Global Information Assurance Certification Paper

From the Shelves to the Internet

A Step-by-Step Program For Securing Windows 2000

Prepared by:
David Chacon

04 April 2001

Table of Contents

1. INTRODUCTION 1

SCOPE AND INTENT 2
THREAT ANALYSIS 3
COUNTER-THREAT MEASURES 4
POLICIES AND STANDARDS TO IMPLEMENT 5
OVERVIEW OF CHAPTERS 6

2. WINDOWS 2000 SECURITY FEATURES 7

SECURITY FEATURES 8
NETWORK FEATURES 9

3. USER AND GROUP SETTINGS 11

USER SETTINGS 11
GROUP SETTINGS 12
AUTHENTICATION 13

4. GROUP AND LOCAL POLICIES 15

ADMINISTRATOR CONSIDERATIONS 15
DEFAULT GROUP POLICIES 16
INHERITANCE 18
BLOCKING INHERITANCE 19
NO OVERRIDE 20

5. ACTIVE DIRECTORY 21

SECURING THE ACTIVE DIRECTORY 21
IP SECURITY 22
KERBEROS VS. NTLM AUTHENTICATION 25

6. LOG FILES AND AUDITING 26

QUESTIONS TO ASK YOURSELF 26
AUDIT POLICIES 29
EVENT LOGS 30

7. CONCLUSION 31

8. APPENDIX A 32

9. REFERENCES 35

Table of Figures

Figure 1 Security Templates Snap-In 8
Figure 2 Guest Account Restrictions 12
Figure 3 RUNAS Command Authentication 13
Figure 4 Group Account Creation 14
Figure 5 Local Security Policy 15
Figure 6 Password must be at least 8 characters 16
Figure 7 Security Settings Extensions in Group Policy 17
Figure 8 Remove Group Policy Settings 18
Figure 9 Blocking Policy Inheritance 19
Figure 10 No Override Settings 20
Figure 11 Group Policy IPSec Settings 22
Figure 12 IPSec Security Properties 23
Figure 13 IPSec Filtering 24
Figure 14 Event Viewer 27
Figure 15 Security Event Default 28
Figure 16 Audit Policy Categories 29
Figure 17. Recommended Audit Policy Settings 29
Figure 18 Log Size Recommendations 30
Figure 19 Log Retention Recommendations 30

Part I

1. Introduction

Perhaps one of the most challenging aspects of a System Administrator's job is that of not only keeping his or her management happy, and insuring that their servers are safe from outsiders, but also keeping the customers happy. At times when we have found the perfect solution to locking down the machine, keeping the access tight, and restricting unwanted guests to the many systems we manage on a daily basis, our customers and solution providers find these restrictions unworkable. They rarely understand the importance of a secure environment and consider these tools an obstacle. Let us not also forget that there are the times when we finally have the registry secure so as to prevent outside attacks, however, now three programs and the OS do not function in harmony as they used to. Is there a happy medium to the flow of server management and security? The key in a nutshell, is simple trial and error over and over. These are the same kind of solutions that unions and management often find themselves deliberating over. In a society where we are often on top of the latest and greatest gizmos, gadgets and techie-toys to make our machines perform to their fullest, we often fail at catching up on the security side of the house.

Throughout the Internet, Department of Defense, Department of Energy and the vast array of security sites and organizations around the world, there are literally hundreds of different configuration guides to "lock" down machines. Information provided for free to lighten a System Administrator's job is always a blessing. However, the one aspect many administrators fail to overlook is that they sometimes never understand where or what the threat to their local environment really is. Without this key information, you simply have systems that many outsiders are very familiar with, since they study and detect the same vulnerabilities.

The methods discussed in this guide are designed to give new system administrators a guideline on the threats as well as issues to look at when securing Microsoft Windows 2000. No two government agencies or corporations are alike in anyway. This one straight and forward fact alone will require the System Administrator to carefully adapt the security plans to his or her own environment.

Scope and Intent

Microsoft Windows 2000 was a blessing for some when it was released with its abundance of security features. To cover all of the features in this document would mean a publication close to three hundred pages of instructions and details. Rather it is the intent of this document to cover the most commonly covered areas in government agencies and private corporations. Another point to remember, is that to fully cover the security aspect, I would have had to incorporate the profiles of the hacking community so that a new System Administrator would be able to fully understand what areas of his or her systems are most likely to be attacked. Windows 2000 has been out for sometime now and so have all of the "Securing Windows 2000" books. It is not my intent to simply repeat every single key area in a Windows 2000 network. My assumption is that you as a System Administrator probably already have a vast background and prior experience on Windows NT Server 4.0. Based on recent numbers it would appear that most System Administrators at a minimum have their Microsoft Certified Professional number.

Instead, this document covers only key areas that the users will have a working knowledge of. I am assuming that you are very familiar with the administrators' manuals and can diagnose based on the information you receive from these books and tech articles. At no time does this document cover third party vendors in detail. There are so many vendors on the market now with enhanced products that I would do a great injustice trying to cover so many in this short document. Besides, most small corporations simply do not have the capital to invest in third party products, as is the case for some small state and federal government agencies. This document will not teach you how to install Windows 2000 server. You should and probably already have this experience and are looking for ways to tighten your current configurations. If this is the case, then you should have by now been comfortable with Active Directory fundamentals, Security Policies and Organizational Groups.

Nothing would be further from the truth, to say that no matter how much trial and error you put into your secure environment, the ability to compromise security can simply lie within your own users. How many times have we changed passwords, only to find a sticky note on the monitor with the users last four of their social security? Or what about the secure email the user just received from your corporation, with their Kerberos passwords and Smart Card information lying on the dash of their car at the local shopping mall. Once again the happy medium must be calculated into your secure solution. The more challenges and enforcement you instate on your systems, users will generally find ways to make life easier for themselves. These loopholes often leave the threat inside the organization instead of outside the organization. Keep in mind that even the experts recommend that you do not completely lock down a system.

Threat Analysis

One of the biggest misunderstood aspects about system security analysis is that the word "Hacker" refers to an evil empire or person attempting to steal your valuable corporate data. Although most of this statement is quite true these days, the threat now lies within our own organizations, states and yes country. The breach of security is no longer limited to Defense Department secrets but also corporation secrets. Research and Development information would be a great asset for a small country that cannot afford to research on its own. Based on recent statistics, the threat can also now come from disgruntled employees within your own organization, the next-door neighbor who can figure out your password based on your dog's name, or your Internet account with your high school graduation date for a password.

The same manuals we as System Administrators purchase on Windows Security are also read in depth by people attempting to exploit weaknesses on your very systems. When trying to figure out what exactly needs to be locked down on a machine, take a serious look at what is it your company or organization does now. Will this information have an impact in today's economy or in the next five years? One compromised memorandum for the Vice President of the corporation to your Research and Development department on your ten-year plan could make you a target of opportunity very shortly. Have you switched your practice of doing business from secure line to the Internet? If this is the case, does your corporation know the full extent of damage that can occur if your new web site is compromised?

Has management considered who exactly is to be included in the planning phases of your plan? Do they have an understanding that a disgruntled System Administrator can cause significant damage if the passwords are not immediately changed? Is management also aware of your sub-contractors working under that new government bid you just won? Can they be fully trusted with your data?

Have the proper Networking Security features been put in place first? Are you closely working with the Network Engineers to ensure that all avenues of attack are covered? It would be useless for you to lock down your new server only to find out that the firewall hasn't been working since the spring of 1999. Is your Network Intrusion Detection software fully implemented and being monitored by the networking group? Have your fellow employees been properly trained on the art of social engineering? Do they know not to leave their Smart Cards in plain view? Do they know not to give valuable information over the phone or via email? All of these topics must be covered prior to assessing how tight to secure your systems.

As a System Administrator, do you continually update your skills and knowledge by reading the latest security bulletins from the security community? As an administrator, can you identify ways the hacking community can infiltrate your systems? With so many questions to answer, you can see why the trial and error process is a continuing one. As new vulnerabilities are detected, your plan is modified a little bit more to include new service packs, add-ons, and new registry edits.

Counter-Threat Measures

Now that you have identified your corporation or agency as a candidate for attack, it is time to determine how to prevent these with well-known methods. The most basic form and often compromised is that of the password policy. Install a bootup password when the machine first comes on. Disable bootup by CD if possible, and ensure that Drive C is the bootup drive only. Use software that generates passwords by algorithms rather than by dictionary. The chances are still high that you will still see these passwords written down under the keyboard, but then again they will be a lot harder to break into from the outside. By incorporating a mixture of numbers, letters and specific lengths, the hashing and hacking process becomes more complex. With Windows 2000 and the new version of NTLM, the process of cracking passwords will become more complex.

When working with the networking group in your organization, have they talked to you about their ability to defeat "sniffing" on your lines? By controlling who has access to your phone switches, wiring closets and cable leading to your building, you have one less avenue to worry about. If you were using fiber optic cabling, now would be a good time to implement strategies on implementing your secure rooms for possible classified data.

Not only do you have to worry what restrictions to apply to groups, but you have to worry about the health of the machines you manage as well. Have you implemented virus protection on your data? Will you be able to implement your disaster recovery plan in the event some type of file deleting virus that has been waiting on your system for months has now launched and compromised you? Ensure that your disaster recovery covers fire, theft, flood or other disasters.

See what resources you have today to start. Place your servers in an area where they are not next to a high flow of traffic. Control to the best of your ability personnel that can enter the room where you have them in place. Identify the security where your building is located. Does a small security force protect it? Is it fenced in, or clearly marked as a secure site?

Install the latest and greatest patches for Microsoft Windows 2000 as they become available. If feasible, test updates in your test lab prior to installing on the server. The patch might work just fine on the server alone, but what about the server with that piece of software created by the Data Base administrators and some entry-level third party software. Actions like these will defeat an entire machine on the inside rather than from the outside.

Policies and Standards to Implement

Once you have pretty much identified what all of your possible threats are, and are confident that you have covered every aspect of security when dealing with your data, the next step is to determine what can you basically get away with without jeopardizing your customer relations and at the same time, keeping management confident in your abilities to provide a secure system. We have already discussed the issue of passwords for starters. Historically, the compromise of passwords has been the easiest way to gain access to one's system.

Generally speaking, if you work for a large corporation or government agency that has been in existence for quite some time with significant computing power, then policies and procedures are in place for you. For instance, most military plans cover the policy for employees on "Need to Know" information. Some policies cover the extent of how much information you are allowed to share with prospective contacts at trade shows. As System Administrators, if your company is fairly new or you are creating a policy and procedures document, it is imperative that you first assess what the price tag is on your data. A secure network of Windows 2000 servers is futile if there are no policies and procedures for personnel to follow and protect it.

One effective analysis formula to use when determining lost revenues to the company is that of:

Risk to Company = (Value of Data)(Probability of Exploitation)

As the probability of exploitation increases, so does risk.[1] Will you have the information controlled by one organization within a company, or will there be multiple keepers? You must figure this out, as you will need this to determine your user lists and later on as you also determine who is ultimately placed in the Administrator's group and domains. Under the new Windows 2000 server environment, the domain model will have more power than that of the NT 4.0 environment did. Administrator's should be clearly defined and trusted with the great responsibility they have on their shoulders. For instance at certain government facilities, it is not uncommon to see Administrators with at least eight years of networking experience and certifications galore running the top secure classified networks. This background is then topped with a high-level security clearance. These are policies that agencies have in place to ensure they can trust the security of their valuable data and their key personnel.

Once you have a security policy in place for what can and cannot be conducted on your Windows 2000 box, it must be considered a working document as well. Just like the security plan that helps you tighten down your machine, changes will no doubt come and go as the technology changes.

