Global Information Assurance Certification Paper

Effective Methods of Addressing The Perpetual Security Patchwork of Microsoft Network Operating Systems

Aaron_Ray_GSEC
July 5, 2002 (*resubmission)*
Version 1.4

Abstract

Maintaining a secure Microsoft operating system presents a formidable challenge for any security or network administrator. This study begins by presenting a brief background discussion of major Microsoft OS and application vulnerabilities that eventually formed the basis of widely distributed and destructive worm-based attacks such as *Code Red* and *Nimda* prompting the need for proper patching of systems. While these events compelled Microsoft to quickly develop automated tools to address these vulnerabilities, most were seriously flawed and found to be of limited value. This is followed by a discussion of effective methods in which operating system vulnerabilities can be identified, corrected, logged, and verified through the use of Microsoft system and third party utilities. The methods and tools presented should help provide a security administrator with the means to ensure that a Microsoft server operating system security and data integrity are preserved in a networked environment thus minimizing potential vulnerability exploits.

Introduction

Although numerous efforts have been made by software vendors and the network security community to establish a unified solution to mitigate the virtually endless procession of Microsoft Network Operating System and application security holes, no single approach has yet been proven completely effective.

The extensive proliferation of worm-based attacks such as *Code Red* and *Nimda* which propagated with lightning speed, exploited a combination of known Microsoft OS vulnerabilities resulting in over a billion dollars of lost productivity worldwide due to downtime and server and database rebuilds. Although these widespread attacks eventually compelled Microsoft to take a more serious stance on security, their efforts resulted in less than successful attempts at addressing OS vulnerabilities using their own automated tools with users of these operating systems often receiving conflicting information or none at all. Extensive problems with Microsoft's automated Windows Update interface have continually been the focal point of the majority of network administrator complaints.

However, a composite approach, which incorporates the use of other Microsoft OS integrated utilities, third party software to scan a server for the existence of current fixes such as St. Bernard's *Update Expert,* and a method to verify that

patched servers are no longer vulnerable to specific exploits such as eEye's *Retina* scanner, can substantially reduce potential exposure to loss. Determining the viability of a patch is also crucial as there may be occasions when such an installation could compromise the proper operation of a device or application. Finally, quick initial notification of a potential vulnerability via a number of network security based email lists along with regular visits to security web sites can also provide precious lead-time in addressing issues.

While developing such a comprehensive approach will not completely eliminate the appearance of Microsoft OS vulnerabilities, ensuring a high level of awareness in these areas is maintained will definitely reduce the potential exposure of an organization to a damaging exploit.

Code Red and *Nimda* Underscore the Need For Better OS Security Via Continuous Patch Maintenance

The rapid proliferation of the *Code Red* and *Code Red II* worms, followed by multi headed *Nimda* worm attack, reinforced the need for better methods in which to keep Microsoft's network operating systems protected from exploits.

Code Red II and its predecessor *Code Red* successfully exploited a known buffer overflow vulnerability with versions of Microsoft's IIS index service `.dll`, in which affected servers were directed to launch distributed denial of service attacks against other Microsoft Internet Information Servers via port 80. If the exploit was successful, the worm began executing on the affected host. When well over 250,000 hosts were eventually compromised, the phrase:

```
HELLO! Welcome to http://www.worm.com! Hacked By Chinese!
```

became the obvious badge of a *Code Red* affected IIS server as many English language based servers infected by an earlier variant of the worm were defaced in this manner. In addition, *Code Red* used affected servers to eventually direct a denial of service attack on a specific IP address, which actually was assigned to http://www.whitehouse.gov.

Code Red II took the process a step further by exploiting additional vulnerabilities that allowed the placement of Trojan versions of the `explorer.exe` command and allowed commands to be remotely executed on the compromised server by providing access to the `cmd.exe` command. Essentially, the process created a backdoor by which other individuals and systems could further exploit affected servers.

