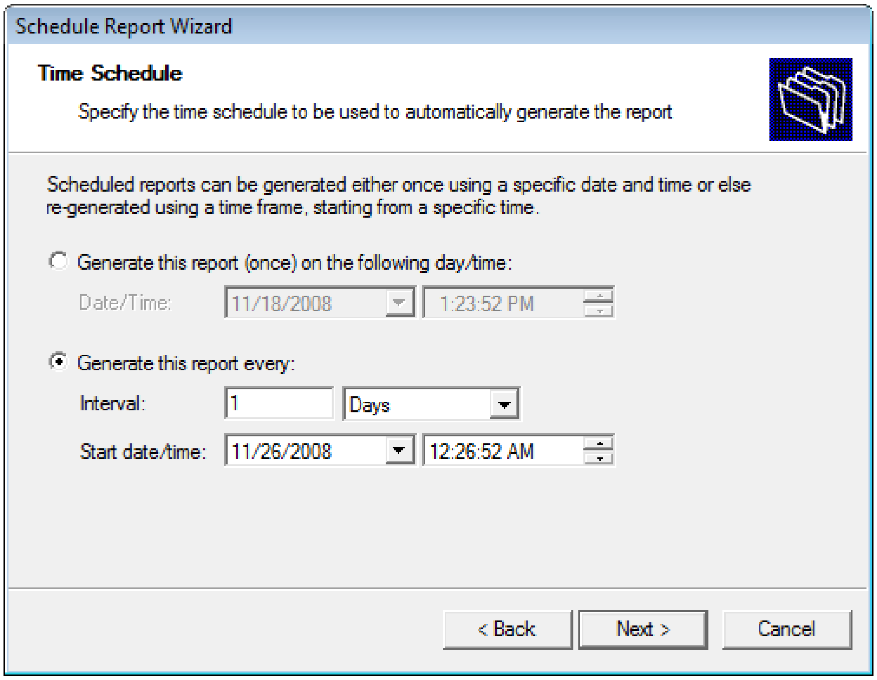
○ Date range

From: 11/18/2008 1:23:02 PM

To: 11/18/2008 1:23:02 PM

Screenshot 31 - Select date/time of network scan

4. Select the option ***'Relative'*** and from the provided drop down list select *'Last month'*. Click on **Next** to proceed to the next dialog.



Schedule Report Wizard

Time Schedule

Specify the time schedule to be used to automatically generate the report

Scheduled reports can be generated either once using a specific date and time or else re-generated using a time frame, starting from a specific time.

○ Generate this report (once) on the following day/time:

Date/Time: 11/18/2008 1:23:52 PM

● Generate this report every:

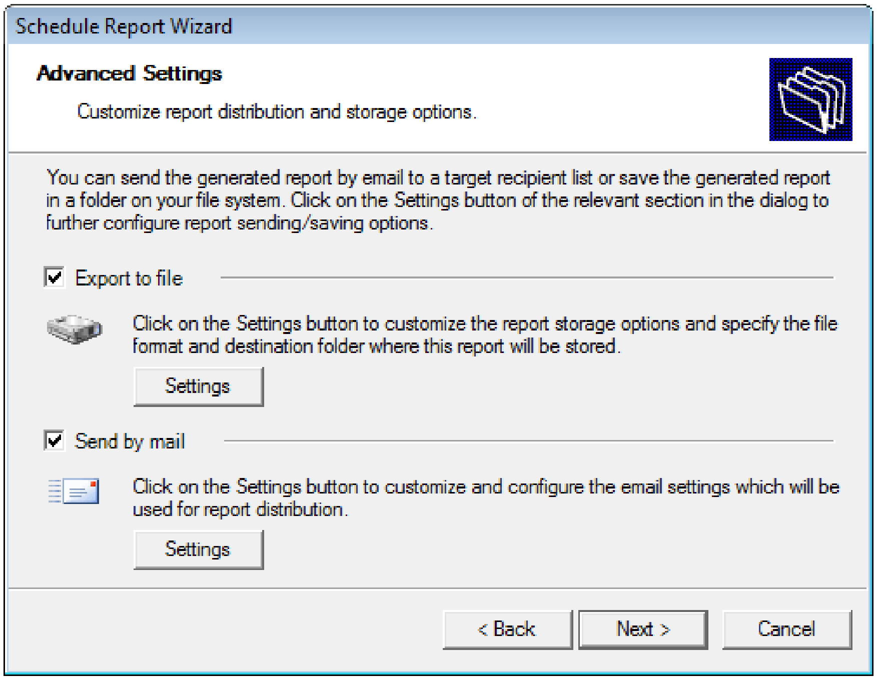
Interval: 1 Days

Start date/time: 11/26/2008 12:26:52 AM

Screenshot 32 – Specifying the scheduling options

5. To generate this report on a monthly basis, select the option *'Generate this report every:'* and set the interval to *'30 Days'* .

6. Set the start date to *'18/11/2008'* and time to *'20:00'*. Click **Next** to continue.


Schedule Report Wizard

Advanced Settings

Customize report distribution and storage options.

You can send the generated report by email to a target recipient list or save the generated report in a folder on your file system. Click on the Settings button of the relevant section in the dialog to further configure report sending/saving options.

☑ Export to file

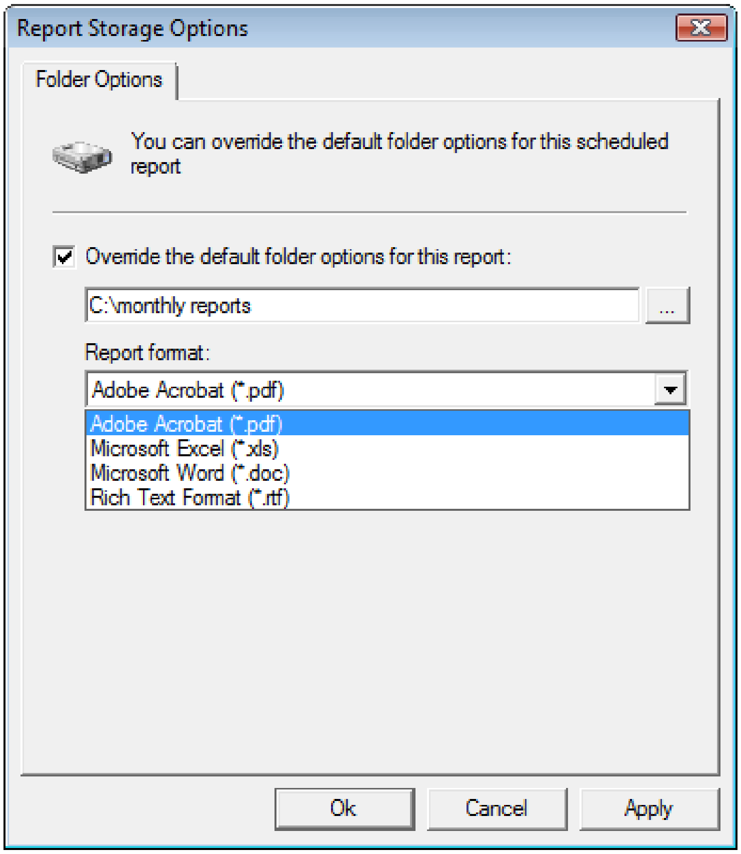
Click on the Settings button to customize the report storage options and specify the file format and destination folder where this report will be stored.

☑ Send by mail

Click on the Settings button to customize and configure the email settings which will be used for report distribution.

Screenshot 33 - Advanced Settings dialog

7. From the ‘Advanced Settings’ dialog, click on the **Settings** button underneath the *‘Export to file’* option.


Report Storage Options

You can override the default folder options for this scheduled report

☑ Override the default folder options for this report:

C:\monthly reports

Report format:

Adobe Acrobat (*.pdf)

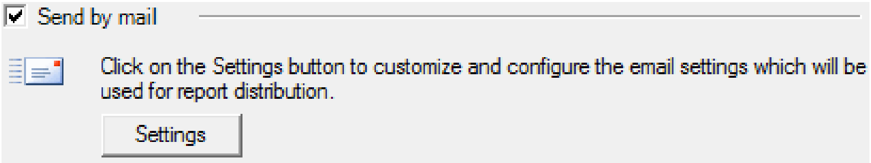
- Adobe Acrobat (*.pdf)
- Microsoft Excel (*.xls)
- Microsoft Word (*.doc)
- Rich Text Format (*.rtf)

Screenshot 34 - Advanced Settings: Export to file options

8. Select the option *‘Override the default folder options for this report:’*

9. Specify the complete path where this report will be saved i.e. *'C:\Monthly Reports'*.

10. From the report format drop down select '*PDF'* and click **OK**.

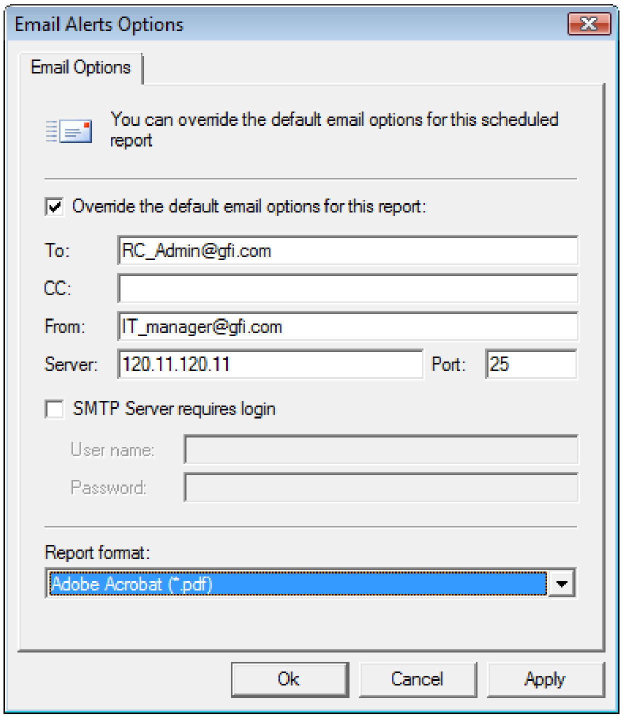


☑ Send by mail

Click on the Settings button to customize and configure the email settings which will be used for report distribution.

Screenshot 35 - Advanced Settings dialog: Send by email settings button

11. From the 'Advanced Settings' dialog, click on the **Settings** button underneath the *'Send by email'* option.



You can override the default email options for this scheduled report

☑ Override the default email options for this report:

To: RC_Admin@gfi.com

CC:

From: IT_manager@gfi.com

Server: 120.11.120.11 Port: 25

□ SMTP Server requires login

User name:

Password:

Report format: Adobe Acrobat (*.pdf)

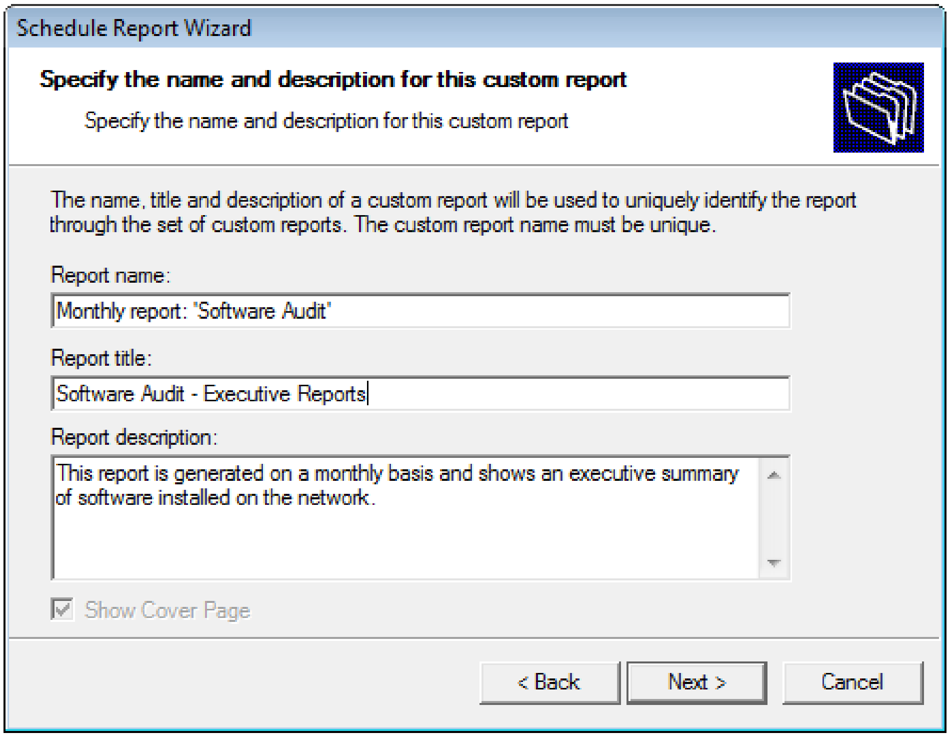
Screenshot 36 - Report distribution options

12. Select the option *'Override the default email options for this report:'*

13. Specify the following parameters:

- **To:** *'RC_Admin@gfi.com'*
- **From:** *'IT_manager@gfi.com'*
- **Server:** *'120.11.120.11'.*

14. From the report format drop down select *'PDF'* and click **OK** to finalize your email settings.



Specify the name and description for this custom report

Specify the name and description for this custom report

The name, title and description of a custom report will be used to uniquely identify the report through the set of custom reports. The custom report name must be unique.

Report name: Monthly report: 'Software Audit'

Report title: Software Audit - Executive Reports

Report description: This report is generated on a monthly basis and shows an executive summary of software installed on the network.

☑ Show Cover Page

Screenshot 40 – Custom report name and description

15. Click **Next** and specify the following parameters:

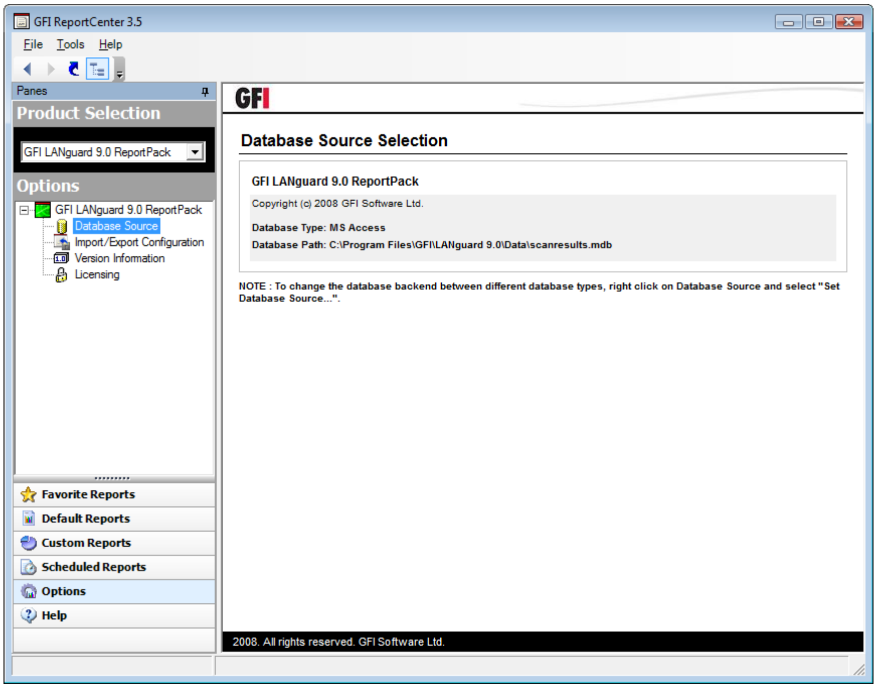
- **Report Name**: *'Monthly report: 'Software Audit'*
- **Report Title**: *'Software Audit – Executive reports'*
- **Report Description**: This report is generated on a monthly basis and shows an executive summary of software installed on the network.

16. Click **Next** to proceed to the final dialog.
17. Click **Finish** to finalize your custom report configuration settings.

Configuring default options

Introduction

The GFI LANguard ReportPack allows you to configure a default set of parameters which can be used when generating reports. These parameters are first set during installation. However, you can still reconfigure any of these parameters via the **Options** navigation button and the **Tools** menu provided in the GFI ReportCenter management console.



Database Source Selection

GFI LANguard 9.0 ReportPack

Copyright (c) 2008 GFI Software Ltd.

Database Type: MS Access

Database Path: C:\Program Files\GFI\LANguard 9.0\Data\scanresults.mdb

NOTE : To change the database backend between different database types, right click on Database Source and select "Set Database Source...".

2008. All rights reserved. GFI Software Ltd.

Screenshot 37 - Options navigation button and Tools menu

Through the **Options** navigation button you can configure the following parameter:

- **Database source:** Use this node to specify the database backend from where the ReportPack will extract the required reporting data.

Through the **Tools** menu you can configure the following parameters:

- **Default scheduling settings:** Use this menu option to configure the default export to file parameters and report emailing parameters of scheduled reports.

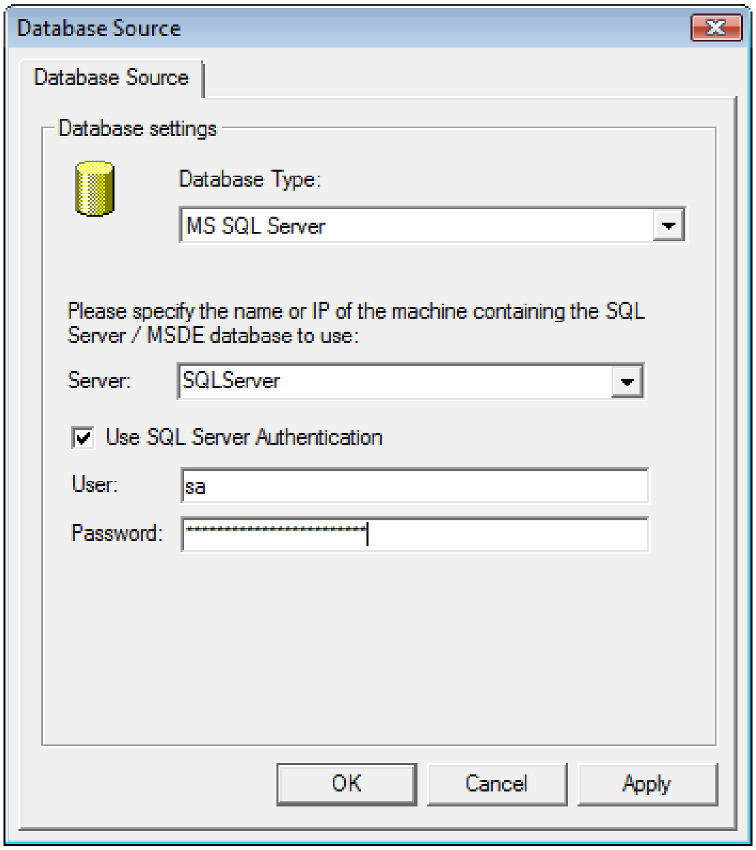
You can also backup your configuration settings for the ReportPack through the **Import/Export Configuration** node in the **Options** section. Exported configurations may be imported into a separate GFI ReportCenter instance, provided that the same ReportPacks are installed on both instances.

Configuring database source: Microsoft SQL Server

To configure MS SQL Server your database source:

1. Click on the **Options** navigation button.

2. Right-click on the **Database Source** node and select **Set Database Source…** This will bring up the database source configuration dialog.



Database Type: MS SQL Server

Please specify the name or IP of the machine containing the SQL Server / MSDE database to use:

Server: SQLServer

☑ Use SQL Server Authentication

User: sa

Password: ************************

Screenshot 38 - Database source configuration dialog: SQL Server

3. Select '*MS SQL Server*' as the database type from the provided list of supported databases.

4. Specify the name or IP address of your MSDE/MS SQL Server database backend.

5. To use the credentials of an SQL Server account, select the *'Use SQL Server authentication'* option and specify the user name and password in the provided fields.

NOTE: By default, the GFI LANguard ReportPack uses Windows logon credentials to authenticate to the SQL Server.

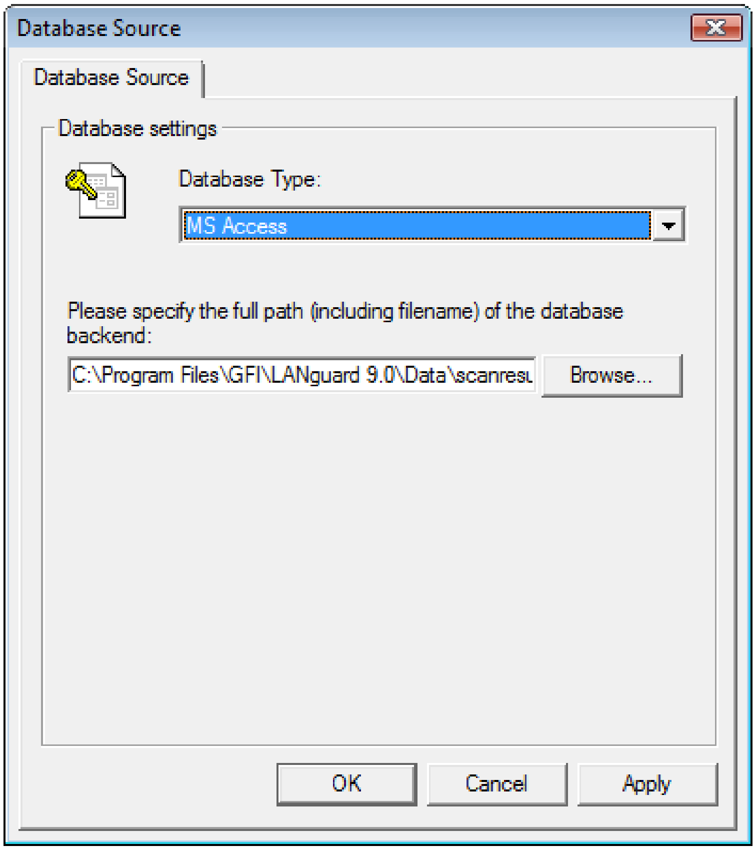
6. Click on **OK** to finalize your configuration settings.

Configuring database source: Microsoft Access

To configure Microsoft Access as your database source:

1. Click on the **Options** navigation button.

2. Right-click on the **Database Source** node and select **Set Database Source…** This will bring up the database source configuration dialog.



Database Source

Database Source

Database settings

Database Type: MS Access

Please specify the full path (including filename) of the database backend:

C:\Program Files\GFI\LANguard 9.0\Data\scanresu

Screenshot 39 - Database source configuration dialog: MS Access

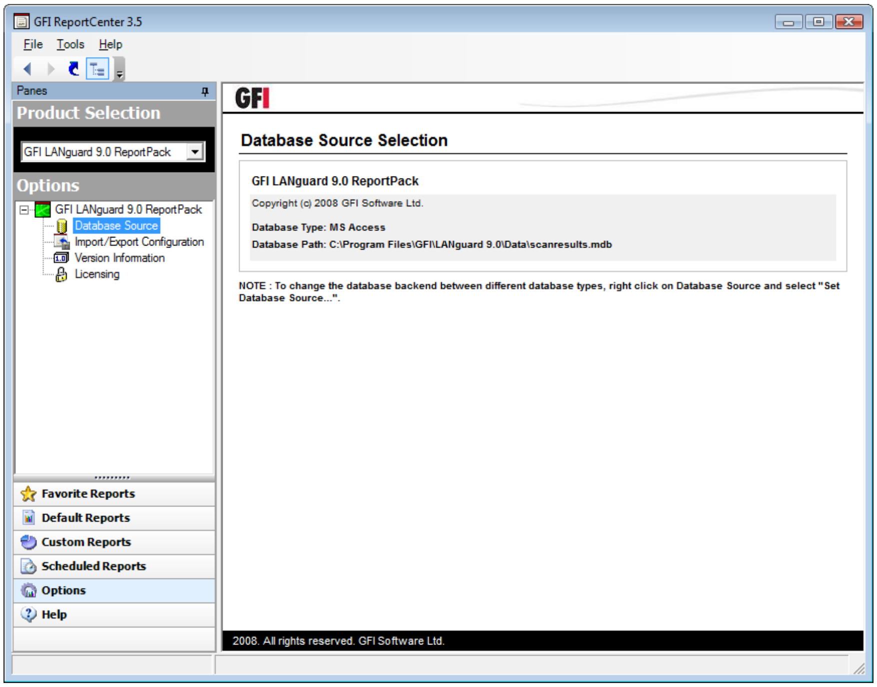
3. Select '*MS Access*' as the database type from the provided list of supported databases.

4. Specify the complete path to the database backend. If the database source is not stored locally, specify the complete path using Universal Naming Convention (UNC).

(e.g., *\\Security_Server\Program Files\GFI\LANguard 9\Data\scanresults.mdb*).

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

Viewing the current database source settings



Database Source Selection

GFI LANguard 9.0 ReportPack

Copyright (c) 2008 GFI Software Ltd.

Database Type: MS Access

Database Path: C:\Program Files\GFI\LANguard 9.0\Data\scanresults.mdb

NOTE : To change the database backend between different database types, right click on Database Source and select "Set Database Source...".

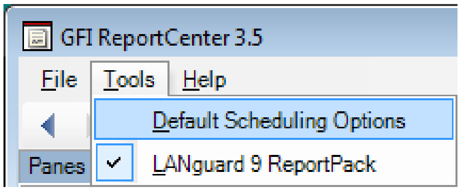
2008. All rights reserved. GFI Software Ltd.

Screenshot 40 - Database source configuration settings

After configuration, you can view the current database source settings by clicking on the **Database Source** node.

Configuring default scheduling settings

To configure the default settings to be used by scheduled reports:

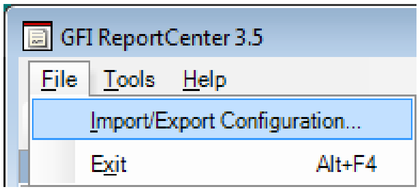


Screenshot 41 - Default scheduling options node

1. From the pull-down menu, click on the **Tools ▸ Default Scheduling Options**.

2. Configure the required parameter as described in the ‘Configuring Advanced Settings’ section of the Scheduling Reports chapter.

Importing/Exporting the configuration



Screenshot 42 – Import/Export Configuration node

The GFI ReportCenter allows you to backup your configuration settings for the ReportCenter and all ReportPacks through **Import/Export Configuration…** in the **File** pull-down menu. Settings are exported for:

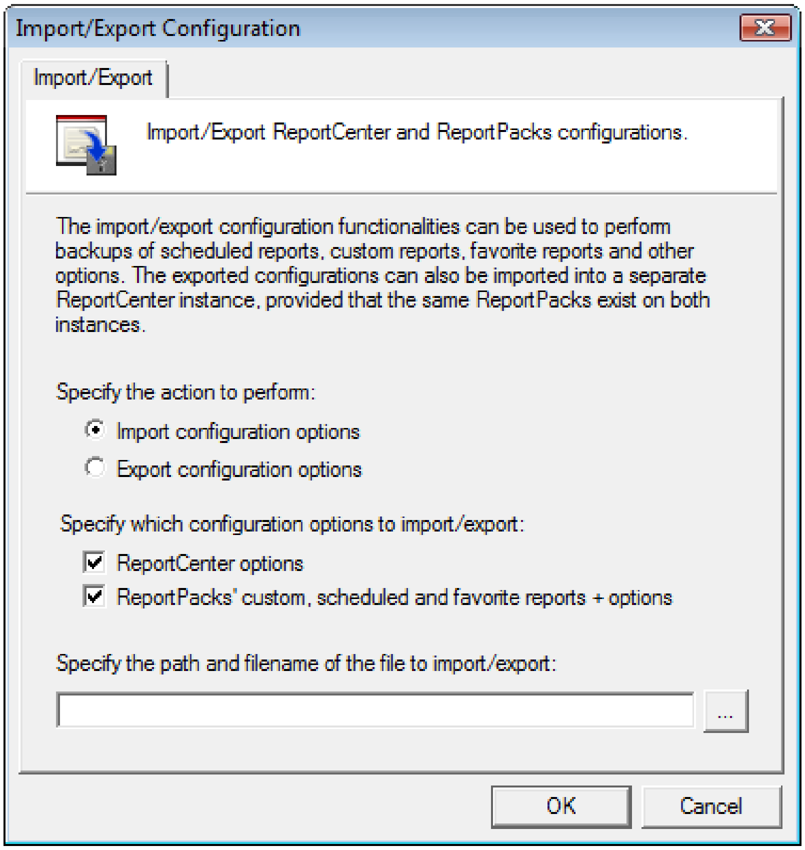
- Default scheduling options
- Custom reports
- Scheduled reports
- Favorite reports.

