GFI LANguard

Network Security Scanner

Security scanning and patch management

GFI LANguard Network Security Scanner (N.S.S.) checks your network for all potential methods that a hacker might use to attack it. By analyzing the operating system and the applications running on your network, GFI LANguard N.S.S. identifies possible security holes. In other words, it plays the devil's advocate and alerts you to weaknesses before a hacker can find them, enabling you to deal with these issues before a hacker can exploit them.

GFI LANguard N.S.S. scans your entire network, IP by IP, and provides information such as service pack level of the machine, missing security patches, wireless access points, USB devices, open shares, open ports, services/applications active on the computer, key registry entries, weak passwords, users and groups, and more. Scan results can easily be analyzed using filters and reports, enabling you to proactively secure your network – for example, by shutting down unnecessary ports, closing shares, installing service packs and hotfixes, etc.

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

Identifies security vulnerabilities and recommends action (or solutions)

Once GFI LANguard N.S.S. has completed scanning a computer, it categorises security vulnerabilities and recommends a course of action (or solutions). Wherever possible, further information or a web link is included regarding the security issue, for example a BugTraq ID or a Microsoft Knowledge Base article ID.

Fast TCP/UDP port scanning and service fingerprint identification

GFI LANguard N.S.S. includes a fast TCP/IP and UDP port scanning engine, allowing you to scan your network for unnecessary open ports. While identifying key open ports (such as www, FTP, Telnet, SMTP) through banner processing, GFI LANguard N.S.S. will also query the service running behind the detected open ports to ensure that no port hijacking took place.

Features & benefits

Audit your network for security vulnerabilities (Windows and Linux)

Detect unnecessary shares, open ports and unused user accounts on workstations

Check for and deploy missing security patches and service packs in OS and Office

Wireless node/link detection and USB device scanning

#1 Windows security scanner (voted by NMAP users and 200,000+ sold).

Network-wide patch and service pack management

You can deploy missing service packs and patches network-wide, without user intervention. GFI LANguard N.S.S. is the ideal tool to monitor that Microsoft SUS is doing its job properly and it performs tasks SUS cannot do such as; deploying Microsoft Office patches and custom software patches, patch reporting and immediate deployment of high alert patches.

Patching support for multilingual operating systems

GFI LANguard N.S.S. supports detection of missing Microsoft security updates and their deployment on both English and also on non-English Windows operating systems.

Automatically downloads security patches and vulnerability information

Through its auto-update system, GFI LANguard N.S.S. is always kept updated with information about newly released Microsoft security updates as well as new vulnerability checks issued by GFI.

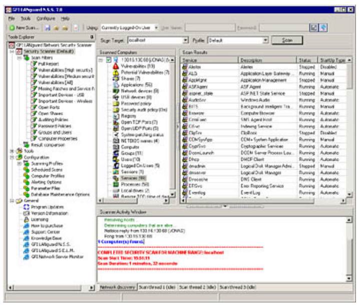
Automatically alerts you of new security holes

GFI LANguard N.S.S. can perform scheduled scans (for instance daily or weekly) and can automatically compare the results to previous scans. Any new security holes or changes appearing on your network are emailed to you for analysis. This enables you to quickly identify newly created shares, installed services, installed applications, added users, newly opened ports and more.

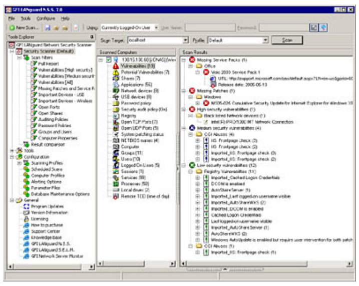
Ensures that third party security applications such as anti-virus and anti-spam offer optimum protection

It is possible to check that supported security applications such as anti-virus and anti-spyware software are updated with the latest definition files and are functioning correctly. For example, you may ensure that supported security applications have all key features (such as real-time scanning) enabled.

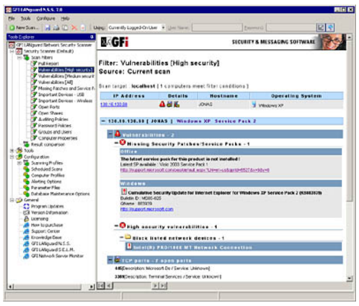
GFI LANguard Network Security Scanner



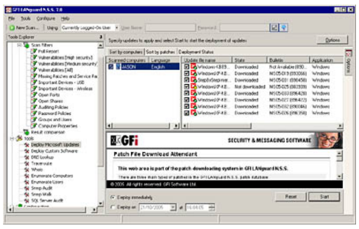
GFI LANguard Network Security Scanner main screen



