GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

"Four Pillars" Of Trustworthy Computing

Displayed through Patch Management

-with a tutorial on Microsoft's Baseline Security Analyzer

GIAC Security Essentials Certification
Practical Assignment January 10, 2005
Assignment Option 1

by Daniel J Powers

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Index….

Prologue	**3**
Abstract	**5**
Section I…The Four Pillars	**6**
1. Security	**6**
2. Privacy	**8**
3. Reliability	**9**
4. Business Integrity	**10**
Section II…Patch Management	**11**
1. Standards	**11**
1.1. Standardizing the Patch Experience	**12**
1.2. Standardizing Documentation	**12**
1.3. Technology and Communication	**13**
1.4. Patch Size Reduction	**13**
1.5. Behavior Changes	**14**
1.6. Patch Communication	**14**
2. Updates in a Desktop Environment	**15**
2.1. Automatic Updates in SP2	**16**
3. Updates in a Network Environment	**17**
3.1. WUS	**18**
3.2. SMS	**19**
3.3. Baseline Security Analyzer	**19**
Section III…Baseline Security Analyzer	**20**
1. Picking a Host to Scan	**21**
1.1. Single PC Scanning	**21**
1.2. Multiple PC Scanning	**22**
2. Security Report	**23**
3. What was Scanned	**24**
4. How to Correct This?	**26**
5. Keeping History	**27**

© SANS Institute 2000 - 2005, Author retains full rights.

Prologue

In July of 2002, Bill Gates sent out an email to sum 50,000 Microsoft employees. Bill Gates's email is a defining moment for both the industry and Microsoft's future. It was on a concept that Microsoft would put into play for years to come with all development of products. The concept was for establishing Trustworthy Computing which Bill Gate's describes as the highest priority of the industry for the next decade.

July 18, 2002
Trustworthy Computing (an email by Bill Gates)

As I've talked with customers over the last year - from individual consumers to big enterprise customers - it's clear that everyone recognizes that computers play an increasingly important and useful role in our lives. At the same time, many of the people I talk to are concerned about the security of the technologies they depend on. They are concerned about whether their personal data is being protected. Although they know that computers can do amazing things, they are frustrated that their technology doesn't always work consistently. And they want assurances that the high-tech industry takes these concerns seriously and is working to improve their computing experience.
Six months ago, I sent a call-to-action to Microsoft's 50,000 employees, outlining what I believe is the highest priority for the company and for our industry over the next decade: building a Trustworthy Computing environment for customers that is as reliable as the electricity that powers our homes and businesses today.
This is an important part of the evolution of the Internet, because without a Trustworthy Computing ecosystem, the full promise of technology to help people and businesses realize their potential will not be fulfilled. Ironically, it is the growth of the Internet and the advent of massive computing systems built from loose affiliations of services, machines, communications networks and application software that have helped create the potential for increased vulnerabilities.
There are already solutions that eliminate weak links such as passwords and fake email. At Microsoft we're combining passwords with "smart cards" to authenticate users. We're also working with others throughout the industry to improve Internet protocols to stop email that could propagate misleading information or malicious code that falsely appears to be from trusted senders. And we are making fundamental changes in the way we develop software, in our operational and business practices, and in our customer support efforts to make the computing experiences we provide more trustworthy.
For example, we've historically made our software and services more compelling for users primarily by adding new features and functionality. While we are continuing to invest significantly in delivering new capabilities that customers ask for, we are now making security improvements an even higher priority than adding features. For example, we made changes to Microsoft Outlook to block email attachments associated with unsafe files, prevent access to a user's address book, and give administrators the ability to manage email security settings for their organization. As a result of these changes, the number of email virus incidents has dropped dramatically. In fact, email viruses like the recent "Frethem" virus propagate only to systems that have not been updated - underscoring the importance of updating them regularly.
We are also undertaking a rigorous and exhaustive review of many Microsoft products to minimize other potential security vulnerabilities. Earlier this year, the development work of more than 8,500 Microsoft engineers was put on hold while we conducted an intensive security

© SANS Institute 2000 - 2005 Author retains full rights.

analysis of millions of lines of Windows source code. Every Windows engineer and several thousand engineers in other parts of the company were also given special training in writing secure software. We estimated that the stand-down would take 30 days. It took nearly twice that long, and cost Microsoft more than $100 million. We've undertaken similar code reviews and security training for Microsoft Office and Visual Studio .NET, and will be doing so for other products as well.

THE TRUSTWORTHY COMPUTING FRAMEWORK

Trustworthy Computing has four pillars: reliability, security, privacy and business integrity. "Reliability" means that a computer system is dependable, is available when needed, and performs as expected and at appropriate levels. "Security" means that a system is resilient to attack, and that the confidentiality, integrity and availability of both the system and its data are protected. "Privacy" means that individuals have the ability to control data about themselves and that those using such data faithfully adhere to fair information principles. "Business Integrity" is about companies in our industry being responsible to customers and helping them find appropriate solutions for their business issues, addressing problems with products or services, and being open in interactions with customers.

Creating a Trustworthy Computing environment requires several steps:

- Making software code more secure and reliable. Our developers have tools and methodologies that will make an order-of-magnitude improvement in their work from the standpoint of security and safety.
- Keeping ahead of security exploits. Distributing updates using the Internet so that all systems are up to date. Windows Update and Software Update Services, discussed below, provide the infrastructure for this.
- Early Recovery. In case of a problem, having the capability to restore and get systems back up and running in exactly the same state they were in before an incident, with minimal intervention.

FIRST STEPS TOWARD MORE TRUSTWORTHY COMPUTING

There is still much work that Microsoft and others in our industry must do to make computing more trustworthy. Here is a summary of some of the progress we've made, six months after my email to Microsoft employees:

- We have changed the way we design and develop software at all phases of the product development cycle. Our new processes should greatly minimize errors in software, and speed up the development process for new products and services.
- Software Update Services (SUS) is a security management tool for business customers that enables IT administrators to quickly and reliably deploy critical updates from inside their corporate firewall to Windows 2000-based servers and desktop computers running Windows 2000 Professional and Windows XP Professional.
- Microsoft Baseline Security Analyzer is a new tool that customers can use to analyze Windows 2000 and Windows XP systems for common security misconfigurations, and to scan for missing security hot fixes and vulnerabilities on a variety of products, including newer versions of Internet Information Server, SQL Server and Office.
- In addition to providing customers with tools and resources to help them maximize the security of Windows 2000 Server environments, we are committed to shipping Windows .NET Server 2003 as "secure by default." We believe it's critical to provide customers with a foundation that has been configured to maximize security right out of the box, while continuing to provide customers with a rich set of integrated features and capabilities.
- The error-reporting features built into Office XP and Windows XP are giving us an enormous amount of feedback and a much clearer view of the kinds of problems customers have, and how we can raise the level of reliability in those products - and that of products made by other companies. As part of this effort, we recently created a secure Web site where software and hardware vendors can view error reports related to their drivers, utilities and applications that are reported through our system. This enables the vendors who work with us to identify recurring problems and address them far more quickly than in the past. All of our server software products

© SANS Institute 2000 - 2005 Author retains full rights.

will incorporate these error-reporting features in subsequent versions of the products.
- With Microsoft Windows Update, we are completing the customer-feedback loop based on the error-reporting features mentioned above. This globally available Web service delivers more than 300 million downloads per month of the most current versions of product fixes, updates and enhancements. When customers connect to the site, they can choose to have their computer automatically evaluated to check which updates need to be applied in order to keep their system up-to-date, as well as identify any critical updates to keep their system safe and secure.
- We are working on a new hardware/software architecture for the Windows PC platform, code-named "Palladium*," which will significantly enhance users' system integrity, privacy and data security. This new technology, which will be included in a future version of Windows, will enable applications and application components to run in a protected memory space that is highly resistant to tampering and interference. This will greatly reduce the risk of viruses, other attacks, or attempts to acquire personal information or digital property with malicious or illegal intent. Our goal is for the "Palladium" development process to be a collaborative industry initiative.
- We've incorporated what is known as P3P (Platform for Privacy Preferences) technology in the Internet Explorer browser technology in Windows XP, which enhances a user's ability to set privacy levels to suit his or her needs. The P3P standard enables a user's browser to compare any P3P-compliant Web site's privacy practices to that user's privacy settings, and to decide whether to accept cookies from that site.
Identifying and addressing critical Trustworthy Computing issues will require significant collaboration across our industry. One example of the kind of cross-industry effort we need more of is the recent creation of the Web Services Interoperability (WS-I) Organization (http://www.ws-i.org/). Founded by IBM, Microsoft and other industry leaders including Intel, Oracle, SAP, Hewlett-Packard, BEA Systems and Accenture, WS-I's mission is to enable consistent and reliable interoperability of XML-based Web services across a variety of platforms, applications and programming languages. Among other things, WS-I will create a suite of test tools aimed at addressing errors and unconventional usage in Web services specifications implementations, which in turn will improve interoperability among applications and across platforms.
We are doing everything we can at Microsoft to make software as trustworthy as possible. By building awareness, through collaborative work and with a long-term commitment, I am confident we can and will create a truly Trustworthy Computing environment[1].

Bill Gates

Abstract

Today many people are still very reluctant to put their trust with such personal information like medical and financial records into computer systems. As Microsoft puts it, we will have to persuade people that the systems, the software, the services, the people, and the companies have all, collectively, achieved a new level of availability, dependability, and confidentiality[2]. For technology to truly leave its mark in history a higher level of trust must be established between the industry and the user. Thus Microsoft's Trustworthy Computing initiative is put forth.

[1] Trustworthy Computing an email by Bill Gates
http://www.microsoft.com/mscorp/execmail/2002/07-18twc.asp
[2] Trustworthy Computing Whitepaper http://www.microsoft.com/mscorp/twc/twc_whitepaper.mspx

© SANS Institute 2000 - 2005 Author retains full rights.

In early attempts to show their commitment to trustworthy computing, Microsoft introduced AutoUpdate. AutoUpdate was the introduction and breakthrough to patch management. Through the years Microsoft has developed and evolved AutoUpdate and patch management. Now patch management has become a full product line covering their series of successful desktop operating systems to its vas management server line that pushes the newest technology of delta patches to its networked stations.