The configuration is backed up into an XML file which may be imported into a separate GFI ReportCenter instance, provided that the same ReportPacks are installed on both instances.

You can also import/export the configuration for a particular ReportPack through the **Import/Export Configuration** node in the **Options** section of the ReportPack.

Exporting the configuration

To export the GFI LANguard configuration:


Import/Export Configuration
Import/Export
Import/Export ReportCenter and ReportPacks configurations.

The import/export configuration functionalities can be used to perform backups of scheduled reports, custom reports, favorite reports and other options. The exported configurations can also be imported into a separate ReportCenter instance, provided that the same ReportPacks exist on both instances.

Specify the action to perform:

● Import configuration options

○ Export configuration options

Specify which configuration options to import/export:

☑ ReportCenter options

☑ ReportPacks' custom, scheduled and favorite reports + options

Specify the path and filename of the file to import/export:

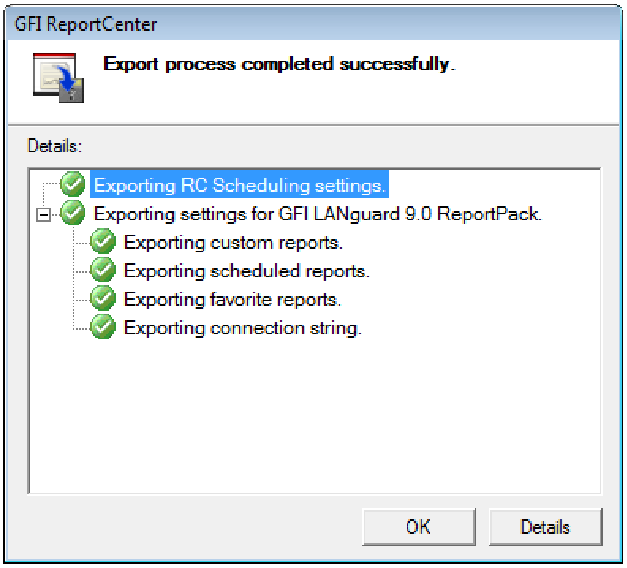
Screenshot 43 – Import/Export configuration dialog

1. From the pull-down menu, click on the **File ▸ Import/Export Configuration…** . This will bring up the configuration dialog.

2. Select the option ‘***Export configurations options***’.

3. Specify which configuration options to export.

4. Specify the path and filename of the XML file to export. Click on **OK** to proceed with the export.



Export process completed successfully.

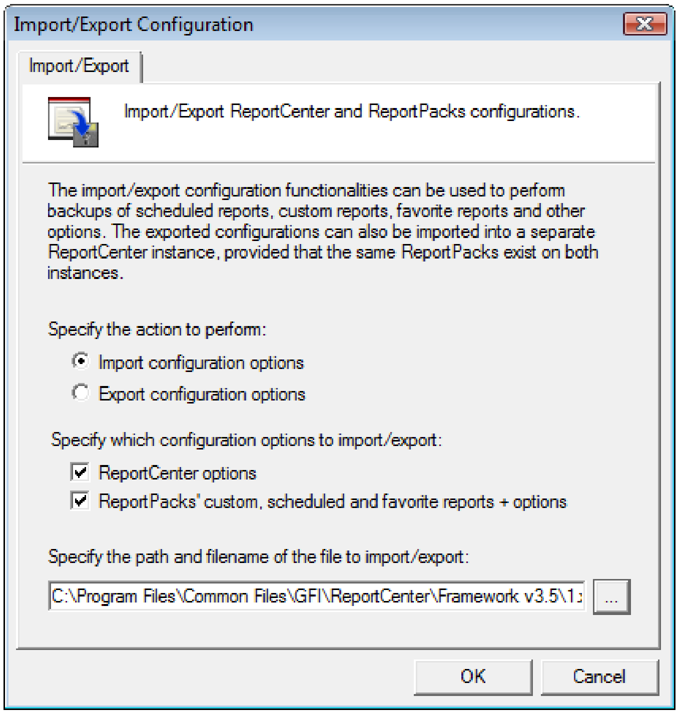
Details:

- Exporting RC Scheduling settings.
- Exporting settings for GFI LANguard 9.0 ReportPack.
  - Exporting custom reports.
  - Exporting scheduled reports.
  - Exporting favorite reports.
  - Exporting connection string.

Screenshot 44 – Export configuration success

Importing the configuration

To import the GFI LANguard configuration:



Import/Export ReportCenter and ReportPacks configurations.

The import/export configuration functionalities can be used to perform backups of scheduled reports, custom reports, favorite reports and other options. The exported configurations can also be imported into a separate ReportCenter instance, provided that the same ReportPacks exist on both instances.

Specify the action to perform:

● Import configuration options

○ Export configuration options

Specify which configuration options to import/export:

☑ ReportCenter options

☑ ReportPacks' custom, scheduled and favorite reports + options

Specify the path and filename of the file to import/export:

C:\Program Files\Common Files\GFI\ReportCenter\Framework v3.5\1.:

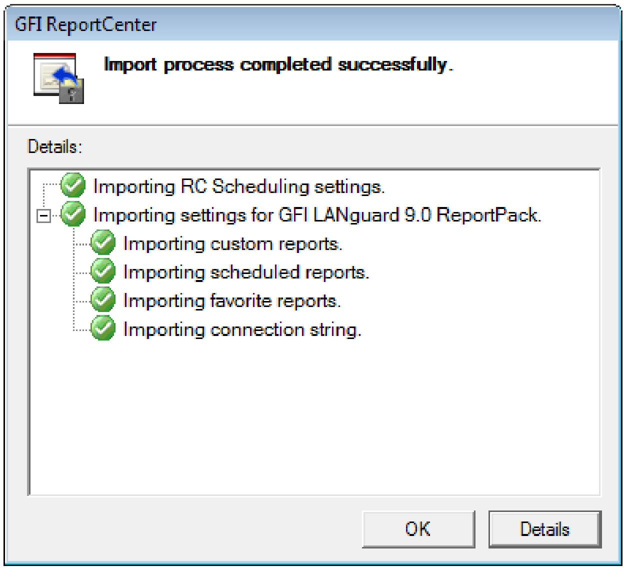
Screenshot 45 – Import configurations dialog

1. From the pull-down menu, click on the **File ▸ Import/Export Configuration…** . This will bring up the configuration dialog.

2. Select the option '***Import configurations options***'.

3. Specify which configuration options to import.

4. Specify the path and filename of the XML file to import. Click on **OK** to proceed with the import.

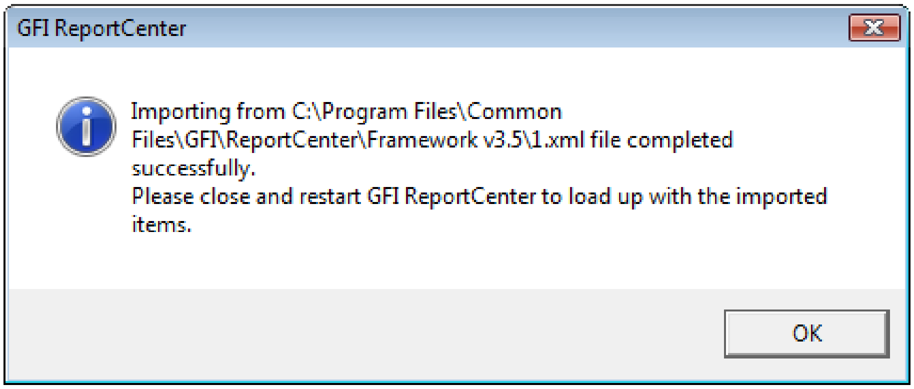


Import process completed successfully.

Details:

- ✓ Importing RC Scheduling settings.
- ✓ Importing settings for GFI LANguard 9.0 ReportPack.
  - ✓ Importing custom reports.
  - ✓ Importing scheduled reports.
  - ✓ Importing favorite reports.
  - ✓ Importing connection string.

Screenshot 46 – Import configuration success



Importing from C:\Program Files\Common Files\GFI\ReportCenter\Framework v3.5\1.xml file completed successfully.
Please close and restart GFI ReportCenter to load up with the imported items.

Screenshot 47 - Import configuration success - restart notification

5. Close and restart GFI ReportCenter to activate the imported items.

General options

Viewing the product ReportPack version details

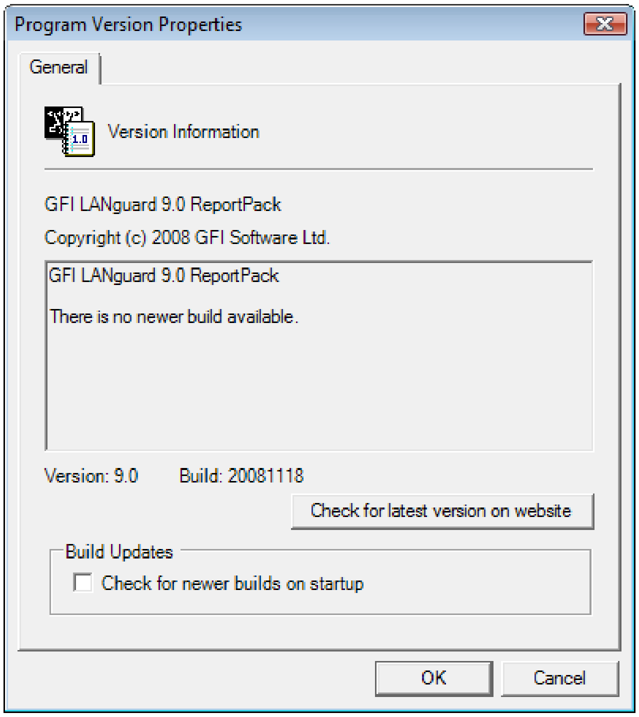
To view the version information of your product ReportPacks:

1. Select the product ReportPack from the **Product Selection** drop down list.

2. Click on the **Options** navigation button and select the **Version Information** node. The version details will be displayed in the right pane of the management console.

Checking the web for newer builds

Periodically GFI releases product and ReportPack updates which can be automatically downloaded from the GFI website. To check if a newer built is available for download:


Program Version Properties
General
Version Information

GFI LANguard 9.0 ReportPack

Copyright (c) 2008 GFI Software Ltd.

GFI LANguard 9.0 ReportPack

There is no newer build available.

Version: 9.0 Build: 20081118

Check for latest version on website
Build Updates

□ Check for newer builds on startup

Screenshot 48 - Version Properties: Check for newer builds dialog

1. Select the respective product (for example, GFI LANguard 9.0 Reports) from the **Product Selection** drop down list.

2. Click on the **Options** navigation button.

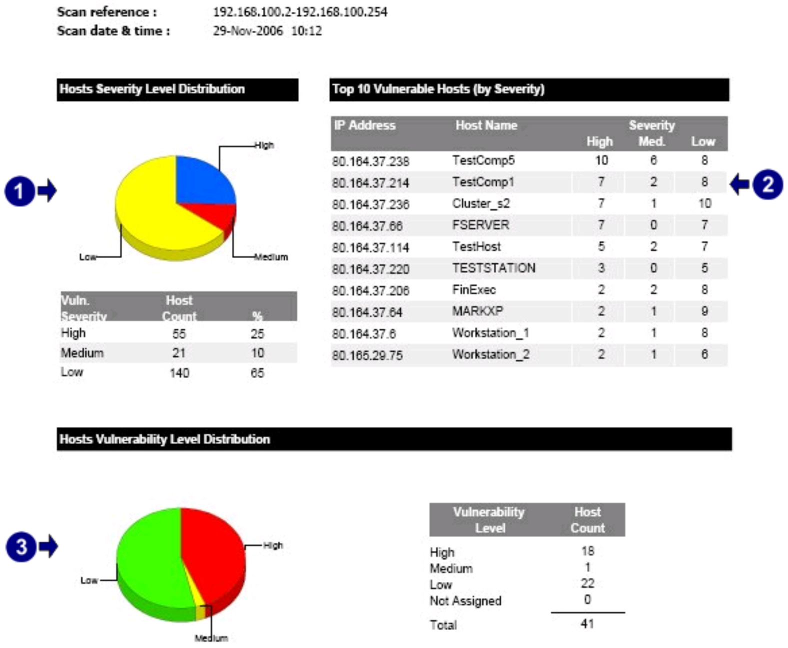
3. Right-click on the **Version Information** node and select **Checking for newer builds…**

NOTE: GFI LANguard 9.0 ReportPack is configured by default to check for newer builds on startup.

Appendix: GFI LANguard default reports

Vulnerability assessment reports

Network vulnerability summary



Scan reference : 192.168.100.2-192.168.100.254
Scan date & time : 29-Nov-2006 10:12

Hosts Severity Level Distribution

Vuln. Severity	Host Count	%
High	55	25
Medium	21	10
Low	140	65

Top 10 Vulnerable Hosts (by Severity)

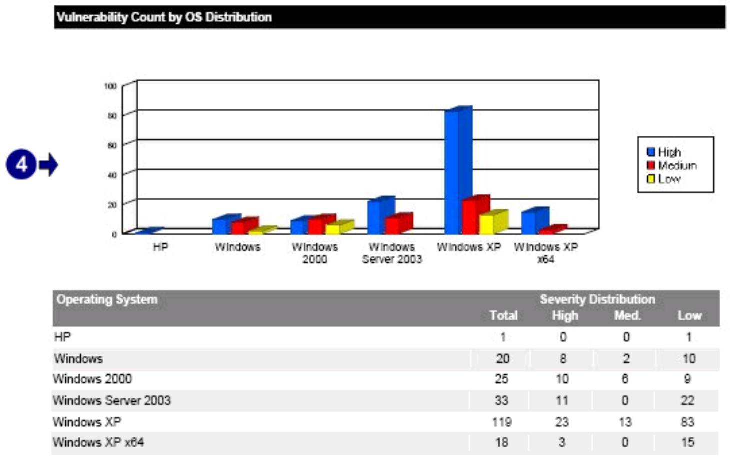
IP Address	Host Name	Severity		
		High	Med.	Low
80.164.37.238	TestComp5	10	6	8
80.164.37.214	TestComp1	7	2	8
80.164.37.236	Cluster_s2	7	1	10
80.164.37.66	FSERVER	7	0	7
80.164.37.114	TestHost	5	2	7
80.164.37.220	TESTSTATION	3	0	5
80.164.37.206	FinExec	2	2	8
80.164.37.64	MARKXP	2	1	9
80.164.37.6	Workstation_1	2	1	8
80.165.29.75	Workstation_2	2	1	6

Hosts Vulnerability Level Distribution

Vulnerability Level	Host Count
High	18
Medium	1
Low	22
Not Assigned	0
Total	41

Screenshot 49 – Sample report showing network vulnerability summary

1	Chart displaying vulnerability severity distributions
2	List showing the top 10 most vulnerable host machines ordered by severity
3	Chart displaying vulnerability level distributions across host machines on the network

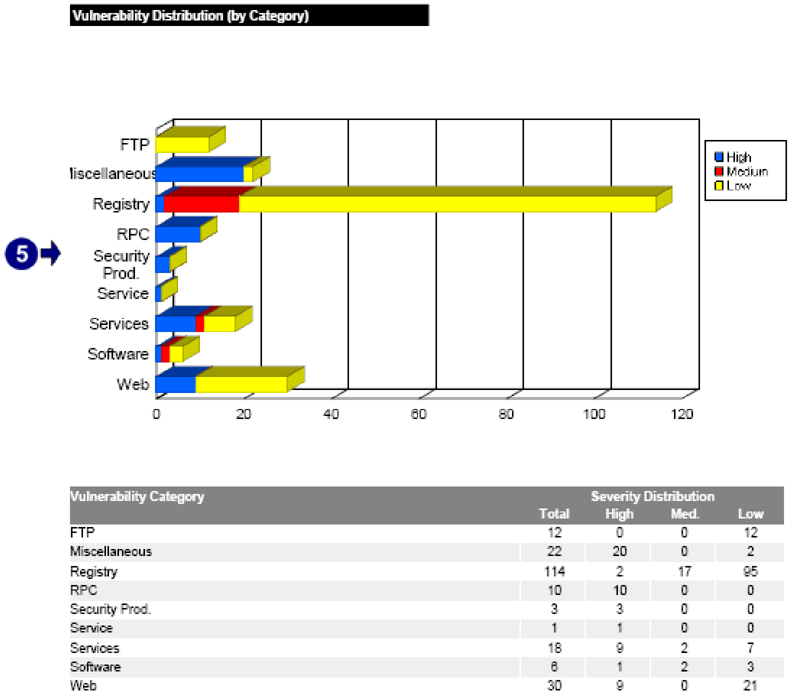


Vulnerability Count by OS Distribution

Operating System		Severity Distribution		
	Total	High	Med.	Low
HP	1	0	0	1
Windows	20	8	2	10
Windows 2000	25	10	6	9
Windows Server 2003	33	11	0	22
Windows XP	119	23	13	83
Windows XP x64	18	3	0	15

Screenshot 50 – Sample report showing network vulnerability summary

4	Chart displaying the vulnerability distribution for each operating system on the network

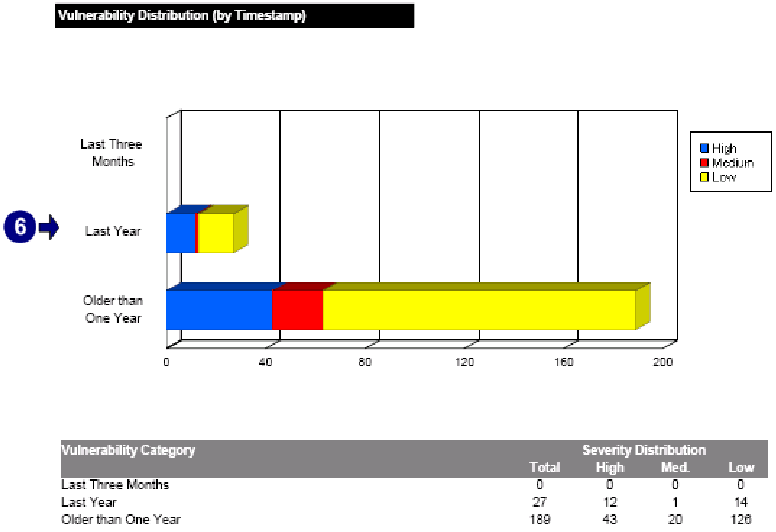


Vulnerability Distribution (by Category)

Vulnerability Category		Severity Distribution		
	Total	High	Med.	Low
FTP	12	0	0	12
Miscellaneous	22	20	0	2
Registry	114	2	17	95
RPC	10	10	0	0
Security Prod.	3	3	0	0
Service	1	1	0	0
Services	18	9	2	7
Software	6	1	2	3
Web	30	9	0	21

Screenshot 51 – Sample report showing network vulnerability summary

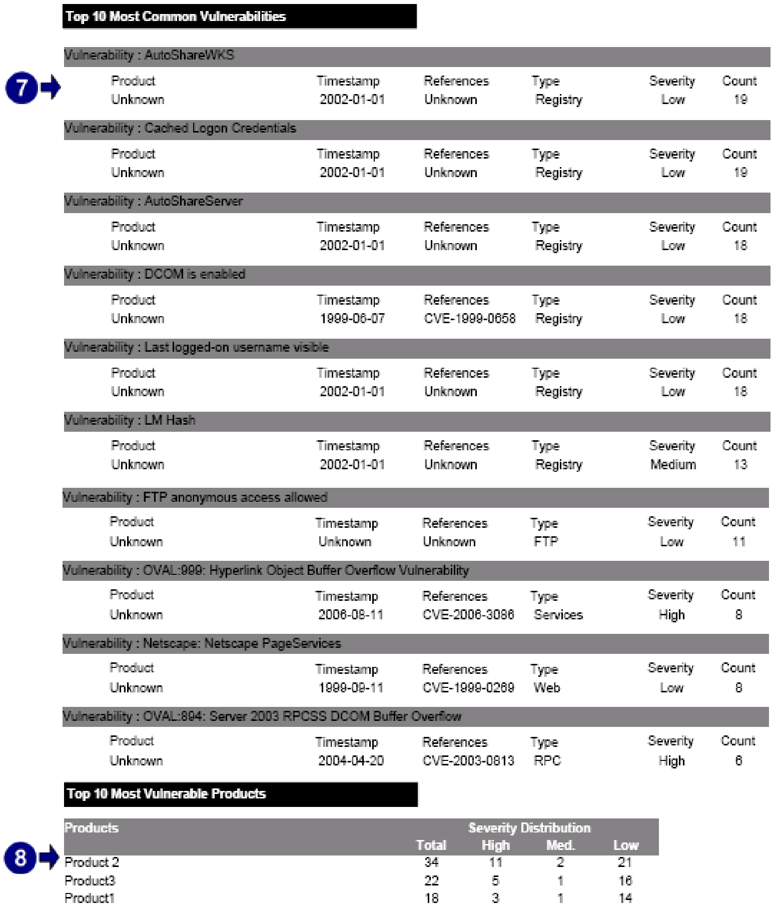
5	Chart displaying vulnerability categories and their distribution



Vulnerability Category		Severity Distribution		
	Total	High	Med.	Low
Last Three Months	0	0	0	0
Last Year	27	12	1	14
Older than One Year	189	43	20	126

Screenshot 52 – Sample report showing network vulnerability summary

6	Chart displaying the vulnerability distribution over time



Top 10 Most Common Vulnerabilities

Vulnerability : AutoShareWKS

Product	Timestamp	References	Type	Severity	Count
Unknown	2002-01-01	Unknown	Registry	Low	19

Vulnerability : Cached Logon Credentials

Product	Timestamp	References	Type	Severity	Count
Unknown	2002-01-01	Unknown	Registry	Low	19

Vulnerability : AutoShareServer

Product	Timestamp	References	Type	Severity	Count
Unknown	2002-01-01	Unknown	Registry	Low	18

Vulnerability : DCOM is enabled

Product	Timestamp	References	Type	Severity	Count
Unknown	1999-06-07	CVE-1999-0658	Registry	Low	18

Vulnerability : Last logged-on username visible

Product	Timestamp	References	Type	Severity	Count
Unknown	2002-01-01	Unknown	Registry	Low	18

Vulnerability : LM Hash

Product	Timestamp	References	Type	Severity	Count
Unknown	2002-01-01	Unknown	Registry	Medium	13

Vulnerability : FTP anonymous access allowed

Product	Timestamp	References	Type	Severity	Count
Unknown	Unknown	Unknown	FTP	Low	11

Vulnerability : OVAL:999: Hyperlink Object Buffer Overflow Vulnerability

Product	Timestamp	References	Type	Severity	Count
Unknown	2006-08-11	CVE-2006-3086	Services	High	8

Vulnerability : Netscape: Netscape PageServices

Product	Timestamp	References	Type	Severity	Count
Unknown	1999-09-11	CVE-1999-0269	Web	Low	8

Vulnerability : OVAL:894: Server 2003 RPCSS DCOM Buffer Overflow

Product	Timestamp	References	Type	Severity	Count
Unknown	2004-04-20	CVE-2003-0813	RPC	High	6

Top 10 Most Vulnerable Products

Products		Severity Distribution		
	Total	High	Med.	Low
Product 2	34	11	2	21
Product3	22	5	1	16
Product1	18	3	1	14

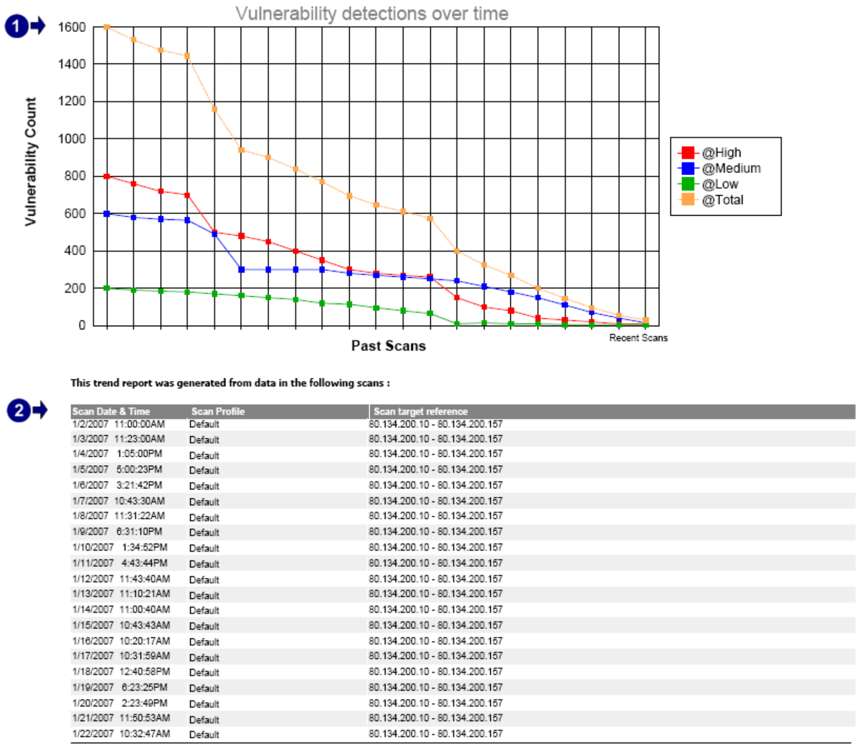
Screenshot 53 – Sample report showing network vulnerability summary

7	Chart displaying the 10 most common vulnerabilities
8	Chart displaying the 10 most vulnerable products

Use this report to:

- Display vulnerability counts for different categories
- Identify the 10 most vulnerable host machines
- Identify the 10 most vulnerable products
- Identify the 10 most common vulnerabilities.

Network vulnerability trend



This trend report was generated from data in the following scans :

Scan Date & Time	Scan Profile	Scan target reference
1/2/2007 11:00:00AM	Default	80.134.200.10 - 80.134.200.157
1/3/2007 11:23:00AM	Default	80.134.200.10 - 80.134.200.157
1/4/2007 1:05:00PM	Default	80.134.200.10 - 80.134.200.157
1/5/2007 5:00:23PM	Default	80.134.200.10 - 80.134.200.157
1/6/2007 3:21:42PM	Default	80.134.200.10 - 80.134.200.157
1/7/2007 10:43:30AM	Default	80.134.200.10 - 80.134.200.157
1/8/2007 11:31:22AM	Default	80.134.200.10 - 80.134.200.157
1/9/2007 6:31:10PM	Default	80.134.200.10 - 80.134.200.157
1/10/2007 1:34:52PM	Default	80.134.200.10 - 80.134.200.157
1/11/2007 4:43:44PM	Default	80.134.200.10 - 80.134.200.157
1/12/2007 11:43:40AM	Default	80.134.200.10 - 80.134.200.157
1/13/2007 11:10:21AM	Default	80.134.200.10 - 80.134.200.157
1/14/2007 11:00:40AM	Default	80.134.200.10 - 80.134.200.157
1/15/2007 10:43:43AM	Default	80.134.200.10 - 80.134.200.157
1/16/2007 10:20:17AM	Default	80.134.200.10 - 80.134.200.157
1/17/2007 10:31:59AM	Default	80.134.200.10 - 80.134.200.157
1/18/2007 12:40:58PM	Default	80.134.200.10 - 80.134.200.157
1/19/2007 6:23:25PM	Default	80.134.200.10 - 80.134.200.157
1/20/2007 2:23:49PM	Default	80.134.200.10 - 80.134.200.157
1/21/2007 11:50:53AM	Default	80.134.200.10 - 80.134.200.157
1/22/2007 10:32:47AM	Default	80.134.200.10 - 80.134.200.157

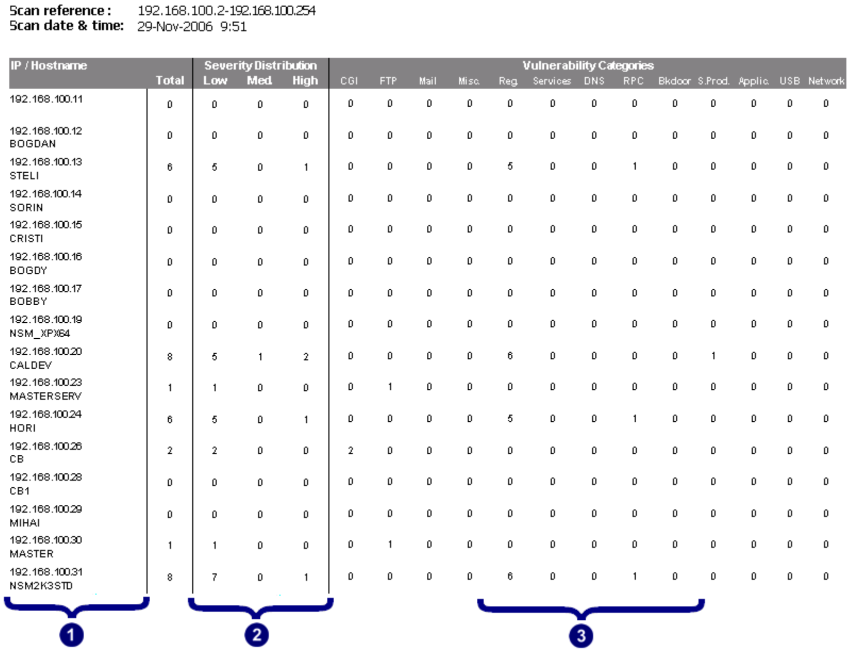
Screenshot 54 – Sample report showing network vulnerability trend

1	Chart displaying past scans and vulnerability totals for each scan
2	List of past scans and respective scan profiles

Use this report to:

- Graphically illustrate how the number of vulnerabilities on the network has changed over a given time span.

