



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 permitted 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>

GCWN Practical v.4.0
Option 2

by Lloyd V Ardoin

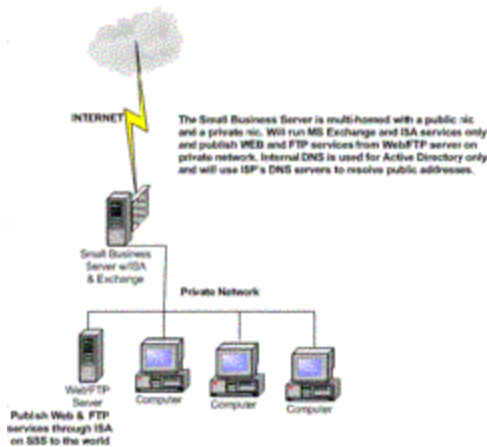
Submitted 06/15/2004

Reducing the attack surface of the Microsoft
Small Business Server 2000

The purpose of this paper is to document the installation and configuration of the Microsoft Small Business Server 2000 and provide a documented process for future installs of this product. The goal of this process is to implement additional steps during the installation process and immediately thereafter that all combined will produce a more 'hardened' Server. Following the SANS philosophy of defense in depth the process will not focus on one or two procedures but demonstrate that by applying several different procedures we can in affect produce a kind of layering effect. The focus of this paper is from the installation of the Windows 2000 operating system up to placing it into a production environment. The day to day administration is beyond the scope of this paper and publications are listed at the end that covers this subject matter in great depth.

The process will start with the installation of the Windows 2000 operating system and then continue with the install of the Small Business Server product which includes IIS, Exchange 2000, Internet and Acceleration Server, SQL server, shared fax service and shared modem service. This paper will also document the steps, recommendations and tools needed to harden the box based on several resources including Microsoft, SANS, Center for Internet Security, and the NSA.

This Small Business Server will be configured as a dual homed PC and will be placed in a small business environment connected to a cable modem with a static IP address provided by an ISP on the public NIC and will provide a gateway for the private network via its private NIC. It will be used to provide a web presence and mail services on the Internet and the ISA server service will provide the firewall to protect the private network. The SQL Server 2000 components will be installed to add to the completeness of this document. Since there will not be a current need for them, the SQL services will be disabled later in this process but may be used in future web development. The ISP will be hosting the public domain name including an MX record for the mail. Below is a diagram that illustrates the setup.



Small Business Server 2000 is a product that allows a small company or startup to purchase a package that can provide essential services such as web hosting, mail, a database engine, etc. all included for a reasonable cost. But with this value also comes some limitations. There is no limit on the number of user accounts that can be created but Small Business Server 2000 is limited to a maximum of 50 client computer connections. There can be other domain controllers and member servers in the Domain but only one Small Business Server. The Small Business Server is installed as the root domain of a single forest and is limited to a single domain environment which means no child domains can be created. The upside to this is that the Small Business Server setup Wizard removes the complexities of setting up an Active Directory, Forests, transitive trusts, etc. The 50 client computer limitation will not be an issue here since this network will be comprised of this server, a web server and a few other hosts. Because it is a 'package' and does provide services that are normally found placed on separate servers, it is complex, demands attention to detail and can be easily miss-configured leaving the box potentially vulnerable to attacks.

Microsoft made a change when they produced Exchange 2000 and removed the directory service that was found in previous versions of Exchange. Exchange 2000 utilizes the directory services of Windows 2000 Active Directory which means that the Small Business Server 2000 along with the services mentioned above is also a Domain Controller and will provide DNS services for the local network. This of course brings another level of complexity into the situation. When building an Active Directory network, Microsoft recommends that each domain contain at least two domain controllers. This in turn would provide redundancy in case of a hardware failure or other types of catastrophes. The long term plan is to incorporate another domain controller on the network but due to budget constraints we will have to start with just this one DC. The plan is to use an external storage device and basically back the complete system up so that given a worst case scenario the system could be brought back on line in a matter of 2 or 3 hours. Based on the current business model for this environment that is acceptable but may not work in other business environments such as a Web based business that needs a 24/7 presence. In that case a more resilient redundancy system such as raid 1 or raid 5 should be used.

The hardware was purchased through a local retailer. The sales person I worked with recommended that the parts be ordered from each of their appropriate manufacturers which would reduce the costs from the typical 'floor prices' in the store. By doing this I did see about a 30%+ decrease in cost versus purchasing the same parts from off the shelf. I did not get the pretty packaging that comes with off the shelf products but found that to be a non-issue and was quite pleased with the savings.

Microsoft's ¹[minimum requirements](#) for SBS 2000 are - Pentium II 300 MHZ, 128 Meg Ram, 4GIG available drive space, CD-ROM drive, 1 Network Adapter and a video card that will support 256 colors at 800x600 pixels. The recommended requirements are - PIII 500 MHz, or Dual PII 300 MHz processor or higher, 256 MB of RAM, two mirrored 4 GB hard disks, two modems, one for Shared Fax and one for Remote Access, Shared Modem service and Internet & Acceleration Server dial-up service.

Parts list:

Computer cabinet – Antec with 400watt power supply

Mother board – Gigabyte

Processor – AMD Athlon 1500 XP

RAM – 1024 Meg PC 2700

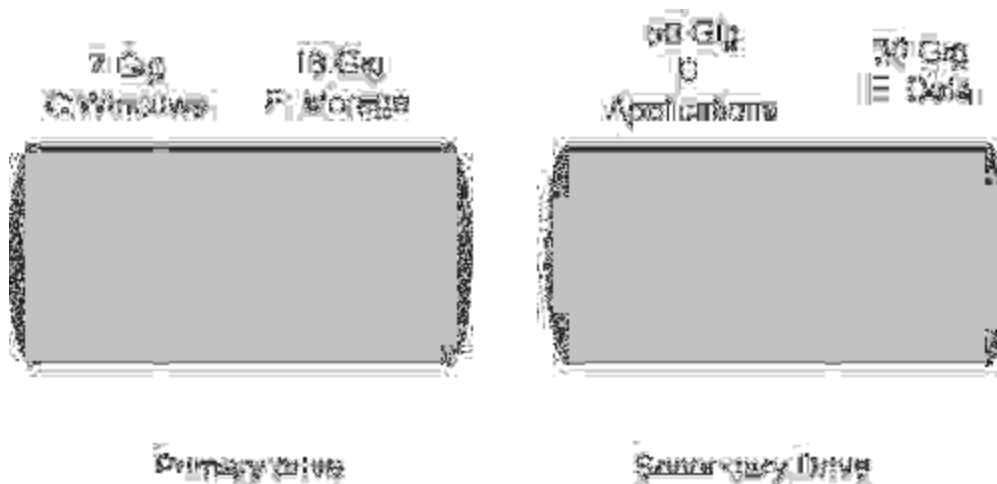
Hard drives – Western Digital 20 gig 7200 RPM, Western Digital 80 gig 7200 RPM

DVD – Samsung

CDRW – Samsung

Floppy Diskette – Sony

After building the computer - which came up with out a glitch – I was ready to proceed with the OS install.



The diagram above illustrates how the partitioning was to be done. Windows would be contained on the first partition of the primary drive and all the applications would be installed on the first partition of the secondary drive along with the Inetpub folder. The second partition of the secondary drive will be used for data and the second partition on the primary drive will be used for storage. There is also an external 120 gig drive that will connect via IEEE 1394 Firewire that will be used for backing up the complete system. All drives will be partitioned with NTFS. Small Business Server 2000 does require NTFS partitioning.

Small Business Server 2000 comes as a 3 Disc set along with a CD that contains Outlook 2000 and a CD that contains FrontPage 2000. There is also a CD set for the Small Business Server Service pack 1a which was ordered and will be applied at the appropriate time during the setup.

Before starting the install the decision was made not to use the default install path of C:\winnt. Although a small thing, it was felt that by not installing under the default path would add to the overall hardening of the PC. Since some malicious code has been written with the default path of the OS hard coded and by not using the default path on the install this could potentially break some malicious code, which of course would be a good thing. The other decision that was made would be to place the Inetpub folder away from its default path of being located on the same partition as the operating system. To accomplish both these goals I would not be able to do a normal install from the CD-ROM but would have to utilize the procedure called an unattended install. This procedure can be done in several different ways depending on what your needs are; setting up a single computer or several. Since I was going to be setting up just one system I decided to do a CD-ROM install and use an answer file located on a diskette. This specific procedure requires that the answer file be named 'winnt.sif'. The documentation and some utilities can be found on the install CD located under the \Support\Tools folder in a cab file called Deploy. The documentation does a good job of explaining how to build an answer file and provides a list of all of the possible headers and values as there are many. There are a few Knowledge Base articles that are definitely worth reviewing before you get started. These can be found at <http://support.microsoft.com/default.aspx?scid=kb;en-us;252504> ,

<http://support.microsoft.com/default.aspx?scid=kb;en-us;243286> and one that explains how to use the setupmgr.exe tool to create an answer file located at <http://support.microsoft.com/default.aspx?scid=kb;en-us;308662> .

The steps I actually used were –

- 1) Did a manual install of Windows 2000
- 2) Used the setupmgr.exe utility found in the deploy cab file to create a basic answer file of the system.
- 3) Modified that file to incorporate the necessary changes that would result in the install path of the operating system being different than the default and moving the root path of Inetpub (IIS) to a different partition away from the operating system.

One point that is extremely important and can save you from many hours of frustration that I experienced is that each header section of the answer file seems to have its own syntax. For example some sections use 'Yes or No' as values while others use '1 or a 0'. So the point is this – pay strict attention to this or you will also see the 'Invalid Value at line #' message when you start the install. The final point on this specific procedure that should also be noted is that since I am moving the IIS installation to a different physical drive and partition, the partition will have to already exist. This requires that the partitioning and formatting of the drives be done before the install actually starts. This can be accomplished by hanging the drives off an existing Windows 2000 system or using a partitioning tool like Partition Magic or following the procedure that I used above.

Below is the answer file that was used to assist in the unattended install with some sanitizing.