Microsoft has pioneered the market of patch management and has answered one of the biggest out cries for safe computing. This document will define Microsoft's Four Pillars of Trustworthy Computing and breakdown a core component of trustworthy computing, Patch Management. The document will end with an inside look at a free and very small utility offered through Microsoft. This utility, The Baseline Utility Analyzer, will display the true effects of patch management.

Section I

The Four Pillars

Microsoft defines their Trustworthy Computing Initiative as a label for a whole range of advances that have to be made for people to be as comfortable using devices powered by computers and software as they are today using a device that is powered by electricity[3]. Microsoft doesn't place a time frame on how long this effort may take to achieve. "It may take us ten to fifteen years to get there, both as an industry and as a society", quoted by Craig Mundie – Senior Vice President and CTO, Advanced Strategies and Policy for Microsoft[4].

Microsoft has specified four core areas in which makes up the Trustworthy Computing Initiative.

- Security
- Privacy
- Reliability
- Business Integrity

1. Security

Security- measures taken to guard against espionage or sabotage, crime, attack, or escape[5]

---

[3] Trustworthy Computing Whitepaper
http://www.microsoft.com/mscorp/twc/twc_whitepaper.mspx

[4] Trustworthy Computing Whitepaper http://www.microsoft.com/mscorp/twc/twc_whitepaper.mspx

© SANS Institute 2000 - 2005, Author retains full rights.

- Merriam-Webster

Information Security- the protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measure necessary to detect, document, and counter such threats[6].

- National Information Systems Security Glossary

"There are no quick fixes for digital security. And with the number of security vulnerabilities, breaches, and digital disasters increasing over time, it's vital that you learn how to manage the vulnerabilities and protect your data in this networked world. You need to understand who the attackers are, what they want, and how to deal with the threats they represent."

Bruce Schneier[7]

Information Security deals with several different trust aspects of data. Information security applies to all aspects or safeguarding data in whatever form and is not confined to just computer systems or information in electronic form. Three widely accepted elements of Information Security are confidentiality, integrity, and availability also known as the mnemonic "CIA".

- *Confidentiality* is a central trust between information providers and information gatheriers. The Public Health Service Act (42 USC 242m) reads, no information, if an establishment or person supplying the information or described in it is identifiable, obtained in the course of activities undertaken may be used for any purpose other than the purpose for which it was supplied unless such establishment or person has consented[8], thus providing confidentiality.
- *Integrity* is derived from not only the orginisation but the individual team members. Components such as trust, ability and character are the defining building blocks that create an orginizations integrity.
- *Availability* according to the U.S. Nuclear Regulatory Commission is the degree to which information or processes are reasonably accessible and usable, upon demand, by an authorized entity, allowing authorized access to resources and timely performance of time-critical operations.

Hackers, crackers, white hats, black hats, script kiddies to the elite attackers agree security or lack of security is their topic of choice. While tools such as BO2K which has been proclaimed legitimate for "white hats" or security administrators by computer underground group Cult of the Dead Cow, can easy become a tool used for cyber terrorism acts by script kiddies or "black hats".

---

[5] Security defined by Merriam Webster http://www.m-w.com

[6] National Information Systems Security Glossary http://www.nstissc.gov/Assets/pdf/4009.pdf

[7] Secrets & Lies by Bruce Schneier http://www.schneier.com/book-sandl.html

[8] Public Health Service Act (42 USC 242m) http://assembler.law.cornell.edu/uscode/html/uscode42/usc_sec_42_00000242---m000-.html

© SANS Institute 2000 - 2005 Author retains full rights.

Viruses, Trojans and worms are used and relied on heavily in attacks. Companies such as Symantec and McAfee defend and protect against such malware, but yet the possibly biggest threat is still at large and can not be stopped by software. Social Engineering is the art of exploiting weaknesses in people, rather than software, tricking someone into giving out information like passwords that will compromise a systems security. Kevin Mitnick one of the worlds proclaimed hacking legends gives the reason for his status to the art of social engineering. Kevin's book The Art of Deception shows the weakness in organizations and the government by disposing the weakest security link, the end user.

2. Privacy

Privacy- a) the quality or state of being apart from company or observation b) freedom from unauthorized intrusion[9]

- Merriam-Webster

Countries around the world have implemented privacy and data protection legislation such as the Health Insurance Portability and Accountability Act of 1996[10] (HIPAA) in the United States and the European Union's Directives on Data Protection[11] imposes detailed requirements on the collection and use of personal information.

Lack or privacy generated by the informational super highway has created an enormous concern about the insecurities of personal information passed across the web.

Some of the issues of concerns created listed by PrivacyRights.org are;

- Hackers penetrating the most secure facilities of the military and financial institutions[12].
- Internet companies have designed numerous ways to track web users as they travel and shop throughout the Internet. "Cookie" now refers to cyber-snooping[13].
- Identity thieves are able to shop online anonymously using the credit-identities of others[14].
- Web-based information brokers sell sensitive personal information, including Social Security numbers[15].

Following September 11, 2001 The Patriot Act unanimously passed by the Senate 98-1, and 357–66 in the House. Congress took existing legal principles

[9] Privacy defined by Merriam Webster http://www.m-w.com
[10] HIPAA http://www.os.dhhs.gov/news/press/1997pres/970213.html
[11] EU Directives on Data Protection http://www.statewatch.org/news/2001/sep/dataprot.pdf
[12] Issues List by PrivacyRights.orghttp://www.privacyrights.org/AR/Privacy-IssuesList.htm
[13] Issues List by PrivacyRights.orghttp://www.privacyrights.org/AR/Privacy-IssuesList.htm
[14] Issues List by PrivacyRights.orghttp://www.privacyrights.org/AR/Privacy-IssuesList.htm
[15] Issues List by PrivacyRights.orghttp://www.privacyrights.org/AR/Privacy-IssuesList.htm

© SANS Institute 2000 - 2005, Author retains full rights.

and retrofitted them to preserve the lives and liberty of the American people from the challenges posed by a global terrorist network. The Patriot Act was a key leading role in a number of successful operations to protect innocent Americans from the deadly plans of terrorist's acts[16]. However while the Patriot Act is put into place to enhance the protection of American life it severely threatens privacy.

- The Patriot Act expands terrorism laws to include domestic terrorism which could subject political originations to surveillance, wiretapping, harassment, and criminal action for political advocacy[17].
- The Patriot Act expands the ability of law enforcement to conduct secret searches, gives them wide powers of phones and Internet surveillance, and across to highly personal medical, financial, mental health, and student records with minimum judicial oversight[18].

Organizations such as the ACLU will continue to fight such legislation as the Patriot Act. Legislation such as the Patriot Act however will continue to fight global terrorism as long as it remains.

3. Reliability

Reliability- the extent to which an experiment, test, or measuring procedure yields the same results on repeated trials[19]

-Merriam-Webster

The concern for reliability is not anything newly introduced. In the early nineteenth century the Reliability Theory was developed. Apart from the mainstream of probability and statistics, reliability theory was used originally as a tool for maritime insurance and life insurance companies to compute profitable rates to charge their customers[20]. Today, Microsoft is taking new strives to define reliability by defining it in one of their four core areas of Trustworthy Computing.

Relaibiltiy in the content of Trustworthy Computing is presented by Microsoft as more then just reliable software and provding support. Microsoft believes it means being a reliable business partner, maintaining an open dialogue with our customers and industry partners, and seeking feedback about how we can improve our software and services[21].

In engineering and telecommunication, the mean time between failures **(**MTBF**)** is the average time a system will operate without a failure. A primary way to determine the level of reliability provided is to measure the amount of MTBF. MTBF is an indicator of expected system reliability calculated on a statistical

[16] The Patriot Act http://www.lifeandliberty.gov/
[17] ACLU on the Patriot Act http://www.aclu.org/Files/OpenFile.cfm?id=11812
[18] ACLU on the Patriot Act http://www.aclu.org/Files/OpenFile.cfm?id=11812
[19] Reliability defined by Merriam Webster http://www.m-w.com
[20] Reliability theory defined by Wikipedia http://en.wikipedia.org/wiki/Reliability_theory
[21] Reliability by Microsoft http://www.microsoft.com/mscorp/twc/reliability/default.mspx

© SANS Institute 2000 - 2005, Author retains full rights.

basis from the known failure rates of various components of the system usually expressed in hours[22].

It should also be noted that currently:

- There is no standard measure of MTBF
- Its often calculated and inferred rather than tested
- The MTBF applies only statistically (and cannot be taken as an expected lifetime)

In 1984 Charles Perrow wrote a book called Normal Accidents: Living with High Risk Technologies. In it Charles observed that system accidents can be the result of one big failure, but most often are caused by the unexpected interactions between failures of multiple components. The observations by Charles Perrow and others lead to NASA's Normal Accident Theory in which suggests that in complex tightly coupled systems, accidents are inevitable, thus creating MTBF[23].

Normal Accident defined by World Spy is an accident that is the nearly inevitable result of technological interactions so complex that they cannot fully predicted or controlled[24].

4. Business Integrity

Integrity- the quality or state of being complete or undivided[25]
-Merriam-Webster

Business integrity is the essence of a company and its team members. In an article from WebProNews in 2004 mentions of research that was performed by the Institute of Business Ethics. It was found that companies displaying a "clear commitment to ethical conduct" almost invariably outperform companies that do not display ethical conduct[26].

Basic integrity principles also displayed in 2004 article from WebProNews states all the following maybe considered as some of the essentials of building business integrity.

- A company must display and earn the trust with the client. Trust is assured reliance on the character, ability, strength, of a business[27].
- Character feedback and opinions from clients and team members will display leadership and open up ideas for improvement[28].

---

[22] MTBF defined by T-Cubed Systems http://www.t-cubed.com/faq_mtbf.htm
[23] NASA's Normal Accident Theory http://www.hq.nasa.gov/office/codeq/accident/accident.pdf
[24] Normal Accidents defined by Word Spy http://www.wordspy.com/words/normalaccident.asp
[25] Integrity defined by Merriam Webster http://www.m-w.com
[26] WebProNews article on Business Integrity http://www.webpronews.com/ebusiness/smallbusiness/wpn-2-20040713The7PrinciplesofBusinessIntegrity.html

© SANS Institute 2000 - 2005, Author retains full rights.

