



GFI LANguard

Network Security Scanner

Security scanning & patch management

GFI LANguard Network Security Scanner (N.S.S.) checks your network for all potential methods that a hacker might use to attack your network. 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 hackers can exploit them.

■ Provides in-depth information about all machines/devices

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, open shares, open ports, services/applications active on the computer, key registry entries, weak passwords, users and groups, and more. Scan results are outputted to an HTML report, which can be customized/queried, enabling you to proactively secure your network – for example by shutting down unnecessary ports, closing shares, installing service packs and hotfixes, etc.

■ Network-wide patch & service pack management

GFI LANguard N.S.S. is a complete patch management solution. After it has scanned your network and determined missing patches and service packs – both in the operating system (OS) and in Microsoft applications – GFI LANguard N.S.S. can deploy those service packs and patches network-wide, without user intervention. GFI LANguard N.S.S. is the ideal companion to Microsoft SUS: Use GFI LANguard NSS to deploy service packs, Microsoft Office patches and patch reporting; and use Microsoft SUS for operating system patches. GFI LANguard supports service pack and application patching for English, Spanish, Italian, French and German versions of Windows NT/2000/2003/XP. For those who do not want to use Microsoft SUS, GFI LANguard N.S.S. can deploy patches for English versions of Windows NT/2000/2003/XP. English-version Microsoft Exchange Server, Microsoft SQL Server and Microsoft ISA Server patches can also be deployed.

Benefits

Use GFI LANguard N.S.S. to:

- Check for missing security patches and service packs
- Deploy service packs and patches
- Check for security alerts/vulnerabilities
- Detect unnecessary shares and open ports
- Check for unused user accounts on workstations
- Check password policy and strength

■ Fast TCP & UDP port scanning & 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. GFI LANguard N.S.S. identifies well-known services (such as www/FTP/telnet/SMTP) and also supports "banner grabbing".

■ Finds all shares on your network

GFI LANguard N.S.S. enumerates all shares on your network, including administrative shares (C\$, D\$, ADMIN\$) and printer shares. Using this feature you can:

- 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.

■ GFI LANguard N.S.S. "alerts" pinpoint security issues & recommends action

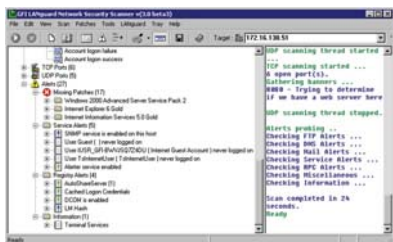
Once GFI LANguard N.S.S. has completed scanning a computer, it generates an "Alerts" node which details key security issues and recommends a course of action. Wherever possible, GFI LANguard N.S.S. includes further information about the security issue or a web link to more information, for example a BugTraq ID or a Microsoft KnowledgeBase article ID.

■ Automatically detect NEW security holes with scheduled scan results comparisons

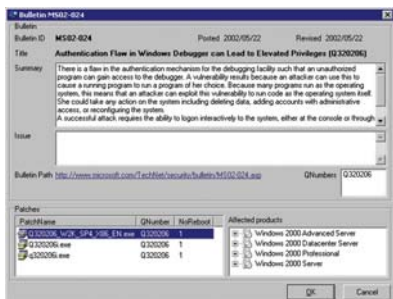
GFI LANguard N.S.S. can compare scan results and identify new security holes on your network. The scheduled scan feature allows you to schedule daily or weekly network scans, which can then be automatically compared to previous scan results. This enables you to quickly identify changes such as newly created shares, installed services, added users or added ports. It can also automatically email you a list of changes.

■ Find unused local users and groups

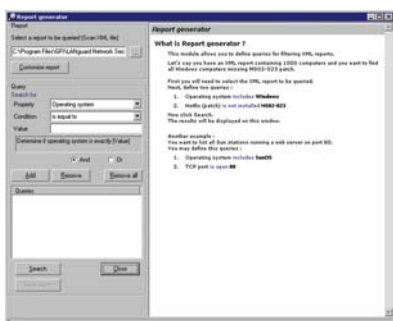
GFI LANguard N.S.S. enumerates all local users and groups, and marks user accounts not being used. It is important to disable all unused accounts and ensure that the used accounts (administrator) have a strong password.



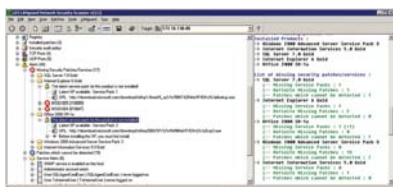
GFI LANguard N.S.S. main window



Detailed information on each Microsoft bulletin



Use the report generator to create custom queries on scan results



Using GFI LANguard N.S.S. to deploy missing service packs and patches network-wide



System requirements

- Windows 2000/2003 or Windows XP.

■ Automatically downloads Microsoft security patch information

GFI LANguard N.S.S. always has up-to-date information about Microsoft security patches, exploits and Hotfixes because it automatically downloads the Hotfix and security bulletins from the Microsoft website.

■ Vulnerabilities database includes UNIX/CGI issues

GFI LANguard N.S.S. also audits for UNIX and cgi vulnerabilities. The GFI LANguard N.S.S. vulnerabilities database is regularly updated with issues reported to BugTraq. New vulnerabilities can be downloaded automatically from the GFI site.

■ Query generator for scan reports

Because scan reports can include a lot of data, GFI LANguard N.S.S. includes a query generator that allows you to filter the XML scan reports for specific data. For example, you can query a scan result for all machines with shares, or for all machines running FTP servers.

■ Identifies all installed NT/2000/XP services

Disable all services that you do not need! All services running on the scanned machines are listed. Each service can be a potential security risk, so closing/switching off what you do not need automatically reduces the security risk.

■ Check password policy

GFI LANguard N.S.S. can automatically check password policy for all machines on the network. You can ensure that the password policy is secure, for example, by enabling a maximum password age, password lockout and password history.

■ Check if auditing is enabled & enable network-wide auditing

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 permits you to enable auditing remotely. Security event auditing allows you to detect intruders in real time. GFI LANguard N.S.S.'s companion product GFI LANguard S.E.L.M. automates network-wide, real time analysis of security events.

■ Other features:

- Check for programs that run automatically (potential Trojans)
- HTML/XML reports
- Make an inventory of your network
- LANguard Scripting
- Find out if the OS is advertising too much information.

■ You're in good company

Many leading companies have chosen GFI LANguard N.S.S. Here are just a few: Daimler Chrysler, Siemens, EDS, United Overseas Bank Ltd, Virgin Mobile and many more.

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

Computers Plus (01296) 658974