[1] Cox, P. Sheldon, T. Windows 2000 Security Handbook. New York (NY): Osborne/McGraw-Hill; 2000 57 p.

Overview of Chapters

2. Windows 2000 Security Features

This is basically a guideline to let you know what new features Windows 2000 has in the line of security and networking tools that will help streamline the System Administrator's job. It will briefly cover some new architecture as well.

3. User and Group Settings

If you already have a strong background in Windows NT 4.0 Server, then the following should be a good refresher for you. As always, the way user rights are determined goes back to "What information do they really need access to"? These topics once again are geared towards the areas of domains.

4. Group Policies

Because there are already a few good web sites out there, not to mention numerous excellent books on the subject, this section will only cover items that are more necessary than most. Most group policies are nothing more than a compilation of policies that define group and user settings.

5. Active Directory

The ability for an Administrator to control access to all of the sensitive data, yet allow certain users access to their files is the control that Active Directory can provide in an enterprise environment. As networks grow or shrink in the work area, the Administrator needs to know that he or she will be able to handle whatever task may come his or her way in regards to distributed security. At the same time the administrator can feel confident that Active Directory will be able to span through multiple organizations or possibly countries and yet be still be able to often click on certain areas of his or her scheme and make changes as necessary.

6. Log Files and Auditing

In a dream world setting, the Administrator would be able to collect and analyze all the data he or she has collected to evaluate possible threats. With constraining work budgets, low IT budgets and not enough highly trained computing professionals, Windows 2000 has made it easier to create auditing policies and help the Administrator analyze what needs to be further evaluated in terms of breaches in the network.

Part II

2. Windows 2000 Security Features

Perhaps one of the most anticipated features that most Administrators waited for was that of the ability to have control and delegation of authority over a vast array of domains, based on group memberships. Because of Active Directory, this is now possible. Whether you are a mom and pop business or International corporation, Windows 2000 has the ability to shrink or grow on a moments notice without severely impacting day-to-day activities. Gone are the days of NT 4.0, trying to remember who trusted whom and which resources could use what. With Windows 2000, a complete transitive trust model is now in place. The users of a defined account in Domain A can now be authenticated by Domain B to use its printers. Domain A and Domain B simply maintain an implicit trust as long as they are both part of the same Tree.

What is new for the System Administrator is "snap-ins". Under Windows 2000, the Security Templates and Security Configuration make locking down systems a breeze. Basically they allow the Administrator to determine weak points and incorporate those changes onto the local machine or across the network. For the larger enterprise, this is usually a job that requires many administrators to accomplish under the old NT 4.0 system. As the corporations need change, different System Administrators can manipulate the security in one area rather from many different areas.

With Windows 2000, user logons are no longer complex as well. For the small e-commerce site, this is a blessing to the users. They do not have to be concerned about the different types of security logons. The users credentials are centrally managed under Windows 2000 and are checked against the verifying security protocols to determine access rights. When converting from Windows NT 4.0 Server to Windows 2000 Server, the security will need to be reviewed once again. The questions that were used to determine systems safety will also be addressed once again. What are my threats? What is the value of my data? These questions can be answered more clearly now with Windows 2000 using the new Security Configuration Tools. The Secure templates provide increased security for areas of the operating system that are not covered by permissions, including: increased security settings for the account policy, increased settings for auditing, and increased security settings for some well-known security relevant registry keys.[2] They allow you to reevaluate the local and account policies, system services and members of restricted groups. There are also the default configurations that can be used if the need for custom applications is not necessary within the secure machine. The policies and procedures if established will only need minor adjustments. If migrating security policies from NT 4.0 to Windows 2000, this is also an easy task with the backward compatibility features.

[2] Q234926, Windows 2000 Security Templates are Incremental, Last Reviewed: December 30, 1999

Security Features

The best way to describe the difference between NT 4.0 and Windows 2000 is the fact that the 2000 machine will have the Active Directory in place. This is the sole provider for distributed security functionality. With any install of Windows 2000 you will by default receive the security default settings. These settings are basically set to moderate. Another words, they are tighter than what NT 4.0 used to have, but they are not at their full capacity at this point. As covered in Part I of this document, only after thoroughly covering all aspects of the security plan, can you determine how much more security you will need to add to the default templates. Under Windows 2000 items such as files, devices and processes are considered "Objects". A typical application may be built from hundreds of objects. A good analogy is a car, which is built by assembling many small objects. It connects to those objects through a standard interface. Think of an Object as a box that contains information and functions for manipulating that information.[3] As mentioned before, the new Security Configuration Tool Set now will be able to save agencies money, since the need for personnel is streamlined with this security feature. The Security Configuration Tool Set also provides functionality to analyze a given system's security configuration against that defined in a specified security policy.[4] A System Aministrator new to Windows 2000 will be able to open Microsoft Management Console and select from various pre-defined snap-ins to determine the level they prefer for their systems.

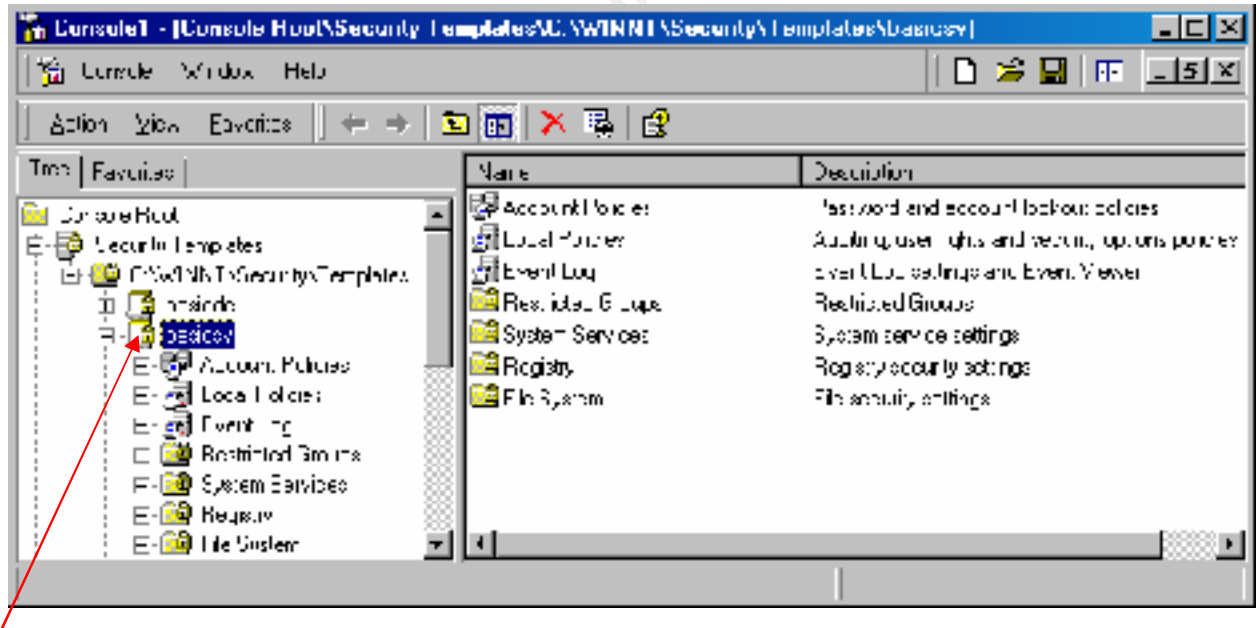


Figure 1 Security Templates Snap-In

Ensure that you select the right template.

[3] Cox, P. Sheldon, T. Windows 2000 Security Handbook. New York (NY): Osborne/McGraw-Hill; 2000 57 p.
[4] Internet Security Systems. Windows 2000 Security Technical Reference. Redmond (WA): Microsoft Press; 2000 300 p.

Network Features

Not all corporations or agencies will benefit from all of the networking features provided by Windows 2000, however a general understanding will help you prepare as your machines and network expand in the future. The main features commonly addressed in regards to Networking include:

Remote Access

Internet Protocol Security

Dynamic DNS

Dynamic Host Configuration Protocol Security

Remote Access

Three of the most common tools that can be used to help you establish connections from remote places for your customers are:

Routing and Remote Access Service (RRAS)

Internet Authentication Service

Terminal Services

For the purpose of simplicity, we will discuss the RRAS and the Terminal Services since they are the most commonly used tools. The RRAS is installed by default on your Windows 2000 system and must be manually set to start it. If you plan on participating within a domain environment, then you can use the authentication list for access control. In order to use this feature, you must select a remote access server or network access server.

When choosing Terminal Services, you have the option of either an Internet connection or Dial-Up connection. The Terminal Services simply provides the users and customer's access to your centrally server-run applications. One of the most common benefits is the fact that you do not need to purchase many workstations to accomplish tasks. Instead upgrades and hardware repairs are done on one central supporting server.

Internet Protocol Security

One of the exciting features of IPSec is that the receiver and sender are the only ones who are aware of the security key. IPSec can help the Aministrator effectively perform their job, since security is on the outside as well as the inside. The way IPSec works, the data is encapsulated and then IP headers are placed on the packet. Any interim

stop on the path to the final destination only sees that the packet is destined for the other end of the Virtual Private Network.[5]

Dynamic DNS

The biggest news about DNS under Windows 2000 is that it has replaced the ability of WINS to resolve computer names to the IP addresses. It is pretty much a mandatory tool since Active Directory will need DNS to provide it with the name space. That is in Windows 2000, domains are created with DNS names. Unlike Windows NT 4.0 Server, the new DNS also has the ability to dynamically update records. Under Windows 2000, it is almost essential that you tie DNS and DHCP together for complete security. If the DHCP security is compromised, then DNS records are vulnerable.

Dynamic Host Configuration Protocol Security

One worry that Administrators frequently worry about when dealing with Dynamic Host Configuration Protocol servers, is the possibility of "unauthorized" DHCP servers on the network. There is also the possibility that the DHCP servers on the old Windows NT 4.0 domain can be spoofed or sniffed by potential hackers or adversaries. Most of the time, it is merely a simple mistake on the Administrator's part. However, there are times when it is possible that someone may be able to install a DHCP server on your network. The threat of this is that it is possible to issue out unapproved IP addresses on the network. When this happens, communication problems begin to occur, or information is stolen.

With Windows 2000, they have tried to prevent this by having an authorized DHCP list of servers on the domain. Since Active Directory contains all of the information per domain, it is also necessary to install the DHCP on the domain controller, so that it can be managed. If the new server is not authorized on the Active Directory, its service will not be started. In order to make changes to the new DHCP server, you must be a member of the Enterprise Admin groups. Although this may seem like a burden, it assures that the right personnel are making only the necessary changes necessary. It also reduces the possibility that a new Administrator will not divulge information accidentally. Secondly, the installation of DHCP is assuming that you as the Administrator will be installing only Windows 2000 DHCP machines. This leaves you with the possibility of not migrating any old Windows NT 4.0 DHCP machines from your previous domains.

[5] Cox, P. Sheldon, T. Windows 2000 Security Handbook. New York (NY): Osborne/McGraw-Hill; 2000 115 p.