- Evaluate all print materials including advertising, brochures and other business documents making sure they are clear, precise and professional[29].
- Remain involved in community related issues and activities. This will demonstrate that your business is a responsible community contributor[30].
- Keep a hands-on approach in to accounting and record keeping. Gaining control of accounting and record keeping allows you to end any dubious activities promptly[31].
- Treat all others with the utmost of respect always[32].

Microsoft has committed itself to carry the highest level of business integrity. They have introduced its vision of trustworthy computing and have displayed trustworthy computing throughout their product line. Microsoft continues to carry a number of corporate initiatives and programs focusing on the upkeep of business integrity. These types of initiatives and programs in Microsoft and other organizations keep the core values of trustworthy computing strong.

Section II

Patch Management

In a short article published from Cert.org, Larry Rogers states to 95% of all network intrusions could be avoided by keeping computers up to date and patched. According to Microsoft, patch management is the process of controlling the deployment and maintenance of provisioned software releases into production environments. Companies such as Altiris build their entire business model around patch management but it began at Microsoft.

---

[27] WebProNews article on Business Integrity
http://www.webpronews.com/ebusiness/smallbusiness/wpn-2-20040713The7PrinciplesofBusinessIntegrity.html
[28] WebProNews article on Business Integrity
http://www.webpronews.com/ebusiness/smallbusiness/wpn-2-20040713The7PrinciplesofBusinessIntegrity.html
[29] WebProNews article on Business Integrity
http://www.webpronews.com/ebusiness/smallbusiness/wpn-2-20040713The7PrinciplesofBusinessIntegrity.html
[30] WebProNews article on Business Integrity
http://www.webpronews.com/ebusiness/smallbusiness/wpn-2-20040713The7PrinciplesofBusinessIntegrity.html
[31] WebProNews article on Business Integrity
http://www.webpronews.com/ebusiness/smallbusiness/wpn-2-20040713The7PrinciplesofBusinessIntegrity.html
[32] WebProNews article on Business Integrity
http://www.webpronews.com/ebusiness/smallbusiness/wpn-2-20040713The7PrinciplesofBusinessIntegrity.html

© SANS Institute 2000 - 2005, Author retains full rights.

All the following should be considerations for why poor Patch Management can become a financial impact.

- Downtime. What's the amount of downtime involved and at what amount of financial loss because of this downtime?
- Remediation Time.
- Questionable Data Integrity
- Lost Credibility
- Negative Public Reaction
- Legal Issues
- Stolen Intellectual Property

Depending of the onlooker, Patch management can live on many different scales. To the desktop user patch management doesn't really exists, just Automatic Updates. To organizations patch management has been escalated to more then a mere time filler for network administrators. Patch management has now in its own rights have become a full-time duty requiring up-to-date knowledge of vulnerabilities and threats as well as training and education of emerging server products to assists control and distribution. For the distributor such as Microsoft, patch registration which is still under development will soon introduce a standard to which an entry will be left in the system registry to identify installed patches and will assist with overall management and distribution.

1. Standards

In 2002 Microsoft formed a task force to identify opportunities for improving the software update and security update management process and technologies. The Patch Management Task Forced distilled the input they recovered into four key areas of focus:

1. Provide clear and timely communications and guidance.
2. Provide consistency in standards and behaviors.
3. Provide high-quality security updates that reduce recalls, update sizes, and system restarts.
4. Provide consolidated and cost-conscious tools.

1.1 Standardizing the Patch Experience

Microsoft's Standardizing the Patch Experience article was put out in efforts to produce a roadmap to the future of software patches. Is this document Microsoft outlines three areas of focus and changes that are being applied to the patch experience.

1. Changes designed to clarify the documentation that accompanies patches through the use of standard terms and document formats[33].
1. Changes deigned to reduce the management burden associated with patches, through the adoption of uniform technologies and engineering

[33] Standardizing the Patch Experience
http://www.microsoft.com/technet/security/topics/patch/stdpatex.mspx

© SANS Institute 2000 - 2005 Author retains full rights.

practices[34].

2. Changes designed to improve manageability by standardizing patches' behavior on the user's system[35].

1.2 Standardizing Documentation

Under documentation standards Microsoft addressed issues regarding the patch naming convention, terminology used for each patch, and documentation format to accompany the patch. Microsoft setup to define a consistent and well understood method of providing the most complete information they could to the user.

Hotfixes, critical updates, and upgrades are a few of the many terms used when working with patches. These and other terms have been unclear and misunderstood for most of their times Microsoft's article 824684, Description of the Standard Terminology[36] put out in July, 2004 has placed a standardized meaning to each of these terms.

In March, 2004 Microsoft released Article 824685[37], Description of the File Names That Are Used for Microsoft Product Updates, Tools, and Add-ins. This article put a company wide naming convention into place rather the previous department issued name. The standardized file naming schema that Microsoft is adopting for packages that contain product updates, tools, and add-ins uses the following format:
ProductName-KB*ArticleNumber*-*Option*-*Language*.exe

Microsoft continued to define the third issue of documentation that would accompany the patch. In the past there would be two documents that would accompany the patch, a security bulletin and a Knowledge Base article. The security bulletins has carried a standard format but the Knowledge Base articles have been primarily been more free-form. After the release of article 824689, Description of the format of Microsoft Knowledge Base articles for Microsoft Security Updates a standard has been put into action. Now Knowledge Base articles will focus primarily on the patch – how to install it, verify its successful installation, troubleshoot problems. The security bulletins will then focus primarily on the security vulnerability that necessitated the patch[38].

1.3 Technology and Communication

---

[34] Standardizing the Patch Experience
http://www.microsoft.com/technet/security/topics/patch/stdpatex.mspx
[35] Standardizing the Patch Experience
http://www.microsoft.com/technet/security/topics/patch/stdpatex.mspx
[36] Description of the standard terminology that is used to describe Microsoft software updates
http://support.microsoft.com/?kbid=824684
[37] Description of the File Names That Are Used for Microsoft Product Updates, Tools, and Add-ins http://support.microsoft.com/?kbid=824685
[38] Standardizing the Patch Experience
http://www.microsoft.com/technet/security/topics/patch/stdpatex.mspx

© SANS Institute 2000 - 2005 Author retains full rights.

Microsoft historically has allowed each product team to develop their technologies and engineering processes. With the emergence of larger and more complex products, Microsoft set out to standardize the development process.

Due to the Architectural differences among Microsoft products there have been some differences in how patches are applied. The standard mandates that all patches use one of two installers:

1. The Windows Installer (MSI), which is most commonly used by applications.
2. Updater.exe will be utilized for the Windows operating systems and a small number of applications.

Microsoft carries goal to have a single installer that will handle both applications and operating systems one day. Microsoft has reach great strives in the patches that are bring distributed through these installers. These installers are now pushing out what Microsoft is calling delta patches.

Microsoft defines a delta patch as a delta-compressed Windows Installer patch created using a tool, such as Patchwiz.dll, that supports delta compression. Patches that use delta compression can reduce the size of an update by providing only the differences (deltas) between existing files on a target computer and the desired new files. The desired new files are then synthesized from the existing files and the downloaded deltas.

1.4 Patch Size Reduction

Limited bandwidth for some Microsoft users has created an issue with patch sizes. Delta patching was a major breakthrough in patch size reduction. Another factor that determines the size of a patch is whether debug symbols are included in it. These symbols are important to the engineering and quality control process, but are not needed to install and use the patch. Removing them will allow faster patch downloads, and should encourage patch uptake which is described in Microsoft's Standardizing the Patch Experience article[39]. The standards now mandate that all debugging symbols are removed from patches before they are released. For administrators in need of debugging symbols they can be obtained from Microsoft's Symbol Server as described in article 311503[40], Use the Microsoft Symbol Server to obtain debug symbol files.

1.5 Behavior Changes

An established set of run-time options that all installers support has been created in efforts to continue Microsoft's migration to a more consistent user experience. These options or switches are included in the command line.

---

[39] Standardizing the Patch Experience
http://www.microsoft.com/technet/security/topics/patch/stdpatex.mspx
[40] Use the Microsoft Symbol Server to obtain debug symbol files
http://support.microsoft.com/?kbid=311503

© SANS Institute 2000 - 2005 Author retains full rights.

Article 824687, Command-line switches for Microsoft software update packages defines the switches and their behaviors[41].

/help; /h; /? – Displays a dialog box that shows the correct usage of the Setup command, including a list of all its command-line switches and their behaviors. You can display this help information in the command-line interface (CLI) or the graphical user interface (GUI). If you use any command-line switch incorrectly, this help switch is invoked and the correct usage is displayed. The dialog box also provides references to more online information.
/quiet – Runs the Setup program or the removal program in "quiet" mode. The program does not prompt the user with any messages. The program enters all messages in a log file. By default, the program restarts the computer with no prompt or warning if the process requires a restart for the changes to take effect. To change the default restart behavior, use a different restart mode.
/passive – Runs the Setup program or the removal program in "passive" mode. The program does not prompt the user with any error messages. The user sees a progress bar that indicates that the installation or the removal is occurring. The user cannot cancel the installation or the removal. By default, the program invokes the **/warnrestart** switch. If the program is installing multiple updates, the progress bar indicates the progress of the installation or the removal for each update.
/norestart – Does not restart the computer after the installation or the removal, even if the process requires a restart for the changes to take effect.
/forcerestart – Restarts the computer after the installation or the removal, even if the process does not require a restart for the changes to take effect. Restarting forces programs that are running to close.
/warnrestart[:*x*] – Invokes a dialog box that warns the user that a restart will occur in *x* seconds (in 30 seconds if no value is specified). For example, to warn that a restart will occur in 60 seconds, type **/warnrestart:60**. The dialog box contains a **Cancel** button and a **Restart Now** button. If the user clicks **Cancel**, the computer is not restarted.
/promptrestart – Prompts the user that the computer must be restarted for the changes to take effect. The user can select whether to restart the computer.
/uninstall – Removes the package.
/log – Enables the user to define the path for the local log file. This switch invokes the default logging behavior.
/extract – Enables you to extract the installation files to a specified folder.

1.6 Patch Communication

To take the necessary and appropriate actions to assists customers in managing operational risks such as software updates and security updates, Microsoft has created The Security Bulletin Notification Service. Customers can sign up and be notified via email of the latest Security Bulletins. The Security Bulletins provides customers a first point of information that allows them to determine if the security risk is relative to their products or not. The Security Bulletin also explains to IT Professionals how and when to download and deploy the security updates, and how the updates affect to their overall IT infrastructures.

