Baseline Security Analyzer

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In April 2002, Microsoft released the Microsoft Baseline Security Analyzer (MBSA) Version 1.0. This specialized vulnerability scanner runs on Windows 2000 and Windows XP systems and identifies known vulnerabilities in target systems running Windows NT 4.0, Windows 2000, Windows XP, Internet Information Server (IIS) 4.0 and 5.0, SQL Server 7.0 and 2000, Internet Explorer (IE) 5.01 and later, and Office 2000 and 2002.

Thomas McGuire posted a valuable guide to the product a few weeks after Microsoft released it. His paper shows screen-captures that illustrate the details of how to configure and use the vulnerability scanner.

Commentators noted that the MBSA is another step in the advance of security within Microsoft, long known for its apparent indifference to software quality assurance and security. With Bill Gates determination to make security the number-one priority in future software development and releases, the software giant has been appointing security experts to its staff, publishing books about security, and releasing security tools to the user community.

The MBSA product relies on a database of patches maintained by Microsoft; users will no longer need to monitor a Microsoft Web page to find out about newly discovered vulnerabilities and patches. However, notes writer Brian Fonseca, Microsoft’s bad reputation in the security arena has even led to skepticism among users about the reliability of its new product.

About a three weeks after MBSA was released, Menashe Eliezer of the Finjan Malicious Code Center reported that MBSA leaves a plaintext file on the user’s hard disk will full details about vulnerabilities found on a computer that has been scanned. The advisory warned that any exploit that allows local files to be read without authorization would compromise the target systems. Such exploits include active content in Web pages, e-mail-enabled worms that get infected attachments through out-of-date or disabled antivirus products, and Trojan horses downloaded from insecure sites.

This exploit reminds us that sensitive data should be encrypted on disk. Any vulnerability scanner should be protected by access controls that allow dynamic decryption of the data but which preclude automated processes from accessing cleartext data. In addition, firewalls must be configured to stop outbound data being sent by unauthorized processes.

More generally, we know that most of the exploits used to penetrate systems are old, not new. If the MBSA can push a few more system administrators (and get more support from the people they report to) into patching their systems, the product will do security a service. Protecting systems by having up-to-date operating system software and applications not only benefits the owners and users of the protected systems but also reduces the incidence of hijacked computers that are used to launch port scans, denial-of-service attacks and penetrations of other poorly protected systems.
For further reading


SecuriTeam (2002). Microsoft Baseline Security Analyzer exploit (exposed vulnerabilities list). http://www.securiteam.com/windowsntfocus/5KP0Q1P6US.html

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www.norwich.edu/msia> for full details.


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2002 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.