In the case of the initial discovery of the *Code Red* exploit, a bulletin and corresponding patch, (http://www.microsoft.com/technet/security/bulletin/MS01-033.asp) was issued by Microsoft on June 18, 2001, to address the core

vulnerability responsible for the tremendous propagation of these worms. However, failure of many to heed the initial warnings and properly patch their servers fell victim to the *Code Red II* variant as well as the dreaded *Nimda* attack, which was soon to follow.

Even with the volume of press coverage these particular exploits received, hundreds of thousands of servers remained unpatched and eventually became vulnerable to a new composite threat known as the *Nimda* worm. *Nimda* took the worm to a new level by leveraging the power of administrator inertia by combining a mixed bag of exploits in a single package to wreak havoc on IIS servers. *Nimda* incorporated all previously discovered exploits including those first appearing in Code Red to hijack servers, consume tremendous bandwidth, and generally cause chaos to those sites ill prepared for such a deluge of activity. In addition, Nimda added another means of attack via email, which incorporated dangerous executable attachments or payloads that would further propagate the worm when launched by the user. [1]

Clearly, the message to remain diligent in the application of Microsoft OS and application security patches still was not reaching a large percentage of the public and additional efforts had to be made to attempt to bridge this communication gap. Also, Microsoft needed to develop an effective means with which to accomplish the patching process. Initial efforts by Microsoft to accomplish this task would be presented but only serve to further frustrate their customers.

Microsoft Misses The Mark With Windows Update

Microsoft's attempts at automating software patch delivery and installation of their operating systems with the Windows Update interface have been met with mixed results at best. Windows Update, originally designed as a means to streamline and automate the process of keeping critical OS and Microsoft application patches current, has instead posed its own series of problems often compromising the stability of the systems it was designed to protect.

For those early adopters of the system, many were dismayed by the inconsistent nature in which the tool would apply particular patches, often nullifying its own efforts by overwriting newer versions of `.dll` and other system files with earlier releases. Not only would patches be applied in such an inconsistent manner that an older patch might overwrite newer code, but these problems could manifest themselves into leaving a system in an inoperable state or vulnerable to security holes.[2]

[1] CERT®, "CERT® Advisory CA-2001-26 Nimda worm"
[2] Fontana, John, "Microsoft users tired of patch management headaches"

Unfortunately, efforts to improve this interface have been limited and its use as an effective patch management tool has been virtually ignored by responsible network administrators. To further complicate the issue, Microsoft recently introduced a new version of the interface for centralized management of larger environments called *Corporate Windows Update*. However, this version of the tool fails to address the patch consistency problems inherent in the original *Windows Update* and will probably meet the same fate as its predecessor as a viable management tool.

Although, all hope is not lost. Fortunately, Microsoft is making some progress in this area by attempting to make their tools more compatible and does offer other utilities that can be effectively utilized in the maintenance of its OS and application patches.

Establishing A Server Security Patch Baseline

Security baselines for operating systems and applications must be established for every IT environment to suit the particular needs of an organization. Types of applications, functional server roles (e.g., database, web, or file servers), and server network location (public or private) form the basis on which standards should be established. Such standards should also incorporate baselines for server security patches as well.

Although Microsoft has received substantial criticism in the past for not providing an effective means for keeping their own operating systems and applications code up to date in regard to addressing security vulnerabilities, their recent release of the Microsoft Baseline Security Analyzer (MBSA) Version 1.0 in April 2002 is clearly a step in the right direction. The MBSA is available as a free download from Microsoft at:
http://support.microsoft.com/directory/article.asp?ID=KB;EN-US;Q320454

In addition to establishing a recommended security baseline for application installation settings based upon the particular role defined for the server (e.g., SQL 7.0 database server, IIS web server, or file server), the MBSA also allows the user to automatically remove unnecessary components, which could introduce potential security vulnerabilities if left installed.