[Data]

AutoPartition=0
MsDosInitiated="0"
UnattendedInstall="Yes"

[Unattended]

UnattendMode=ProvideDefaults
OEMSkipEula=Yes
OemPreinstall=No
TargetPath=\WINNT50

[GuiUnattended]

OEMSkipWelcome=1
OEMSkipRegional=1
AdminPassword=thepasswordhere
TimeZone=XX

```
[UserData]
  FullName="My name"
  OrgName="My Company"
  ComputerName=COMPUTERNAME
  ProductID="XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX"
```

```
[Display]
  BitsPerPel=8
  Xresolution=800
  YResolution=600
  Vrefresh=60
```

```
[LicenseFilePrintData]
  AutoMode=PerServer
  AutoUsers=5
```

```
[TapiLocation]
  CountryCode=1
  AreaCode=555
```

```
[RegionalSettings]
  LanguageGroup=1
```

```
[Identification]
  JoinWorkgroup=WORKGROUP
```

```
[Components]
  accessopt=Off
  calc=On
  cdplayer=Off
  certsrv=Off
  certsrv_client=Off
  certsrv_server=Off
  charmap=Off
  chat=Off
  deskpaper=Off
  dialer=On
  fp=On
  freecell=Off
  hypertrm=On
  iis_common=On
  iisdbg=Off
  iis_doc=Off
  iis_ftp=On
  iis_htmla=Off
```

iis_inetmgr=On
iis_nnntp=On
iis_nnntp_docs=Off
iis_smtp=On
iis_smtp_docs=Off
iis_www=On
indexsrv_system=On
LicenseServer=Off
media_clips=Off
media_utopia=Off
minesweeper=Off
mousepoint=Off
mplay=Off
msmq=Off
mswordpad=On
netcis=On
netoc=On
objectpkg=Off
paint=Off
pinball=Off
rec=Off
reminst=Off
rstorage=Off
solitaire=Off
templates=Off
TSClients=On
TSEnable=On
vol=On

[Networking]

InstallDefaultComponents=No

[NetAdapters]

Adapter1=params.Adapter1

Adapter2=params.Adapter2

[params.Adapter1]

INFID=pci\ven_10ec&dev_8139&subsys_813910ec

ConnectionName = "Private"

[params.Adapter2]

INFID=pci\ven_10b7&dev_9200&subsys_100010b7

ConnectionName = "Public"

[NetClients]

MS_MSClient=params.MS_MSClient

```
[NetServices]
    MS_SERVER=params.MS_SERVER

[NetProtocols]
    MS_TCPIP=params.MS_TCPIP

[params.MS_TCPIP]
    DNS=No
    UseDomainNameDevolution=No
    EnableLMHosts=Yes
    AdapterSections=params.MS_TCPIP.Adapter1,params.MS_TCPIP.Adapter2

[params.MS_TCPIP.Adapter1]
    SpecificTo=Adapter1
    DHCP=No
    IPAddress=192.168.101.10
    SubnetMask=255.255.255.0
    DefaultGateway=192.168.101.10
    WINS=No
    NetBIOSOptions=0

[params.MS_TCPIP.Adapter2]
    SpecificTo=Adapter2
    DHCP=No
    IPAddress=XXX.XXX.XXX.XXX
    SubnetMask=XXX.XXX.XXX.XXX
    DefaultGateway=XXX.XXX.XXX.X
    DNSServerSearchOrder=XXX.XXX.X.X,XXX.XXX.X.X
    WINS=No
    NetBIOSOptions=0

[NetOptionalComponents]
    ACS=0
    DHCPServer=0
    DNS=1
    IAS=0
    ILS=1
    LPDSVC=0
    MacPrint=0
    MacSrv=0
    Netcm=1
    NETMONTTOOLS=0
    SimpTcp=0
    SNMP=0
    WINS=0
```

```
[InternetServer]
  PathFTPRoot="d:\Inetpub\Ftproot"
  PathWWWRoot="d:\Inetpub\Wwwroot"
```

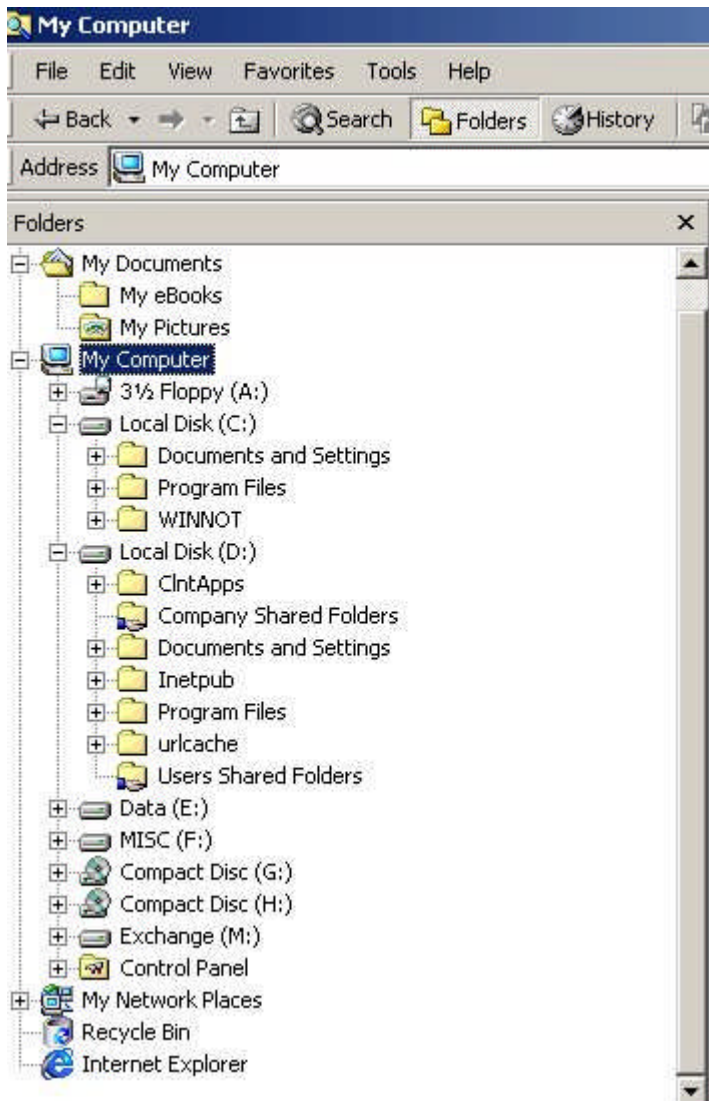
```
[TerminalServices]
  ApplicationServices=0
  PermissionsSetting=0
```

The [Unattended] header is where the values are placed that describes the install type and the path of the OS install. The choices for the install type are - GuiAttended, ProvideDefaults, DefaultHide, ReadOnly and FullUnattended. The FullUnattended and ProvideDefaults were used during testing. The 4th line provides the ability to point the install path to something other than c:\winnt – TargetPath=\WINNT50. A valid value does not contain a drive letter just the path name (i.e. \WINNT50). To move the IIS install from the default partition to a different one is found in the header [InternetServer] with the two options being PathFTPRoot and PathWWWRoot. The values for these two options do include the drive letter as shown in the listing above. The [Components] header section is where the instructions are found to include IIS as part of the install. This section basically provides the ability to include or not include any components during the Windows install.

To use this answer file with a CD-ROM install the file must be named winnt.sif and placed on a diskette that will be inserted into the floppy drive once the PC boots up and accesses the CD-ROM for startup. If you prefer you can change the startup sequence and place the CD-ROM before the diskette drive so you don't have to worry about the timing. My choice was to change the startup sequence in the BIOS to just the CD-ROM and then the primary hard drive as the secondary boot option and eliminate the floppy all together which keeps the install from being an eye hand coordination test.

When the text portion of the install starts the first step is to choose a partition to install Windows 2000. Since the partitioning and formatting had already been done on the previous install the only interaction required was to delete and recreate the 'C' partition with a fresh copy of the NTFS file system. If there is a previous install and the partition is not removed and recreated you could end up with a '001' as part of the file system name because Windows remembers previous installations. Once the 'C' partition has been deleted and recreated the setup files are immediately copied and the system will reboot. Since the diskette drive had been eliminated as a boot option the PC started back up and proceeded with the GUI portion of the install. The install process continued to completion using the answer file parameters and once completed did one more reboot.

We now have a basic Windows 2000 installation with an alternate path of 'c: \WINNOT' and Inetpub is located away from the operating system partition and is located on 'D' as seen below.



Another option that can be considered for installing the Inetpub folder on a different partition than the Windows operating system is to use the sysocmgr.exe utility. If you have an existing Windows server and you want to move or add the IIS services to that server you can follow a similar procedure using an answer file and sysocmgr.exe. The answer file is in the same format as the one used for the unattended install and an example is shown below.

[Components]

```
iis_www = on           ;World Wide Web Server

iis_common = on        ;Commonfiles

iis_inetmgr = on       ;Internet Information Services Snap-in

iis_ftp = on           ;File Transfer Protocol (FTP)
```

```

ins = off           ;NNTP Server

ims = on           ;SMTP Service

iis_htmla = off    ;Internet Services Manager (HTML)

iis_doc = off      ;Documentation

fp_extensions = off ;FrontPage 2000 Server Extensions

fp_vid_deploy = off ;Visual InterDev RAD REmote Deployment Support

```

```
[InternetServer]
```

```
PathFTPRoot="E:\Inetpub\FTPRoot"
```

```
PathWWWRoot="E:\Inetpub\WWWRoot"
```

As you can see above there are headers and under each header are options with values just like the unattended file that was used earlier.

```

/i: <master_oc_inf> - (required) Specifies the name of the master inf.
    The installation source path is taken from here.

/u: <unattend_spec> - Specifies unattended operation parameters.

/r          - Suppress reboot (when reboot is necessary).

/z          - Indicates that args that follow are not OC args
    and should be passed to components.

/n          - Forces the specified master inf to be treated as new.

/f          - Indicates that all component installation states
    should be initialized as if their installers had
    never been run.

/c          - Disallow cancel during final installation phase.

/x          - Suppresses the 'initializing' banner.

/q          - for use with /u. Runs the unattended installation
    without UI.

/w          - for use with /u. If a reboot is required, prompt
    the user instead of automatically rebooting.

/l          - Multi-Language aware installation

```

Here is a screen shot of the possible options that are available to you. So to continue with the example of using iis.txt as the answer file the command line syntax would be:


```
C:>\sysocmgr.exe /I:%windir%\inf\sysoc.inf /w /u:a:\iis.txt
```

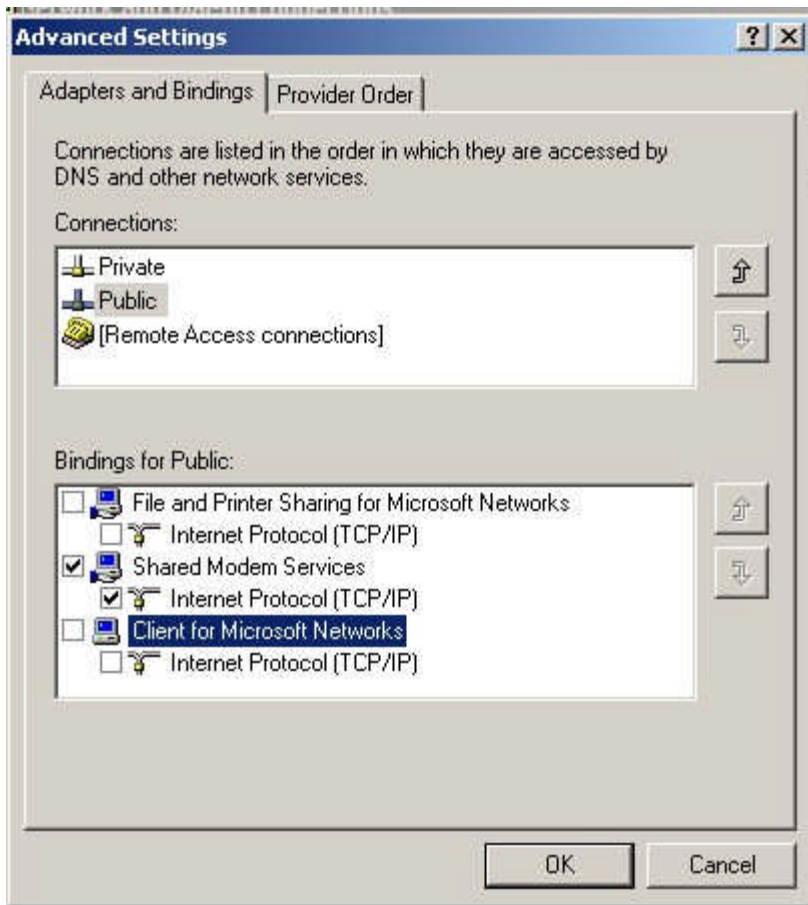
This would install the Inetpub folder on the 'E' partition and once it was finished would prompt for a reboot if required. The 'I' switch is required and points to the sysoc.inf file which is normally located in the hidden 'inf' Windows folder. The 'w' switch will cause the process to prompt for a reboot if required instead of proceeding and the 'u' switch points to the answer file which is located on the 'a' drive in the example above.

