GIAC CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Securing Windows and PowerShell Automation (Security 505)"
at http://www.giac.org/registration/gcwn

Securing Windows 2000 Professional Desktops in a Development Environment

GCNT Practical Assignment
Version 3.0
Option 2 – Securing Windows 2000 with Security Templates

© SANS Institute 2000 - 2005, Author retains full rights.

Steven R. Sheldon
January 29, 2001

© SANS Institute 2000 - 2005 Author retains full rights.

Table of Contents

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Introduction

Over the past several years the task of maintaining a corporate network has become more tedious, despite significant improvements in the stability and reliability of the software and hardware. In our organizations we have had to deal with much more than just physical security and misuse of computing resources, but also wide spread viruses and the more recent threats of damaging worms.

To make the task even more of a challenge, I work in a development group which means virtually every user is a local administrator and experimenting with a variety of software. This tends to cause frequent rebuilds of the machines in order to maintain them with the appropriate version levels of software. This can be a fairly tedious process if one doesn't have a method for automating the installation and configuration of the machine.

There are a variety of tools we may use to automate the installation of the software to the machine, but modifying system settings to secure the workstation against threats can be extremely tedious. Fortunately Windows 2000 provides a number of new features to aid in the configuration of the desktop. One of the most important is the introduction of Group Policies in the Active Directory to assist in automatically maintaining system settings.

This document will address how to use Group Policies to automatically configure security settings on a developer desktop. First, we will start by evaluating the needs of the desktop environment, and then create a security template, which can be used to meet those needs. We will then proceed to test the automatically configured environment, and evaluate its effectiveness.

Windows 2000 Workstation for Developers

Hardware Configuration

The type of desktop used as a development workstation is not unique. It is typically a

© SANS Institute 2000 - 2005 Author retains full rights.

standard desktop computer from a major vendor such as Dell or Compaq. Usually it is a more powerful Pentium III with more than the usual amount of memory.

Not being able to obtain a suitable test computer, for this exercise the test environment was created virtually using a product called VMware 3.0[1]. This is a very useful utility that works exceptionally well for testing software configurations that are not hardware specific, which is the case for this exercise.

With VMWare, a new Virtual Machine was created, configured with Windows 2000 Professional as the Guest operating system. 256 Megs of RAM was allocated to this environment, the max drive size was set to 4 Gigs and bridged networking was used to allow the virtual computer to connect to the test LAN.

System Software

Microsoft Windows 2000 Professional
NTFS Partition created during install
Internet Information Services 5.0 (See Appendix D for further configuration options)
Microsoft Data Access Components v2.6sp1
Applicable service packs and updates as of 26-Dec-01 (See Appendix A)

Application Software

Microsoft Office 2000
Microsoft Visual Studio 6.0
Internet Explorer 5.5 SP2
Adobe Acrobat Reader 5.0
Oracle 8i (8.1.7) SQLNet Client
Applicable service packs and updates as of 26-Dec-01 (See Appendix B)

Security Software

Norton Antivirus 2002
Applicable service packs and updates as of 26-Dec-01 (See Appendix C)

System Role

The role of the developer desktop is fairly broad. It is most commonly used for the development and localized testing of n-tier applications intended for deployment to IIS web servers. In addition it may be used to install and evaluated third party applications, developer tools and so forth. Because of this, the end user of the workstation is most typically setup as a local administrator and must have permissions to change most everything.

It is considered the responsibility of the developer that they document any substantial configuration changes made to the machine, as well as ensure that the security mechanisms of the desktop(such as virus scanning) are kept in place and functional.

This creates a relatively hostile environment, and without careful configuration has been proven to be a source of frustration. The recent Code Red and Nimda worms in

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

particular spread rapidly across such machines if the same care to protect the production IIS servers is not also applied to these development machines.

Furthermore in a development environment it is quite common for there to exist Company Confidential information on the machines. This primarily consists of source code, but may include other data or documentation. Therefore physical security is a concern, specifically unauthorized access to the machine on or off the network.

Checklist Selection

As explained in the section describing the system's role, the security configuration needs of these machines are somewhat unique. In terms of protecting the machine from the end user, the security needs are minimal as they will be a local admin and have need to modify many aspects of the system. However, we do want to protect the machine from unanticipated influences such as worms or viruses as well as unauthorized usage.

A number of security templates included with Windows 2000 were evaluated, specifically the basicws.inf, securews.inf and hisecws.inf. The high security template is too intrusive for our developer environment as it configures the machine such that it can no longer be accessed by older workstations. There are still NT4 workstations in the environment, and interoperability must be maintained. The securews.inf and basicws.inf offer reasonable baselines to work with.

There are also a variety of checklists available including one from SANS[2], but while very detailed they were not suitable to our needs and required a great deal of further modification. Microsoft has provided a very basic checklist entitled "Windows 2000 Professional Baseline Security Checklist"[3] which can be found at Microsoft's security website under the Tools and Checklists[4] section.

A decision was made to utilize the checklist from Microsoft because it provided a very general security base, and highlighted security policies as well as security configuration items. Using this checklist a custom template could be created and applied to our development workstations.

The Windows 2000 Professional Baseline Security Checklist

Many of the recommendations provided in this checklist are process related, but many of them are configuration items for a security template. Each item will be identified as to whether it needs to be configured in the security template, or if the action is process related.

<u>Verify that all disk partitions are formatted with NTFS</u>

This is of particular importance, since many of the security configuration items cannot be performed with a FAT or FAT32 partition. It is also important to note that Windows 2000 must be installed initially to a NTFS partition in order for the default file system ACLs to be put in place. Using the convert utility will result in all files being set to

© SANS Institute 2000 - 2005 Author retains full rights.

Everyone: Full Control.

In our particular case, the drive was installed as NTFS. However just in case we will make certain to include the default file system ACLs as part of our security template in case one was to use convert in the process of an install.

Decision: Procedural. Install operating system with NTFS initially.

Verify that the Administrator account has a strong password

The checklist advises to use a longer password preferably at least nine characters long which includes at least one punctuation mark or nonprinting character in the first seven characters. This seven character recommendation is because of the peculiarities of the rather weak LANman hash[5]. It also goes on to say the password should not be synchronized across multiple computers, and that different passwords should be used on each computer to raise the level of security in the workgroup or domain.

I'm not certain how one would best handle this. In a large environment with many desktops, using a different password on each machine would be very difficult to keep track of. However one could relatively easily derive a password from a common string and something specific to the desktop, such as the asset identifier. This would not protect all of the desktops in the domain against a human attack; however it would probably discourage a worm from spreading from one machine to another.

Decision: Procedural. Develop policy for setting Administrator account passwords.

Disable unnecessary services

The checklist advises that we should disable any network services not required for the computer; specifically it mentions IIS 5 web services.

In our particular case we want the IIS 5 Web Services to be running, however we probably do not need the FTP or SMTP Services if they are installed, so we will add these services to our checklist. They will be set to Manual, just in case the developer does find themselves needing them they can start them up easily.

Decision: In our security template we will define settings for the Web, FTP and SMTP Services.

Disable or delete unnecessary accounts

Review the list of active accounts on the system and disable, or delete any non-active accounts.

In our particular case, there are 5 accounts on the computer after installing our software configuration. Administrator, Guest, IUSR_<computername>, IWAM_<computeruser> and VUSR_<computername>. All of these with the exception of Guest are necessary. While the security templates allow you to restrict who is added to groups, there is no way to configure accounts. Therefore we will rely upon

© SANS Institute 2000 - 2005 Author retains full rights.

the Guest account being disabled by default.

Decision: Procedural. Develop policy on local account creation.

Protect files and directories

The default permissions from the Windows 2000 installation[6] are adequate to protect the system in our environment. As discussed earlier in relation to the use of a NTFS, we should have the default file system permissions as part of our template.

However, because this is a development desktop it will have local copies of source code that may be sensitive. It would probably be a good idea to identify a standard location for the source code to be saved locally, and then specify permissions on that directory. Also depending on the sensitivity of the source code, it may be worth investigating the Encrypted File System to help protect the file in case the machine is physically stolen from the office.

Additionally because of the installation of IIS, it would be wise to tighten down the permissions on the c:\inetpub directory. Looking at the default directories created during install, I choose to configure them as such:

Folder Name	Administrators & System	Everyone
C:\inetpub	Full Control	None
C:\inetpub\AdminScripts	Full Control	None
C:\inetpub\ftproot	Full Control	Read & Execute
C:\inetpub\iissamples	Full Control	None
C:\inetpub\mailroot	Full Control	None
C:\inetpub\Scripts	Full Control	None
C:\inetpub\wwwroot	Full Control	Read & Execute

These permissions should allow the services to function and aid in protecting against possible IIS worms. Additional permissions may be necessary for the use of the SMTP service; this is largely dependent upon how it will be utilized as CDONTS will require the user sending the mail to have write permissions to the mailroot\pickup directory.

Decision: Include default Windows 2000 file system permissions in template. Define location (c:\source) and permissions (Administrators:Full only). Define permissions for inetpub directories as specified in table.

Make sure the Guest account is disabled

The Guest account should already be disabled.

Decision: Procedural. Verify account remains disabled.

Protect the registry from anonymous access

© SANS Institute 2000 - 2005 Author retains full rights.

The checklist advises that we should protect from anonymous access to the registry. It discusses the registry key associated with this, but then points out that by default Windows 2000 already restricts access to the Administrators and Backup Operators groups. The recommendation is to limit this access to the Administrators group only.

Decision: Change registry permissions on HKLM\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg to Administrators:Full only.

Apply appropriate registry ACLs

The default permissions from the Windows 2000 install are adequate to protect the system in our environment. We should have the default registry ACLs as part of our security template as a precaution.

Decision: Include Windows 2000 default registry ACLs in our security template.

Restrict access to public Local Security Authority (LSA) information

The checklist advises us to restrict anonymous access to the LSA. By default the LSA permits anonymous access, which means that anybody could connect to the machine remotely and retrieve a list of userids and their attributes. The checklist refers to the registry entry HKLM\SYSTEM\CurrentControlSet\LSA\RestrictAnonymous and indicates that the value should be set to 1. The value of 1 refers to "Do not allow enumeration of SAM accounts and names" under the "Additional restrictions for anonymous connections" of the Security Options in our security template.[7]
Upon investigating this setting further, it was found that the value of 1 does not completely eliminate the security opening. In an article on SecurityFriday.com[8], a tool named GetAcct is provided which will grab the account names and properties despite the fact that the RestrictAnonymous registry entry has been set to 1. The tool does not work if this is set to "No access without explicit anonymous permissions."

This extra strict setting should not cause any undue side-effects. If this machine were a domain controller it would not be appropriate if we had pre-Windows 2000 machines in our environment as they would be unable to logon to the domain. But since this is just a desktop, there is no need for this backwards compatibility.

Decision: In our security template, set the "Additional restrictions for anonymous connections" settings to "No access without explicit anonymous permissions."

Set stronger password policies

The checklist recommends using the Local Security policy to strengthen the password policies. The checklist suggests the following 4 items be changed:

- Minimum password length should be set to at least 8 characters.
- Minimum password age should be set to an appropriate value.
- Maximum password age should be set to an appropriate value, no more than

© SANS Institute 2000 - 2005 Author retains full rights.

42 days.

- Password history should be set to at least 6.

One item that is important but not explicitly mentioned in the checklist is the setting ‘Passwords must meet complexity requirements’, which forces the password. Enabling this setting enforces that passwords meet the following three conditions[9]:

1. Passwords must be at least six (6) characters long.
2. Passwords must contain characters from at least three (3) of the following four (4) classes:

Description	Examples
English upper case letters	A, B, C, ... Z
English lower case letters	a, b, c, ... z
Westernized Arabic numerals	0, 1, 2, ... 9
Non-alphanumeric ("special characters")	such as punctuation symbols

3. Passwords may not contain your user name or any part of your full name.

Since our particular environment is a local desktop which is connected to a domain, we shouldn’t have too many local accounts beyond Administrator, Guest and the accounts used by IIS. Even so, if the enduser does create new local accounts it is best to ensure they do not introduce security backdoors.

Decision: Set minimum password length to 8, minimum password age to 1, maximum password age to 42 and password history to 6. Also enforce password complexity.

Set account lockout policy

The checklist recommends that we set the account lockout feature to disable the account after 3 to 5 failed attempts, reset the count after 30 minutes, and the lockout duration to forever.

The checklist also mentions that by using the passprop.exe tool in the Windows NT Server Resource Kit you may change an additional setting that allows the Administrator account to be locked out. I’m not going to pursue this at this time, as our desktops are not typically subjected to those sorts of attacks. This is more of an issue for domain accounts, or with web servers.

Decision: In our security template, set the account lockout feature to disable account after 5 failed attempts, reset count after 30 minutes and set the lockout duration to forever.

Configure the Administrator account

This item in the checklist advises that we should rename the Administrator account to something not so obvious. It also suggests creating a new account named Administrator to act as a decoy.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

There is an option titled ‘Rename administrator account’ in the security options, but it would be more difficult to automate the creation of a decoy account.