Microsoft Security Response Center has standardized bulletins to be distributed monthly on the second Tuesday of the month except in the case of a known exploit. The Security Bulletins now are distributed in to different formats, the original format for IT Professionals and a less technical version for other consumers. Microsoft has also created a web search tool to allow for a single location for customers to view released Security Bulletins on any given Microsoft product. Finally to clarify communications with its customers; Microsoft has

[41] Command-line switches for Microsoft software update packages http://support.microsoft.com/?kbid=824687

© SANS Institute 2000 - 2005 Author retains full rights.

redefined the definition of their severity rating.

Rating	Definition
Critical	A vulnerability whose exploitation could allow the propagation of an Internet worm/virus without user action.
Important	A vulnerability whose exploitation could result in compromise of the confidentiality, integrity, or availability of users' data, or of the integrity or availability of processing resources.
Moderate	Exploitability is mitigated to a significant degree by factors such as default configuration, auditing, or difficulty of exploitation.
Low	A vulnerability whose exploitation is extremely difficult, or whose impact is minimal.

Figure 1 Severity Rating Definitions[42]

Microsoft also offers further resources to communicate with its customers.

- **Security Guidance Kit**[43] which is distributed free for Microsoft in CD format. The kit is complete with tools, templates, and how-to guides.
- **Virus Information Alliance** which Microsoft has established industry partners Computer Associates, McAfee, Sybari, Symantec, and Trend Micro to provide customers with the latest virus alert information.
- **Solution Accelerators Provide Prescriptive Guidance**[44] to assist customer in designing effective security processes with Microsoft tools.

2. Updates in a Desktop Environment

In June of 2004 Group Manager for Server Patch Management at Microsoft Brian Keogh, was interviewed for TechNet Radio. During the conversation Brian estimates that his department stretched over 450 Building, 160 sites has roughly 128,000 odd devices that they collect data on. The data collection of both hardware and software allows the Server Patch Management Group to provide various reports from a Microsoft desktop point of view.

Still with the amazing steps taken by Microsoft there is still an ongoing uphill battle to secure its desktop OS. To date Secunia[45] has listed 79 vulnerability advisories for Microsoft's XP Professional operating system with still 21 of those vulnerabilities remaining "unpatched".

[42] Understanding Patch and Update Management: Microsoft's Software Update Strategyhttp://www.microsoft.com/technet/security/topics/patch/patchmanagement.mspx
[43] Security Guidance Kit http://www.microsoft.com/security/guidance/default.mspx
[44] Improve Platform Management http://www.microsoft.com/business/reducecosts/efficiency/manageability/patch.mspx
[45] XP Professional vulnerabilities provided by Secunia http://secunia.com/product/22/

© SANS Institute 2000 - 2005 Author retains full rights.

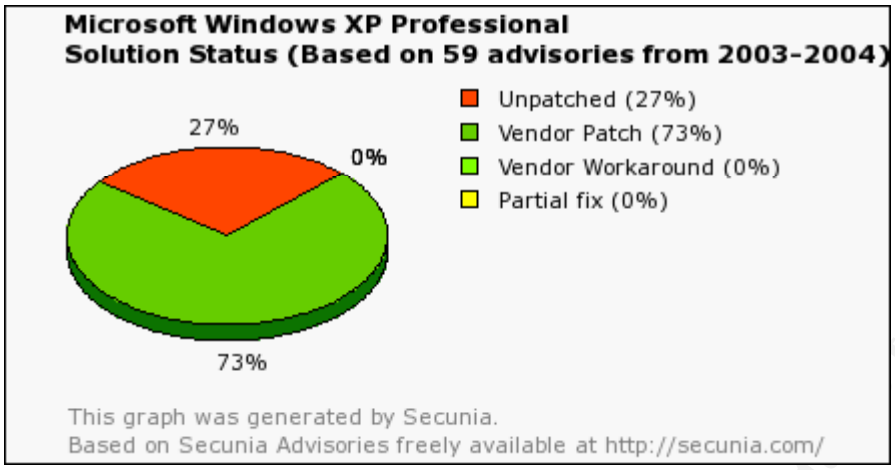


Figure 2 The "Solution Status" pie graph shows the percentages of "Unpatched", "Vendor Patched", "Vendor Workaround" and "Partial Fixed" Secunia advisories affecting Microsoft Windows XP Professional[46].

To combat the vulnerabilities Microsoft introduced AutoUpdate[47] in late November of 1999 in its Windows Millennium Edition. Then again in 2000 Microsoft introduce AutoUpdates, but this time it was for its widely used Office product. This was the introduction of a major feature that is now bundled with every Microsoft product today.

2.1 Automatic Updates in SP2

In the summer of 2004 Microsoft release Service Pack 2 (SP2) for Windows XP. With SP2 its users were introduce to the new Security Center. One of the components that make up the Microsoft's Windows XP SP2 Security Center is a new automatic updates category. Microsoft has lead the way in the delivery of software updates electronically, however this time Microsoft is placing a much larger emphasis on having critical patches distributed and install even quicker then ever before.

After installation of SP2 and a quick reboot, users will be presented with Microsoft's full page advertisement which strongly recommends turning on Automatic Updates.

[46] The Solution Status http://secunia.com/product/22/
[47] The release of AutoUpdate
http://www.winsupersite.com/showcase/windowsme_autoupdate.asp

© SANS Institute 2000 - 2005 Author retains full rights.

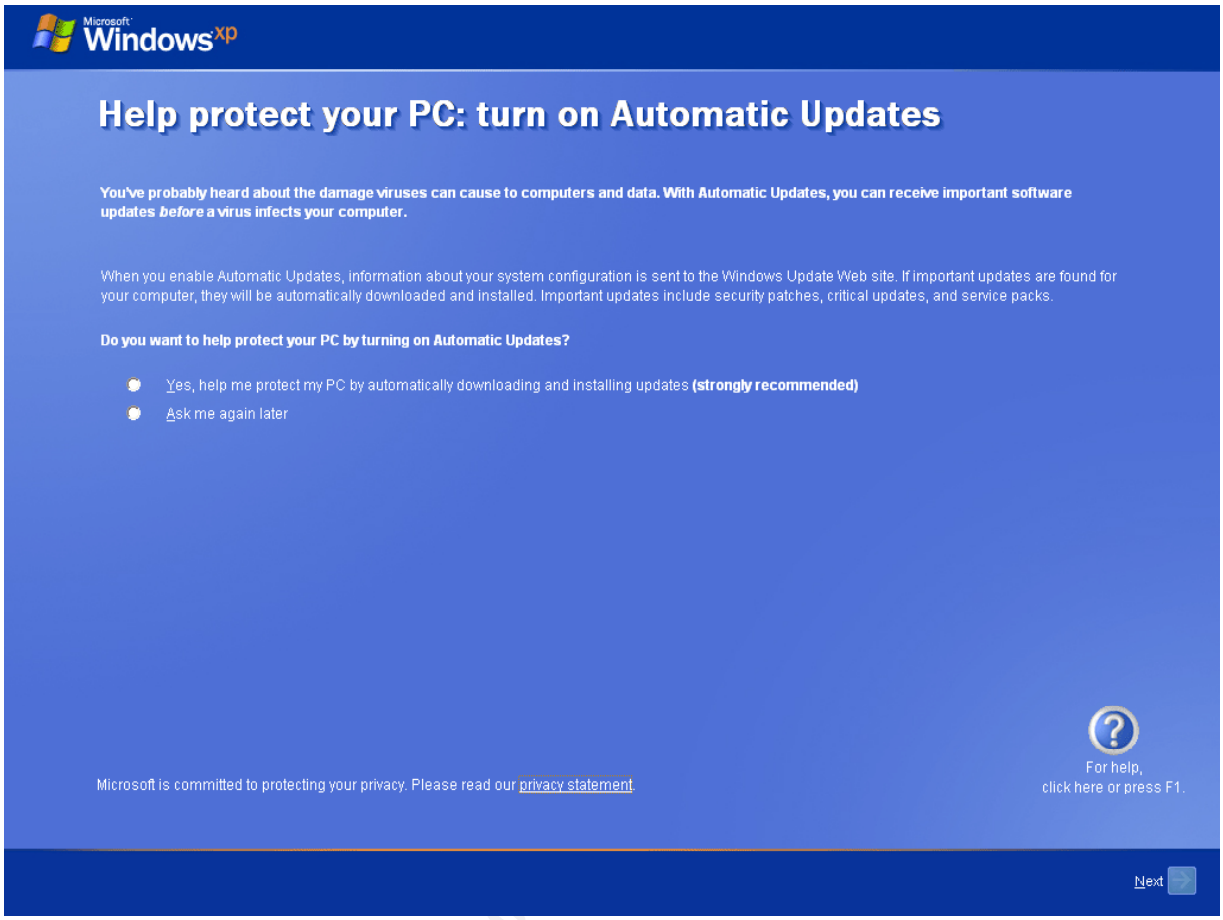


Figure 3 Automatic Updates Ad

By default not only are automatic updates set to download updates but also to install critical updates immediately. The installations of these updates are critical for the upkeep and overall reliability of a system.

In the backend Microsoft has greatly improved the patch management that drives automatic updates. SP2 also introduced a new compression with delta patching technology. Delta patching technology is a core component in Microsoft's Patch Management Strategy today.

SP2 also introduces a new feature called "install on shutdown". If a critical update is temporarily ignore Windows XP SP2 will simply install it for you, automatically, the next time you shut down. This allows the system to be up-to-date on the next boot up.

3. Updates in a Network Environment

In organizations, patch testing along with quick but reliable deployment is essential to its patch management scheme. Microsoft has taken the steps to allow organizations to control what patches are deployed, when they are deployed and to what machines they are pushed out to. Microsoft does this

© SANS Institute 2000 - 2005 Author retains full rights.

through its server line products.

3.1 WUS

Microsoft's Windows Update Server (WUS)[48] is the next generation patch management and distribution server replacing the original Software Update Sever (SUS). The original SUS was developed to simplify the process of keeping Windows based computers up to date with the latest critical updates and was available free from Microsoft. SUS which is ran on Windows 2000 and Windows 2003 server would allow from quick deployment of updates to Windows 2000 and XP machines. SUS was ideal for providing updates within a corporate firewall for corporation not already using Systems Management Server (SMS).

