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.

### 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

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.
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 to 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.

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 to innovation, performance, ease of integration into existing environments, ease of use and manageability, functionality and value.

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

GFI LANguard Network Security Scanner is a registered trademark, and GFI and the GFI logo are trademarks of GFI Software Ltd. in Germany, USA, the United Kingdom and other countries.