The checklist does not mention renaming the Guest account, but as that option is also provided in the security options it was decided to utilize that as well in the security template.

Decision: Set the ‘Rename administrator account’ property in our security template, as well as the ‘Rename guest account’. Use “srsuser” for the Administrator account and something innocuous for the guest account like FredUser.

Remove all unnecessary file shares

The checklist advises that unnecessary file shares to prevent malicious users from accessing data, or the local system. This is mostly a procedural step, as any user with at least Power User access rights can share a local directory. Disabling the ability to share folders will prevent our users from being able to do their job, so we’ll simply have to instruct them to be careful.

Decision: Procedural

Set appropriate ACLs on all necessary file shares

Again referring to file shares, the checklist points out that by default the share level permissions are Everyone:Full, which is not a good setting. Unfortunately after researching the issue there appears to be no way to change this default, so we are presented with a procedural issue of relying upon the users to set share level permissions correctly.

Decision: Procedural

Install antivirus software and updates

The checklist points out that it is absolutely necessary to install and maintain up to date antivirus software. For our desktop Norton Antivirus 2002 was chosen as the anti-virus solution. This product has a mechanism to automate the downloading of patches and updated virus definition files from the internet. In a live environment one would purchase a corporate version of the antivirus product which would allow you to automate the distribution of updates via your own internal servers. This allows for testing of an update before deployment, plus it reduces the traffic on your Internet connection.

Decision: Procedural. Install antivirus software and download updates. (See Appendix C)

Install the latest Service Pack

Service Packs are a combination of all the released fixes up to that point and time for the operating system. It is imperative to keep up to date with these fixes in order to

© SANS Institute 2000 - 2005 Author retains full rights.

protect against security vulnerabilities. The checklist provides the following link to the Windows 2000 Service Pack 2 files:

http://www.microsoft.com/windows2000/downloads/servicepacks/sp2/

Decision: Procedural. Verify Windows 2000, SP2 is installed on test system.

Install the appropriate post-Service Pack security hotfixes

The checklist mentions the Microsoft Security Notification Service[10] which will send out emails notifying you of critical issues relating to Microsoft's products. When these bulletins are issued, it is important to read them and understand if and how you are impacted and if necessary follow the recommendations to patch or workaround the problem, as necessary.

Microsoft has provided a number of tools to help with the installation of security hotfixes. The most prominent is WindowsUpdate, which is prominently displayed in the Windows 2000 Start Menu, or otherwise available at http://windowsupdate.microsoft.com. This service is primarily intended for individual users. Patches generally appear on this site 2-3 days after the bulletins have been issued.

The other tool, which is most useful, is HFNetchk[11], this is a command line tool, which compares the present system against an online XML database to insure it is up to date. A report is generated listing each security bulletin that should be addressed. Further information on how to use to tool, as well as a link to download it, is available at this site:

http://support.microsoft.com/directory/article.asp?ID=KB;EN-US;q303215

Appendix A shows how to use the tool, and provides an example of its output.

Decision: Procedural. Run HFNetchk and obtain a list of appropriate hotfixes to install.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005

Author retains full rights.

Template Creation

From our review of the Windows 2000 Baseline Security Checklist the following items need to be included in our template:

- Define startup settings for the IIS Web, FTP and SMTP services.
- Include default Windows 2000 file system permissions. Define additional folder c:\source and set permissions to Administrators:Full only. Define permissions for the c:\inetpub as specified.
- Change registry permissions on HKLM\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg to Administrators:Full only.
- Include Windows 2000 default registry ACLs in our security template.
- In our security template, set the “Additional restrictions for anonymous connections” setting to “No access without explicit anonymous permissions.”
- Set minimum password length to 8, minimum password age to 1, maximum password age to 42 and password history to 6. Also enforce password complexity.
- In our security template, set the account lockout feature to disable account after 5 failed attempts, reset count after 30 minutes and set the lockout duration to forever.
- Set the ‘Rename administrator account’ property in our security template, as well as the ‘Rename guest account’. Use “srsuser” for the Administrator account and a random string for the guest account.

It is easier to start a template by building upon an existing one. Given what we’ve discussed so far, we want to start with a template which includes the default permissions for both the file system and registry. Of the templates available from Microsoft, the basicwk.inf template defines the default Windows 2000 settings, especially the file system and registry permissions and makes a good base template.

The first step to creating our new template is to load the Security Templates applet. This applet is not one of the default icons under the Administrative tools, but is available as a Snap-in within the Microsoft Management Console(MMC). The simplest way to gain access to this tool is to run mmc.exe from the Start -> Run dialog, and then proceed into the Console menu and Add the Security Templates snap-in. The MMC is very powerful and the interface to these administrative Snap-in tools can be customized for your own individual needs. A brief description of how to customize the MMC can be found in knowledge base article Q230263[12].

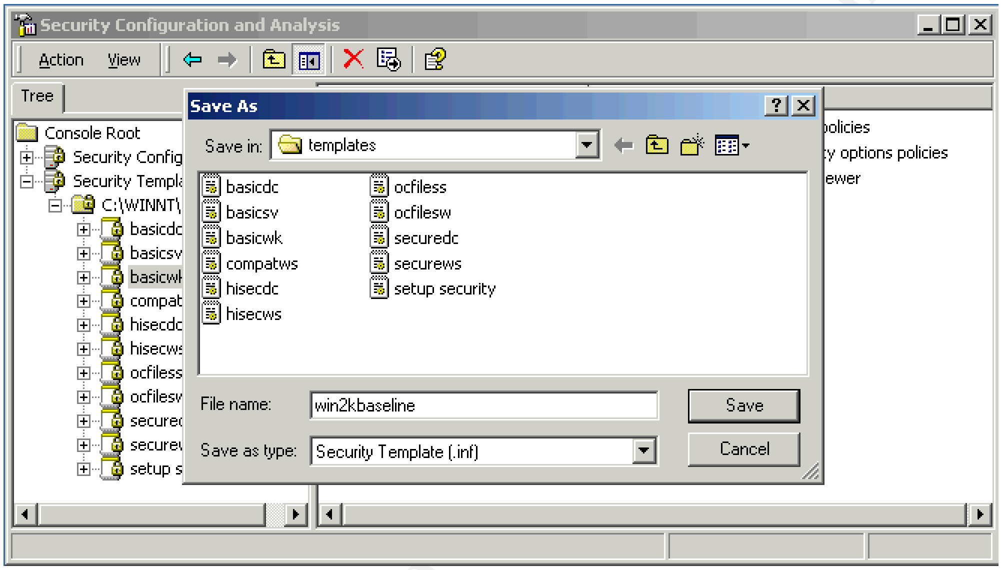
Note: It is generally best if you create the template on a Windows 2000 desktop

© SANS Institute 2000 - 2005

Author retains full rights.

configured the same as your target machine. This makes it easier to modify settings for file and registry permissions, services and such because they will be available in the browse window.

Once in the Security Templates Snap-in, we first copy the existing basicwk.inf template to a new name. This is done by right clicking on the item and selecting SaveAs. A dialog box will then appear asking you for a new filename. For our purposes I choose to name this win2kbaseline.inf.


Save As

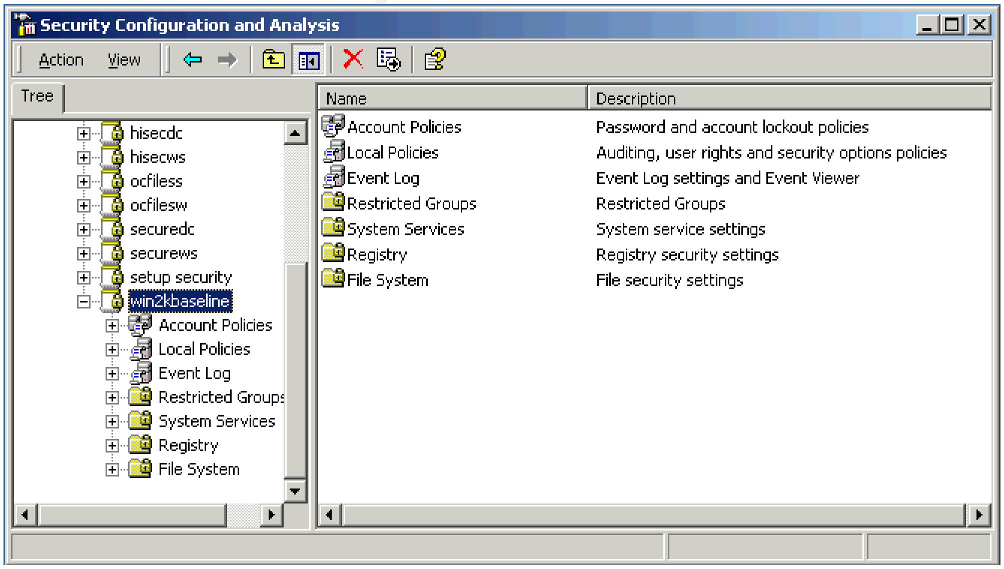
Save in: templates

basicdc	ocfiless
basicsv	ocfilesw
basicwk	securedc
compatws	securews
hisecdc	setup security
hisecws	

File name: win2kbaseline

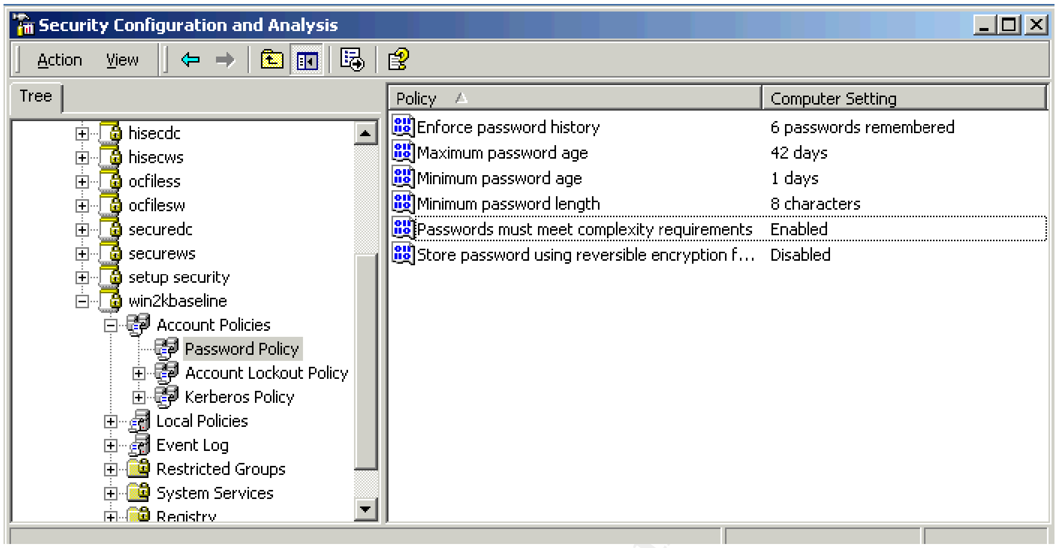
Save as type: Security Template (.inf)

After the new file is created, select it and expand the options underneath it.


Name	Description
Account Policies	Password and account lockout policies
Local Policies	Auditing, user rights and security options policies
Event Log	Event Log settings and Event Viewer
Restricted Groups	Restricted Groups
System Services	System service settings
Registry	Registry security settings
File System	File security settings

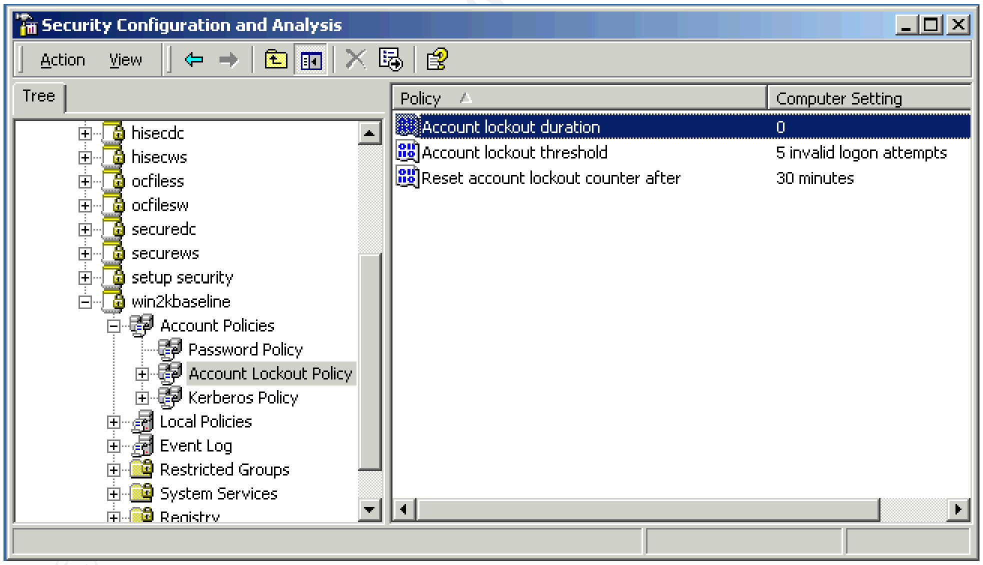
© SANS Institute 2000 - 2005 Author retains full rights.