Vulnerability distribution by host



Scan reference : 192.168.100.2-192.168.100.254
Scan date & time: 29-Nov-2006 9:51

IP / Hostname		Severity Distribution			Vulnerability Categories												
	Total	Low	Med.	High	CGI	FTP	Mail	Misc.	Reg.	Services	DNS	RPC	Bkdoor	S.Prod.	Applic.	USB	Network
192.168.100.11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
192.168.100.12 BOGDAN	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
192.168.100.13 STELI	6	5	0	1	0	0	0	0	5	0	0	1	0	0	0	0	0
192.168.100.14 SORIN	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
192.168.100.15 CRISTI	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
192.168.100.16 BOGDY	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
192.168.100.17 BOBBY	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
192.168.100.19 NSM_XPX64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
192.168.100.20 CALDEV	8	5	1	2	0	0	0	0	6	0	0	0	0	1	0	0	0
192.168.100.23 MASTERSERV	1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
192.168.100.24 HORI	6	5	0	1	0	0	0	0	5	0	0	1	0	0	0	0	0
192.168.100.26 CB	2	2	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0
192.168.100.28 CB1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
192.168.100.29 MIHAI	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
192.168.100.30 MASTER	1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
192.168.100.31 NSM2K3STD	8	7	0	1	0	0	0	0	6	0	0	1	0	0	0	0	0

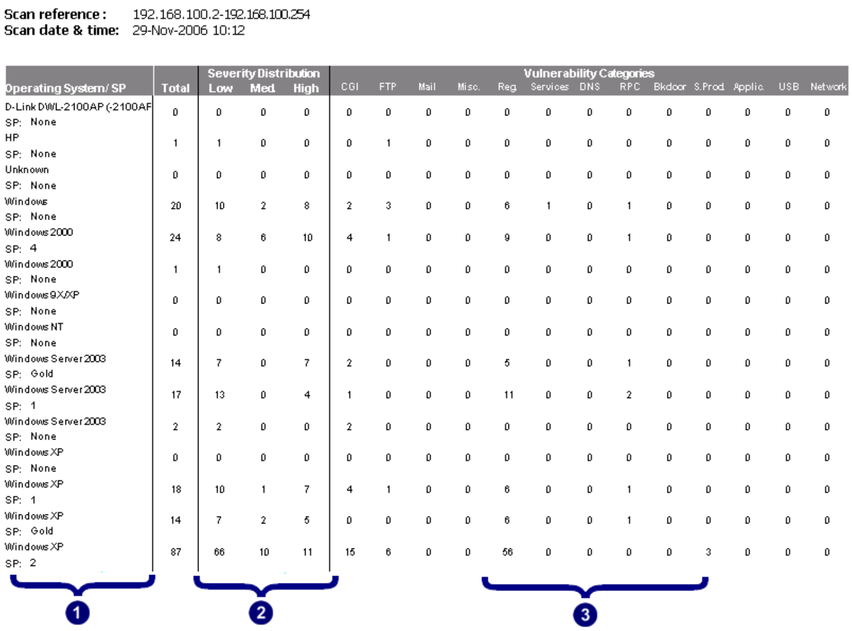
Screenshot 55 – Sample report showing vulnerability distribution by host

1	List of IP addresses and host names on which vulnerabilities were detected
2	The number of low, medium and high severity vulnerabilities detected on each host
3	The number of vulnerabilities detected on each host distributed by vulnerability category

Use this report to:

- Generate statistics showing vulnerability counts for each host machine.

Vulnerability distribution by operating system



Scan reference : 192.168.100.2-192.168.100.254
Scan date & time: 29-Nov-2006 10:12

		Severity Distribution								Vulnerability Categories							
Operating System/ SP	**Total**	**Low**	**Med.**	**High**	CGI	FTP	Mail	Misc.	Reg.	Services	DNS	RPC	Bkdoor	S.Prod.	Applic.	USB	Network
D-Link DWL-2100AP (-2100AF SP: None	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
HP SP: None	1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
Unknown SP: None	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Windows SP: None	20	10	2	8	2	3	0	0	6	1	0	1	0	0	0	0	0
Windows 2000 SP: 4	24	8	6	10	4	1	0	0	9	0	0	1	0	0	0	0	0
Windows 2000 SP: None	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Windows 9X/XP SP: None	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Windows NT SP: None	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Windows Server 2003 SP: Gold	14	7	0	7	2	0	0	0	5	0	0	1	0	0	0	0	0
Windows Server 2003 SP: 1	17	13	0	4	1	0	0	0	11	0	0	2	0	0	0	0	0
Windows Server 2003 SP: None	2	2	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0
Windows XP SP: None	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Windows XP SP: 1	18	10	1	7	4	1	0	0	6	0	0	1	0	0	0	0	0
Windows XP SP: Gold	14	7	2	5	0	0	0	0	6	0	0	1	0	0	0	0	0
Windows XP SP: 2	87	66	10	11	15	6	0	0	56	0	0	0	0	3	0	0	0

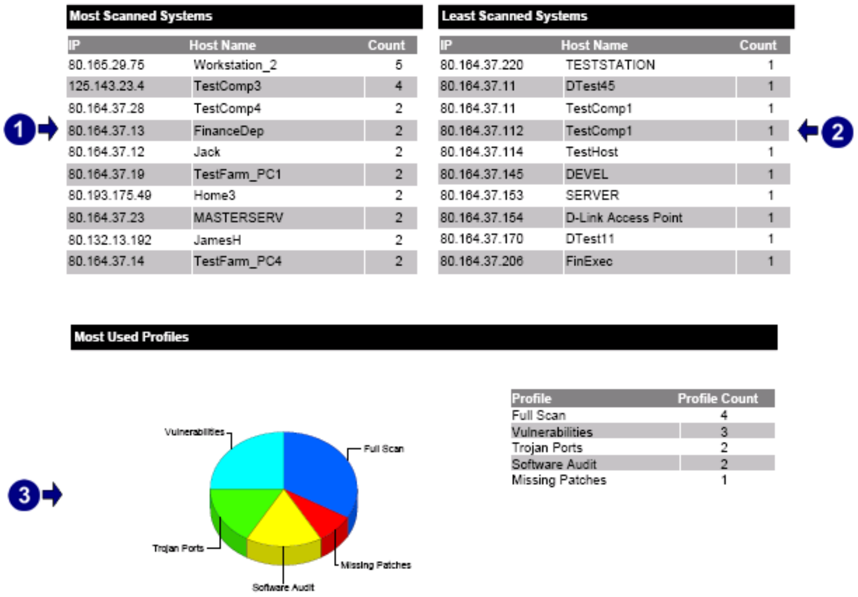
Screenshot 56 – Sample report showing vulnerability distribution by operating system

1	List of operating systems and service packs affected by one or more vulnerabilities
2	The number of low, medium and high severity vulnerabilities detected on each operating system
3	The number of vulnerabilities detected on each operating system distributed by vulnerability category

Use this report to:

- Generate statistics showing vulnerability counts for each operating system.

Security scans history



Most Scanned Systems

IP	Host Name	Count
80.165.29.75	Workstation_2	5
125.143.23.4	TestComp3	4
80.164.37.28	TestComp4	2
80.164.37.13	FinanceDep	2
80.164.37.12	Jack	2
80.164.37.19	TestFarm_PC1	2
80.193.175.49	Home3	2
80.164.37.23	MASTERSERV	2
80.132.13.192	JamesH	2
80.164.37.14	TestFarm_PC4	2

Least Scanned Systems

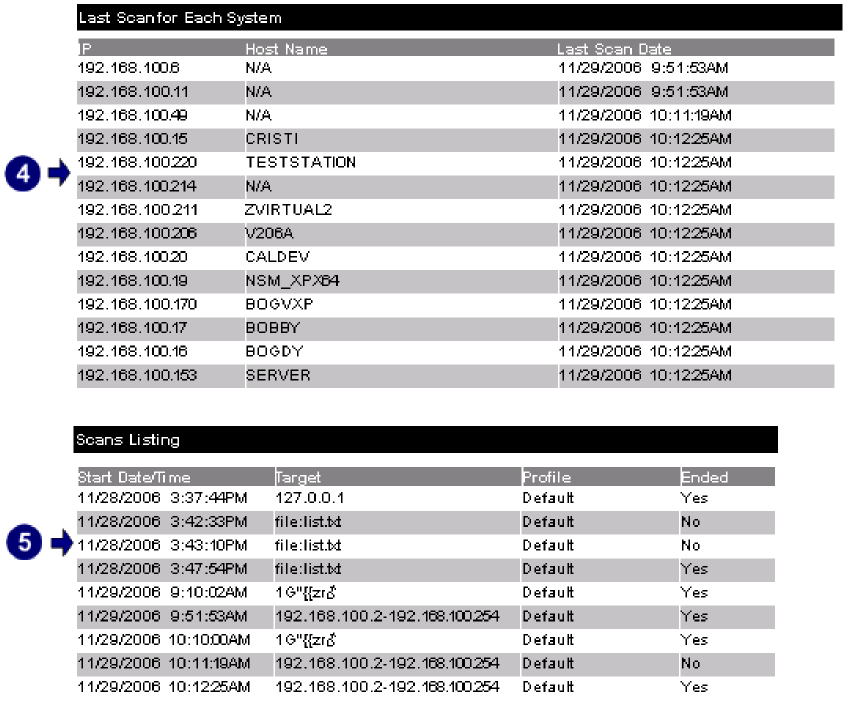
IP	Host Name	Count
80.164.37.220	TESTSTATION	1
80.164.37.11	DTest45	1
80.164.37.11	TestComp1	1
80.164.37.112	TestComp1	1
80.164.37.114	TestHost	1
80.164.37.145	DEVEL	1
80.164.37.153	SERVER	1
80.164.37.154	D-Link Access Point	1
80.164.37.170	DTest11	1
80.164.37.206	FinExec	1

Most Used Profiles

Profile	Profile Count
Full Scan	4
Vulnerabilities	3
Trojan Ports	2
Software Audit	2
Missing Patches	1

Screenshot 57 – Sample report showing security scans history

1	List showing the host machines with the highest number of scans and the respective scan count
2	List showing the host machines with the lowest number of scans and the respective scan count
3	Chart displaying scan profile usage



Last Scan for Each System

IP	Host Name	Last Scan Date
192.168.100.8	N/A	11/29/2006 9:51:53AM
192.168.100.11	N/A	11/29/2006 9:51:53AM
192.168.100.49	N/A	11/29/2006 10:11:19AM
192.168.100.15	CRISTI	11/29/2006 10:12:25AM
192.168.100.220	TESTSTATION	11/29/2006 10:12:25AM
192.168.100.214	N/A	11/29/2006 10:12:25AM
192.168.100.211	ZVIRTUAL2	11/29/2006 10:12:25AM
192.168.100.206	V206A	11/29/2006 10:12:25AM
192.168.100.20	CALDEV	11/29/2006 10:12:25AM
192.168.100.19	NSM_XP64	11/29/2006 10:12:25AM
192.168.100.170	BOGVXP	11/29/2006 10:12:25AM
192.168.100.17	BOBBY	11/29/2006 10:12:25AM
192.168.100.16	BOGDY	11/29/2006 10:12:25AM
192.168.100.153	SERVER	11/29/2006 10:12:25AM

Scans Listing

Start Date/Time	Target	Profile	Ended
11/28/2006 3:37:44PM	127.0.0.1	Default	Yes
11/28/2006 3:42:33PM	file:list.txt	Default	No
11/28/2006 3:43:10PM	file:list.txt	Default	No
11/28/2006 3:47:54PM	file:list.txt	Default	Yes
11/29/2006 9:10:02AM	1G"{{zrծ	Default	Yes
11/29/2006 9:51:53AM	192.168.100.2-192.168.100.254	Default	Yes
11/29/2006 10:10:00AM	1G"{{zrծ	Default	Yes
11/29/2006 10:11:19AM	192.168.100.2-192.168.100.254	Default	No
11/29/2006 10:12:25AM	192.168.100.2-192.168.100.254	Default	Yes

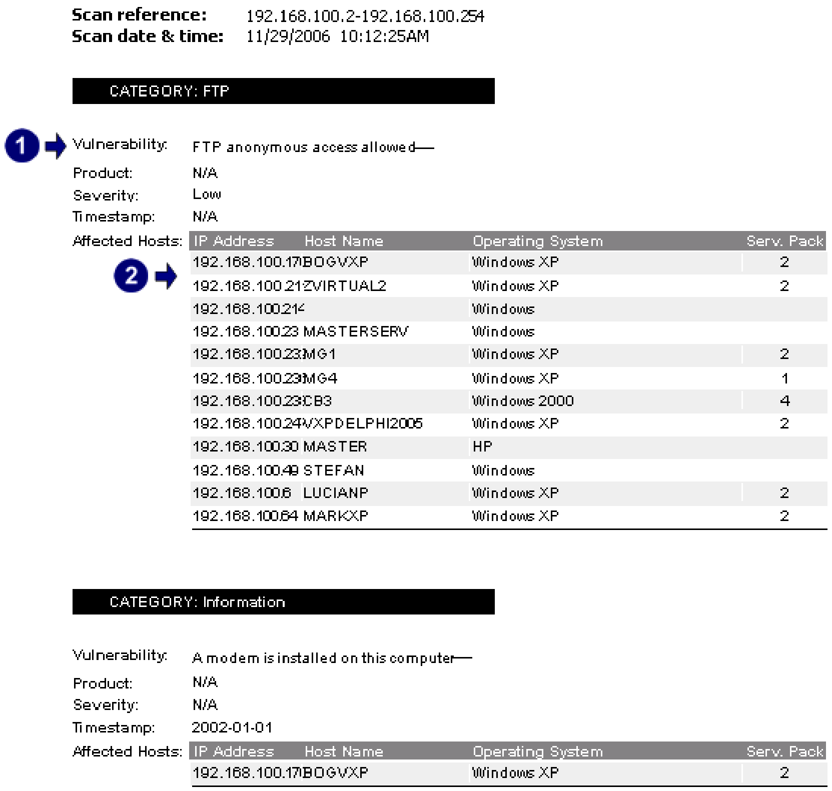
Screenshot 58 – Sample report showing security scans history

4	List showing date and time of the last scan performed on each host
5	List showing all scans performed

Use this report to:

- Display information and statistics on all network security scans performed.

Vulnerability listing by category



Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 11/29/2006 10:12:25AM

CATEGORY: FTP

Vulnerability: FTP anonymous access allowed
Product: N/A
Severity: Low
Timestamp: N/A
Affected Hosts:

IP Address	Host Name	Operating System	Serv. Pack
192.168.100.17	BOGVXP	Windows XP	2
192.168.100.21	ZVIRTUAL2	Windows XP	2
192.168.100.214		Windows	
192.168.100.23	MASTERSERV	Windows	
192.168.100.23	MG1	Windows XP	2
192.168.100.23	MG4	Windows XP	1
192.168.100.23	CB3	Windows 2000	4
192.168.100.24	VXPDELPHI2005	Windows XP	2
192.168.100.30	MASTER	HP	
192.168.100.49	STEFAN	Windows	
192.168.100.6	LUCIANP	Windows XP	2
192.168.100.64	MARKXP	Windows XP	2

CATEGORY: Information

Vulnerability: A modem is installed on this computer
Product: N/A
Severity: N/A
Timestamp: 2002-01-01
Affected Hosts:

IP Address	Host Name	Operating System	Serv. Pack
192.168.100.17	BOGVXP	Windows XP	2

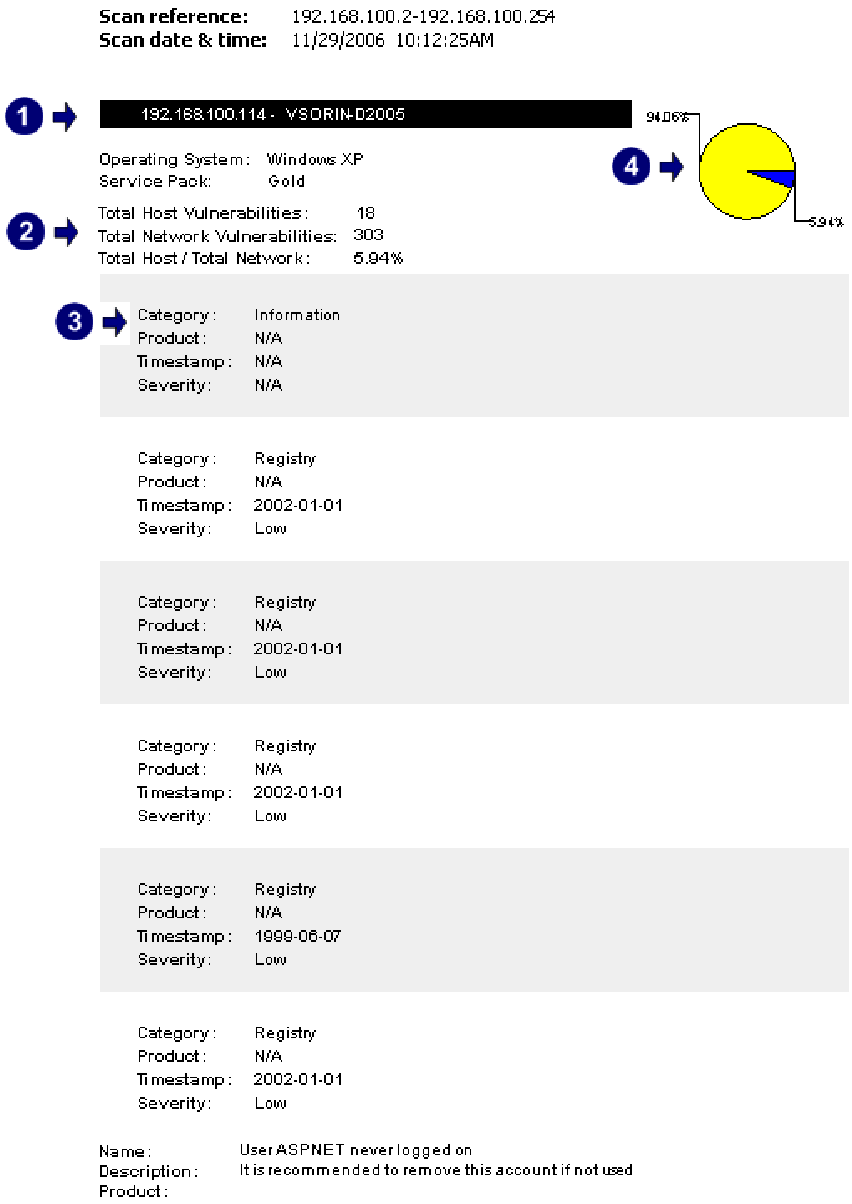
Screenshot 59 – Sample report showing vulnerability listing by category

1	Vulnerability details including name, description and severity
2	List of host machines affected by each vulnerability detected

Use this report to:

- List detected vulnerabilities grouped by category, and the host machines affected by each vulnerability.

Vulnerability listing by host



Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 11/29/2006 10:12:25AM

192.168.100.114 - VSORIN-D2005

Operating System: Windows XP
Service Pack: Gold

Total Host Vulnerabilities: 18
Total Network Vulnerabilities: 303
Total Host / Total Network: 5.94%

Category: Information
Product: N/A
Timestamp: N/A
Severity: N/A

Category: Registry
Product: N/A
Timestamp: 2002-01-01
Severity: Low

Category: Registry
Product: N/A
Timestamp: 2002-01-01
Severity: Low

Category: Registry
Product: N/A
Timestamp: 2002-01-01
Severity: Low

Category: Registry
Product: N/A
Timestamp: 1999-06-07
Severity: Low

Category: Registry
Product: N/A
Timestamp: 2002-01-01
Severity: Low

Name: User ASPNET never logged on
Description: It is recommended to remove this account if not used
Product:

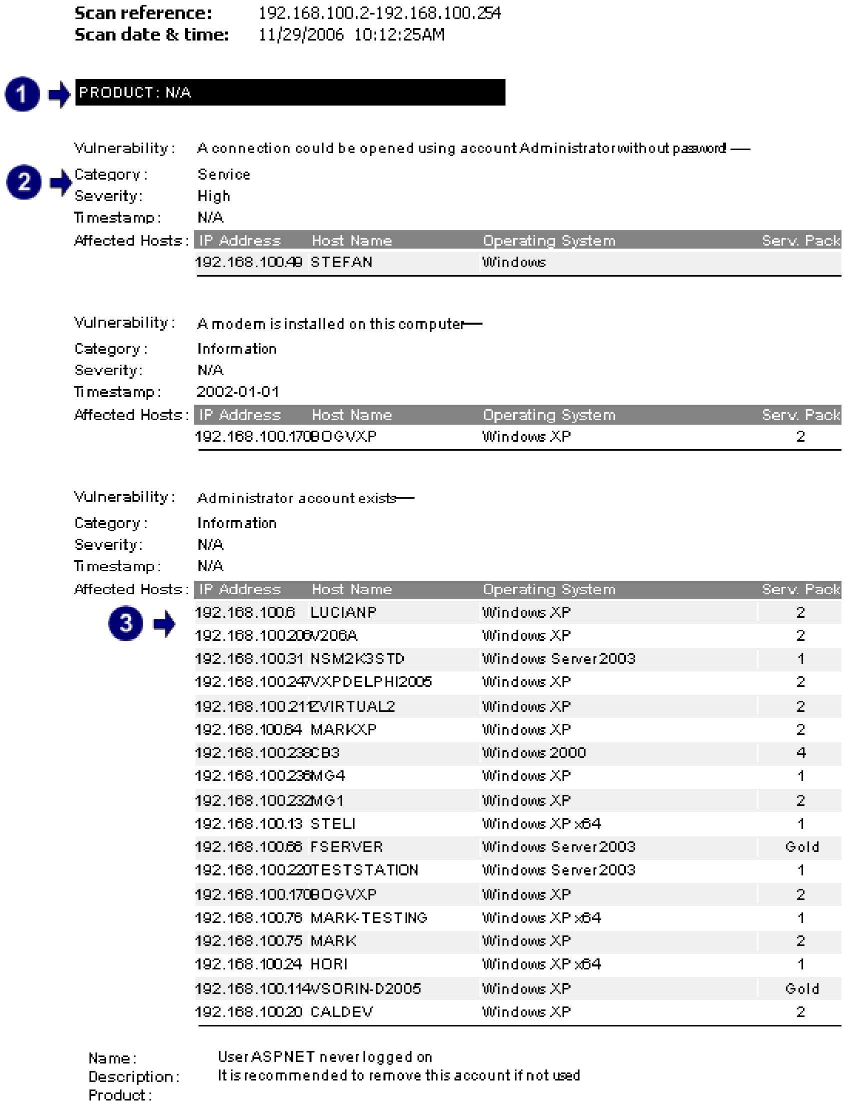
Screenshot 60 – Sample report showing vulnerability listing by host

1	Host machine details on which vulnerabilities were detected
2	Vulnerability count for each host, also shown as a percentage of total vulnerabilities detected on the network
3	List of vulnerability details for each host, including name, description and severity
4	Chart displaying percentage of vulnerabilities detected on each host compared to total vulnerabilities detected on the network

Use this report to:

- List the vulnerabilities detected for each host machine on the network.

Vulnerability listing by product



Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 11/29/2006 10:12:25AM

PRODUCT : N/A

Vulnerability : A connection could be opened using account Administrator without pasword
Category : Service
Severity: High
Timestamp : N/A
Affected Hosts :

IP Address	Host Name	Operating System	Serv. Pack
192.168.100.49	STEFAN	Windows	

Vulnerability : A modem is installed on this computer
Category : Information
Severity: N/A
Timestamp : 2002-01-01
Affected Hosts :

IP Address	Host Name	Operating System	Serv. Pack
192.168.100.170	BOGVXP	Windows XP	2

Vulnerability : Administrator account exists
Category : Information
Severity: N/A
Timestamp : N/A
Affected Hosts :

IP Address	Host Name	Operating System	Serv. Pack
192.168.100.6	LUCIANP	Windows XP	2
192.168.100.206	V206A	Windows XP	2
192.168.100.31	NSM2K3STD	Windows Server 2003	1
192.168.100.247	VXPDELPHI2005	Windows XP	2
192.168.100.212	VIRTUAL2	Windows XP	2
192.168.100.64	MARKXP	Windows XP	2
192.168.100.238	CB3	Windows 2000	4
192.168.100.236	MG4	Windows XP	1
192.168.100.232	MG1	Windows XP	2
192.168.100.13	STELI	Windows XP x64	1
192.168.100.66	FSERVER	Windows Server 2003	Gold
192.168.100.220	TESTSTATION	Windows Server 2003	1
192.168.100.170	BOGVXP	Windows XP	2
192.168.100.76	MARK-TESTING	Windows XP x64	1
192.168.100.75	MARK	Windows XP	2
192.168.100.24	HORI	Windows XP x64	1
192.168.100.114	VSORIN-D2005	Windows XP	Gold
192.168.100.20	CALDEV	Windows XP	2

Name : User ASPNET never logged on
Description : It is recommended to remove this account if not used
Product :

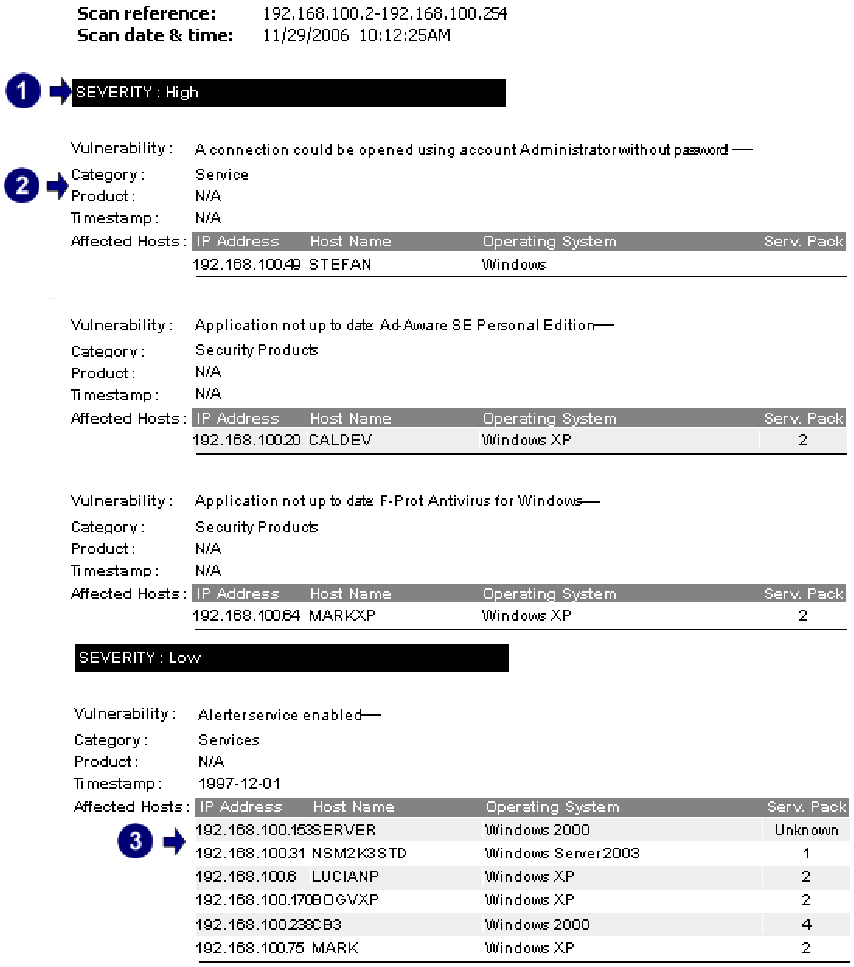
Screenshot 61 – Sample report showing vulnerability listing by product

1	Name of product for which vulnerabilities were detected
2	Vulnerability details for each product, including name, description and severity
3	List of host machines affected by each product vulnerability detected

Use this report to:

- List detected vulnerabilities grouped by product, and the host machines affected by each vulnerability.

