Common Errors in OS Hardening Instructions, Security Audit Findings and Security Patch Information for Windows NT

Dave Loschiavo

Introduction:

Security guidelines are proliferating almost as rapidly as new exploits. As system administrators become more aware of the importance of securing their computers, more companies and individuals are stepping forward to offer guidance in this effort. Security guidelines, security reviews and updates of existing products are three areas that have seen an increase in activity as administrators attempt to keep their systems secure.

This paper will focus on the errors that the author has encountered in various guides, security reviews, and information regarding product updates. The reason for writing the paper is to increase the awareness of mistakes that commonly occur, in the hope that they will be easier to avoid in the future, and in order to ensure that system administrators look at security instructions with a critical eye.

As my experience is primarily with Microsoft operating systems, I will limit my discussion to this area.

Types of errors:

Most of the errors I run across fit into one of five groups.

These groups, and specific examples are:

1. <u>Instructions that do not have the affect indicated in the guide or review.</u>

   This is an example is more common in security certification test reports. A security finding that I often see in these documents is that a system does not have the following registry value set: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\RestrictAnonymousAccess = 1.

   According to the reviews, this key is supposed to prevent guest access to the registry on a Windows NT system. There is no factual basis for this assertion, and the actual means for accomplishing this can be found in two Q articles published by Microsoft. The correct method is to set the ACL on HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg. This is detailed in Q153183 and Q155363.

   Another example is a finding stating that null sessions are allowed on the system, and that HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\Restrict

Anonymous = 1 should be set to prevent null session connections. While this does prevent enumeration from a null session, it does not prevent the ability to establish a null session.

A third example can be found in the current draft version of the *Secure Windows NT Installation and Configuration Guide*. This guide instructs the system administrator to add the following value in the registry: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\RestrictNullSessAccess = 1, in order to prevent null session access. The functionality of this key exists by default in Windows NT. Were this key added and the value set to "0" then shares that are set to allow "Everyone" access could be accessed via a null session. Adding the key and setting it equal to one provides no added security to the system.

Mistakes such as these can usually be avoided by performing research. If you run across an instruction that is new to you, double-check your source. The RestrictNullSessAccess error could have been avoided by researching the setting at Security Focus' website. While the null session issue could have been resolved by consulting any number of quality publications or Microsoft's Knowledge Base (Q143474). As for the RestrictAnonymousAccess setting, a good dose of suspicion never hurt the security professional. If an extensive search of published sources, as well as an Internet search, fails to turn up a corroborating source, its time to contact whoever is making the recommendation and find out what source they used in when deciding to make the recommendation. If they cannot come up with a corroberating source, it should safe to judge the instruction to be incorrect.

2. <u>Instructions that cannot be followed.</u>

Occasionally I run across an instruction that cannot be carried out. The *Secure Windows NT Installation and Configuration Guide* has just such an instruction. Section 9 of this guide (User Manager for Domains Configuration) directs the system administrator to remove all group memberships from the default Administrator account, with the exception of the "local Administrators group". This instruction cannot be followed. All users must belong to a primary group, and it is not possible to assign the local Administrators group as a primary group.

Sitting down at a system and actually performing the recommended steps can prevent errors such as this. This a critical step that should always be performed prior to publishing a security guide. Securing a system can be difficult and frustrating, having impossible instructions in the guide will not make the experience any easier for the system administrator.

If, as a system administrator, you run across an instruction that appears to be impossible to carry out, it is important to determine if the problem is due to the configuration of the system you are working with, or the instruction itself.

Attempt the instruction on at least two (non-production) systems before looking to the guide as being the source of the problem. If through testing it becomes apparent that the problem is the instruction, contact the author. Odds are they will already be aware of the issue and will able to provide better instructions.

3. Instructions that may severely affect the stability of a system.

   The NSA publication, *Guide to Securing Microsoft Windows NT Networks* directs the system administrator to set HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\CrashOnAuditFail = 1. This setting sacrifices system stability to protect the integrity of the security logs. With this registry value set as per the instruction, the system will lock up if the security event log fills. While there are some environments where this may be desirable behavior, it is vital that the system administrator be made aware of the possible consequences of settings such as this.