The Windows Update Services adds on features to the original Software Update Services. Microsoft is offering expanded support for products such as Office, SQL, Exchange and hardware drivers. WUS also offers the ability to filter updates, maximize bandwidth efficiency, improved reporting capabilities and more.

Microsoft offers a recommended approach to using WUS. This approach is broken down into four processes.

1. **Assess**
   Administrators should first asses and understand possible threats to their particular environment. This will in turn help them understand and prepare their environment for such threats. Assessment is a consistent, ongoing process.

2. **Identify**
   Administrators should identify all new updates and determine how the update will affect their particular environment. This will help determine the priority of the update.
3. **Evaluate and Plan**
   Administrators should evaluate and test each update separately from the production network to determine if it compromises any business applications. This will assist in determining the necessary tasks needed to be taken to deploy each update.
4. **Deploy**
   Administrators should test, approve and schedule update installations. After installation a complete review of the process should be completed.

By using WUS, administrators have full control and managing and the distribution of all Microsoft release updates to their network.

3.2 SMS

[48] Windows Update Server http://www.microsoft.com/windowsserversystem/default.mspx

© SANS Institute 2000 - 2005, Author retains full rights.

Microsoft Systems Management Server (SMS)[49] is a complete solution for organizations to handle configuration changes across the Microsoft platform. This allows organizations to push software and updates to users quickly and cost effectively. Microsoft's list the following key capabilities for SMS 2003.

- Application Development

Deliver critical business productivity applications reliably and easily to users in the right place at the right time[50].

- Asset Management

Reduce software costs and stay compliant by understanding the installed application base and its usage. [51]

- Security Patch Management

Improve security of the Microsoft Windows environment through increased vulnerability awareness and reliable targeted delivery of updates[52].

- Mobility

Deliver enterprise management to the growing mobile workforce through industry standards independent of connection or location[53].

- Windows Management Services Integration

Reduce operational costs by fully utilizing the management capabilities built into the Windows platform[54].

- Integrating Operations and Technology

Microsoft Solutions for Management Solution Accelerators provide a blueprint for addressing key management issues by combining people, processes, and technology to help solve specific customer scenarios. Solution Accelerators are lab-tested, customer-approved Microsoft best practices that are intended to be used by Microsoft Consulting Services or Microsoft partners to help customers achieve optimal solutions[55].

3.3 Baseline Security Analyzer

Microsoft's Baseline Security Analyzer[56] (MBSA) is a vulnerability assessment tool for Windows based platforms and is offered for free through Microsoft. Microsoft's Baseline Security Analyzer runs on Windows 2000, Windows XP and Windows 2003 Server. MBSA scans from common misconfigurations on products such as IIS, IE, Office SQL and others. Please refer to Section III Baseline Security Analyzer from further information.

Further Reference

Keep operating software and application software up to date. *A practice from the CERT® Security Improvement Modules*
http://www.cert.org/security-improvement/practices/p067.html

[49] System Management Server http://www.microsoft.com/smserver/
[50] SMS Key Capabilities http://www.microsoft.com/smserver/evaluation/overview/default.asp
[51] SMS Key Capabilities http://www.microsoft.com/smserver/evaluation/overview/default.asp
[52] SMS Key Capabilities http://www.microsoft.com/smserver/evaluation/overview/default.asp
[53] SMS Key Capabilities http://www.microsoft.com/smserver/evaluation/overview/default.asp
[54] SMS Key Capabilities http://www.microsoft.com/smserver/evaluation/overview/default.asp
[55] SMS Key Capabilities http://www.microsoft.com/smserver/evaluation/overview/default.asp
[56] Microsoft Baseline Security Analyzer http://www.microsoft.com/technet/security/tools/mbsahome.mspx

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005, Author retains full rights.

Section III

Baseline Security Analyzer

Microsoft's Baseline Security Analyzer (MBSA) is a vulnerability assessment tool for the Microsoft platform and is available for free download through www.microsoft.com. MBSA is perfect for IT Professional assessing the overall security management strategy.

When opening MBSA the Welcome screen is displayed providing you with your scanning options.

1. Scan a Computer
2. Scan more than one computer

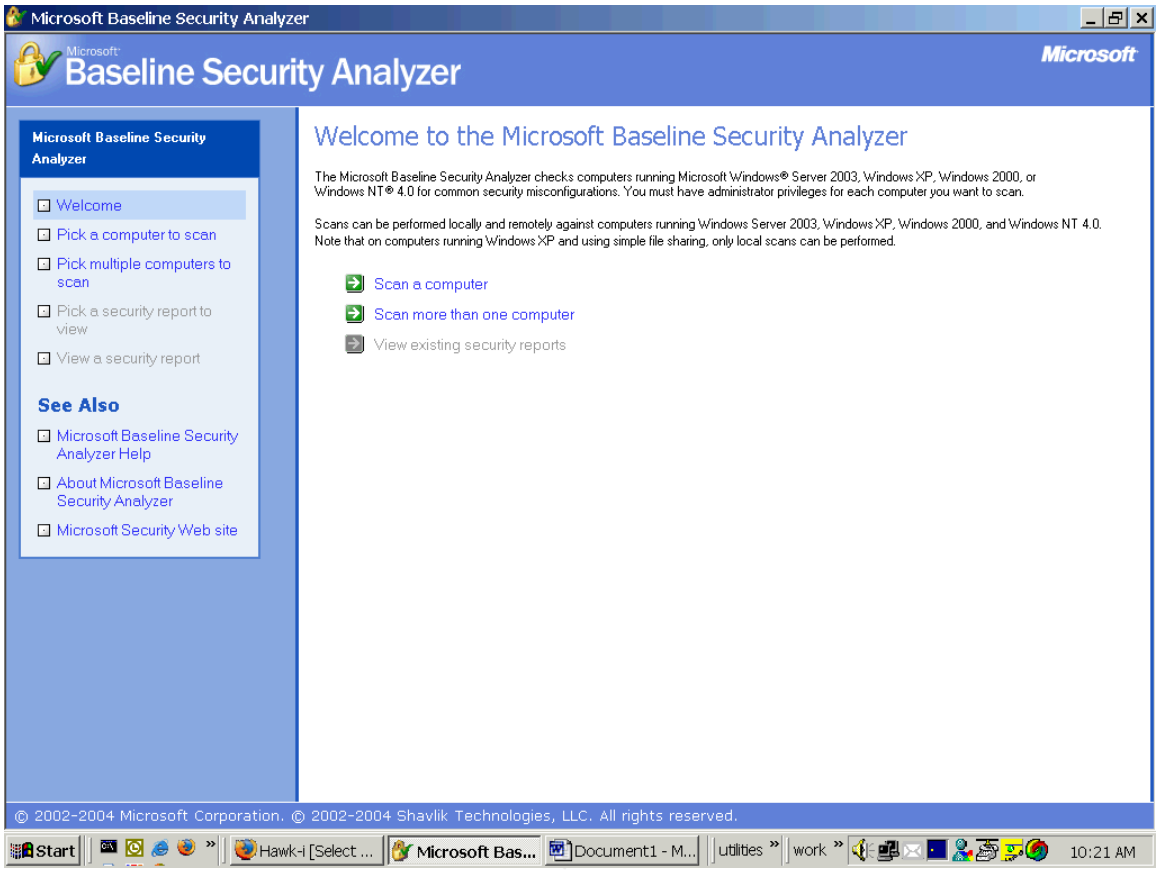


Figure 4 MBSA Welcome Screen

1. Picking a Host to Scan

1.1 Single PC Scanning

MBSA offers the option of canning a single PC or scanning multiple PCs. With the single PC option, scanning can be preformed by choosing computer name or IP address of the computer of choice.

© SANS Institute 2000 - 2005 Author retains full rights.

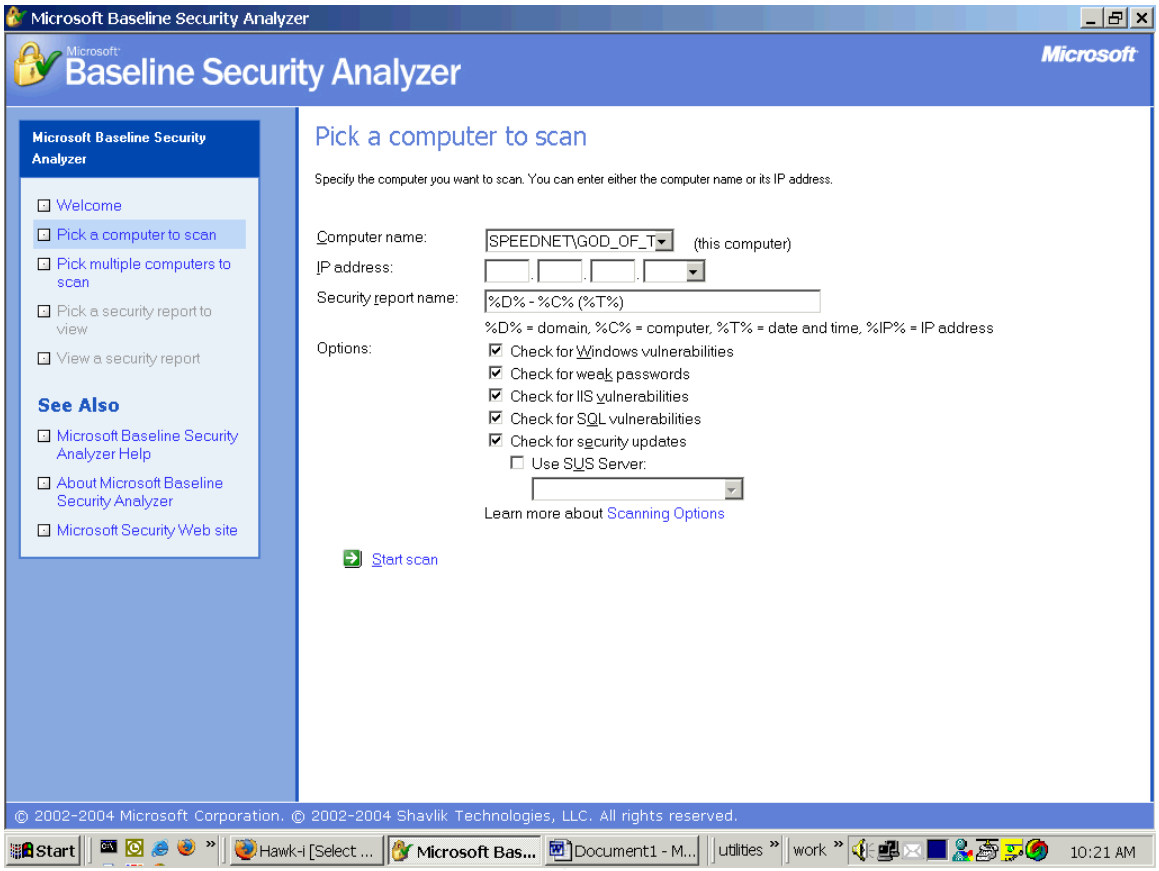


Figure 5 Preparing to scan a Single PC

© SANS Institute 2000 -

1.2 Multiple PC Scanning

If selecting multiple PCs for scanning, the MBSA gives the option to scan per domain or per IP range.