The settings for stronger password policies are found under the Account Policies section. Expand this section, and change the settings as we have discussed.



Policy	Computer Setting
Enforce password history	6 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	8 characters
Passwords must meet complexity requirements	Enabled
Store password using reversible encryption f...	Disabled

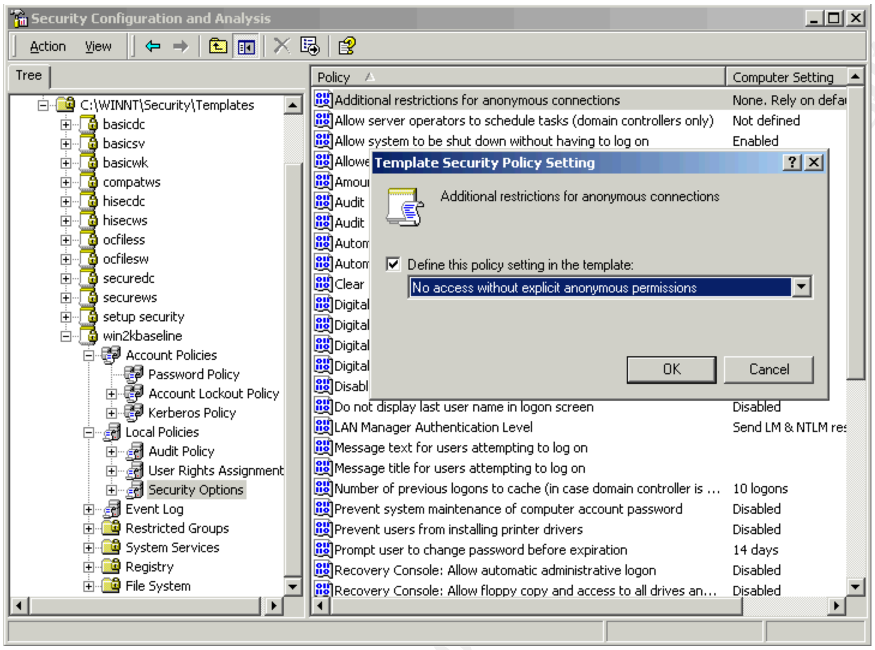
The settings for account lockout policy are found in the next tab down also under the Account Policies section.



Policy	Computer Setting
Account lockout duration	0
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	30 minutes

© SANS Institute 2000 - 2005 Author retains full rights.

The settings for “Additional restrictions for anonymous connections”, “Rename administrator account” and “Rename guest account” are found under the Local Policies section.



Policy	Computer Setting
Additional restrictions for anonymous connections	None. Rely on defa
Allow server operators to schedule tasks (domain controllers only)	Not defined
Allow system to be shut down without having to log on	Enabled
Allowe	
Amou	
Audit	
Audit	
Autor	
Autor	
Clear	
Digital	
Digital	
Digital	
Digital	
Disabl	
Do not display last user name in logon screen	Disabled
LAN Manager Authentication Level	Send LM & NTLM res
Message text for users attempting to log on	
Message title for users attempting to log on	
Number of previous logons to cache (in case domain controller is …	10 logons
Prevent system maintenance of computer account password	Disabled
Prevent users from installing printer drivers	Disabled
Prompt user to change password before expiration	14 days
Recovery Console: Allow automatic administrative logon	Disabled
Recovery Console: Allow floppy copy and access to all drives an…	Disabled

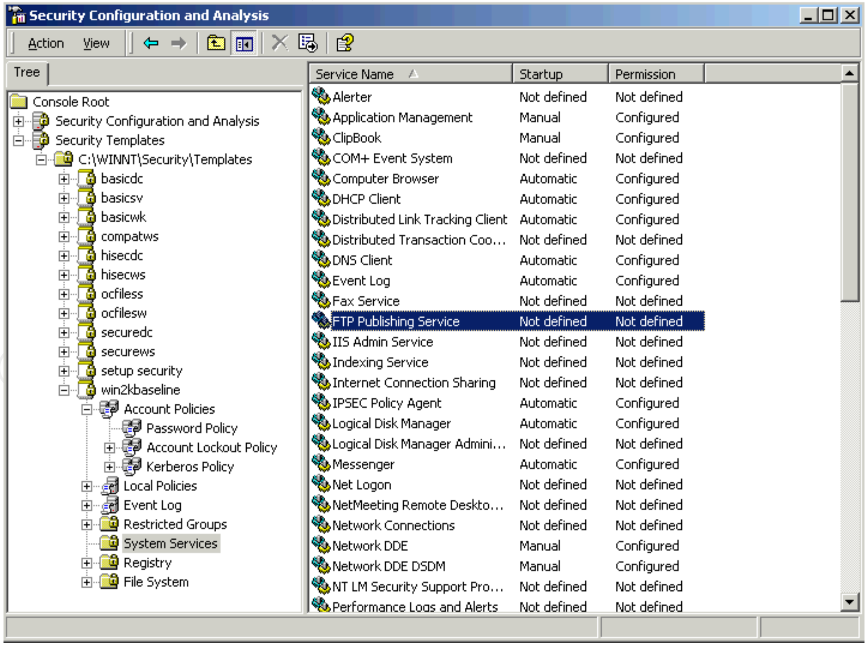
Template Security Policy Setting

Additional restrictions for anonymous connections

☑ Define this policy setting in the template:

No access without explicit anonymous permissions

Under the System Services section we change the settings for the IIS Web, FTP and SMTP Services. These services will appear in this list only if you are running the Security Templates editor on a desktop which has IIS installed. By default they are listed as ‘Not Configured’.



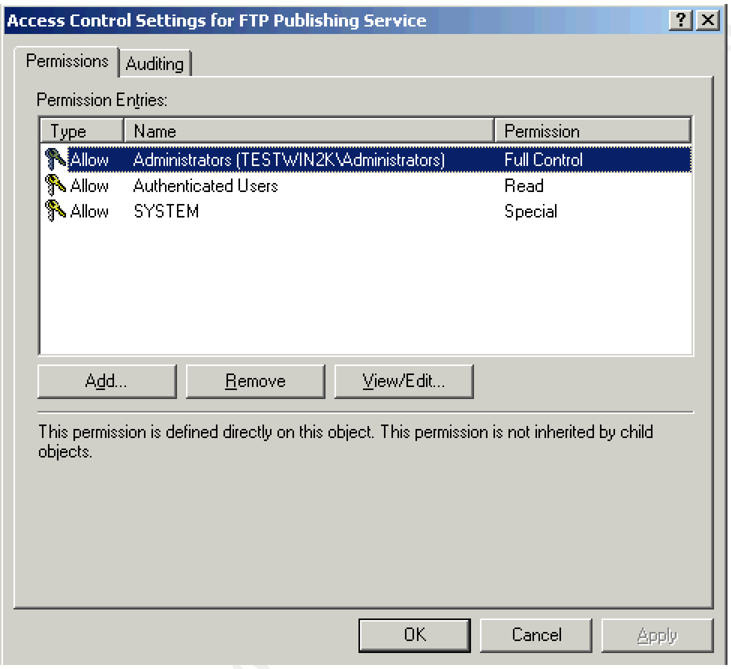
Service Name	Startup	Permission
Alerter	Not defined	Not defined
Application Management	Manual	Configured
ClipBook	Manual	Configured
COM+ Event System	Not defined	Not defined
Computer Browser	Automatic	Configured
DHCP Client	Automatic	Configured
Distributed Link Tracking Client	Automatic	Configured
Distributed Transaction Coo…	Not defined	Not defined
DNS Client	Automatic	Configured
Event Log	Automatic	Configured
Fax Service	Not defined	Not defined
FTP Publishing Service	Not defined	Not defined
IIS Admin Service	Not defined	Not defined
Indexing Service	Not defined	Not defined
Internet Connection Sharing	Not defined	Not defined
IPSEC Policy Agent	Automatic	Configured
Logical Disk Manager	Automatic	Configured
Logical Disk Manager Admini…	Not defined	Not defined
Messenger	Automatic	Configured
Net Logon	Not defined	Not defined
NetMeeting Remote Deskto…	Not defined	Not defined
Network Connections	Not defined	Not defined
Network DDE	Manual	Configured
Network DDE DSDM	Manual	Configured
NT LM Security Support Pro…	Not defined	Not defined
Performance Logs and Alerts	Not defined	Not defined

Change the ‘IIS Admin Service’ and ‘World Wide Web Publishing Service’ to start

© SANS Institute 2000 - 2005 Author retains full rights.

automatically, and the ‘FTP Publishing Service’ and ‘Simple Mail Transport Protocol (SMTP)’ service to start manually. You will also be prompted in each case to set security on these services. Security should be set to Full Control for the Administrators group, Read Only for the Authenticated Users group, and Read plus Start, Stop, Pause for the SYSTEM identity.

If you click on the Advanced tab of the security settings, it looks something like this:



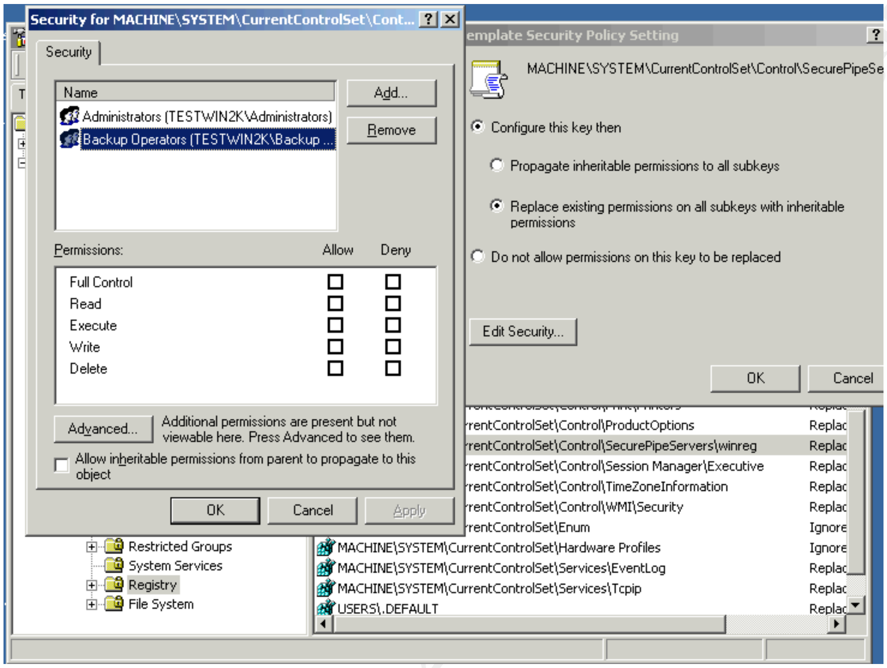
Permission Entries:

Type	Name	Permission
Allow	Administrators (TESTWIN2K\Administrators)	Full Control
Allow	Authenticated Users	Read
Allow	SYSTEM	Special

This permission is defined directly on this object. This permission is not inherited by child objects.

© SANS Institute 2000 - 2005 Author retains full rights.

Under the Registry is the list of all the default registry permissions we obtained from copying the basicwk.inf template. Find the SecurePipServers\winreg entry and change the permissions on this key, by removing the Backup Operators from the list. Administrators are already defined properly on this key.


Security for MACHINE\SYSTEM\CurrentControlSet\Cont...

Security

Name
Administrators (TESTWIN2K\Administrators)
Backup Operators (TESTWIN2K\Backup ...

Permissions:	Allow	Deny
Full Control	□	□
Read	□	□
Execute	□	□
Write	□	□
Delete	□	□

Additional permissions are present but not viewable here. Press Advanced to see them.