3. User and Group Settings

User Settings

The good thing about user and group accounts in Windows 2000 is that you don't have any options to not install the security features for your system. The bad part is that Administrators should not take it for granted that the tightest security will be implemented by default as well. After thorough analyzing, it once again up the Administrator as to what kind of security is actually needed with users as well as managed groups. One point of thought needs to be brought out at this point. That is, most manuals on the market at this point tend to concentrate on the clean install of Windows 2000. If you have no intentions of doing a clean install, then I must point out that the default security installation only applies to Windows 2000 and not the upgrade features.[6] Under the new security features, Windows will now let users mess with the registry settings, system files, program files, and have no rights to any questionable sensitive paths like they used to in Windows NT 4.0. Secondly, they also will not be able to run programs that have been installed by other users. Where this feature comes in handy is for virus protection. A Trojan horse program will need to find a new way to run. As an Administrator the first thing you can do to protect your systems with default security is to ensure that only software that has the "2000 Application Specifications", is installed on the system. Avoid the fly-by-night software to ensure security. Applications that meet the Windows 2000 Application Specification will run successfully under this context.[7]

Just like Windows NT 4.0, any user in a decent secure environment must have a user account to access the system. Under Windows 2000 the default accounts that are installed are:

Administrator

Guest

When dealing with the Guest account, it is installed by default with the disabled button selected. As the Administrator, verify that it remains disabled at all times. If this account remains active, it is a primary opportunity for someone on the inside or outside to access any data or areas on the system that have rights open to the Guest account or Everyone Group. The other problem is that it now becomes a heavy burden to try and track down who is using the Guest account.

[6] Q2170505, Description of Default Security Settings in Windows 2000, Last Reviewed: January 26, 2001
[7] Bragg, Robert, Windows 2000 Security. Indianapolis, Indiana: New Riders; 2001 129 p.

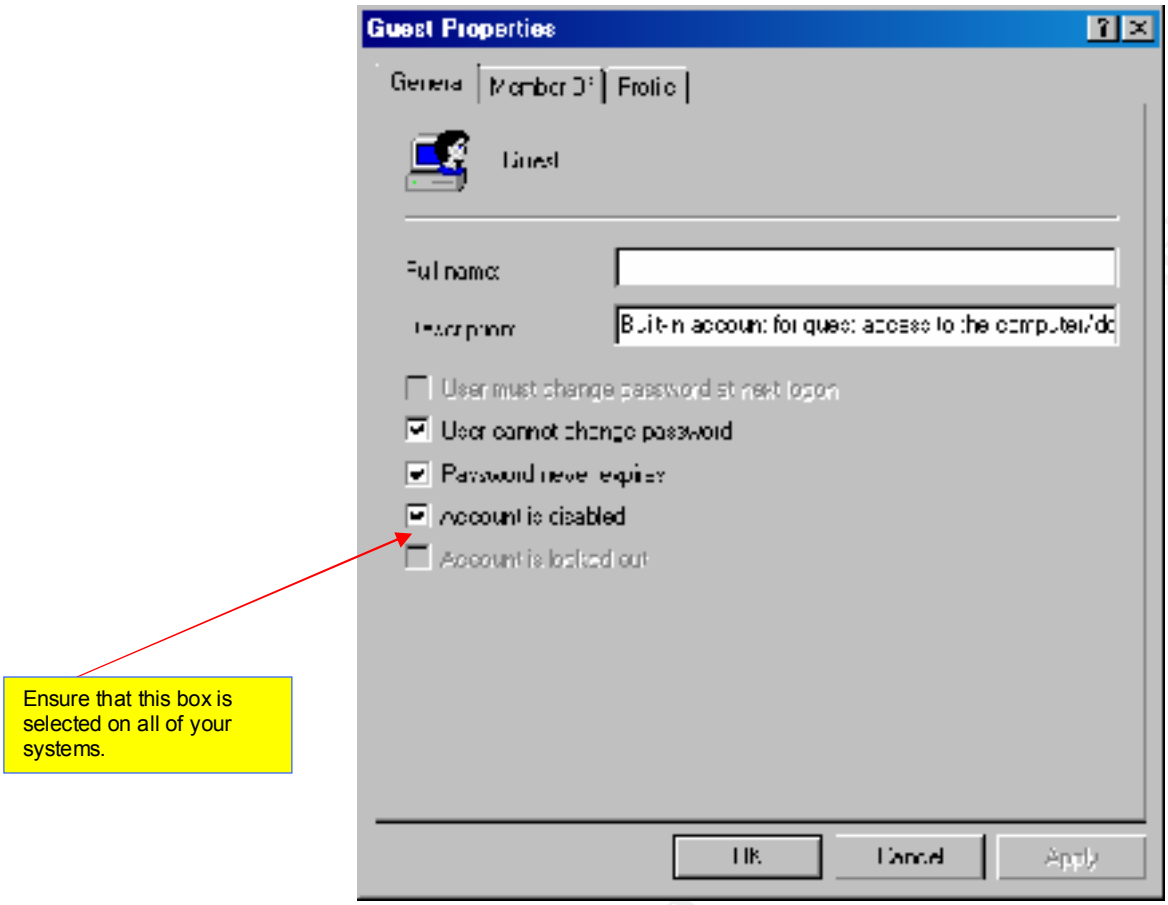


Figure 2 Guest Account Restrictions

Group Settings

Under Windows 2000, there are three types of Administrator accounts. They are:

Administrators
Enterprise Administrators (Only in a traditional domain environment)
Domain Administrators (Only in a traditional domain environment)

The Administrator by default has the ability to grant permissions, restrict privileges, and has the power to enter the registry files on a system by taking ownership if need be. The Windows 2000 Kit includes many tools to help you with performing administrative tasks, automating application deployment, and other jobs.[8] Under Windows NT 4.0, it wasn't uncommon for the Administrator's account to be renamed, in order to prevent hacking or the curious insider from breaking in. The problem with this is that the day your Administrator found a better paying job, he took the information with him as well.

[8] Q274305 – Free Windows 2000 Resource Kit Tools for Administrative Tasks, Last Reviewed: October 26, 2000.

Authentication

Under Windows 2000, if you have given yourself a user account on the systems, the best thing to do is to use the RUNAS command. This command will prevent you from running and logging into the Administrator account and compromising the system if your network is being sniffed. It simply lets the person accessing the application to run the program with the privileges that the user account was given. To use the RUNAS command through the shell, select the executable, press Shift, and right-click.[9] You will get a screen like this:

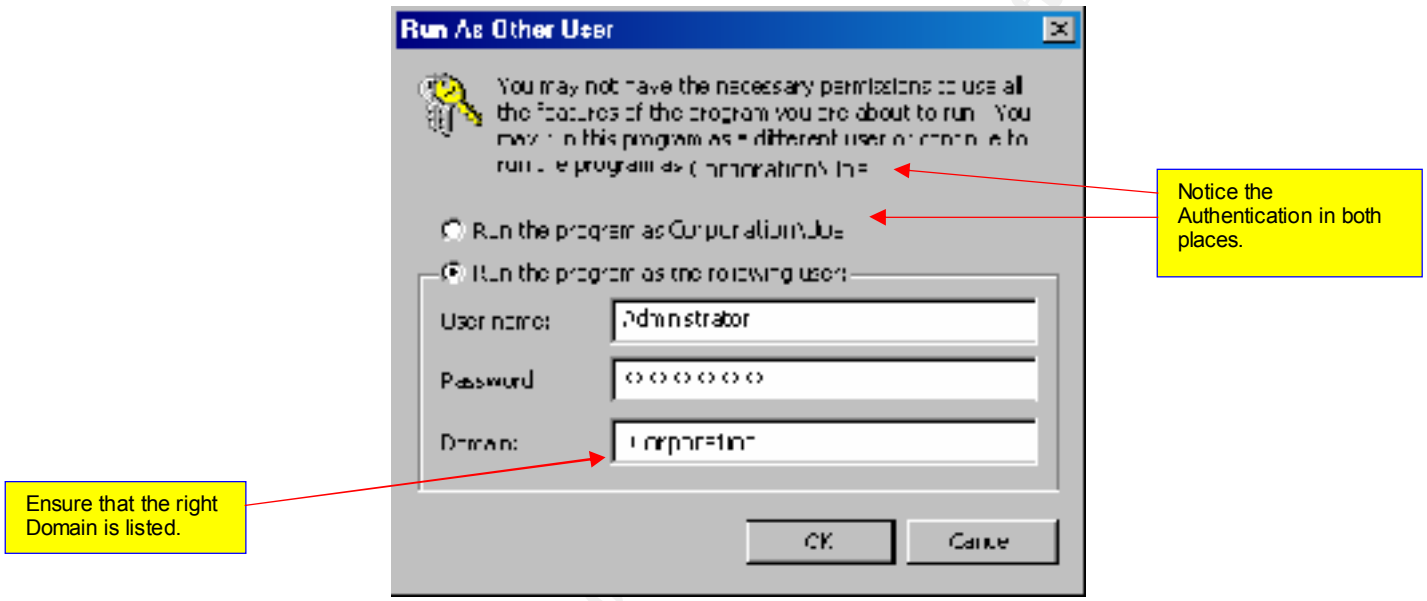


Figure 3 RUNAS Command Authentication

Being as how Administrators are human like anyone else, the final point to make with the Administrator's account is that of passwords. With Windows 2000, the maximum length of the password can be 128 characters. This may sound like a great deal to further prevent the attempted break in, but keep in mind the longer the password, the harder it is to remember. The more complicated the password, the more chances are that you or your co-worker will forget it, or simply write it down and put it some place convenient. The recommended length for the Administrator's account should be at a minimum of eight characters. Under 2000, there is a smaller chance that your passwords will be compromised, but the operating system is still very young, and in a few years, chances are some small company will figure out to crack those as well.

Finally, the last thing to keep in mind is to secure your system and regenerate a new password every time you have turnover within your system administrators. If you remember, the chances are higher for a breach of security from within than from the outside.

[9] Bragg, Robert, Windows 2000 Security. Indianapolis, Indiana: New Riders; 2001 128 p

Under Windows 2000, the Group Accounts are a little more complicated than before. This is not to say that you cannot work with them, they just fall under different areas for storage. Such is the case as they now fall into the Active Directory. The Group Accounts are nothing more than a compilation of specific users that you place into them to basically make your job easier. You can control access to shared resources, or control what applications are to run. Why bother you ask? Simply put, it would take an enormous amount of time to administer five thousand user accounts. Which people would have printing rights? Which people would have access to corporate secrets? Finally, which people would you consider management? With a Group Account you place the personnel into the Group and give the Group the rights they need. For example, lets say that your specific computing organization handles the classified data for your corporation. If there were twenty people on your team, it would be very annoying to have to add specific permissions on all of your teammates. What you could do is create a Group called "Windows Server Team". This is an example, so you could re-word this to something similar in nature. You would then assign permissions to the Group and your team would have all of the domain rights needed to access the classified corporate information. See the example listed below:

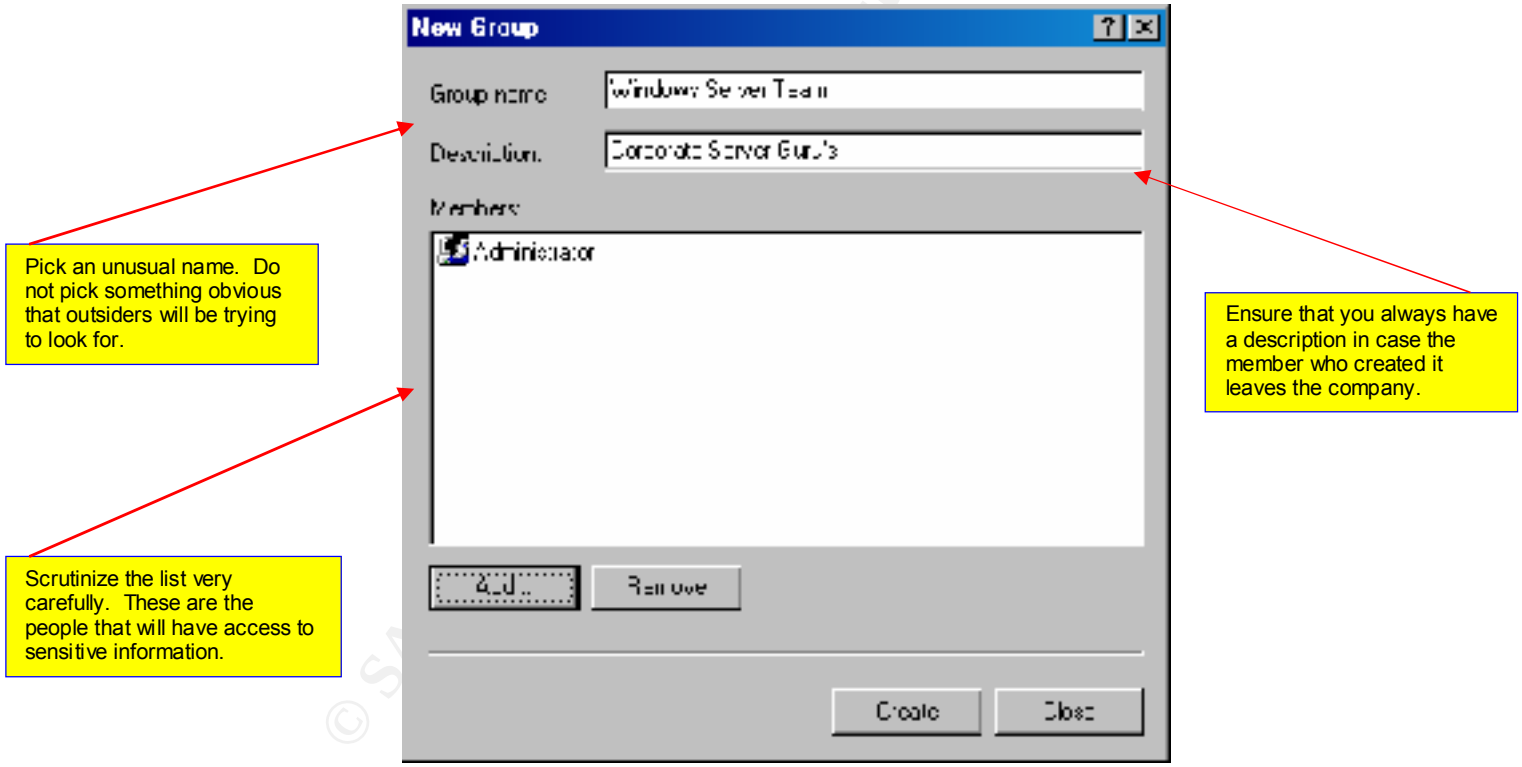


Figure 4 Group Account Creation

4. Group and Local Policies

Administrator Considerations

One of the best tools on your systems and network is that of security policies. With security policies you as the Administrator can prevent waste, fraud and abuse within your corporation or simply within your domain. For the purpose of this discussion we will discuss Group policies at a minimum. You should successfully be able to implement at least one policy to prevent unwanted abuse amongst your users. Not only will this keep down the number of violations within your organization, but it will also prevent damage to your system configuration from curious users.

On a standalone computer, that is a sensitive machine that contains data, research or information that cannot afford to be placed on the network, you can use a Local System Policy and get away with that. In this example, we will create a password policy on our standalone system, to ensure that our scientists do not use simple passwords to protect our sensitive data. To create a system policy on a standalone computer, follow these steps:

Go to Start, then Programs, then Administrative Tools, and select Local Security Policy. Go to and expand Account Policies. Open Password Policy and you should see an image like this:

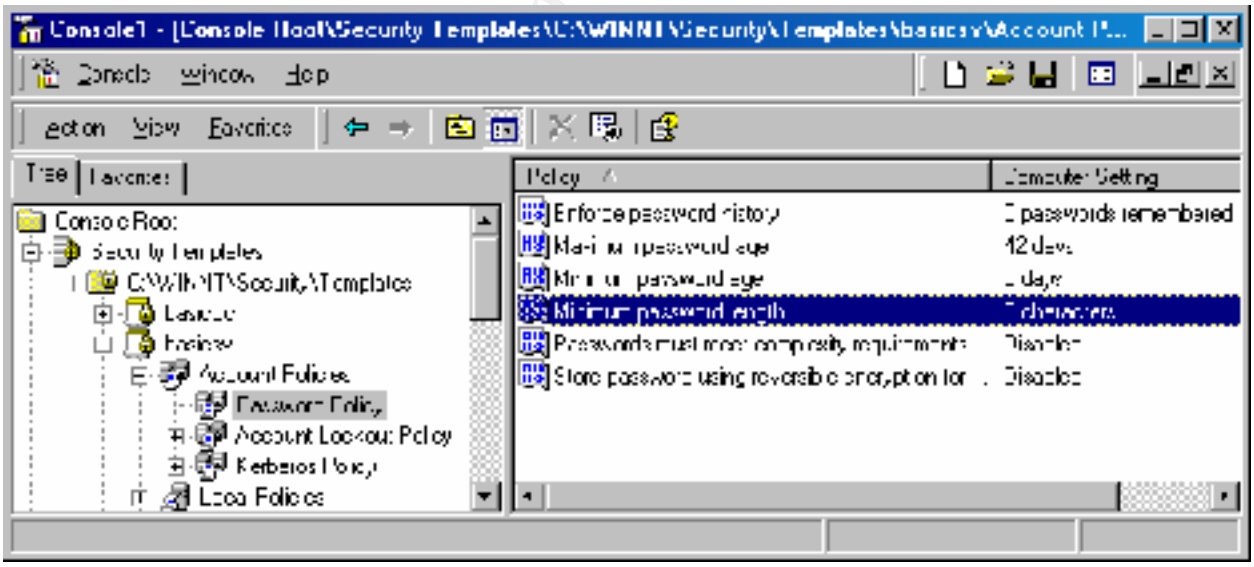


Figure 5 Local Security Policy

1. Select Minimum password length, and you should see an image like this one:

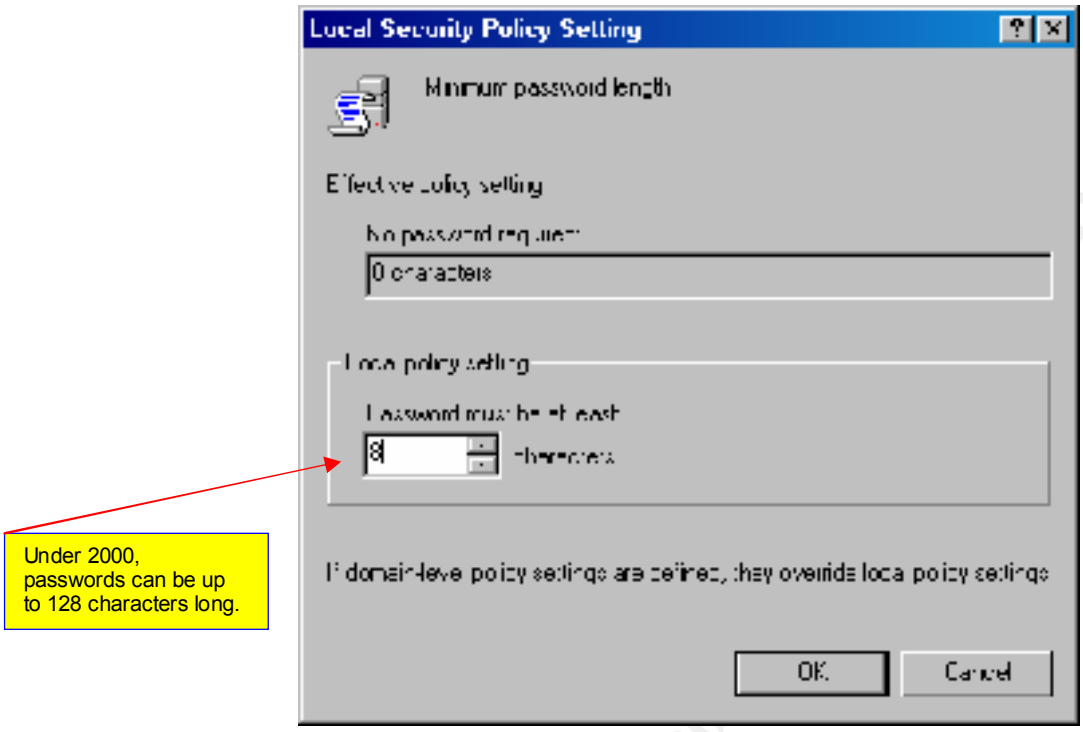


Figure 6 Password must be at least 8 characters

2. After you have entered the number you choose, in this case "**8**", select OK and close the Console.

3. Your policy is now in place, test on the system prior to implementing across the board.

Default Group Policies

Group Policy is a key component of IntelliMirror ™ management technologies in the Windows 2000 operating systems.[10] Group policy allows you to implement security across the network, by defining user and computer configurations. An Administrator can edit the policy for any site or domain. In addition to this, the administrator can also edit the Organizational Unit (OU) within the domain. With these policies, you can effectively manage scripts, software, security and settings. When you specify Group Policy settings, they are placed in a Group Policy Object (GPO) that, in turn, is associated with selected Active Directory objects (a site, domain, or Organizational Unit).[11] The data generated by Group Policy is stored in a Group Policy object (GPO),

[10] Microsoft White Paper, Group Policy Simplifies Administration, Published: November 4, 1999.
[11] McLean, Ian, Windows 2000 Security A Little Black Book Scottsdale, Arizona: Coriolis; 2000 79 p.

which is replicated in all domain controllers within a single domain.[12] The two sections are the User Configuration and Computer Configuration. Under the Windows 2000 network, you can find three different kinds of policies. These are:

Local Group Policy – This policy resides on the system that it is designed for. It is there for the administrator to install policies on their machine, that is not part of the Active Directory domain. This policy supports everything, except software installation and folder redirection.

Active Directory Group Policy – This allows full access to all of the support provided to the GPO. This policy will be linked to any domain, site or Organizational Unit within the Active Directory.

WINNT System Policy – Under Windows NT 4.0, Administrators utilized POLEDIT.EXE to create and maintain policies. When you choose the upgrade option, the system policies come across and are placed into the SYSVOL directory from your old Domain Controller on the NT 4.0 network. They are simply transferred and not converted to a Group Policy Object. The following table describes the file extensions that can be modified under the policies of both Local and Global:

IPSecurity Policies	Allows for the configuration of Internet Protocol Security. This is the industry standard for securing TCP/IP.
Public Key Policies	Allows configuration of certificates and encrypted data recovery agents.
System Services	Configuration of services during startup.
Registry	Configuration of security keys.
File System	Allows the Administrator the ability to secure file paths.
Restricted Groups	Allows for the configuration of managed groups, such as Administrators. Other groups may be added into the Restricted Groups for ease of control.
Local Policies	Allows for the configuration of security settings, auditing policies, user rights and other options.
Account Policies	Allows for the configuration of policies such as passwords, lockout procedures, and kerberos policies.
Event Log	Allows configuration of the security, system and application logs.

Figure 7 Security Settings Extensions in Group Policy

[12] Microsoft White Paper, Step-by-Step Guide to Understanding the Group Policy Feature Set, Published: January 31, 2000.

Inheritance

As the Administrator of your systems, you have the option of selecting, which machines you want to avoid having Group Policies propagated down to. There is a specific order in which Policies are pushed on down to the machines. These areas are:

Site
Domain
Organization Unit

The Policy Objects for all of your Organizational Units above your object are processed at the top level first. The Group Policy Object closest to the user or computer takes precedence at a conflict.[13] The best thing for the Administrator to do is to remove the "Allow" permissions on their systems. This will avoid problems on your systems. Keep in mind that sometimes you yourself can be bumped.