Next I added the recovery console by inserting CD 1 of the set, opening a command window and typing driveletter:\i386\winnt32.exe /cmdcons. Once installed it provides an additional option on start up to access a type of shell which can be used to possibly fix problems such as replacing damaged or missing files, disabling or enabling services, fixing the mbr, etc.

The next step was to install the drivers for the hardware. All install paths were changed from C: to D: which is the Applications partition.

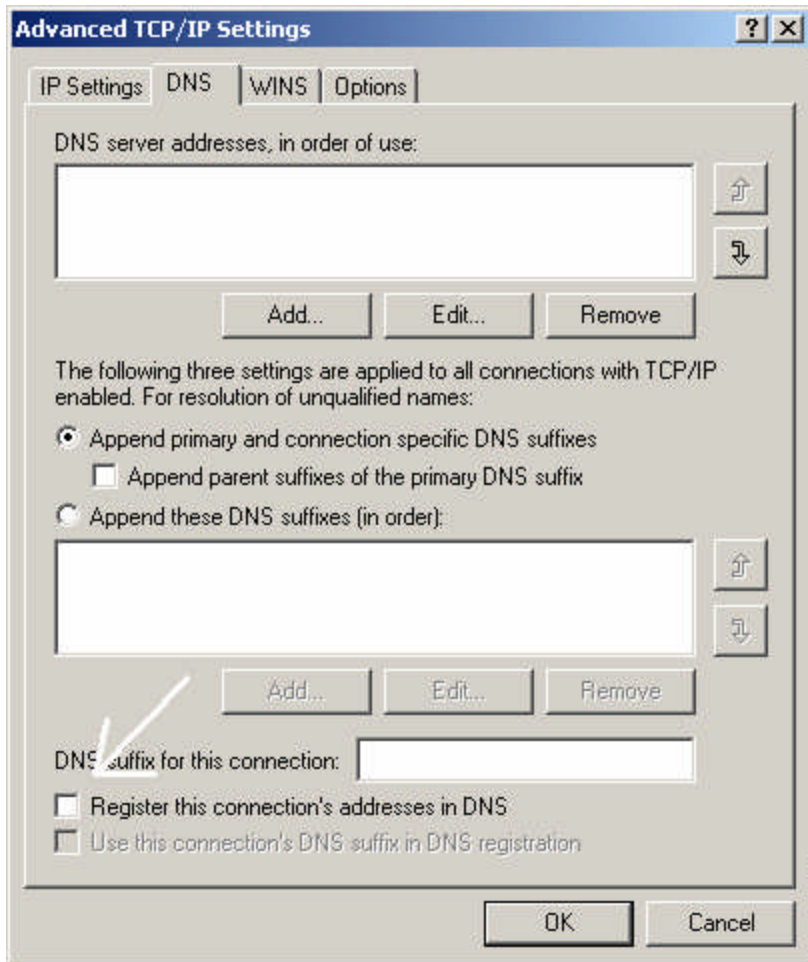
- Install ATI video drivers and DirectX
- Install Motherboard Drivers
- Install CD burning software (Nero 5.5)

Back on the Desktop I selected My Network Places, right clicked and selected properties to check and see if in fact my two connections had been renamed per the answer file to Private from Local Area Connection and to Public from Local Area Connection2 and they were. On the menu I selected Advanced and then Advanced Settings to display the Adapters and Bindings properties as shown in the screen shot below.



Once there I selected the Private adapter in the list and moved it so that it was listed first, selected the Public interface and unchecked the File and Printer Sharing for Microsoft Networks and unchecked the Client for Microsoft Networks. This step of moving the private adapter first is very important on a Multi-Homed PC that will be promoted to a domain controller later so that you don't encounter problems like are described in Microsoft's Q article [Q258296](http://support.microsoft.com/kb/q258296).²

© SANS Institute



Another important item on a multihomed computer that is going to be promoted to a domain controller is to uncheck the 'Register this connection's address in DNS' on the public NIC TCP/IP settings advanced properties page which is annotated above. This step and another which will be done once DNS is installed is described in the Microsoft Q article [Q272294](#)³ 'Active Directory Communication Fails on Multihomed Domain Controllers'.

To finish the Network changes I selected each connection name, right clicked and selected properties. Once there I checked the 'Show icon in taskbar when connected' check box. This is not required but just a preference of mine. I then closed the Network and Dial-up Connections window.

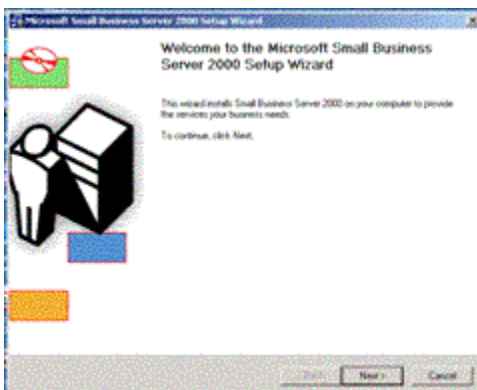
The next step was to start the Small Business Server install. One point I feel compelled to make at this juncture is that I did attempt a couple of variations which included updating the Windows Service pack level, applying hot fixes and upgrading the browser at this point of the install. These variations lead to the SBS install having errors and resulted in having to start the process from the beginning. The conclusion I came away with was to start the SBS install immediately after Windows 2000 has been installed and place the other items later in the process. The other steps to complete at this juncture was to

rename the Administrator account, leave the guest account disabled but changed the password to a long complex password and created an account to be used by the SQL server with a long complex password. One thing that I have found useful is to use Notepad to type in a long password or pass phrase so it can be copied into the account password fields when assigning passwords to accounts like above.

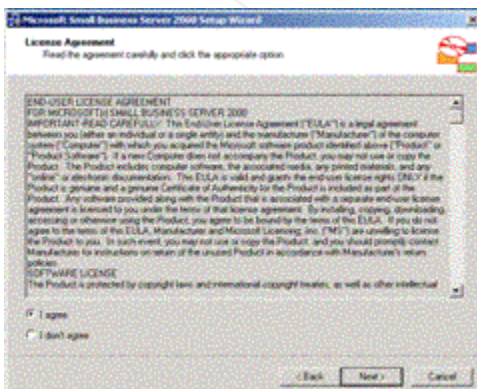
Starting the Small Business Server install is just a matter of placing CD 1 of the set back in the PC and the SBS opening screen should appear.



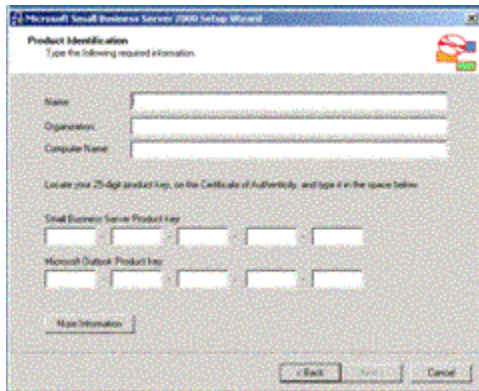
From here we click the 'Setup Small Business Server' link.



The Welcome screen appears and we click 'Next' to continue.

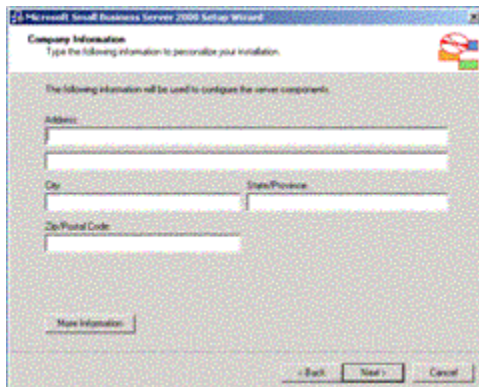


You are presented the EULA (license agreement). Select 'I agree' and click the 'Next' button.



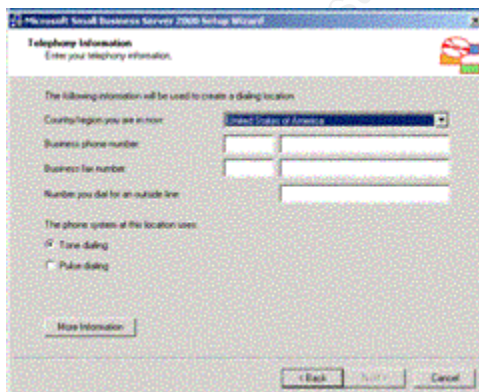
The screenshot shows the 'Product Identification' screen of the Microsoft Small Business Server 2000 Setup Wizard. The window title is 'Microsoft Small Business Server 2000 Setup Wizard'. The subtitle is 'Product Identification' with the instruction 'Type the following required information.' Below this, there are three text input fields for 'Name', 'Organization', and 'Computer Name'. A note states: 'Locate your 25-digit product key, on the Certificate of Authenticity, and type it in the space below.' There are two rows of five-character product key input boxes. The first row is for the 'Small Business Server Product key' and the second row is for the 'Microsoft Outlook Product key'. A 'More Information' button is located below the product key fields. At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

Next is the Product Identification screen that requires your Name, Organization, Company Name and product keys for both SBS and Outlook.