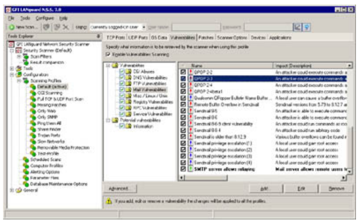
Indicates vulnerabilities found



Extensive HTML security reports

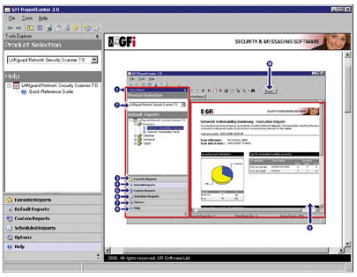


Deploy Microsoft patches node



Configuring the vulnerabilities to scan

GFI LANguard Network Security Scanner ReportPack



Quick Reference Guide

Multiply the value of GFI LANguard N.S.S. with powerful reporting

Reports designed to satisfy the requirements of both management and technical staff deliver a graphical view of the security health status of your network. From trend reports for management (ROI) to daily drill-down reports for technical staff; the GFI LANguard N.S.S. ReportPack provides you with the easy-to-view information you need, to fully understand the ever-changing security environment of your network. Full automation and custom scheduling allow you true install-and-forget functionality!

Extensive, industrial-strength vulnerabilities database

GFI LANguard N.S.S. ships with a complete vulnerabilities database, which also includes top SANS issues, as well as Linux and CGI vulnerabilities. This vulnerabilities database is regularly updated with issues reported to BugTraq, SANS, CVE and other sources. New vulnerabilities can be downloaded automatically from the GFI website.

Easily creates different types of scans and vulnerability tests

Administrators can configure scans for different types of information; such as open shares on workstations, security audit/password policies and machines missing a particular patch or service pack. Different types of vulnerabilities can be scanned for, and the scan can also be performed using different identities.

Enables easy filtering of scan results

Easily analyze the scan results by clicking on one of the default filter nodes to show, for example, machines with high security vulnerabilities or machines that are missing a particular service pack. Custom filters can be easily created from scratch and it is also simple to customize existing filters. You can also export scan results data to XML.

Finds unused local users and groups

GFI LANguard N.S.S. enumerates all local users and groups, and identifies user accounts that are no longer being used. You may then remove or disable these accounts, which could present a security risk to your network.

Finds all shares on your network

GFI LANguard N.S.S. enumerates all shares on your network, including administrative and printer shares (C$, D$, ADMIN$) and shows you who has access to the share. Use this feature to:

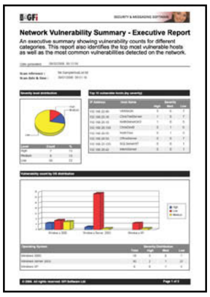
- Check if permissions of shares are set correctly
- Check whether a user is sharing his/her whole drive with other users
- Prevent anonymous access to shares
- Ensure that startup folders or similar system files are not shared as this could allow less privileged users to execute code on target machines.

Lists and detects blacklisted applications

With GFI LANguard N.S.S. you can enumerate all the applications that are currently installed on the target computers. You may also identify unauthorized or dangerous software by specifying the list of blacklisted applications that you want to locate and associate with a high security vulnerability alert.

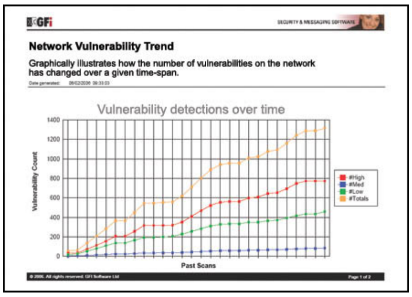
GFI LANguard N.S.S. ReportPack add-on

The GFI LANguard N.S.S. ReportPack is a full-fledged reporting companion to GFI LANguard Network Security Scanner. This reporting package can be scheduled to automatically generate graphical IT-level and management reports based on the data collected during your security scans.



Network Vulnerability Summary - Executive Report

An executive summary showing vulnerability counts for different categories. This report also identifies the top most vulnerable hosts as well as the most common vulnerabilities detected on the network.



Network Vulnerability Trend

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

Date generated: 08/02/2006 09:33:03

© 2006. All rights reserved. GFI Software Ltd

Page 1 of 2

Operating System and Service Pack Distribution

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

Detects wireless nodes and links

GFI LANguard N.S.S. can detect machines or devices which are connected to your network via a wireless link. Wireless links are a tremendous security risk if they are not secured properly.

