

End to End Security for Windows 2000 Server

by: DaAnZeR, 10/21/2004

<http://www.securitydocs.com/library/2647>

Summary

This document provides background information and detailed steps that should be taken in order to harden the windows 2000 operating systems against common network security attack. Please note however that operating system hardening procedures cannot be followed blindly. Operating system hardening involves, among other things, turning off all services that are not required for particular application. For this reason, each operating system hardening instance must be customized and this document should only be considered as a general guideline to follow during this customization.

Purpose of this Document

The purpose of this document is to protect Windows 2000 Servers and network elements connected to networks, which may be vulnerable to attacks. The following is a list of commonly known types of attacks:

1. Viruses, worms, backdoors and Trojans
2. Wire tapping and sniffing
3. Password cracking
4. Exploits of known vulnerabilities such as software buffer overflow
5. Denial of services (DOS).

Responsibility

The administrator should use this document for implementation. The administrator should update this document as per the new vulnerability and updates are found.

Prerequisite

One particular installation's requirements can differ significantly from another. Therefore, it is necessary for Administrator to individually evaluate their particular environments and requirements before implementing any of the security configurations suggested within this document. Implementing security settings can affect system configurations already in use or effect requirement variations in the future. Certain applications installed on Windows 2000 Server may require more relaxed settings to function properly than others because of the nature of the product. Therefore Administrators are strongly advised to carefully evaluate recommendations in the context of their system configurations and environment. Before implementing this document it is recommended that the changes be tested. Any changes must be made on the Test Server before and after successful testing of these changes, it can then be implemented on the live server.

Installation

First and foremost is USING the NTFS file system - especially for the boot partition. Yes, it is possible to secure a FAT partition from a remote users perspective, but the use of FAT increases risk considerably.

Another issue that needs to be corrected during installation is the default directory. Do not install system files in the WINNT directory. Rename the directory anything else you like -- MANDRIK and LINUX are two popular examples. I'll refer to the system directory as SUNOS for the remainder of this paper. This step will prevent attacks hard coded to refer to files in the WINNT directory.

Documentation of configuration

Make sure that the current configuration of the system is documented. Update the same after any change is made to the system.

NTFS Permissions

After the installation has completed you will need to correct the NTFS permissions. The primary goal is to get rid of all occurrences of "EVERYONE". Try the following, in your test environment first of course:

- Reset permissions at the logical drive level for all of your drives as shown below. Apply the settings to all child objects and enable propagation of inheritable permissions.

Administrators Full Control

Authenticated Users Modify

Read and Execute

List Folder Contents

Read

Write

CREATOR OWNER Full Control

SYSTEM Full Control

- After this has been done remove all permissions for Authenticated Users from SUNOS (the system directory) and its child objects.

- Allow Authenticated Users Modify, Read and Execute, List Folder Contents, Read and Write to the following directories and all of their child objects:

Documents and Settings

SUNOSInstaller (Note: It's hidden...)

SUNOSSystem32Spool

SUNOSSystem32Config

SUNOSRepair

- Allow Authenticated Users Read and Execute, List Folder Contents and Read to SUNOSSystem32SpoolDrivers. This is an important step as it prevents users from uploading trojaned drivers that would be distributed to other users.

- Set the appropriate permissions on your user directories.

Share Permissions

We have already locked down the file system, but you should still check your share permissions if applicable. It is a little extra work, but I never turn down the opportunity to add a layer of security to my servers.

Services

Now is a good time to disable any unnecessary services. These are the ones I typically do not require to be running on a server:

DHCP Client

Fax Service

Internet Connection Sharing

Intersite Messaging

Remote Registry Service

RunAs Service

Simple TCP/IP Services

Telnet

Terminal Services

Utility Manager

If your server is destined to be an intrusion detection box it would be wise to disable services like Computer Browser and Server as well.

Protocols

Unbind protocols like IPX and NetBIOS from interfaces where they are not required. They love to broadcast, and broadcasts are evil.

User Accounts

Next we will secure the local user accounts.

- Disable the Guest account and give it a very strong password.
- Disable the TsInternetUser account and give it a very strong password. Create the account if it does not exist. Do not delete the account even if it is not being used, since when you later upgrade the OS the account will be created if it does not exist. I am assuming you already created a very strong password for the Administrator account during the installation.

Set Account Lockout Policy

Windows 2000 includes an account lockout feature that will disable an account after an administrator-specified number of logon failures. In case of standalone server use the Local Security Policy) snap-in to set the following parameters for implementing account lockout policy:

- Account Lockout duration
- Account Lockout threshold
- Reset account lockout counter after

Registry

Restrict Anonymous

There are a couple of registry keys that are pertinent here as well:

HKLM\System\CurrentControlSet\Control\Lsa\RestrictAnonymous "HKLM" refers to the hive "HKEY_LOCAL_MACHINE". If this is set to "1" anonymous connections are restricted. An anonymous user can still connect to the IPC\$ share, but is restricted as to which information is obtainable through that connection. A value of "1" restricts anonymous users from enumerating SAM accounts and shares. A Value of "2", added in Windows 2000, restricts all anonymous access unless explicitly granted. **Null Session Shares and Null Session Pipes**

The other keys to inspect are:

HKLM\SYSTEM\CurrentControlSet\Services\LanmanServerParameters\NullSessionShares
and:

HKLM\SYSTEM\CurrentControlSet\Services\LanmanServerParameters\NullSessionPipes

These are MULTI_SZ (multi-line string) registry parameters that list the shares and pipes, respectively, that are open to null sessions. Verify that there are no shares and pipes open that you do not want open. Put security on the above keys as well so they can't be easily modified. Verify that only "SYSTEM" and "Administrators" have access to these keys.

