

WHITE PAPER:
HARDENING WINDOWS 2000
SECOND EDITION, DECEMBER 2002

BY ANDREW PLATO

ANITIAN

3800 SW CEDAR HILLS BOULEVARD, SUITE 298 ♦ BEAVERTON, OR 97005
(503) 644-5656 OFFICE ♦ (503) 644-8574 FAX ♦ WWW.ANITIAN.COM

COPYRIGHT INFORMATION

Hardening Windows 2000, Second Edition

Copyright © 2002, Anitian Corporation and Andrew M. Plato

All Rights Reserved

The use and copying of this product is subject to a license agreement. Any other use is strictly prohibited. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system or translated into any language, in any form, by any means without the prior written consent of the Anitian Corporation. Information in this document is subject to change without notice and does not constitute any commitment on the part of Anitian Corporation.

This document is intended for informational purposes only. Readers are expected to carefully consider the ramifications of implementing some of the suggestions in this document. Anitian Corporation and the author are not liable in any manner for any loss, disruption in service, or fault that arises directly or indirectly from the information in this document. The reader accepts all information “AS IS” without any warranty expressed or implied.

Windows®, Windows NT®, Windows 2000®, Windows XP®, and Microsoft ® are all registered trademarks of Microsoft Corporation.

All products mentioned in this manual are the trademarks or registered trademarks of their respective owners.

Anitian Corporation
3800 SW Cedar Hills Boulevard, Suite 298
Beaverton, OR 97005
(503) 644-5656 Office
(503) 644-8574 Fax
www.anitian.com

1. EXECUTIVE SUMMARY

System hardening refers to the process of configuring a computer to be more resistant to various security vulnerabilities. This may involve disabling, removing, or obscuring various features or services to eliminate or reduce the chance of compromise.

System hardening is an inherently difficult process. As computer systems have become easier to use and more integrated, security vulnerabilities have become more pervasive. The default installation of most systems is terribly insecure. However, if you shut off all the vulnerable services in a computer, you render it virtually useless. Thus, the process of hardening a computer involves not merely turning off services or reconfiguring software, but carefully analyzing how individual systems are used and then crafting appropriate hardening policies for those systems.

This paper focuses on practical, real-world solutions for hardening Windows 2000 and Windows NT machines. The goal of this paper is to help information technology professionals establish a checklist of issues they need to address while hardening their computer systems.

1.1. Assumptions

Hardening systems is not something to be taken lightly. Improperly hardening a system could make the system totally unstable and may even require completely rebuilding the system from scratch. Therefore, this guide assumes you have the responsibility and authority to completely manage the systems you are hardening.

Furthermore, this guide is intended for experienced system administrators who are very well versed in managing Windows servers. If you are new to Windows systems, some of the issues and concepts in this white paper might seem foreign.

1.2. Windows NT 4.0 Hardening

This document focuses mostly on how to harden Windows 2000 machines. However, much of the information in this document applies to Windows NT systems as well.

Windows NT 4.0 does not have many of the features and capabilities of Windows 2000 systems. It also does not have nearly as many security features. It is therefore suggested that you upgrade your systems to Windows 2000.

If you chose to continue using Windows NT, much of the information in this document can still be valuable. However, you will have to interpret the information for NT machines.

One option you should consider is obtaining the Harden NT application available from Security Focus.com, <http://online.securityfocus.com/tools/1789>. This tool offers an easy-to-use interface for selecting among options for hardening an NT machine. The application requires you to have the AUDITPOL.EXE, NTRIGHTS.EXE, REGINI.EXE, and XCALCS.EXE programs, which are all available on the Windows NT Resource Kit.

ANITIAN

This application does not actually harden the system, but it creates a series of scripts that will perform the actions for you. This excellent application is one that should be in every security administrator's tool kit.

2. GETTING STARTED

The first step with any security hardening procedure is to consider the role of the machine. You need to ask some basic questions about what the system does or will be expected to do..

2.1. Computer Role

What is the role of this computer?

Computer Role	Description
Workstation	An installation of Windows 2000 Professional or Windows NT Workstation. Intended for general use such as office applications, e-mail, etc.
Stand-Alone Server	A Windows 2000/NT Server. Intended use is running a specific service. Not intended for file sharing or resource sharing. This server is not part of a Windows domain.
Domain Server	A Windows 2000/NT Server intended for use as a sharing platform for files or similar. This server is part of a Windows domain.
Domain Controller	A user authentication server running Active Directory (Windows 2000).
Internet Server	A server running an Internet-style service such as Internet Information Server.
E-Mail Server	A server running Microsoft Exchange 5.5 or 2000.

It is important to distinguish between these types of machines, because what you can do to a system to harden it greatly depends on what you expect that machine to do. For example, if you expect to use a server for file sharing, then there are numerous services that must be running for the system to function correctly.

2.2. Isolate, Modularize, Simplify

When it comes to servers, these three concepts are absolutely critical. One of the most common mistakes companies make is to deploy one or two gigantic servers that can do everything. In a secure environment, it is best to deploy many smaller systems that have a highly specialized role.

Exercise great care, however, when decentralizing the servers' roles. Isolate systems from areas of your network where they should not be. For example, domain controllers should be isolated from file servers. Never load Exchange on your DNS server. Isolate each function on its own machine.

Simplify each machine. Rather than try to manage racks and racks of disparate systems, standardize and simplify the systems across your entire domain. This is extremely beneficial if a hacker does manage to penetrate your network. If all your systems have essentially the exact same build and OS partition, it is much easier to spot anomalies or suspicious installations on a system because you can compare that system to other systems.

For example, if you have a typical network of 200 to 500 users, you will likely need three file servers, two DNS servers, one email server, one intranet server, three domain controllers, one backup server, and then as many Internet servers as necessary deployed to your DMZ.

The point is to modularize your network. Rather than deploy two mammoth servers that do everything, deploy 10 smaller servers that spread out the load. This also allows you to independently secure each system. For example, your DNS servers should not have ANY file sharing, nor should your domain controllers. File servers should never do any name resolution.

Lastly, if you have the resources, build a testing environment with one or two servers that are isolated from the network. Use these servers to examine new applications or test new security patches. One of the most common problems in many organizations is that changes and updates to systems are done in a haphazard manner just to “plug holes.” Often these changes can introduce more problems than they solve. For example, a recent Microsoft security patch caused Microsoft Exchange Servers to stop forwarding e-mail unless a registry edit was made to the global catalog server. If this was deployed to a production environment, it could cause downtime on the mail server.

2.3. Physical Security

Although this guide is devoted to hardening the computer operating system, it is important to note that all the hardening in the world will not stop somebody from walking up to the machine and hitting it with a sledge hammer.

With that in mind, it is important to physically secure the systems you are hardening. When possible, servers should always be placed in a room or cabinet that has some kind of access control such as a locked door. Furthermore, systems should be placed on a shelf, table, or rack of some type to ensure good airflow around the machine.

Some computer vendors sell locking mechanisms for the front panel of systems. Although this may seem like an inexpensive way to secure a system, many of these are easily defeated using paper clips or common office supplies. Rather than attempting to protect individual machines, focus on how you can cordon off all your critical systems in a secure location.

2.4. Backups

Another critical element to any server system is performing regular backups of the data on the system. After installing the system and applying the appropriate service packs, you should immediately backup the system to tape or file.

Windows 2000 systems include an easy to use backup program (NTBACKUP.EXE) that copies the entire system to a file. Use this to create a snapshot of your system before you begin hardening. Thus, if something goes wrong during the backup process, you can restore the system from this backup.

Windows NT includes a backup program as well, but it requires a tape drive. You may want to obtain a backup program that can write to a file.

After hardening your system, make sure to implement some kind of scheduled backup of the system. For more information about backups and how to schedule them, refer to the documentation included with Windows.

2.5. Passwords

In the security industry, nothing is more fundamental to security than passwords. However, if you strolled through the server rooms of some of the nation's largest firms, you would be amazed how many places use blank passwords, easily guessable passwords, or put plain text password lists into Excel spreadsheets.

Unfortunately, like most IT professionals, you probably have many passwords to remember. And remembering hundreds of strings of letters and numbers is difficult.

Passwords are an area where simple solutions work best.

- Create complex passwords that use a combination of letters, numbers, and punctuation. Use both uppercase and lowercase letters.
- When possible, do not use English words in your password. These can be cracked with simple dictionary cracks.
- If you need to store passwords in a file, place them into an encrypted file on a floppy disk. Keep the floppy disk under lock and key. Alternatively, you may want to write the passwords in a notebook. Keep the notebook locked up.
- Do not store passwords on network drives, even in an encrypted file.
- Change passwords often.