Allows you to predefine authentication details

GFI LANguard N.S.S. allows you to store separate authentication details for every target computer on your network, avoiding the need to specify authentication credentials prior to every scan. In a single scanning session, it is possible to audit all the targets in your network, even if they require different authentication details/methods.

Enables creation of custom vulnerabilities

Using scripts and conditions, you can add your own vulnerability checks using conditions, such as checking for particular registry entries and values. You can also write complex vulnerability checks using the GFI LANguard N.S.S. VBScript-compatible script engine. GFI LANguard N.S.S. includes a script editor and debugger to help with script development.

Checks if security auditing is enabled network-wide

GFI LANguard N.S.S. checks if each NT/2000/XP machine has security auditing enabled. If not, GFI LANguard N.S.S. alerts you and allows you to enable auditing remotely. Security event auditing is highly recommended – it allows you to detect intruders in real time. GFI LANguard N.S.S.'s companion product GFI LANguard Security Event Log Monitor (S.E.L.M.) automates network-wide, real time analysis of security events.

Deploys custom/3rd party software and patches network-wide

Besides deploying patches and service packs, GFI LANguard N.S.S. allows you to easily deploy 3rd party software or patches network-wide. Use this feature to deploy client software, update custom or non-Microsoft software, virus updates and more. The custom software deployment feature obsoletes the need for Microsoft SMS, which is too complex and expensive for small to medium sized networks.

Scans for dangerous USB devices

USB devices can be a potential security problem since almost any device can be connected. This creates a potential security risk and as an administrator you have little control. GFI LANguard N.S.S. scans all devices connected to the USB hub, filters authorized USB devices (such as the mouse) and only alerts you to dangerous or unknown USB devices.

Reports NTFS and share permissions

GFI LANguard N.S.S. will display both share and NTFS permissions for all shares in your network, allowing you to easily check and lock down your shares.

Scans and retrieves OS data from Linux systems

It is possible to remotely extract OS data from Linux-based systems and scan results are presented in the same way as for Windows. This means that both Linux and Windows-based target computers can be investigated in a single scanning session! GFI LANguard N.S.S. includes numerous Linux security checks including rootkit detection.

Authentication to Linux targets through SSH Private Keys

GFI LANguard N.S.S. can use SSH Private Key files instead of the conventional password string credentials to authenticate to Linux-based target computers.

Checks status of GFI LANguard Portable Storage Control (P.S.C.)

GFI LANguard N.S.S. can also check that the portable storage control service is active. GFI LANguard P.S.C. gives you network-wide control of portable storage devices: Control which users can use a USB stick, MP3 player, IPOD, floppies and more.

Silent installation support

You can perform an unattended default installation of GFI LANguard N.S.S. on multiple computers in the background without any user interaction or intervention. Customization of the deployment parameters is also possible through the creation of Microsoft Transform (MST) Files.

Reviews

GFI LANguard Network Security Scanner named Gold Winner - TechTarget's SearchWindowsSecurity.com named GFI LANguard N.S.S. as Gold Winner of the Testing and Auditing category of its 2005 "Products of the Year" awards. The winners were selected according innovation, performance, ease of integration into existing environments, ease of use and manageability, functionality and value.

- SearchWindowsSecurity.com, January 2006

System requirements

- Windows 2000 (SP4) / XP (SP2) / 2003 operating system.
- Internet Explorer 5.1 or higher.
- Client for Microsoft Networks component – this is included by default in Windows 95 or higher.
- Secure Shell (SSH) – this is included by default in every Linux OS distribution pack.

Download your evaluation version from http://www.gfi.com/lannetscan/

GFI Software Ltd UK
Unit 2, St. John's Mews
St. John's Rd, Hampton Wick
Kingston-upon-Thames
Surrey KT1 4AN, UK
Tel +44 (0) 870 770 5370
Fax +44 (0) 870 770 5377
sales@gfi.co.uk

GFI Software USA, Inc.
15300 Weston Parkway
Suite 104
Cary, NC 27513
USA
Tel +1 (888) 243-4329
Fax +1 (919) 379-3402
sales@gfiusa.com

GFI Software GmbH
Bargkoppelweg 72
22145 Hamburg
Germany
Tel +49(0) 40 3068 1000
Fax +49(0) 700 3068 1010
sales@gfisoftware.de

GFI Asia Pacific Pty Ltd
83 King William Road
Unley 5061
South Australia
Tel +61 8 8273 3000
Fax +61 8 8273 3099
sales@gfiap.com

GFI Software Ltd
GFI House
San Andrea Street
San Gwann SGN 05 Malta
Tel +356 21 382418
Fax +356 21 382419
sales@gfi.com

Microsoft GOLD CERTIFIED Partner

www.gfi.com