Now we will need to fire up REGEDT32 and add or edit the following values. Most of them are intended to defend against Denial of Service attacks, while the others help prevent such things as the enumeration of accounts by unauthenticated users.

Under HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet \Services add or modify the following values:

Key: TcpipParameters

```

Value: SynAttackProtect
Value Type: REG_DWORD
Parameter: 2
Key: TcpipParameters
Value: TcpMaxHalfOpen
Value Type: REG_DWORD
Parameter: 100
Key: TcpipParameters
Value: TcpMaxHalfOpenRetried
Value Type: REG_DWORD
Parameter: 80
Key: TcpipParameters
Value: EnablePMTUDiscovery
Value Type: REG_DWORD
Parameter: 0
Key: TcpipParameters
Value: EnableDeadGWDetect
Value Type: REG_DWORD
Parameter: 0
Key: TcpipParameters
Value: KeepAliveTime
Value Type: REG_DWORD
Parameter: 300000
Key: TcpipParameters
Value: EnableICMPRedirect
Value Type: REG_DWORD
Parameter: 0
Key: TcpipParametersInterfaces
Value: PerformRouterDiscovery
Value Type: REG_DWORD
Parameter: 0
Key: NetbtParameters
Value: NoNameReleaseOnDemand
Value Type: REG_DWORD
Parameter: 1
Under HKEY_LOCAL_MACHINE SYSTEM CurrentControlSet Control add or modify
the following value:
Key: Lsa
Value: RestrictAnonymous
Value Type: REG_DWORD
Parameter: 1

```

You may have noticed that I failed to have you fix the known flaws in the registry key permissions. Since we disabled the Remote Registry Service earlier it is not really necessary to do so.

Another neat trick is changing the file association for the .REG extension to something like NOTEPAD.EXE. This will prevent malicious web sites from adding registry keys without your knowledge. But since we're talking about servers here, the only site you are likely to visit from the console is a trusted one like <http://windowsupdate.microsoft.com> -- so I guess we don't really need to worry about that issue...

Revoke the Debug Programs User Right

By default, Windows 2000 grants administrators the Debug programs user right. This right can be exploited by trojans to capture sensitive system information from the system memory, such as hashed passwords. Microsoft suggests that you revoke this right for all users except specific user accounts that require debug privileges.

Console

Enable a screen saver, password protect it, and set it for some short interval like 5 minutes. This will protect you in the rare occurrence in which you forget to lock the computer before walking away from it.

Auditing

Next we will enable Auditing. This may be configured at the domain level, so you may not need to configure this for every server. I typically configure the Auditing settings as shown:

Audit Account Logon Events Success and Failure

Audit Account Management Success and Failure

Audit Directory Access No Auditing

Audit Logon Events Success and Failure

Audit Object Access Success

Audit Policy Change Success and Failure

Audit Privilege Use Success and Failure

Audit Process Tracking No Auditing

Audit System Events Success and Failure

Now we need to change the log settings so they have the potential to serve some purpose. Keeping the settings at their defaults may cause the server to crash when a log gets full. Increase the maximum size of the Application, Security and System logs to at least 10,048 KB each. Configure them to overwrite events as needed.

Security Policy

The local security policy is configured rather well in a default installation, but I usually change the following settings: Clear virtual memory pagefile when system shuts down Enabled Digitally sign server communication (when possible) Enabled Shut down system immediately if unable to log security audits Enabled

Telnet

Now we have to worry about telnet to Windows boxes. Create a group named "TelnetClients". Leave it empty if you are not using the service. If you are using the service, add your users to this group.

Trojans

This step is most helpful on workstations, but you will learn to like it on your servers as well.

Many, if not most of the trojans currently circulating take advantage of the Windows feature of hiding the extensions of known file types. This is what makes the executable script CLICKONME.BMP.VBS appear to be the bitmap file CLICKONME.BMP. This behavior makes it simple to trick people into executing files they believe are benign. To fix the problem navigate to My Computer – Tools – Folder Options – View. Deselect "Hide file extensions for known file types". While you are here, you might want to deselect "Hide protected operating system files" as well. Being able to see the protected OS files doesn't benefit security much, but it will assist you in future troubleshooting. If you have no need for Visual Basic or other scripts on your server, you can protect yourself further by preventing the scripts from executing by default. Simply change the file associations for some or all of the following file extensions to NOTEPAD.EXE:

.JS

.JSE

.VBE

.VBS

.WSF

Service Packs

You know the drill. New vulnerabilities are found in computing products every day. Keep an eye out for applicable Service Packs and Hotfixes and apply them as soon as possible.