3. INSTALLATION

Ideally, you should be installing a brand new server. However, the rules in this guide apply to existing systems as well. If you are working with an existing system, you can skip this section.

3.1. Dual Boot Systems

Hardening dual-boot systems is considerably more difficult than single-boot systems. Moreover, dual boot systems usually require using a simpler disk format, such as FAT, which does not have the security capabilities of NTFS.

Therefore, do not set up dual boot systems if you want to maximize security.

3.2. Disk Partitioning

The initial installation of Windows is fairly self-explanatory. If you're familiar with Windows systems, you will have undoubtedly gone through the Windows installation experience many times.

The first issue of importance is how to partition the system drives. The trick to partitioning drives in a secure environment is to divide up your drive space based on what applications and services you plan to run. Since each partition can be secured differently, it is always a good idea to isolate critical services, such as Active Directory on their own partitions. This not only makes for a more secure system, it also can speed up performance, especially if more than one drive is used.

3.2.1. Drive Partitioning Suggestions

Use the following check list to help you decide how to partition your drives.

- ✓ Always partition drives using NTFS. NTFS allows object-level security on the drive, which is very significant.
- ✓ Install the Windows operating system on a single, primary, 4GB partition (C:\ drive). Do not install any applications to this partition.
- ✓ For Windows 2000 Domain Controllers, create a special “Active Directory” partition of 4GB. When you promote the system to a domain controller, you will be prompted for a location to save the Active Directory files. Save them to this partition.
- ✓ For Internet Servers, create a special “InetPub” partition. Make sure to make the partition large enough to support whatever Internet applications or sites you will place there. You might even want to create multiple partitions to accommodate FTP, NNTP, and WWW traffic. If the server will be handling a lot of traffic, you may want to use a special RAID set that operates independently of the main drives.
- ✓ For E-Mail servers, create a special “Information Store” partition. Make sure to create a partition that is large enough to support your information store. For an extremely large organization, you may want to use a special RAID set that operates independently of the main drives.
- ✓ Finally, create a “Data” partition to handle all installed applications, such as Microsoft Office.

3.2.2. RAID or Not?

Whether you RAID drives or not really depends on the level of performance and integrity you want. From a security perspective, there is nothing fundamentally different between a RAID set and a non-RAID drive. Most security issues concerning drive contents are handled through the operating system.

However, as mentioned in the previous section, there is some value to placing critical services on different partitions. This allows for easier application of security policies. Moreover, if you are building a web server or e-mail server that will be heavily used, there are definite performance advantages to creating RAID sets where you can lay down these special partitions.

3.2.3. Use Disk Manager

When you first install Windows, it is easiest to create your base operating system partition. Once the system is up and running, use the Disk Manager utility in Windows to create and change each disk. You can also use disk manager to create spanned and mirrored sets. If you have a data partition that is especially critical, you may want to create a mirrored drives for extra safety. See the Disk Manager utility documentation for more information on how to create mirrored drives.

3.3. Windows Installation Options

The next phase in installation is selecting which options you want to install. Use the following table to determine if you need the following service.

Service / Option	Description	Security Risks
Accessories and Utilities	A collection of common Windows programs.	Most of these applications are relatively innocuous. Avoid installing the phone dialer or other communication items.
Certificate Services	Provides secure certificate issuing for e-mail, IPSec, and smart-card authentication.	Install if necessary for your environment. Otherwise, do not install.
Indexing Service	Software that provides search functions for documents stored on disk, allowing users to search for specific document text or properties.	Only useful on general file servers. Do not install unless you're setting up a file server.
IIS - Internet Information Server	A collection of Internet services such as a web server, news server, SMTP server, and many other web related services	Remove this from all servers except Internet servers or Microsoft Exchange servers. Do not run IIS on ANY server that does not absolutely require it. IIS has many vulnerabilities.
Management and Monitoring tools	A collection of convenience tools.	Don't install any of these, especially SNMP. The network monitor can be useful for sniffing packets.
DHCP- Dynamic Host Configuration Protocol	This service automatically assigns network settings to machines.	DHCP servers can offer a great deal of information about your network. A network really only needs one or two DHCP servers. Do not install this service unless you do not already have a DHCP server on your network.
DNS - Domain Name Server	The primary address resolution for the Internet and Windows 2000/XP-based networks.	DNS servers are critical points on your network that are tempting targets for hackers. Ideally, DNS servers should not have any other services running on them. If you are installing a Microsoft Exchange 2000 server, you should install DNS on the machine.
WINS – Windows Internet Naming Service	An obsolete name-resolution service for Windows NT and 9x network.	Unless you have Windows NT and 9x clients using WINS resolution, do not install WINS. Like DNS it can present a tempting target to a hacker.
Remote Installation Services	This service allows for the centralized deployment of Windows 2000 professional.	This exposes some vulnerabilities on the machine. Don't install this service unless absolutely necessary.

Service / Option	Description	Security Risks
IAS - Internet Authentication Service	Supports authentication for dial-in users	This poses many security risks, since dial-in and VPN connections are tempting targets to hackers. Unless you are specifically deploying a system to authenticate remote users, do not install this feature.
Simple TCP/IP Services	A collection of low-level TCP services.	Do not install.
Site Server ILS	Supports IP telephony applications.	IP telephony does not seem to have many vulnerabilities, probably because it is not a widely used technology. Unless you use telephony applications such as Netmeeting, on your network, do not install this component.
Remote Storage	Allows for rotation of data to removable media.	Do not install.
Terminal Services	Allows remote access to machine allowing users to run virtual sessions on their local machine.	This a great tool for remotely administering server systems. However it is also a tempting target for hackers. Unless absolutely necessary, don't install.
Script Debugging	Allows detailed debugging of scripts for development.	Do not install.

In general, if you are not sure you need a service...do not install it. You can always add these items later via the Add Software options on the Control Panel.

3.4. Network Installation Options

The next step is to setup your network connection. Presumably your computer has a network interface card already installed.

The key here is file sharing. In a Windows environment, file sharing and NetBIOS traffic comprise one of the greatest vulnerabilities to the system. Unfortunately, most systems and services rely on NetBIOS to exchange information. Therefore, you are probably going to be stuck leaving the Client for Microsoft Networks and Windows File and Printer Sharing enabled.

Guidelines

- ✓ Windows domain controllers and e-mail servers should have fixed IP addresses.
- ✓ Avoid installing protocols you do not need. A purely Windows environment can work fine with TCP/IP.
- ✓ When it comes time to configure the actual network address, make sure you enter the IP address correctly. Click **Advanced** for the configuration and make the following changes.
 - On the DNS tab, make sure to enter all the proper DNS servers. Ideally, your systems should resolve only to internal DNS servers. Also if your DNS servers

support it, check the “Register this connection’s address in DNS” this will automatically add an entry on your DNS server to point to your machine. This is especially important for Windows 2000 networks where DNS is the primary transport.

- On the WINS tab, uncheck the Enable LMHOST lookup. This is a vulnerability.
- If you do not plan on doing any file sharing, you can select the Disable NetBIOS over TCP/IP.

4. SERVICE PACKS

Once the system is installed and running, the next step is to place all the latest security patches and service packs. This is easily accomplished using Microsoft's Windows Update feature.

To start Windows Update, select **Windows Update** from the **Start** menu or type <http://www.windowsupdate.com> into the **Address** field of Internet Explorer.

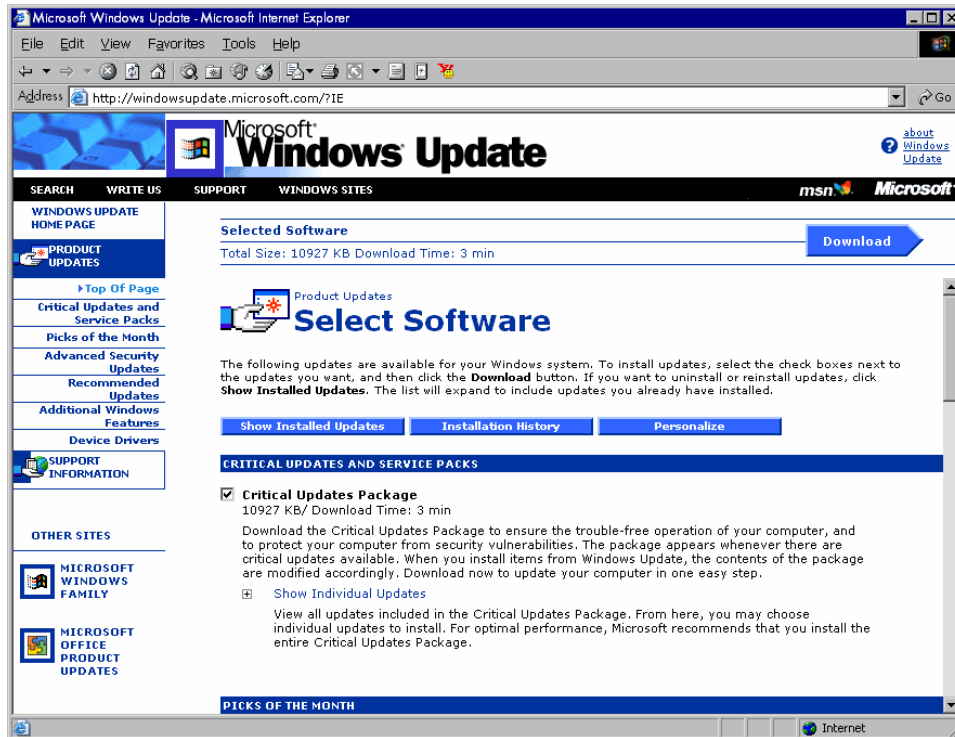


Figure 1 – Windows Update.

