Quickshot: Securing Windows 2000

Technical Consulting Services
Unisys Corp.

Created October 30, 2002
Chris Mikolajewski

Version Control

Version	Date	Summary of Changes
0.9	10/30/02	Initial document created
0.9a	11/20/02	Updated permissions section
0.9b	11/21/02	Added registry information for screen saver configuration
0.9c	11/26/02	Added section on SUS, updated disabled services list, updated section on account lockout
0.9d	12/20/02	Revised “Purpose” and LM password hash section
1.0	1/16/03	Final version

Purpose

The purpose of this document is to provide a short and concise method for securely installing and configuring Windows 2000. The steps described in this document can be used to secure any version of Windows 2000 (Professional, Server, Advanced Server, and Datacenter), but is focused on hardening the “server” versions of Windows 2000 (i.e. Windows 2000 Server and higher). Both pre- and post-installation recommendations are offered. The steps are listed in order of importance; therefore the list should be followed and implemented in a top-down fashion.

This document does not contain any information on securing IIS, the web services included with Windows 2000. Due to the large number of security risks associated with IIS, a separate document was created that deals with securing IIS. It is called “QuickShot: Securing IIS 5.0.”

A Windows security template has also been created that can automatically apply many of the security settings detailed in this document. If an item in the checklist can be automated via the security template, it is noted.

Tighter security always comes at the expense of convenience. The most secure system would be a host that is not attached to a network and locked in a vault. The server would be impossible to compromise, but at the same time its utility as a legitimate business tool would be minimal. This is an example of the constant trade-off between security and convenience that must be continually evaluated when implementing any type of security or hardening.

The checklists in this document are provided to give administrators an idea on how to secure Windows 2000. Some hosts may require more hardening, while others will require less. Special attention should be placed on Internet facing hosts, as Windows systems serve as popular targets for hackers.

NOTE: This document is intended for advanced Windows administrators who have a full and complete understanding of the configuration changes recommended in this document. In some cases, applying the changes could cause certain systems and applications to stop functioning properly. Please understand the implications in making the changes before applying them, or test them in a non-production environment first.

Windows 2000 Pre-Installation Checklist

1. **Do a clean install of the operating system, not an upgrade.**
   A clean install of Windows 2000 applies a relatively secure level of default permissions the NTFS partitions and the registry. Upgrading from Windows NT 4.0 will import the insecure permissions from NT 4.0 and apply them to the Windows 2000 installation.

2. **Install Windows 2000 while disconnected from the network.**
   Until the required Service Packs and security hot-fixes are applied, Windows 2000 is not sufficiently safe from malicious attacks that could take place occur over the network. Install the operating system by booting from the Windows 2000 CD (preferably with the latest Service Pack integrated) while unplugged and make sure to install the necessary patches before connecting to the network.

3. **Install the operating system on an NTFS partition.**
   With Windows 2000, the NTFS file system is the only choice that offers file and directory access control and secure auditing for files and directories. FAT16 and FAT32 partitions both lack these features. As a general guideline, you should always try to create and use NTFS partitions unless there is a need (typically compatibility reasons) to create FAT partitions.

4. **Only install the Windows components that are needed.**
   The main reason Windows has so many security holes is by default all the options get installed and enabled. If you do not need an optional system component, do not install it. Some examples are IIS, Indexing Service, and the SNMP service.

5. **If possible, install the operating system and data files on different partitions.**
   This is a general guideline that can be helpful to follow. Install the operating system on the C:\ drive, and put the data files on the D:\ drive. This “segments” critical data files from the system and boot partition, and aids in backup/restore and setting file permissions.

Windows 2000 Post-Installation Checklist

1. **Apply the latest patches for Windows and stay current with newly released critical security updates.**
   Microsoft continually releases new critical security updates for vulnerabilities that are discovered in Windows 2000 and its components. Once downloaded and tested on non-production systems, these updates should be installed on all affected servers in an organization.

   Windows 2000 Service Pack 3 was released in August of 2002. Install Service Pack 3 on all Windows 2000 systems along with any critical security updates that have been issued since its release.

In some cases, their may be a technical reason not to install Service Pack 3 (i.e. an incompatibility with existing applications). If this is the case, install Service Pack 2 and ensure that the latest post-SP2 critical security updates are also applied.