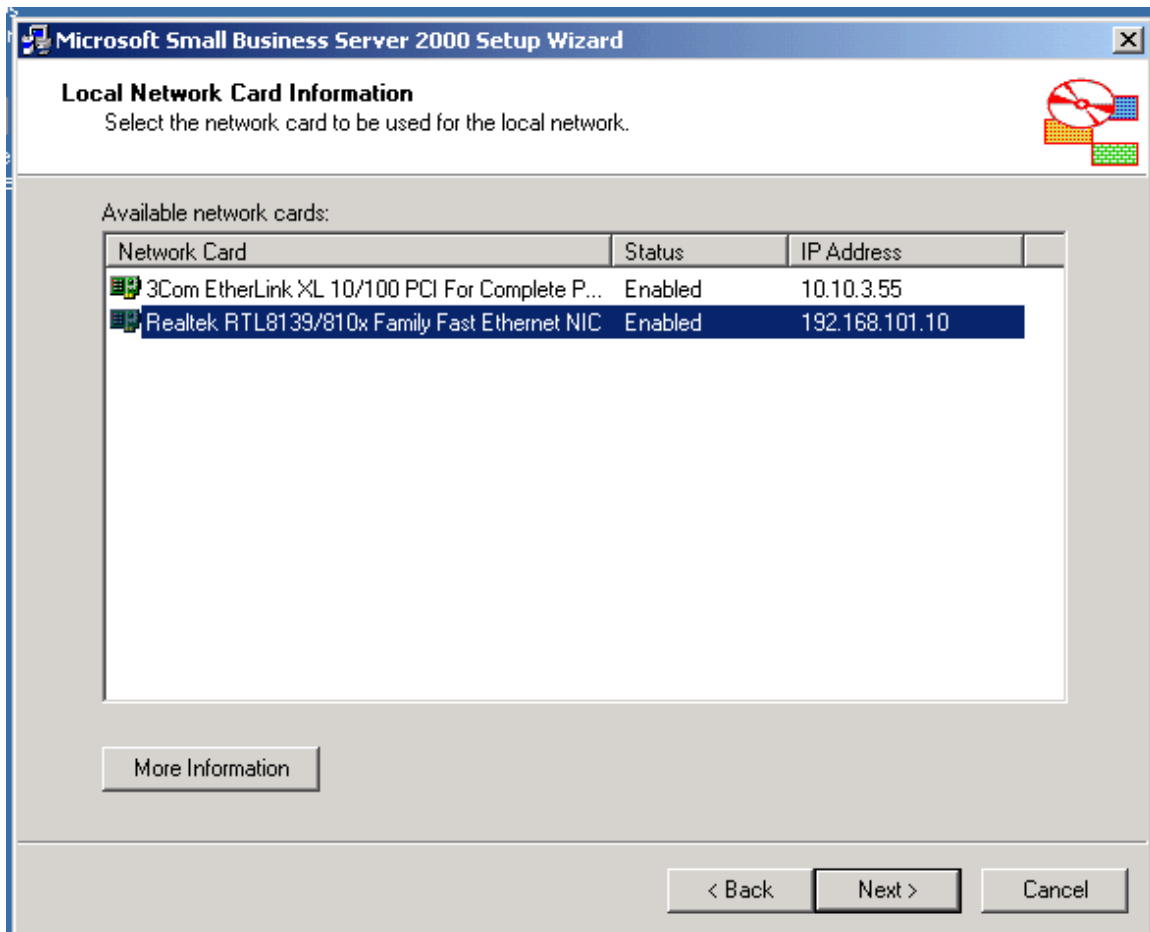
The screenshot shows the 'Company Information' screen of the Microsoft Small Business Server 2000 Setup Wizard. The window title is 'Microsoft Small Business Server 2000 Setup Wizard'. The subtitle is 'Company Information' with the instruction 'Type the following information to personalize your installation.' Below this, a note states: 'The following information will be used to configure the server components.' There are four text input fields: 'Address', 'City', 'State/Province', and 'Zip/Postal Code'. A 'More Information' button is located below the input fields. At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

The next screen is the Company Information screen for the business address.

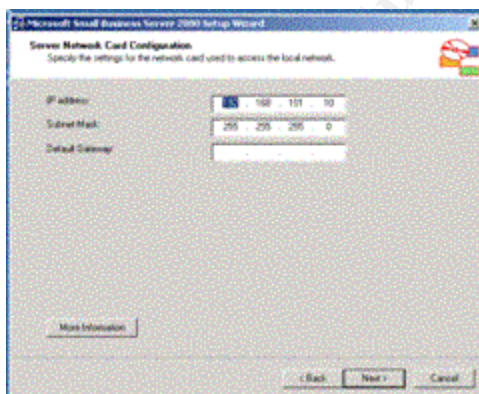


The screenshot shows the 'Telephony Information' screen of the Microsoft Small Business Server 2000 Setup Wizard. The window title is 'Microsoft Small Business Server 2000 Setup Wizard'. The subtitle is 'Telephony Information' with the instruction 'Enter your telephony information.' Below this, a note states: 'The following information will be used to create a dialing location.' There is a dropdown menu for 'Country/region you are in now' with 'United States of America' selected. Below this are three text input fields for 'Business phone number', 'Business fax number', and 'Number you dial for an outside line'. There are two radio buttons for 'The phone system at this location uses': 'Tone dialing' (which is selected) and 'Pulse dialing'. A 'More Information' button is located below the input fields. At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

Next is the Telephony Information screen for the business phone number and fax numbers.



The next screen show above is where you select the 'local' network or 'inside' network card.



The next screen allows you to change the IP address of the private address. I plan to use the current address space so we just click next to continue.

Microsoft Small Business Server 2000 Setup Wizard

New Domain Information
Type the DNS and NetBIOS names for the new domain.

Type the full DNS name for the new domain (for example: smallbusiness.local). If you have a domain name and will host an Internet site on this server, click More Information for additional details on naming your domain.

Full DNS name for new domain:

Type the full NetBIOS name for the new domain. This is the name that earlier versions of Windows will use to identify the new domain.

Domain NetBIOS Name:

[More Information](#)

< Back Next > Cancel

Next is the New Domain Information screen. This is where the Fully Qualified Domain name of your company is entered. The NetBIOS name will be automatically entered as you type in the FQDN name. This is the name that Active Directory will use on the internal LAN. It is considered best practice to use a non-registered DNS name like mycompany.local versus mycompany.com. This will help to keep potential DNS problems from occurring along with potential security issues.

Directory Services Restore Mode Administrator Password
Specify a password to use when starting the computer in Directory Services Restore Mode.

Type and confirm the password you want to assign to this server's Directory Services Restore Mode Administrator account. To be used when the computer is started in Directory Services Restore Mode.

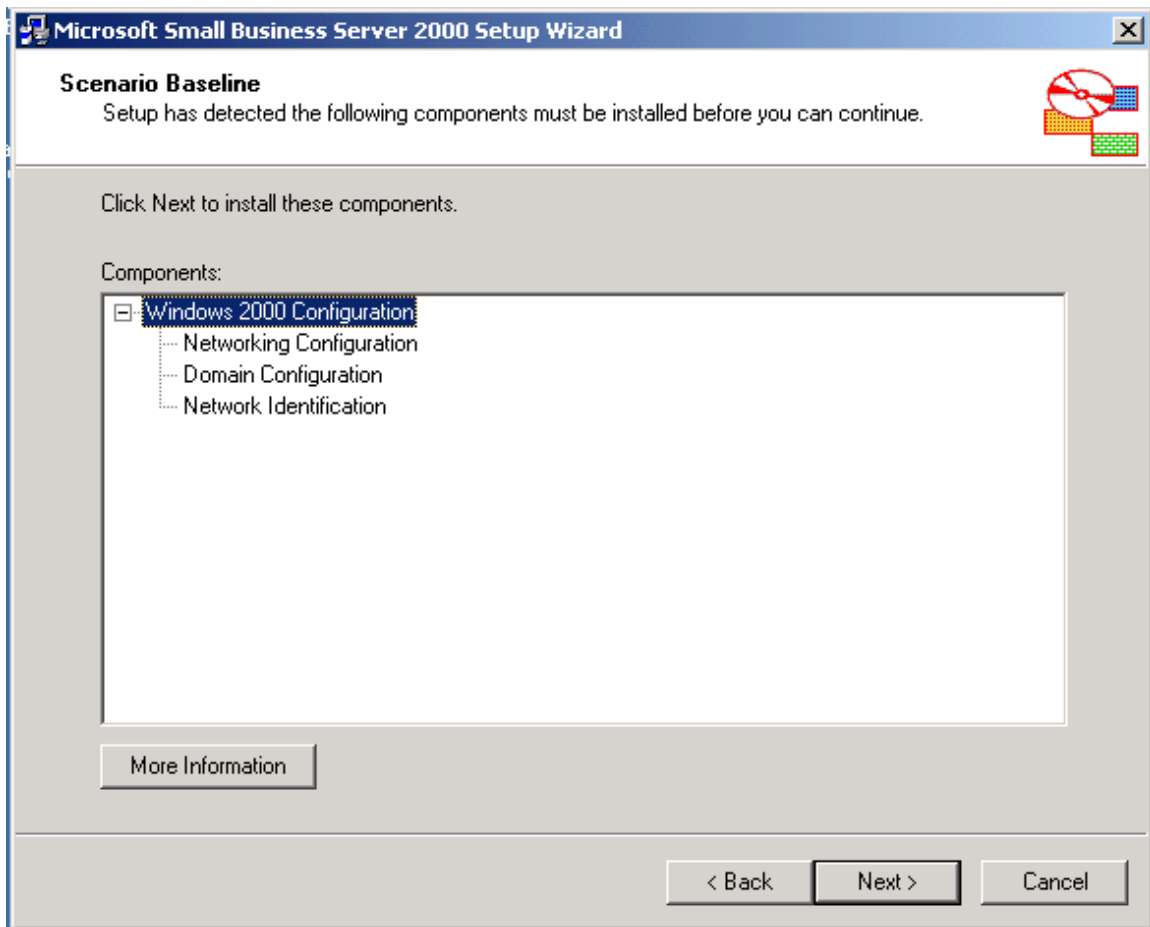
Password:

Confirm password:

[More Information](#)