When Using Windows Update follow these general guidelines.

- ✓ Install the latest service packs first. Then install the security hot fixes.
- ✓ Do not install the media player, Direct X, or any of the other unnecessary convenience features on server systems.
- ✓ If you have a large network, you may want to centralize the deployment of hot fixes. You can use the Qchain.exe program to create batches of hotfixes and then roll them out. See the Windows documentation for more information about centrally deploying hotfixes.
- ✓ You will likely have to perform multiple reboots to install all the changes.

5. SERVICES

The next step is to start turning off services. Windows comes “out of the box” with a lot of unnecessary services turned on. These services expose the system to more vulnerabilities. The problem is, if you shut off too many services, the machine will become unstable.

This section provides a general guidelines for which services you should leave on and which you can shut off

1. To access the services on Windows 2000 machines, right-click on the My Computer icon.
2. Select **Manage**. The Computer Management window displays.
3. Use the tree on the left and locate **Services** under **Services and Applications**.

5.1. Services in Windows 2000 Professional (Workstation)

Name	Description	Required?
Alerter	Notifies selected users and computers of administrative alerts.	No, disable this service.
Application Management	Provides software installation services such as Assign.	Yes
Automatic Updates	Enables the download and installation of critical Windows updates. If the service is disabled, the operating system can be manually updated at the Windows Update Web site. This service was added in Windows 2000 Service Pack 3.	This is a controversial service. On one hand, keeping your systems automatically updated is a good way to stop a lot of common attacks. But on the other hand, this does introduce a sort of “back door” into the system since it is automatically downloading executable code. If you want maximum security for your systems, don’t enable this service. Update your systems manually, just make sure to do it regularly. If you are willing to take a little risk, this is a very useful service and may be worth enabling.
Background Intelligent Transfer Service	Transfers files in the background using idle network bandwidth. If the service is disabled, then any functions that depend on BITS, such as Windows Update or MSN Explorer will be unable to automatically download programs and other information.	This is part of the Windows Update feature set. Enable this only if you are using the Automatic Updates. Otherwise, disable this service.
ClipBook	Supports ClipBook Viewer.	No, disable this service

Name	Description	Required?
COM+ Event System	Provides automatic distribution of events to subscribing COM components.	Yes.
Computer Browser	Maintains an up-to-date list of computers on your network and supplies the list to programs that request it.	Enable only if network neighborhood features are used. Disable otherwise.
DHCP Client	Manages network configuration by registering and updating IP addresses and DNS names.	Yes if you use DHCP. No if your IP addresses are fixed.
Distributed Link Tracking Client	Sends notifications of files moving between NTFS volumes in a network domain.	Yes, if you plan to do any file sharing.
Distributed Transaction Coordinator	Coordinates transactions that are distributed across two or more databases.	This service is really intended for systems with SQL Server that must coordinate transactions between more than one machine. This is rarely necessary and therefore should be disabled.
DNS Client	Resolves and caches Domain Name System (DNS) names.	Yes, this is required for Internet browsing.
Event Log	Logs event messages issued by programs and Windows. Event Log reports contain information that can be useful in diagnosing problems. Reports are viewed in Event Viewer.	Yes
Fax Service	Helps you send and receive faxes	No
File Replication Service	Maintains file synchronization of file directory contents among multiple servers.	Only necessary for file servers or domain controllers.
Indexing Service	Indexes files on local drives.	No
Internet Connection Sharing	Provides network address translation	No. This should NEVER be used, it is a very insecure technology.
IPSEC Policy Agent	Manages IP security policy and starts the ISAKMP/Oakley (IKE) and the IP security driver.	Yes, if you will be using IPSEC on your network. Otherwise, no.
Logical Disk Manager	Logical Disk Manager Watchdog Service	Yes
Logical Disk Manager Administrative Service	Administrative service for disk management requests	Yes
Messenger	Sends and receives messages transmitted by administrators or by the Alerter service.	No

Name	Description	Required?
Net Logon	Supports pass-through authentication of account logon events for computers in a domain.	This is required on domain controllers or any server that must authenticate users. For file servers or other special use systems, this is not required and can be disabled.
NetMeeting Remote Desktop Sharing	Allows authorized people to remotely access your Windows desktop using NetMeeting.	No, this is a very insecure technology.
Network Connections	Manages objects in the Network and Dial-Up Connections folder	Yes
Network DDE	Provides network transport and security for dynamic data exchange (DDE).	No
Network DDE DSDM	Manages shared dynamic data exchange and is used by Network DDE	No
NT LM Security Support Provider	Provides security to remote procedure call (RPC) programs that use transports other than named pipes.	Yes
Performance Logs and Alerts	Configures performance logs and alerts.	Yes
Plug and Play	Manages device installation and configuration and notifies programs of device changes.	Once the system is setup and running, this can be disabled. However, it will prevent the system from detecting any new hardware.
Print Spooler	Loads files to memory for later printing.	Yes if you plan to do any printing. Otherwise, no.
Protected Storage	Provides protected storage for sensitive data	Yes
QoS RSVP	Provides network signaling and local traffic control setup functionality for QoS-aware programs and control applets.	No, but this is a useful utility.
Remote Access Auto Connection Manager	Creates a connection to a remote network whenever a program references a remote DNS or NetBIOS name or address.	Yes, for file sharing.
Remote Access Connection Manager	Creates a network connection.	Yes, for file sharing.
Remote Procedure Call (RPC)	Provides the endpoint mapper and other miscellaneous RPC services.	Yes, for file sharing. Otherwise, no.
Remote Procedure Call (RPC) Locator	Manages the RPC name service database.	Yes for file sharing.

Name	Description	Required?
Remote Registry Service	Allows remote registry manipulation.	This is required on domain controllers and Exchange servers. Otherwise, disable this service always.
Removable Storage	Manages removable media	No
Routing and Remote Access	Offers routing services to businesses in local area and wide area network environments.	No.
RunAs Service	Enables starting processes under alternate credentials	Yes
Security Accounts Manager	Stores security information for local user accounts.	Yes
Server	Provides RPC support and file	If the system will host any shared folders than this must be enabled. If you disable this service, you will not be able to access the default administrative shares (c\$, d\$, etc.) on the system. This may cause some management and administration software to stop working.
Smart Card	Manages and controls access to a smart card inserted into a smart card reader attached to the computer.	If you use smart cards, yes. If not, no.
Smart Card Helper	Provides support for legacy smart card readers attached to the computer.	If you use smart cards, yes. If not, no.
System Event Notification	Tracks system events such as Windows logon	Yes
Task Scheduler	Enables a program to run at a designated time.	This is a useful service for scheduling backups and other maintenance functions. However it can also be used by hackers to schedule the system to do bad things. If you need this service, use it, but keep an eye on the jobs and make sure nothing strange pops up here.
TCP/IP NetBIOS Helper Service	Enables support for NetBIOS over TCP/IP (NetBT) service and NetBIOS name resolution.	Yes, for file sharing.
Telephony	Provides Telephony API (TAPI) support for programs that control telephony devices and IP based voice connections on the local computer and	No, but a lot of things depend on this horrible service, so you'll probably be stuck leaving it enabled.

Name	Description	Required?
Uninterruptible Power Supply	Manages an uninterruptible power supply (UPS) connected to the computer.	No, unless you're using a UPS.
Utility Manager	Starts and configures accessibility tools from one window	No
Windows Installer	Installs Windows components.	No
Windows Management Instrumentation	Provides system management information.	Yes
Windows Management Instrumentation Driver Extensions	Provides systems management information to and from drivers.	Yes
Windows Time	Sets the computer clock.	Yes
Workstation	Provides network connections and communications.	Yes, for file sharing.

