

## security

### Product Review

## GFI LANGUARD NSS SEES FROM HACKER'S VIEW

APPTech, a solution provider based in Tacoma, Wash., has specialized in network and software services since 1988. APPTech is a Microsoft Certified Partner and a Symantec Enterprise Solution Provider. This product was tested and reviewed by APPTech CEO Darrel Bowman; Debbie Block, Certified in Security+ and NSA; and John Jolly, Certified in MCSE, MCPs, MCSO, MCPsI, MCNPs and Security+.



GFI LANguard Network Security Scanner is an auditing tool used to proactively secure networks. GFI LANguard NSS scans entire networks from a hacker's perspective. The tool analyzes devices on

a network for missing security patches, service packs, open ports, unused user accounts and more—in short, searching for any vulnerabilities.

Administrators can easily lock down their network against hackers using this tool. If the tool finds potential points of entry, it will remotely deploy missing patches and service packs in applications and operating systems.

GFI LANguard NSS uses a Windows-based GUI to perform DNS

lookups, pings and trace routes, as well as to display vulnerability alerts. It performs operating system detection and password-strength testing; detects registry issues; and shows all users and groups, services, processes, and more.

Another key feature is a patch management solution. GFI LANguard NSS first checks the service pack level and searches for installed hot fixes. Then the tool scans the network to determine where missing patches and service packs should be deployed, and applies them networkwide.

We planned to test GFI LANguard NSS in two environments, but we were only successful in one. Our initial test was conducted in our test network, which consists of 15 PCs using Windows 2000/XP Professional and three servers running Windows 2003, Red Hat and


Windows 2000, respectively. In addition, our test network has an 802.11x wireless connection, a Symantec 360 Firewall and a Cisco switch.

Installing the software was a snap. After running the initial scan, we were impressed with the tool's ease of use. The initial report was very detailed and informative. The reports generated were very accurate and actually caught more vulnerabilities than we thought we had. However, we thought there should have been an easier way to chart, graph and summarize the information when customizing the report for executive management.

After verifying the results, it

### TOP 6 GFI LANGUARD KEY FEATURES

- 1
**IDENTIFIES** security vulnerabilities and recommends appropriate action
- 2
**SCANS AND IDENTIFIES** fast TCP & UDP ports
- 3
**MANAGES** patches and service pack installations
- 4
**DETECTS** existing wireless nodes and links
- 5
**SCANS** attached USB devices for vulnerabilities
- 6
**CHECKS** Linux OS for vulnerabilities



SOURCE: APPTech

was on to the next task. We decided to load the software onto a Dell Latitude laptop with a fresh installation of Windows XP Pro and take it to a neighboring college to test in the college's training network. Although in theory this was a great idea, we had to abort the plan. The laptop installation caused the program to generate several errors before we even left our network. After reviewing the manual and online knowledgebase, we decided to try GFI's online chat support.

This was a great opportunity to anonymously check out the tech support at GFI. This process gave us a huge amount of confidence in GFI's tech support, as well as the company's level of knowledge about its product and all facets of security. As of this writing, our errors have not been diagnosed, but we did, after all, have a deadline for this review. Like most other engineers, we know when we're being snowed by tech support, and this was not the case here.

The manual we reviewed was a great example of GFI's engineering and security expertise—it is very informative and easy to

read. In fact, it's one of the few manuals we've read that actually provides valid reasons for errors and methods for correcting vulnerabilities.

The software does have a weak point in its ability to perform SNMP audits by testing password strength against a dictionary of commonly used passwords. The process takes less than five seconds. Even the least skilled administrator knows this indicates a rather small, skimpy dictionary. A larger built-in dictionary would be useful here.

Another possible drawback is SNMP community string scanning. For each community string, the software needs to complete an entire scan of all IP addresses rather than simply checking each device against a list of community strings and then moving on to the next device. This feature is sure to slow down scans of larger networks and might bog down resources considerably.

Channel sales opportunities are available for resellers and distributors. The full retail prices for the GFI LANguard NSS tool are competitive

## GFI LANGUARD NETWORK SECURITY SCANNER

> **Company:** GFI Software  
Cary, N.C.  
(888) 243-4329  
www.gfi.com

> **Tech Rating:** ★★★★★

> **Channel Rating:** ★★★★★

> **Distributors/Integrators:**  
Direct from vendor

NOTE: RECOMMENDED STATUS IS EARNED WITH A SCORE OF AT LEAST EIGHT STARS OUT OF 10.

and start at \$375 for 25 IP addresses and \$999 for an unlimited number of addresses. A full consultant license is \$1,999—a great price for solution providers offering network security services.

There is no cost or authorization requirements to become a reseller, and partners receive demonstration copies, sales leads, a partner newsletter and technical and sales support by e-mail, fax and phone.