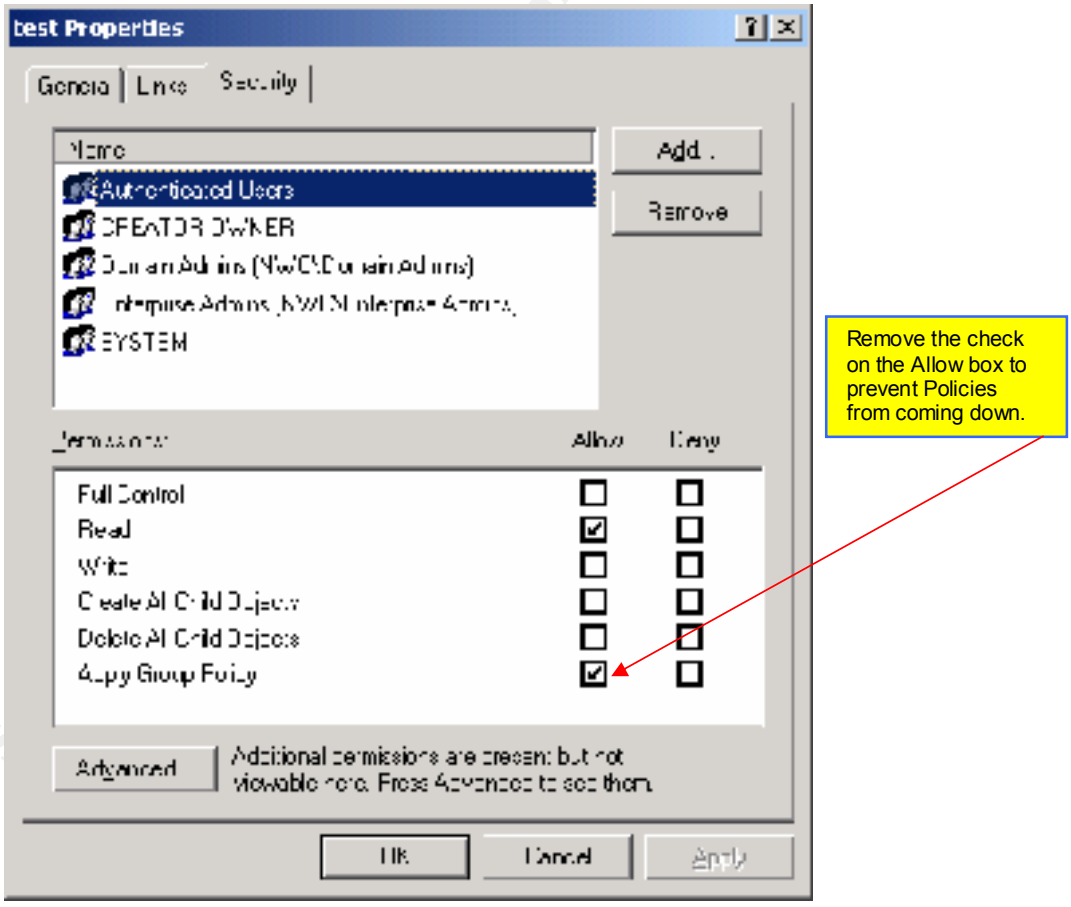


Figure 8 Remove Group Policy Settings

[13] Wood, Adam. Windows 2000 Active Directory Black Book, Scottsdale (AZ): Coriolis; 2000 299 p.

Blocking Inheritance

Under 2000, you do have the ability to block Group Policy Inheritance on your domains or Organizational Units. Basically all this states is that anything from a higher GPO can be ignored. The one exception is No Override settings, which aren't blocked.[14] Keep a tight control on these restrictions when you implement them, or seriously document these settings close to the machine. People have a tendency to forget what they have applied in the past.

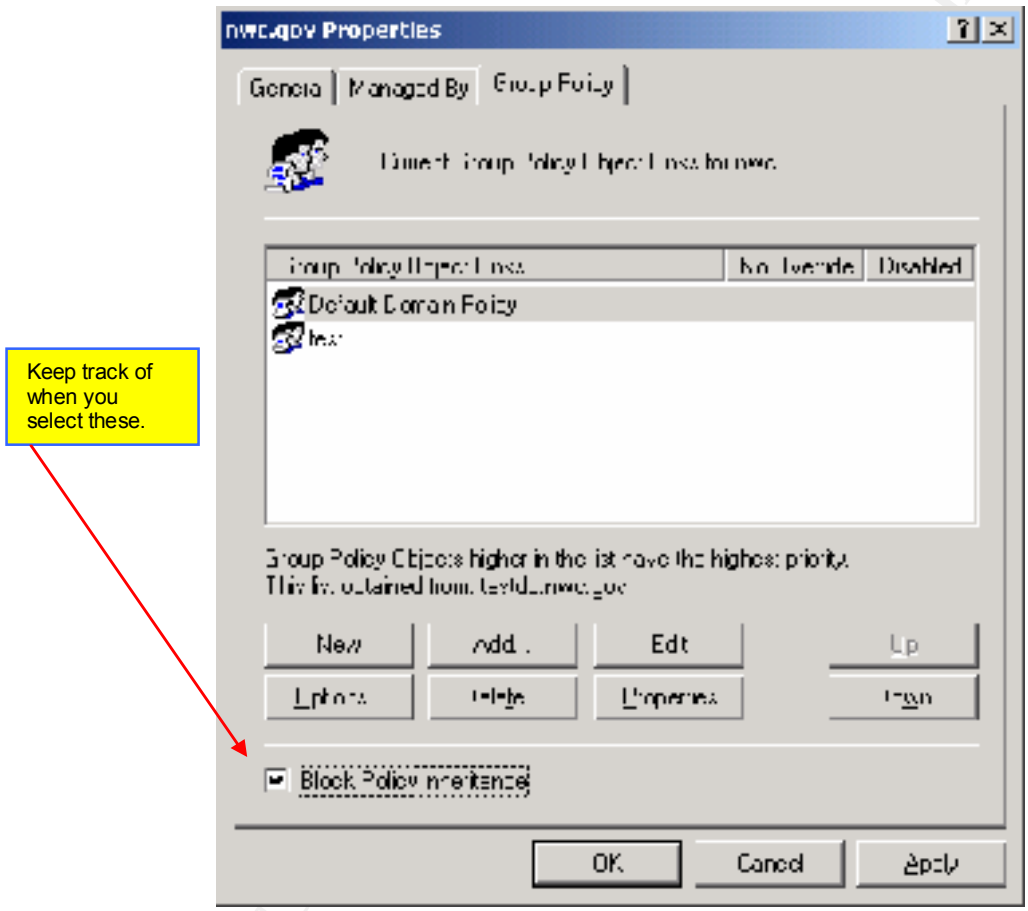


Figure 9 Blocking Policy Inheritance

[14] Wood, Adam. Windows 2000 Active Directory Black Book, Scottsdale (AZ): Coriolis; 2000 301 p

No Override

Finally, the No Override ability can be utilized for specific containers. Although Administrators may feel that they can beat most upper level GPO's, the rule is still the same. A higher-level policy will beat out a lower policy in the event of conflicting policies. As soon as a setting from a GPO flagged as No Override is processed, that setting can't be replaced.[15] Once again, maintain control and documentation of this setting on your sensitive machines. In large corporations, a Computer Security department would more than likely use this command to push down it's policies. You can get to this setting by going into the Options button.

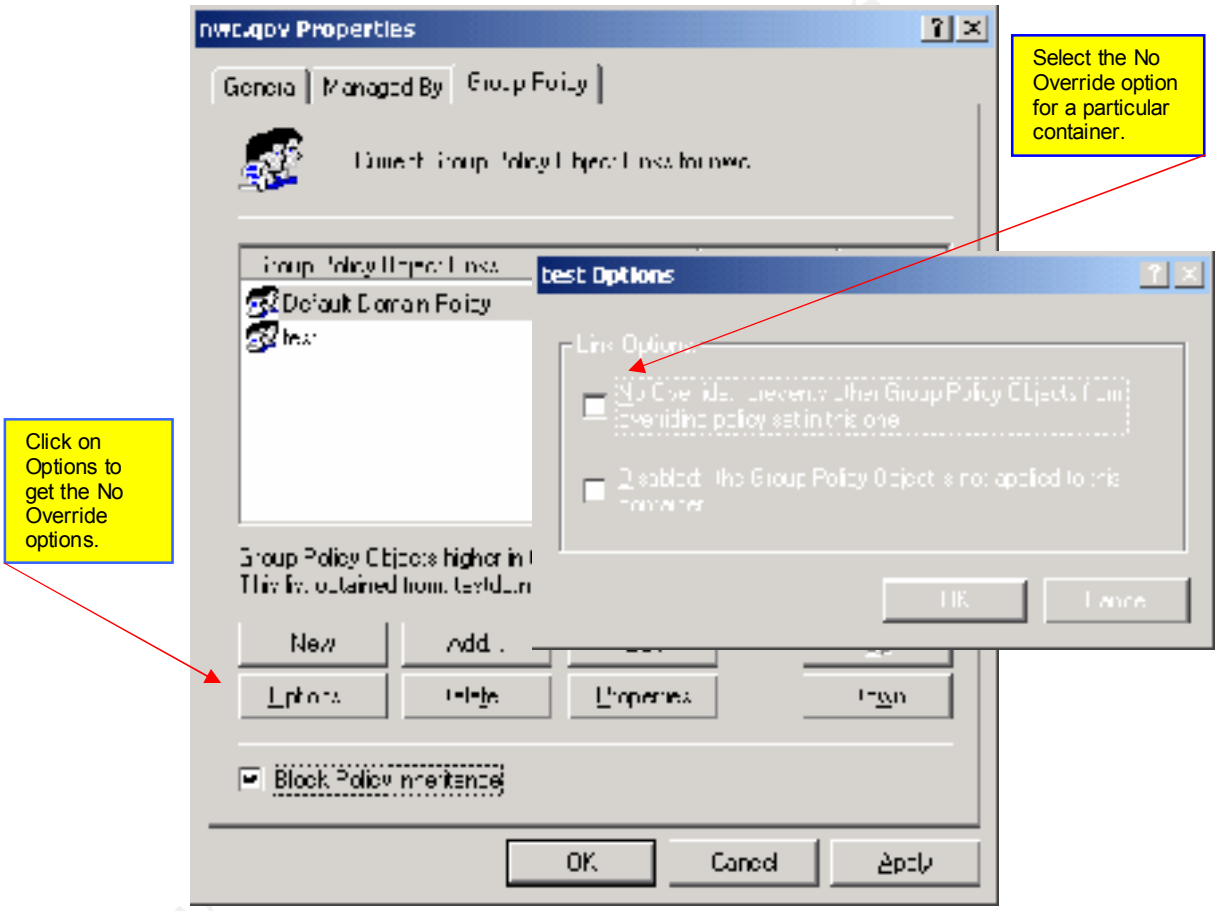


Figure 10 No Override Settings

[15] Wood, Adam. Windows 2000 Active Directory Black Book, Scottsdale(AZ): Coriolis; 2000 301 p

Part III

5. Active Directory

Securing the Active Directory

Under a clean installation of Windows 2000, and properly planned and executed installation of Active Directory, you should have no problems with your security configurations. A system located on the Internet running Active Directory for your corporation should have a solid foundation in regards to System security, Object security and Database security.

System Security
Establish a solid and detailed Group Policy or Local Policies for your systems. When you have strong Group policies in place, they will dictate what password lengths, account lockout procedures, and off-duty restrictions to resources, services, and other factors that can be planned with your Computer Security section. Ensure that everything is running under NTFS protection. Track logon failures at a minimum and backup the results and hold in storage for at least one month.