MBSA functions exceptionally well as a means to detect missing hotfixes and service packs for Windows, IIS, and SQL server. In conjunction with HFNetChk, the utility functions very effectively at determining the correct file revisions for programs it is evaluating, thereby eliminating the substantial file mismatch problems associated with the Windows Update interface. It incorporates an outstanding integrated XML based reporting interface that can generate and store individual computer reports in HTML format. [3]

[3] Microsoft TechNet, "Microsoft Baseline Security Analyzer Introduction"

Although the MBSA provides a great tool for removing unnecessary core OS and application components, it simply reports missing patches and does not provide a mechanism for their reinstallation. As a result, use of this tool is sorely inadequate as a comprehensive solution for addressing actual application of patches or maintaining an accurate database of server configurations.

MBSA developer Shavlik Technologies (http://www.shavlik.com) does provide an enhanced version of the tool entitled *Enterprise Inspector 2.0,* which significantly improves the reporting capability and functionality of the MBSA by allowing analysis to occur on all Windows OS based machines in a large environment. Again, the ability to push required fixes to servers is still absent from this enhanced version unless it is coupled with another Shavlik product HFNetCheckPRO. As a result, a total of three separate tools must be pooled to perform the process of managing server patches, making such an option considerably less attractive and more difficult for a network administrator to effectively manage.

While Microsoft is making efforts to more effectively combine the functionality of Windows Update, Corporate Windows Update, and the MBSA, too many conflicts remain which make the exclusive use of their tools for updating servers very precarious.

However, when the MBSA is combined with a comprehensive third party tool such as St. Bernard Software's *Update Expert*, which automates patch installation, helps to establish baseline requirements, and produces extensive compliance reports, maintaining software security on multiple servers is made a manageable process.

Integrating Third Party Tools In Patch Management

The use of another utility in managing the application of server patches is crucial in easing the burden of what could be an extremely time consuming and tedious process. In addition, maintaining an accurate accounting of all servers in a large IT environment is a formidable task unless other resources are employed.

St. Bernard Software's *Update Expert* (http://www.updateexpert.com) effectively handles this task and offers numerous time saving measures to centrally manage the patch installation and accounting of a very large number of servers. In addition, it incorporates an extensive relational database, which allows the generation of numerous reports that provide an excellent overview of the current status of the patch installation status of all servers. It also provides a scheduling feature that allows the update process to be automated. (***Figure 1***)

Initial setup of the program is relatively simple and only requires a few steps to begin taking advantage of the program's powerful features. By adding all manageable servers by IP address or NetBios name and providing appropriate logon credentials, *Update Expert* can query the server and immediately determine all currently installed software and patch levels. In addition, the program integrates a powerful research feature that provides direct links to all Microsoft supporting documentation on all patches installed and available for installation on the server.