□ Allow inheritable permissions from parent to propagate to this object

emplate Security Policy Setting

MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeSe

● Configure this key then

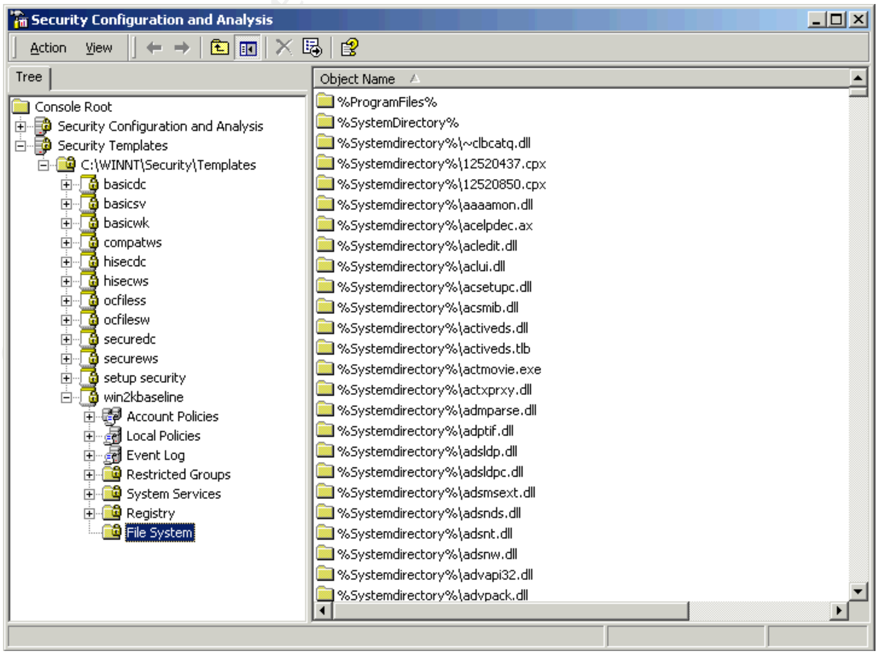
○ Propagate inheritable permissions to all subkeys

● Replace existing permissions on all subkeys with inheritable permissions

○ Do not allow permissions on this key to be replaced

```
rentControlSet\Control\ProductOptions                          Replac
rentControlSet\Control\SecurePipeServers\winreg                Replac
rentControlSet\Control\Session Manager\Executive               Replac
rentControlSet\Control\TimeZoneInformation                     Replac
rentControlSet\Control\WMI\Security                            Replac
rentControlSet\Enum                                            Ignore
MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles             Ignore
MACHINE\SYSTEM\CurrentControlSet\Services\EventLog             Replac
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip                Replac
USERS\.DEFAULT                                                 Replac
```

Finally under the File System section we may change permissions for files and folders. As a result of copying the basicwk.inf template, we will see the default Windows 2000 permissions are already in this list.

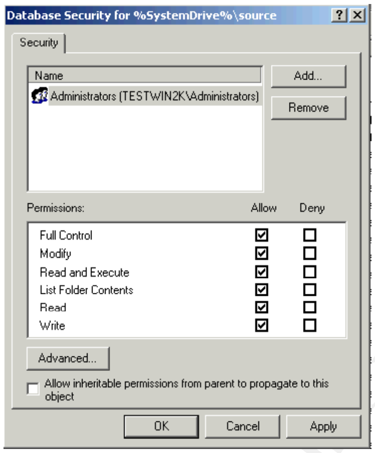

Security Configuration and Analysis

```
Console Root
  Security Configuration and Analysis
  Security Templates
    C:\WINNT\Security\Templates
      basicdc
      basicsv
      basicwk
      compatws
      hisecdc
      hisecws
      ocfiless
      ocfilesw
      securedc
      securews
      setup security
      win2kbaseline
        Account Policies
        Local Policies
        Event Log
        Restricted Groups
        System Services
        Registry
        File System
```

```
%ProgramFiles%
%SystemDirectory%
%Systemdirectory%\~clbcatq.dll
%Systemdirectory%\12520437.cpx
%Systemdirectory%\12520850.cpx
%Systemdirectory%\aaaamon.dll
%Systemdirectory%\acelpdec.ax
%Systemdirectory%\acledit.dll
%Systemdirectory%\aclui.dll
%Systemdirectory%\acsetupc.dll
%Systemdirectory%\acsmib.dll
%Systemdirectory%\activeds.dll
%Systemdirectory%\activeds.tlb
%Systemdirectory%\actmovie.exe
%Systemdirectory%\actxprxy.dll
%Systemdirectory%\admparse.dll
%Systemdirectory%\adptif.dll
%Systemdirectory%\adsldp.dll
%Systemdirectory%\adsldpc.dll
%Systemdirectory%\adsmsext.dll
%Systemdirectory%\adsnds.dll
%Systemdirectory%\adsnt.dll
%Systemdirectory%\adsnw.dll
%Systemdirectory%\advapi32.dll
%Systemdirectory%\advpack.dll
```

© SANS Institute 2000 - 2005   Author retains full rights.

Right click on File System and select ‘Add File’. Type in the name of the folder that needs to be defined, in our case ‘c:\source’. For the permissions on this folder set it to Full Control for the Administrators group only. Deselect the ‘Allow inheritable permissions from parent to propagate to this object’, and click OK.



Database Security for %SystemDrive%\source

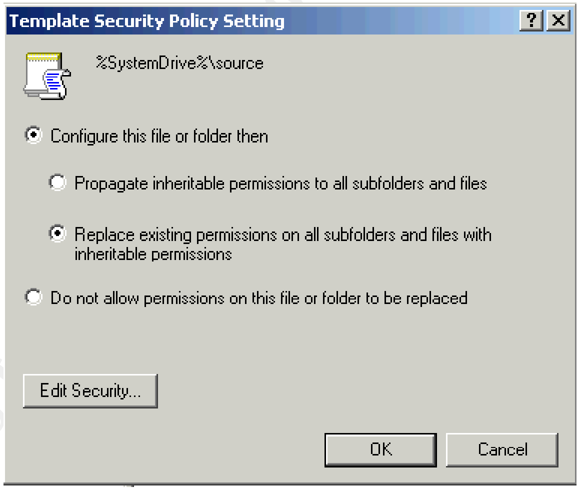
Security

Name
Administrators (TESTWIN2K\Administrators)

Permissions:	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read and Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□

□ Allow inheritable permissions from parent to propagate to this object

You will now be prompted as to how to configure the folder permissions. Change this to the ‘Replace existing permissions on all subfolders and files with inheritable permissions’ selection, and click OK.



Template Security Policy Setting

%SystemDrive%\source

● Configure this file or folder then

○ Propagate inheritable permissions to all subfolders and files

● Replace existing permissions on all subfolders and files with inheritable permissions

○ Do not allow permissions on this file or folder to be replaced

Make a note that the path has been redefined by the editor as ‘%SystemDrive%\source’ rather than ‘c:\source’, that may be important if your System Drive is something other than C:.

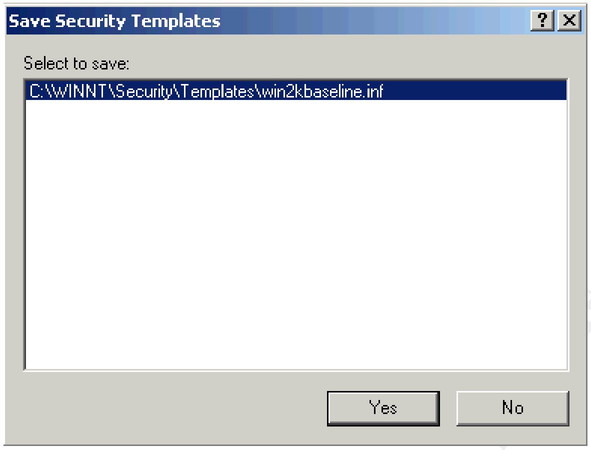
Continue to add the permissions for the c:\inetpub directories.

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2000 - 2005

Author retains full rights.

Now when you exit the Security Templates editor you will be prompted whether or not you wish to save the changes made to this template.



C:\WINNT\Security\Templates\win2kbaseline.inf

Select OK to save.

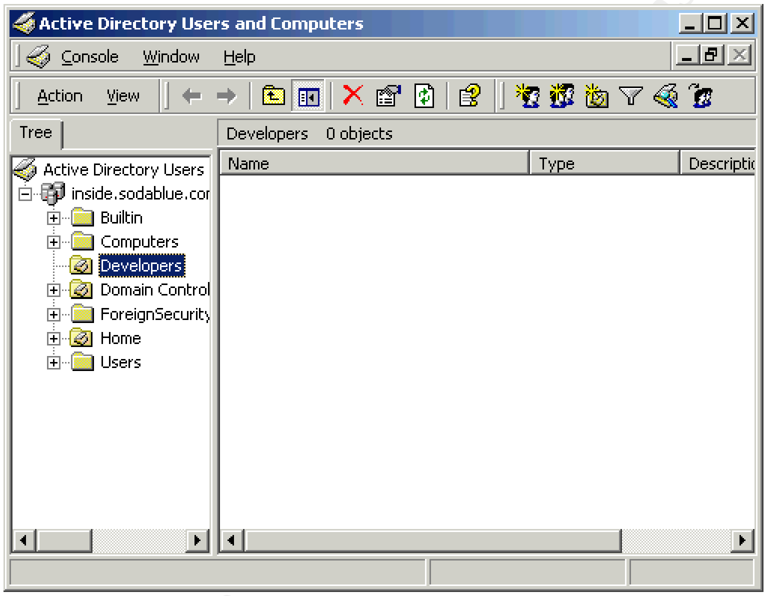
© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

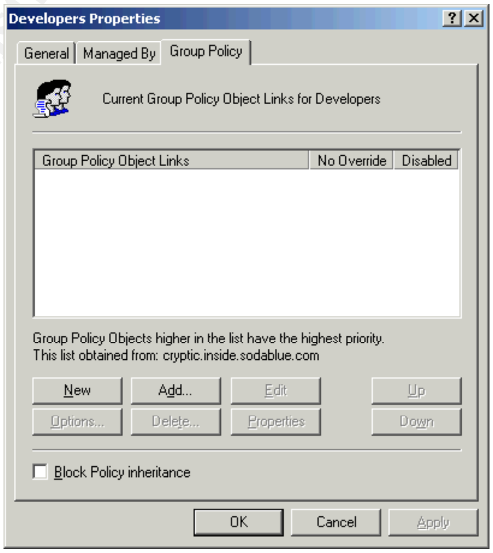
Applying the Template

The win2kbaseline.inf template will be found in the c:\winnt\security\templates directory. The first step to applying this template automatically is to copy that file to the same directory location on the domain controller.

Next, on the domain controller open up the Active Directory Users and Computers console. Create a new Organizational Unit called 'Developers' to place our configured machines.



Right click on the Developers OU and bring up properties. Select the Group Policy tab.

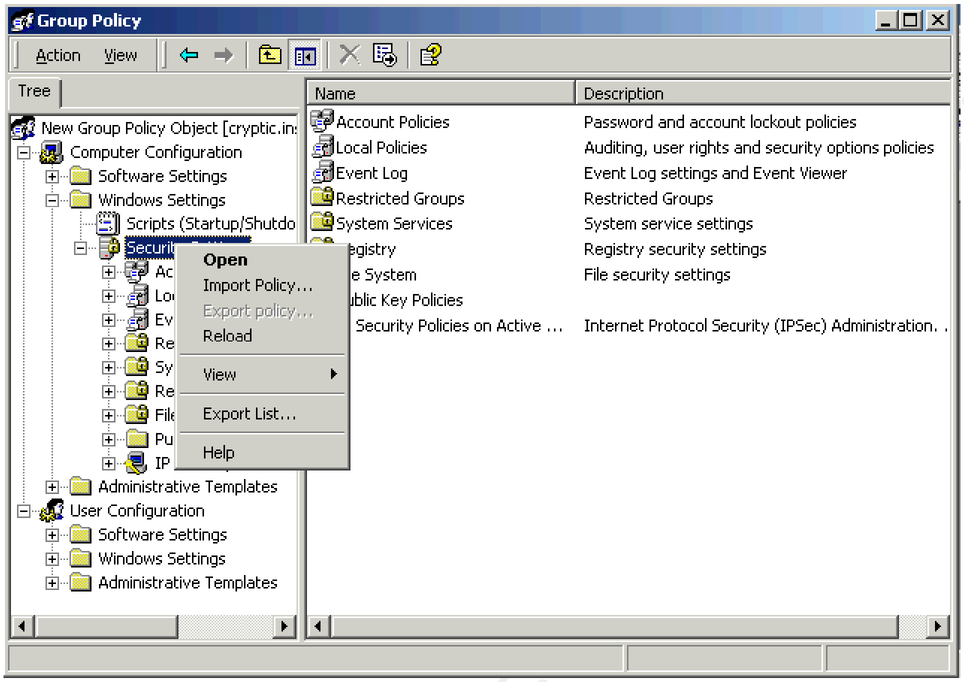


Group Policy Objects higher in the list have the highest priority.
This list obtained from: cryptic.inside.sodablue.com

□ Block Policy inheritance

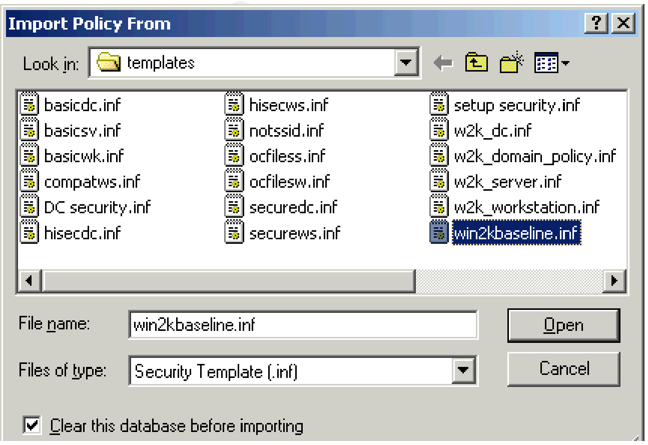
© SANS Institute 2000 - 2005 Author retains full rights.

Create a new Group Policy Object, and then click the Edit button.



Name	Description
Account Policies	Password and account lockout policies
Local Policies	Auditing, user rights and security options policies
Event Log	Event Log settings and Event Viewer
Restricted Groups	Restricted Groups
System Services	System service settings
egistry	Registry security settings
e System	File security settings
blic Key Policies	
Security Policies on Active ...	Internet Protocol Security (IPSec) Administration. .