5.2. Services in Windows 2000 Server

Name	Description	Required
Alerter	Notifies selected users and computers of administrative alerts.	No
Automatic Updates	Enables the download and installation of critical Windows updates. If the service is disabled, the operating system can be manually updated at the Windows Update Web site. This service was added in Windows 2000 Service Pack 3.	This is a controversial service. On one hand, keeping your systems automatically updated is a good way to stop a lot of common attacks. But on the other hand, this does introduce a sort of "back door" into the system since it is automatically downloading executable code. If you want maximum security for your systems, don't enable this service. Update your systems manually, just make sure to do it regularly. If you are willing to take a little risk, this is a very useful service and may be worth enabling.
Background Intelligent Transfer Service	Transfers files in the background using idle network bandwidth. If the service is disabled, then any functions that depend on BITS, such as Windows Update or MSN Explorer will be unable to automatically download programs and other information.	This is part of the Windows Update feature set. Enable this only if you are using the Automatic Updates. Otherwise, disable this service.
Application Management	Provides software installation services such as Assign	Yes

Name	Description	Required
Certificate Services	Issues and revokes X.509 certificates for public key-based cryptography technologies.	If the system will be a CA, then yes. Otherwise, this can be disabled.
ClipBook	Supports ClipBook Viewer	No
COM+ Event System	Provides automatic distribution of events to subscribing COM components.	Yes
Computer Browser	Maintains an up-to-date list of computers on your network and supplies the list to programs that request it.	No
DHCP Client	Manages network configuration by registering and updating IP addresses and DNS names.	Yes, if the network interfaces use DHCP. If the addresses are fixed, then no.
DHCP Server	Provides dynamic IP address assignment and network configuration for Dynamic Host Configuration Protocol (DHCP) clients.	Yes, if the system will be a DHCP server. Otherwise, this should be disabled.
Distributed File System	Manages logical volumes distributed across a local or wide area network.	Yes, if the system is a domain controller. Otherwise, no.
Distributed Link Tracking Client	Sends notifications of files moving between NTFS volumes in a network domain.	Yes, if the system is a domain controller, otherwise no.
Distributed Link Tracking Server	Stores information so that files moved between volumes can be tracked for each volume in the domain.	Yes, if the system is a domain controller. Otherwise, no.
Distributed Transaction Coordinator	Coordinates transactions that are distributed across two or more databases	No, unless the system is running SQL Server or some other database that must use this feature.
DNS Client	Resolves and caches Domain Name System (DNS) names.	Yes.
DNS Server	Answers query and update requests for Domain Name System (DNS) names.	If the server will be a DNS server. Otherwise, disable this service.
Event Log	Logs event messages issued by programs and Windows. Event Log reports contain information that can be useful in diagnosing problems. Reports are viewed in Event Viewer.	Yes.
Fax Service	Helps you send and receive faxes	No
File Replication	Maintains file synchronization of file directory contents among multiple servers.	Yes, if the system is a domain controller. Otherwise, no.

Name	Description	Required
Indexing Service	Indexes contents and properties of files on local and remote computers; provides rapid access to files through flexible querying language.	No
Internet Connection Sharing	Provides network address translation	No.
Intersite Messaging	Allows sending and receiving messages between Windows Advanced Server sites.	No
IPSEC Policy Agent	Manages IP security policy and starts the ISAKMP/Oakley (IKE) and the IP security driver.	No, unless you are using IPSEC to secure network traffic.
Kerberos Key Distribution Center	Generates session keys and grants service tickets for mutual client/server authentication.	No, except on domain controllers which require this service.
License Logging Service	Manages licensing information for Windows systems.	No
Logical Disk Manager	Logical Disk Manager Watchdog Service	Yes
Logical Disk Manager Administrative Service	Administrative service for disk management requests	Yes
Messenger	Sends and receives messages transmitted by administrators or by the Alerter service.	No
Net Logon	Supports pass-through authentication of account logon events for computers in a domain.	Yes, if the system is a domain controller. Otherwise no. Make sure to turn this off on any Internet exposed system.
NetMeeting Remote Desktop Sharing	Allows authorized people to remotely access your Windows desktop using NetMeeting.	No
Network Connections	Manages objects in the Network and Dial-Up Connections folder	Yes
Network DDE	Provides network transport and security for dynamic data exchange (DDE).	No
Network DDE DSDM	Manages shared dynamic data exchange and is used by Network DDE	No
NT LM Security Support Provider	Provides security to remote procedure call (RPC) programs that use transports other than named pipes.	Yes
Performance Logs and Alerts	Configures performance logs and alerts.	Yes

Name	Description	Required
Plug and Play	Manages device installation and configuration and notifies programs of device changes.	Once the system is installed and stable, you might want to disable this service. However, the system will no be able to detect any new hardware you add.
Print Spooler	Loads files to memory for later printing.	Only enable when you need to print from the service.
Protected Storage	Provides protected storage for sensitive data	Yes
QoS RSVP	Provides network signaling and local traffic control setup functionality for QoS-aware programs and control applets.	No, but this is a useful service to have.
Remote Access Auto Connection Manager	Creates a connection to a remote network whenever a program references a remote DNS or NetBIOS name or address.	No
Remote Access Connection Manager	Creates a network connection.	No
Remote Procedure Call (RPC)	Provides the endpoint mapper and other miscellaneous RPC services.	For domain controllers, file servers, and Exchange servers, yes. For all internet exposed servers this should be disabled.
Remote Procedure Call (RPC) Locator	Manages the RPC name service database.	For domain controllers, file servers, and Exchange servers, yes. For all internet exposed servers this should be disabled.
Remote Registry Service	Allows remote registry manipulation.	This must be enabled on Exchange and domain controllers. All other servers should disable this service.
Removable Storage	Manages removable media	Yes.
Routing and Remote Access	Offers routing services to businesses in local area and wide area network environments.	No
RunAs Service	Enables starting processes under alternate credentials	Yes
Security Accounts Manager	Stores security information for local user accounts.	Yes
Server	Provides RPC support and file	For domain controllers, file servers, and Exchange servers, yes. For all internet exposed servers this should be disabled. This will effectively remove the Administration shares, which may cause some software that is dependent upon those shares to stop working.

Name	Description	Required
Smart Card	Manages and controls access to a smart card inserted into a smart card reader attached to the computer.	Enable only if you are using Smart Cards.
Smart Card Helper	Provides support for legacy smart card readers attached to the computer.	Enable only if you are using Smart Cards.
System Event Notification	Tracks system events such as Windows logon	Yes.
Task Scheduler	Enables a program to run at a designated time.	Disable for all Internet exposed systems.
TCP/IP NetBIOS Helper Service	Enables support for NetBIOS over TCP/IP (NetBT) service and NetBIOS name resolution.	Disable on all Internet exposed servers.
Telephony	Provides Telephony API (TAPI) support for programs that control telephony devices and IP based voice connections on the local computer and	Disable on all Internet exposed servers.
Telnet	Allows a remote user to log on to the system and run console programs using the command line.	Never enable.
Terminal Services	Provides a multisession environment that allows client devices to access a virtual Windows 2000 Professional desktop session and Windows-based programs running on the server.	Never enable this for an Internet exposed server. For internal servers, this can be a useful way to remotely manage systems. Terminal service communications are encrypted.
Trivial FTP Daemon	Implements the Trivial FTP Internet standard	No. This is a very serious vulnerability.
Uninterruptible Power Supply	Manages an uninterruptible power supply (UPS) connected to the computer.	Yes, if you're using a UPS.
Utility Manager	Starts and configures accessibility tools from one window	Yes
Windows Installer	Installs Windows components.	No
Windows Management Instrumentation	Provides system management information.	Yes
Windows Management Instrumentation Driver Extensions	Provides systems management information to and from drivers.	Yes
Windows Time	Sets the computer clock.	Yes
Workstation	Provides network connections and communications.	No. Unless you plan to use file sharing to access other systems.

6. GROUP POLICIES

Group Policies provide a consistent mechanism to manage and control a wide array of configuration and security issues for Windows 2000 systems. With Group Policies you can establish rules for registry access, security settings, software usage, user rights, logon scripts, and many other system features. Group Policies were a major improvement over Windows NT profiles and are reason alone to upgrade from Windows NT to 2000.

Group Policies are extremely flexible and powerful, which is good for security-minded organizations. However, Group Policies are not something to take lightly. Improperly configured policies or failure to assess the ramifications of a policy in your environment could lead to serious performance degradation and even system crashes.