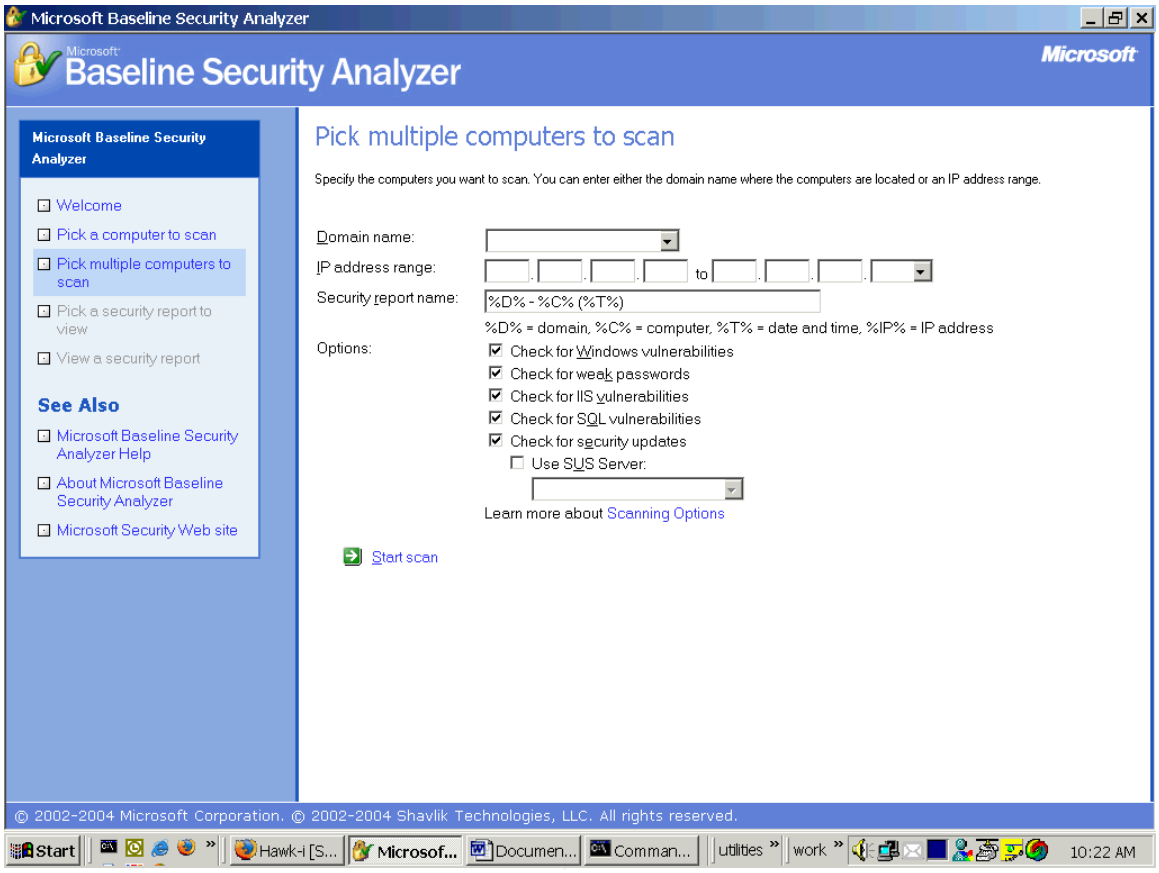


Figure 6 Picking Multiple PCs

© SANS Institute 2000 -

2. Security Report

Following the scan the MBSA displays a full report covering multiple categories. On this particular PC the MBSA reports back on five different categories.

1. Security Update Scan Results
2. Windows Scan Results
    a. Vulnerabilities
    b. Additional System Information
3. Internet Information Services (IIS) Scan Results
    a. Vulnerabilities
    b. Additional System Information
4. SQL Server Scan Results
5. Desktop Application Scan Results
    a. Vulnerabilities

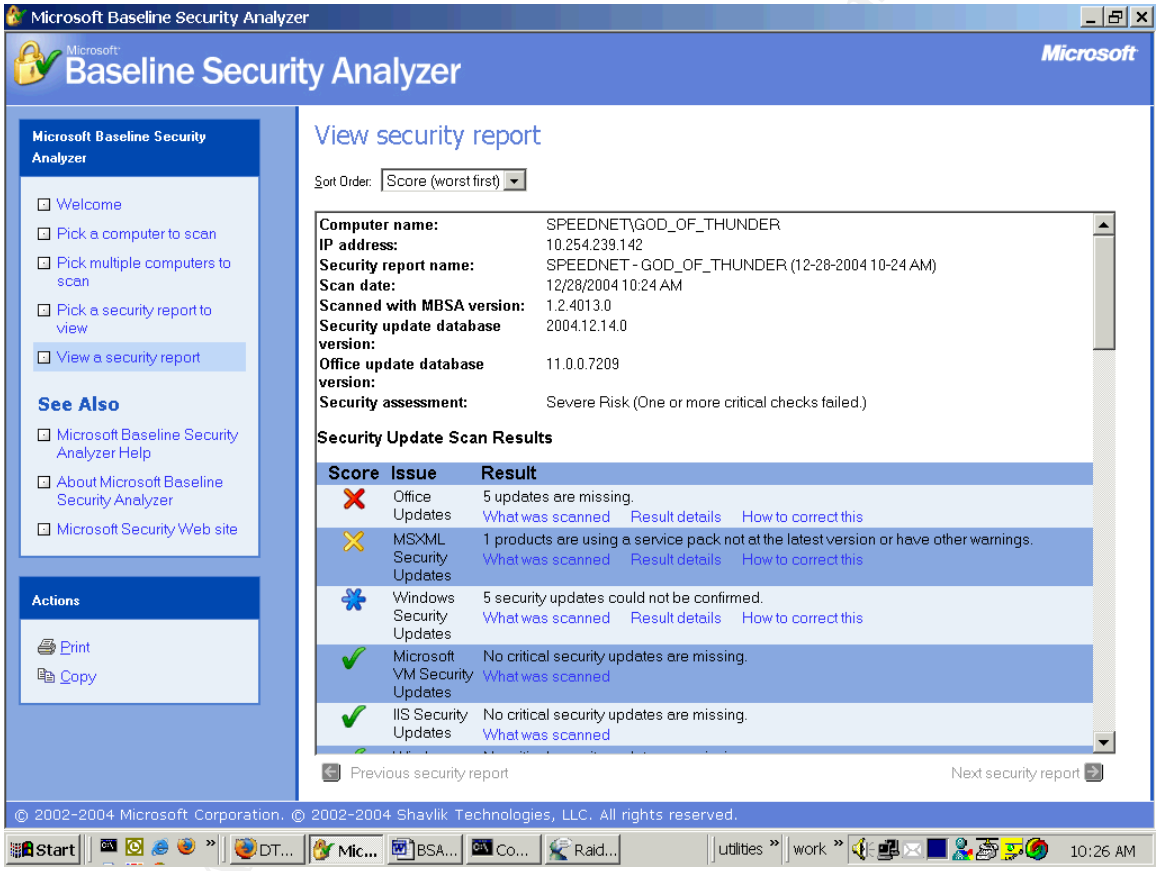


Figure 7 Security Report Screen

3. What was Scanned?

The scan determines what security patches, hotfixes and updates are missing

© SANS Institute 2000 - 2005 Author retains full rights.

and leaving vulnerabilities from the host machine.