In the Computer Configuration section, go to Windows Settings -> Security Options and right click. Select Import Policy.



File name: win2kbaseline.inf

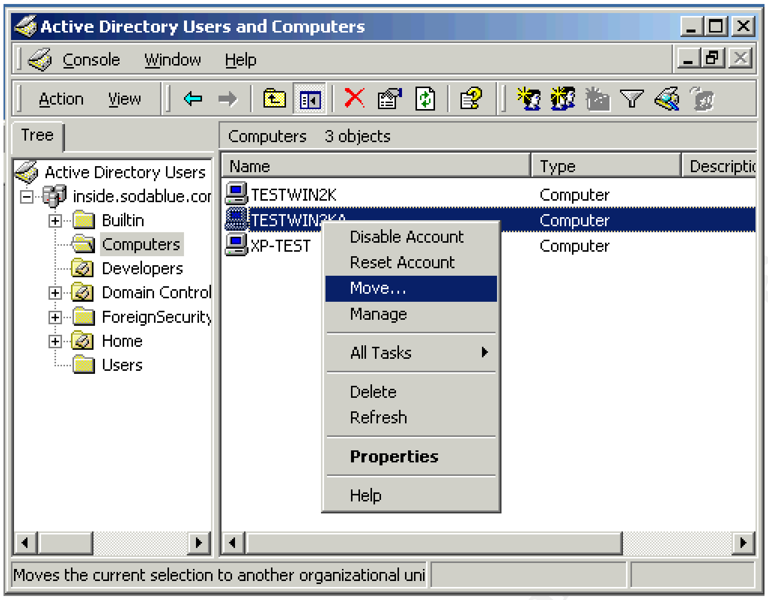
Files of type: Security Template (.inf)

☑ Clear this database before importing

Select the win2kbaseline.inf file we created and import it. Close out of the Group Policy editor.

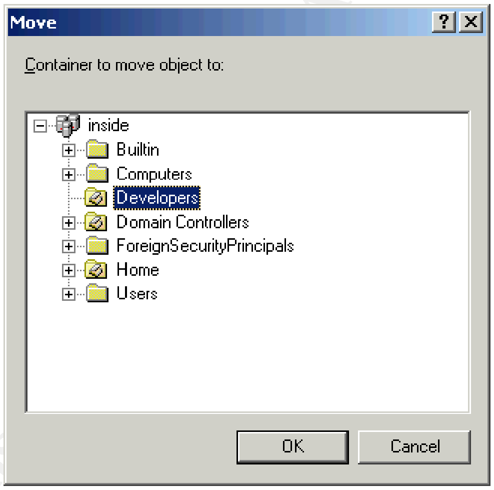
Now we need to move our test computer into the new Developers OU. Open up the Active Directory Users and Computers management console. Find the test computer under the Computers OU and right click on it.

© SANS Institute 2000 - 2005 Author retains full rights.



Moves the current selection to another organizational uni

Select Move, and then move it to the Developers OU.



Now start the test computer and have it reconnect to the network.

Template Automation and Maintenance

Now that the template has been created and applied to an Organizational Unit, whenever a new desktop is to be installed for use by our Developers its object only needs to be moved to the appropriate OU in the Active Directory. Once the machine starts up under its new OU, the template settings will be automatically applied to the machine.

Over time changes may be required to the template. These changes could be made directly to the Group Policy Object; however it is probably best if they are maintained by

© SANS Institute 2000 - 2005

Author retains full rights.

modifying a saved copy of the win2kbaseline.inf template we had created. Then after the template has been modified as needed, it can be re-imported into the Group Policy Object security settings. Make sure to check the 'Clear this database before importing' to insure the results are as expected.

By keeping and modifying a saved copy of the template file, you have insurance in case something was to accidentally happen to the Organization Unit. Also you now have the option of importing this template into additional Organization Units, or saving it to another template and creating additional variations.

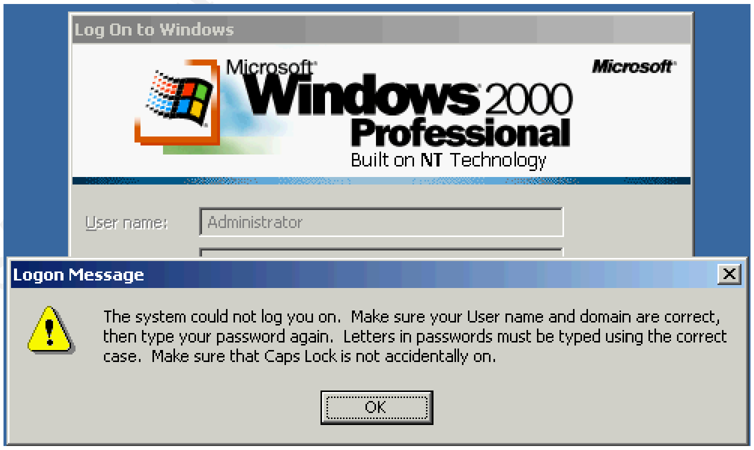
It is also recommended that an OU be created specifically for the purpose of testing modifications to the template before they are redeployed. If you keep good notes as to what changed from one release to the next, you can more efficiently target your testing to focus on those areas that may be most impacted.

Testing the Template

Validate Template has been applied

Test Case 1

Test: Attempt to logon to the workstation as the local Administrator user. Use 'Administrator' for the user name, insure that the domain is set to the local computer and enter the known password.
Expected: Failure, the Administrator account has been renamed by the security template.
Result: Test Success.



User name: Administrator

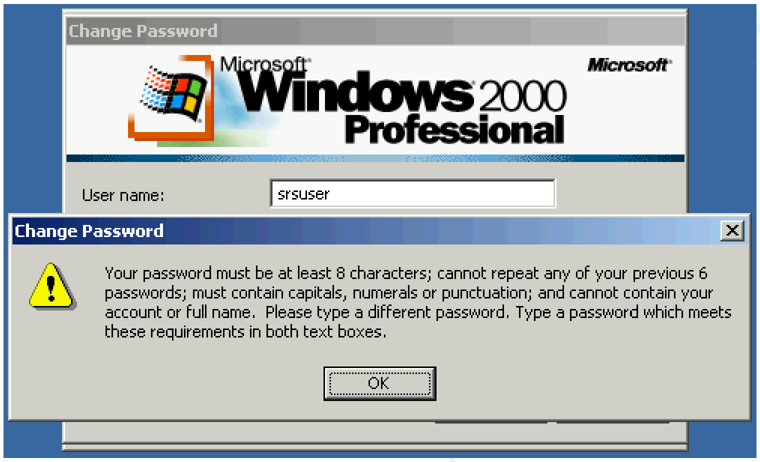
The system could not log you on. Make sure your User name and domain are correct, then type your password again. Letters in passwords must be typed using the correct case. Make sure that Caps Lock is not accidentally on.

Test: Follow through by changing the username to 'srsuser' and logging on.
Expected: Success, the Administrator account has been successfully renamed by the security template.
Result: Test Success.

© SANS Institute 2000 - 2005 Author retains full rights.

Test Case 2

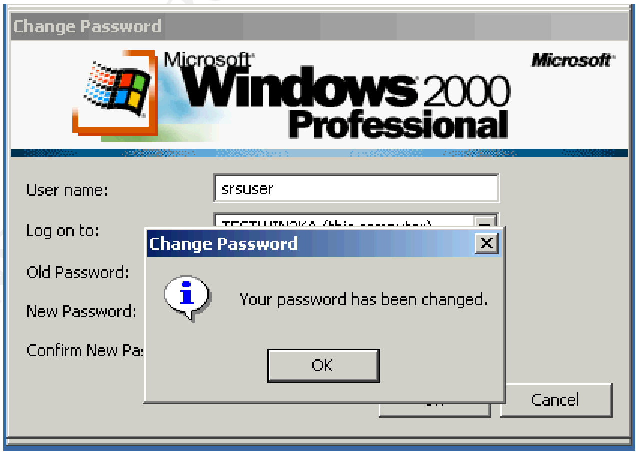
Test: Attempt to change the password for the ‘srsuser’ to ‘hello’.
Expected: Failure, the password ‘hello’ fails to meet minimum password length settings defined in the security template.
Result: Test Success.



Your password must be at least 8 characters; cannot repeat any of your previous 6 passwords; must contain capitals, numerals or punctuation; and cannot contain your account or full name. Please type a different password. Type a password which meets these requirements in both text boxes.

Test Case 3

Test: Attempt to change the password for ‘srsuser’ to ‘123ABCdef’.
Expected: Success, the password ‘123ABCdef’ meets minimum password length settings, as well as complexity settings.
Result: Test Success

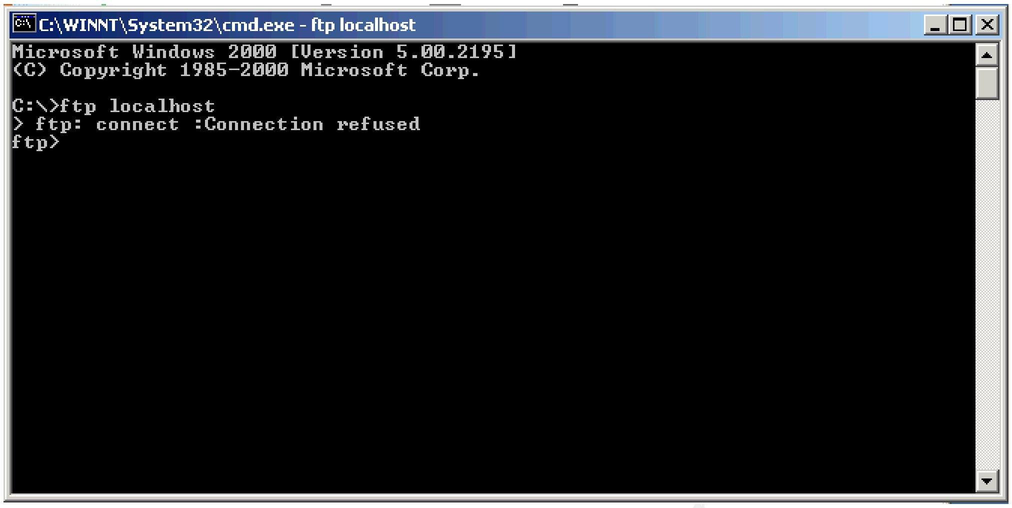


Your password has been changed.

Test Case 4

Test: Attempt to connect to the local FTP service
Expected: Failure, the FTP service was set to Manual by the security template and should not be started.
Result: Test Success

© SANS Institute 2000 - 2005 Author retains full rights.

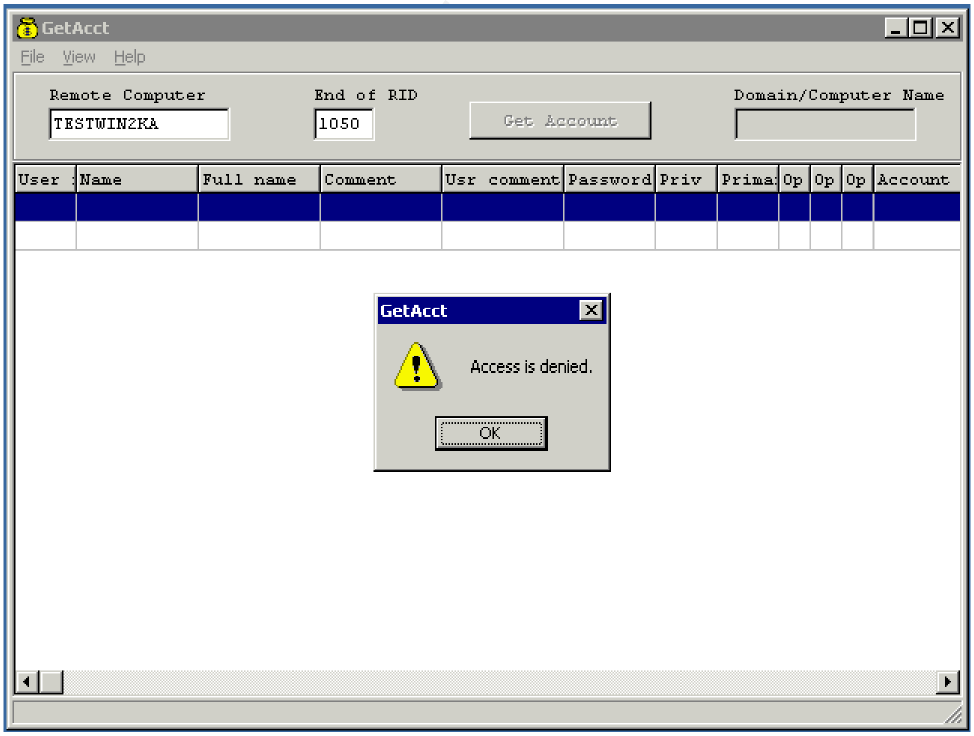


```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>ftp localhost
> ftp: connect :Connection refused
ftp>
```