6.1. Policy Planning

Before you start making security policy changes, you really need to do some planning to figure out what you want to implement. Policies are very powerful and flexible, but you can also cause serious usability problems if you implement an overly restrictive policy.

Therefore, the first step is to learn about Windows 2000 policies. There are a number of outstanding books on the topic. Microsoft also offers an excellent paper that explains how to manage and use policies. This paper is available at:

<http://www.microsoft.com/windows2000/docs/grouppolwp.doc>

6.2. Group Policy MMC Plug-In

You need to become familiar with the Security Policy MMC snap-in. This component lists the various tools you have to secure various aspects of the system.

To view the Local Security Policy, select **Administrative Tools > Local Security Policy** from the Start menu (for local Policies, on domain controllers there is also an item for Domain Controller Policy).

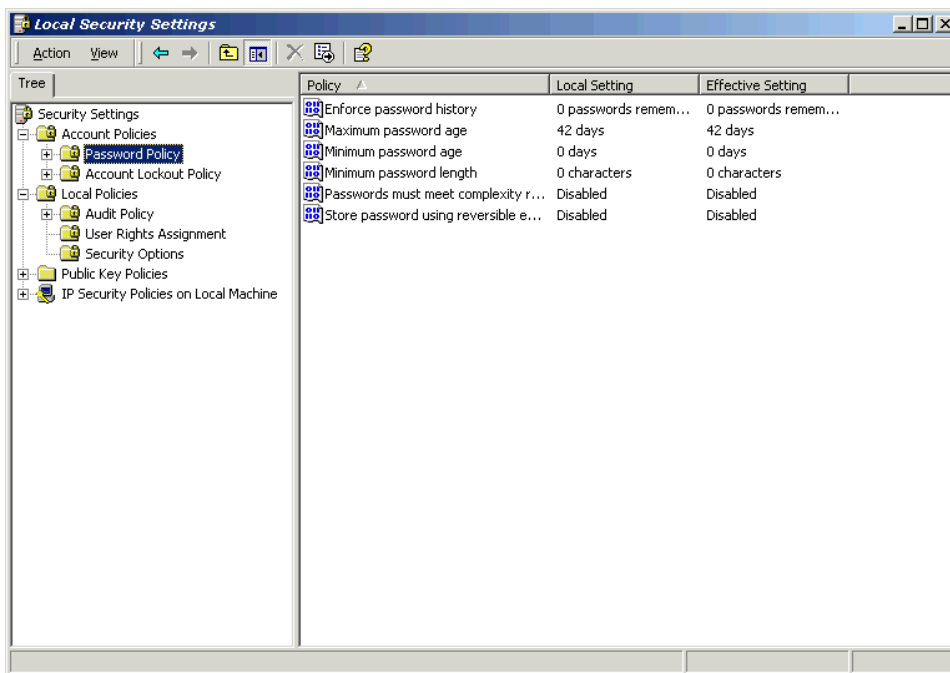


Figure 2 – Local Security Policy window.

To access policies within the Active Directory, right click on an organizational unit in the Active Directory Users and Computers snap-in.

6.3. Policy Hierarchy

It is important to consider how Windows 2000 systems implement policies. On a Windows 2000 domain running Active Directory, you can manage a central security policy that is applied to a whole group of systems. This is an excellent way to lock down systems as a group, rather than individually editing the security policies for each machine. You can also create domain-wide policies and domain-controller policies. Thus the hierarchy looks something like this

- Organizational Unit
 - Domain
 - Group
 - Local

When a system boots, it implements policies in a “bottom-up” fashion. Local policies are implemented first, then group, then domain, and finally organizational unit.

Parent policy elements can overwrite any child policy element, but the policies as a whole are cumulative. For example, if a local policy establishes a particular setting, that setting will remain in effect unless a parent policy specifically overwrites or disables it.

6.4. Policy Suggestions

When you are ready to implement policies on your domain or local machine, use this section to help guide you in choosing the security settings you wish to implement. This paper focuses exclusively on the Security Settings portion of Group Policies

6.4.1. Account Policies: Password Policy

This policy sets how the system or domain handles passwords. Users must be forced to use complex passwords, otherwise password cracking programs such as L0pht Crack will make it extremely easy for hackers to penetrate systems with stolen credentials.

Policy Element	Suggestion
Enforce Password History	Set to 10 – 20 passwords.
Maximum Password Age	45 days
Minimum password age	5 days
Minimum Password Length	7 characters
Passwords must meet complexity requirements	Enable
Store passwords using reversible encryption	Disabled

6.4.2. Account Policies: Account Lockout Policy

This policy determines when and for whom an account will be locked out of the system. These settings will cause the system to lock out users who attempt to logon to a system using incorrect credentials. This will effectively stop any brute force password grinding of the system itself.

Policy Element	Suggestion
Account Lockout duration	30 minutes
Account Lockout Threshold	5 invalid attempts
Reset account lockout counter after	60 minutes
Minimum Password Length	7 characters

6.4.3. Local Policies: User Rights Assignment

This is perhaps the trickiest policy to get right. You have to be very careful who gets what rights. If you remove too many rights, you could wind up with a machine that is unusable. In general, the Administrator or Domain Administrator should have rights to just about everything. Remove rights from as many groups as you possibly can and avoid assigning rights to specific users.

Policy Element	Suggestion
Access this computer from the network	For domain controllers, email servers, and other machines that must interact with your network, allow only the groups that comprise your internal users as well as all the Administrators. Do not allow "Everybody."
Act as part of the operating system	Administrator and SYSTEM only.
Add workstations to domain	Any group that must administer your domain.
Back up files and directories	Administrators and any users authorized to make backups.
Bypass traverse checking	All regular users
Change the system time	Regular users
Create a pagefile	Administrators only.
Create a token object	Blank
Create permanent shared objects	Blank
Debug programs	Administrators only.
Deny access to this computer from the network	This item, and the next three are excellent ways to harden your system from Internet-exposed accounts. For example, if you have a specific user for Internet applications on a web server, you may want to specifically deny that user from accessing internal machines, such as domain controller. Add any groups, such as groups with Internet users, that you want to specifically deny from accessing the system over the network.
Deny logon as a batch job	Add any groups, such as groups with Internet users, that you specifically want to deny from running batch jobs on the system.
Deny logon as a service	Add any groups, such as groups with Internet users, that you specifically want to deny from starting any services.
Deny logon locally	Add any users or groups you want to prohibit from logging on interactively (to the actual machine).
Enable computer and user accounts to be trusted for delegation	Administrator only.
Force shutdown from a remote system	Administrators only.
Generate security audits	Administrators only.
Increase quotas	Administrators and anybody managing the computer.

Policy Element	Suggestion
Increase scheduling priority	Blank.
Load and unload device drivers	Administrators and other trusted users.
Lock pages in memory	Blank
Log on as a batch job	Administrators only.
Log on as a service	Administrators and any accounts you use to run services. For example, on a Microsoft Exchange server it is a good idea to create a special account specifically for executing Exchange services. In this case, you would need to add the account or group to this right.
Log on locally	Any group that is allowed to interactively logon to the machine. Ideally, this should be Administrators only.
Manage auditing and security log	Administrators only.
Modify firmware environment values	Administrators only.
Profile single process	Administrators only.
Profile system performance	Administrators only.
Remove computer from docking station	Administrators only.
Replace a process level token	Administrators only.
Restore files and directories	Administrators and any backup service accounts.
Shut down the system	Administrators only.
Synchronize directory service data	Administrators only. On a domain controller you may need to add the accounts of other systems.
Take ownership of files or other objects	Administrators only.
Access this computer from the network	All users and groups who are allowed to access the system from the network.
Act as part of the operating system	Administrators only.
Add workstations to domain	Administrators only.

6.4.4. Local Policies: Security Options

The security options includes a broad array of miscellaneous security features. Some are innocuous, others are very troublesome. Step lightly here and pay attention to the help text.