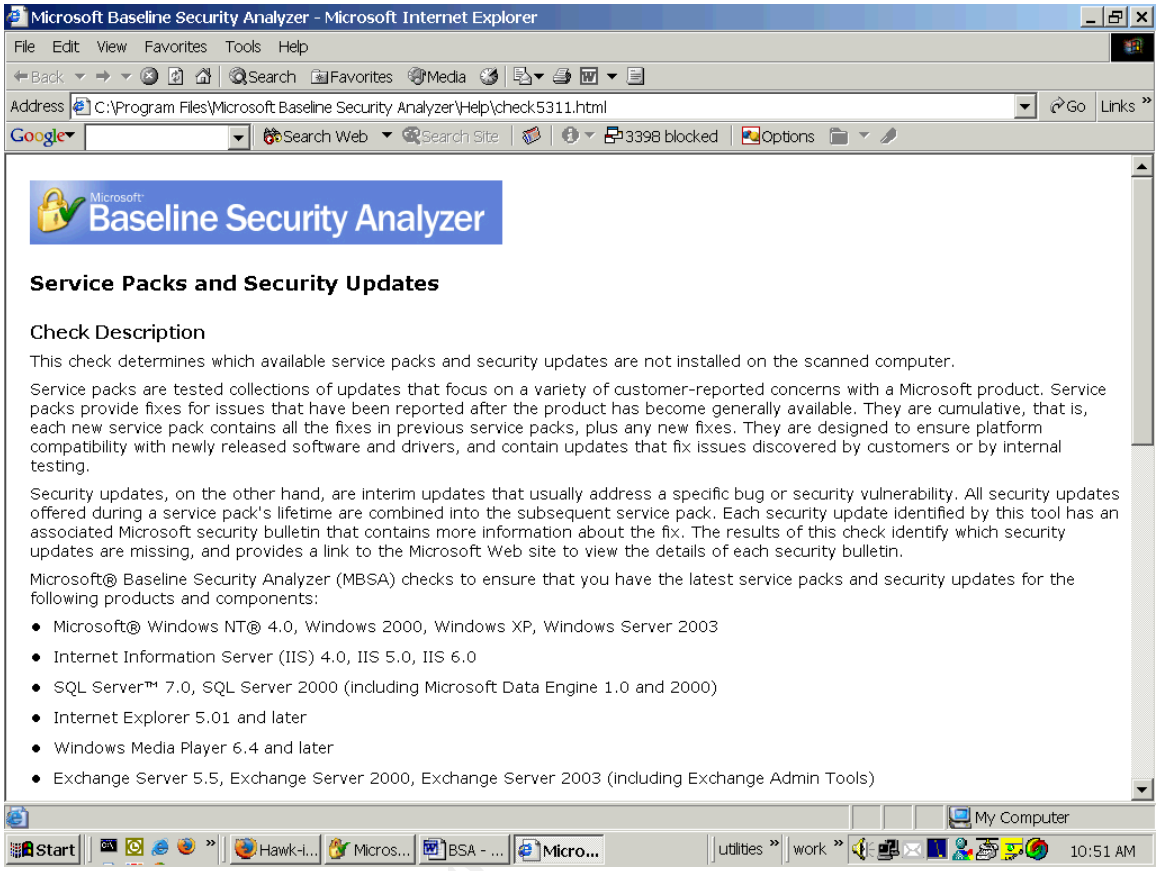


Figure 8 Defining what was scanned

The following information is provided from the MBSA help file that is accompanied with the Microsoft Baseline Security Analyzer.

Service packs are tested collections of updates that focus on a variety of customer-reported concerns with a Microsoft product. Service packs provide fixes for issues that have been reported after the product has become generally available. They are cumulative, that is, each new service pack contains all the fixes in previous service packs, plus any new fixes. They are designed to ensure platform compatibility with newly released software and drivers, and contain updates that fix issues discovered by customers or by internal testing.
Security updates, on the other hand, are interim updates that usually address a specific bug or security vulnerability. All security updates offered during a service pack's lifetime are combined into the subsequent service pack. Each security update identified by this tool has an associated Microsoft security bulletin that contains more information about the fix. The results of this check identify which security updates are missing, and provides a link to the Microsoft Web site to view the details of each security bulletin.

Microsoft® Baseline Security Analyzer (MBSA) checks to ensure that you have the latest

© SANS Institute 2000 - 2005 Author retains full rights.

service packs and security updates for the following products and components:

- *Microsoft® Windows NT® 4.0, Windows 2000, Windows XP, Windows Server 2003*
- *Internet Information Server (IIS) 4.0, IIS 5.0, IIS 6.0*
- *SQL Server™ 7.0, SQL Server 2000 (including Microsoft Data Engine 1.0 and 2000)*
- *Internet Explorer 5.01 and later*
- *Windows Media Player 6.4 and later*
- *Exchange Server 5.5, Exchange Server 2000, Exchange Server 2003 (including Exchange Admin Tools)*
- *Microsoft Data Access Components (MDAC) 2.5, MDAC 2.6, MDAC 2.7, MDAC 2.8*
- *Microsoft Virtual Machine (VM)*
- *MSXML 2.5, MSXML 2.6, MSXML 3.0, MSXML 4.0*
- *Content Management Server 2001, Content Management Server 2002*
- *Commerce Server 2000, Commerce Server 2002*
- *BizTalk® Server 2000, BizTalk Server 2002, BizTalk Server 2004*
- *SNA Server 4.0, Host Integration Server 2000, Host Integration Server 2004*
- *Microsoft Office*

This check is performed by using information obtained from Microsoft.com in the form of a signed .cab or .xml file (Mssecure.xml). The tool downloads this information from Microsoft.com each time it is run. If it is not able to contact Microsoft.com, it will use a version of the database cached on the local machine. There is also an option to perform this check against an approved updates list from a local Software Update Services (SUS) server, rather than against the complete list of available updates from Microsoft.com.

Default Settings. *Security update scans executed from the Microsoft Baseline Security Analyzer (MBSA) graphical user interface (GUI) or from Mbsacli.exe (MBSA-style scan) will scan and report missing updates marked as critical security updates in Windows Update (WU), also referred to as baseline critical security updates. When a security update scan is executed from Mbsacli.exe using the /hf switch (HFNetChk-style scan), all security-related security updates will be scanned and reported. A user running an HFNetChk-style scan can choose to scan for WU critical security updates only, and can suppress notes or warnings, if not desired, through the command-line parameters.*

SUS Scan Option. *This option will search for missing security updates included in an approved items list on the SUS server, rather than from the full list of available security updates in the Mssecure.xml file from the Microsoft Web site. When this option is selected in the GUI, MBSA attempts to automatically obtain the local SUS server name from the local registry.*

© SANS Institute 2000 - 2005, Author retains full rights.

Otherwise, MBSA will use the SUS server name that is entered by the user. MBSA connects over HTTP to the specified SUS server and reads the Approveditems.txt file to identify security updates that have been explicitly approved by the SUS administrator. MBSA notes the approved security updates and then looks at a mapping table in the Mssecure.xml file to match the SUS security updates to the updates in the XML file. MBSA will then perform the security updates scan based on the selected updates in the Mssecure.xml file, which is mapped to the approved updates on the local SUS server.[57]

4. How to Correct This?

The MBSA provides the details on the issue discovered, a solution to the issue and any additional notes that may relate to the known issue.

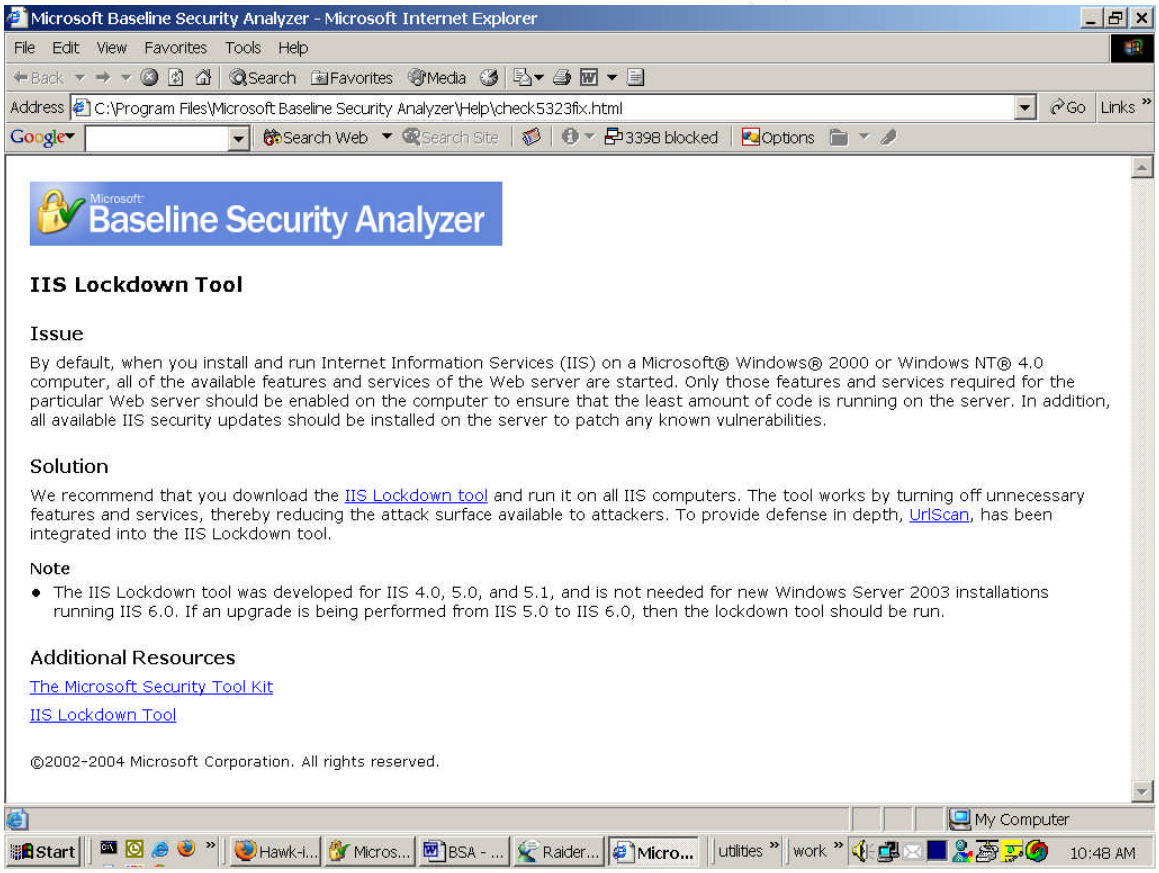


Figure 9 Breakdown on how to correct issues discovered by MBSA

[57] What was scanned is defined by the MBSA help file.

© SANS Institute 2000 - 2005 Author retains full rights.

5. Keeping History

After the initial scan by MBSA, the reports are save and available for later viewing. You will now notice a “view existing security reports option”.

