

Tools and Services That Find the Top 20 Vulnerabilities On Your Systems And Networks*

Updated October 2003 | Page 1 of 1

Services You Can Use To Scan Your Systems Without Installing New Software

Qualys:

In support of the SANS Institute initiative, Qualys(tm), Inc., the leader in Managed Vulnerability Assessment, is offering a free network scan designed specifically to help companies detect and eliminate the 20 critical vulnerabilities announced today by SANS, the FBI and FedCIRC. The free, Web-based scan, available immediately at <http://sans20.qualys.com>, will enable companies to identify and remedy these threats on any IP address within their network. The free scan leverages QualysGuard's fully automated Web platform, with its proprietary Inference-Based Scanning Engine, to ensure accuracy and speed of scanning. For more information: Email support@qualys.com / Web <http://sans20.qualys.com>

Commercial Software Products You Can Buy To Scan Your Systems

Foundstone:

Foundstone is a major proponent and driving force behind universal, measurable security standards such as the SANS/FBI Top 20. Organizations depend on this expertise every day to identify their true risks and focus their scarce resources on critical vulnerabilities. Every day companies drown in a kaleidoscope of meaningless vulnerability checks that choke IT staff's time and resources with false positives, or worse deliver a false sense of security when they miss real vulnerabilities with false negatives. An optional setting within the FoundScan Enterprise Vulnerability Management System (EVMS) product targets only the SANS/FBI Top 20 vulnerability checks, allowing companies to target the most critical of risks across their global enterprise. For more information, please call 1-877-91-FOUND, send email sales@foundstone.com, or visit www.foundstone.com.

eEye Retina Network Security Scanner

Recognized as the #1 rated scanner on the market in terms of speed, ease of use, non-intrusiveness and vulnerability assessment capabilities. Retina can be used to identify weaknesses and vulnerabilities before they become an issue. Retina scans every machine on your network, including a variety of operating system platforms, databases and third-party or custom applications, all in record time. After scanning, Retina delivers a comprehensive report that details all vulnerabilities and appropriate corrective actions and fixes.

www.eeye.com/retina

* The claims of these vendors have not yet been tested. Updated lists of scanners promising to test the SANS/FBI Top 20, and test results demonstrating that they test accurately, will be posted in the "Related Resources" box at www.sans.org/top20/