Vulnerability listing by severity



Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 11/29/2006 10:12:25AM

SEVERITY : High

Vulnerability : A connection could be opened using account Administrator without password
Category : Service
Product : N/A
Timestamp : N/A
Affected Hosts :

IP Address	Host Name	Operating System	Serv. Pack
192.168.100.49	STEFAN	Windows	

Vulnerability : Application not up to date Ad-Aware SE Personal Edition
Category : Security Products
Product : N/A
Timestamp : N/A
Affected Hosts :

IP Address	Host Name	Operating System	Serv. Pack
192.168.100.20	CALDEV	Windows XP	2

Vulnerability : Application not up to date F-Prot Antivirus for Windows
Category : Security Products
Product : N/A
Timestamp : N/A
Affected Hosts :

IP Address	Host Name	Operating System	Serv. Pack
192.168.100.64	MARKXP	Windows XP	2

SEVERITY : Low

Vulnerability : Alerter service enabled
Category : Services
Product : N/A
Timestamp : 1997-12-01
Affected Hosts :

IP Address	Host Name	Operating System	Serv. Pack
192.168.100.153	SERVER	Windows 2000	Unknown
192.168.100.31	NSM2K3STD	Windows Server 2003	1
192.168.100.6	LUCIANP	Windows XP	2
192.168.100.170	BOGVXP	Windows XP	2
192.168.100.238	CB3	Windows 2000	4
192.168.100.75	MARK	Windows XP	2

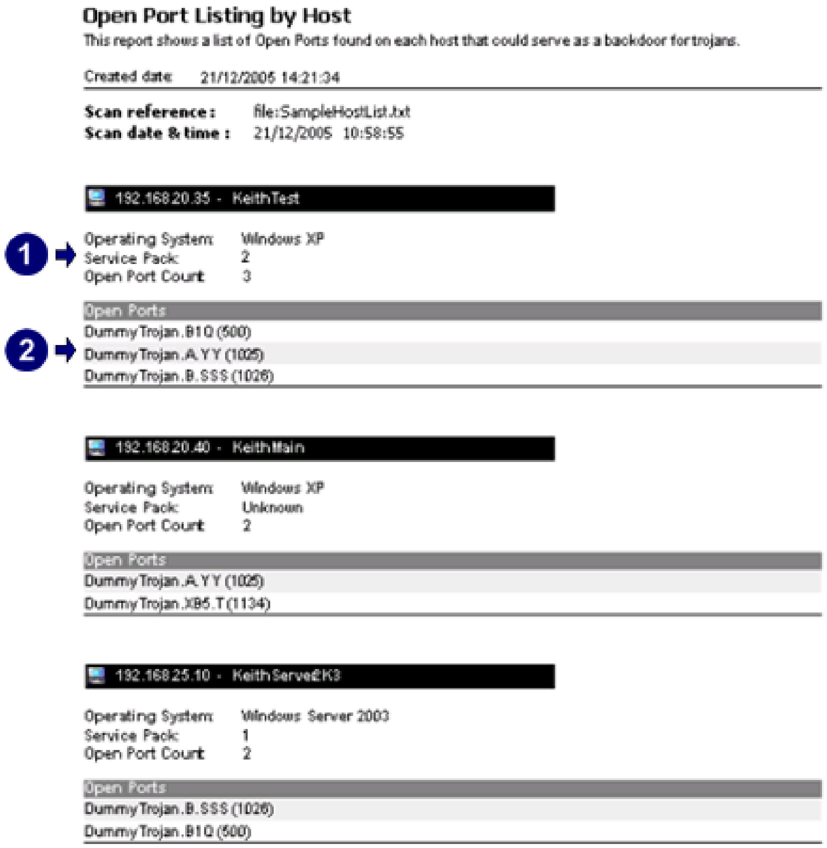
Screenshot 62 – Sample report showing vulnerability listing by severity

1	Severity level
2	Vulnerability details for each severity level, including name and description
3	List of host machines affected by vulnerabilities detected for each security level

Use this report to:

- List detected vulnerabilities grouped by severity, and the host machines affected by each vulnerability.

Open Trojan ports by host



Open Port Listing by Host

This report shows a list of Open Ports found on each host that could serve as a backdoor for trojans.

Created date 21/12/2005 14:21:34

Scan reference : file:SampleHostList.txt
Scan date & time : 21/12/2005 10:58:55

192.168.20.35 - KeithTest

Operating System:	Windows XP
Service Pack:	2
Open Port Count	3

Open Ports
DummyTrojan.B1Q (500)
DummyTrojan.A.YY (1025)
DummyTrojan.B.SSS (1026)

192.168.20.40 - KeithMain

Operating System:	Windows XP
Service Pack:	Unknown
Open Port Count	2

Open Ports
DummyTrojan.A.YY (1025)
DummyTrojan.XB5.T (1134)

192.168.25.10 - KeithServer2K3

Operating System:	Windows Server 2003
Service Pack:	1
Open Port Count	2

Open Ports
DummyTrojan.B.SSS (1026)
DummyTrojan.B1Q (500)

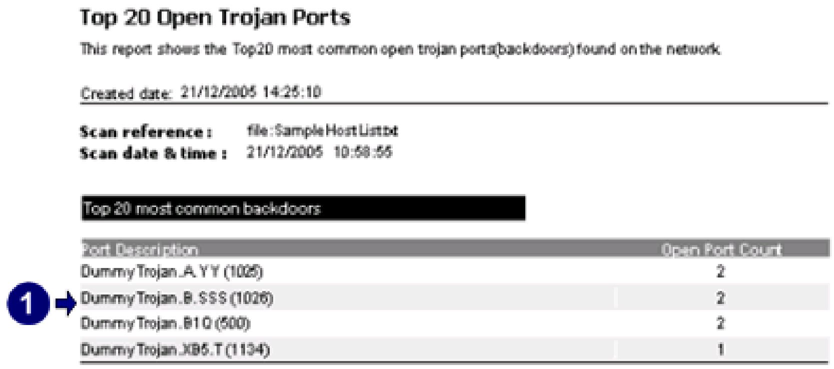
Screenshot 63 – Sample report showing open Trojan ports by cost

1	Details of host machines having open ports associated with trojans
2	List of open ports for each host and the names of trojans targeting each port

Use this report to:

- List open ports, grouped by host machine, which could potentially serve as a backdoor for trojans.

Open Trojan ports



Top 20 Open Trojan Ports

This report shows the Top20 most common open trojan ports(backdoors) found on the network.

Created date: 21/12/2005 14:25:10

Scan reference : file:SampleHostListtxt
Scan date & time : 21/12/2005 10:58:55

Top 20 most common backdoors

Port Description	Open Port Count
DummyTrojan.A.YY (1025)	2
DummyTrojan.B.SSS (1026)	2
DummyTrojan.B1Q (500)	2
DummyTrojan.XB5.T (1134)	1

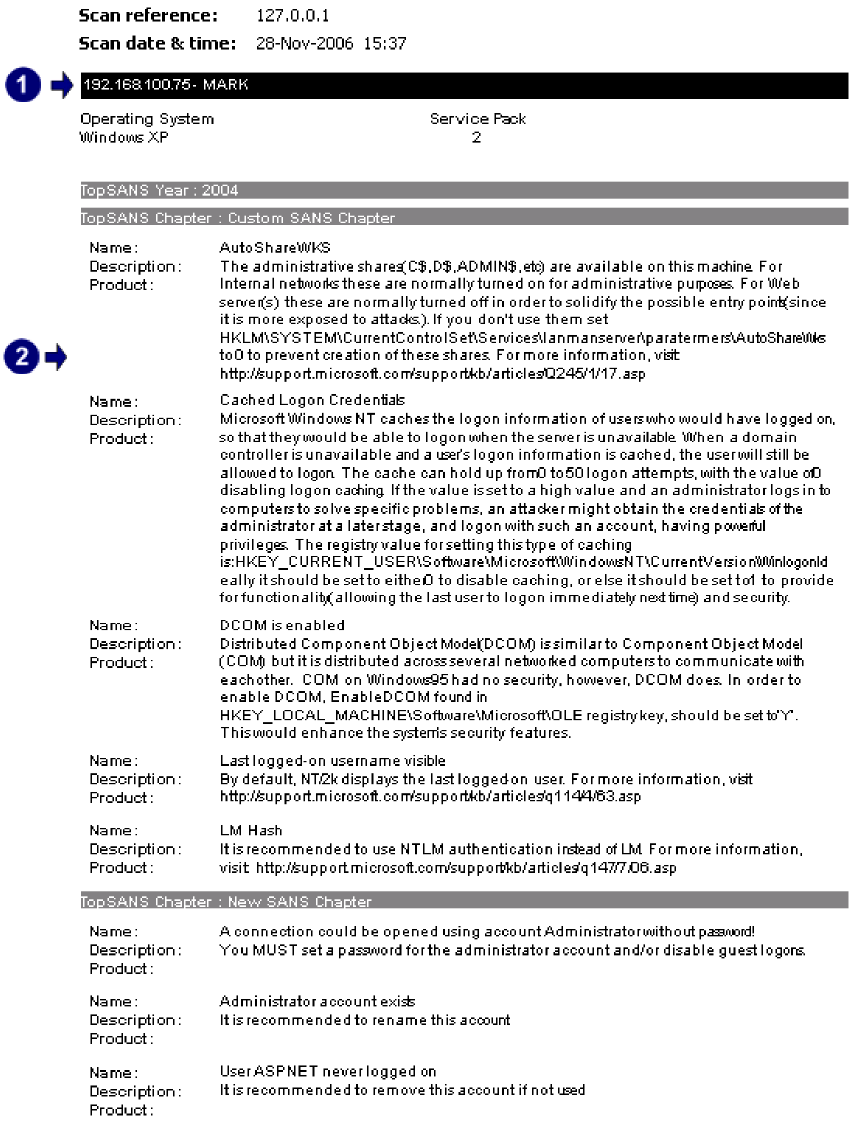
Screenshot 64 – Sample report showing open Trojan ports

1	List showing the most common open Trojan ports detected on the network

Use this report to:

- List the 20 most common open ports found on the network, which could potentially serve as a backdoor for trojans.

Top SANS vulnerabilities status



```
Scan reference:     127.0.0.1
Scan date & time:   28-Nov-2006  15:37

192.168.100.75- MARK

Operating System                          Service Pack
Windows XP                                     2

TopSANS Year : 2004
TopSANS Chapter : Custom SANS Chapter

 Name :          AutoShareWKS
 Description :   The administrative shares(C$,D$,ADMIN$,etc) are available on this machine. For
 Product :       Internal networks these are normally turned on for administrative purposes. For Web
                 server(s) these are normally turned off in order to solidify the possible entry points(since
                 it is more exposed to attacks). If you don't use them set
                 HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\paratermers\AutoShareWks
                 to0 to prevent creation of these shares. For more information, visit
                 http://support.microsoft.com/support/kb/articles/Q245/1/17.asp

 Name :          Cached Logon Credentials
 Description :   Microsoft Windows NT caches the logon information of users who would have logged on,
 Product :       so that they would be able to logon when the server is unavailable. When a domain
                 controller is unavailable and a user's logon information is cached, the user will still be
                 allowed to logon. The cache can hold up from0 to50 logon attempts, with the value of0
                 disabling logon caching. If the value is set to a high value and an administrator logs in to
                 computers to solve specific problems, an attacker might obtain the credentials of the
                 administrator at a later stage, and logon with such an account, having powerful
                 privileges. The registry value for setting this type of caching
                 is:HKEY_CURRENT_USER\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\Id
                 eally it should be set to either0 to disable caching, or else it should be set to1 to provide
                 for functionality(allowing the last user to logon immediately next time) and security.

 Name :          DCOM is enabled
 Description :   Distributed Component Object Model(DCOM) is similar to Component Object Model
 Product :       (COM) but it is distributed across several networked computers to communicate with
                 eachother.  COM on Windows95 had no security, however, DCOM does. In order to
                 enable DCOM, EnableDCOM found in
                 HKEY_LOCAL_MACHINE\Software\Microsoft\OLE registry key, should be set to'Y'.
                 This would enhance the system's security features.

 Name :          Last logged-on username visible
 Description :   By default, NT/2k displays the last logged-on user. For more information, visit
 Product :       http://support.microsoft.com/support/kb/articles/q114/4/63.asp

 Name :          LM Hash
 Description :   It is recommended to use NTLM authentication instead of LM. For more information,
 Product :       visit  http://support.microsoft.com/support/kb/articles/q147/7/06.asp

TopSANS Chapter : New SANS Chapter

 Name :          A connection could be opened using account Administrator without password!
 Description :   You MUST set a password for the administrator account and/or disable guest logons.
 Product :

 Name :          Administrator account exists
 Description :   It is recommended to rename this account
 Product :

 Name :          User ASPNET never logged on
 Description :   It is recommended to remove this account if not used
 Product :
```

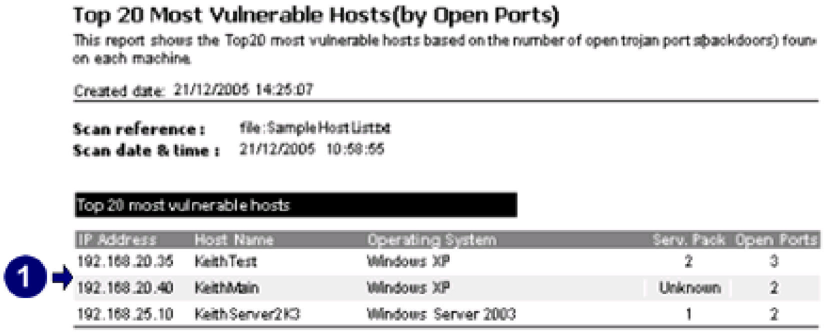
Screenshot 65 – Sample report showing top SANS vulnerabilities status

1	Host machine details on which vulnerabilities reported by SANS were detected
2	List showing SANS vulnerability details, including name, description and product affected. SANS vulnerabilities are grouped by year and chapter

Use this report to:

- List the vulnerabilities detected for each host machine, based on the SANS top-20 report of vulnerabilities.

Vulnerable hosts based on open ports



Top 20 Most Vulnerable Hosts(by Open Ports)

This report shows the Top20 most vulnerable hosts based on the number of open trojan ports(backdoors) foun on each machine.

Created date: 21/12/2005 14:25:07

Scan reference : file:SampleHostList.txt
Scan date & time : 21/12/2005 10:58:55

Top 20 most vulnerable hosts

IP Address	Host Name	Operating System	Serv. Pack	Open Ports
192.168.20.35	KeithTest	Windows XP	2	3
192.168.20.40	KeithMain	Windows XP	Unknown	2
192.168.25.10	KeithServer2K3	Windows Server 2003	1	2

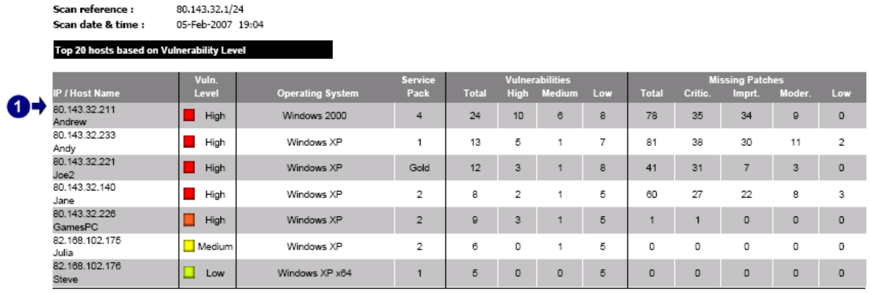
Screenshot 66 – Sample report showing vulnerable hosts based on open ports

1	List showing the top 20 host machines most likely to be compromised by trojans

Use this report to:

- List the 20 most vulnerable host machines, based on the number of open Trojan ports found.

Vulnerable hosts based on vulnerability level



Scan reference : 80.143.32.1/24
Scan date & time : 05-Feb-2007 19:04

Top 20 hosts based on Vulnerability Level

	Vuln.		Service		Vulnerabilities				Missing Patches			
IP / Host Name	Level	Operating System	Pack	Total	High	Medium	Low	Total	Critic.	Imprt.	Moder.	Low
80.143.32.211 Andrew	🟥 High	Windows 2000	4	24	10	6	8	78	35	34	9	0
80.143.32.233 Andy	🟥 High	Windows XP	1	13	5	1	7	81	38	30	11	2
80.143.32.221 Joe2	🟥 High	Windows XP	Gold	12	3	1	8	41	31	7	3	0
80.143.32.140 Jane	🟥 High	Windows XP	2	8	2	1	5	60	27	22	8	3
80.143.32.226 GamesPC	🟧 High	Windows XP	2	9	3	1	5	1	1	0	0	0
82.168.102.175 Julia	🟨 Medium	Windows XP	2	6	0	1	5	0	0	0	0	0
82.168.102.176 Steve	🟩 Low	Windows XP x64	1	5	0	0	5	0	0	0	0	0

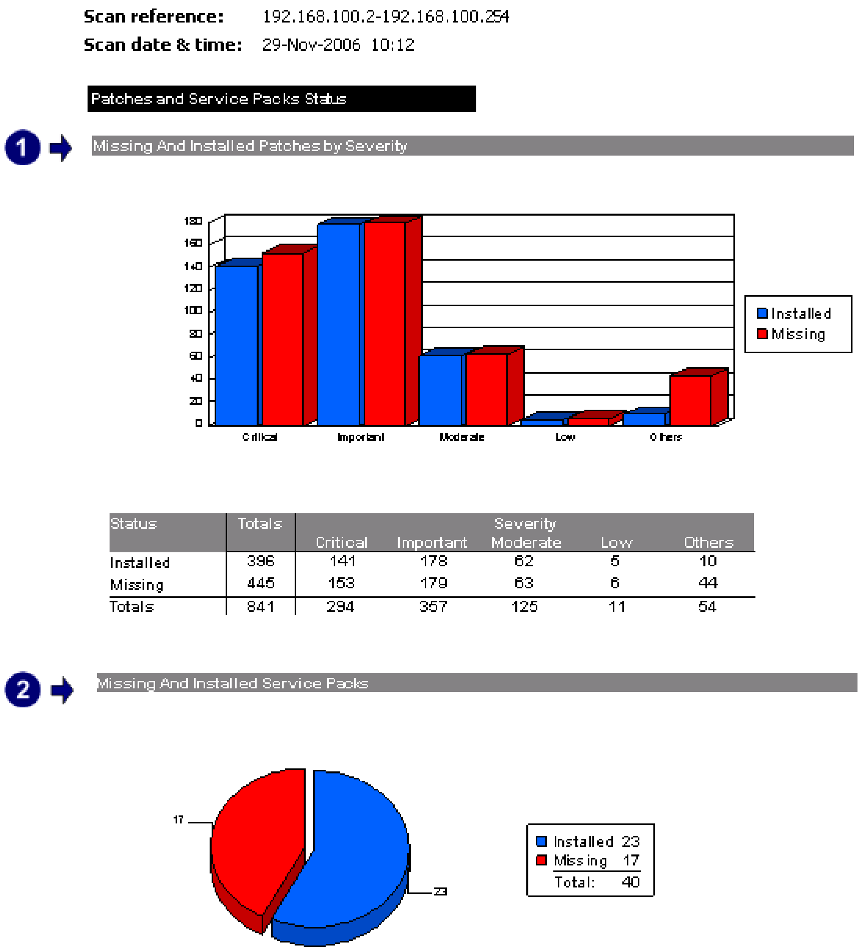
Screenshot 67 – Sample report showing vulnerable hosts based on vulnerability level

1	Host machine details showing the number of vulnerabilities and missing patches detected according to criticality

Use this report to:

- List the 20 most vulnerable host machines for each network security scan, based on vulnerability level.

Network patching status



Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 29-Nov-2006 10:12

Patches and Service Packs Status

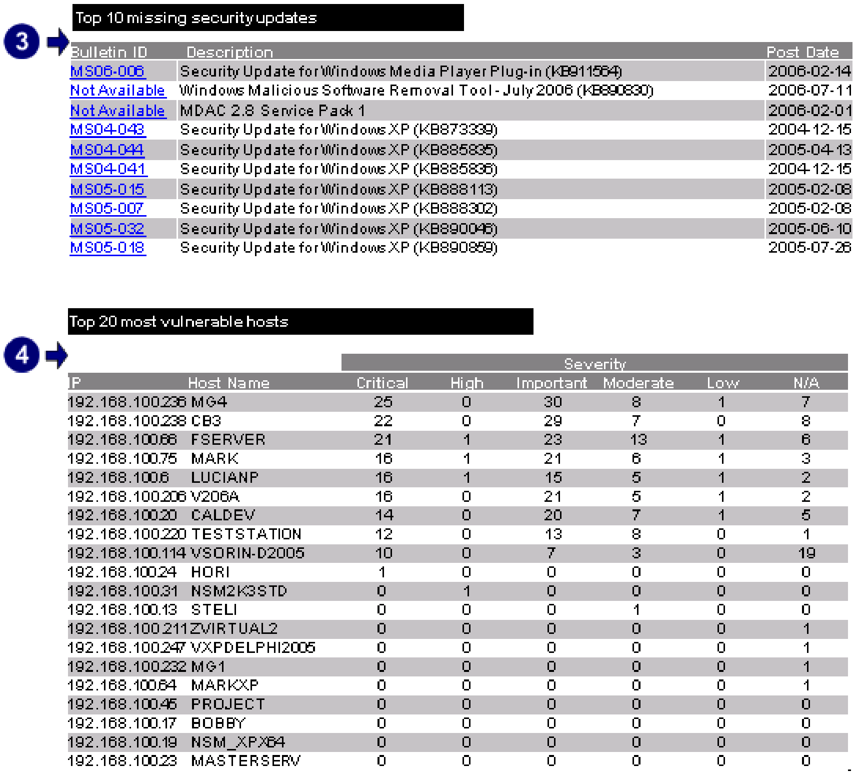
1 ➡ Missing And Installed Patches by Severity

Status	Totals			Severity		
		Critical	Important	Moderate	Low	Others
Installed	396	141	178	62	5	10
Missing	445	153	179	63	6	44
Totals	841	294	357	125	11	54

2 ➡ Missing And Installed Service Packs

Screenshot 68 – Sample report showing network patching status

1	Chart displaying the number of installed and missing patches, grouped by severity
2	Chart displaying the number of installed and missing service packs



Top 10 missing security updates

Bulletin ID	Description	Post Date
MS06-006	Security Update for Windows Media Player Plug-in (KB911564)	2006-02-14
Not Available	Windows Malicious Software Removal Tool - July 2006 (KB890830)	2006-07-11
Not Available	MDAC 2.8 Service Pack 1	2006-02-01
MS04-043	Security Update for Windows XP (KB873339)	2004-12-15
MS04-044	Security Update for Windows XP (KB885835)	2005-04-13
MS04-041	Security Update for Windows XP (KB885836)	2004-12-15
MS05-015	Security Update for Windows XP (KB888113)	2005-02-08
MS05-007	Security Update for Windows XP (KB888302)	2005-02-08
MS05-032	Security Update for Windows XP (KB890046)	2005-06-10
MS05-018	Security Update for Windows XP (KB890859)	2005-07-26

Top 20 most vulnerable hosts

		Severity					
IP	Host Name	Critical	High	Important	Moderate	Low	N/A
192.168.100.236	MG4	25	0	30	8	1	7
192.168.100.238	CB3	22	0	29	7	0	8
192.168.100.66	FSERVER	21	1	23	13	1	6
192.168.100.75	MARK	16	1	21	6	1	3
192.168.100.6	LUCIANP	16	1	15	5	1	2
192.168.100.206	V206A	16	0	21	5	1	2
192.168.100.20	CALDEV	14	0	20	7	1	5
192.168.100.220	TESTSTATION	12	0	13	8	0	1
192.168.100.114	VSORIN-D2005	10	0	7	3	0	19
192.168.100.24	HORI	1	0	0	0	0	0
192.168.100.31	NSM2K3STD	0	1	0	0	0	0
192.168.100.13	STELI	0	0	0	1	0	0
192.168.100.211	ZVIRTUAL2	0	0	0	0	0	1
192.168.100.247	VXPDELPHI2005	0	0	0	0	0	1
192.168.100.232	MG1	0	0	0	0	0	1
192.168.100.64	MARKXP	0	0	0	0	0	1
192.168.100.45	PROJECT	0	0	0	0	0	0
192.168.100.17	BOBBY	0	0	0	0	0	0
192.168.100.19	NSM_XPX64	0	0	0	0	0	0
192.168.100.23	MASTERSERV	0	0	0	0	0	0

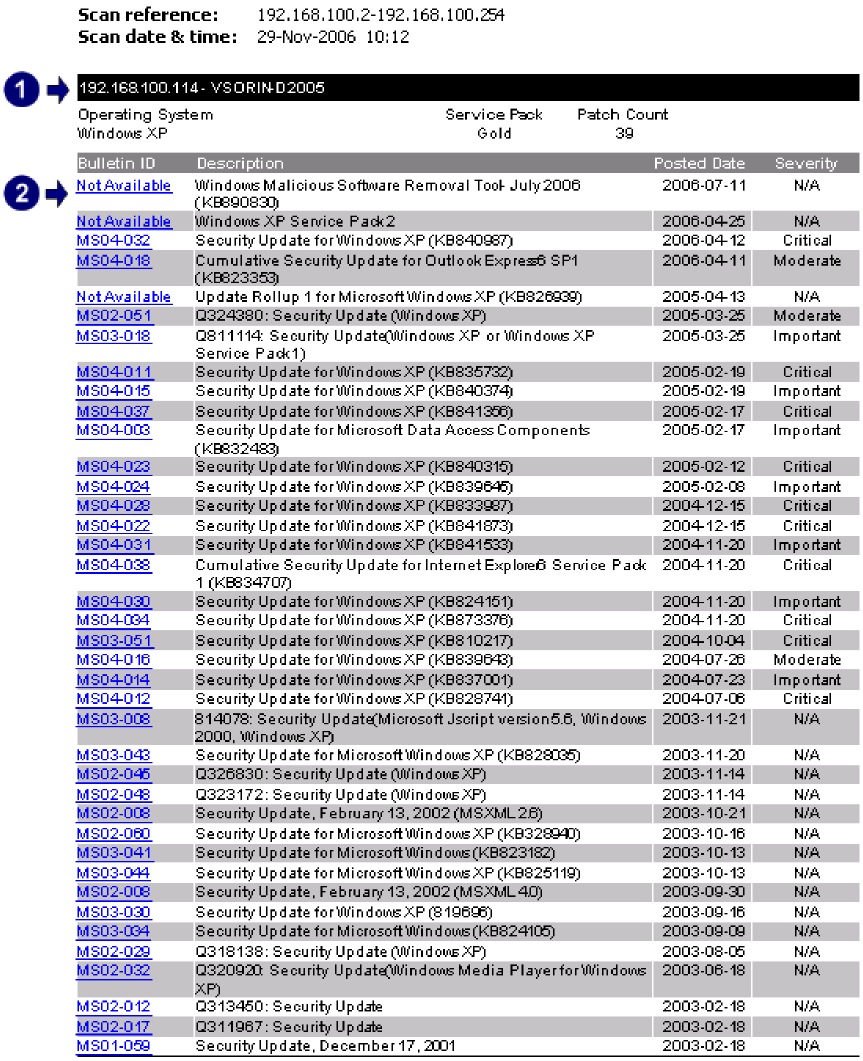
Screenshot 69 – Sample report showing network patching status

3	List showing the top 10 missing security updates
4	List showing the top 20 most vulnerable host machines, as a result of missing patches and service packs. The number of vulnerabilities detected is split according to severity

Use this report to:

- Illustrate the status of patches and service packs for host machines on the network.