Test Case 5

Test: From another computer attempt to connect anonymously to test computer using GetAcct and retrieve the account names from the SAM database.
Expected: Failure, Anonymous access to the Local Security Authority has been disabled by the security template.
Result: Test Success



Remote Computer: TESTWIN2KA

End of RID: 1050

Domain/Computer Name:

User	Name	Full name	Comment	Usr comment	Password	Priv	Prima	Op	Op	Op	Account

GetAcct

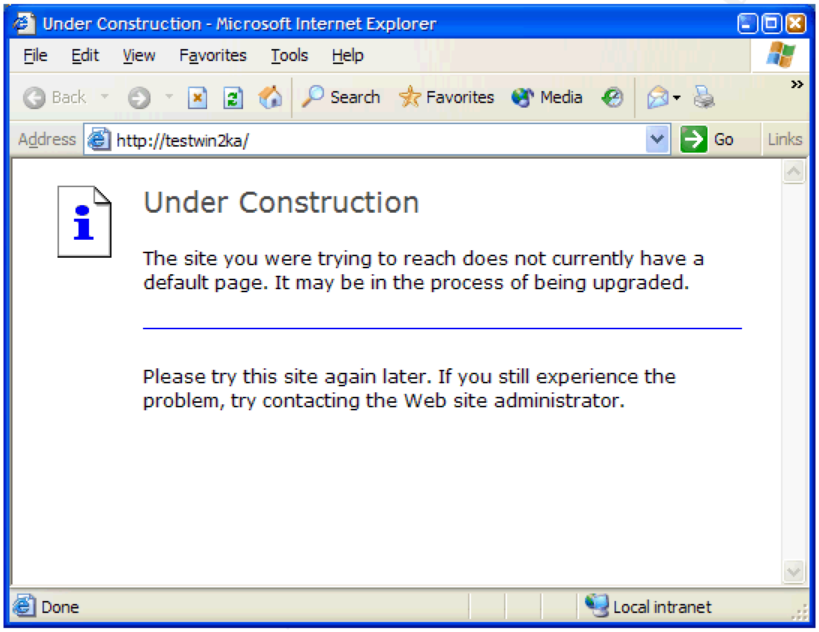
Access is denied.

© SANS Institute 2000 - 2005 Author retains full rights.

Validate System is Functioning for its Intended Use

Test Case 1

Test: Connect to web server from another machine and verify the service is responding.
Expected: Success, the Web service was set to start automatically by the security template.
Result: Test Success



Under Construction - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://testwin2ka/ Go Links
Done
Local intranet

Under Construction

The site you were trying to reach does not currently have a default page. It may be in the process of being upgraded.

Please try this site again later. If you still experience the problem, try contacting the Web site administrator.

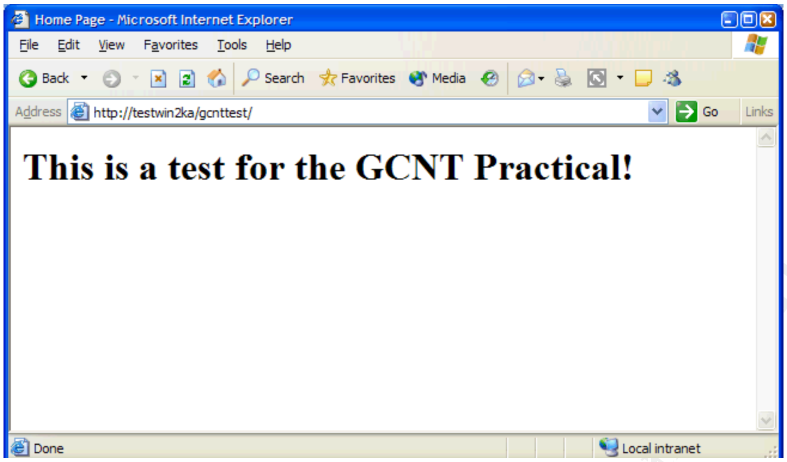
Test Case 2

Test: Using FrontPage 2000 on the test machine, create a new web site on the local machine and enter content in the Default.html page. From another machine, connect to this website and verify content was saved.
Expected: Success, FrontPage extensions should still function on the test computer.
Result: Test Success

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005

Author retains full rights.


Home Page - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://testwin2ka/gcnttest/
Go Links
Done
Local intranet

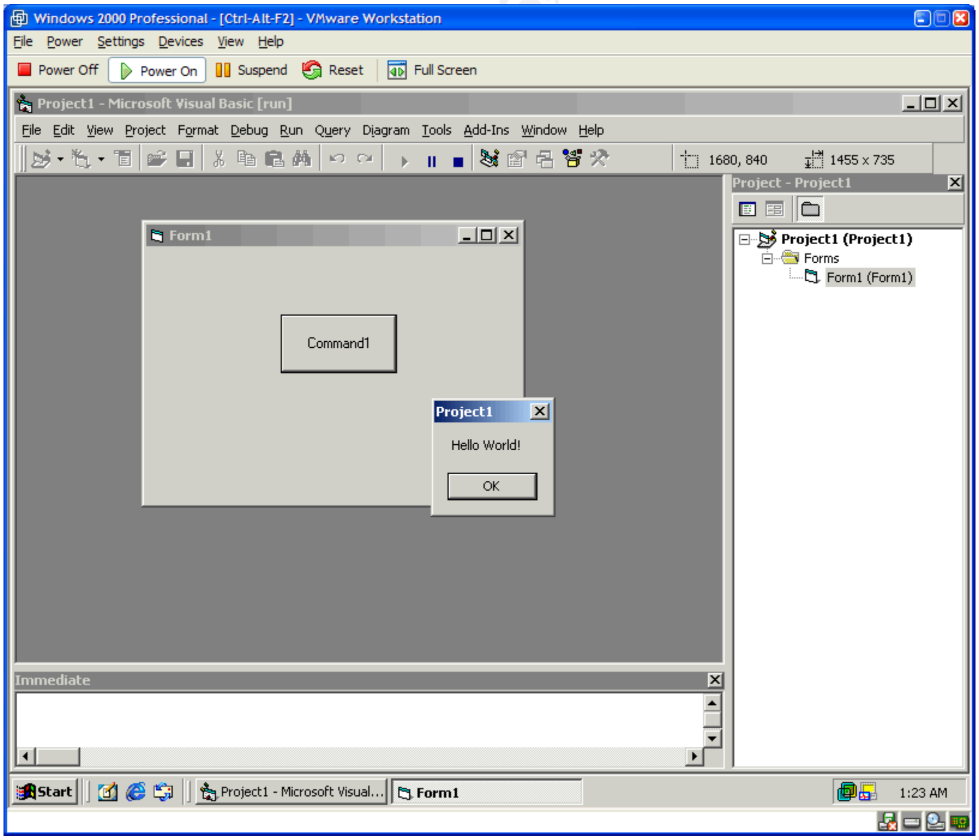
This is a test for the GCNT Practical!

Test Case 3

Test: On the test machine open up Visual Studio 6.0 and create and compile a test application.

Expected: The user should be able to use Visual Studio to create and compile software.

Result: Test Success


Windows 2000 Professional - [Ctrl-Alt-F2] - VMware Workstation
File Power Settings Devices View Help
Power Off Power On Suspend Reset Full Screen
Project1 - Microsoft Visual Basic [run]
File Edit View Project Format Debug Run Query Diagram Tools Add-Ins Window Help
1680, 840
1455 x 735
Project - Project1
Project1 (Project1)
Forms
Form1 (Form1)
Form1
Command1
Project1
OK
Immediate
Start
Project1 - Microsoft Visual...
Form1
1:23 AM

Hello World!

© SANS Institute 2000 - 2005

Author retains full rights.

Is It Secure? (The Trials and Tribulations of IIS)

In and of itself, the configuration items from the Windows 2000 Baseline Checklist as applied to a security template and distributed by Group Policy do not do enough to really provide a secure environment for our development workstations. As one can plainly see from the analysis of the template, many of the items to be performed were procedural. Insuring hotfixes are applied, ensuring folders are not created without thought and other issues that can leave systems vulnerable.

From our experiences with IIS attacks such as Code Red and Nimda, probably the most important aspect of the Baseline checklist is the installation of service packs and hotfixes. Unfortunately while service packs can be distributed via the Group Policy Objects, hotfixes cannot be at this time. This means either manual application, or using additional management tools such as SMS or Tivoli.

The Appendices of this document detail additional steps taken that are important to achieve the goal of a secure development workstation.

- Appendix A details tools available from Microsoft to aid in the identification and validation of system software updates.
- Appendix B details tools and locations for updating application software.
- Appendix C details tools provided with Norton AntiVirus for keeping the virus scanner up to date.
- Appendix D details tools available from Microsoft to aid in securing IIS.

While this IIS Lockdown tool detailed in Appendix D is useful, it is unfortunate that these configuration items are not available at all through Group Policy. Even with the unattended install of this tool it requires someone manually running the program on the machine. It may be possible to distribute these files through Group Policy and execute them as startup scripts, which is something that should be investigated further.

Regarding the items in the checklist which were identified as procedural, it is clear that some sort of Security Policy needs to be written to cover the deployment of desktops in our development environment. This policy would list what is required by the end-user to monitor or maintain their system, such as verifying Antivirus is always functional and that they do not share folders or create additional accounts in such a way as to open up holes.

Another concern is rogue IIS servers, as it is entirely possible that other individuals within the company who are not necessarily associated with development groups may have the web services installed on their desktops. There is an interesting article in Microsoft Consulting Services entitled “Manage Security of Your IIS Web Services”[13] and it warns of this situation.

© SANS Institute 2000 - 2005 Author retains full rights.

The articles #1 recommendation is “All Systems Must Become Managed.” This may mean a security policy for the rest of the company, perhaps further templates that automatically disable IIS Web services unless the machine is a member of the Managed Developers group.

Additionally it is the responsibility of the administrators to stay up to date with ongoing security issues. Audit the machines for potential problems and update the security templates and policies to account for them. Always endeavor to automate security settings as much as possible because this helps to ensure they will be in place in a repeatable manner. The fewer manual steps, the lower the chances of a mistake being made.

Conclusion

The template created as a result of Microsoft’s Windows 2000 Professional Baseline Checklist is a good start towards automating security policies in the organization. The checklist does not address a number of items which could be very beneficial to our particular configuration.

Some additional areas that were not mentioned in the Baseline that should be investigated and implemented in future versions of the Template:

Audit Policies

Enabling audit policies is useful not just for intrusion detection, but also for debugging of applications especially by auditing logon events and object access.

Additional Security Options

- ‘Do not display last user name in logon screen’ could be enabled in situations where it is undesirable for persons to easily obtain usernames.
- ‘LAN Manager Authentication Level’ should be set as strong as possible. Preferably you should be using NTLM2, however care should be taken with testing application compatibility before changing this to its highest setting of ‘Refuse LM & NTLM’. For this to work properly, NT4 machines must be at SP4 or higher, and Win9x machines need to run the DSclient patch from the Windows 2000 CD.
- ‘Message text for users attempting to logon’ is very often mandated by corporate legal requirements.
- ‘Prompt user to change password before expiration’ could be modified. Many users find the default 14 days to be annoying given a short 42 days between password changes.

Event Log Settings

- The default size for System and Application logs as well as the length of time events are retained is seldom adequate for a development environment. Development apps frequently log a variety of error messages and other information,

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

and it would be beneficial to adjust these settings as a convenience to the end user. Especially if auditing is also enabled as discussed previously.

The registry could be further locked down. By default Windows 2000 allows members of the Power Users group to write to the HKLM\Software key, which means they may install or modify software and the requisite settings. This is probably not that big of an issue given our scenario, however if a development machine is to be used by other users for testing it may be a good idea to restrict the ability to break settings.

Additionally, a better definition of file system permissions for the c:\inetpub\mailroot directory would be advised if the developers are going to make use of this service. Other file system permissions should be added as they are identified.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Appendix A – System Software Updates

As mentioned previously in our discussion of the checklist, the most recent Service Pack at this time for Windows 2000 is SP2. This was installed on our test machine as part of an integrated installation[14].

The next step is to execute the HFNetchk tool referred to in our discussion regarding maintaining up to date hotfixes. The tool is very simple to install and use and on may find instructions for using it in the following knowledge base article:

http://support.microsoft.com/default.aspx?scid=kb;EN-US;Q303215

Using the following modified instructions from the knowledgebase article:

1. Download the nshc32.exe file that is listed in the Download section of this article.
2. Run the nshc32.exe file that you downloaded, and then follow the installation instructions.
3. At a command prompt, locate the folder you created.
4. Type hfnetchk, and then press Enter.