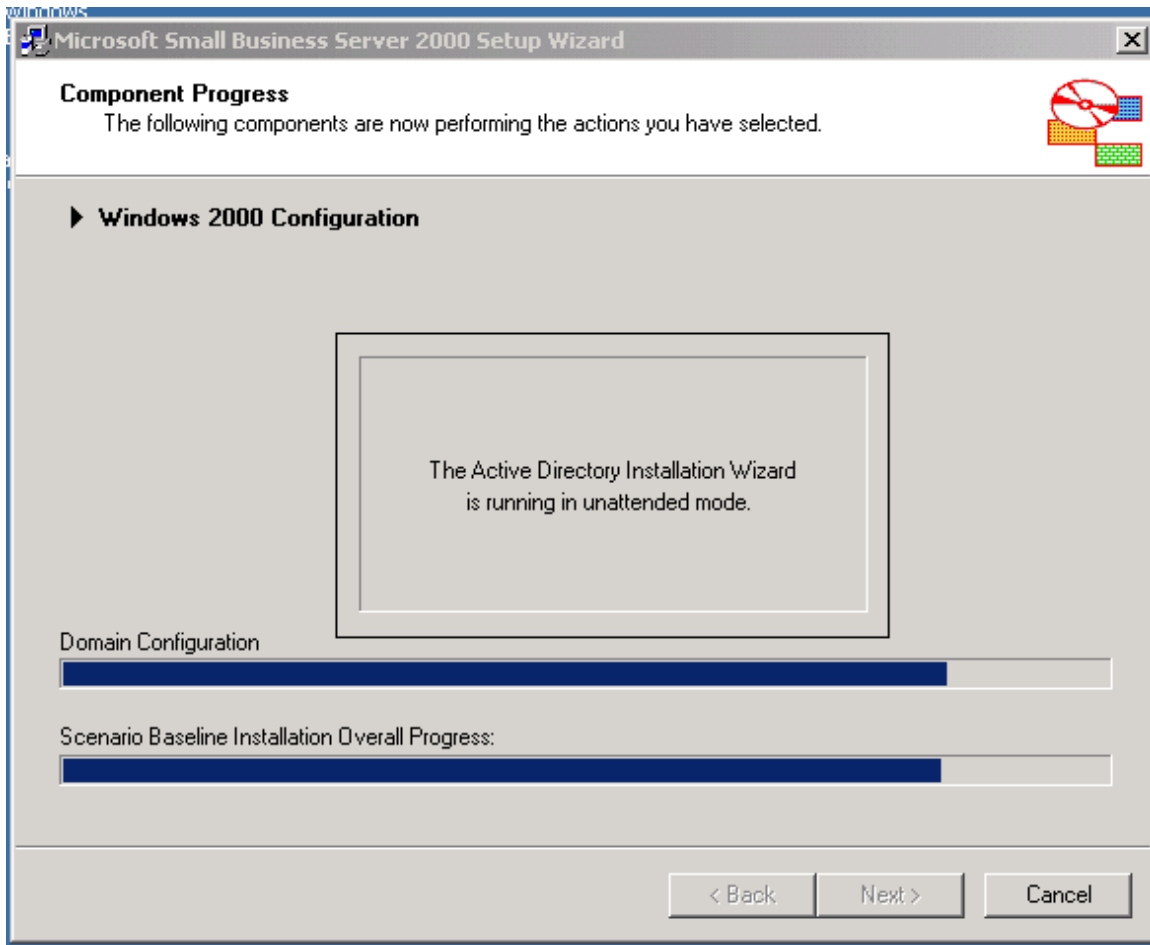
< Back Next > Cancel

Next is the Directory Services Password. This is the password that you will enter when you start the PC in the Active Directory Restore mode. This password should be different than the Administrator password.

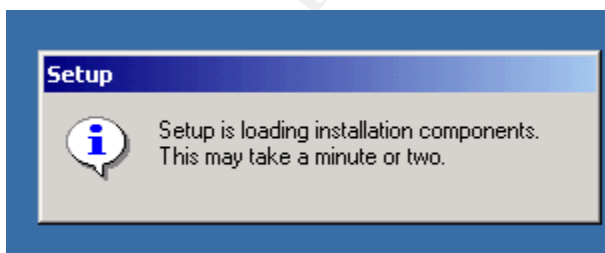


Next you will see the Scenario Baseline screen which will list the components that need to be installed. Click 'Next' to continue.

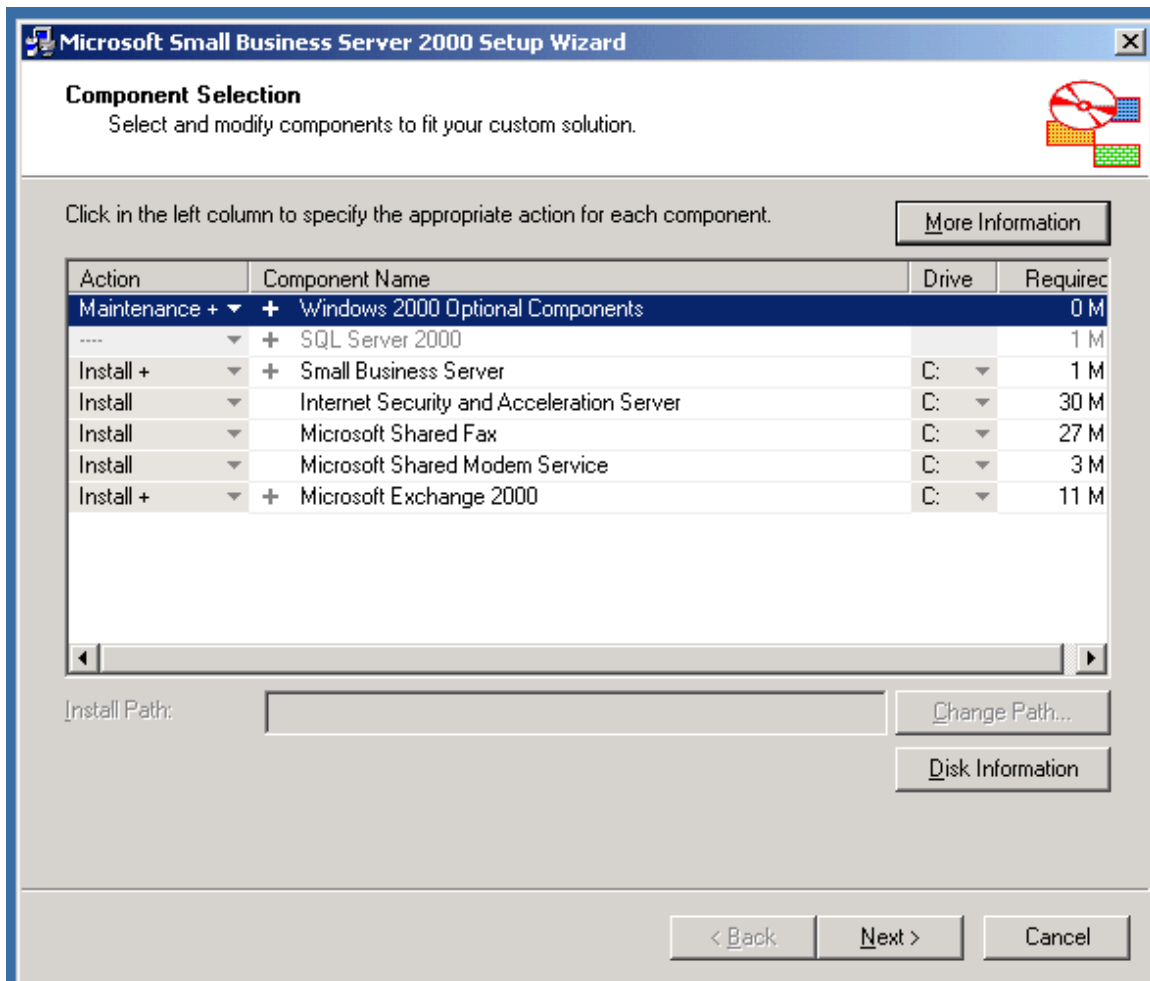
© SANS Institute



The Component Progress screen will keep you abreast of the current action that is taking place. This specific process may require a couple of restarts depending on what changes need to be made. For example if you are changing the PC name to something different, a restart is required for that change to take effect before the Active Directory service is installed during the unattended DC Promo stage.

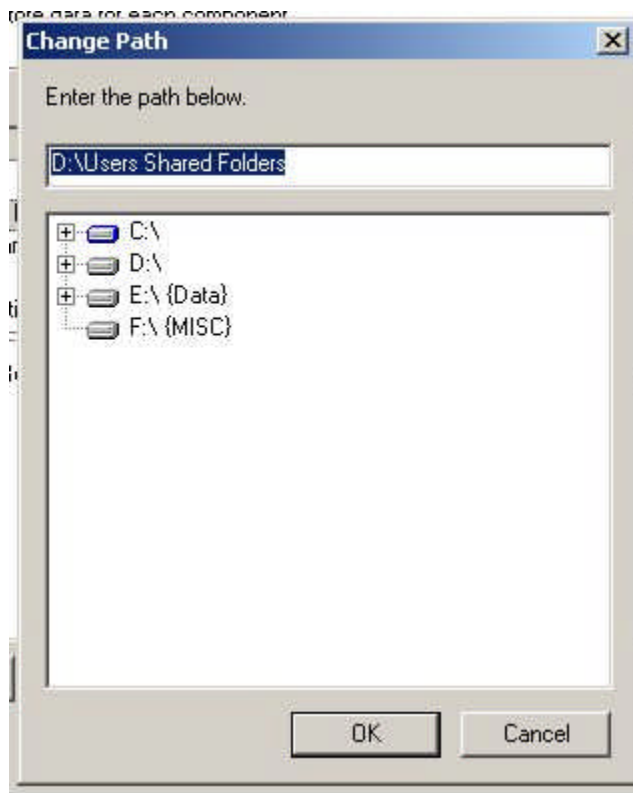


After each restart you will see the Setup message again. But do not be alarmed as the process is not actually starting over but will continue where it had left off.



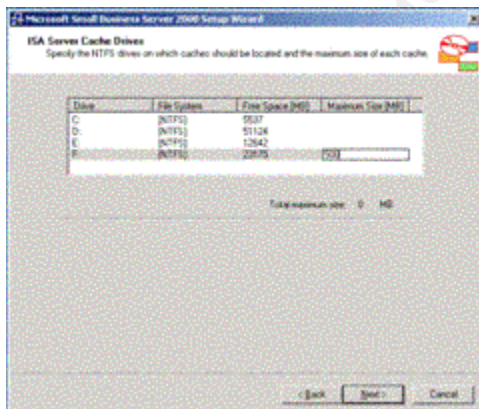
After the multiple restarts the Small Business Server 2000 Setup Wizard will start. The component selection screen shown above allows you to select or deselect the different components. As you can see by default SQL server is not selected. If you choose to install SQL Server 2000 you must also expand the listing and select the child components or you will not get a complete install of SQL.