Object Security
This is possibly the simplest yet most overlooked option to check for the Administrator. By keeping tight tabs on who can administer or who work on your network, you are one step ahead of the game. You Access Control Lists should also be monitored monthly. Ensure that the Everyone group has been removed, since most default installations contain this option.

Database Security
Once again, control who has administrative privileges on your systems. An unfriendly user can access the Ntds.dit file using third party tools to dump passwords hashes or usernames. At a minimum of monthly, audit this file for either attempts, or changes in permissions. Protect your backups, as well since they also contain these files. Ensure top-level protection of your PDC to prevent dual-boot attempts.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

IP Security

Do not fail to overlook the benefits of IPSec on your systems. This little piece of information can prevent hackers or insiders from prying into your systems. IPSec is nothing more than an encrypted form of IP. When you install IPSec onto your systems, it determines how systems will respond to other requests. At a minimum, install the IPSec policy under Group Policies to prevent outside pinging on your machines.

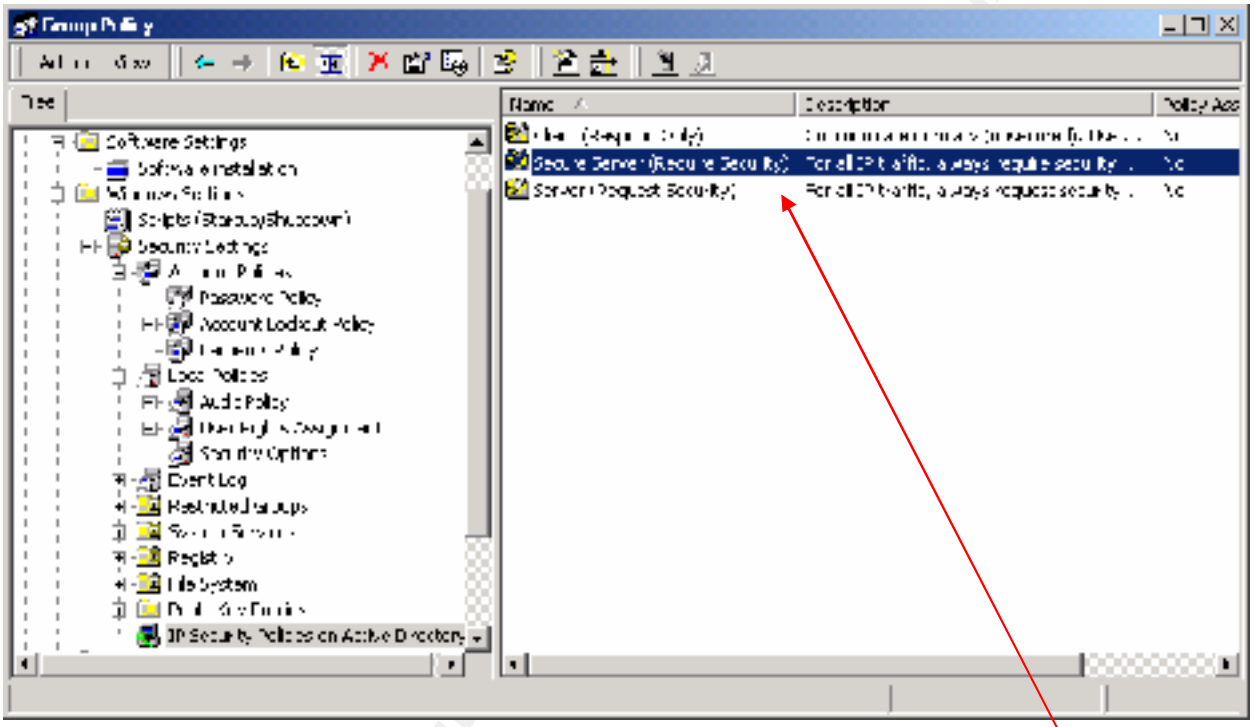


Figure 11 Group Policy IPSec Settings

Once you have selected Secure Server, you have the option of stopping All Traffic, ICMP Traffic, or Dynamic.

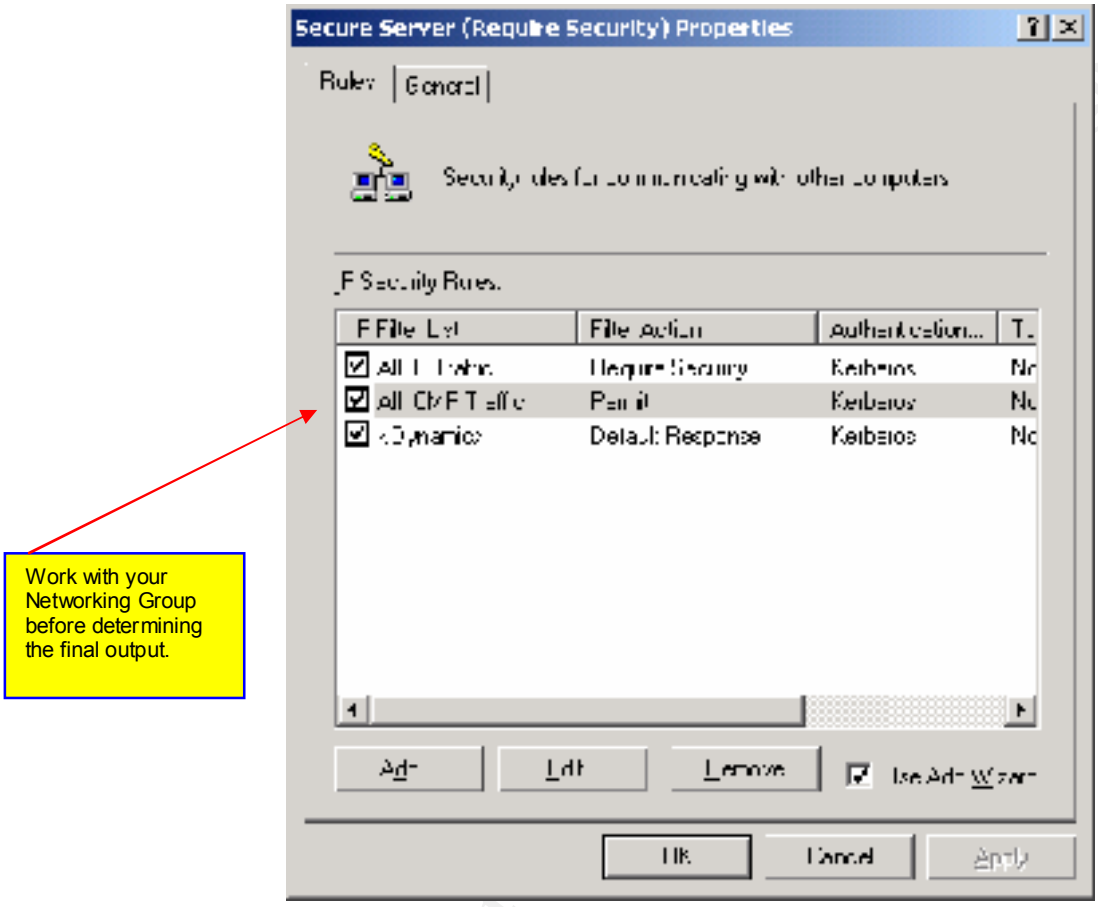


Figure 12 IPSec Security Properties

The setting below will be sufficient for the average network. For larger corporations, the **All IP Traffic** option would benefit the IT department and Computer Security departments, since they have a larger amount of systems and data to manage. For an extremely detailed analysis of IPSec, go to the following site from Microsoft: http://www.microsoft.com/windows2000/library/planning/security/ipsecsteps.asp

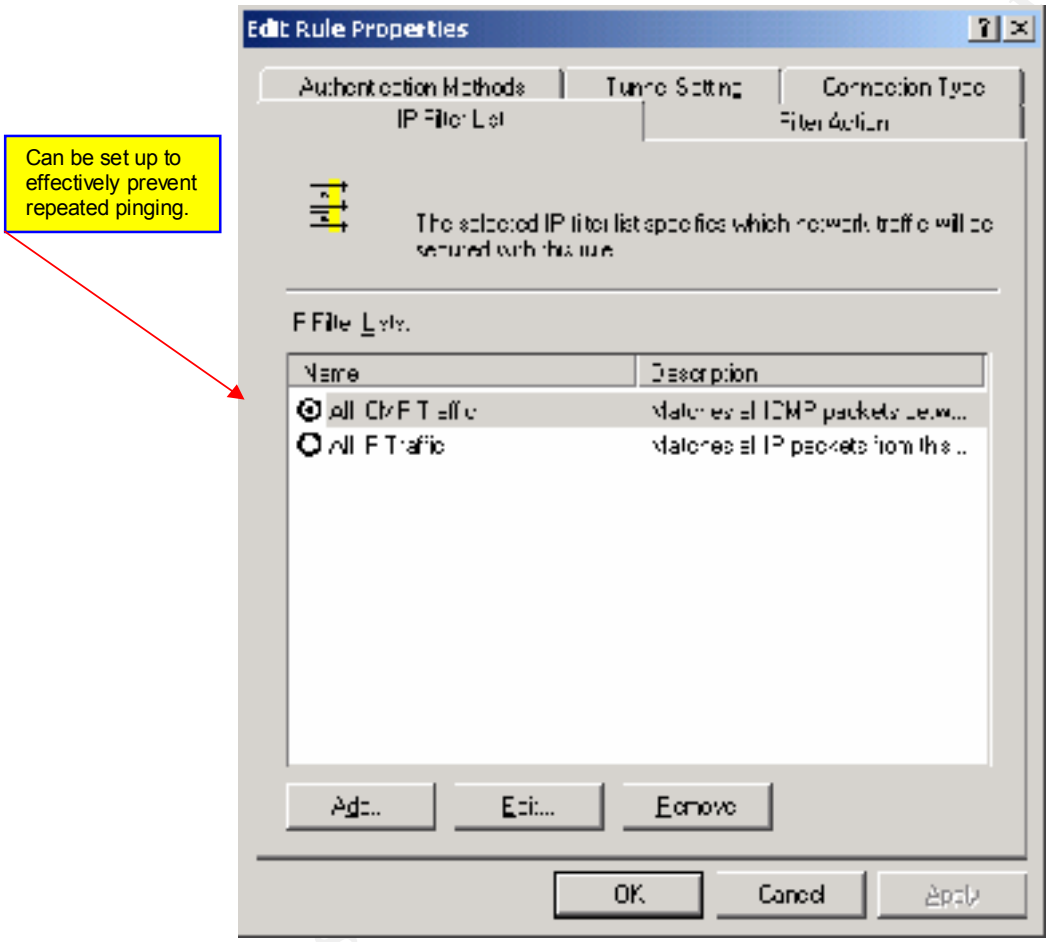


Figure 13 IPSec Filtering

Kerberos vs. NTLM Authentication

In addition to the topics covered previously, there should be some consideration given to NTLM Authentication and Kerberos. As I mentioned before, most of the books assume that you are dealing with a pure Windows 2000 environment. In reality, most corporations are running mixed environments until special applications can be re-written or new third party add-ons are distributed to the computing environment. If you are not familiar with NTLM authentication, then this tidbit of information should help refresh you. In the NTLM atmosphere, which is currently in use by Windows NT 4.0, all of the pertinent information is given an identifier known as a Security Identification Number. These SID's are stored in the Security Accounts Manager database located on your PDC. The Access Control List defines what type of access your users have to resources or other items defined on your networks. Every time the user logs on, the SID is pulled from the SAM presents it in an access token. If your user wants to access to the local scanner, the access list is compared to the token, to see if he or she can gain access.