The output will look like this:

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

```
C:\nshc32>hfnetchk
Microsoft Network Security Hotfix Checker, 3.2
Developed for Microsoft by Shavlik Technologies, LLC
info@shavlik.com (www.shavlik.com)


 ** Attempting to download the XML from:
http://download.microsoft.com/download/xml/security/1.0/NT5/EN-US/mssecure.cab

 ** File was successfully downloaded. **

 ** Attempting to load C:\nshc32\mssecure.xml. **
Using XML data version = 1.0.1.173  Last modified on 12/20/2001.

Scanning TESTWIN2KA
.............
Done scanning TESTWIN2KA

Please use the -v switch to view details for
Patch NOT Found, Warning and Note messages


Please use the -nosum switch when scanning non English-language
systems.

----------------------------
TESTWIN2KA
----------------------------



        * WINDOWS 2000 SP2

        Patch NOT Found MS00-077        Q299796
        Patch NOT Found MS00-079        Q276471
        Patch NOT Found MS01-007        Q285851
        Patch NOT Found MS01-013        Q285156
        NOTE            MS01-022        Q296441
        Patch NOT Found MS01-025        Q296185
        Patch NOT Found MS01-031        Q299553
        Patch NOT Found MS01-037        Q302755
        Patch NOT Found MS01-041        Q298012
        Patch NOT Found MS01-046        Q252795

        * Internet Information Services 5.0

        Patch NOT Found MS01-025        Q296185
        Patch NOT Found MS01-044        Q301625

        * Internet Explorer 5.5 SP2

        Patch NOT Found MS01-058        Q313675
```

Each one of these items corresponds to a patch that needs to be installed to the system. Notice that the patches are grouped by product affected. This tool will also check for patches on Windows NT 4 and Windows XP installs, as well as for patches to SQL Server version 7 or higher.

Pay attention to the NOTE entry for bulletin MS01-022, this is discussed in knowledgebase article Q306460[15]. This entry comes up as a NOTE because the tool was not able to reliably test the version of this particular DLL. From the information provided in the article, it was determined that this machine was vulnerable.

© SANS Institute 2000 - 2005 Author retains full rights.

We now have to do a little bit of manual work, and look each one of these issues up to understand what they mean, and what needs to be done to patch the system. One can look up these issues by either referring to the security bulletin (of the format MSxx-yyyy) at:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/current.asp

Or by referring to the knowledgebase article id (of the format Qxxxxxx) at:

http://support.microsoft.com/

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

The following is a list of my findings on each of these patches, containing a brief description of the vulnerability and a link to the patch:

MS00-077/Q299796 - NetMeeting Desktop Sharing Vulnerability
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=30963
MS00-079/Q276471 - HyperTerminal Buffer Overflow Vulnerability
http://www.microsoft.com/windows2000/downloads/security/q276471/default.asp
MS01-007/Q285851 - Network DDE Agent Requests Can Enable Code to Run in System Context
http://www.microsoft.com/windows2000/downloads/security/q285851/default.asp
MS01-013/Q285156 - Windows 2000 Event Viewer Contains Unchecked Buffer
http://www.microsoft.com/windows2000/downloads/security/q285156/default.asp
MS01-022/Q296441 - WebDAV Service Provider Can Allow Scripts to Levy Requests as User
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=29129
MS01-025/Q296185 - Index Server Search Function Contains Unchecked Buffer
http://www.microsoft.com/windows2000/downloads/critical/q296185/default.asp
MS01-031/Q299553 - Predictable Named Pipes Could Enable Privilege Elevation via Telnet
http://www.microsoft.com/windows2000/downloads/critical/q299553/default.asp
MS01-037/Q302755 - Authentication Error in SMTP Service Could Allow Mail Relaying
http://www.microsoft.com/windows2000/downloads/security/q302755/default.asp
MS01-041/Q298012 - Malformed RPC Request Can Cause Service Failure
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=31434
MS01-046/Q252795 - Access Violation in Windows 2000 IRDA Driver Can Cause System to Restart
[Link to patch was unavailable]
MS01-044/Q301625 - 15 August 2001 Cumulative Patch for IIS
http://www.microsoft.com/windows2000/downloads/critical/q301625/default.asp
MS01-058/Q313675 - 13 December 2001 Cumulative Patch for IE
http://www.microsoft.com/windows/ie/downloads/critical/Q313675/default.asp

In total we have 11 patches to install as of 25-December-2001. It is not clear as to why the patch for MS01-046 does not resolve properly, but upon studying the article it is not an issue with our machine as it does not have IRDA ports.

Microsoft provides another tool named QChain which will allow us to combine all of these patches and install them at one time. This tool is documented at here:

http://support.microsoft.com/default.aspx?scid=kb;EN-US;q296861

To use this tool you create a batch file which executes each of the hotfixes without rebooting. This is done typically by appending the command line arguments –z and –m.

For our patches, the batch file resembles this:

© SANS Institute

© SANS Institute 2000 - 2005

Author retains full rights.

```
@echo off
setlocal
Q276471_W2K_SP3_x86_en.EXE -z -m
Q285156_W2K_SP3_x86_en.EXE -z -m
Q285851_W2K_SP3_x86_en.EXE -z -m
Q296185_W2K_SP3_x86_en.EXE -z -m
Q298012_W2K_SP3_x86_en.EXE -z -m
Q299553_W2K_SP3_x86_en.EXE -z -m
Q299796_W2k_SP3_x86_en.exe -z -m
Q301625_W2K_SP3_x86_en.EXE -z -m
Q302755_W2k_SP3_x86_en.exe -z -m
q313675.exe
rbupdate.exe
qchain.exe
```

Note that the last two hotfixes do not have the command line arguments appended. This is because they have slightly different behavior. The q313675 works interactively and at the end prompts manually for whether or not to reboot. Rbupdate did not support the command lines, nor did it wish to reboot after being installed.

After running the above batch file we have to manually reboot the system. Once this has occurred, we can verify the installation of these hotfixes by rerunning the HfNetchk program.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

```
C:\nshc32>hfnetchk
Microsoft Network Security Hotfix Checker, 3.2
Developed for Microsoft by Shavlik Technologies, LLC
info@shavlik.com (www.shavlik.com)


 ** Attempting to download the XML from:
http://download.microsoft.com/download/xml/security/1.0/NT5/EN-US/mssecure.cab

 ** File was successfully downloaded. **

 ** Attempting to load C:\nshc32\mssecure.xml. **
Using XML data version = 1.0.1.173  Last modified on 12/20/2001.

Scanning TESTWIN2KA
................................................................................
...........................
Done scanning TESTWIN2KA

Please use the -v switch to view details for
Patch NOT Found, Warning and Note messages


Please use the -nosum switch when scanning non English-language
systems.

----------------------------
TESTWIN2KA
----------------------------



        * WINDOWS 2000 SP2

        NOTE            MS01-022        Q296441
        Patch NOT Found MS01-046        Q252795

        * Internet Information Services 5.0

        INFORMATION     All necessary hotfixes have been applied

        * Internet Explorer 5.5 SP2

        INFORMATION
        All necessary hotfixes have been applied.
```

We still have the NOTE regarding MS01-022, and it still indicates that it could not find the patch for MS01-046 (the one with the broken download link), but otherwise it's reporting that all necessary hotfixes have been applied.

Another tool which is useful in verifying the installation of hotfixes is named QfeCheck and information regarding it is available at:

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q282784

This program installs as a system tool and can be run at any time to verify the hotfixes installed on a system. It will also connect to remote machines, if you have Administrator privileges to them.

© SANS Institute 2000 - 2005

Author retains full rights.

```
C:\qfecheck

Windows 2000 Hotfix Validation Report for \\TESTWIN2KA
Report Date: 12/26/2001  9:30pm

Current Service Pack Level:  Service Pack 2

Hotfixes Identified:
Q282784:  Current on system.
Q276471:  Current on system.
Q285156:  Current on system.
Q285851:  Current on system.
Q296185:  Current on system.
Q298012:  Current on system.
Q299553:  Current on system.
Q299796:  Current on system.
Q301625:  Current on system.
Q302755:  Current on system.
```

We only have 10 Hotfixes identified, but that is because the rbupdate.exe from MS01-022 is not classified as a hotfix in the same way, either is Q313675 from MS01-058. We also have an extra hotfix listed as Q282784, and that is actually the QfeCheck program itself.

In addition to these hotfixes, further updates are available from WindowsUpdate which may be useful depending on the specific environment. Compatibility updates, driver updates, additional tools, utilities and bug fix patches may be available. In this particular exercise, this option was not pursued.

Microsoft Data Access Components v2.6sp1

This update to MDAC was obtained from:
http://www.microsoft.com/data/download_26sp1.htm

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Appendix B – Application Updates

Microsoft Office 2000

Microsoft has provided a service very similar to WindowsUpdate for their Office product. It is accessible at this address: http://office.microsoft.com/ProductUpdates/default.aspx

Using this service, Office 2000 was updated to the most recent patches. The list of installed patches includes:

Office 2000 Service Release 1a (SR-1a) (Incorporated in Office 2000 install CD)
Office 2000 Service Pack 2 (SP-2)
Outlook 2000 Collaboration Data Objects (CDO) Update: Security (installed with SP2)
Microsoft Office 2000/Windows 2000 Registry Repair Utility (installed with SP2)
Outlook 2000 SR-1 E-mail Security Update (installed with SP2)
Outlook 2000 SR-1: Extended E-mail Security Update (English version)
Outlook 2000 SR-1 View Control Security Update
Excel 2000 SR-1 Macro Modification Security Update
Word 2000 Security Update: Macro Vulnerability
PowerPoint 2000 SR-1 Macro Modification Security Update
Office 2000 SR-1 Update: Web Client Security
Office 2000 Security Update: UA Control Vulnerability
Access 2000 and SQL Server 2000 Readiness Update (English version)

Microsoft Visual Studio 6.0

The most recent update for Visual Studio 6.0 is Service Pack 5 and is available from: http://msdn.microsoft.com/vstudio/sp/vs6sp5/default.asp

Internet Explorer 5.5 SP2

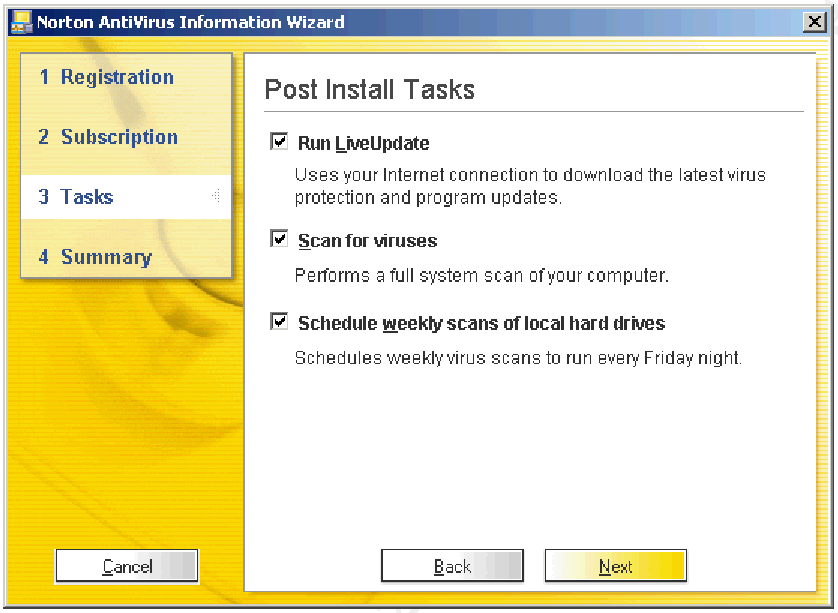
This update to the Internet Explorer web browser was obtained from: http://www.microsoft.com/windows/ie/downloads/recommended/ie55sp2/default.asp

© SANS Institute 2000 - 2005

Author retains full rights.

Appendix C – Keeping Norton AntiVirus Updated

Norton Antivirus includes a very valuable feature called LiveUpdate. You are prompted to activate it towards the end of the install.



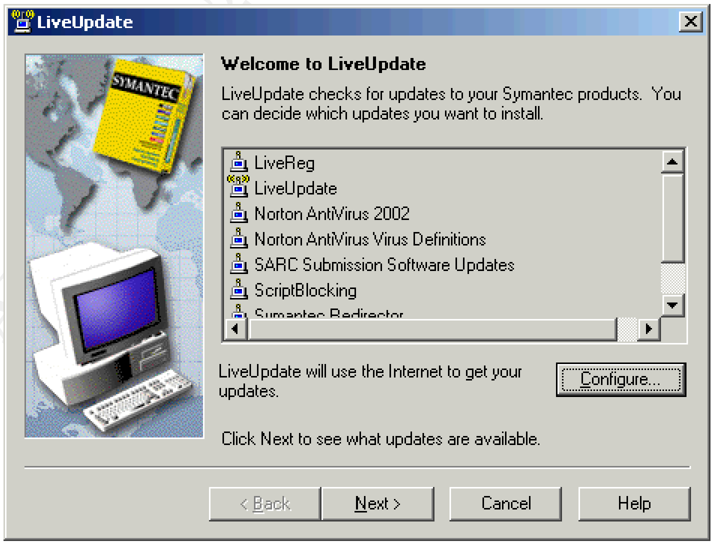
Post Install Tasks

☑ Run LiveUpdate
Uses your Internet connection to download the latest virus protection and program updates.

☑ Scan for viruses
Performs a full system scan of your computer.

☑ Schedule weekly scans of local hard drives
Schedules weekly virus scans to run every Friday night.