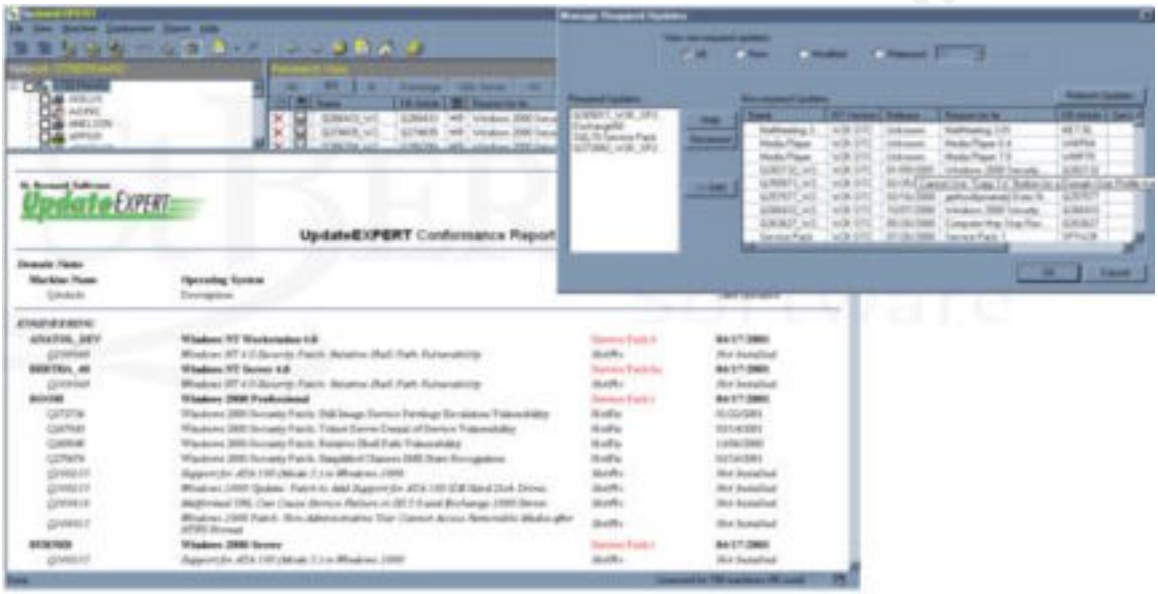

***Figure 1* – Update Expert Conformance Report and Updates Dialog**

While most large code patches such as OS or applications service packs are usually compulsory in their installation, interim patches more commonly identified as "hot-fixes," are not always recommended unless there is a critical security need. Proprietary applications and special configurations can often be adversely affected by the premature application of a patch. *Update Expert's* research interface allows easy, instant access to this information making the decision of whether a patch should be applied less time consuming.

Update Expert's intuitive logic also determines appropriate patch levels with a high level of accuracy based upon which specific applications are running on a server. This results in fewer potential misapplications of patches that could have disastrous effects on the operating system including application instability or the dreaded "blue screen of death." (***Figure 2***)