Microsoft has released a software package called Software Update Services (SUS) that makes it easier to download and deploy critical updates, critical security updates, and security roll-ups for Windows 2000, XP, and .NET Server hosts. An administrator creates an update server within the organization that automatically downloads any new updates from Microsoft. Once the administrator approves the downloaded updates, they are pushed out to all the host machines configured with the SUS client software. The SUS software and documentation can be found at the following link:

http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp

Use the Microsoft Hot Fix Network Checker (HFNETCHK) to easily check what service packs and updates have been applied to a system. HFNETCHK is a free tool from Microsoft that can be used to check and see what patches and hot-fixes have been applied to servers. Use this tool to verify that all the servers have had the most recent critical security updates applied.

Subscribe to the Microsoft Security Notification Service. This is a free email notification service that Microsoft uses to send out security updates to subscribers. Whenever a new security bulletin is posted, an email will get sent to subscribers detailing the bulletin. The link to subscribe is listed below:

http://www.microsoft.com/technet/security/bulletin/notify.asp

2. **Install an anti-virus software package, and configure it to automatically update its virus definitions.**

3. **Disable any unneeded services or components.**
   By default Windows 2000 installs many services and options when doing a default install. While attempting to configure a secure system, try taking the “minimalist approach.” Install and enable only the services that are specifically needed on the server.

   Below is a list of services that can safely be disabled on most Windows systems. It should also work on domain controllers, but extra caution should be taken. Once again, an understanding of what the server will be used for should help determine what services are needed.

   - Automatic Updates
   - ClipBook
   - Fax Service
   - Indexing Service
   - Internet Connection Sharing
   - IPSEC Policy Agent
   - NetMeeting Remote Desktop Sharing
   - QoS RSVP
   - Remote Access Auto Connection Manager
   - Remote Registry Service
   - Telnet

If IIS is installed (which it is by default) and not needed, either remove it (Control Panel | Add/Remove Programs | Add/Remove Windows Components) or disable the following services:

- FTP Publishing Service
- IIS Admin Service
- Network News Transport Protocol (NNTP) Service
- Simple Mail Transport Protocol (SMTP) Service
- World Wide Web (WWW) Publishing Service

NOTE: This setting can be modified via the Local Security Policy, domain Group Policy, or with the security template.

Also, Windows 2000 (the Server version and above) creates a user account called **TsInternetUser** when it is installed. This user account is used when the Terminal Services Internet Connector License is activated on the server. This allows up to 200 anonymous (Internet) connections to the Terminal Service server. The **TsInternetUser** account is granted the "Access this computer from the network" and the "Log on locally" user rights. Even though the password is managed by Window 2000, it is still recommended that you disable or delete this user on systems where the Terminal Services Internet Connector License will not be utilized.

4. **Secure any unprotected Windows networking shares.**
Windows allows host systems to share folders and files to users across the network via Windows network shares. These shares utilize the SMB (Server Message Block) protocol, also known as the Common Internet File System (CIFS), and allow remote users to access and manipulate local files as if they were connected to the system locally.

   You can view a list of shares on a machine by opening the Computer Management MMC snap-in from the Administrative Tools folder. Expand Shared Folders and click Shares. This shows a complete listing of all network shares available on the machine, including the administrative shares.

   It is highly recommended that organizations disable file sharing on all Internet-facing systems. HTTP or FTP methods can be used for remote file management instead. File sharing can be disabled by viewing the Properties for each network connection and un-checking "File and Printer Sharing for Microsoft Networks." This will prevent remote machines from connecting to SMB/CIFS services on the machine and will close port 445 (TCP and UDP). Port 139 (TCP) will still be listening on the server, but will not return any information if queried.

   If file sharing needs to be enabled on a system, then the default permissions for the share should be secured. By default, when file shares are created the **Everyone** group is granted Full Control. Remove the **Everyone** group and replace it with a specific user group, or the **Authenticated Users** group.

5. **Restrict null session connections (anonymous logons).**
A null session connection allows an anonymous (or unauthenticated) user to connect to a Windows host over the network and retrieve sensitive information (user names and shares) from the server. This poses a security risk because it allows any user on the network to gain access to sensitive information on remote Windows hosts.

   The registry key that controls anonymous access on Windows 2000 systems is:

HKLM\System\CurrentControlSet\Control\LSA

Value: RestrictAnonymous
Value Type: REG_DWORD
Value Data: 0x0-0x2 (Default is 0x0)

Below is an explanation of each setting:

0x0: None. Rely on default permissions.
0x1: Do not allow enumeration of SAM accounts and names
0x2: No access without explicit anonymous permissions

The recommended setting is 0x1—this restricts the amount of information that will be passed to anonymous connections, but still allows servers such as domain controllers to function. 0x2 provides the most protection, but can cause problems because many legitimate applications use null sessions to connect to remote hosts. For example, down-level Windows NT clients will no longer be able to change their password once they expire if 0x2 is set on the domain controllers. Only set the value to 0x2 after extensive testing within the organization.