   When an instruction such as this made, it is imperative that the author of the guide take extra precautions to ensure the system administrator is aware of the possible detrimental impacts that these settings may have. Ultimately it falls on the system administrator to ensure that the actions they take do not adversely affect the systems for which they are responsible. Test configurations in a non-production environment, and always study the possible (and observed) consequences of configuration changes.

4. Incorrect security patch recommendations.

   Recently, I received a draft of the *Secure Windows NT Installation and Configuration Guide*. One section of the guide dealt with the security patches that should be installed on Windows NT computers that are running SP6a. Though the guide is specific to Windows NT, there were numerous patches (listed as mandatory) that apply only to Windows 9x, Windows 2000, or to software that does not run on Windows NT (such as the Mac version of Internet Explorer).

   Performing a careful check of the information maintained by Microsoft at the Microsoft Security website would have prevented these mistakes, and would also prevent installing uneeded (and possibly undesired) patches.

5. Problems at official vendor sites.

   This issue isn't specific to security guide writers, rather this is an issue I often encounter when working with the information posted at a vendor's website.

As an example, let's look at Q271752. This article deals with a vulnerability in the Microsoft Virtual Machine. The article states, "To resolve this potential problem, install the latest version of the Microsoft VM as specified in this section… 3300-series Microsoft VM customers Upgrade to build 3316 or later from http://www.microsoft.com/java/vm/dl_vm40.htm." The system I am using to write this document is running Windows 2000 SP1. When I check the version number of the VM, I find that it is 5.00.3310. This would seem to indicate that I am running a vulnerable version of the VM. However, four days prior to my writing this document, the same article also stated, "This problem was first corrected in Windows 2000 Service Pack 1", which is in opposition to the earlier statement. This error has since been corrected, and the article no longer indicates that the problem was resolved in Windows 2000 SP1. (Which also means I need to look at installing a security patch on my notebook.)

Conclusion:

As a writer of security guidelines, or a system administrator trying to secure your systems, it is imperative that you sanity check all instructions, even if they do come from the vendor of the product in question.

References:

1. Microsoft Corp. "How to Restrict Access to NT Registry from a Remote Computer". Microsoft Support Knowledge Base. January 31, 1999. URL: http://support.microsoft.com/support/kb/articles/Q153/1/83.asp?LN=EN-US&SD=gn&FR=0
2. Microsoft Corp. "HOWTO: Regulate Network Access to the Windows NT Registry". Microsoft Support Knowledge Base. August 26, 2000. URL: http://support.microsoft.com/support/kb/articles/Q155/3/63.asp?LN=EN-US&SD=gn&FR=0
3. Microsoft Corp. "Restricting Information Available to Anonymous Logon Users". Microsoft Support Knowledge Base. August 26, 2000. URL: http://support.microsoft.com/support/kb/articles/Q143/4/74.asp?LN=EN-US&SD=gn&FR=0
4. Microsoft Corp. "FIX: Microsoft VM Applet Vulnerability". Microsoft Support Knowledge Base. September 25, 2000. URL: http://support.microsoft.com/support/kb/articles/Q271/7/52.ASP?LN=EN-US&SD=gn&FR=0).
5. Microsoft Technet Security Website, various bulletins. URL: http://www.microsoft.com/security/default.asp
6. SecurityFocus. "Installing and Securing Windows NT 4.0: Create and Modify Registry Settings". December 6, 1999. http://www.securityfocus.com/focus/microsoft/nt/ntsecure_reg.html#keys
7. McClure, Scambry, Kurtz, "Hacking Exposed: Network Security Secrets & Solutions". 1999 McGraw-Hill Companies.
8. Department of the Navy, Space and Naval Warfare Systems Command, Naval Information Systems Security Office, PMW 161, "Secure Windows NT Installation and Configuration Guide, Service Pack 6a – Draft" and , "Secure Windows NT Installation and Configuration Guide, Service Pack 3" September 27, 2000 and date unknown. URL: http://support.microsoft.com/support/kb/articles/Q143/4/74.asp?LN=EN-US&SD=gn&FR=0

9. National Security Agency, Network Attack Techniques Division of the Systems and Network Attack Center, “Guide to Securing Microsoft Windows NT Networks”. February 3, 2000.