Install Antivirus Software and Updates

It is imperative to install antivirus software and keep up-to-date on the latest virus signatures on the server. Virus definitions and scan engines both need to be update as soon it's available. It prevents our servers from any malfunctioning due to virus, worms and Trojans.

Firewall

Finally I recommend to install a personal firewall, It should d be configured in such a way that all incoming and out going traffic from the host should be filtered, Meaning configure the firewall to alert you to give popup message when ever the remote systems is trying to establish a connection with the host. Mostly used Personal firewall are 1) Zone Alarm 2) Kerio firewall 3) Sygate Personal Firewall

Emergency Repair Disk (ERD)

Emergency Repair Disk contains files that contain settings and configuration information that can be used to return the operating system back to its condition when the ERD was created.

To create a Windows 2000 ERD disk:

- Start
- Run
- Enter ntbackup and click OK
- Click on Emergency Repair Disk button on the Welcome to the Windows 2000 Backup and Recovery Tools window

There are key times to update the emergency repair disk information:

- Any time a change is made to the system's registry or SAM database (account/permissions information)
- After any change to the physical disk volumes -- add, delete or change to volume sets, stripe sets, mirror sets, etc.
- Conversion of the boot partition from FAT to NTFS.
- Before and after applying a service pack.
- It hasn't been run for a long time or you just feel like doing it.

Useful Security Tools

1. Microsoft Baseline Security Analyzer V1.2

MBSA Version 1.2 includes a graphical and command line interface that can perform local or remote scans of Windows systems. MBSA runs on Windows 2000, Windows XP, and Windows Server 2003 systems and will scan for common system misconfigurations in the following products: Windows NT 4.0, Windows 2000, Windows XP, Windows Server 2003, Internet Information Server (IIS), SQL Server, Internet Explorer, and Office. MBSA 1.2 will also scan for missing security updates for the following products: Windows NT 4.0, Windows 2000, Windows XP, Windows Server 2003, IIS, SQL Server, IE, Exchange Server, Windows Media Player, Microsoft Data Access Components (MDAC), MSXML, Microsoft Virtual Machine, Commerce Server, Content Management Server, BizTalk Server, Host Integration Server, and Office application.

2. Nessus

The "Nessus" Project aims to provide to the Internet community a free, powerful, up-to-date and easy to use remote security scanner. A security scanner is software, which will audit remotely a

given network and determine whether bad guys (aka 'crackers') may break into it, or misuse it in some way.

Unlike many other security scanners, Nessus does not take anything for granted. That is, it will not consider that a given service is running on a fixed port - that is, if you run your web server on port 1234, Nessus will detect it and test its security. It will not make its security tests regarding the version number of the remote services, but will really attempt to exploit the vulnerability.

Nessus is very fast, reliable and has a modular architecture that allows you to fit it to your needs.

Protection against Sniffing Attacks

Among various types of attacks on an ethernet network, "sniffing attack" is one of the most difficult attacks to handle. System administrators are facing difficulties to detect and deal with this attack, since it does not interfere with the network traffic at all. Sniffers are programs that allow a host to capture any packets in an ethernet network, by putting the host's network interface card (nic) into the promiscuous mode. Many basic services, such as ftp, telnet and smtp, send passwords and data in clear text in the packets; sniffers can be used by hackers to capture passwords and confidential data.

- AntiSniff (<http://www.securitysoftwaretech.com/antisniff>)
- PromiScan (http://www.securityfriday.com/ToolDownload/PromiScan/promiscan_doc.html)
- PromiscDetect (<http://ntsecurity.nu/toolbox/promiscdetect>)

Security Checklist

The purpose of this document is to give instructions for configuring a baseline level of security on Windows 2000 server.

Step

- Verify that all disk partitions are formatted with NTFS
- Disable unnecessary services
- Disable or delete unnecessary accounts
- Make sure the Guest account is disabled
- Protect the Registry from Anonymous Access
- Restrict access to public Local Security Authority (LSA) information
- Set stronger password policies
- Configure the Administrator Account
- Set Account Lockout Policy
- Revoke the Debug programs user right
- Remove all unnecessary File shares
- Set appropriate ACLs on all necessary file shares
- Enable security Event Auditing
- Install Antivirus Software and updates
- Install Service Packs and patches
- Emergency Repair Disk

The following information serves as a checklist to help you make sure you've covered all necessary areas. It is important that you carefully review these suggestions and use them to derive your own corporate settings and policies.

Disclaimer

The information and opinions in document were prepared by DaAnZeR and he has no obligation to tell

you when opinions or information in this document changes. This document is based on public information / gathered information / best industry practices. Author makes every effort to use reliable, comprehensive information, but Author makes no representation or warranty, express or implied, as to the accuracy, completeness or fairness of the information and opinions contained in this document.