Missing patches grouped by host



Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 29-Nov-2006 10:12

192.168.100.114 - VSORIN-D2005

Operating System	Service Pack	Patch Count
Windows XP	Gold	39

Bulletin ID	Description	Posted Date	Severity
Not Available	Windows Malicious Software Removal Tool - July 2006 (KB890830)	2006-07-11	N/A
Not Available	Windows XP Service Pack 2	2006-04-25	N/A
MS04-032	Security Update for Windows XP (KB840987)	2006-04-12	Critical
MS04-018	Cumulative Security Update for Outlook Express 6 SP1 (KB823353)	2006-04-11	Moderate
Not Available	Update Rollup 1 for Microsoft Windows XP (KB826939)	2005-04-13	N/A
MS02-051	Q324380: Security Update (Windows XP)	2005-03-25	Moderate
MS03-018	Q811114: Security Update (Windows XP or Windows XP Service Pack 1)	2005-03-25	Important
MS04-011	Security Update for Windows XP (KB835732)	2005-02-19	Critical
MS04-015	Security Update for Windows XP (KB840374)	2005-02-19	Important
MS04-037	Security Update for Windows XP (KB841356)	2005-02-17	Critical
MS04-003	Security Update for Microsoft Data Access Components (KB832483)	2005-02-17	Important
MS04-023	Security Update for Windows XP (KB840315)	2005-02-12	Critical
MS04-024	Security Update for Windows XP (KB839645)	2005-02-08	Important
MS04-028	Security Update for Windows XP (KB833987)	2004-12-15	Critical
MS04-022	Security Update for Windows XP (KB841873)	2004-12-15	Critical
MS04-031	Security Update for Windows XP (KB841533)	2004-11-20	Important
MS04-038	Cumulative Security Update for Internet Explorer 6 Service Pack 1 (KB834707)	2004-11-20	Critical
MS04-030	Security Update for Windows XP (KB824151)	2004-11-20	Important
MS04-034	Security Update for Windows XP (KB873376)	2004-11-20	Critical
MS03-051	Security Update for Windows XP (KB810217)	2004-10-04	Critical
MS04-016	Security Update for Windows XP (KB839643)	2004-07-26	Moderate
MS04-014	Security Update for Windows XP (KB837001)	2004-07-23	Important
MS04-012	Security Update for Windows XP (KB828741)	2004-07-06	Critical
MS03-008	814078: Security Update (Microsoft Jscript version 5.6, Windows 2000, Windows XP)	2003-11-21	N/A
MS03-043	Security Update for Microsoft Windows XP (KB828035)	2003-11-20	N/A
MS02-045	Q326830: Security Update (Windows XP)	2003-11-14	N/A
MS02-048	Q323172: Security Update (Windows XP)	2003-11-14	N/A
MS02-008	Security Update, February 13, 2002 (MSXML 2.6)	2003-10-21	N/A
MS02-060	Security Update for Microsoft Windows XP (KB328940)	2003-10-16	N/A
MS03-041	Security Update for Microsoft Windows (KB823182)	2003-10-13	N/A
MS03-044	Security Update for Microsoft Windows XP (KB825119)	2003-10-13	N/A
MS02-008	Security Update, February 13, 2002 (MSXML 4.0)	2003-09-30	N/A
MS03-030	Security Update for Windows XP (819696)	2003-09-16	N/A
MS03-034	Security Update for Microsoft Windows (KB824105)	2003-09-09	N/A
MS02-029	Q318138: Security Update (Windows XP)	2003-08-05	N/A
MS02-032	Q320920: Security Update (Windows Media Player for Windows XP)	2003-06-18	N/A
MS02-012	Q313450: Security Update	2003-02-18	N/A
MS02-017	Q311967: Security Update	2003-02-18	N/A
MS01-059	Security Update, December 17, 2001	2003-02-18	N/A

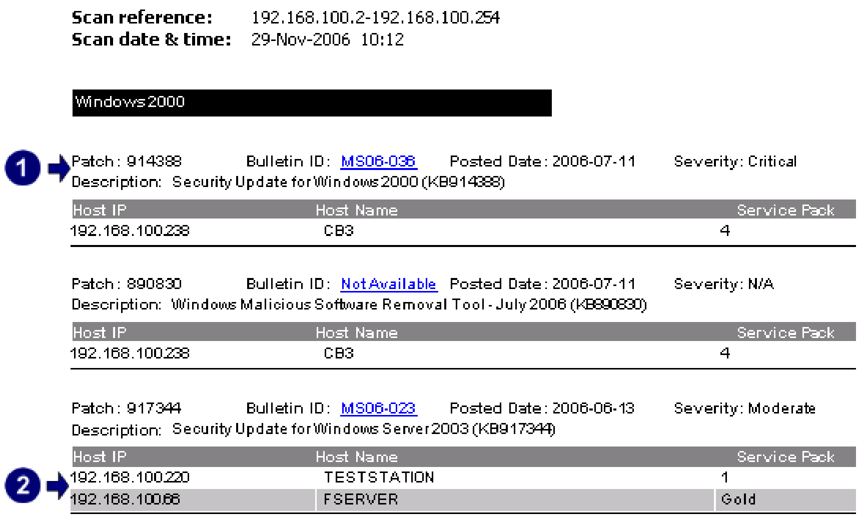
Screenshot 70 – Sample report showing missing patches grouped by host

1	Host machine details on which missing patches were detected
2	List of missing patch details for each host, including severity and URL link for further information

Use this report to:

- List missing patches grouped by host machine, including URL links providing further information on each missing patch.

Missing patches grouped by operating system



Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 29-Nov-2006 10:12

Windows 2000

Patch : 914388 Bulletin ID : MS06-036 Posted Date : 2006-07-11 Severity : Critical
Description: Security Update for Windows 2000 (KB914388)

Host IP	Host Name	Service Pack
192.168.100.238	CB3	4

Patch : 890830 Bulletin ID : Not Available Posted Date : 2006-07-11 Severity : N/A
Description: Windows Malicious Software Removal Tool - July 2006 (KB890830)

Host IP	Host Name	Service Pack
192.168.100.238	CB3	4

Patch : 917344 Bulletin ID : MS06-023 Posted Date : 2006-06-13 Severity : Moderate
Description: Security Update for Windows Server 2003 (KB917344)

Host IP	Host Name	Service Pack
192.168.100.220	TESTSTATION	1
192.168.100.66	FSERVER	Gold

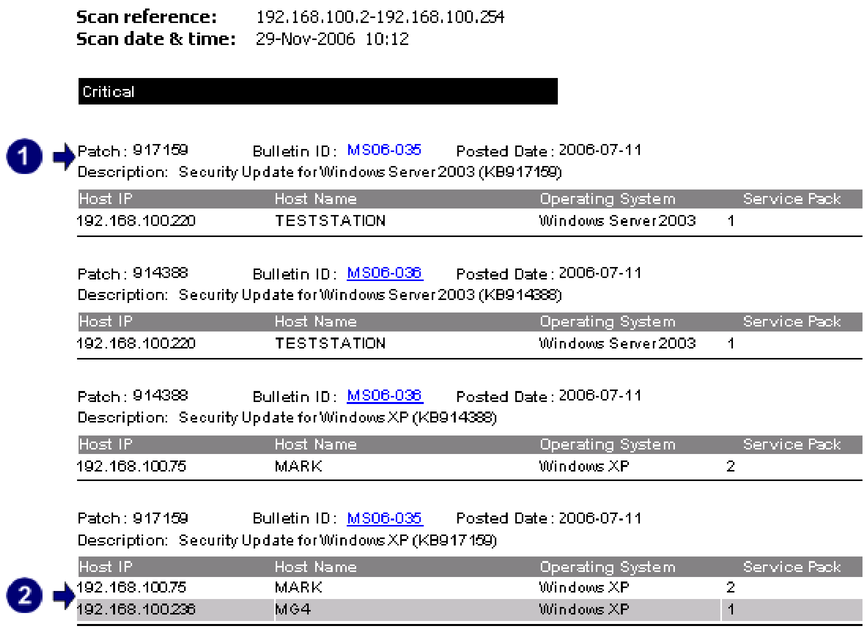
Screenshot 71 – Sample report showing missing patches grouped by operating system

1	Missing patch details for each operating system
2	List of host machines on which specific patches were found to be missing

Use this report to:

- List missing patches grouped by operating system, including the host machine names for each missing patch.

Missing patches grouped by severity



Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 29-Nov-2006 10:12

Critical

Patch : 917159 Bulletin ID : MS06-035 Posted Date : 2006-07-11
Description: Security Update for Windows Server 2003 (KB917159)

Host IP	Host Name	Operating System	Service Pack
192.168.100.220	TESTSTATION	Windows Server 2003	1

Patch : 914388 Bulletin ID : MS06-036 Posted Date : 2006-07-11
Description: Security Update for Windows Server 2003 (KB914388)

Host IP	Host Name	Operating System	Service Pack
192.168.100.220	TESTSTATION	Windows Server 2003	1

Patch : 914388 Bulletin ID : MS06-036 Posted Date : 2006-07-11
Description: Security Update for Windows XP (KB914388)

Host IP	Host Name	Operating System	Service Pack
192.168.100.75	MARK	Windows XP	2

Patch : 917159 Bulletin ID : MS06-035 Posted Date : 2006-07-11
Description: Security Update for Windows XP (KB917159)

Host IP	Host Name	Operating System	Service Pack
192.168.100.75	MARK	Windows XP	2
192.168.100.236	MG4	Windows XP	1

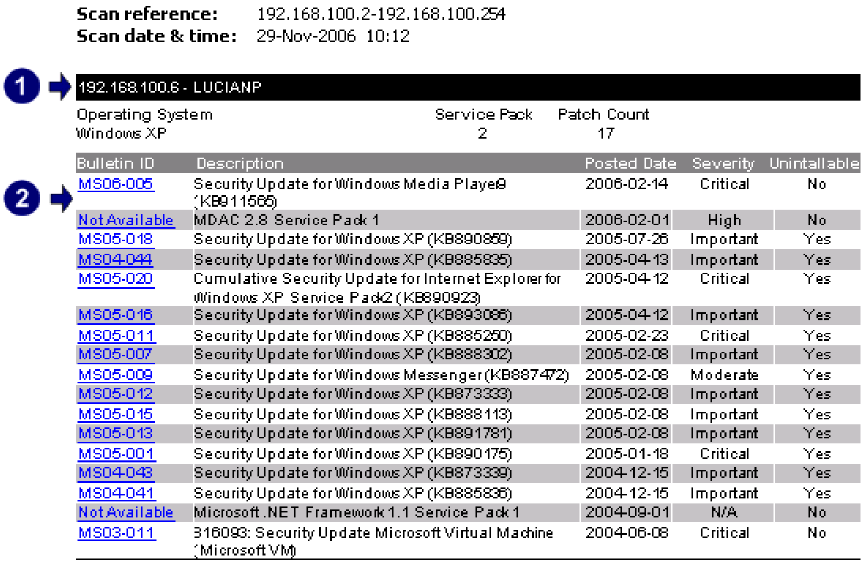
Screenshot 72 – Sample report showing missing patches grouped by severity

1	Missing patch details for each severity level
2	List of host machines on which specific patches were found to be missing

Use this report to:

- List missing patches grouped by severity, including the host machine names for each missing patch.

Installed patches grouped by host



Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 29-Nov-2006 10:12

192.168.100.6 - LUCIANP

Operating System	Service Pack	Patch Count
Windows XP	2	17

Bulletin ID	Description	Posted Date	Severity	Unintallable
MS06-005	Security Update for Windows Media Player9 (KB911565)	2006-02-14	Critical	No
Not Available	MDAC 2.8 Service Pack 1	2006-02-01	High	No
MS05-018	Security Update for Windows XP (KB890859)	2005-07-26	Important	Yes
MS04-044	Security Update for Windows XP (KB885835)	2005-04-13	Important	Yes
MS05-020	Cumulative Security Update for Internet Explorer for Windows XP Service Pack2 (KB890923)	2005-04-12	Critical	Yes
MS05-016	Security Update for Windows XP (KB893086)	2005-04-12	Important	Yes
MS05-011	Security Update for Windows XP (KB885250)	2005-02-23	Critical	Yes
MS05-007	Security Update for Windows XP (KB888302)	2005-02-08	Important	Yes
MS05-009	Security Update for Windows Messenger (KB887472)	2005-02-08	Moderate	Yes
MS05-012	Security Update for Windows XP (KB873333)	2005-02-08	Important	Yes
MS05-015	Security Update for Windows XP (KB888113)	2005-02-08	Important	Yes
MS05-013	Security Update for Windows XP (KB891781)	2005-02-08	Important	Yes
MS05-001	Security Update for Windows XP (KB890175)	2005-01-18	Critical	Yes
MS04-043	Security Update for Windows XP (KB873339)	2004-12-15	Important	Yes
MS04-041	Security Update for Windows XP (KB885836)	2004-12-15	Important	Yes
Not Available	Microsoft .NET Framework 1.1 Service Pack 1	2004-09-01	N/A	No
MS03-011	316093: Security Update Microsoft Virtual Machine (Microsoft VM)	2004-06-08	Critical	No

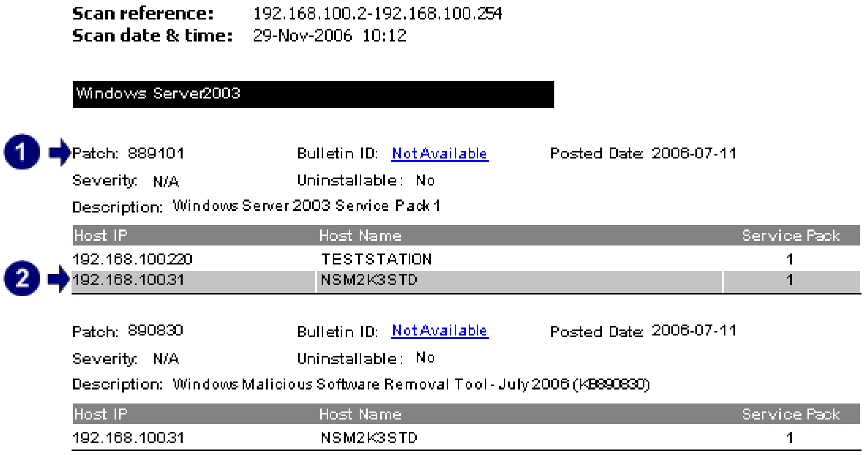
Screenshot 73 – Sample report showing installed patches grouped by host

1	Host machine details on which installed patches were detected
2	List of installed patch details for each host, including severity, URL link for further information and indication if the patch can be uninstalled

Use this report to:

- List installed patches grouped by host machine, including URL links providing further information on each installed patch.

Installed patches grouped by operating system



Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 29-Nov-2006 10:12

Windows Server2003

Patch: 889101 Bulletin ID: Not Available Posted Date: 2006-07-11
Severity: N/A Uninstallable: No
Description: Windows Server 2003 Service Pack 1

Host IP	Host Name	Service Pack
192.168.100.220	TESTSTATION	1
192.168.100.31	NSM2K3STD	1

Patch: 890830 Bulletin ID: Not Available Posted Date: 2006-07-11
Severity: N/A Uninstallable: No
Description: Windows Malicious Software Removal Tool - July 2006 (KB890830)

Host IP	Host Name	Service Pack
192.168.100.31	NSM2K3STD	1

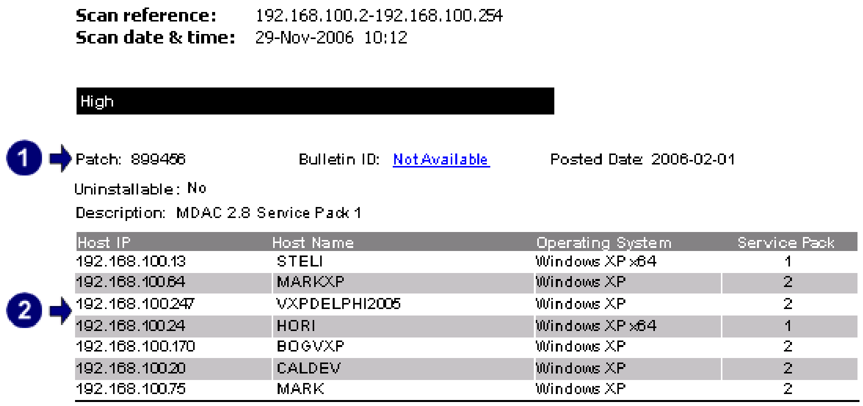
Screenshot 74 – Sample report showing installed patches grouped by operating system

1	Installed patch details for each operating system
2	List of host machines on which specific patches were found to be installed

Use this report to:

- List installed patches grouped by operating system, including the host machine names for each installed patch.

Installed patches grouped by severity



Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 29-Nov-2006 10:12

High

Patch: 899456 Bulletin ID: Not Available Posted Date: 2006-02-01

Uninstallable: No

Description: MDAC 2.8 Service Pack 1

Host IP	Host Name	Operating System	Service Pack
192.168.100.13	STELI	Windows XP x64	1
192.168.100.64	MARKXP	Windows XP	2
192.168.100.247	VXPDELPHI2005	Windows XP	2
192.168.100.24	HORI	Windows XP x64	1
192.168.100.170	BOGVXP	Windows XP	2
192.168.100.20	CALDEV	Windows XP	2
192.168.100.75	MARK	Windows XP	2

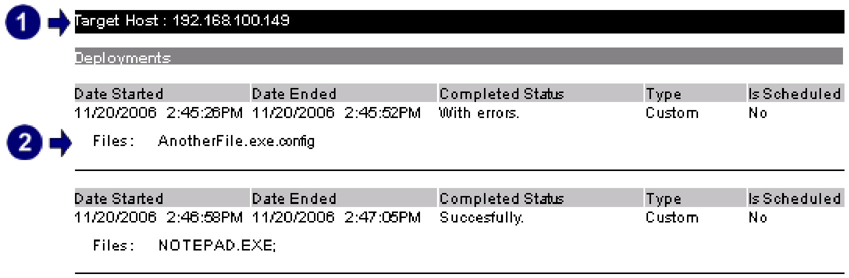
Screenshot 75 – Sample report showing installed patches grouped by severity

1	List of installed patches grouped by their severity level, including information on each patch
2	List of host machines on which specific patches were found to be installed

Use this report to:

- List installed patches grouped by severity, including the host machine names for each installed patch.

Remediation history by host



Target Host : 192.168.100.149

Deployments

Date Started	Date Ended	Completed Status	Type	Is Scheduled
11/20/2006 2:45:26PM	11/20/2006 2:45:52PM	With errors.	Custom	No

Files: AnotherFile.exe.config

Date Started	Date Ended	Completed Status	Type	Is Scheduled
11/20/2006 2:46:58PM	11/20/2006 2:47:05PM	Succesfully.	Custom	No

Files: NOTEPAD.EXE;

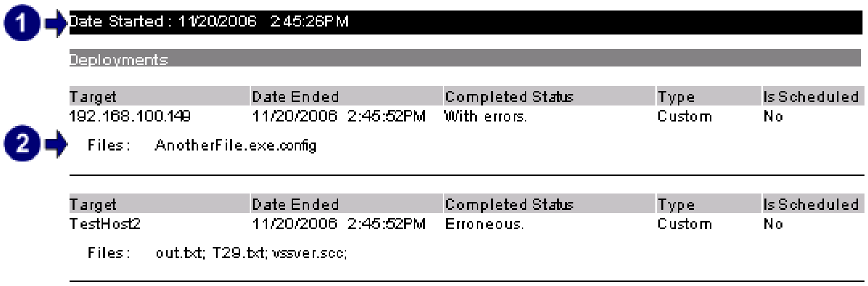
Screenshot 76 – Sample report showing deployment history by host

1	Host machine on which deployments were made
2	List of deployment details for each host, including file names deployed, and deployment status

Use this report to:

- Display patch deployment information grouped by host machine, including deployment details such as date and status.

Remediation history by date



Date Started : 11/20/2006 2:45:26PM

Deployments

Target	Date Ended	Completed Status	Type	Is Scheduled
192.168.100.149	11/20/2006 2:45:52PM	With errors.	Custom	No

Files : AnotherFile.exe.config

Target	Date Ended	Completed Status	Type	Is Scheduled
TestHost2	11/20/2006 2:45:52PM	Erroneous.	Custom	No

Files : out.txt; T29.txt; vssver.scc;

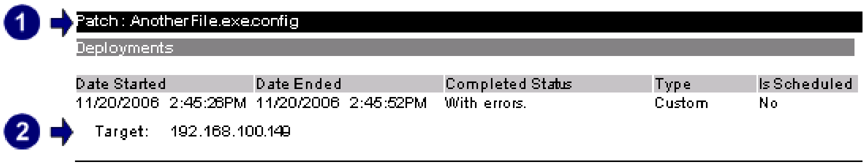
Screenshot 77 – Sample report showing deployment history by date

1	Deployment starting date
2	List of deployment details grouped by host, including file names deployed, and deployment status

Use this report to:

- Display patch deployment information by date and time, including details such as host machine names for each deployment.

Remediation history by patch/application



Patch : AnotherFile.exe.config

Deployments

Date Started	Date Ended	Completed Status	Type	Is Scheduled
11/20/2006 2:45:26PM	11/20/2006 2:45:52PM	With errors.	Custom	No

Target: 192.168.100.149

Screenshot 78 – Sample report showing deployment history by patch

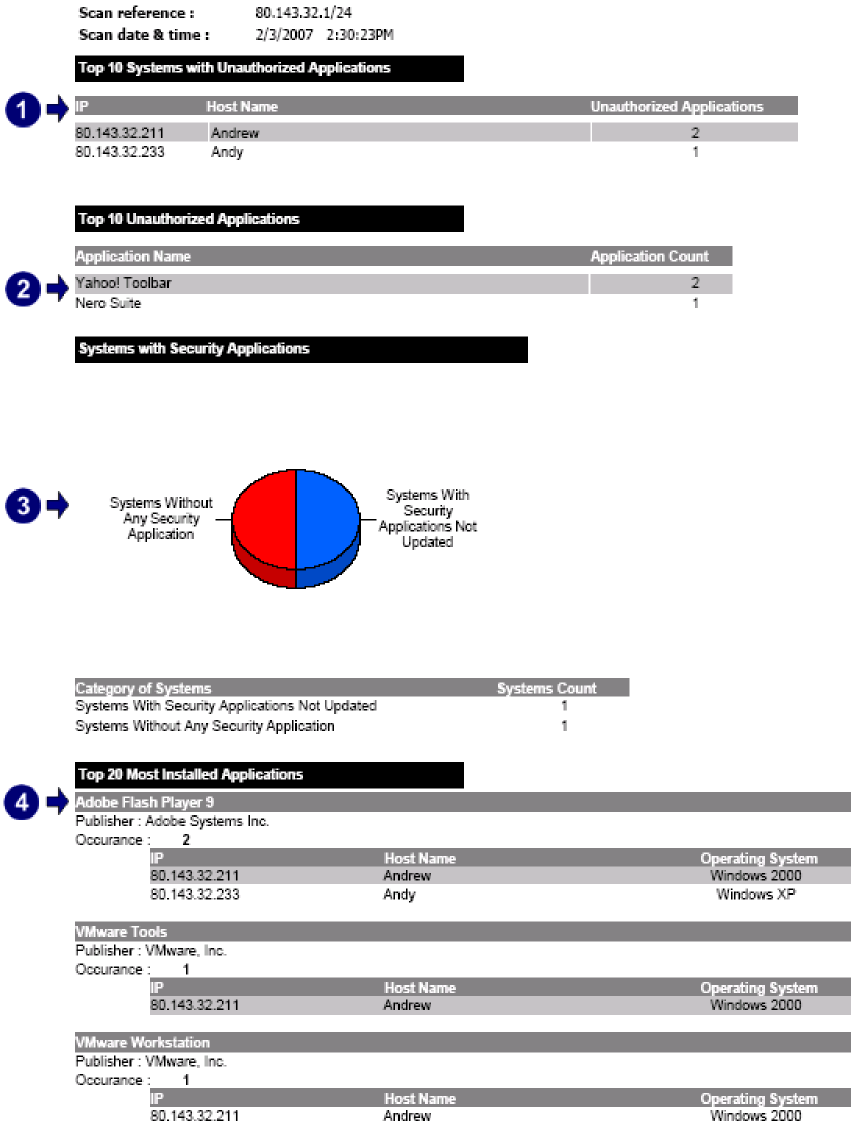
1	Name of patch deployed
2	List of host machines on which the patch was deployed and deployment details, including deployment status

Use this report to:

- Display patch deployment information grouped by patch applied, including details such as host machine names for each deployment.

Network and software audit reports

Software audit


1
2
3
4
Systems Without Any Security Application
Systems With Security Applications Not Updated

Scan reference : 80.143.32.1/24
Scan date & time : 2/3/2007 2:30:23PM

Top 10 Systems with Unauthorized Applications

IP	Host Name	Unauthorized Applications
80.143.32.211	Andrew	2
80.143.32.233	Andy	1

Top 10 Unauthorized Applications

Application Name	Application Count
Yahoo! Toolbar	2
Nero Suite	1

Systems with Security Applications

Category of Systems	Systems Count
Systems With Security Applications Not Updated	1
Systems Without Any Security Application	1

Top 20 Most Installed Applications

Adobe Flash Player 9
Publisher : Adobe Systems Inc.
Occurance : 2

IP	Host Name	Operating System
80.143.32.211	Andrew	Windows 2000
80.143.32.233	Andy	Windows XP

VMware Tools
Publisher : VMware, Inc.
Occurance : 1

IP	Host Name	Operating System
80.143.32.211	Andrew	Windows 2000

VMware Workstation
Publisher : VMware, Inc.
Occurance : 1

IP	Host Name	Operating System
80.143.32.211	Andrew	Windows 2000

Screenshot 79 – Sample report showing software audit

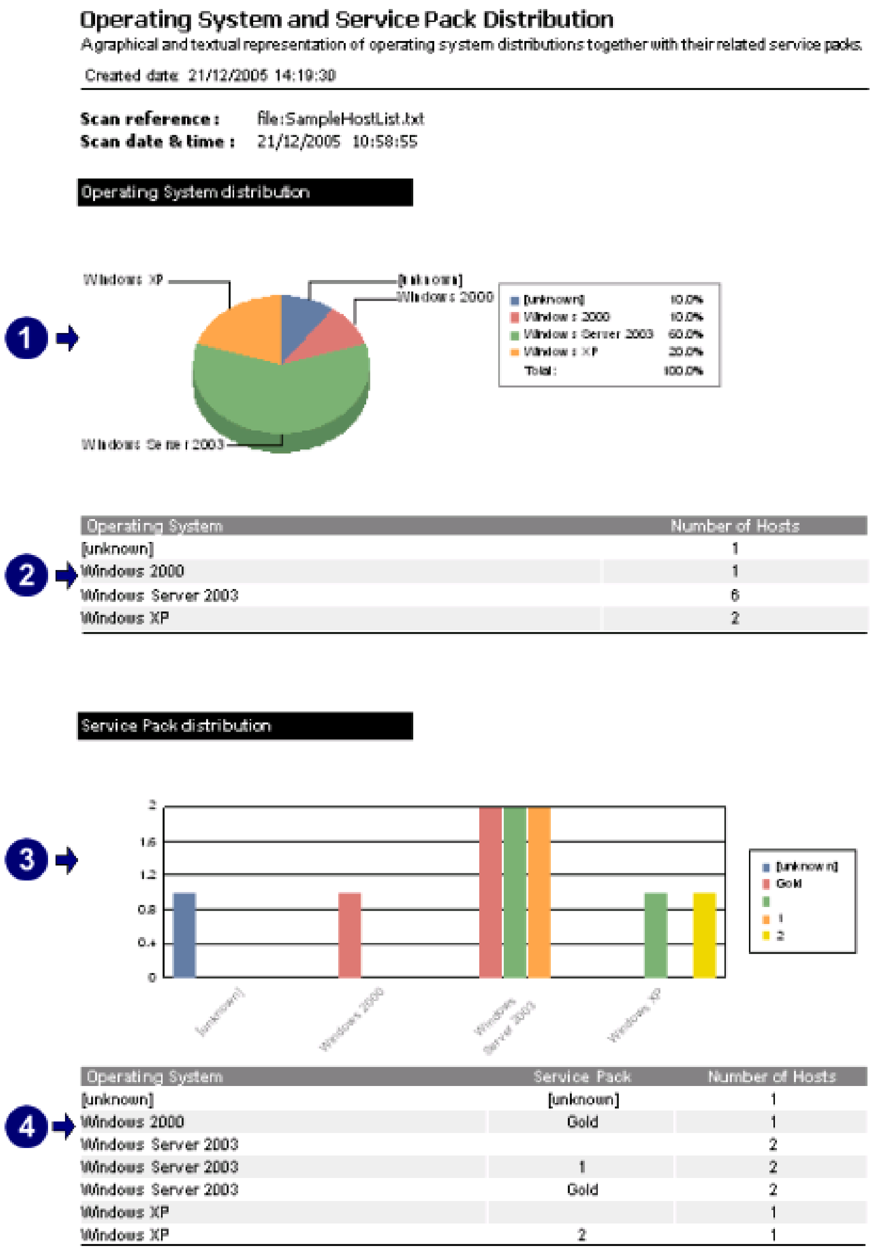
1	List showing the top 10 host machines with unauthorized applications
2	List showing the top 10 unauthorized applications
3	Chart displaying the status of security applications on host machines
4	List showing the top 20 installed applications

Use this report to:

- Identify unauthorized applications installed on host machines, detected during network security scans

- Identify the top 10 host machines with unauthorized applications
- Identify the top 10 unauthorized applications with highest number of installations
- Identify the top 20 installed applications
- Graphically represent the number of host machines without security applications, or with security applications not updated.

