

# LANguard Network Security Scanner 3.3

➔ by **Andrea Pompili** (apompili@infomedia.it)

About three years ago GFI launched a freeware application called LANguard, capable of performing in-depth probing especially on Windows-type systems. The program was actually capable of both doing netbios queries and verifying the contents of the analysed host's registry, therefore providing quite complete and effective results.

Over the years the product has evolved and acquired an increasingly commercial nature up to version 3.3, which has many interesting features both for security management purposes and vulnerability analyses.

Although this description pertains to the commercial version, a freeware version of the product is also available, although devoid of some security management features (patch management, handling of reports and so on) it is useful in performing "impromptu" analyses of the network.

## Probing the network

Once installed, LANguard can be used to scan the same workstation or an entire subnet by simply filling the required field with either the host name, a single IP address or a range of addresses, or even specifying a file name referring to a list of the host to be verified.

After the scan has been started using the required button, the program will begin a discovery activity of the selected network using initially a standard ping; if no answer is returned, the program will first send a netbios query and then a SNMP query. If none of these three produces a positive result, the host is marked as "inactive" and, if the scan has only been performed on it, the program will recommend the user to increase the timeout and then retry the scan.

Once the discovery of all the active network elements has been performed (or just the accessibility of a certain host), LANguard will begin to execute a series of probes with different degrees of complexity, each one based upon the following controls:

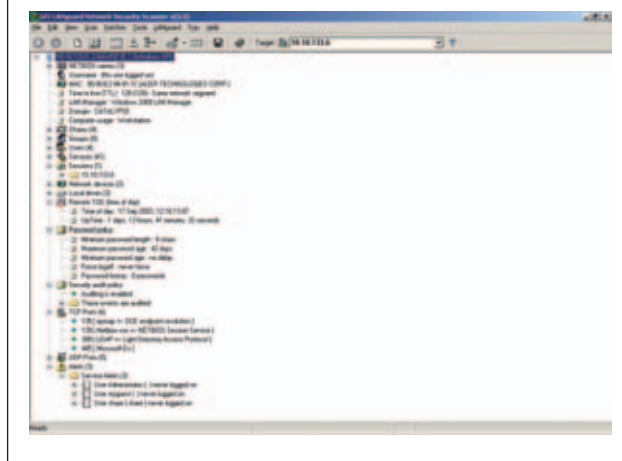
1. First of all LANguard collects the system's netbios names (the joined domain, the currently connected user and the machine name).
2. Then all the available shares and the related authorisations are verified. The analysis implies also verification of the strength of the access credentials. This activity can be configured, providing specific credentials to be used or even trying a brute force activity (enabling this option significantly slows the scan down).
3. A connection to the remote registry is then made to download all the information regarding ma-

*LANguard is one of the "all-purpose" tools that are invaluable for people who monitor and control network security. The offered functions and the product's solid background contribute as well to make this product more efficient with respect to other similar, quite ambiguous, products that clutter up the market nowadays.*

chine configuration, enabled audits, installed patches and active services.

4. The next step is the extraction of all the users configured on the host, including the groups it belongs to and the associated privileges. At the same time, a preliminary password check is made (for example to check if there is a non-existent password or it's equal to the account ID).
5. Then the whole SNMP tree (if active) associated to the host is rebuilt.
6. After these simple probes a Vanilla scan is performed on all the best known TCP ports. The banner returned after each access is then extracted and analysed. So the TCP scan is executed by completing the entire three-handshake-protocol on each controlled port.
7. Then an ICMP port unreachable scanning is performed on all the main UDP ports (an UDP packet is sent and the reception of an ICMP\_PACKET\_UNREACH packet, the typical answer of some operative systems if the port is closed, is checked).
8. After the scan the program performs OS fingerprinting: some test packets are sent to verify,

**FIGURE 1** A whole bunch of detailed technical information is displayed really fast. In a few seconds you can get an adequate level of auditing details without being a security wizard



more or less accurately, the operative system. For example, if the host TTL is 128 LANguard will deduce that the system is “probably of the Windows type”, but if the other tests on open ports or on the banners returned by the available services provide further results, the answer can be refined until the real nature of the system (98, 2000 or XP for example) is assessed. The configuration files for this activity are found in the Fingerprint directory of LANguard and can be easily extended or modified by the system user.

- Using the just retrieved information, the system executes a vulnerability check and some possible configuration error tests, e.g. users that are never actually used, open shares or weakness in the authentication system. If the system is part of the Windows family, missing patches and service packs are also checked using information collected remotely from the local registry. The tests to be performed are all stored in an internal database that can be updated by connecting to the GFI site using the Check for Security Update menu under the Help heading in the main menu.