© SANS Institute

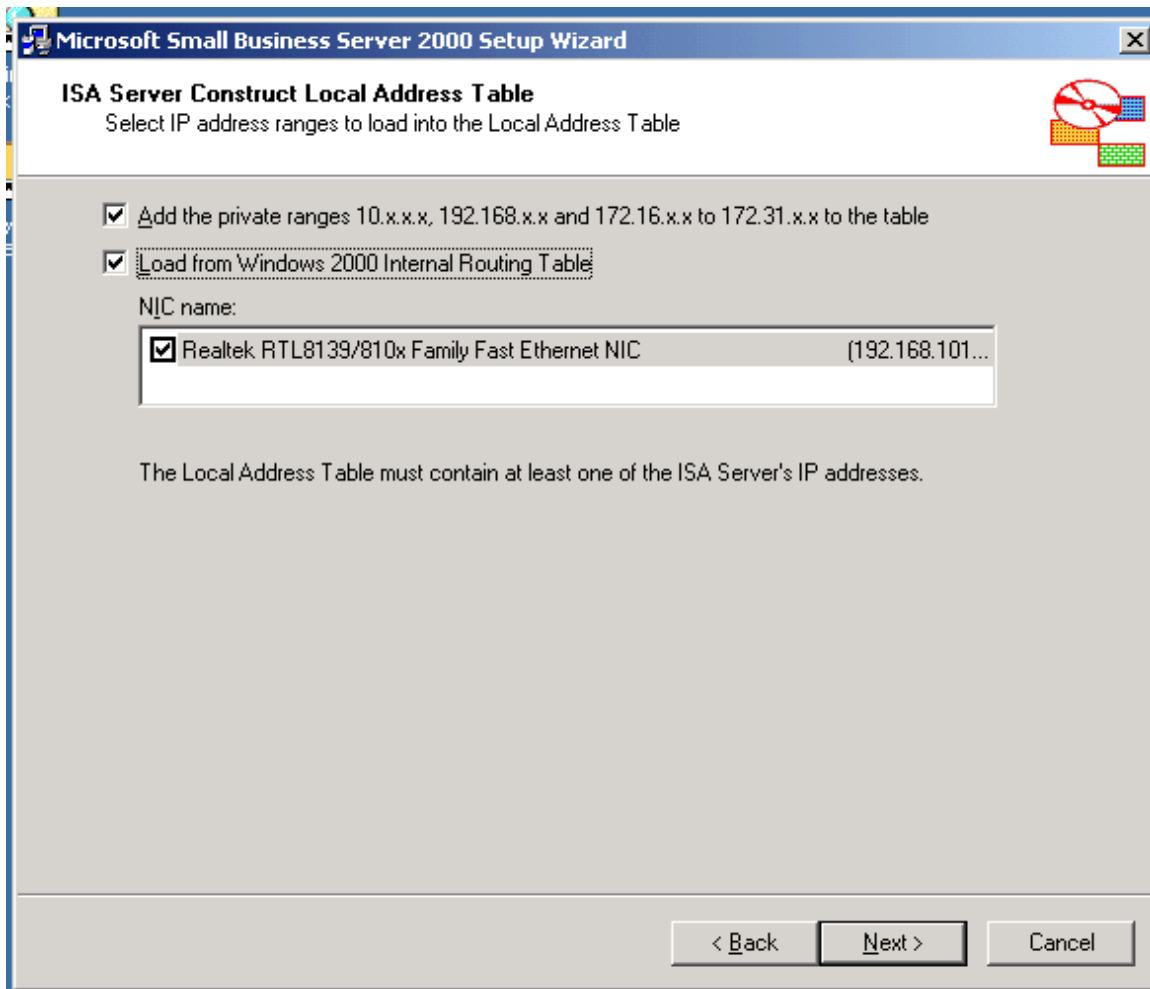


We are also changing the drive letter here to 'D' to keep our OS as isolated as possible.

If you have chosen to include SQL in the install you will be presented with a couple of screens with choices (i.e. SQL collation settings, network libraries, etc.). Accepting the defaults for most situations is acceptable.



Next is the ISA Server Cache Drives. The default is 100 Meg. You can change the default size and location. The recommendation for calculating a total is to start with 100 Meg and add .5 Meg for each user.



The ISA Server Construct Local Address Table will build your local address table for you by using the options listed above. My choice it to uncheck these options and just add my local address space manually like below.

© SANS Institute

Microsoft Small Business Server 2000 Setup Wizard

ISA Server Local Address Table Configuration

Enter the IP address ranges which span the internal network address space.

To create a new internal IP range, type in the range and click Add.

From: 192 . 168 . 101 . 0 To: 192 . 168 . 101 . 255

Add

Internal IP ranges:

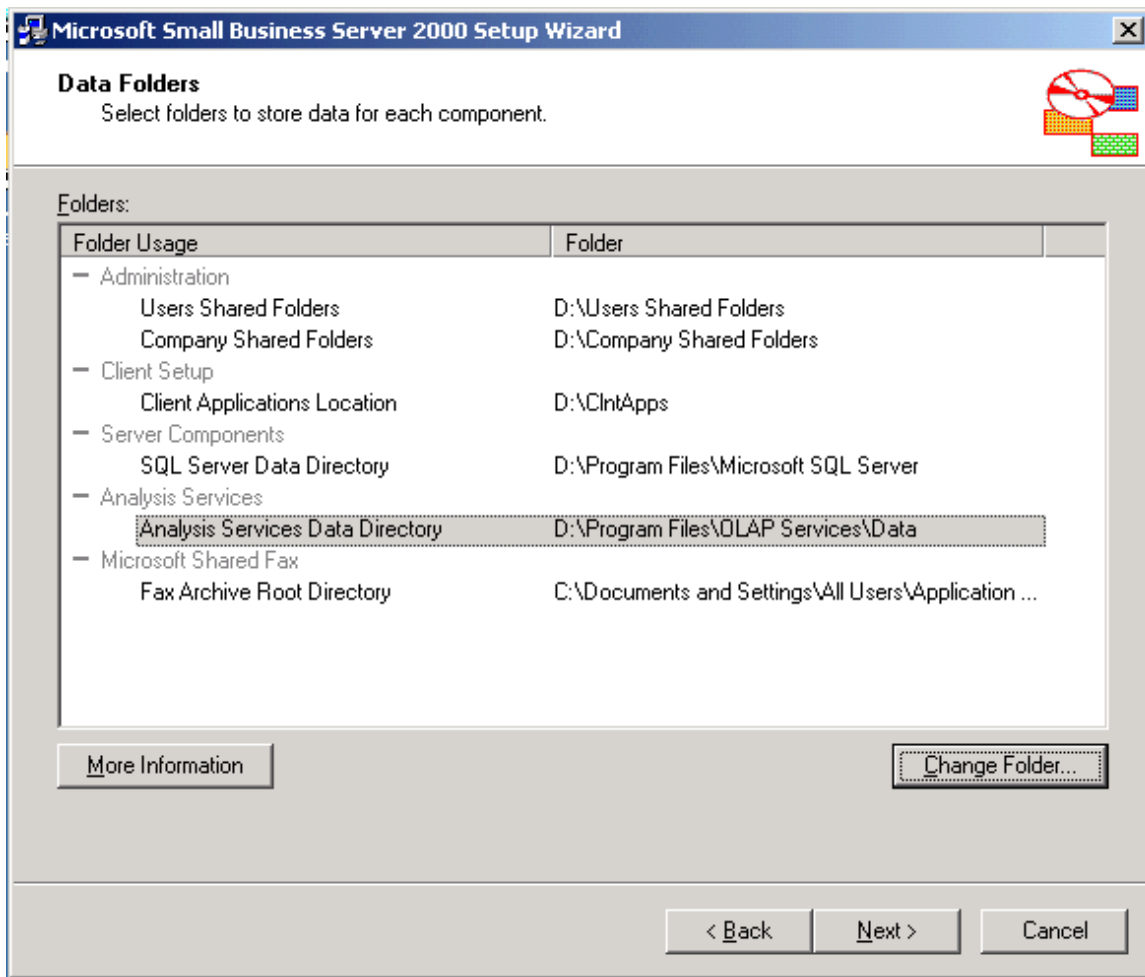
From	To

Remove

< Back Next > Cancel

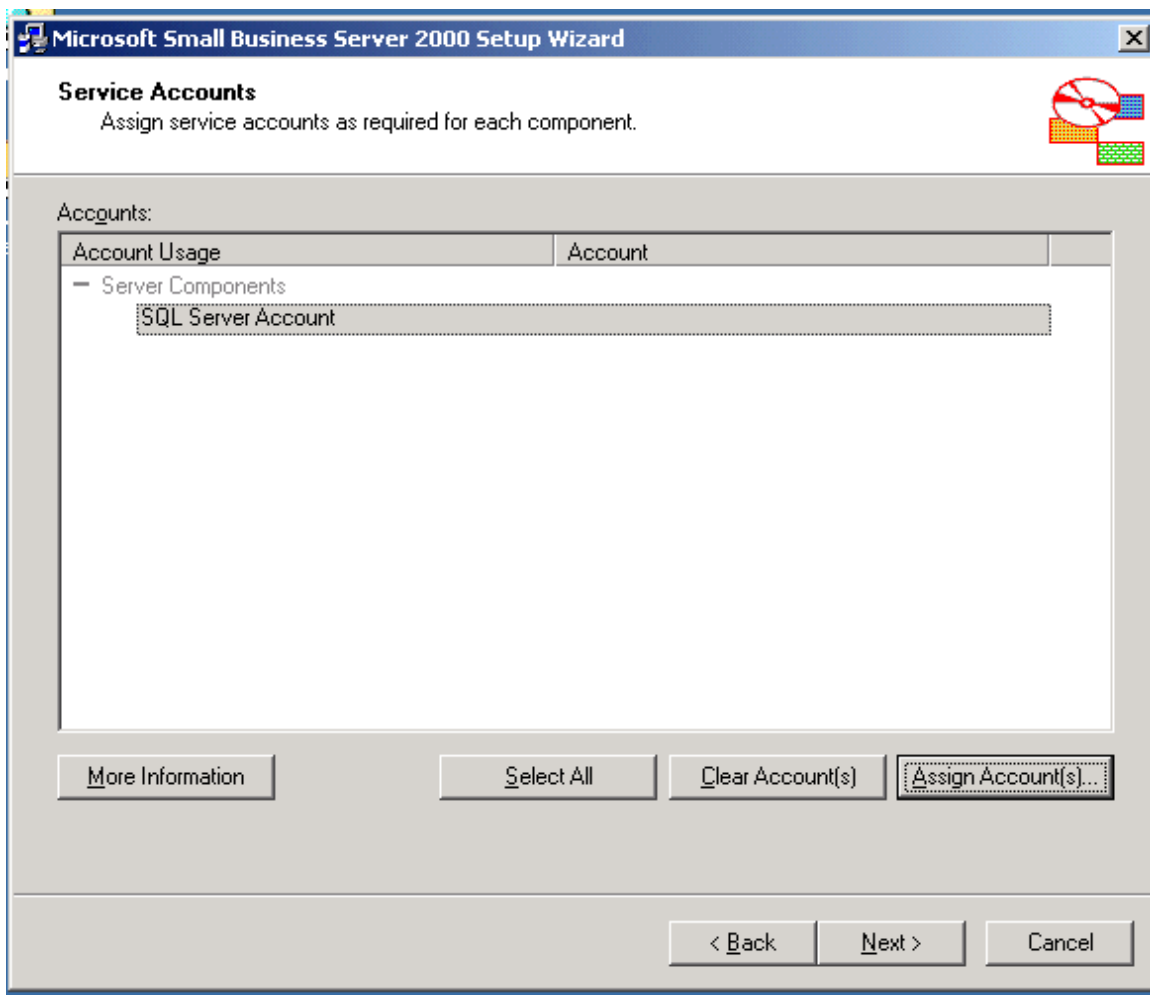
Enter the address space of your local network and then click the Add button then click 'Next' to continue.