Policy Element	Suggestion
Additional restrictions for anonymous connections	Enable
Allow server operators to schedule tasks (domain controllers only)	Enable
Allow system to be shut down without having to log on	Enable
Allowed to eject removable NTFS media	Enable
Amount of idle time required before disconnecting session	15 minutes
Audit the access of global system objects	Enable (this will cause performance degradation on the system)
Audit use of Backup and Restore privilege	Enable
Automatically log off users when logon time expires (local)	Enable
Clear virtual memory pagefile when system shuts down	Enable. This will cause the machine to take a long time when shutting down, as the system must wipe out all the data in the page file.
Digitally sign client communication (always)	Enable if you plan to use IPSEC on your network. Otherwise, leave disabled.
Digitally sign client communication (when possible)	Enable if you plan to use IPSEC on your network. Otherwise, leave disabled.
Digitally sign server communication (always)	Enable if you plan to use IPSEC on your network. Otherwise, leave disabled.
Digitally sign server communication (when possible)	Enable if you plan to use IPSEC on your network. Otherwise, leave disabled.
Disable CTRL+ALT+DEL requirement for logon	Disable
Do not display last user name in logon screen	Enable
LAN Manager Authentication Level	If you have a purely Windows NT/2000/XP environment – use <i>Sent NTLMv2 Refuse NTLM and LM</i> . If you have older Windows 9x clients, you have to leave NTLM on. If you have any Windows 3.11 clients, you have to leave LM on.
Message text for users attempting to log on	Use this field to display a message to users when they logon. This is an excellent place to notify users that they are on a company system and that their actions are being monitored. You might want to work with your legal team to craft a notification.
Message title for users attempting to log on	This is the name of the window that displays the message text.

Policy Element	Suggestion
Number of previous logons to cache (in case domain controller is not available)	0 (zero)
Prevent system maintenance of computer account password	Enable
Prevent users from installing printer drivers	Probably only want to disable this on Internet exposed systems.
Prompt user to change password before expiration	Enable
Recovery Console: Allow automatic administrative logon	Disable
Recovery Console: Allow floppy copy and access to all drives and all folders	Enable
Rename administrator account	This is one of the single easiest, and least done security measures. No system should EVER use the default "Administrator" account. Rename the account to anything other than the default. You may want to do this domain-wide.
Rename guest account	As with the administrator account, it's a good idea to rename this account as well.
Restrict CD-ROM access to locally logged-on user only	Enable
Restrict floppy access to locally logged-on user only	Enable
Secure channel: Digitally encrypt or sign secure channel data (always)	This is tricky to implement. You have to make sure all the systems that will interface with this system are set up to use a PKI infrastructure. If you do not have such an infrastructure, leave this disabled.
Secure channel: Digitally encrypt secure channel data (when possible)	This is tricky to implement. You have to make sure all the systems that will interface with this system are set up to use a PKI infrastructure. If you do not have such an infrastructure, leave this disabled.
Secure channel: Digitally sign secure channel data (when possible)	This is tricky to implement. You have to make sure all the systems that will interface with this system are set up to use a PKI infrastructure. If you do not have such an infrastructure, leave this disabled.
Secure channel: Require strong (Windows 2000 or later) session key	This is tricky to implement. You have to make sure all the systems that will interface with this system are set up to use a PKI infrastructure. If you do not have such an infrastructure, leave this disabled.
Send unencrypted password to connect to third-party SMB servers	Disable
Shut down system immediately if unable to log security audits	This is a very drastic setting, but you might want to enable it for high-security systems.
Smart card removal behavior	Select the appropriate setting if you are using smart cards. Otherwise, leave this as "No Action."
Strengthen default permissions of global system objects (e.g. Symbolic Links)	Enable

Policy Element	Suggestion
Unsigned driver installation behavior	This setting controls how the system responds when a user attempts to install a driver. If you do not allow installation, users will not be able to install any software. Since this is not always an ideal situation, you may want to set this to Warn but allow. However, this will cause the system to display a lot of notification dialogs when installing any software, which could be very annoying. In general for domain controllers and other high-security systems, the best setting is to warn.
Unsigned non-driver installation behavior	This setting controls how the system responds when a user attempts to install software. If you do not allow installation, users will not be able to install any software. Since this is not always an ideal situation, you may want to set this to <i>Warn but allow</i> . However, this will cause the system to display a lot of notification dialogs when installing any software, which could be very annoying. In general for domain controllers and other high-security systems, the best setting is to warn.

7. USING IPSEC

One of the greatest problems with the TCP/IP protocol suite is that the raw IP traffic between hosts has virtually no security features built into the various protocols. Therefore, secure communications between hosts had to take place at higher levels, hence application level protocols such as Secure Sockets Layer (SSL).

IPSec (which stands for IP Security) was designed to introduce a security level at the IP level (sometimes called Layer 2). This security is transparent to both higher level protocols in applications and to the Ethernet frames. Furthermore, session layer protocols, such as TCP and UDP can also use IPsec.

Thus, the goal of IPSec is:

- Authentication of communications.
- Encrypted IP traffic.
- Protection from a wide variety of attacks that take advantage of IP weaknesses.

IPSec is an excellent way to deliver a very significant level of security to your network. Using IPSec your network will become significantly harder to hack.

However, implementing IPSec is very complicated. Implementing IPSec can be a painful and difficult process if it not planned carefully. Furthermore, IPSec is not always compatible with all network hardware. It also requires operating systems that are compatible with IPSec standards. Currently, only Windows 2000 and XP (of the Windows family) are compatible. Some versions of Linux and BSD have IPSec capabilities.

A comprehensive explanation of IPSec is really beyond the scope of this document. However, if you are serious about implementing IPSec, you should start by becoming familiar with the technology. There is an excellent series of articles on Security Focus regarding implementing IPSec in a Windows 2000/XP environment. The article is located at:

`http://online.securityfocus.com/infocus/1519`

Alternatively, you may want to seek the help of a security expert. IPSec is not something that can be thrown on to a network over a weekend. It requires careful planning to ensure minimal disruption of network usability.

8. HARDENING TCP/IP

Now that you have shut off every service and implemented restrictive security policies, the last piece of the puzzle is to close some of the doors into the system. This involves tightening up the TCP/IP network interface to the machine.

8.1. Unbind Unnecessary Services

By default, TCP/IP in Windows is bound to two main services, Client for Microsoft Networks and File and Printer Sharing. If you do not plan to share any files and the system is not part of a domain, you can unbind both of the services and close one of the largest holes in Windows for good.

1. To do this, select **Start > Settings > Network and Dial-Up Connections**.
2. Highlight the network interface and click Properties.

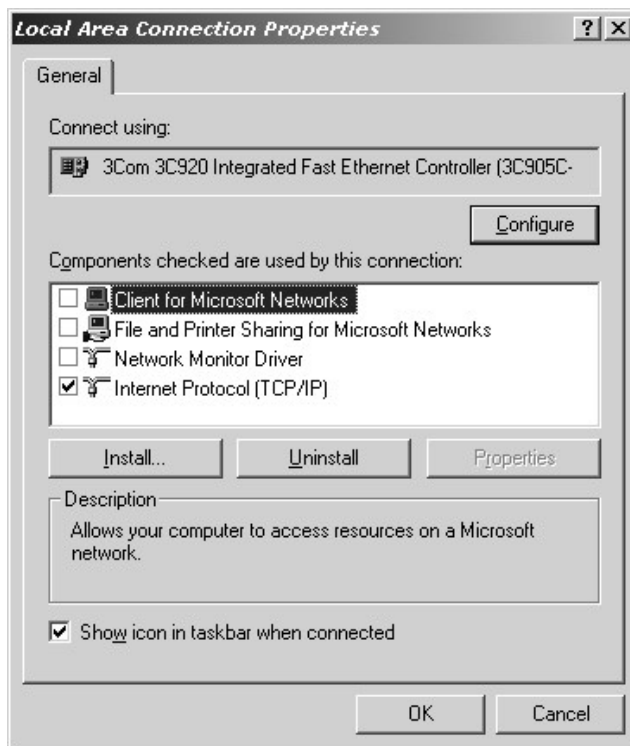


Figure 3 — Network Properties.

3. Uncheck the Client for Microsoft Networks and File and Printer Sharing for Microsoft Networks.

NOTE: Remember, if you make this change, the system will not be able to logon to a domain. Therefore, do not remove these services on domain controllers, email servers, or file servers.

8.2. Traffic Filtering

Windows 2000 includes a rudimentary, but effective packet filter on each network interface. While this is not meant to replace a good firewall, filtering is very useful for systems exposed to the Internet. For internal systems, it is very hard to get this right, therefore it is best to just forgo traffic filtering on internal systems.

Another thing to remember about traffic filtering is that it affects inbound traffic only. Outbound traffic is never filtered using Windows filters.

A perfect use for this would be on an Internet exposed web server where users should only be accessing port 80. A TCP filter allowing only port 80 will stop hosts from attempting to connect to any other port.

1. To establish filters, select **Start > Settings > Network and Dial-Up Connections**.
2. Highlight the appropriate network interface and click **Properties**.
3. Highlight **Internet Protocol (TCP/IP)** and click **Properties**.
4. On the General tab, click **Advanced**
5. Select the **Options** tab.
6. Select **TCP/IP filtering** from the Optional Settings box and click **Properties**.