Once a scan has been completed (Figure 1) it is possible to carry out some additional tests like a dictionary attack on the collected credentials or a simple LanMan Hash crack if the system belongs to the Windows 9x family. In the first case it is possible to use an adequate dictionary file, i.e. a list of words to be used in all possible combinations (LANguard comes with a base dictionary, that contains only English words, located in the Config directory). In the latter case the attempted attack is one well known on the Windows 9x machines and based on the weaknesses of the stored hash (<http://support.microsoft.com/support/kb/articles/Q273/9/91.ASP&NoWebContent=1>). Other available options are the sending of messages through NETBIOS Messenger using a spoofed IP or machine name, or the deployment of patches or service packs. In order to perform an optimal scan, LANguard must be configured beforehand using the Options panel under the Scan heading of the main menu. The number of options that can be configured is astonishing and LANguard allows one to configure all the probes described in the previous list (including the timeout and the ports to be checked, with the associated services), to specify the account to be used during the netbios connections to the file system and the remote registry (choosing between the currently connected user, a NULL session or a specific account) and lastly performs checks on databases and installed patches, if there are any. As mentioned in the user manual, LANguard does not perform mechanisms to bypass firewalls or IDS as the well known Nmap or N-Stealth (a quite efficient CGI scanner produced by Nstalker) do. All the probes can consequently be detected by these protection systems and therefore reported as attacks. So it is a good idea to agree on these activities with the administrators beforehand.

Moreover, the scanner is absolutely Windows-oriented and, although it can detect other systems with an appreciable accuracy as well (including Cisco's IOS), the tested vulnerabilities are surely less than those related to the Redmond's system. It must be mentioned that, as we will see with greater detail later, LANguard offers the possibility to write down one's own tests, and therefore has a great versatility from this point of view as well.

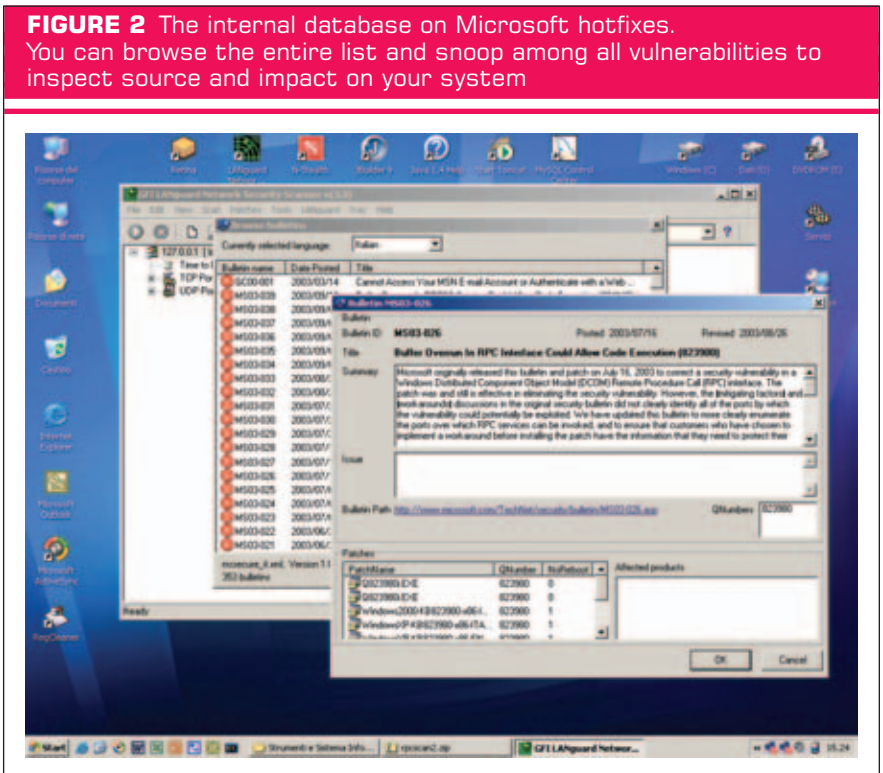
### Report and results analyses.

After the scan is finished, it is possible to save all the returned data on a the local hard drive both in HTML and XML format choosing the headings and the specific report format. LANguard uses XSL and XML to format HTML reports and to store the returned data. It is also possible to define one's own template using one of the following procedures: write an XSL file which can be put in the xsl directory (a subdirectory of Config) and then added with a proper registration line inside the custom\_reports.xml file in the same directory, or even visually customising one of the predefined models at the time of saving. The first option is much more flexible and makes it possible to customise the report's graphic layout, which is necessary if one wants the firm's logo on the report's title page or to use specific colours or formats. The second option, instead, allows only the modification of the report's header and footer and the specification of the data to be printed or not.