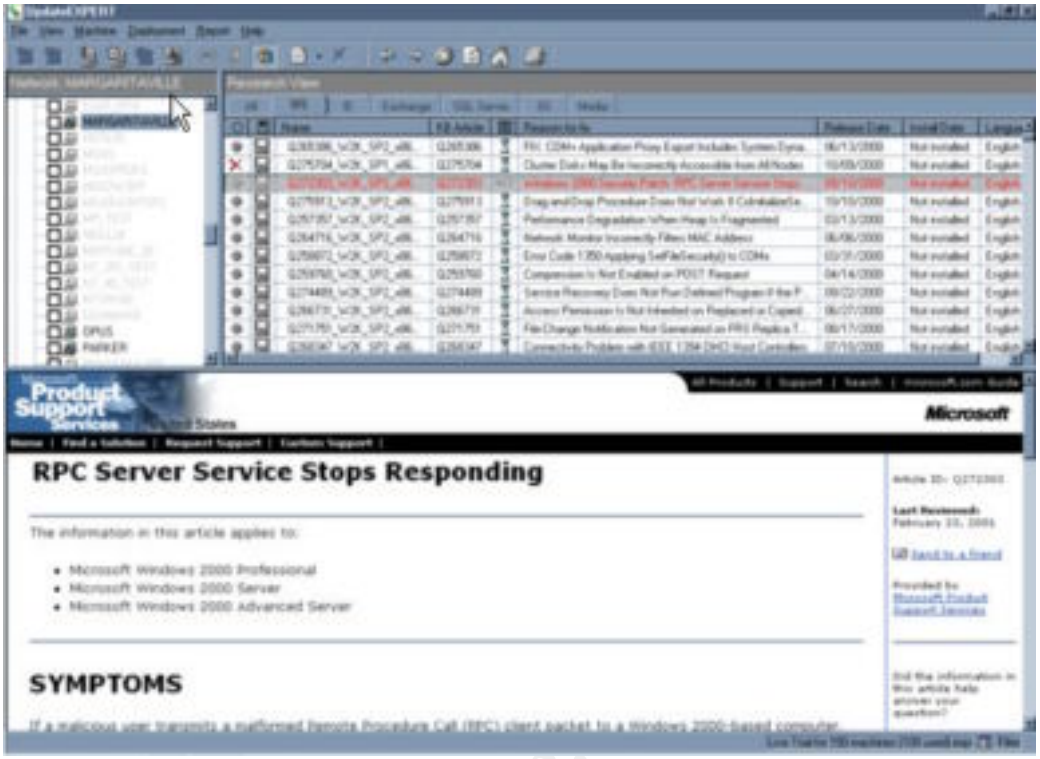

Figure 2 – **Update Expert Research Interface Screen**

As part of a Microsoft OS and application security patch management system, *Update Expert* functions quite well and can be an extremely effective weapon in the update war arsenal. Although, no single system can be a panacea for all the challenges maintaining a secure OS and additional precautions must be always be carefully taken to ensure a particular system maintains stability following application of security patches.

Verifying The Integrity Of New Security Patches

Application of new patches immediately upon their release is not necessarily always an appropriate course of action. Although network administrators must remain diligent in addressing all potential software vulnerabilities as they are discovered, erring on the side of caution is often a very wise approach given the reactionary nature of developers at Microsoft or other major software vendors when presented with potentially exploitable vulnerabilities in their code.

Although many commercial software manufacturers make a reasonable effort to test their applications using newly released OS system hotfixes or service packs, most proprietary application developers often use the path of least resistance when developing their code. That is, applications developed might be based upon default installations of the operating system or incorporate elements that require broad access to system executables or files. As a result, installation of

new OS service packs or files might have a tendency to break or disrupt proper operation of the program. In order to avoid initiating unnecessary conflict between an administration and development group, it is usually advisable to adopt a phased implementation approach, which will give both groups the opportunity to review their respective areas for problems affecting the operation of applications and offer viable suggestions for change. [4]

Moreover, as numerous organizations run proprietary applications on their mission critical production servers, it is strongly recommended that a parallel production-testing environment be created on which to test new patches to ensure applications are not adversely affected by their installation.

While this approach may not always be an option for a smaller company, other steps can be taken to mitigate the risk of patch application including regular system backups or disk images and the creation of Windows NT emergency repair disks (ERD), which would allow a system to return to its pre-patched state. Both methods should be maintained within any IT environment, however.

Even when patches appear to be distributed in a fairly expedient manner, their ability to fully address vulnerabilities is occasionally viewed as suspect by industry security experts who may feel that the code developers are simply taking a reactionary stance to potential vulnerabilities and not doing their homework.

Microsoft's past efforts to address security vulnerabilities have often been met with considerable skepticism in that their attempts appear to be either contradictory to their own efforts or negligent in addressing all issues identified. Multiple past patch releases have often been revised without Microsoft providing proper notification to its customers resulting in conflicts with future patch releases that create an unstable operating system. Also, many patches released are simply reactionary addressing only a symptom and don't identify a problems root cause.[5]

In this case, questions were posed about the particular Microsoft patch's ability to completely address issues identified as exploitable holes in the application. Although such situations don't necessary warrant delaying application of a particular patch, they simply underscore the need to perform due diligence by regularly consulting as many security resources as possible.

Again, the ability to successfully test a patch on a similarly configured backup server is probably the best means of ensuring a production server will remain stable following patch installation.