© SANS Institute



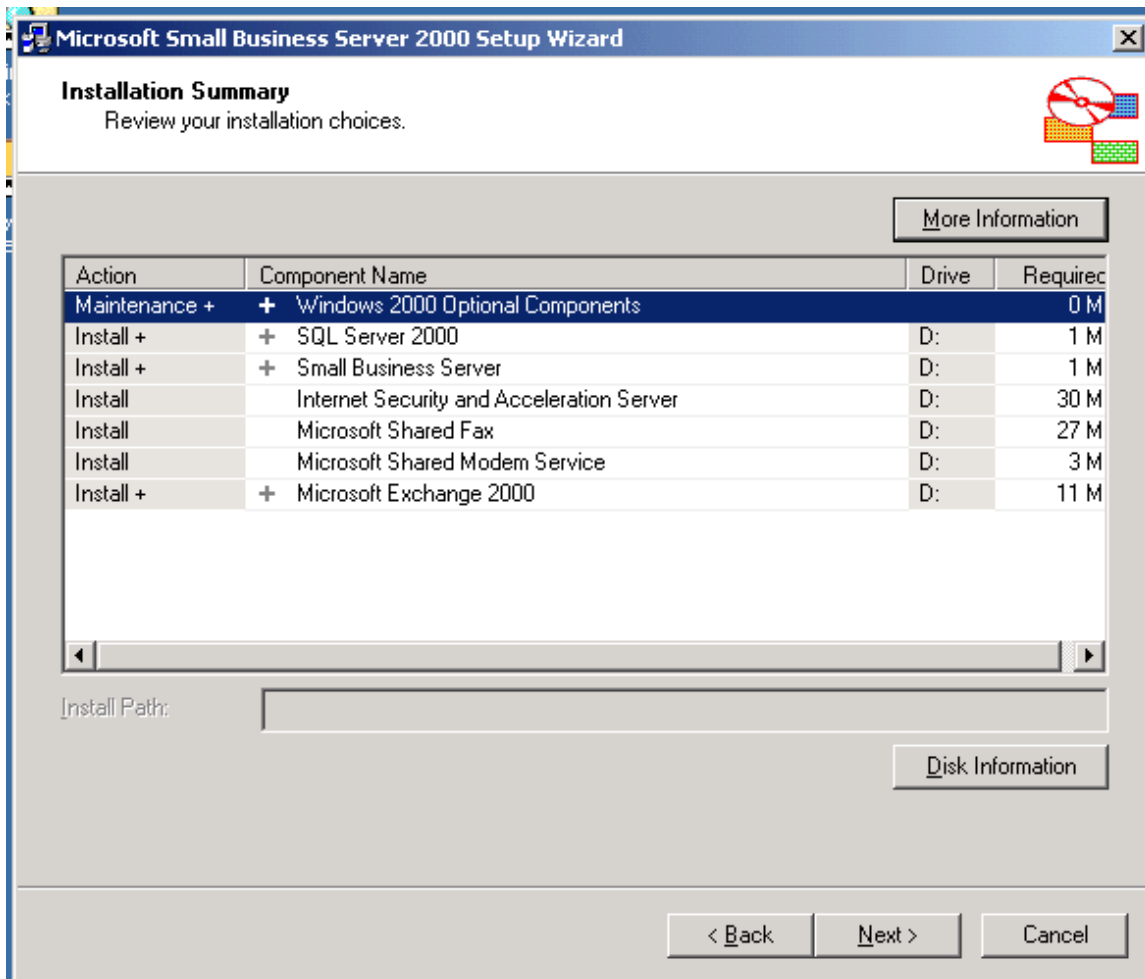
Next the data folders path is also changed from the default of 'C' to 'D'.

© SANS Institute 2004

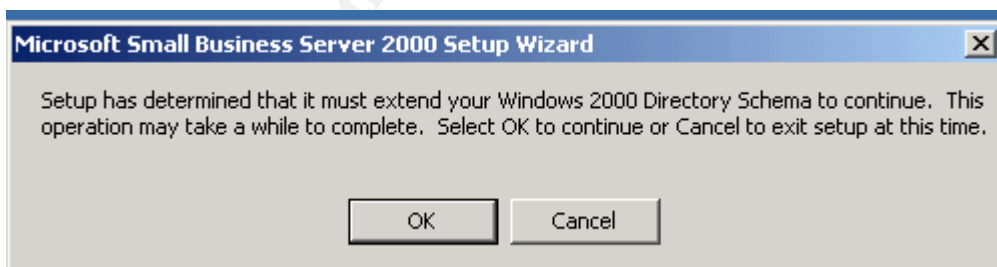


The Service Accounts screen prompts for a user account to use. The account must already exist and if you do not choose a specific account the local service account will be used. This is where we will use the account that was created earlier for SQL server.

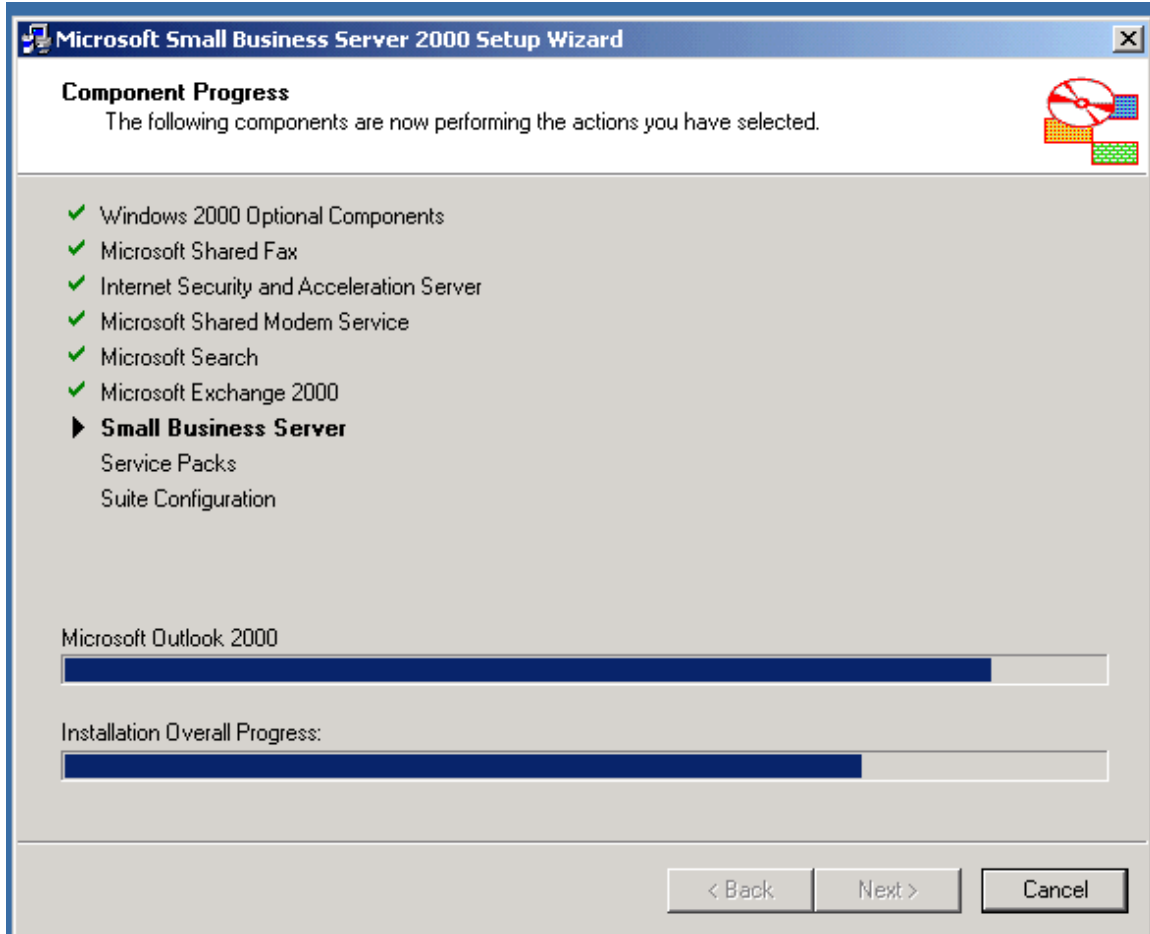
© SANS Institute



Here is the Install Summary screen where we can review the changes that were made. Once we are satisfied with our choices we can click 'Next' to continue.



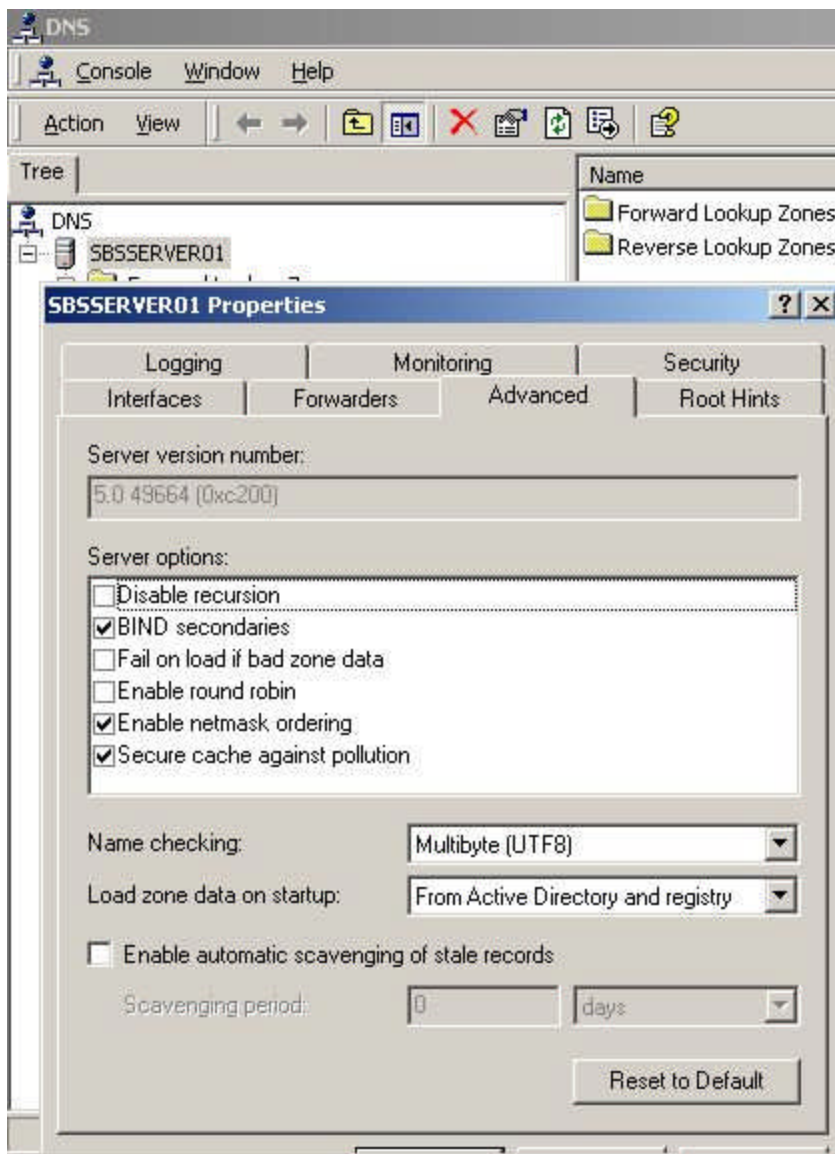
Since Exchange is being installed as part of the process the Active Directory Schema has to be extended. It is important to mention that for this process to be successful you must be logged on with an account that has permission to extend the schema. By default the local administrator of the Small Business Server is a member of the Schema Admins group.