The generated reports can then be reloaded on the system using the Report Generator, which also offers the option of querying, researching or further formatting. Another interesting function is the possibility to compare the results of two subsequent scans using the Results Comparison function. Just specify two XML reports and the system will verify all the difference between them, which will be presented on the screen together with an explanation note. This function can be also used for scheduled scans, which LANguard manages by means of the relevant panel under the Scan heading of the main menu. To perform scheduled activities it is necessary to start up the GFI LANguard N.S.S. Scheduled Scans Service that the program configures during installation. Then you must specify the date and time of the scan and the concerned subnets and LANguard will perform the tests autonomously storing the generated report in the default directory. The program can also compare the current results with the previous ones and, in case there are some differences, notify the system administrator by e-mail.

### Patch management

Despite appearances, LANguard is more oriented towards prevention and security management. In fact the key featu-



re of this instrument is the possibility of distributing patches and service packs on Windows systems from a remote station once the vulnerabilities or the missing updates have been revealed.

The patches can either be simple hotfixes, whole service packs or autonomously made corrections or programs. LANguard behaves as a software distribution system and makes it possible to decide which hosts have to be updated, the updating approach and the items to be installed.

The program can be configured to automatically download the list of the latest updates available directly from the Microsoft website in the desired language (in the previous version this function was available only for Windows systems in the English language). It is therefore possible to navigate all the available patches and download them locally on the own system and then distribute them later on the controlled machines.

Each patch is equipped with a detailed description and all the official references in order to help the network administrator in identifying the most important ones and to inform him on all the associated vulnerabilities (Figure 2).

LANguard handles both updates for the Operating System (NT, 2000 and XP), Internet Explorer (from version 4.0 to 6.0), Office 2000 and XP, and other Windows server applications such as ISA Server, IIS (from 3.1 to 5.1), SQLserver 7 and 2000, and Exchange 5.5 and 2000.

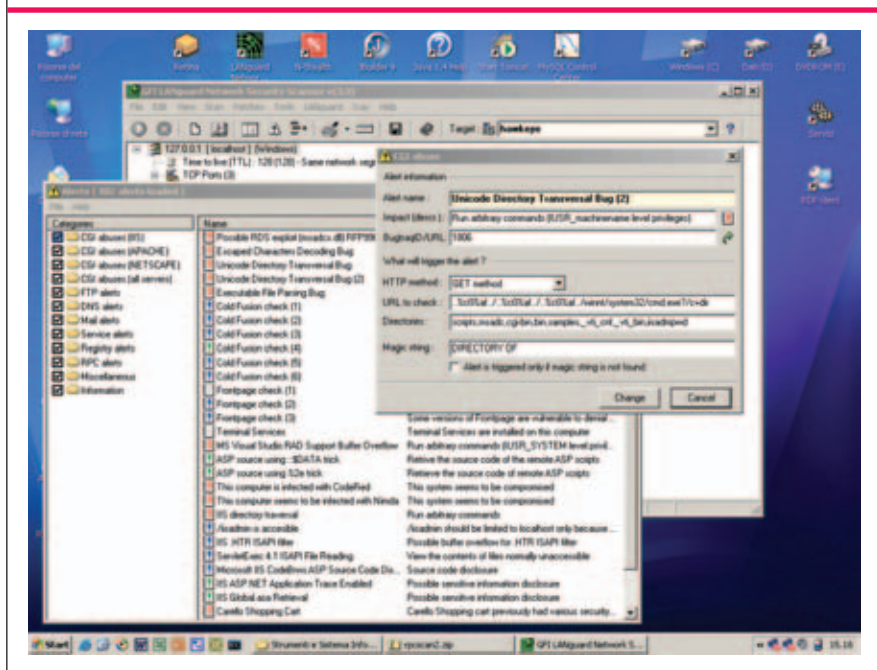
Regarding custom patches, LANguard allows one to specify both the operating system and the specific software it pertains to, in order to guide installation in the next steps. Using this function it is possible, for example, to install additional applications such as Flash plug-ins, DirectX upgrades or third-part applications.