The following sites are outstanding independent resources for current information on network security and potential threats:

[4] ZD Staff, "'Patchwork' security is right for you"
[5] Costello, Sam, "Researchers: Newest Microsoft IE patch flawed"

- **Security Administrator** is an excellent source for security based technical information including virus tracking and offers a mailing list (http://www.secadministrator.com)
- **Incidents.org** provides a global perspective on web traffic and can offer insights to unusual activity, which often can be the result of a new exploit. A great recent example was the quick identification of the recent SQL worm when unusually high levels of traffic were discovered propagating on port 1433 throughout the Internet. (http://www.incidents.org)
- **CERT** provides great resources for software and hardware security vulnerabilities as well as information on network security planning and industry trending operated by Carnegie Mellon University in Pennsylvania (http://www.cert.org)
- **ZDNet's Security Update** is a good media resource for broader based security issues. It compiles information from multiple sources and presents issues in a reasonable clear and timely manner. (http://techupdate.zdnet.com/techupdate/filters/mrc/0,14175,6020424,00.html)

Confirming The Integrity of Application and Operating System Security

Even the most conscientious effort in the regular installation of Microsoft OS and application security patches will be rendered moot if their efficacy is not regularly and thoroughly tested through use of an accurate network scanner such as eEye's *Retina* (http://www.eeye.com/html/Products/Retina/index.html)

Retina's ability to accurately detect the majority of multiple OS vulnerabilities including Windows NT, Linux/Unix, and AIX makes it an excellent tool to use to verify if regular patching of servers has been completed in a manner that ensures system security has been maintained. It can also serve as an effective means to determine if any other vulnerabilities exist that may have been recently discovered by the security community but not yet specifically addressed by Microsoft.

Retina's fairly straightforward graphical user interface (GUI) makes conducting device scans quite simple and can speed the process of detection and verification of potential exploits. (***Figure 3***)