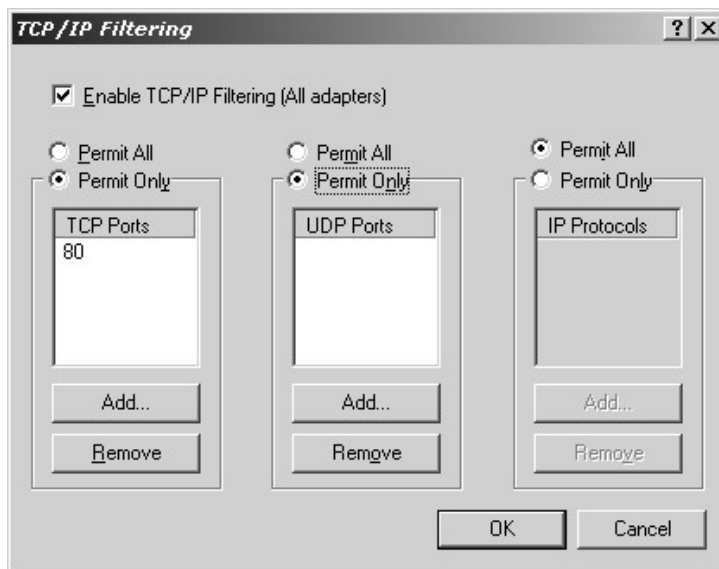


Figure 4 – TCP/IP Filtering

7. Click **Permit Only** to establish a filter for TCP ports, UDP ports, and IP protocols.

For a complete list of the IP protocol numbers, see:

<http://www.iana.org/assignments/protocol-numbers>

The ones most used are: 1 – ICMP, 6 – TCP, and 17 – UDP.

8. Click **OK** when finished. You will need to reboot the machine for these settings to take effect.

8.3. Network Interface Tightening

The TCP/IP stack in Windows was designed for maximum usability. Thus, some settings are a little loose for a secure environment. The following is a list of registry edits you can perform to further secure the network interface on a machine.

WARNING: Be very careful when making registry changes. You may want to make your changes on a test system first to make sure the changes work in your network environment.

Setting	Registry Key & Type	Description
SYN Attack Protection	HKEY_LOCAL_MACHINE\ System\CurrentControlSet\ Services\Tcpip\Parameters\ SynAttackProtect REG_DWORD	The default setting is 0, which offers no protection. If you set this to 1, Windows will reduce the number of retries it will make to a SYN request as well as delaying any changes to the route cache. Setting this to 2 does the same thing as 1 except it also delays Winsock notification. A setting of 2 is recommended.
TCP Max Half-Open Connections	HKEY_LOCAL_MACHINE\ System\CurrentControlSet\ Services\Tcpip\Parameters\ TcpMaxHalfOpen REG_DWORD	The default is 100 for Windows 2000 Professional and Server and 500 for Advanced Server. This value controls how many connections can be in the SYN-RCVD state (that is a SYN packet was received but a connection has not been made yet) before SYN Attack Protection is implemented. Be careful with this setting on Internet exposed systems. If you make this setting to low, you could block legitimate users who are connecting over slow connections.
TCO Max Half-Open Retries	HKEY_LOCAL_MACHINE\ System\CurrentControlSet\ Services\Tcpip\Parameters\ TcpMaxHalfOpenRetried REG_DWORD	Similar to the Max Half-Open Connections, this sets how many SYN-RCVD connections can exist where there has been at least one retransmission of the SYN. The default is 80 for Windows 2000 Professional and Server and 400 for Advanced Server. This too is a setting you may want to decrease for Internet exposed systems.
ICMP Redirect	HKEY_LOCAL_MACHINE\ System\CurrentControlSet\ Services\Tcpip\Parameters\ EnableICMPRedirects REG_DWORD	This controls if Windows will alter its route table in response to an ICMP redirect message. The default is 1 (true), this should be set to 0 (false) for all Internet exposed systems.

Setting	Registry Key & Type	Description
Keep Alive Interval	HKEY_LOCAL_MACHINE\ System\CurrentControlSet\ Services\Tcpip\Parameters\ KeepAliveTime REG_DWORD	This controls how often Windows will verify an idle connection. The default is 7,200,000 milliseconds, or 2 hours. Lowering this value will force systems to more rapidly check for dead connections. This is especially true of Internet exposed systems. A value of 600,000 (ten minutes) is recommended.

9. ACCESS CONTROL

The last step in this hardening process is to lock down all the directories on the machine to ensure only the appropriate users can access the system. You will need to carefully consider which aspects of the system need to be available to

Use the following checklist as guidelines when setting up ACLs for directories.

- ✓ Avoid the use of the Everybody group wherever possible.
- ✓ Restrict the Windows NT root directory (C:\WINNT by default) to Administrators and SYSTEM.
- ✓ Do not allow full-access to any users except Administrators. This prevents other users from deleting files.
- ✓ Manage via groups wherever possible.
- ✓ Be very careful with some of the Active Directory shares. Other domain controllers must be able to access this using their system account.
- ✓ Be very careful with the NETLOGON share. All domain users must be able to access this.
- ✓ Exchange E-Mail servers create some shares that have unique ACLs. Before you change the defaults, make note of how the system configured those directories.
- ✓ Create shares that direct users to the directories they are allowed to access. If users cannot see directories they are not supposed to access, they won't be tempted to hack them.
- ✓ Remove any Windows resource kit from the system. The files in the resource kit could be used against the machine.

- ✓ Protect the following special files that could be used against a machine by a hacker. You might want to move these or specifically set a more restrictive ACL on them.

arp.exe	ipconfig.exe	Nbtstat.exe
at.exe	net.exe	Netstat.exe
atsvc.exe	nslookup.exe	ping.exe
cacls.exe	posix.exe	qbasic.exe
Cmd.exe	rcp.exe	rdisk.exe
debug.exe	regedit.exe	regedt32.exe
edit.com	rexec.exe	route.exe
edlin.exe	rsh.exe	Runonce.exe
finger.exe	secfixup.exe	syskey.exe
ftp.exe	telnet.exe	Tracert.exe
xcopy.exe		

10. SECURITY APPLICATIONS

Once the main operating system is hardened, you may want to consider installing one (or more) of the many security applications available. This section summarizes some of those applications and the benefits they offer.

10.1. Anti-Virus

Anti-virus (AV) is almost a mandatory add-on for any system. A good AV package can detect and stop worms, Trojans, and of course viruses before they lead to compromise.

Some things to consider when choosing an anti-virus package.

- If you will be securing many systems, you may want to consider a commercial anti-virus package that includes central monitoring and management. This will make the task of deploying and administering the anti-virus software much easier.
- Run a full anti-virus scan at least once a week.
- Try to get a package that either includes or can be easily configured to automatically download new virus definitions. Automatic downloads do pose some risk in terms of security, however in the case of anti-virus, there is a good reason to do this automatically. Some commercial vendors have high-security mechanisms that use SSL tunnels to download the latest virus definitions.
- Test the anti-virus system periodically. Download the EICAR Test String from the Internet and put it on the system. This string is used for testing AV systems. Most commercial AV products will detect any file with the EICAR string as a virus, although the string itself is harmless.

10.2. Host-Based Intrusion Detection / Protection

Host-based IDS (HIDS) has become very popular in the last few years. A HIDS monitors all communications between the local system and the network (or Internet) for suspicious or threatening behavior. A HIDS can significantly increase the security of a Windows system, provided the technology is implemented and used in a diligent and responsible manner.

There is a lot of confusion and misleading marketing hype surrounding HIDS. Many product claim to provide comprehensive protection systems, when in fact they lack a lot of features and capabilities. These deficiencies compounded with a great deal of misinformation regarding host-based protection software from self-proclaimed security gurus.

One term that is often abused is the concept of “personal firewalls.” The whole personal firewall market has become flooded with a lot of questionable products targeted at home users. Some of these products are superficially attractive and seem to offer a lot of features. Yet when these products are analyzed in depth, many of the features are easily circumnavigated by widely available hacking tools.

Most security experts do not consider “personal firewalls” the same as a host-based. IDS. Personal firewalls are intended for small, home-office use. HIDS are designed for corporate network use and even though these products may share the same name as their consumer brethren, HIDS products are not always comparable to “personal firewalls.”

In general, all HIDS products have at least two fundamental components:

1. An IDS engine that detects malicious activity and,
2. An active response mechanism that blocks or prevents intrusion based on the analysis and detection features.

When considering a HIDS product, there are a few basic capabilities that should be evaluated as summarized in the following sections.

10.2.1. Communications Monitoring

When most security experts think of IDS, they think of communications monitoring. Communications monitoring is when a product monitors the network communications between the local computer and all other computers. When a remote computer is “talking” to the local computer, a host-based IDS monitors these conversations. If one systems “says” something that looks or sounds like an intrusion, the IDS will generate an alert.

