Microsoft Baseline Security Analyzer V1.1

Mike Fahland, Eric Schultze 2002-12-19

Earlier this month, Microsoft released version 1.1 of the Microsoft Baseline Security Analyzer (MBSA). MBSA is the first product deliverable from the recently formed Microsoft Security Business Unit (SBU), a key division within Microsoft's Trustworthy Computing Initiative.

MBSA 1.0, originally released as a response to the Code Red and Nimda worms, is a multi-threaded security scanner that analyzes an individual computer or a group of computers for missing security patches and other common security misconfigurations. Craig Fiebig, General Manager of SBU Product Marketing, said that "MBSA v1.1 simplifies desktop and server security vulnerability assessment, delivering another step on the path to Trustworthy Computing."

The 1.1 release of MBSA provides bug fixes and enhancements to the original scanner as well as replacing Microsoft's command line hotfix scanner, HFNetChk, by exposing full HFNetChk functionality via the MBSA command line interface. Below we will discuss some of the new features of the 1.1 release, highlighting some of the technical aspects that are not covered elsewhere. Microsoft documentation, including links to the product download, FAQ, and technical whitepaper, are available at the Microsoft MBSA Web site. It should be noted that MBSA was developed for Microsoft by Shavlik Technologies LLC by whom the authors of this paper are employed.

Product Overview

In addition to checking the standard fare (blank or easily guessed user passwords, auto-admin login, unnecessary services, etc), MBSA also scans for unprotected IIS servers; looking for Web servers that haven't run the IIS lockdown tool or that are still running the IIS sample code. Of particular value is MBSA's ability to scan multiple instances of SQL server, evaluating the SQL authentication mode, looking for blank SA password and checking for privilege escalation opportunities exposed via the SQL Server service account, among other items. While not many individuals are running full blown SQL installs, how many people are aware that many applications, such as Visio Enterprise, install mini-versions of SQL Server (known as MSDE) with a blank SA password?! MBSA 1.1 detects each installed SQL or MSDE instance and provides detailed remediation information.

MBSA can be executed via command line or graphical user interface. In either instance you can

specify hostnames, IP address (including IP ranges), or domain names that you'd like to scan. Output is presented on a per host basis via an html interface built into MBSA. Data is saved in XML format on the MBSA host machine.

What's New in Version 1.1

The following new features have been added in Version 1.1:

- Security update detection for Exchange 5.5, Exchange 2000, and Windows Media Player 6.4 and above.
- Scans all instances of SQL Server (v1.0 scanned only the default instance).
- Version checking:
  - When viewing a report, if a newer version of the XML file (containing patch information) is available than what was used to generate a report, the user will be notified of this in the report header.
  - When scanning, the user is notified if a newer major version of the MBSA tool is available.
- Support for Software Update Services (SUS) 1.0, which allows an administrator to specify which missing patches should be reported and which should not (either because they are not applicable or are known to cause issues with enterprise applications).
- The MBSA command line tool (mbsacli.exe) offers full support for HFNetChk v3.81 switches, meaning that MBSA V1.1 replaces the stand-alone HFNetChk tool.
- When checking for passwords that never expire, you can provide a list of accounts that should not be reported as security warnings. By default this list include the IIS accounts, IUSR_* and IWAM_*, whose passwords are usually managed by IIS. An MBSA user can add to that list any other accounts that are okay to have non-expiring passwords by editing the file NoExpireOk.txt.

In addition, some helpful changes have been made to the user interface, such as:

- The security update checks are grouped together in a new separate report section.
- The security update details report now includes the reason each patch is reported as missing or out of date.
- Hotfix checks are not dependent on OS, IIS or SQL checks being selected, and the Windows Password check is not dependent on OS check being selected. You can also disable the SQL password check (by de-selecting "Check for Weak Passwords") and still

perform the other SQL checks.

- As with the original tool, MBSA v1.1 only allows one copy of the tool to be scanning from a given machine. However, if you start MBSA passing it the name of an MBSA output file, or if you drag one of its output files onto the desktop shortcut, a report-only copy of MBSA will start up. This allows you to view reports from previous scans while scanning additional systems. You can also display any number of reports simultaneously using this method.

Version 1.1 is better at locating machine that are in different domains and workgroups, does not require DNS name resolution if scanning by IP address, and is less dependent on the Workstation service running on the remote machines that are being scanned. And, as you'd expect, a number of less common but potentially annoying bugs have been fixed.

How To Use MBSA

To become acquainted with MBSA, start by using the graphical interface. When you click on "Pick a computer to scan", your local machine name will appear with all scan options except for SUS server selected. Simply click "Start scan". When the progress bar reaches its limit, the output report will be displayed. The output is organized by section (Security Updates, Windows, IIS, SQL, etc.) with the most serious vulnerabilities listed at the top of each section. You can specify a different computer by providing its name in the form of Domain/Computer, or by specifying its IP address. You must have administrator rights on the machine being scanned.

To scan multiple machines click on "Pick multiple computers to scan" either in the navigation pane or on the Welcome screen. There, you specify either a domain to scan, or a single range of IP addresses. MBSA can scan up to 10,000 machines in a single invocation. When the scan is complete, you will first see a list of machines that could not be scanned (if any). If a machine cannot be scanned, it is usually because the machine is not online or you are not an administrator on that machine. Clicking "Continue" will display a list of the machines that were successfully scanned and the overall grade assigned. Click on any machine in that list to view the full report.