Kerberos Version 5, as RFC 1510 defines, is the primary security protocol in Windows 2000.[16] Unlike NTLM, Kerberos utilizes the Active Directory instead of Security Accounts Manager. The reason why you the Administrator need to implement Kerberos on your network is primarily due to logons. With Kerberos, a server and client must authenticate when logging on to the domain. This prevents intruders from coming onto your network under impersonation. Kerberos is a shared secret authentication protocol, which means that both the client and another computer, known as the Key Distribution Center (KDC), know passwords.[17]

When Kerberos authenticates logons, it follows this process:

User Credentials Authenticated with the KDC

⇩

KDC issues Ticket Granting Ticket to the Client

⇩

User presents TGT to KDC when resources are needed

⇩

KDC returns Session Ticket

⇩

Key Code Evaluated

⇩

Access Granted to Client if Authenticated

Why is this Kerberos a great feature to add on to your network? The reason is because the authentication process is safer and more reliable. Secondly, it has been established as a standard protocol within the Internet community. Finally, you have the ability to work across various platforms.

[16] Loughry, Marcia, Active Directory for Dummies, Foster City, CA: IDG Books; 2000 145 p.
[17] Loughry, Marcia, Active Directory for Dummies, Foster City, CA: IDG Books; 2000 147 p.

6. Log Files and Auditing

Questions to Ask Yourself

Just like Windows NT 4.0, the event logs allow you to monitor at a minimum security and software problems. They still also allow you to monitor hardware and software changes that are made on a daily basis to your system. The problem with log files is that the tighter you lock your machine down, the more entries you have to go through. It is strongly suggested to choose carefully which auditing event you want. In theory, the System Administrator would be able to check logs daily for vulnerabilities. In the real world, after managing many machines on a daily basis as well as performing additional duties, this simply does not happen. There are third party applications that can screen your logs and pick out what is important based on your settings and allow you to go from there. However, as most corporations work on a tight yearly budget, we will not get into these. We will simply stick to the basics to help your prevent further intrusions.

In Windows 2000, you have the following monitoring logs:

Security –
Records events such as invalid or valid attempts onto the machine. In addition to these, the Administrator of the machine has the capability of selecting various other issues on file permissions.

System –
The system log records daily operations on your Windows 2000 box. For instance, if you removed an application and the drivers failed on logon, this log would record what is happening. If you have network connection errors, this would also be recorded here.

Application –
All applications or programs utilized in Windows 2000 are logged into this area. New to Windows 2000, is the Dr. Watson program error debugger. Although we are very familiar with the errors and the log files it generates, these entries are now listed in the application log file as “Drwtsn32.log”.

Just keep in mind that the logs are placed into their associated topics in sequential order. By this, I mean that from the most recent, to the oldest recorded event. As the Administrator, you are also able to filter your information for specific information. Unlike NT 4.0, the Event Viewer is now accessed in Administrative Tools, then Computer Management.

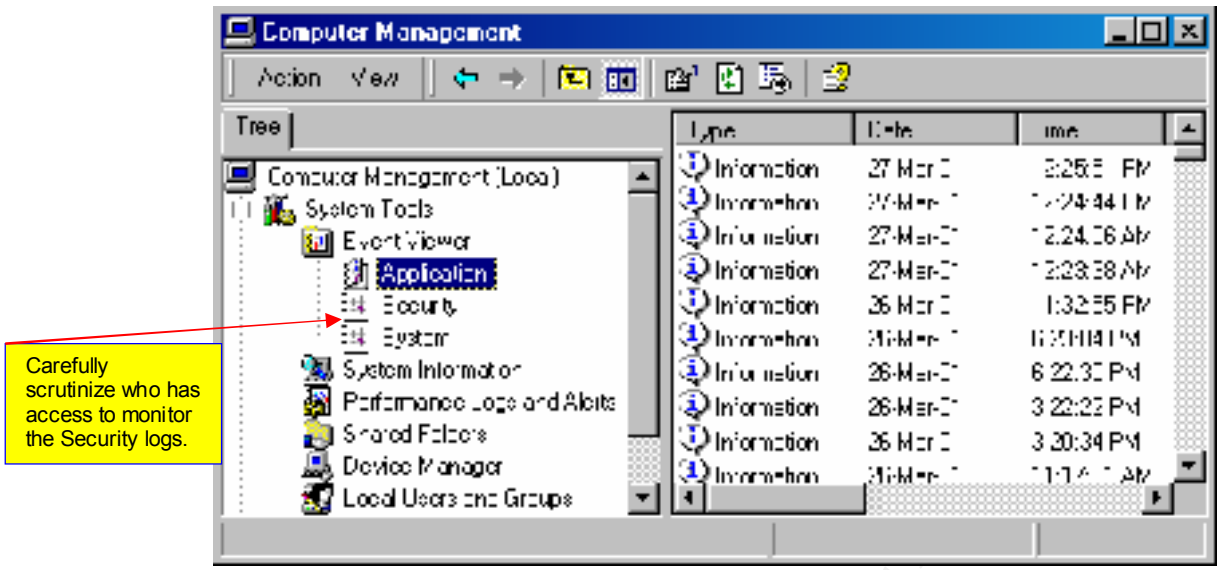


Figure 14 Event Viewer

The first thing to implement before adding items to your log is that of your company's policy on what it wants to monitor. Planning is required on this part. If you log everything, not only do you not have enough time, but you also begin to fill up your log files daily and will have to continuously change the buffer size or the overwrite feature.

The following list is not exhaustive, but includes some of the questions that you need to answer as part of the process of choosing an auditing strategy.[18]

- Why are you auditing?
- Do you need different auditing requirements for different systems?
- Who is responsible for log collection and archive, and should this archive be independent of the system backup?
- Who should have access to audit logs?
- Is the loss of some audit information acceptable?
- How long do you need to keep logs?
- Who is responsible for reviewing audit logs?
- How often should the logs be reviewed?
- Are tools required to assist in the review of the logs?
- What is the escalation procedure when something suspicious is found?
- Does the discovery of some events require immediate notification?
- If you require immediate notification of events, who is going to respond and how?
- Do you need to collect audit logs centrally?
- Do you need to analyze logs from multiple systems simultaneously?

[18] Internet Security Systems. Windows 2000 Security Technical Reference. Redmond (WA): Microsoft Press; 2000 345 p.

Administrators can only access Manage Auditing and Security Log if they have the necessary privileges, which they do by default.[19] Out of all the topics discussed for auditing, perhaps the most significant is that of backing up the log files. It is almost a sure thing that your company will not be able to keep up with logs. If an event does occur, you will be able to go to your backup tapes and determine when the event started or possibly detect a pattern. When backing up the files, you have three choices to choose from. These formats are .txt, .csv, and .evt. In order to keep formats readable, it is strongly suggested to stick with the default of .evt. By default the settings of the Security log are as follows:

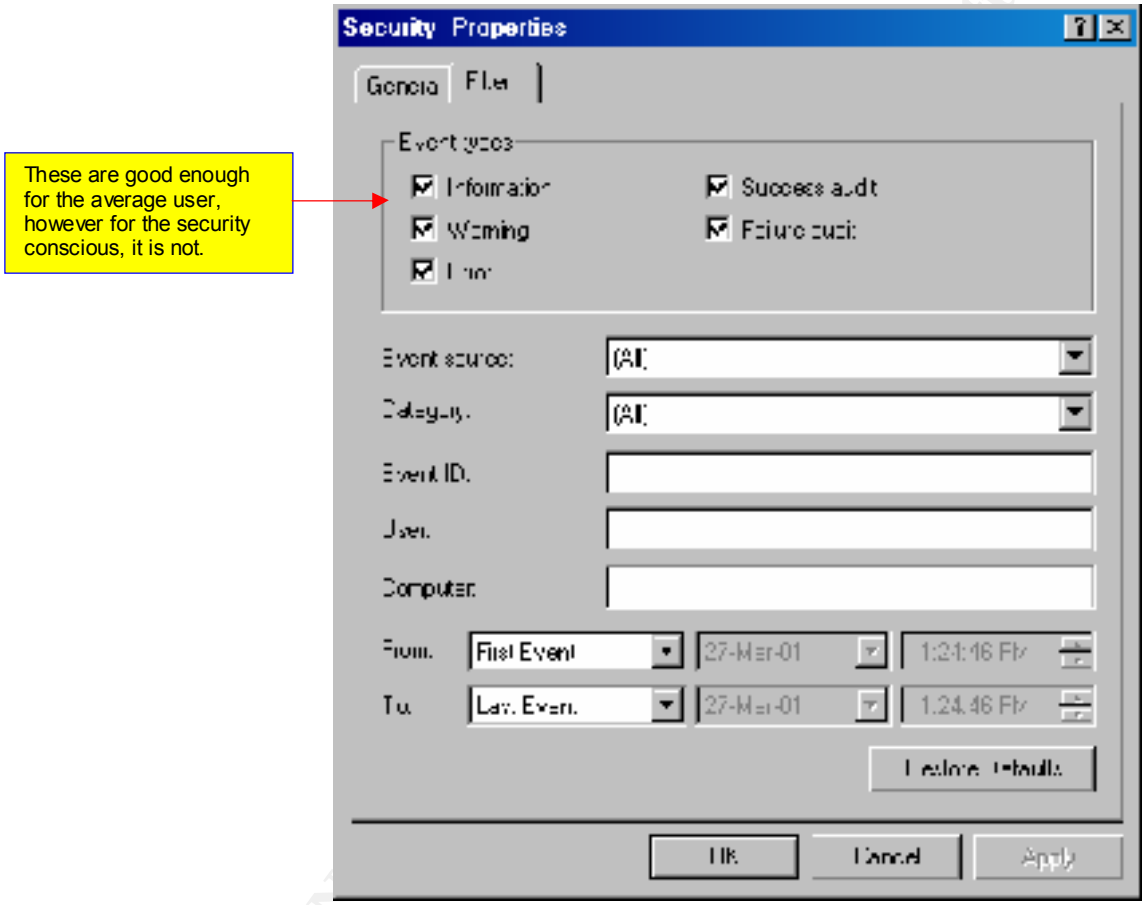


Figure 15 Security Event Default

From a security analyst's perspective, the three broad categories that can be monitored are logon and logoff, object access, and process tracking.[20] These default settings are okay if you are not serious about tracking, however a more effective route is that of Audit Policies.

[19] Internet Security Systems. Windows 2000 Security Technical Reference. Redmond (WA): Microsoft Press; 2000 350 p.
[20] Cox, P. Sheldon, T. Windows 2000 Security Handbook. New York (NY): Osborne/McGraw-Hill; 2000 387 p.

Audit Policies

There are nine different audit policy categories that we can select from.

