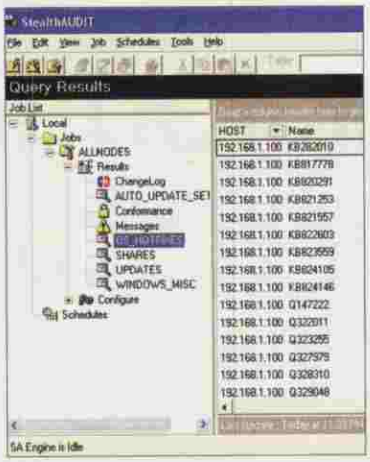
Targeting Known Weak Spots

Most of the products in this roundup follow one principle: You point them at all or part of your network, then let them loose to scan the terrain for any vulnerabilities. What you receive back are reams of data on all types of potential problems, in all areas of your network.

If you're already aware of specific problems on your network and want to zero in on them, however, an auditing tool like Stealthbits Technologies' StealthAudit could be the answer. StealthAudit can narrow your network scans based on queries you feed it. For example, if you know that some nodes on your network don't have the critical Microsoft Security Bulletin MS03-039 installed and want to identify those nodes, you could query StealthAudit with that specific request. This eliminates the burden on your network of performing an extensive, hours-long vulnerability scan that would produce a heap of unneeded information.



StealthAudit's queries can be customized to scan for specific hot fixes based on Microsoft's database.

StealthAudit is a comprehensive and extremely configurable agentless audit application for Windows-based networks. Information gathering with StealthAudit identifies more than just patch-level issues; it provides a wide range of information about network nodes. The application provides an easy-to-use and extremely intuitive interface.

StealthAudit's query tools help you zero in on specific problems.

StealthAudit is organized around the creation of *jobs*, which include the query, results, and accompanying report. You can create the query manually or via a wizard. By using resources like remote registry access, WMI (Windows Management Instrumentation), perfmon statistics, Active Directory, and the event log, queries can cover an infinite number of issues. Examples of queries include Windows log-on–related settings and user privileges, a system shutdown without a valid log-on, display of disabled accounts, and password expiration. Queries can also identify Web servers that were secured with the IIS lockdown tool, high-risk services running on hosts, and NetBIOS-related vulnerabilities. The queries can be customized down to the level of manually editing the XML source, which can be helpful if you have a complex environment.

You can use all queries to generate reports, which you can then publish to your Web server, indicating the name of the user that generated them and providing a hyperlink to the report. There are also many predefined reports available.

Regardless of the size of your network, StealthAudit is an indispensable tool, especially if you often find yourself trying to collect targeted information from many nodes. The application also runs fast without taxing your network bandwidth, according to our anecdotal testing. (50-node license, $300 list per server, $3 per desktop; for Microsoft Exchange networks, $300 per host, $3 per individual mailbox or public folder. Stealthbits Technologies, 630-357-2513, *www.stealthbits.com*.)—*OK*

specifically required by important systems on their network.

Deployment of Security Analyzer's agent is very straightforward. You need to specify a port, generate an encryption key, and place that key in a DAT file for host-to-console communication. Also, from a log-on script, the agent can be installed on target systems in silent mode. You can either run tests on demand or use the scheduler to launch the scan profiles at predetermined times.

Security Analyzer ships with a number of predefined scan profiles you might perform regularly, such as Microsoft Security Bulletin, Common Vulnerabilities and Exposures, and CERT and BugTraq advisory and analysis. Alternatively, you can create your own scan profiles from 21 different categories.

Scan results are displayed in an organized, straightforward three-pane window. A tabbed interface lets you view your data in the left-hand pane based on host IP address, risk level, vulnerabilities, services running, users, fixes needed (ranked by risk), and the testing policies applied to the scan. The right-hand pane displays detailed information for the data element selected in the left-hand pane. The pane running across the bottom of the screen shows you a description of the vulnerability with links to additional information, as well as recommendations for fixes with links to patches, if available.

Similar to Retina and SAINT 5, Security Analyzer has a comprehensive report generator. You can choose to generate reports on the current or previous scan results or run a comparative report against previous results to determine your remediation progress. You can also e-mail your reports from within the program.

Organizations with pure Windows environments should be satisfied with the many options and features Security Analyzer provides. And if you're not sure whether to buy it, you can use a limited trial version at NetIQ's Web site.—*CE*

More on the Web

Log on to **www.pcmag.com/securityglossary** for comprehensive definitions of security terms in this story.