Operating system and service pack distribution



Operating System and Service Pack Distribution

A graphical and textual representation of operating system distributions together with their related service packs.

Created date: 21/12/2005 14:19:30

Scan reference : file:SampleHostList.txt
Scan date & time : 21/12/2005 10:58:55

Operating System distribution

Operating System	Number of Hosts
[unknown]	1
Windows 2000	1
Windows Server 2003	6
Windows XP	2

Service Pack distribution

Operating System	Service Pack	Number of Hosts
[unknown]	[unknown]	1
Windows 2000	Gold	1
Windows Server 2003		2
Windows Server 2003	1	2
Windows Server 2003	Gold	2
Windows XP		1
Windows XP	2	1

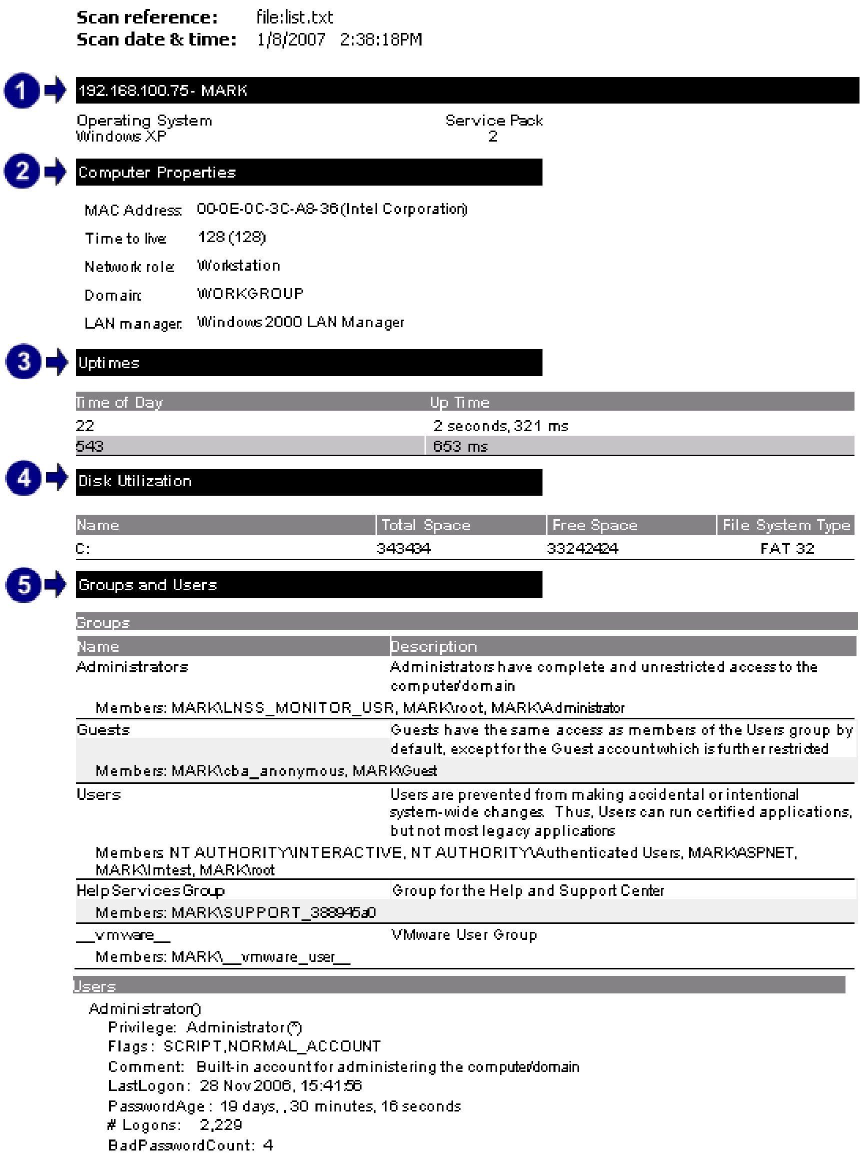
Screenshot 80 – Sample report showing operating system and service pack distribution

1	Chart displaying distribution percentage of each operating system on the network
2	List of operating systems, including the number of host machines on which they are installed
3	Chart displaying service pack distribution for each operating system
4	List of operating system service packs, including the number of host machines on which they are installed

Use this report to:

- Graphically represent operating systems detected on the network
- List the number of host machines for each operating system
- Graphically represent service packs detected on the network for each operating system
- List the number of host machines for each service pack installed.

System information



Scan reference: file:list.txt
Scan date & time: 1/8/2007 2:38:18PM

192.168.100.75 - MARK

Operating System	Service Pack
Windows XP	2

Computer Properties

MAC Address:	00-0E-0C-3C-A8-36 (Intel Corporation)
Time to live:	128 (128)
Network role:	Workstation
Domain:	WORKGROUP
LAN manager:	Windows 2000 LAN Manager

Uptimes

Time of Day	Up Time
22	2 seconds, 321 ms
543	653 ms

Disk Utilization

Name	Total Space	Free Space	File System Type
C:	343434	33242424	FAT 32

Groups and Users

Groups

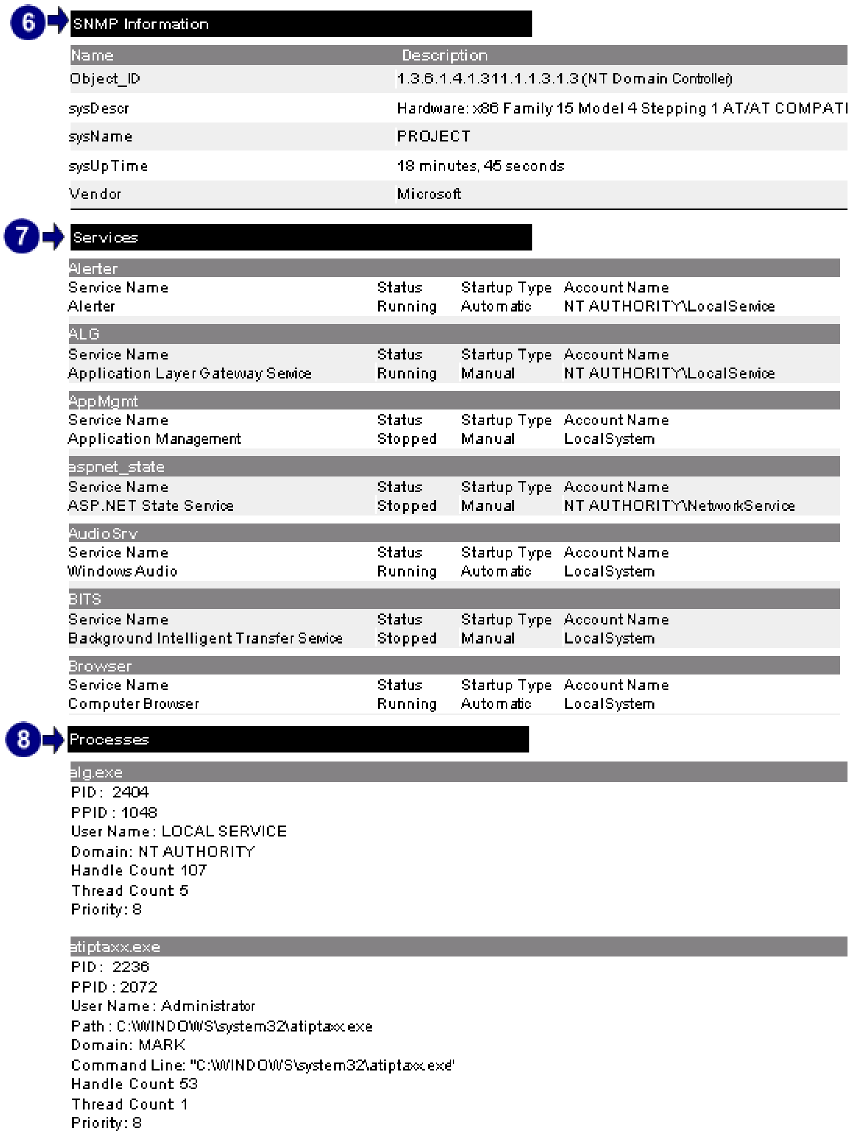
Name	Description
Administrators	Administrators have complete and unrestricted access to the computer/domain
Members: MARK\LNSS_MONITOR_USR, MARK\root, MARK\Administrator	
Guests	Guests have the same access as members of the Users group by default, except for the Guest account which is further restricted
Members: MARK\cba_anonymous, MARK\Guest	
Users	Users are prevented from making accidental or intentional system-wide changes. Thus, Users can run certified applications, but not most legacy applications
Members NT AUTHORITY\INTERACTIVE, NT AUTHORITY\Authenticated Users, MARK\ASPNET, MARK\lmtest, MARK\root	
HelpServicesGroup	Group for the Help and Support Center
Members: MARK\SUPPORT_388945a0	
__vmware__	VMware User Group
Members: MARK__vmware_user__	

Users

Administrator()
Privilege: Administrator(*)
Flags: SCRIPT,NORMAL_ACCOUNT
Comment: Built-in account for administering the computer/domain
LastLogon: 28 Nov 2006, 15:41:56
PasswordAge: 19 days, , 30 minutes, 16 seconds
Logons: 2,229
BadPasswordCount: 4

Screenshot 81 – Sample report showing system information

1	Host machine IP and name
2	Host machine details, including MAC address and domain
3	Uptime details for each host machine, including time of day and uptime value
4	Disk utilization details for each host machine, including drive name, file system type, total storage space and free storage space
5	Group and user details for each host machine, including group name, group members, user privileges and user bad password count



SNMP Information

Name	Description
Object_ID	1.3.6.1.4.1.311.1.1.3.1.3 (NT Domain Controller)
sysDescr	Hardware: x86 Family 15 Model 4 Stepping 1 AT/AT COMPATI
sysName	PROJECT
sysUpTime	18 minutes, 45 seconds
Vendor	Microsoft

Services

Alerter			
Service Name	Status	Startup Type	Account Name
Alerter	Running	Automatic	NT AUTHORITY\LocalService

ALG			
Service Name	Status	Startup Type	Account Name
Application Layer Gateway Service	Running	Manual	NT AUTHORITY\LocalService

AppMgmt			
Service Name	Status	Startup Type	Account Name
Application Management	Stopped	Manual	LocalSystem

aspnet_state			
Service Name	Status	Startup Type	Account Name
ASP.NET State Service	Stopped	Manual	NT AUTHORITY\NetworkService

AudioSrv			
Service Name	Status	Startup Type	Account Name
Windows Audio	Running	Automatic	LocalSystem

BITS			
Service Name	Status	Startup Type	Account Name
Background Intelligent Transfer Service	Stopped	Manual	LocalSystem

Browser			
Service Name	Status	Startup Type	Account Name
Computer Browser	Running	Automatic	LocalSystem

Processes

alg.exe

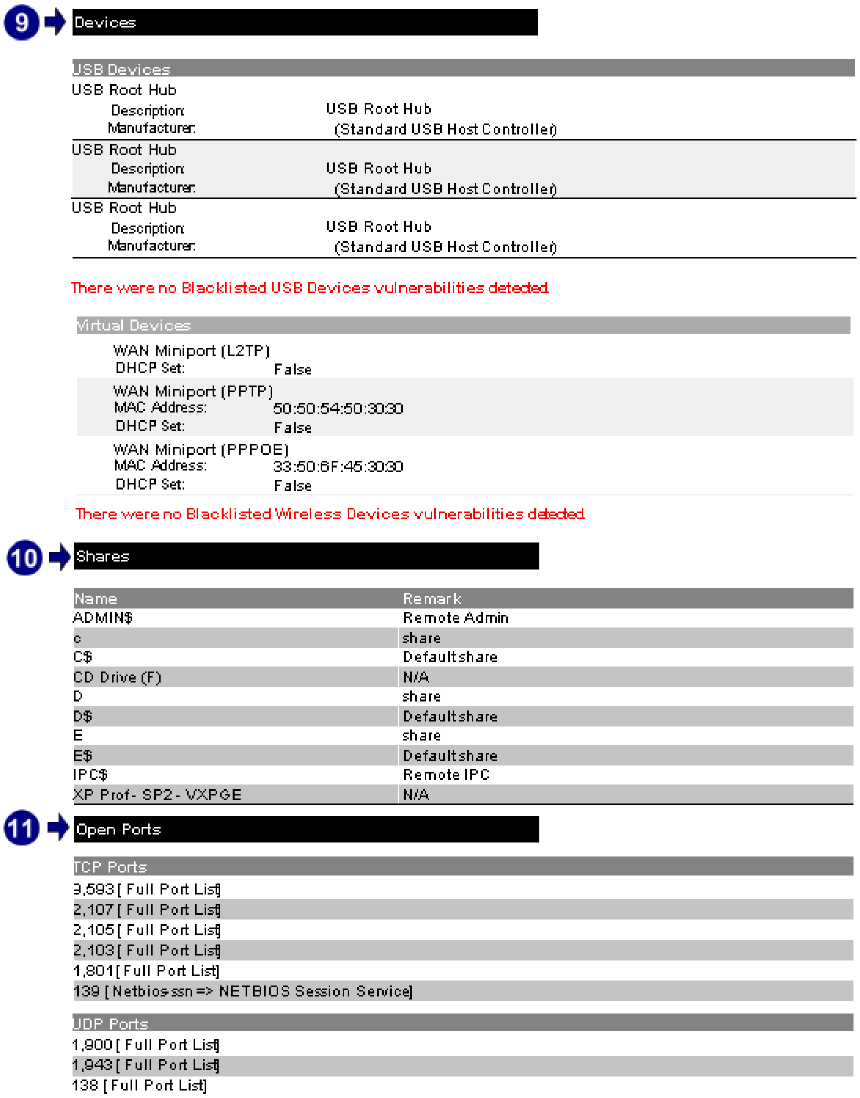
PID : 2404
PPID : 1048
User Name : LOCAL SERVICE
Domain: NT AUTHORITY
Handle Count 107
Thread Count 5
Priority: 8

atiptaxx.exe

PID : 2236
PPID : 2072
User Name : Administrator
Path : C:\WINDOWS\system32\atiptaxx.exe
Domain: MARK
Command Line: "C:\WINDOWS\system32\atiptaxx.exe"
Handle Count 53
Thread Count 1
Priority: 8

Screenshot 82 – Sample report showing system information

6	SNMP details for each host machine, including name and description
7	Service details for each host machine, including name, description, status, startup type and account name
8	Process details for each host machine, including process ID and account name



Devices

USB Devices

USB Root Hub
Description: USB Root Hub
Manufacturer: (Standard USB Host Controller)

USB Root Hub
Description: USB Root Hub
Manufacturer: (Standard USB Host Controller)

USB Root Hub
Description: USB Root Hub
Manufacturer: (Standard USB Host Controller)

There were no Blacklisted USB Devices vulnerabilities detected

Virtual Devices

WAN Miniport (L2TP)
DHCP Set: False

WAN Miniport (PPTP)
MAC Address: 50:50:54:50:30:30
DHCP Set: False

WAN Miniport (PPPOE)
MAC Address: 33:50:6F:45:30:30
DHCP Set: False

There were no Blacklisted Wireless Devices vulnerabilities detected

Shares

Name	Remark
ADMIN$	Remote Admin
c	share
C$	Default share
CD Drive (F)	N/A
D	share
D$	Default share
E	share
E$	Default share
IPC$	Remote IPC
XP Prof - SP2 - VXPGE	N/A

Open Ports

TCP Ports

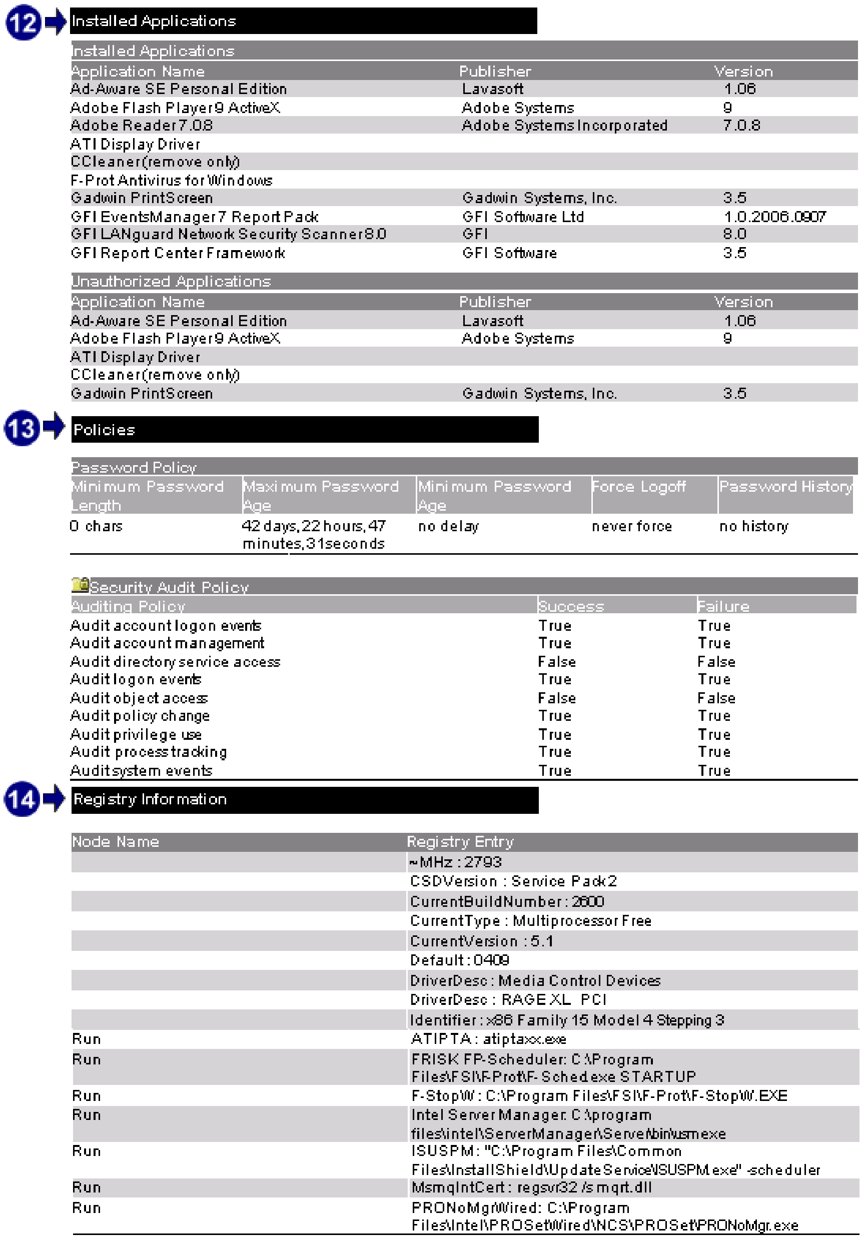
3,593 [Full Port List]
2,107 [Full Port List]
2,105 [Full Port List]
2,103 [Full Port List]
1,801 [Full Port List]
139 [Netbios-ssn => NETBIOS Session Service]

UDP Ports

1,900 [Full Port List]
1,943 [Full Port List]
138 [Full Port List]

Screenshot 83 – Sample report showing system information

9	List showing USB devices, blacklisted USB devices, network cards and black listed wireless devices
10	Share folder details for each host machine, including name and remarks
11	Open port details for each host machine, including port number and name



Installed Applications

Installed Applications		
Application Name	Publisher	Version
Ad-Aware SE Personal Edition	Lavasoft	1.06
Adobe Flash Player9 ActiveX	Adobe Systems	9
Adobe Reader 7.08	Adobe Systems Incorporated	7.0.8
ATI Display Driver		
CCleaner(remove only)		
F-Prot Antivirus for Windows		
Gadwin PrintScreen	Gadwin Systems, Inc.	3.5
GFI EventsManager 7 Report Pack	GFI Software Ltd	1.0.2006.0907
GFI LANguard Network Security Scanner 8.0	GFI	8.0
GFI Report Center Framework	GFI Software	3.5

Unauthorized Applications		
Application Name	Publisher	Version
Ad-Aware SE Personal Edition	Lavasoft	1.06
Adobe Flash Player9 ActiveX	Adobe Systems	9
ATI Display Driver		
CCleaner(remove only)		
Gadwin PrintScreen	Gadwin Systems, Inc.	3.5

Policies

Password Policy				
Minimum Password Length	Maximum Password Age	Minimum Password Age	Force Logoff	Password History
0 chars	42 days, 22 hours, 47 minutes, 31 seconds	no delay	never force	no history

Security Audit Policy		
Auditing Policy	Success	Failure
Audit account logon events	True	True
Audit account management	True	True
Audit directory service access	False	False
Audit logon events	True	True
Audit object access	False	False
Audit policy change	True	True
Audit privilege use	True	True
Audit process tracking	True	True
Audit system events	True	True

Registry Information

Node Name	Registry Entry
	~MHz : 2793
	CSDVersion : Service Pack 2
	CurrentBuildNumber : 2600
	CurrentType : Multiprocessor Free
	CurrentVersion : 5.1
	Default : 0409
	DriverDesc : Media Control Devices
	DriverDesc : RAGE XL PCI
	Identifier : x86 Family 15 Model 4 Stepping 3
Run	ATIPTA : atiptaxx.exe
Run	FRISK FP-Scheduler: C:\Program Files\FSI\F-Prot\F-Sched.exe STARTUP
Run	F-StopW : C:\Program Files\FSI\F-Prot\F-StopW.EXE
Run	Intel Server Manager: C:\program files\intel\ServerManager\Server\bin\usm.exe
Run	ISUSPM : "C:\Program Files\Common Files\InstallShield\UpdateService\ISUSPM.exe" -scheduler
Run	MsmqIntCert : regsvr32 /s mqrt.dll
Run	PRONoMgrWired: C:\Program Files\Intel\PROSetWired\NCS\PROSet\PRONoMgr.exe

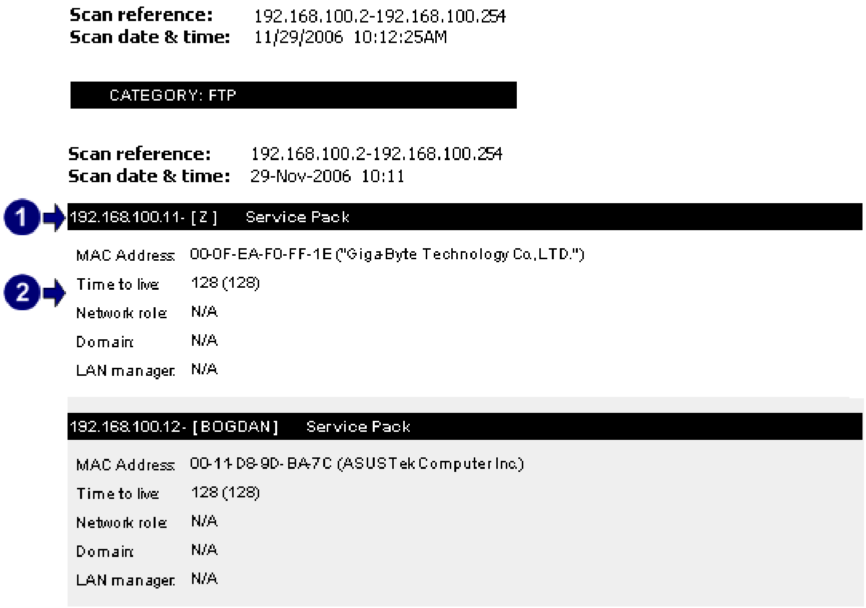
Screenshot 84 – Sample report showing system information

12	Installed application details for each host machine, including name, publisher and version
13	List showing password policy details security audit policy details
14	List of registry entry details for each host machine

Use this report to:

- List detailed technical information for each host machine, including services, installed applications, policies and devices.

Computer properties



Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 11/29/2006 10:12:25AM

CATEGORY: FTP

Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 29-Nov-2006 10:11

192.168.100.11- [Z] Service Pack

MAC Address:	00-0F-EA-F0-FF-1E ("GigaByte Technology Co.,LTD.")
Time to live:	128 (128)
Network role:	N/A
Domain:	N/A
LAN manager:	N/A

192.168.100.12- [BOGDAN] Service Pack

MAC Address:	00-11-D8-9D-BA-7C (ASUSTek Computer Inc.)
Time to live:	128 (128)
Network role:	N/A
Domain:	N/A
LAN manager:	N/A

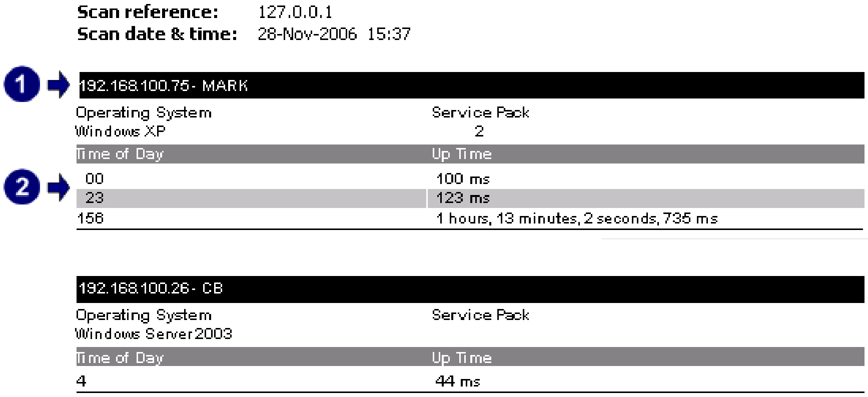
Screenshot 85 – Sample report showing computer properties

1	Host machine IP and name
2	Host machine details, including MAC address and domain

Use this report to:

- List information for each host machine, including MAC address, network role and domain.

Uptimes



Scan reference: 127.0.0.1
Scan date & time: 28-Nov-2006 15:37

192.168.100.75- MARK

Operating System	Service Pack
Windows XP	2

Time of Day	Up Time
00	100 ms
23	123 ms
156	1 hours, 13 minutes, 2 seconds, 735 ms

192.168.100.26- CB

Operating System	Service Pack
Windows Server 2003	

Time of Day	Up Time
4	44 ms

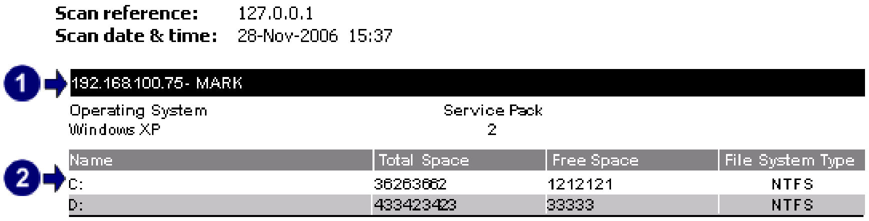
Screenshot 86 – Sample report showing uptimes

1	Host machine IP and name
2	Uptime details for each host machine, including time of day and uptime value

Use this report to:

- List uptime for each host machine, grouped by network scan.