Patch deployment can be performed manually once the network scan has been completed. It is possible to decide which updates install (hotfix, service pack or custom programs) and whether they must be installed on all the detected machines or only on one. LANguard will automatically verify which elements are missing and will install them on the remote system (it is necessary to use credentials associated to administrative users on the remote machines to perform the operation correctly). It is also possible to input a warning message which will be returned to the connected users when the installation is launched, to decide whether to halt the services to be updated or not, to force the updated machine to reboot or not (the majority of patches require this after installation) and lastly whether to execute the installation immediately or delay it to a chose time and date.

### Customised tests and LANS

Another LANguard feature is its versatility with regards to the type of tests that can be carried out. Besides the upgradeable internal database provided by GFI, it is possible to build your own custom tests using one or more approaches depending on the complexity of the test itself. Using the Configure Alerts panel, under the Scan heading, it is possible to handle the internal test database by choosing the tests to be performed, removing some or adding others. In particular, all the tests are divided in predefined categories. Unfortunately it is possible to activate or deactivate only an entire test's family: specific tests can be deactivated only removing them independently from the internal database.

**FIGURE 3** A CGI text example on IIS and Unicode Traversal Directory. The software sends a HTTP get against the host to execute a directory browse using DOS CMD command. If you get a result which includes a "DIRECTORY OF" then the system is assumed as exploitable



Creation of a new test is rather simple. Just select one category, set the information on the vulnerability type and the Bugtraq ID and then use the Wizard to add the basic tests that will determine the presence of the vulnerability issue.

As regards CGI tests, which are the tests used to control vulnerability on HTTP services, the configuration is even simpler: just insert the URL to be launched, the http query type and the string to be verified in the returned http reply. Figure 3 shows an example of CGI test on IIS for the Unicode Traversal Directory bug. Basic tests can instead be based upon different types of information:

- Operating System type
- The existing of specific opened or closed TCP/UDP ports
- The installation (or lack of) specific services (IIS, RPC and so on).
- The installation (or lack of) specific hotfixes or service packs.
- The presence or absence of registry keys or paths and the confirmation of certain values found in them
- Analysis of the banners returned by the detected services (strings contained in them, regular expressions and so on).
- Values returned by a LANS script (true or false).

The first checks can all be configured using a wizard, specifying the validity condition, the element to be verified and, in some cases, the comparison value. On the other hand, the last feature employs one of the product's key features: the LANguard Scripting language, or LANS. LANS is nothing but a proprietary scripting language, whose syntax resembles C, that allows the building of quite complex tests using predefined networking functions and other string management features. A LANS script can therefore return true or false as a value. This value is interpreted by the LANguard engine and handled according to the condition which the implemented test was based upon. The scripts can be written using a special editor installed with LANguard which, besides syntax highlighting, allows the execution of the scripts in a safe environment for tests and correctness checks.

**Product Technical Sheet**

Name and Version	LANguard N.S.S.
Category	Vulnerability scanner and patch management system
Builder	GFI Software Ltd. 15300 Weston Parkway Suite 104 Cary, NC 27513 USA Tel. +1 (888) 2 GFIFAX Tel. +1 (888) 243 4329 Tel. +1 (919) 379-3397 Fax +1 (919) 388 5621 Tech support +1 (919) 297-1350
Distributor	GFI Divisione Italia GFI House San Andrea Street San Gwann SGN 05 Malta - Tel. 049 8649076
Download the Trial from	<a href="http://www.gfi.com">http://www.gfi.com</a> <a href="http://www.gfi-italia.com">http://www.gfi-italia.com</a>
Price	Up to 25 IP: 295 € Up to 50 IP: 375 € Up to 100 IP: 475 € Up to 250 IP: 750 € Unlimited IP: 925 € (for each person using the product)
Operative System	Windows NT/2000/XP
Disk Space	~17 Mb

For further information about the language syntax and the defined functions please refer to the guide distributed with LANguard, which is quite detailed and complete and provides many good examples.

**Conclusions**

LANguard is surely a fundamental instrument for those who handle small-sized networks or are in need for a “quick” tool to verify specific LAN within one’s own Intranet. Moreover, the program’s versatility and the functions included inside represent an enormous added value to security which, taking into account the product’s price, make LANguard really much more desirable than other, more expensive, solutions.

**Bibliography**

[1] GFI Software Ltd., “GFI LANguard Network Security Scanner 3.3 Manual”, 10/07/2003

**Biografical notes**

*Andrea Pompili* is a Computer Engineering graduate. Since graduating he has worked in the analysis and development of Enterprise-type Portals on Java platforms. Later he turned to architecture and assessments of computer security in the Telecommunications sector. At the moment he works for the Telecom Italia S.p.A. group.