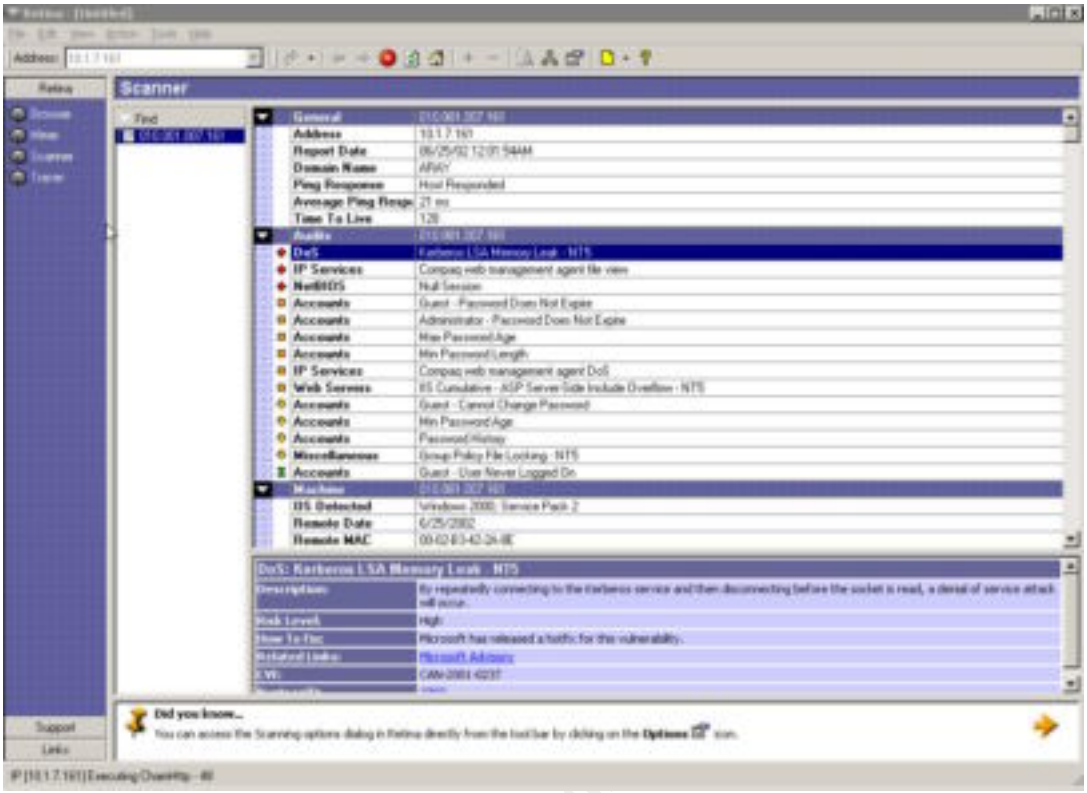

Figure 3 – **Retina's Scanning Results**

In the lower frame of *Retina's* scanning panel, complete explanations of discovered vulnerabilities are provided along with links to additional resources including patches that will address the security hole. Concerns about the accuracy and integrity of *Retina's* detection data are few as the application can be automatically configured to update its database from the latest information available from eEye's central file server.

Of course numerous other network vulnerability scanning packages are available such as:

- Network Associates Cyber Cop (http://www.sniffer.com/services/support/technical-support/supp-home.asp?pCode=CYS)
- Internet Security Systems (http://www.iss.net)
- Net IQ Security Analyzer (http://www.netiq.com/products/sa/default.asp) Nessus (http://www.nessus.org)
- Symantec Net Recon (http://enterprisesecurity.symantec.com/products/products.cfm?productID=46)

However, Retina has consistently maintained better ratings for ease of use and accuracy in the detection of network vulnerabilities and has even garnered the

Blue Ribbon award from Network World Fusion buying guide for its performance.[6]

In any case, utilizing a network security scanner as part of an overall patch maintenance approach, is crucial for ensuring servers are actually protected from exploits.

Maintaining Awareness Of New Vulnerabilities

No approach to addressing the Microsoft security patchwork would be complete without ensuring that information about new or modified exploits is received at regular intervals. Discovering the existence of a new Microsoft vulnerability by becoming a victim of an exploit is probably a great way to adversely affect job security.

Fortunately, numerous mailing lists exist that provide an invaluable wealth of information about suspected Microsoft vulnerabilities and are often an early indicator of the efficacy of recently released patches. Early patch adopters also serve as a great resource for more extensive testing of patches in a much wider variety of network environments, which may not be possible at many sites.

Subscribing to the following mailing lists will significantly increase an individual's knowledge base and allow for a much quicker identification and resolution of potential problems posed by suspected vulnerabilities:

- **NTBugTraq** (http://www.ntbugtraq.com) is probably one of the most respected independent community think tanks for the identification and analysis of Microsoft NT based vulnerabilities. List moderator Russ Cooper has been responsible for bringing a number of potential exploits to the attention of Microsoft, which resulted in the release of official patches. The list also serves as an effective aggregator of official Microsoft patch bulletins
- **NT Security** (http://www.ntsecurity.net) is another outstanding mailing list which is a bit broader in nature but offers great insight in all NT related security issues
- **Microsoft NT Security** (http://www.microsoft.com/security) Security information directly from the horse's mouth. Microsoft has made a fairly reasonable effort to aggregate all security related issues into a central location and the majority of relevant information can be found here.
- **W2K News** (http://www.w2knews.com) A comprehensive independent resource for all Windows 2000 and NT related issues. Often offers insight in advance of other resources on core or security related OS concerns.

[6] Andress, Mandy, "Network Scanners Pinpoint Problems"

This list represents only a few of the numerous mailing lists available to the security professional. Fortunately, many of these resources also include their own references as well.

Pulling It All Together

Ensuring the security of Microsoft servers is maintained clearly is and will always be a substantial challenge. However, following some of the basic approaches outlined in this study will certainly ease the pressures of an administrator.

While the prevalence of *Code Red* and *Nimda* worm type exploits have diminished considerably given a serious and conscious effort to continually apply Microsoft OS patches, it is important that administrators remain diligent in their efforts. Even today, most Internet Information Server logs will still contain proof that such exploits are being attempted and unfortunately continue to infect a number of vulnerable servers that remain unpatched. It is only a matter of time before other more complex exploits propagate their way through the Internet.