This will cause the LiveUpdate feature to execute at the end of the installation, to ensure you have the most recent updates available at the time of install.



Welcome to LiveUpdate

LiveUpdate checks for updates to your Symantec products. You can decide which updates you want to install.

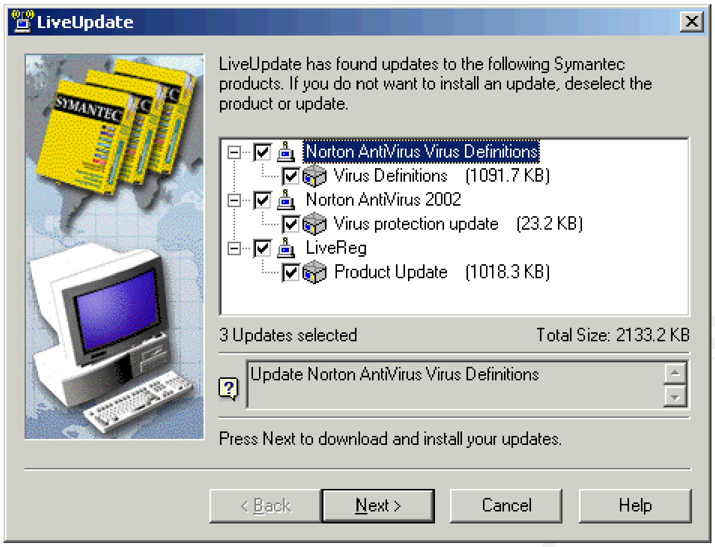
- LiveReg
- LiveUpdate
- Norton AntiVirus 2002
- Norton AntiVirus Virus Definitions
- SARC Submission Software Updates
- ScriptBlocking
- Symantec Redirector

LiveUpdate will use the Internet to get your updates.

Click Next to see what updates are available.

LiveUpdate will connect to the internet and identify which updates are available to install.

© SANS Institute 2000 - 2005 Author retains full rights.



LiveUpdate has found updates to the following Symantec products. If you do not want to install an update, deselect the product or update.

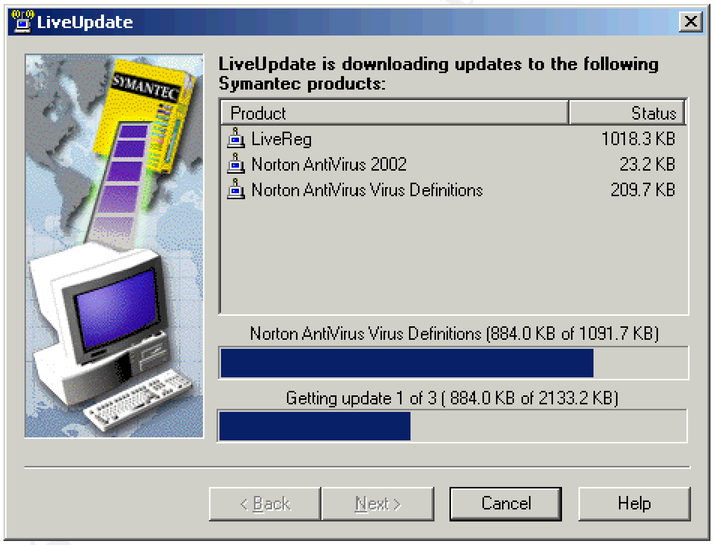
☑ Norton AntiVirus Virus Definitions
  ☑ Virus Definitions (1091.7 KB)
☑ Norton AntiVirus 2002
  ☑ Virus protection update (23.2 KB)
☑ LiveReg
  ☑ Product Update (1018.3 KB)

3 Updates selected Total Size: 2133.2 KB

Update Norton AntiVirus Virus Definitions

Press Next to download and install your updates.

The items are selected by default, so simply verify what will be installed and go on to the next screen to download and install the updates.



LiveUpdate is downloading updates to the following Symantec products:

Product	Status
LiveReg	1018.3 KB
Norton AntiVirus 2002	23.2 KB
Norton AntiVirus Virus Definitions	209.7 KB

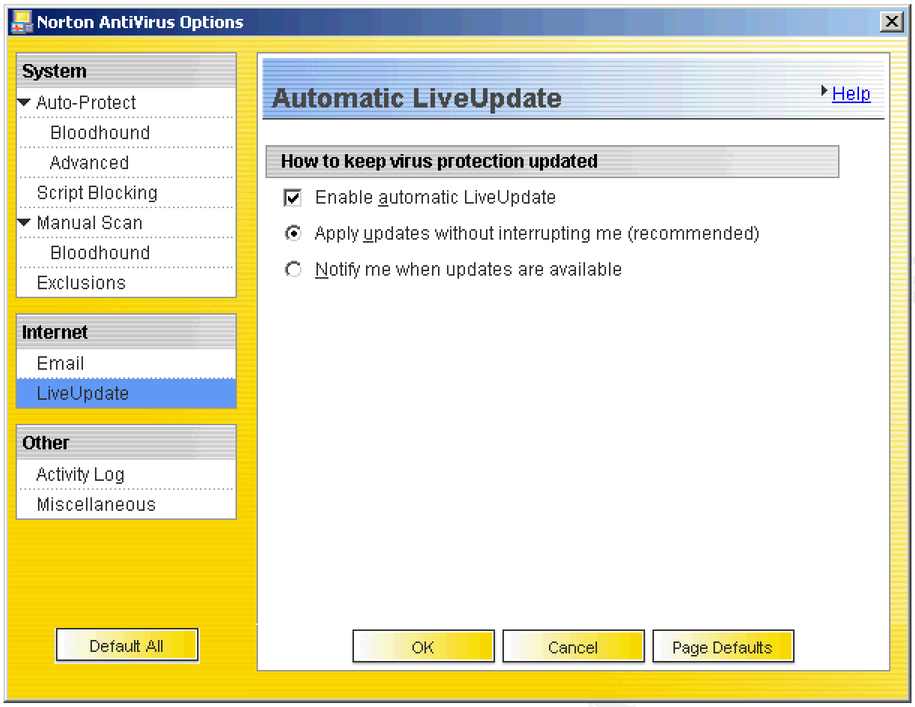
Norton AntiVirus Virus Definitions (884.0 KB of 1091.7 KB)

Getting update 1 of 3 (884.0 KB of 2133.2 KB)

Once it is complete, LiveUpdate will ask to reboot your machine. It may also notify you that you should run LiveUpdate again just to be sure all recent updates have been installed.

Most importantly, by default the Norton Antivirus install configures itself to periodically check for updates to the antivirus definitions and download and install them from the internet. Configuration for this is available from the Norton Antivirus Options, under the Internet -> LiveUpdate settings.

© SANS Institute 2000 - 2005 Author retains full rights.



Automatic LiveUpdate

How to keep virus protection updated

☑ Enable automatic LiveUpdate

● Apply updates without interrupting me (recommended)

○ Notify me when updates are available

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005

Author retains full rights.

Appendix D – Securing Internet Information Services

Over the past couple of years a large number of problems have been caused by worms propagating threw known IIS vulnerabilities. In addition to ensuring the latest service packs and hotfixes have been installed, we can configure IIS properties such that many of these vulnerabilities will simply never be available.

Microsoft provides another checklist which goes over the basics of securing IIS. It is titled the IIS 5.0 Baseline Security Checklist[16], however while this information is useful it is still a pain to have to manually go through and configure many of these recommendations. In addition to the checklist, Microsoft now provides a tool named the IIS Lockdown Tool[17].

The IIS Lockdown Tool performs many of the recommendations from the checklist, and can take templates as input so as to automate the installation for your particular configuration.

After downloading the IIS Lockdown Tool, you can either run it as is, or extract the files out manually using the following command line arguments:

iislockd /C /T:<*directoryname*>

In the directory where you extracted the files, find the RunLockdUnattended.doc as well as the URLScan.doc files and print them out for reference.

Make a backup copy if the iislockd.ini file, and then create a custom one following the directions in the RunLockdUnattended.doc file. You may also wish to look at the iislockd.chm help file for further explanations of the options.

In our particular case, looking at the built in templates, the FrontPage one appears to suit our needs. This is because our developer desktop has FrontPage extensions installed, which are utilized by either FrontPage or Visual Interdev. As such, I customized iislockd.ini to have it install this template automatically. I also modified it to re-enable WebDAV because this is used by Office 2000, notably FrontPage 2000, more on that later.

After we have the customized template in place, simply run iislockd.exe from a command prompt and it will apply the settings. You can also undo the changes by rerunning iislockd.exe again. You have to put the original iislockd.ini back in place, or at least remove the Unattended=TRUE line.

© SANS Institute 2000 - 2005 Author retains full rights.

One should also be aware that URLscan will create logfiles in c:\winnt\system32\inetsrv\urlscan. These are useful for investigating problems, but they may also grow large enough to cause drive space problems.

This is the resulting iislockd.ini file:

```
[Info]
ServerTypesNT4=frontpage2
ServerTypes=frontpage2
UnattendedServerType=frontpage
Unattended=TRUE
Undo=FALSE

[frontpage2]
label="Custom FrontPage Server Extensions Template for GCNT
Practical"

Enable_iis_http= TRUE
Enable_iis_ftp= FALSE
Enable_iis_smtp= FALSE
Enable_iis_nntp= FALSE
Enable_asp= TRUE
Enable_index_server_web_interface= FALSE
Enable_server_side_includes= FALSE
Enable_internet_data_connector= FALSE
Enable_internet_printing= FALSE
Enable_HTR_scripting= FALSE
Enable_webDAV= TRUE
Disable_Anonymous_user_system_utility_execute_rights= TRUE
Disable_Anonymous_user_content_directory_write_rights= FALSE
Remove_iissamples_virtual_directory=TRUE
Remove_scripts_directory=TRUE
Remove_MSADC_virtual_directory=TRUE
Remove_iisadmin_virtual_directory=TRUE
Remove_iishelp_virtual_directory=TRUE
UrlScan_Install=TRUE
UrlScan_IniFileLocation=urlscan_frontpage.ini
AdvancedSetup =
UninstallServices=FALSE
```

In working with the IIS Lockdown template, some care needs to be taken in your approach. After initially installing the default FrontPage template, it was learned that webDAV was required by Office 2000 so this had to re-enabled in the custom template. There may very well be other hidden problems, perhaps with the URLScan template provided. Although upon reviewing it, it appeared as though it should work for most web application development work.

© SANS Institute 2000 - 2005

Author retains full rights.

List of References

[1] VMWare 3.0 may be obtained from http://www.vmware.com

[2] SANS Institute, G6.1 - Windows 2000 Security: Step-by-Step, 2001

[3] Microsoft Corporation, Windows 2000 Professional Baseline Security Checklist (2001)
URL: http://www.microsoft.com/technet/security/tools/w2kprocl.asp

[4] Microsoft Corporation, Security Tools and Checklists (2001)
URL: http://www.microsoft.com/technet/security/tools/tools.asp

[5] mudge@l0pht.com, Windows NT rantings from the L0pht, 24-Jul-1997,
URL: http://packetstorm.decepticons.org/Crackers/NT/l0phtcrack/l0phtcrack-NT-passwd-rant.txt

[6] Microsoft Corporation, Default Access Control Settings in Windows 2000,
URL:
http://www.microsoft.com/TechNet/prodtechnol/windows2000serv/maintain/featusability/secdefs.asp

[7] Microsoft Corporation, How to Use the RestrictAnonymous Registry Value in Windows 2000 (Q246261)
URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;Q246261

[8] Urity, "RestrictAnonymous=1" has no meaning !, Mar-2001,
URL: http://www.securityfriday.com/Topics/restrictanonymous.html

[9] Microsoft Corporation, How to Enable Strong Password Functionality in Windows NT, 8-Aug-2001,
URL: http://support.microsoft.com/directory/article.asp?ID=KB;EN-US;Q161990

[10] Microsoft Corporation, Product Security Notification, December 2001,
URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/notify.asp

[11] Microsoft Corporation, HFNetchk, 2001,
URL: http://www.microsoft.com/technet/security/tools/hfnetchk.asp

[12] Microsoft Corporation, How to Create Custom MMC Snap-in Tools Using Microsoft Management Console (Q230263), 11-Dec-2001, URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;q230263

[13] Microsoft Corporation, Manage Security of Your IIS Web Services, 2001,
URL: http://www.microsoft.com/technet/security/bestprac/MCSWebBP.asp

[14] Microsoft Corporation, How to Integrate Service Pack 1 into a Windows 2000 Installation, 10-Oct-2001, URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;Q271791

[15] Microsoft Corporation, Hfnetchk.exe Returns NOTE Messages for Installed Patches (Q306460), 24-Oct-2001, URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;Q306460

[16] Microsoft Corporation, IIS 5.0 Baseline Security Checklist, 2001,
URL: http://www.microsoft.com/technet/security/tools/iis5cl.asp

[17] Microsoft Corporation, IIS Lockdown Tool (version 2.1), 14-Nov-2001,
URL: http://www.microsoft.com/Downloads/Release.asp?ReleaseID=33961

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.