NOTE: This setting can be modified via the Local Security Policy, domain Group Policy, or with the security template.

6. **Disable LAN Manager (LM) password hashing support.**
Even though most environments have no need for them, Windows stores legacy LAN Manager (LM) password hashes in the local SAM database by default on Windows NT, 2000, and XP hosts. These password hashes use a weak encryption scheme and can be broken in a short period of time. No matter how good the password policy is for an organization, having the LM password hashing enabled makes every password easy to crack.

   In addition, many Windows hosts also end up using LAN Manager authentication since it is enabled on the clients and accepted by the servers. This means weak LM password hashes are sent across the network can be picked up by packet sniffers and cracked b programs such as @Stake LC4 (formerly known as L0pht).

   Follow these two steps to fully disable LM password hashes:

   1. **Disable LM authentication across the network.**

      Beyond LM authentication, Windows supports two other authentication types—NTLM and NTLMv2. Both are more secure then LM, with NTLMv2 being the most secure. The registry key that controls this setting is:

      HKLM\System\CurrentControlSet\Control\LSA

      Value: LMCompatibilityLevel
      Value Type: REG_DWORD
      Value Data: 0-5 (default is 0)

      Below is a description of each of the various settings:

0: Send LM response and NTLM response; never use NTLMv2 session security
1: Use NTLMv2 session security if negotiated
2: Send NTLM authenication only
3: Send NTLMv2 authentication only
4: DC refuses LM authentication
5: DC refuses LM and NTLM authenication (accepts only NTLMv2)

If all the clients and domain controllers are running Windows NT 4.0 SP4+, Windows 2000, Windows XP, or Windows .NET, then use the following configuration:

- Set all domain controllers to 5.
- Set all clients to 3.

If legacy systems still exist on the network (such as Windows 9x or Windows NT 4.0 Pre-SP4), then use the following configuration:

- Set all domain controllers to 4.
- Set all clients to 1.

2. **Prevent the LM password hashes from being stored.**

   Even though the password hashes are prevented from being sent across the network, they are still created and stored locally in the SAM database and Active Directory. Windows 2000 provides a registry key that will disable the LM password hashes from being stored. Browse to the following key:

   HKLM\System\CurrentControlSet\Control\LSA

   Create a new key called **NoLMHash** and reboot the server.

   Creating and setting this key will disable LM password hashes from being created when new users are created. Existing users will still maintain their hashes until they change their password. If this key is created on all of the Windows 2000 domain controllers, the LM hashes will no longer be stored in the Active Directory.

   Please make note, this registry setting was not fully tested until Windows 2000 Service Pack 2. Therefore systems running prior Service Pack levels should not implement this registry key.

NOTE: This setting can be modified via the Local Security Policy, domain Group Policy, or with the security template.

7. **Rename the local Administrator account.**
   Since the local Administrator account is present on every Windows system, it provides a well-known target for hackers. Windows will not allow you to delete the account, but you can rename it to something less conspicuous.

   Rename the local Administrator account to something that is not obvious. Do not use admin, root, or anything name indicative of the account's rights. Create a "dummy" account named Administrator and remove it from any groups. Under the Local Security Policy | User Rights Assignment, add the account to the "Deny access to this computer

from the network" and "Deny logon locally" policies. This prevents an attacker from logging in to the host with the Administrator account. Check the security event log for access attempts on the dummy account.

8. **Enforce a strong password policy.**
Passwords are required for virtually all interaction between users and the system they access. Using brute force attacks, hackers can discover weak passwords and access secured systems undetected. Therefore it is imperative that organizations enforce a strong password policy for all user accounts (domain and local).

   In Windows 2000, password settings are customized through the Local Security Policy | Account Policies | Password Policy. Listed below are the pertinent password policies and their recommended settings.

Policy	Setting
Enforce Password History	Enabled (recommended value is 5)
Maximum Password Age	Enabled (recommended value is 60)
Minimum Password Age	Enabled (recommended value is 5)
Passwords Must Meet Complexity Requirements	Enabled

   If "Passwords Must Meet Complexity Requirements" policy is enabled, the following requirements will be applied to new passwords:

   - Passwords must be at least six characters long.
   - Passwords may not contain your user name or any part of your full name.
   - Passwords must contain characters from at least three of the following four classes:
     - English upper case letters (A,B,C...Z)
     - English lower case letters (a,b,c...z)
     - Westernized Arabic numerals (0,1,2...9)
     - Non-alphanumeric characters (Punctuation marks and other symbols)

   NOTE: Password settings can also be modified through domain Group Policy.