Disk utilization



Scan reference: 127.0.0.1
Scan date & time: 28-Nov-2006 15:37

192.168.100.75 - MARK

Operating System	Service Pack
Windows XP	2

Name	Total Space	Free Space	File System Type
C:	36263662	1212121	NTFS
D:	433423423	33333	NTFS

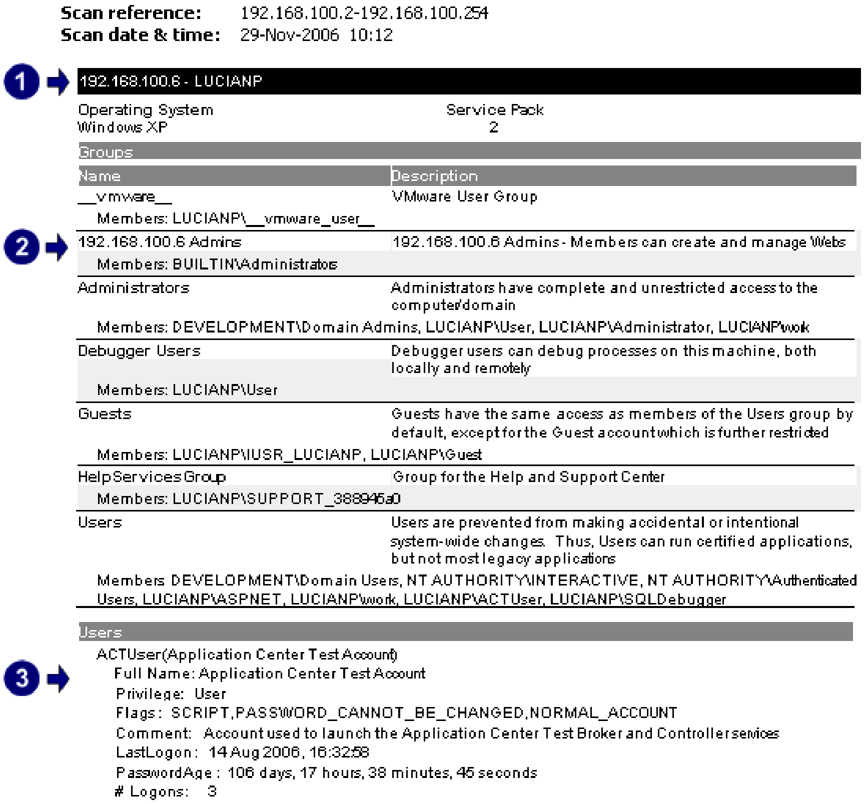
Screenshot 87 – Sample report showing disk utilization

1	Host machine IP and name
2	Disk utilization details for each host machine, including drive name, file system type, total storage space and free storage space

Use this report to:

- List disk utilization information for each host machine, including file system type, total space and free space.

Groups and users



Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 29-Nov-2006 10:12

192.168.100.6 - LUCIANP

Operating System	Service Pack
Windows XP	2

Groups

Name	Description
__vmware__	VMware User Group
Members: LUCIANP__vmware_user__	
192.168.100.6 Admins	192.168.100.6 Admins - Members can create and manage Webs
Members: BUILTIN\Administrators	
Administrators	Administrators have complete and unrestricted access to the computer/domain
Members: DEVELOPMENT\Domain Admins, LUCIANP\User, LUCIANP\Administrator, LUCIANP\work	
Debugger Users	Debugger users can debug processes on this machine, both locally and remotely
Members: LUCIANP\User	
Guests	Guests have the same access as members of the Users group by default, except for the Guest account which is further restricted
Members: LUCIANP\IUSR_LUCIANP, LUCIANP\Guest	
HelpServicesGroup	Group for the Help and Support Center
Members: LUCIANP\SUPPORT_388945a0	
Users	Users are prevented from making accidental or intentional system-wide changes. Thus, Users can run certified applications, but not most legacy applications
Members DEVELOPMENT\Domain Users, NT AUTHORITY\INTERACTIVE, NT AUTHORITY\Authenticated Users, LUCIANP\ASPNET, LUCIANP\work, LUCIANP\ACTUser, LUCIANP\SQLDebugger	

Users

```
ACTUser(Application Center Test Account)
  Full Name: Application Center Test Account
  Privilege:  User
  Flags:  SCRIPT,PASSWORD_CANNOT_BE_CHANGED,NORMAL_ACCOUNT
  Comment:  Account used to launch the Application Center Test Broker and Controller services
  LastLogon:  14 Aug 2006, 16:32:58
  PasswordAge :  106 days, 17 hours, 38 minutes, 45 seconds
  # Logons:   3
```

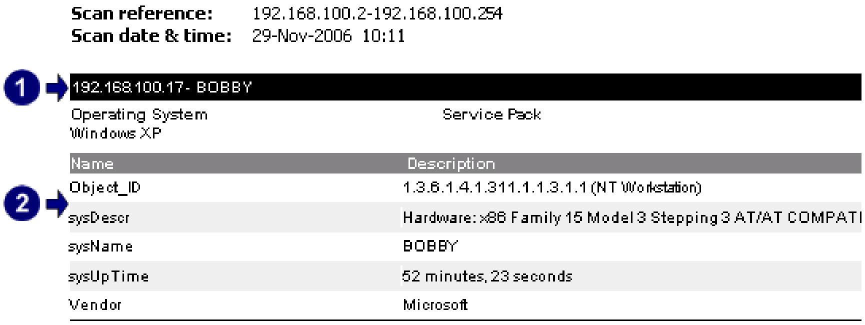
Screenshot 88 – Sample report showing groups and users

1	Host machine IP and name
2	List showing group details for each host machine, including name, description and members
3	List of user details for each group, including user name, privilege, last logon and bad password count

Use this report to:

- List group and user information for each host machine.

SNMP information



Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 29-Nov-2006 10:11

192.168.100.17- BOBBY

Operating System Service Pack
Windows XP

Name	Description
Object_ID	1.3.6.1.4.1.311.1.1.3.1.1 (NT Workstation)
sysDescr	Hardware: x86 Family 15 Model 3 Stepping 3 AT/AT COMPATI
sysName	BOBBY
sysUpTime	52 minutes, 23 seconds
Vendor	Microsoft

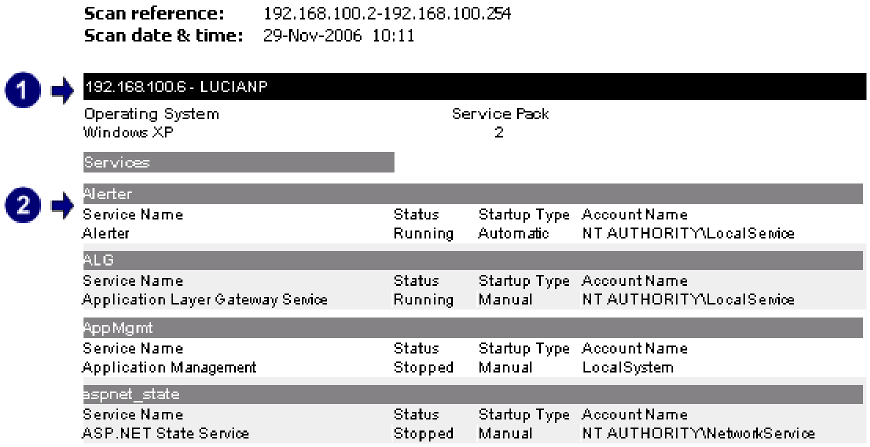
Screenshot 89 – Sample report showing SNMP information

1	Host machine IP and name
2	SNMP details for each host machine, including name and description

Use this report to:

- List SNMP information for each host machine, including name, description and uptime.

Services



Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 29-Nov-2006 10:11

192.168.100.6 - LUCIANP

Operating System Service Pack
Windows XP 2

Services

Alerter

Service Name	Status	Startup Type	Account Name
Alerter	Running	Automatic	NT AUTHORITY\LocalService

ALG

Service Name	Status	Startup Type	Account Name
Application Layer Gateway Service	Running	Manual	NT AUTHORITY\LocalService

AppMgmt

Service Name	Status	Startup Type	Account Name
Application Management	Stopped	Manual	LocalSystem

aspnet_state

Service Name	Status	Startup Type	Account Name
ASP.NET State Service	Stopped	Manual	NT AUTHORITY\NetworkService

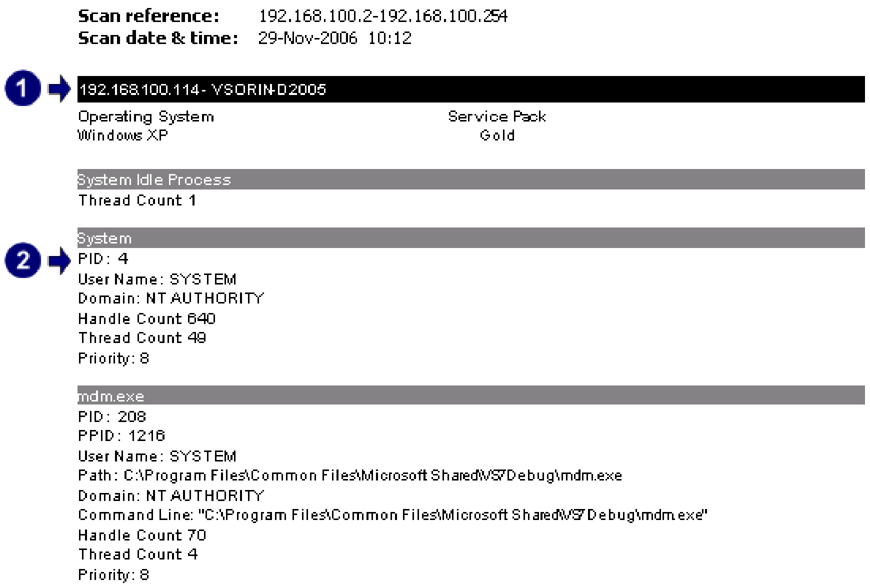
Screenshot 90 – Sample report showing services

1	Host machine IP and name
2	Service details for each host machine, including name, description, status, startup type and account name

Use this report to:

- List service information for each host machine, including description, status, startup type and account name.

Processes



Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 29-Nov-2006 10:12

192.168.100.114 - VSORIN-D2005

Operating System	Service Pack
Windows XP	Gold

System Idle Process
Thread Count 1

System

PID: 4
User Name: SYSTEM
Domain: NT AUTHORITY
Handle Count 640
Thread Count 49
Priority: 8

mdm.exe
PID: 208
PPID: 1216
User Name: SYSTEM
Path: C:\Program Files\Common Files\Microsoft Shared\VS7Debug\mdm.exe
Domain: NT AUTHORITY
Command Line: "C:\Program Files\Common Files\Microsoft Shared\VS7Debug\mdm.exe"
Handle Count 70
Thread Count 4
Priority: 8

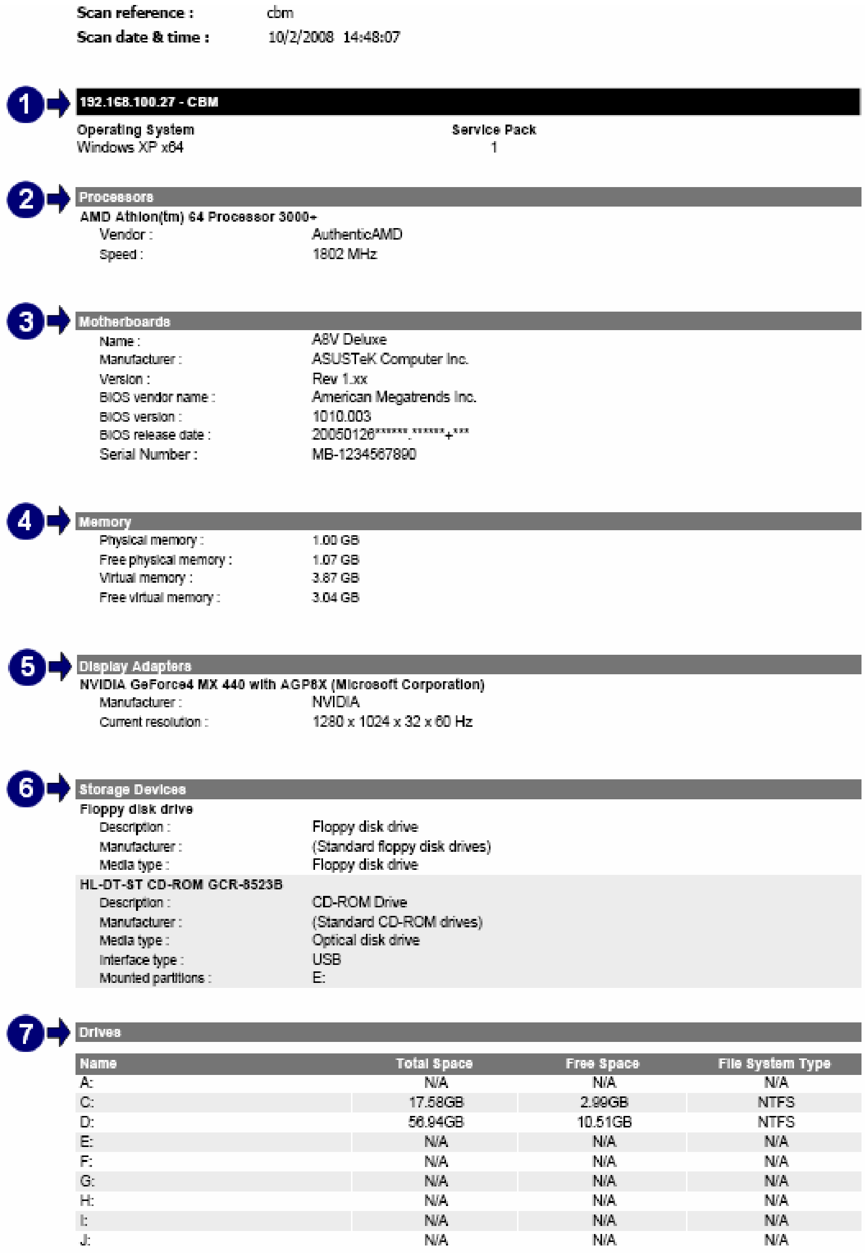
Screenshot 91 – Sample report showing processes

1	Host machine IP and name
2	Process details for each host machine, including process ID and account name

Use this report to:

- List process properties for each host machine.

Hardware Audit



Scan reference :	cbm
Scan date & time :	10/2/2008 14:48:07

192.168.100.27 - CBM

Operating System	Service Pack
Windows XP x64	1

Processors

AMD Athlon(tm) 64 Processor 3000+

Vendor :	AuthenticAMD
Speed :	1802 MHz

Motherboards

Name :	A8V Deluxe
Manufacturer :	ASUSTeK Computer Inc.
Version :	Rev 1.xx
BIOS vendor name :	American Megatrends Inc.
BIOS version :	1010.003
BIOS release date :	20050126******.******+***
Serial Number :	MB-1234567890

Memory

Physical memory :	1.00 GB
Free physical memory :	1.07 GB
Virtual memory :	3.87 GB
Free virtual memory :	3.04 GB

Display Adapters

NVIDIA GeForce4 MX 440 with AGP8X (Microsoft Corporation)

Manufacturer :	NVIDIA
Current resolution :	1280 x 1024 x 32 x 60 Hz

Storage Devices

Floppy disk drive

Description :	Floppy disk drive
Manufacturer :	(Standard floppy disk drives)
Media type :	Floppy disk drive

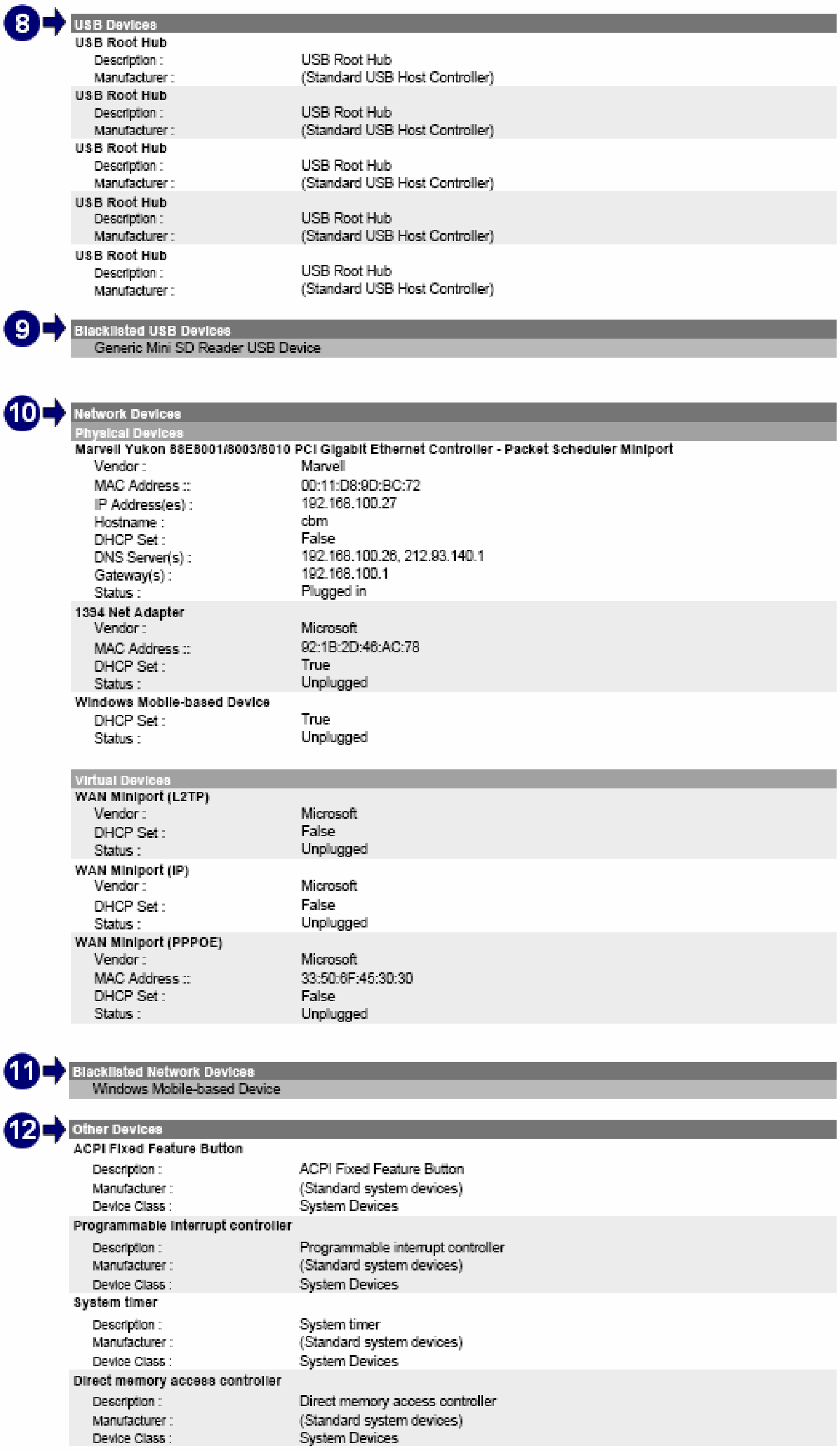
HL-DT-ST CD-ROM GCR-8523B

Description :	CD-ROM Drive
Manufacturer :	(Standard CD-ROM drives)
Media type :	Optical disk drive
Interface type :	USB
Mounted partitions :	E:

Drives

Name	Total Space	Free Space	File System Type
A:	N/A	N/A	N/A
C:	17.58GB	2.99GB	NTFS
D:	56.94GB	10.51GB	NTFS
E:	N/A	N/A	N/A
F:	N/A	N/A	N/A
G:	N/A	N/A	N/A
H:	N/A	N/A	N/A
I:	N/A	N/A	N/A
J:	N/A	N/A	N/A

Screenshot 92 - Sample report showing hardware audit - part 1 of 2



USB Devices

USB Root Hub	
Description :	USB Root Hub
Manufacturer :	(Standard USB Host Controller)
USB Root Hub	
Description :	USB Root Hub
Manufacturer :	(Standard USB Host Controller)
USB Root Hub	
Description :	USB Root Hub
Manufacturer :	(Standard USB Host Controller)
USB Root Hub	
Description :	USB Root Hub
Manufacturer :	(Standard USB Host Controller)
USB Root Hub	
Description :	USB Root Hub
Manufacturer :	(Standard USB Host Controller)

Blacklisted USB Devices

Generic Mini SD Reader USB Device

Network Devices

Physical Devices

Marvell Yukon 88E8001/8003/8010 PCI Gigabit Ethernet Controller - Packet Scheduler Miniport	
Vendor :	Marvell
MAC Address ::	00:11:D8:9D:BC:72
IP Address(es) :	192.168.100.27
Hostname :	cbm
DHCP Set :	False
DNS Server(s) :	192.168.100.26, 212.93.140.1
Gateway(s) :	192.168.100.1
Status :	Plugged in
1394 Net Adapter	
Vendor :	Microsoft
MAC Address ::	92:1B:2D:46:AC:78
DHCP Set :	True
Status :	Unplugged
Windows Mobile-based Device	
DHCP Set :	True
Status :	Unplugged

Virtual Devices

WAN Miniport (L2TP)	
Vendor :	Microsoft
DHCP Set :	False
Status :	Unplugged
WAN Miniport (IP)	
Vendor :	Microsoft
DHCP Set :	False
Status :	Unplugged
WAN Miniport (PPPOE)	
Vendor :	Microsoft
MAC Address ::	33:50:6F:45:30:30
DHCP Set :	False
Status :	Unplugged

Blacklisted Network Devices

Windows Mobile-based Device

Other Devices

ACPI Fixed Feature Button	
Description :	ACPI Fixed Feature Button
Manufacturer :	(Standard system devices)
Device Class :	System Devices
Programmable interrupt controller	
Description :	Programmable interrupt controller
Manufacturer :	(Standard system devices)
Device Class :	System Devices
System timer	
Description :	System timer
Manufacturer :	(Standard system devices)
Device Class :	System Devices
Direct memory access controller	
Description :	Direct memory access controller
Manufacturer :	(Standard system devices)
Device Class :	System Devices

Screenshot 93 - Sample report showing hardware audit - part 2 of 2

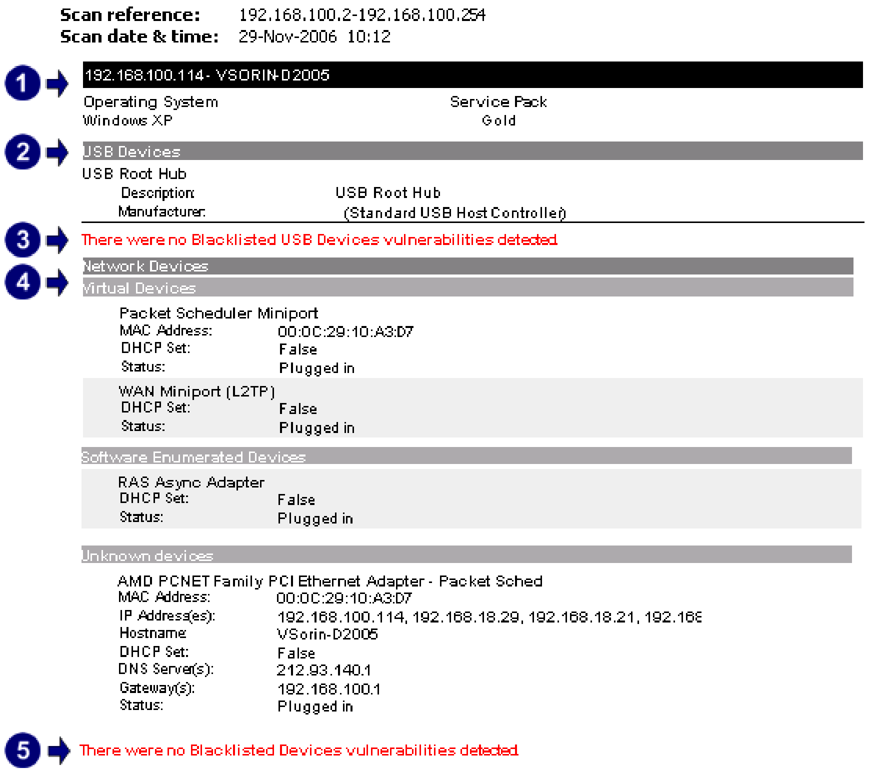
1	Host machine IP and name
2	Processor information
3	Motherboard information
4	Physical and virtual memory
5	Display adaptors
6	Storage devices
7	Drive name, space allocation and file system type
8	USB device information
9	Blacklisted USB devices
10	Physical and virtual network devices
11	Blacklisted network devices
12	Other devices

Use this report to:

- Identify all devices detected on the network for scan computers

NOTE: Devices are grouped by categories. Categories with no devices detected are not displayed.

Devices



Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 29-Nov-2006 10:12

192.168.100.114 - VSORIN-D2005

Operating System	Service Pack
Windows XP	Gold

USB Devices

USB Root Hub

Description:	USB Root Hub
Manufacturer:	(Standard USB Host Controller)

There were no Blacklisted USB Devices vulnerabilities detected

Network Devices

Virtual Devices

Packet Scheduler Miniport

MAC Address:	00:0C:29:10:A3:D7
DHCP Set:	False
Status:	Plugged in

WAN Miniport (L2TP)

DHCP Set:	False
Status:	Plugged in

Software Enumerated Devices

RAS Async Adapter

DHCP Set:	False
Status:	Plugged in

Unknown devices

AMD PCNET Family PCI Ethernet Adapter - Packet Sched

MAC Address:	00:0C:29:10:A3:D7
IP Address(es):	192.168.100.114, 192.168.18.29, 192.168.18.21, 192.168
Hostname:	VSorin-D2005
DHCP Set:	False
DNS Server(s):	212.93.140.1
Gateway(s):	192.168.100.1
Status:	Plugged in

There were no Blacklisted Devices vulnerabilities detected

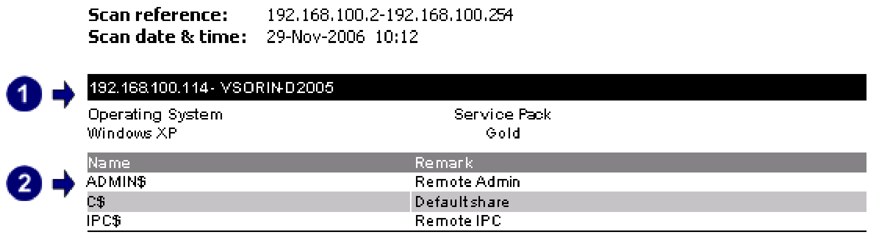
Screenshot 94 – Sample report showing devices

1	Host machine IP and name
2	List showing USB devices detected for each host machine
3	List showing blacklisted USB devices detected for each host machine
4	List showing network cards detected for each host machine
5	List showing blacklisted wireless devices detected for each host machine

Use this report to:

- List information on devices detected on the network including host information and whether the devices are blacklisted.

Shares



Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 29-Nov-2006 10:12

192.168.100.114 - VSORIN-D2005

Operating System	Service Pack
Windows XP	Gold

Name	Remark
ADMIN$	Remote Admin
C$	Default share
IPC$	Remote IPC

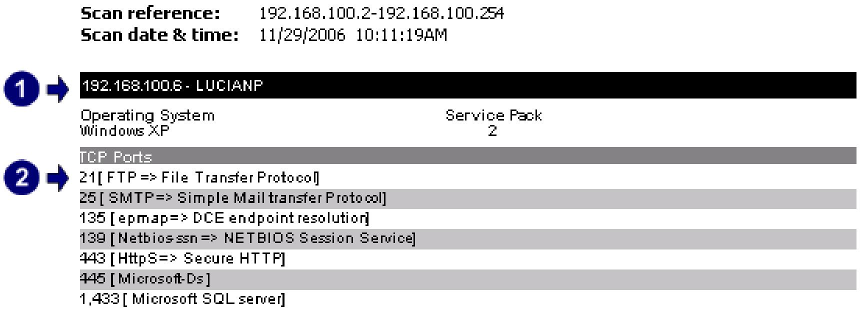
Screenshot 95 – Sample report showing shares

1	Host machine IP and name
2	Share folder details for each host machine, including name and remarks

Use this report to:

- List information on shared folders for each host machine.