Microsoft continues to make significant improvements in providing their own tools to address security vulnerabilities with their operating systems but still have far to go in providing a comprehensive solution to the problem. *Windows Update* and *Corporate Windows Update* continue to present problems for those who attempt to use them for keeping their Microsoft OS levels current. However, their *Microsoft Baseline Security Analyzer* in conjunction with an effective patch management system such as St. Bernard's *Update Expert* can substantially ease the ease the burden of maintaining OS updates. In addition, a patch management system also can provide excellent accounting and provide comprehensive reports of the patch application status on a large quantity of servers as well. Of course, careful attention must also be paid to ensuring the stability of a system once it has been patched. A phased implementation of a new patch in a testing environment will reduce adverse impact to production applications.

Finally, the use of a highly accurate network security scanner such as Retina to ensure that patched vulnerabilities have indeed been addressed is probably one most crucial steps in the process. Not validating the patching process is practically synonymous with ignoring the entire process as a whole and rendering any other effort made as futile.

Although no one approach to addressing the Microsoft patch debacle is a guarantee that a Microsoft OS or application will be kept free of security holes, making a concerted effort to remain aware of existing and new exploits, scanning all servers on a consistent basis for the existence of patches and susceptibility to new exploits, and maintaining comprehensive reports will ensure that any potential impact to the security of an NT server is minimized.

References

1. CERT "Cert Advisory, CA-2001-26-Nimda-Worm" URL: http://www.cert.org/advisories/CA-2001-26.html

2. Fontana, John, "Microsoft users tired of patch management headaches," 22 April 2002 URL: http://www.nwfusion.com/news/2002/131957_04-22-2002.html

3. Microsoft TechNet, "Microsoft Baseline Security Analyzer Introduction" 4 April 2002 URL: http://www.microsoft.com/technet/security/tools/Tools/MBSAhome.asp

4. ZD Staff, "'Patchwork' security is right for you," 25 November 2001 URL: http://zdnet.com.com/2100-1107-504131.html

5. Costello, Sam, "Researchers: Newest Microsoft IE patch flawed" 20 May 2002 URL: http://www.cnn.com/2002/TECH/internet/05/20/ie.patch.flawed.idg

6. Andress, Mandy, "Network Scanners Pinpoint Problems," 04 February 2002 URL: http://www.nwfusion.com/reviews/2002/0204bgrev.html

Microsoft Technet (Index Server .dll vulnerability patch)
http://www.microsoft.com/technet/security/bulletin/MS01-033.asp

Microsoft Baseline Security Analyzer, Microsoft
http://support.microsoft.com/directory/article.asp?ID=KB;EN-US;Q320454

Enterprise Inspector 2.0/HFNetChkPRO, Shavlik Technologies
http://www.shavlik.com

Update Expert, St. Bernard Software
http://www.updateexpert.com

CERT Coordination Center
http://www.cert.org

ZDNet's Security Update
http://techupdate.zdnet.com/techupdate/filters/mrc/0,14175,6020424,00.html
Security Administrator
http://www.secadministrator.com

Incidents.org

http://www.incidents.org

Retina
http://www.eeye.com/html/Products/Retina/index.html

Cyber Cop, Network Associates
http://www.sniffer.com/services/support/technical-support/supp-home.asp?pCode=CYS

Internet Security Systems
http://www.iss.net

Security Analyzer, Net IQ
http://www.netiq.com/products/sa/default.asp

Nessus
http://www.nessus.org

Net Recon, Symantec
http://enterprisesecurity.symantec.com/products/products.cfm?productID=46

NTBugTraq
http://www.ntbugtraq.com

NT Security
http://www.ntsecurity.net

Microsoft NT Security
http://www.microsoft.com/security