BlackICE Defender, RealSecure Server Sensor, Okena StormWatch, and Sygate Secure Enterprise are examples of products that do communications monitoring.

10.2.2. Firewall

It is important to distinguish a “firewall” from the other active protection features such as application control or system integrity. A firewall is designed to control network traffic. Firewalls allow or reject network communications between computers based on a set of rules. Many HIDS products have integrated firewalls that can automatically respond to intrusion attempts with rules that block the offending system.

10.2.3. Application Control

Application control refers to software that can monitor and restrict the applications and processes running on a computer. For example, you could configure one of these products to allow Internet Explorer to run and use the network, but disallow users from running WinAmp. These programs usually have some kind of tracking mechanism that provides a way to monitor which applications are being used or allowed to communicate over a network connection.

Application control sounds good in theory. When hackers break into a system they usually attempt to corrupt applications or plant their own malicious code. Application control software can identify and block the hacker from running these programs.

The problem with application control is two fold. First, the use of application control requires a great deal of administration and monitoring. Every time an application changes or a new DLL is loaded, the application control must be re-initialized to allow the new versions of the software. Considering how often Microsoft releases updates to systems, this can create enormous administrative overhead.

The second problem is the issue of “piggybacking.” Hackers can easily engineer worms and viruses that “piggyback” their malicious requests on to legitimate programs. Hence, malicious activity can pass through the application control system since the hacker’s requests are “piggybacked” on to a legitimate application.

Some application control systems have “learning mode” options where you can merely track changes to applications. This can be useful as it provides a running log of when applications change. Should a system come under attack, you may be able to use such a system to pinpoint what the intruder changed and when those changes took place.

BlackICE Defender, ZoneAlarm, Sygate Secure Enterprise, and Okena StormWatch are examples of products that include Application Controls.

10.2.4. Behavior Control

Behavior control is a relatively new area of security. Unlike an IDS that monitors the communications between the local computer and other computers, a behavior-based IDS actually monitors the system calls and operating system functions. Behavior-based IDS provide a rather unique perspective to security. Arguably, a behavior based IDS could detect extremely subtle intrusions that a communications-based IDS might miss.

The largest drawback of behavior control is performance. These systems tend to use a lot of system resources since they must monitor complex interactions between the operating system and applications. They are also very limited in what they can detect and as such are relatively easy to defeat.

10.2.5. System Integrity

System integrity is a rather simple, although important, security component. System integrity tools monitor a computer file system for any changes. When a file changes, this change is reported.

The largest drawback of system integrity tools is their passivity. A system integrity tool cannot prevent an attack until it has taken place. These technologies are often labeled “after the fact” intrusion detection since they cannot detect an attack until it has been successful in damaging or modifying something on the system.

The most well-known system integrity tool is Tripwire. However, many other products have begun to include system integrity features into their products. For example, Okena StormWatch and ISS Server Sensor can also provide integrity features as well as other capabilities.

10.2.6. Logfile Analysis

Perhaps the crudest and most archaic form of intrusion monitoring is log file analysis. A logfile analyzer examines the output of the Event Viewer and other system log files for odd or suspicious events. Logfile analysis is not a particularly accurate method of assessing intrusions since good hackers will wipe out any reference to their activities. Some products, however, still include limited logfile analysis features, such as Server Sensor from ISS.

10.2.7. Selecting a HIDS

HIDS products should not be taken lightly. The best way to determine what is best is to test numerous products in your environment. There are a lot of HIDS products that sound great on a marketing brochure or when the salesman describes it, but when you plug them in and try to make them work, it’s a real mess.

Here are some factors you will want to consider when evaluating HIDS:

- HIDS products can significantly affect system performance. If you are running Windows on an older PC with limited memory, some HIDS products will cause serious performance problems.
- HIDS are not “set it and forget it” technologies. A decent HIDS system will generate a lot of information about what is happening on your computer. And some of that information will be “false positives.” Those are events that look like intrusions to the software, but are actually normal network or system activities. When you deploy HIDS products, plan to baseline, monitor, and tune the systems for optimal performance.
- If you are going to manage a large number of systems, consider HIDS products that integrate with comprehensive management consoles. This will make the administration, tuning, and deployment of those systems a lot easier.

- Application and behavior control products can be very cumbersome and complex to implement properly. Due to the ever-changing nature of some systems, it can be very difficult to make application controls work properly. Test these systems thoroughly before implementing them. Make sure to set aside the time and resources to baseline and tune these systems.
- A HIDS is only as useful as its owner. HIDS can offer a great deal of protection from intruders. However, they are not perfect solutions. Even a well-hardened system can be still be susceptible to attack. A good HIDS can alert you to suspicious activity, but it's your job to follow up on that activity and determine if the system was actually compromised.

10.3. Vulnerability Scanners

These products encompass a rather wide range of technologies that can spot potential vulnerabilities on a system and then provide suggestions on how to repair those vulnerabilities.

These tools can be very useful to help harden a system. Many of the suggestions in this paper are no different than what a vulnerability scanner would report.

In general, stick to products that can scan the system locally, such as ISS System Scanner, STAT, or Nessus.

10.4. Two-Factor Authentication

In the realm of security, authentication tends to be a real sore point for many organizations. Users are always resistant to anything that makes it harder to access information or the Internet. Two-factor authentication is almost a requirement for any serious security environment. The idea behind two-factor authentication is that a system has two different ways to authenticate the person (or program) using the system.

The first and most common authentication type is “Something you know.” In the case of most systems, this is a logon account and password. When you type in the correct password and logon account, the system authenticates these off a common database of accounts and then allows you to access the system.

The second type of authentication is “something you have.” This is usually some physical object or attribute. For example, a key card, token, or biometric authentication all encompass the “something you have” type of authentication.

The most common example of two-factor authentication is an ATM machine. When you want money from an ATM, you must first insert a card encoded with a special number. This is “something you have.” Once the card is authenticated, you must then enter a PIN code. This code and the card must authenticate together.

Two factor authentication is therefore a considerably more secure way to access system. It is a lot more difficult for a hacker to steal both a physical item, such as a key card or your thumb, and steal your password. Individually, each authentication measure may be fairly weak. But when combined together, the overall effect is increased security.

Perhaps the most significant problem with two-factor authentication is that it is rarely implemented completely. Merely requiring two-factor authentication for interactive (local) logon to the system will not do anything to stop hackers who break in through the network.

Therefore, should you decide to implement some form of dual-mode authentication, make sure to integrate the system completely. Otherwise it may just provide the veneer of security while still leaving holes at the network level.

11. CONCLUSION

Hardening Windows systems might seem like a lot of work, but there is significant pay off. These steps will create a system that is considerably less vulnerable to attack and more stable. A properly configured and optimized Windows 2000 machine can run for months with minimal maintenance.

It is important, however, to remember that no system is 100% safe. For every clever technology invented to thwart hackers, there is an equally clever way to circumnavigate those defenses. Nevertheless, the suggestions in this document should help you protect your systems from the most common types of intrusion.

11.1. For More Information

If you need more help securing your network, contact Anitian. Anitian is a comprehensive provider of network and computer security solutions. Our services include:

- **Security policy development**
Anitian's security consultants can help facilitate and manage the process of developing comprehensive security policies for your organization.
- **Security audits & penetration testing**
Anitian's security consultants can conduct a world-class audit of your network infrastructure.
- **Security products sales and support**
Anitian sells and supports some of the best security products available from respected names in security like Internet Security Systems (ISS), WatchGuard, IntruVert, Okena, eEye Digital Security, Nokia, Trend Micro, Tripwire, Symantec, and CheckPoint.
- **Systems integration**
From e-mail servers to routers, Anitian's network infrastructure team can help design, deploy, and administer your network and information systems.
- **Intrusion detection systems**
One of our specialties is installing, managing, and supporting intrusion detection systems, specifically the RealSecure IDS solutions from ISS.

- **Technical Documentation**

Another of Anitian's other specialties is writing and publishing documentation for security products and projects. Companies like ISS, Network Associates, and VeriSign have utilized Anitian's vast security expertise to help write their technical manuals, white papers, and training material.

- **General security consulting**

Anitian can also help with a wide array of security issues such as implementing IPSec or hardening systems.

- **Intrusion forensics**

Think you might have been hacked? Anitian can conduct objective analysis of your systems to determine the nature and extent of any intrusion you may have experienced.

11.2. Contact Information

Anitian Corporation
3800 SW Cedar Hills Blvd. Suite 298
Beaverton, OR 97005
503-644-5656 office
506-644-8574 fax
www.anitian.com