Open ports



Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 11/29/2006 10:11:19AM

192.168.100.6 - LUCIANP

Operating System	Service Pack
Windows XP	2

TCP Ports

21[FTP => File Transfer Protocol]
25 [SMTP=> Simple Mail transfer Protocol]
135 [epmap=> DCE endpoint resolution]
139 [Netbios ssn => NETBIOS Session Service]
443 [HttpS=> Secure HTTP]
445 [Microsoft-Ds]
1,433 [Microsoft SQL server]

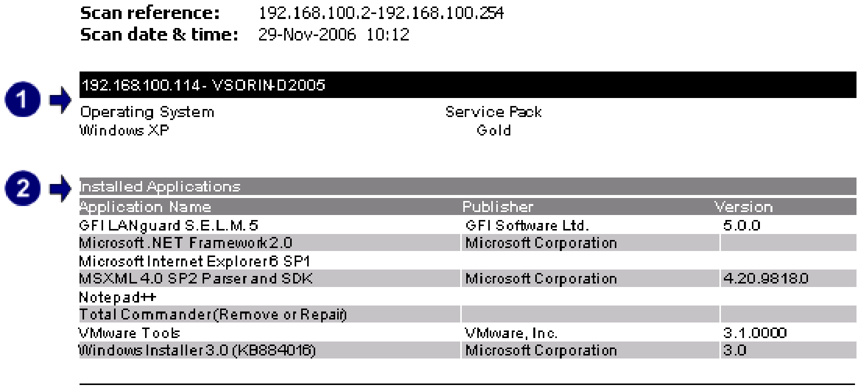
Screenshot 96 – Sample report showing open ports

1	Host machine IP and name
2	Open port details for each host machine, including port number and name

Use this report to:

- List open ports detected for each host on the network including port number and name.

Installed applications by Host



Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 29-Nov-2006 10:12

192.168.100.114 - VSORIN-D2005

Operating System	Service Pack
Windows XP	Gold

Installed Applications

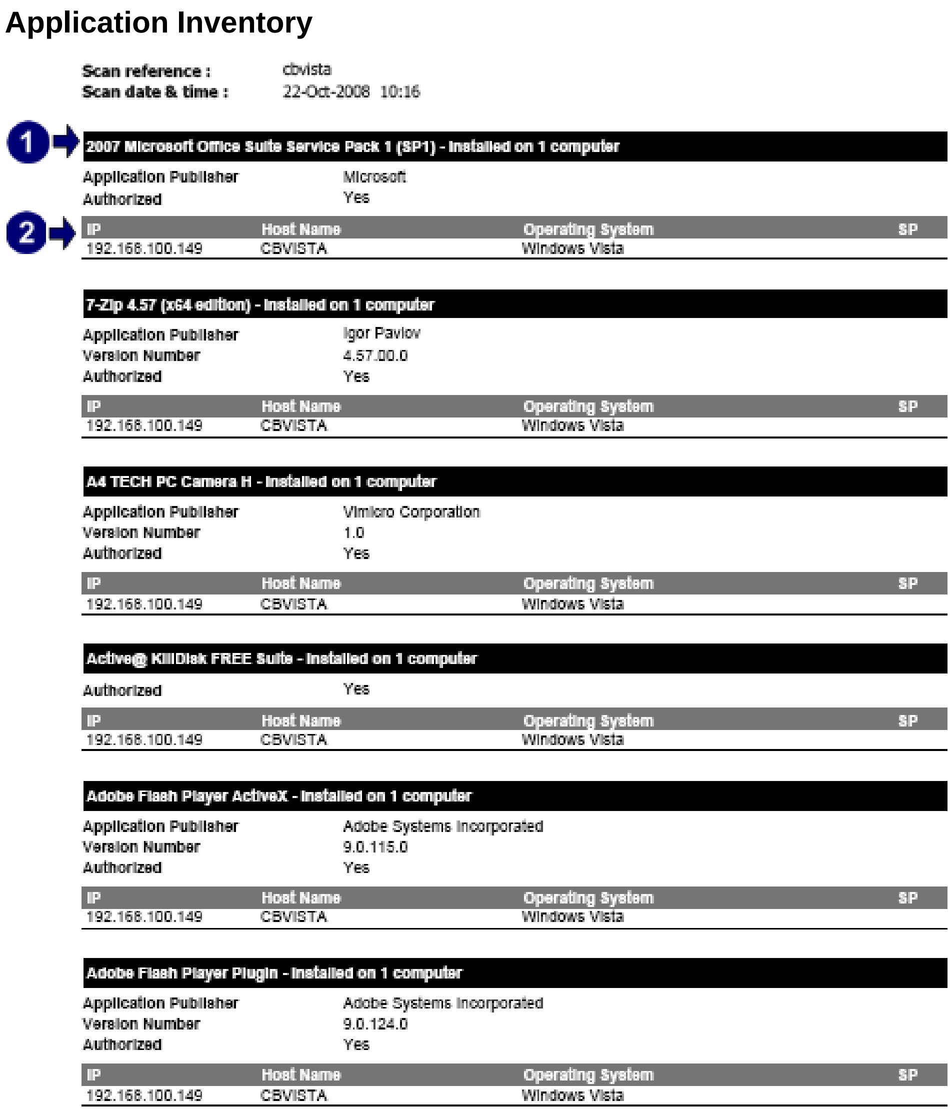
Application Name	Publisher	Version
GFI LANguard S.E.L.M. 5	GFI Software Ltd.	5.0.0
Microsoft .NET Framework 2.0	Microsoft Corporation	
Microsoft Internet Explorer 6 SP1		
MSXML 4.0 SP2 Parser and SDK	Microsoft Corporation	4.20.9818.0
Notepad++		
Total Commander (Remove or Repair)		
VMware Tools	VMware, Inc.	3.1.0000
Windows Installer 3.0 (KB884016)	Microsoft Corporation	3.0

Screenshot 97 – Sample report showing installed applications

1	Host machine IP and name
2	Installed application details for each host machine, including name, publisher and version

Use this report to:

- List installed applications detected for each network host scanned, including publisher and version details.



Application Inventory

Scan reference : cbvista
Scan date & time : 22-Oct-2008 10:16

2007 Microsoft Office Suite Service Pack 1 (SP1) - Installed on 1 computer

Application Publisher Microsoft
Authorized Yes

IP	Host Name	Operating System	SP
192.168.100.149	CBVISTA	Windows Vista	

7-Zip 4.57 (x64 edition) - Installed on 1 computer

Application Publisher Igor Pavlov
Version Number 4.57.00.0
Authorized Yes

IP	Host Name	Operating System	SP
192.168.100.149	CBVISTA	Windows Vista	

A4 TECH PC Camera H - Installed on 1 computer

Application Publisher Vimicro Corporation
Version Number 1.0
Authorized Yes

IP	Host Name	Operating System	SP
192.168.100.149	CBVISTA	Windows Vista	

Active@ KillDisk FREE Suite - Installed on 1 computer

Authorized Yes

IP	Host Name	Operating System	SP
192.168.100.149	CBVISTA	Windows Vista	

Adobe Flash Player ActiveX - Installed on 1 computer

Application Publisher Adobe Systems Incorporated
Version Number 9.0.115.0
Authorized Yes

IP	Host Name	Operating System	SP
192.168.100.149	CBVISTA	Windows Vista	

Adobe Flash Player Plugin - Installed on 1 computer

Application Publisher Adobe Systems Incorporated
Version Number 9.0.124.0
Authorized Yes

IP	Host Name	Operating System	SP
192.168.100.149	CBVISTA	Windows Vista	

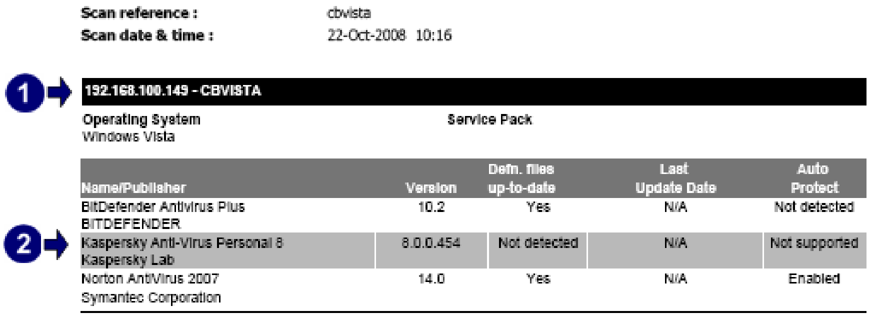
Screenshot 98 - Sample report showing applications inventory

1	Installed application name and details
2	List of computers having application installed

Use this report to:

- Identify all computers which have specific software installed on them.

Antivirus Applications



Scan reference : cbvista
Scan date & time : 22-Oct-2008 10:16

192.168.100.149 - CBVISTA

Operating System	Service Pack
Windows Vista	

Name/Publisher	Version	Defn. files up-to-date	Last Update Date	Auto Protect
BitDefender Antivirus Plus BITDEFENDER	10.2	Yes	N/A	Not detected
Kaspersky Anti-Virus Personal 6 Kaspersky Lab	6.0.0.454	Not detected	N/A	Not supported
Norton AntiVirus 2007 Symantec Corporation	14.0	Yes	N/A	Enabled

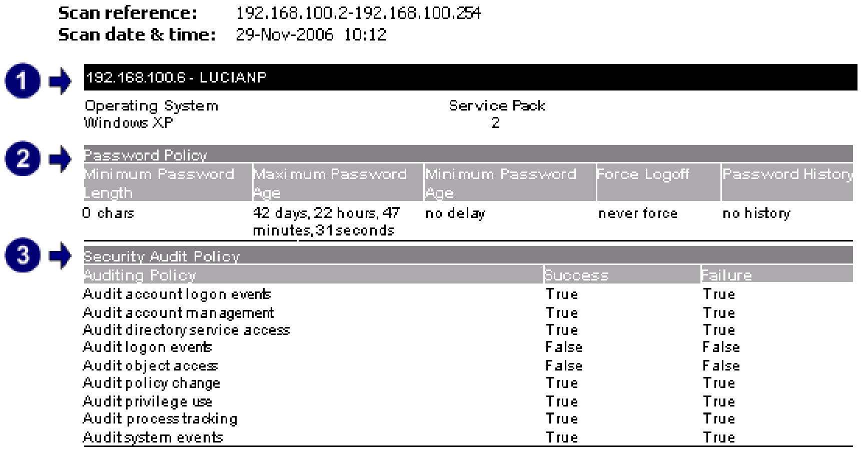
Screenshot 99 – Sample report showing installed anti-virus applications

1	Host machine IP and name
2	Antivirus application details for each host machine, including name, publisher and version

Use this report to:

- List installed antivirus applications detected for each network host scanned, including publisher and version details.

Auditing Policies



Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 29-Nov-2006 10:12

192.168.100.6 - LUCIANP

Operating System	Service Pack
Windows XP	2

Password Policy

Minimum Password Length	Maximum Password Age	Minimum Password Age	Force Logoff	Password History
0 chars	42 days, 22 hours, 47 minutes, 31 seconds	no delay	never force	no history

Security Audit Policy

Auditing Policy	Success	Failure
Audit account logon events	True	True
Audit account management	True	True
Audit directory service access	True	True
Audit logon events	False	False
Audit object access	False	False
Audit policy change	True	True
Audit privilege use	True	True
Audit process tracking	True	True
Audit system events	True	True

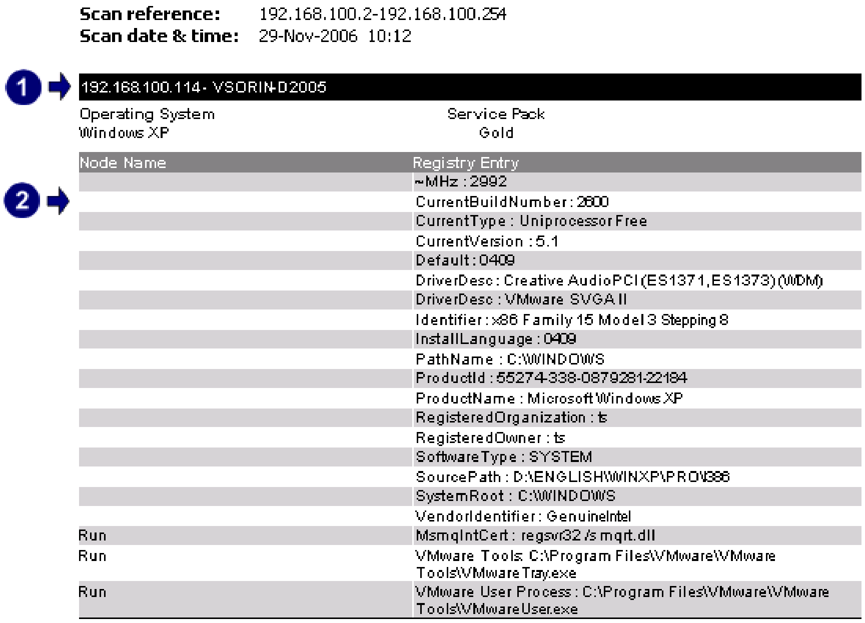
Screenshot 100 – Sample report showing policies

1	Host machine IP and name
2	Password policy details for each host machine, including minimum password length and password history
3	List showing security audit policy details for each host machine

Use this report to:

- List password and security audit policy settings for each network host scanned.

Registry information



Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 29-Nov-2006 10:12

192.168.100.114 - VSORIN-D2005

Operating System	Service Pack
Windows XP	Gold

Node Name	Registry Entry
	~MHz : 2992
	CurrentBuildNumber : 2600
	CurrentType : Uniprocessor Free
	CurrentVersion : 5.1
	Default : 0409
	DriverDesc : Creative AudioPCI (ES1371,ES1373) (WDM)
	DriverDesc : VMware SVGA II
	Identifier : x86 Family 15 Model 3 Stepping 8
	InstallLanguage : 0409
	PathName : C:\WINDOWS
	ProductId : 55274-338-0879281-22184
	ProductName : Microsoft Windows XP
	RegisteredOrganization : ts
	RegisteredOwner : ts
	SoftwareType : SYSTEM
	SourcePath : D:\ENGLISH\WINXP\PRO\I386
	SystemRoot : C:\WINDOWS
	VendorIdentifier : GenuineIntel
Run	MsmqIntCert : regsvr32 /s mqrt.dll
Run	VMware Tools: C:\Program Files\VMware\VMware Tools\VMwareTray.exe
Run	VMware User Process : C:\Program Files\VMware\VMware Tools\VMwareUser.exe

Screenshot 101 – Sample report showing registry information

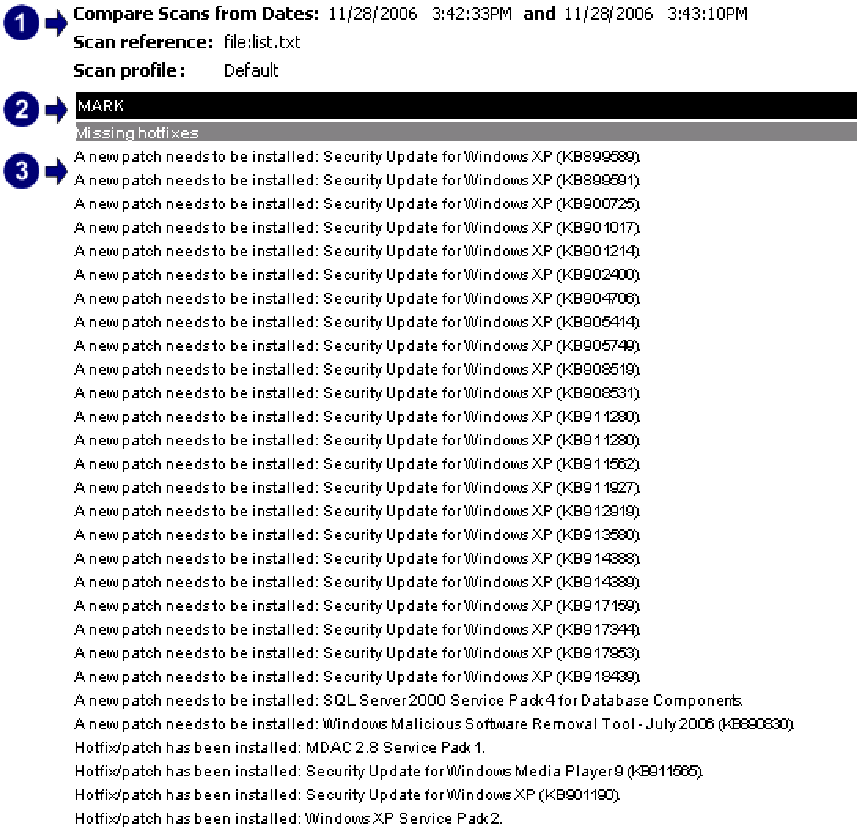
1	Host machine IP and name
2	List of registry entry details for each host machine

Use this report to:

- List system related registry information for each network host scanned.

Results comparison

Network security log by date



```
Compare Scans from Dates: 11/28/2006 3:42:33PM and 11/28/2006 3:43:10PM
Scan reference: file:list.txt
Scan profile: Default
MARK
Missing hotfixes
A new patch needs to be installed: Security Update for Windows XP (KB899589).
A new patch needs to be installed: Security Update for Windows XP (KB899591).
A new patch needs to be installed: Security Update for Windows XP (KB900725).
A new patch needs to be installed: Security Update for Windows XP (KB901017).
A new patch needs to be installed: Security Update for Windows XP (KB901214).
A new patch needs to be installed: Security Update for Windows XP (KB902400).
A new patch needs to be installed: Security Update for Windows XP (KB904706).
A new patch needs to be installed: Security Update for Windows XP (KB905414).
A new patch needs to be installed: Security Update for Windows XP (KB905749).
A new patch needs to be installed: Security Update for Windows XP (KB908519).
A new patch needs to be installed: Security Update for Windows XP (KB908531).
A new patch needs to be installed: Security Update for Windows XP (KB911280).
A new patch needs to be installed: Security Update for Windows XP (KB911280).
A new patch needs to be installed: Security Update for Windows XP (KB911562).
A new patch needs to be installed: Security Update for Windows XP (KB911927).
A new patch needs to be installed: Security Update for Windows XP (KB912919).
A new patch needs to be installed: Security Update for Windows XP (KB913580).
A new patch needs to be installed: Security Update for Windows XP (KB914388).
A new patch needs to be installed: Security Update for Windows XP (KB914389).
A new patch needs to be installed: Security Update for Windows XP (KB917159).
A new patch needs to be installed: Security Update for Windows XP (KB917344).
A new patch needs to be installed: Security Update for Windows XP (KB917953).
A new patch needs to be installed: Security Update for Windows XP (KB918439).
A new patch needs to be installed: SQL Server 2000 Service Pack 4 for Database Components.
A new patch needs to be installed: Windows Malicious Software Removal Tool - July 2006 (KB890830).
Hotfix/patch has been installed: MDAC 2.8 Service Pack 1.
Hotfix/patch has been installed: Security Update for Windows Media Player 9 (KB911565).
Hotfix/patch has been installed: Security Update for Windows XP (KB901190).
Hotfix/patch has been installed: Windows XP Service Pack 2.
```

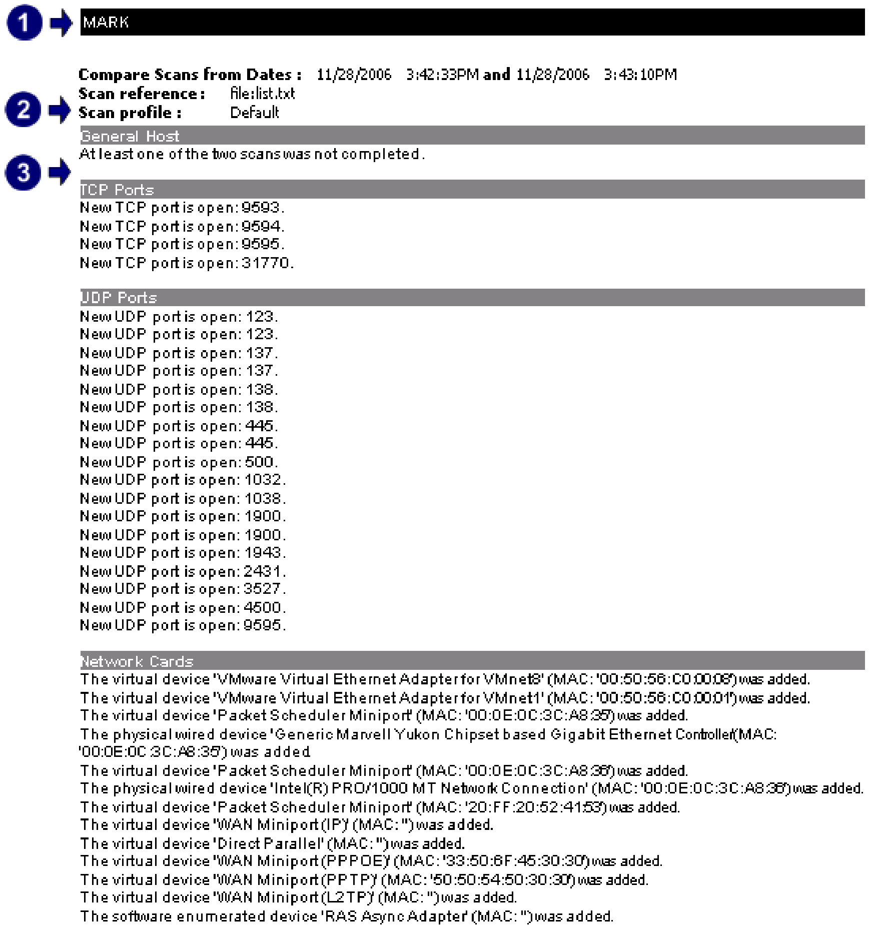
Screenshot 102 – Sample report showing network security log by date

1	Network security scans to be compared
2	Host machine on which the comparison was made
3	List of differences found between comparisons for each host machine. Differences are grouped by category, including backdoors, missing hot fixes, password policy, USB devices and applications

Use this report to:

- Compare results of consecutive scans that have a common profile and target, grouped by scan date.

Network security log by host



```
MARK

Compare Scans from Dates :   11/28/2006   3:42:33PM and 11/28/2006   3:43:10PM
Scan reference :      file:list.txt
Scan profile :        Default
General Host
At least one of the two scans was not completed.
TCP Ports
New TCP port is open: 9593.
New TCP port is open: 9594.
New TCP port is open: 9595.
New TCP port is open: 31770.

UDP Ports
New UDP port is open: 123.
New UDP port is open: 123.
New UDP port is open: 137.
New UDP port is open: 137.
New UDP port is open: 138.
New UDP port is open: 138.
New UDP port is open: 445.
New UDP port is open: 445.
New UDP port is open: 500.
New UDP port is open: 1032.
New UDP port is open: 1038.
New UDP port is open: 1900.
New UDP port is open: 1900.
New UDP port is open: 1943.
New UDP port is open: 2431.
New UDP port is open: 3527.
New UDP port is open: 4500.
New UDP port is open: 9595.

Network Cards
The virtual device 'VMware Virtual Ethernet Adapter for VMnet8' (MAC: '00:50:56:C0:00:08') was added.
The virtual device 'VMware Virtual Ethernet Adapter for VMnet1' (MAC: '00:50:56:C0:00:01') was added.
The virtual device 'Packet Scheduler Miniport' (MAC: '00:0E:0C:3C:A8:35') was added.
The physical wired device 'Generic Marvell Yukon Chipset based Gigabit Ethernet Controller' (MAC:
'00:0E:0C:3C:A8:35') was added
The virtual device 'Packet Scheduler Miniport' (MAC: '00:0E:0C:3C:A8:36') was added.
The physical wired device 'Intel(R) PRO/1000 MT Network Connection' (MAC: '00:0E:0C:3C:A8:36') was added.
The virtual device 'Packet Scheduler Miniport' (MAC: '20:FF:20:52:41:53') was added.
The virtual device 'WAN Miniport (IP)' (MAC: '') was added.
The virtual device 'Direct Parallel' (MAC: '') was added.
The virtual device 'WAN Miniport (PPPOE)' (MAC: '33:50:6F:45:30:30') was added.
The virtual device 'WAN Miniport (PPTP)' (MAC: '50:50:54:50:30:30') was added.
The virtual device 'WAN Miniport (L2TP)' (MAC: '') was added.
The software enumerated device 'RAS Async Adapter' (MAC: '') was added.
```

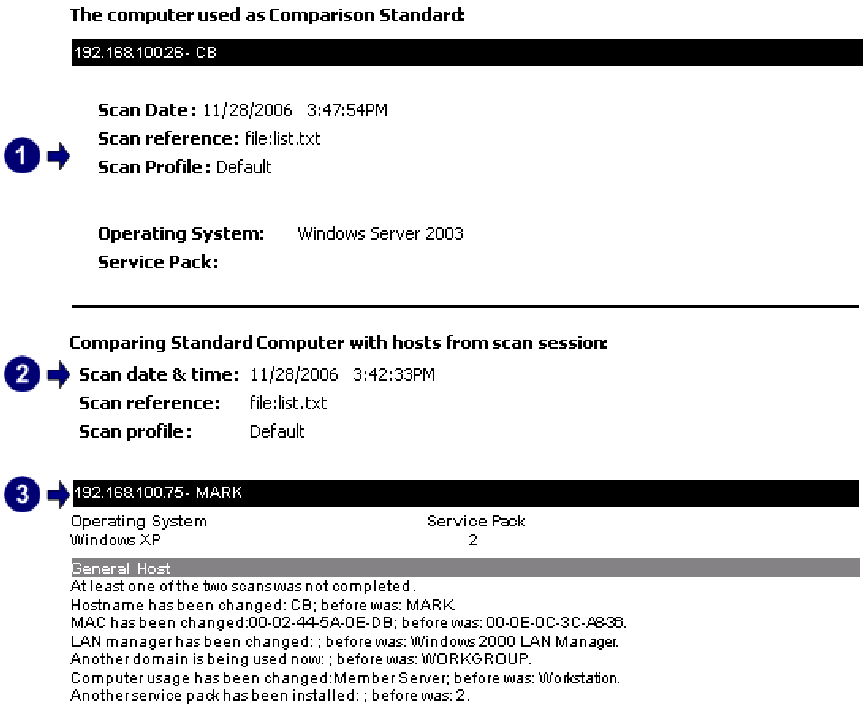
Screenshot 103 – Sample report showing network security log by host

1	Host machine on which the comparison was made
2	Network security scans which were compared
3	List of differences found between comparisons for each host machine. Differences are grouped by category, including backdoors, missing hot fixes, password policy, USB devices and applications

Use this report to:

- Compare results of consecutive scans that have a common profile and target, grouped by host machine.

Baseline changes comparison



The computer used as Comparison Standard:

192.168.100.26 - CB

Scan Date : 11/28/2006 3:47:54PM
Scan reference: file:list.txt
Scan Profile : Default

Operating System: Windows Server 2003
Service Pack:

Comparing Standard Computer with hosts from scan session:

Scan date & time: 11/28/2006 3:42:33PM
Scan reference: file:list.txt
Scan profile : Default

192.168.100.75 - MARK

```
Operating System                       Service Pack
Windows XP                                  2
```

General Host

At least one of the two scans was not completed.
Hostname has been changed: CB; before was: MARK
MAC has been changed:00-02-44-5A-0E-DB; before was: 00-0E-0C-3C-A8-36.
LAN manager has been changed: ; before was: Windows 2000 LAN Manager.
Another domain is being used now: ; before was: WORKGROUP.
Computer usage has been changed:Member Server; before was: Workstation.
Anotherservice pack has been installed: ; before was: 2.

Screenshot 104 – Sample report showing security settings comparison

1	Details of the computer used as comparison standard, including scan date, and scan profile
2	List showing host machines with which the standard computer was compared
3	List of differences found when comparing the host machines with the standard computer. Differences are grouped by category, including backdoors, missing hot fixes, password policy, USB devices and applications

Use this report to:

- Compare results between a chosen computer, used as benchmark, and host machines scanned with the same profile and having the same target.

Troubleshooting

Introduction

The troubleshooting chapter explains how you should go about resolving any software issues that you might encounter. The main sources of information available to users are:

- The manual – most issues can be solved by reading this manual.
- GFI Knowledge Base articles
- Web forum
- Contacting GFI Technical Support

Knowledge Base

GFI maintains a Knowledge Base, which includes answers to the most common problems. If you have a problem, please consult the Knowledge Base first. The Knowledge Base always has the most up-to-date listing of technical support questions and patches. To access the Knowledge Base, visit http://kbase.gfi.com/.

Web Forum

User to user technical support is available via the web forum. The forum can be found at: http://forums.gfi.com/.

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 this page closely to submit your support request.
- **Phone:** To obtain the correct technical support phone number for your region please visit: http://www.gfi.com/company/contact.htm.

NOTE: Before you contact our Technical Support team, please 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: http://customers.gfi.com.

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

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