MBSA is multi-threaded and is capable of scanning an entire domain or large address range in a matter of minutes. A single machine scan can take from a few seconds to several minutes, depending largely on the number of user accounts on the machine. The most time-consuming operation in MBSA is the check for weak passwords. This check tests for blank passwords and

common password patterns (such as the machine name, the user account name, and "admin"). If you scan your enterprise frequently, you may decide not to perform the password scan every time. Unchecking the "Check for weak passwords" option box disables checking passwords for both Windows accounts and SQL accounts.

Scanning and reporting are separate functions in MBSA. MBSA generates an XML output file for each scan of each machine. The XML files are stored in a "SecurityScans" directory that MBSA creates in the path specified by the current %userprofile% environment variable - typically "C:\Documents and Settings\<user_name>". By default, the filename includes the machine name and the time the scan was performed. MBSA provides no summary or correlation tools, and no interface for deleting old reports. Shavlik Technologies, who created the MBSA tool for Microsoft (and by whom both authors of this article are employed), offers Enterprise Inspector 2.1 which includes a SQL database store for all scan results and a reporting tool that can search, sort, and filter the results, perform trend analysis, and automatically delete outdated report information.

Once you become familiar with the capabilities of MBSA, you may choose to schedule regular scans using the command line interface tool, mbsacli.exe. It provides all of the scanning functionality of the graphical tool, plus some finer control over how security update checks are performed. For example, the graphical interface reports only security updates that Microsoft has marked as "baseline" updates. Using the command line tool, you can choose between baseline updates and all updates with the -baseline option. Type For the complete set of options, type the following at the command line: `mbsacli /?`.

New Version of HFNetCHK

With the release of MBSA 1.1, Microsoft is officially retiring the stand-alone version of HFNetChk.exe. Never fear, however, as all functionality from HFNetChk.exe has been rolled into the command line interface of MBSA (mbsacli.exe).

To place MBSA into HFNetChk mode, run: `mbsacli.exe /hf`. Any switches following /hf are interpreted just as HFNetChk switches. To scan a class C network for missing patches using verbose output, the syntax would look like this:

```
mbsacli.exe /hf -r 172.16.1.1-172.16.1.254 -v
```

If you have existing HFNetChk scripts, simply replace "HFNetChk.exe" with "mbsacli.exe /hf"

and the scripts should continue to operate.

New Hotfix Scanning Features

The HFNetChk engine within MBSA is version 3.81. This version supersedes the prior version (3.32) and includes many new enhancements. Most notably, support has been added for NT4 Terminal Server, Exchange 5.5 and 2000 Server, and Windows Media Player versions 6.4 and above.

Aside from the new products, the HFNetChk engine also benefits from significant speed improvements and provides additional information explaining why a patch was considered not found. Also included in this release are minor bug fixes, enhanced error messages, and reduced service dependencies, among other things, as discussed below.

The coolest enhancement can be seen when scanning by IP address or IP range. Before a scan can be initiated, the HFNetChk engine must first determine if a host exists at a given IP address. Ping queries are not the optimal choice, as ICMP may have been blocked between the scanner and the target. Common Microsoft API calls to an IP address that doesn't exist can result in delays of up to 20 seconds before determining that a host doesn't exist. To alleviate these issues and to improve the scanning speed, the HFNetChk engine performs a quick port scan of each IP address.

Each IP is scanned for existence of listening services on both TCP 139 (NetBIOS) and TCP 445 (DirectHost). If either of these ports responds as listening, the scanner attempts to initiate a connection to the target machine and determine if it's indeed a Microsoft host (and if the user performing the scan has administrative authority on this host.) If neither port responds, this can be an indication that no machine exists at this IP address, a machine exists at this address but is not listening on these ports, or this host has been firewalled.

To help differentiate between these responses, the HFNetChk engine listens for replies from the port scan. If no packets are received in response to the query (machine doesn't exist or machine is firewalled and is dropping packets rather then rejecting them), an error 235 is presented:

```
System not found, or NetBIOS ports may be firewalled. Scan not performed.
```

If a machine is present at the specified IP address but is not listening on NetBIOS ports, error 261 will appear:

```
System found but it is not listening on NetBIOS ports. Scan not performed.
```

This indicates that the scanned IP address maybe a non-Microsoft machine, a Microsoft machine with NetBIOS and DirectHost disabled, or a machine with a firewall that is rejecting (not dropping) packets.

Two other new features in the HFNetChk engine within MBSA include the ability to specify a text file containing a list of patches to ignore during the scan (-fq switch) and a file containing a list of hostnames or IP addresses that you wish to scan (-fh and -fip switches respectively). Details on additional command line switches is available by typing: `mbsacli /hf /?`

Mbsacli.exe /hf is a powerful hotfix scanning tool. More information on the HFNetChk engine within MBSA is available from Microsoft in Knowledge Base Article Q303215. For those who still desire the stand-alone version of HFNetChk, the latest version with additional scan features can be obtained from Shavlik.

Privacy Statement
Copyright 2006, SecurityFocus