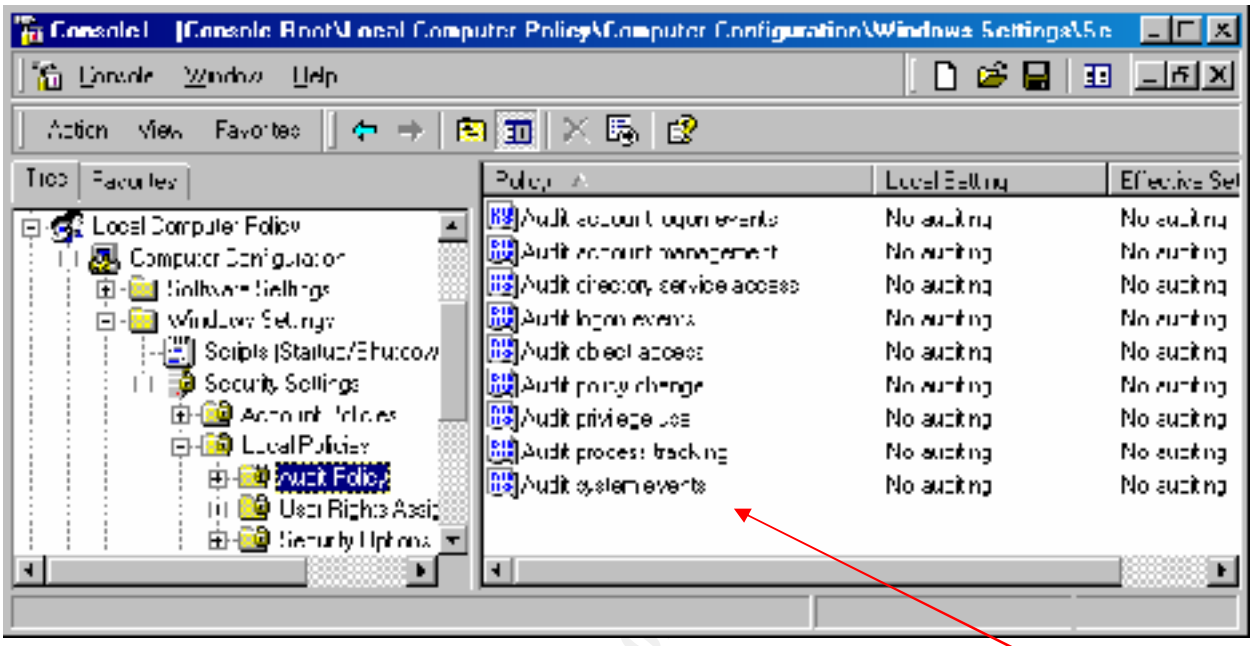


Figure 16 Audit Policy Categories

By default, these are not set. You must choose which categories apply to your corporation.

You must first establish your auditing policy, followed by selecting auditing on specific events. In order to establish the audit policies, you must be a member of the Administrator's group. As the Administrator, you will also have privileges to remotely access your member servers, workstations, and domain controllers. At a minimum the following recommendations will keep you somewhat safe whether you remain stand alone, or hook up to the Internet:

Event Categories	Success	Failure
Audit Account Logon Events	X	X
Audit Account Management	X	X
Audit Directory Service Access		X
Audit Logon Events	X	X
Audit Object Access		X
Audit Policy Change	X	X
Audit Privilege Use		X
Audit Process Tracking		
Audit System Events		X

Figure 17 Recommended Audit Policy Settings[21]

[21] Cox, P. Sheldon, T. Windows 2000 Security Handbook. New York (NY): Osborne/McGraw-Hill; 2000 394 p.

Event Logs

Finally, in addition to a good backup procedure, it is strongly recommended that you go with these guidelines for establishing your Log size settings. These settings will keep your machines from alerting you if this option has been setup, or from dumping critical data during an attempted intrusion from the inside or outside of your corporation.

Log	Domain Controller	File and Print Server	Database Server	Web Server	RAS Server	Workstation
Security Log	5-10 MB	2-4 MB	2-4 MB	2-4 MB	5-10 MB	1 MB
System Log	1-2 MB	1-2 MB	1-2 MB	1-2 MB	1-2 MB	1 MB
Application Log	1-2 MB	1-2 MB	1-2 MB	1-2 MB	1-2 MB	1 MB

Figure 18 Log Size Recommendations[22]

In conjunction with the above table, it is also recommended to increase the overwrite timeframe on your Log settings to the following specifications:

Log	Overwrite Policy Setting
Security Logs	Overwrite events older than 21 days
System Logs	Overwrite events older than 14 days
Application Logs	Overwrite events as necessary

Figure 19 Log Retention Recommendations[23]

The combination of the increased Log size on each event and the additional days should suffice when first installing your system on a stand-alone platform or on the network. It will by your company some time, until you will be able to figure out what is needed and what is not. It will also provide you with some sense of security knowing that you have a record of what is happening on your machine.

[22] Cox, P. Sheldon, T. Windows 2000 Security Handbook. New York (NY): Osborne/McGraw-Hill; 2000 392 p.

[23] Cox, P. Sheldon, T. Windows 2000 Security Handbook. New York (NY): Osborne/McGraw-Hill; 2000 392 p.

7. Conclusion

By sitting down with members of your team, or thoroughly planning current as well as future needs, Microsoft Windows 2000 can be an easy operating system to configure. The small amount of information presented in this document is simply a way to get you started if you have to go on-line immediately. You have found out that simply installing the software and going directly to the Internet is not a wise choice.

Windows 2000 far supersedes Windows NT 4.0 in the areas of default security. The key to this information however, is to plan, plan, and finally plan. The last thing you want to do is assume that your system is not vulnerable to attack from an Internet connection.

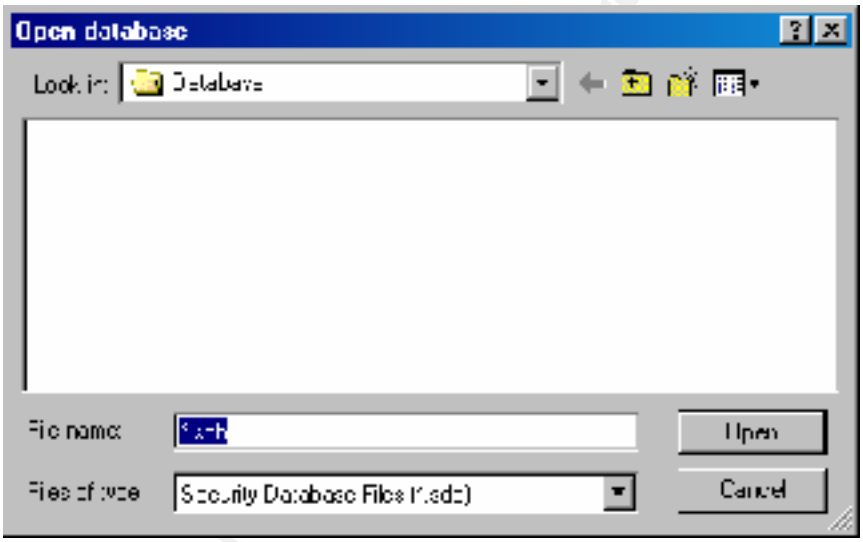
There is plenty of information that is readily available that any Administrator can obtain on the areas of security and tightening down your 2000 systems. For instance Microsoft's white papers offer valuable information for the new Administrator on various security subjects as well as performance topics. With some simple research, there is no reason why you cannot fully implement a secure 2000 environment. Just keep in mind that like education, you must continually stay on top of the latest trends, before an outsider figures out your vulnerabilities.

8. Appendix A

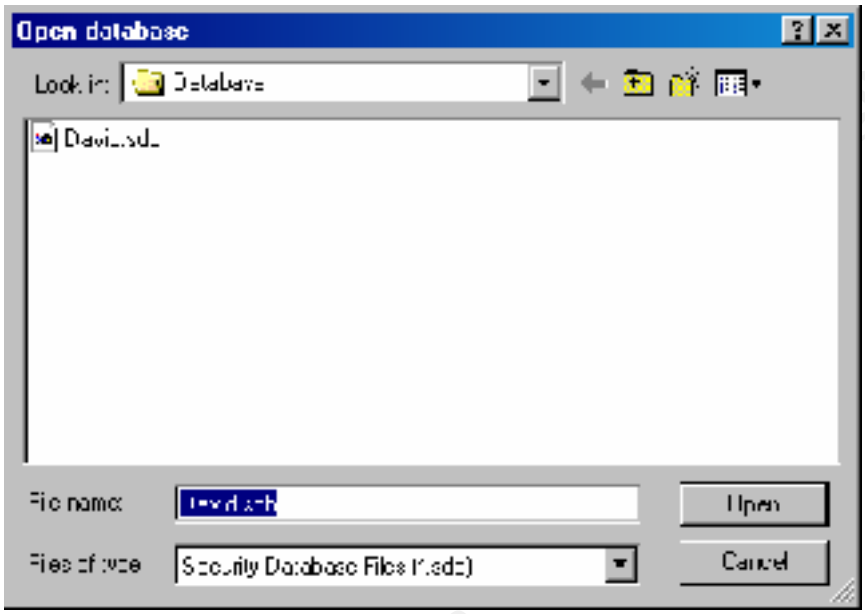
As a means of testing your local security, you can apply a local computer policy as a way of checking for vulnerabilities. For starters, make sure that you completely follow instructions and read all prompts, as it is very possible to end up locking yourself out of your own machine.

To install one the default security templates, follow these steps:

1. Select ***Security Configuration and Analysis*** scope item and right click on it.
2. Choose ***Open Database*.**



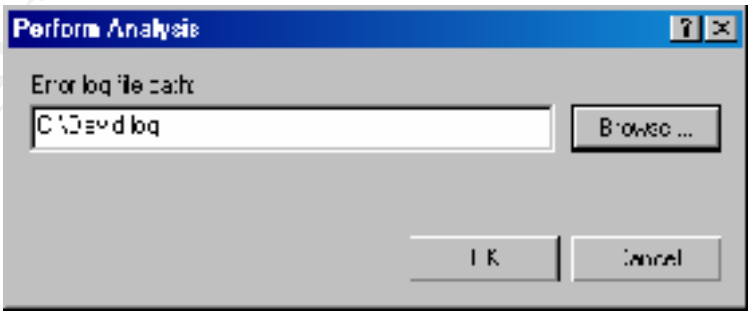
3. In the File name box, type a new database name, and then choose ***Open.***



4. Select a security template to import, and then click ***Open.***

5. Right-click on ***Security Configuration and Analysis***, and choose ***Analyze Computer Now.***

6. In the ***Perform Analysis*** dialog box, choose a safe location for the log file that will analyze your system, and choose ***OK***.



When all of the analysis is completed on your system, you can choose to configure your system by different methods. The most popular method for a new Administrator would be to configure the database you selected to match your current

configuration at this point. In order to perform this operation, all you need to do is double-click the current settings in the windowpane that shows up.

9. References

The following books and articles were utilized in the writing of this document.

Active Directory for Dummies, by Marcia Loughry, IDG Books, ISBN: 0-7645-0659-5, (2000)

Microsoft Windows 2000 Security Technical Reference, by Internet Security Systems Inc., Microsoft Press, ISBN: 0-7356-0858-X, (2000)

Windows 2000 Active Directory Black Book, by Adam Wood, Coriolis, ISBN: 1-57610-256-4, (2000)

Windows 2000 Security Handbook, by Phillip Cox and Tom Sheldon, Osborne-McGraw Hill, ISBN: 0-07-212433-4, (2001)

Windows 2000 Security Little Black Book, by Ian McLean, Coriolis, ISBN: 1-57610-387-0, (2000)

Windows 2000 Security, by Roberta Bragg, New Riders, ISBN: 0-7357-0991-2, (2000)

Q217050 – Description of Default Security Settings in Windows 2000, Last Reviewed: January 26, 2001

Q234926 – Windows 2000 Security Templates Are Incremental, Last Reviewed: December 30, 1999

Microsoft White Paper - Group Policy Simplifies Administration, Posted: Thursday, November 04, 1999

Microsoft White Paper – Step-by-Step Guide to Understanding the Group Policy Feature Set, Posted: Monday, January 31, 2000

Microsoft White Paper – Step-by-Step Guide to Using the Security Configuration Tool Set, Posted: Wednesday, February 16, 2000

Microsoft White Paper – Active Directory Users, Computers, and Groups, Posted: Tuesday, February 29, 2000

Q274305 – Free Windows 2000 Resource Kit Tools for Administrators, Last Reviewed: October 26, 2000