9. **Enable system auditing.**
Auditing is used to track user activities and system-wide events. In Windows 2000, administrators implement an audit policy, which contain a list of events that are currently being audited. Windows 2000 writes these events to the Security Log, which can be accessed through the Event Viewer. Keeping a record of who has logged into a system is an important aspect in maintaining system integrity. By default, auditing is not enabled on Windows 2000 systems.

   At a minimum, the following events should be part of the audit policy. They are configured through the Local Security Policy | Local Policies | Audit Policy

Event	Audit these Attempts
Account Logon Events	Success, Failure
Account Management	Success, Failure

Logon Events	Success, Failure
Policy Change	Success, Failure
System Events	Success, Failure

NOTE: If you need to audit file or directory access, then the "Audit Object Access" policy also needs to be enabled. Then you need to browse to the file or directory and enable file auditing on the resource.

NOTE: System auditing can also be modified through domain Group Policy.

10. **Increase the size of the Event Viewer logs, and archive old log files.**
By default the Event Viewer log files have a maximum size of 512KB. They are also configured to overwrite events older then 7 days once the maximum log file size is reached. This means new events will not be added if no events are older then this period.

    The Event Viewer logs are the primary tools used in troubleshooting Windows hosts and checking for unauthorized access. The logs provide a point-in-time snapshot view of the system, and should be archived on mission-critical and important systems.

    Change the settings for each log file to the following:

    - Increase the maximum log file size from 512KB to 9984KB.
    - Change the log files to overwrite events as needed.

    Also, it is a good idea to archive the logs every quarter. Save them off to a central log file server, where they can be accessed at a later point in time if needed.

    NOTE: This setting can be modified with the security template.

11. **Tighten the default permissions on the hard drive partitions**
While the default NTFS permissions on the C:\ drive (or whatever the system and boot partition may be) are relatively secure, Windows 2000 still uses the **Everyone** token to set access to files and directories. This means anyone who can gain access to the system (whether authenticated or unauthenticated) over the network can view and execute files on the hard drive, depending on the directory selected. The document Win2k_NTFS_Perm.doc lists the default NTFS permissions for a clean install of Windows 2000

    Remove the **Everyone** ACE from the C:\ drive and add the following ACE's:

Type	Name	Permission	Apply To
Allow	Administrators	Full Control	This folder, subfolder, and files
Allow	System	Full Control	This folder, subfolder, and files
Allow	Users	Modify	This folder, subfolder, and files

12. **Configure basic local security settings.**

1. **Configure an account lockout policy.**

   The following settings can be found in Local Security Policy | Account Lockout Policy.

Policy	Setting
Account lockout duration	0 minutes (account is locked out until administrator unlocks it)
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	30 minutes

2. **Configure a password-protected screen saver with a timeout of 30 minutes.** Enable the "Logon" screen saver with a timeout of 30 minutes, and that is password-protected. This means that when a user logs on locally and 30 minutes of inactivity pass, the screen saver will activate and the user will have to type their password to access the system again. This security practice helps protect the host from people with physical access.

3. **Display a legal warning message when users log on locally.**
   Configuration Change:
   Local Security Policy | *Security Options* | *Do not display last user name in logon screen*
   Local Security Policy | *Security Options* | *Do not display last user name in logon screen*

   Windows 2000 can be configured to display a text box whenever a user logs on locally to the system. Typically, the organization's "acceptable use policy" with regards to information services is displayed in the text box.

4. **Disable the user's name who last logged in from appearing in the Log On dialog box.**
   Configuration Change:
   Local Security Policy | *Security Options* | *Do not display last user name in logon screen*

   Having the name of the last user pre-filled in the Log On dialog box gives potential attackers half of the information they need to log on to a host. Now they just need to find the password (either through a brute force crack or social engineering) and they will have access to the system.

5. **Set the server to clear the virtual memory pagefile when system shuts down.**
   Configuration Change:
   Local Security Policy | *Security Options* | *Clear the virtual memory pagefile when system shuts down*

   NOTE: This setting can increase the time it takes a server to shutdown.

NOTE: This setting can be modified via the Local Security Policy, domain Group Policy, or with the security template.