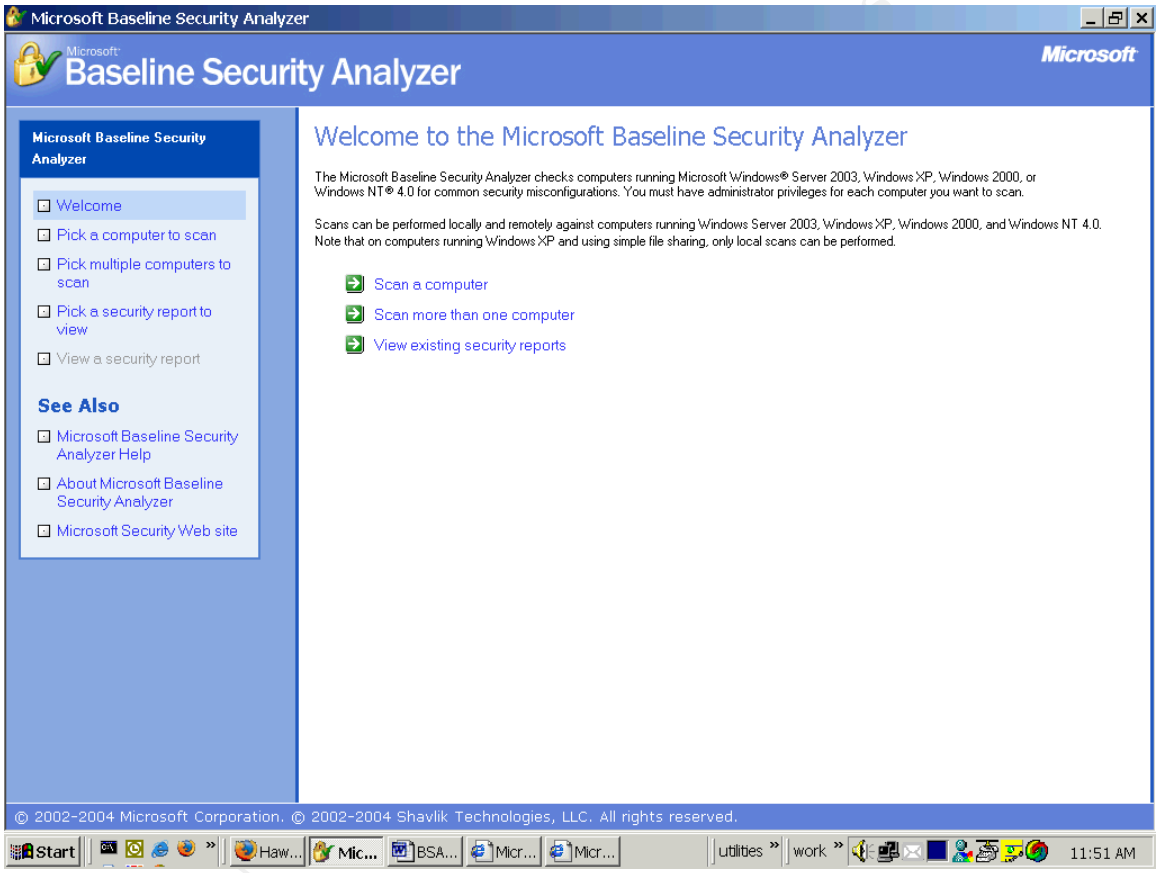


Figure 10 Looking at your History

7. Command-Line Options

There are two types of scans that can be performed using the MBSA command line interface: **MBSA-style scans** and **HFNetChk-style scans**. The following is documentation from Microsoft on the two types of scans preformed and their options.

MBSA-Style Scans *provided by Microsoft TechNet*

© SANS Institute 2000 - 2005 Author retains full rights.

The MBSA-style scan will store results, as was done in MBSA V1.1.1, in individual XML files to later be viewed in the MBSA UI. MBSA-style scans include the full set of available Windows, IIS, SQL, Desktop Application, and security update checks. Note users will have to explicitly use the -nosum switch to perform the same scan as done in the MBSA GUI.
The tool can be run from the command line (in the Microsoft Baseline Security Analyzer installation folder) using "**mbsacli.exe**" with the following parameters:

Selecting computer to scan

<no option> - Scan the local computer
/c <domainname>\<computername> - Scan the named computer
/i <xxx.xxx.xxx.xxx> - Scan the named IP
/r <xxx.xxx.xxx.xxx - xxx.xxx.xxx.xxx> - Scan range of IP addresses
/d <domainname> - scan named domain

Selecting which scan options NOT to perform (can concatenate like /n OS+IIS+Updates)

/n IIS - Skip IIS checks
/n OS - Skip Windows Operating System (OS) checks (note this will also skip the IE/Outlook zones and Office macro security checks)
/n Password - Skip password checks
/n SQL - Skip SQL checks
/n Updates - Skip security update checks

Security update scan options

/sus <SUS server | SUS filename> - Check only for security updates approved at the specified URL of the SUS server or the file path to the approveditems.txt file. If a URL or path is not specified, the value stored in the registry will be used if available.
/s 1 - Suppress security update check notes
/s 2 - Suppress security update check notes and warnings
/nosum - Security update checks will not test file checksums
/nvc - Don't check for a new version of MBSA

Specifying output file name template

/o <filename> - Default filename format is "%d% - %c% (%t%)", where %d% is the domain, %c% is the computername, and %t% is the date and time. %IP% can be used to include the IP address of the scanned machine. Note that report name variables from previous versions of MBSA will also function: "%domain% - %computername% (%date%)"

© SANS Institute 2000 - 2005, Author retains full rights.

Displaying results and details

Note these report options cannot be combined with the security update scan options listed above.
/e - List errors from latest scan
/l - List all reports available
/ls - List of reports from latest scan
/lr <report name> - Display overview report
/ld <report name> - Display detailed report
/v - Display security update reason codes

Miscellaneous options

/? - Usage help
/qp - Don't display progress
/qe - Don't display error list
/qr - Don't display report list
/q - Don't display any of the above
/f - Redirect output to a file
/unicode - Generate unicode output (Users running Japanese MBSA or scanning Japanese Windows machines should specify this switch)

HFNetChk-Style Scans

The HFNetChk-style scan will check for missing security updates and will display scan results as text in the command line window, as is done in the standalone HFNetChk tool. MBSA V1.2 includes the "/hf" flag which will indicate an HFNetChk scan to the MBSA engine. The HFNetChk switches listed below can be used after the "/hf" flag is specified on the command line. Note users will have to explicitly use the -v, and -nosum switches to perform the same scan as done in the MBSA GUI.
Note: the Office security update scan will NOT be performed with the /hf flag as it is performed outside of the HFNetChk engine. Office security updates can be scanned in the MBSA GUI (mbsa.exe) or the MBSA-style scan using mbsacli.exe.

Note: the MBSA-style scan parameters listed above cannot be combined with the /hf flag option. The tool can be run from the command line (in the Microsoft Baseline Security Analyzer installation folder) using "**mbsacli.exe /hf**" followed by any of the parameters below. For a full description of each parameter, please see KB article Q303215.
Selecting computer to scan

© SANS Institute 2000 - 2005, Author retains full rights.

-h <hostname> - Scan the named NetBIOS computer name. Default location is the local host. Multiple hosts can be scanned by separating host names with a comma.
-fh <filename> - Scans the NetBIOS computer names specified in the named text file. Specify one computer name on each line in the .txt file, with a 256 name maximum.
-i <xxx.xxx.xxx.xxx> - Scans the named IP address. Multiple IP address can be scanned by separating each entry with a comma.
-fip <filename> - Scans the IP addresses specified in the named text file. Specify one IP address on each line in the .txt file, with a 256 entry maximum.
-r <xxx.xxx.xxx.xxx - xxx.xxx.xxx.xxx> - Specifies IP address range to be scanned.
-d <domainname> - Specifies the domain name to be scanned.
-n - Specifies that all computers on the local network should be scanned. All computers from all domains in Network Neighborhood are scanned.

Specifying which scan options should/should not be performed or displayed

sus <SUS server | SUS filename> - Check only for security updates approved at the specified URL of the SUS server or the file path to the approveditems.txt file. If a URL or path is not specified, the value stored in the registry will be used if available.
-fq <filename> - Specifies the name of a file that contains Qnumbers to suppress on output. Specify one Qnumber per line. This switch only suppresses the specified item(s) from being displayed in the output; it does not remove the item(s) from consideration during the course of a scan.
-s - Suppresses NOTE and WARNING messages. The default is not to suppress either of these message types. The following options are used with this switch:

(1) Suppresses NOTE messages only.
(2) Suppresses both NOTE and WARNING messages.

-nosum - Specifies to not perform checksum validation for the security update files. You do not need to use this switch under typical circumstances.
-sum - Forces a checksum scan when scanning a non-English language system. Use this switch only if you have a custom XML file with language-specific checksums.
-z - Specifies to not perform registry checks. (Note when this switch is used with -history, registry checks will still be performed for those patches that only have registry key data and no file version information in the mssecure.xml file)
-history - Displays updates that have been explicitly installed, explicitly not installed, or effectively installed. (Updates that are effectively installed indicate that the update itself may not have been explicitly installed, but a later, superseding update was installed that contains the fixes from this earlier update.) This switch is not necessary for normal operation; you do not

© SANS Institute 2000 - 2005 Author retains full rights.

need to use it except under very specific circumstances. The following options are used with this switch:

(1) displays those updates that have been explicitly installed.
(2) displays those updates that have been explicitly not installed.
(3) displays those updates that have been effectively installed.

-v - Displays the reason why a test did not work in wrap mode. You can use this switch to display the reason why a security update is considered "not found" or if you receive a NOTE or WARNING message.
/nvc - Don't check for a new version of MBSA.

Specifying output format and file names

-o - Specifies the desired output format. The following options are used with this switch:
(tab) Displays output in tab-delimited format.
(wrap) Displays output in word-wrapped format.
-f <filename> - Specifies the name of a file in which to store the results. You can use the switch in both wrap and tab output.
-unicode - Generate unicode output (Users running Japanese MBSA or scanning Japanese Windows machines should specify this switch)

Miscellaneous options

-t - Displays the number of threads that are used to run the scan. Possible values are 1 to 128, with the default value being 64. This switch can be used to throttle down (or up) the scanner speed.
-u <username> - Specifies the user name to use when scanning a local or remote computer or groups of computers. You must use this switch with the -p (password) switch.
-p <password> - Specifies the password to use when scanning a local or remote computer or groups of computers. You must use this switch with the -u (username) switch. For security purposes, the password is not sent over the network in clear text. Instead, HFNetChk uses the challenge-response mechanism that is built into Windows NT 4.0 and later to secure the authentication process.
-x - Specifies the XML data source that contains the available security update information. The location may be an XML file name, a compressed XML .cab file, or a Uniform Resource Locator (URL). The default file is the Mssecure.cab file from the Microsoft Web site. When this switch is not used, the mssecure.xml file will be downloaded from the Microsoft Web site.
-? - Displays a menu. You can also call this switch by using the /? syntax. The menu is also

© SANS Institute 2000 - 2005, Author retains full rights.

displayed any time that you pass incorrect syntax at a command prompt[58].

© SANS Institute 2000 - 2005, Author retains full rights.

[58]MBSA Command Line-Options
http://support.microsoft.com/default.aspx?scid=kb;en-us;320454&sd=tech