13. **Secure the TCP/IP stack against denial of service and network attacks.**
Windows 2000 includes a number of configuration settings that can increase the robustness of the TCP/IP stack. These settings should be enabled on all Internet-facing hosts, and may be implemented on internal hosts as well. The settings recommended in this document are relatively safe, and should not cause any serious side effects. Most of the settings also have more restrictive settings which can be enabled. These should be explored on Internet-facing hosts, but keep in mind that achieving greater security usually comes with a price (namely in ease of use).

    The TCP/IP settings are configured through the registry. The recommended settings are listed below. All the parameters should be created under the following key:

    HKLM\System\CurrentControlSet\Services\Tcpip\Parameters

    Value: SynAttackProtect
    Value Type: REG_DWORD
    Valid Range: 0-2
    Default Value: 0
    Recommended Value: 1

    Value: EnableDeadGWDetect
    Value Type: REG_DWORD
    Valid Range: 0-1
    Default Value: 1
    Recommended Value: 0

    Value: KeepAliveTime
    Value Type: REG_DWORD
    Valid Range: 1-0xFFFFFFFF
    Default Value: 7,200,000 (two hours)
    Recommended Value: 300,000 (5 minutes).

    NOTE: This setting can be modified via the domain Group Policy, or with the security template.

14. **Remove the OS/2 and POSIX subsystems.**
Windows 2000 still contains the code necessary to run legacy OS/2 and POSIX applications. This functionality is typically never needed by most organizations, and the legacy subsystems only provide another security hole for attacks. The OS/2 and POSIX subsystem should be disabled if not needed. The easiest way to prevent the OS/2 and POSIX subsystems from loading is by editing the registry entry that loads the subsystems.

    NOTE: You must use REGEDT32.EXE to make this change, as REGEDIT.EXE does not view or edit REG_MULTI_SZ value types correctly.

    Browse to the following registry key:

    HKLM\System\CurrentControlSet\Control\SessionManager\SubSystems

    Locate the “Optional” value.

    Value: Optional

Value Type: REG_MULTI_SZ
Default Value: Os2 Posix

Clear out the default value and leave it blank. This will prevent the OS/2 and POSIX subsystems from loading the next time Windows starts.

For more information, reference Microsoft Knowledge Base Article 320869.

NOTE: This setting can be modified via the domain Group Policy, or with the security template.

15. **Disable or remove Windows Scripting Host.**
The Windows Scripting Host (WSH) is a feature of Windows operating systems. It enables .vbs (VBScript) and .js (JavaScript) files to run in Windows 9x, NT 4.0, Windows 2000, and Windows XP. In the case of the VBS.LoveLetter.A and VBS.NewLove.A worms, it enabled the virus writer to automate actions that ran a direct script execution without end-user intervention.

    Because of its inherent security risks, WSH should be disabled on all Internet-facing hosts, and it should also be potentially disabled on internal hosts. Make note however, that while WSH can be used to write malicious code, many administrative tasks can also be automated using scripts. Organizations will have to determine whether the added security from disabling scripting, is worth the trade-off in the usability of the system.

    The easiest way to disable scripting support in Windows 2000 is through My Computer | Tools | Folder Options | File Types. Delete the following registered file extensions:

    - JS – JScript Script File
    - JSE – JScript Script File
    - VBE – VBScript Script File
    - VBS – VBScript Script File

16. **Configure an IPSec packet-filtering policy.**
Applying an IPSec policy to the web server allows you to specify what TCP/IP traffic the server will respond to. The goal is to restrict access to all ports except those needed for the server to perform its duties. Configuring an IPSec policy is not needed on every server in an organization, but it should be used on all Internet-facing servers, and potentially even on DMZ-based servers. Instructions for configuring an IPSec policy are not included in this document—refer to Microsoft Knowledge Base Article 313190 for more information.

References

"SANS/FBI Top 20 List – The Twenty Most Critical Internet Security Vulnerabilities (Updated);" version 2.6; October 1, 2002; http://www.sans.org.

Maximum Windows 2000 Security; Anonymous; Sams Publishing, 2002.

"Hardening Windows 2000;" Philip Cox; version 1.0; March 30, 2001.

"Security Configuration Tool Set White Paper;" Microsoft; http://www.microsoft.com.

"Windows 2000 Server Baseline Security Checklist;" Microsoft; http://www.microsoft.com.

“Guide to Securing Microsoft Windows 2000 File and Disk Resources;” Owen R. McGovern; National Security Agency; version 1.0; April 19, 2001.