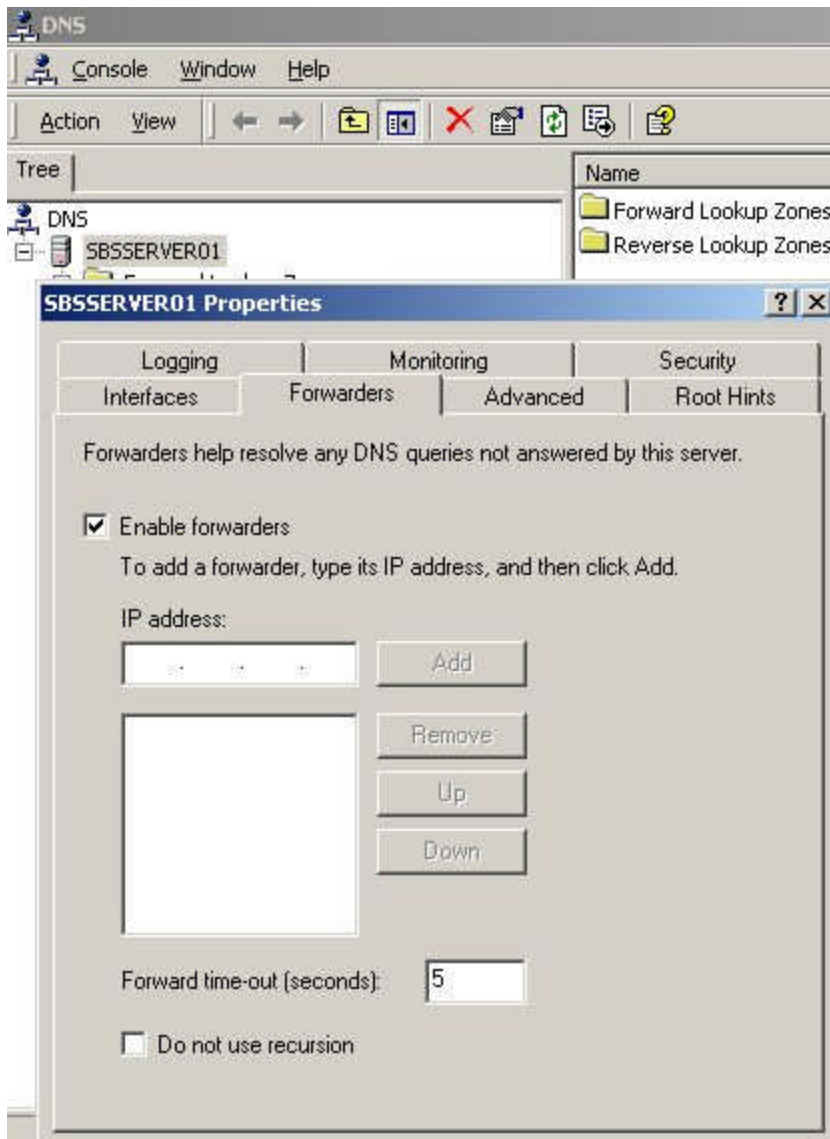
Once this part of the process begins you can just sit back and wait to be prompted for each of the CD's in the set. Keep in mind that depending on the PC specifications this process can take a while to complete.

Once the install is done you will be prompted to do a restart and should have a successful install of the Small Business server up and running.

© SANS Institute

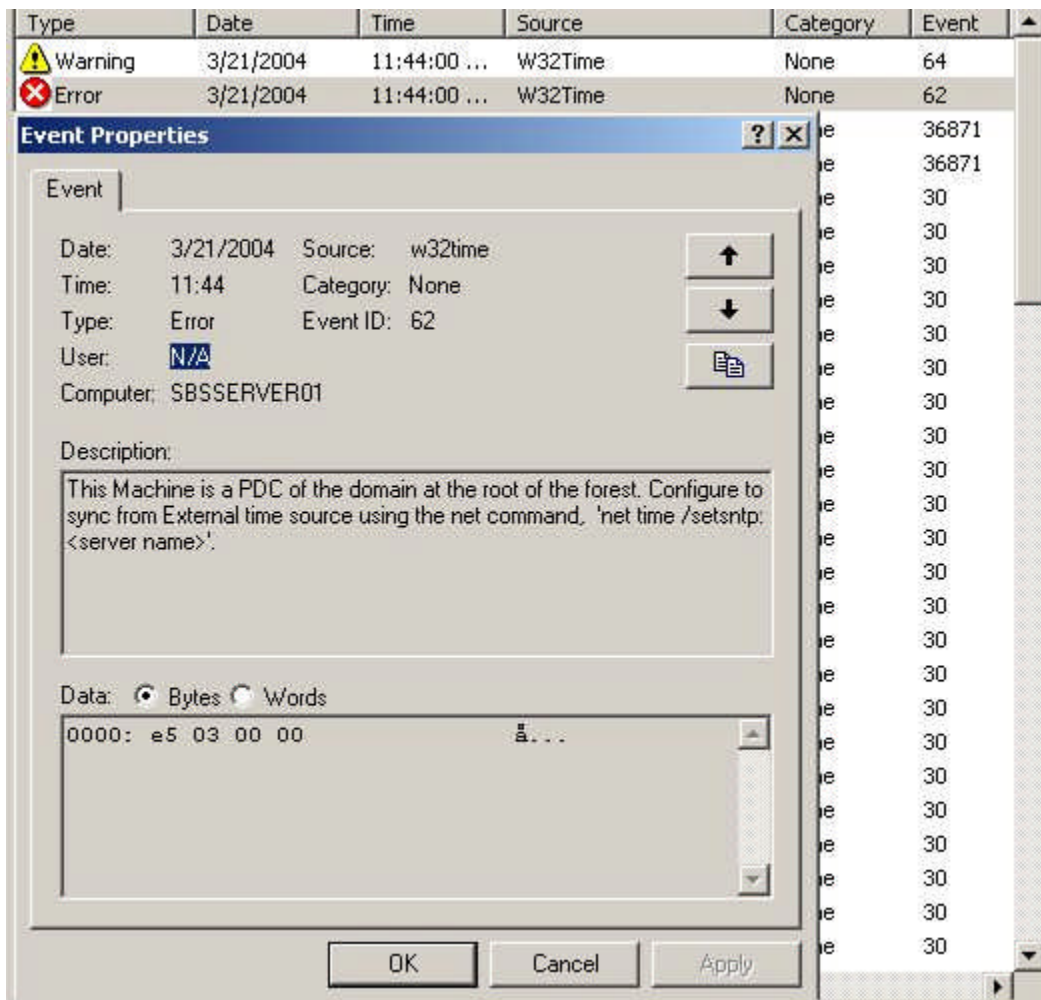


Before proceeding on we want to revisit Microsoft's Q article [Q272294](https://support.microsoft.com/kb/q272294) and complete the second step mentioned there of disabling round robin in DNS. This property is found on the Advanced tab of the DNS server's properties page and should be unchecked.



Also as an option we can restrict the DNS communication of the Small Business Server by enabling forwarders and adding the DNS servers of our ISP. Since the DNS server is only authoritative for the local active directory domain and will need to communicate with outside DNS servers to resolve public addresses we can limit who the Small Business Server talks with so as to limit the chance of being a victim of possible [DNS poisoning](#).

Since this PC is now a Domain Controller of the root domain of a forest and has the PDC emulator FSMO role it is providing time services. Windows 2000 Active Directory utilizes Kerberos authentication which is time sensitive and therefore the time on all the PC's in the domain will need to be kept in sync. If you monitor the Event Log you will see error messages about Windows complaining about it.



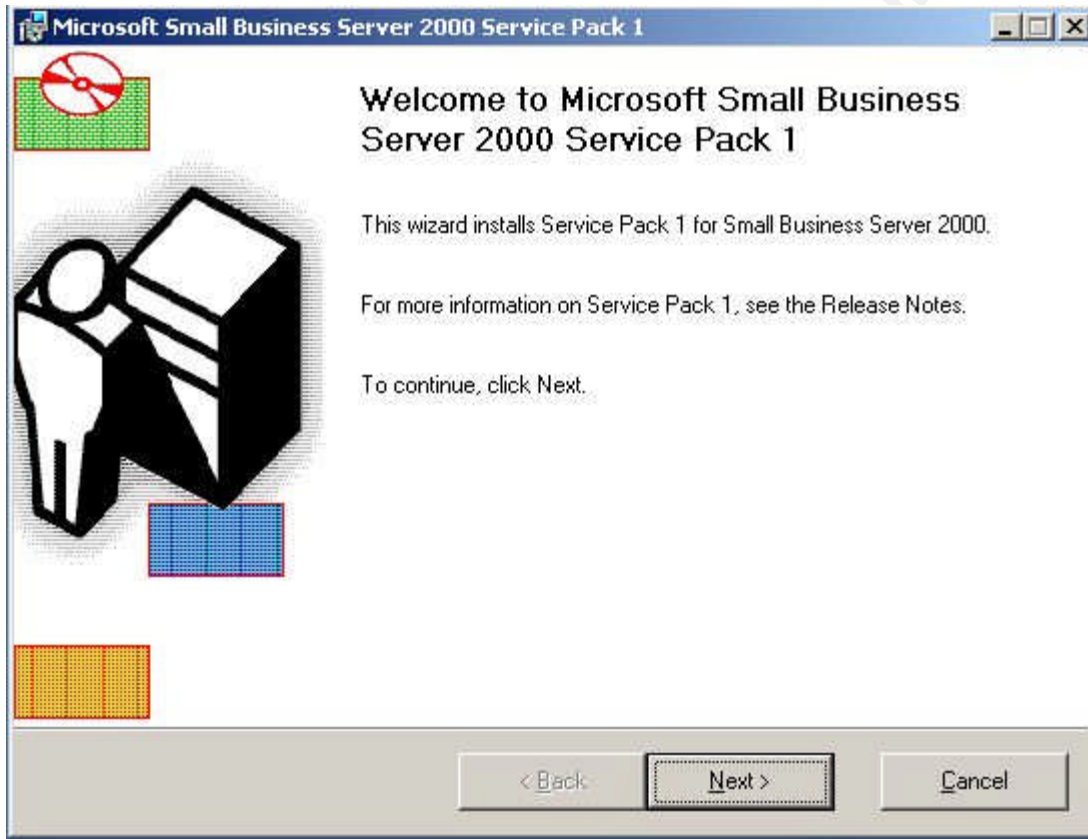
The error provides part of the solution to the issue in the description. The resolution to this problem is actually two fold and detail instructions can be found in the Microsoft Q article [Q323621](#). First we need to create a packet filter for the NTP protocol and then use the net time command and provide time server(s) that it can communicate with. The syntax of the command is –

C:\>net time /setsntp:x.x.x.x or DNS name

There appears to be an issue with the syntax that is provided in the 'net time /?' output. According to information in the Q article the syntax implies using a single server or server list while Microsoft recommends only using one DNS name or IP address and that the "W32Time service only recognizes the first DNS name or IP address that is listed, and listing more than one might return an error"²⁹. It does go on to say that if you need to list multiple time servers, they need to be separated by a space and the list must be placed in quotes. To test that the service has been configured properly you can use the net stop w32time command in a command window and then enter w32tm /resync command and review the output. Look for a line that says '*****SetSystemTime()*****', the next two lines should reflect a successful time sync if the configuration is correct and packet filter

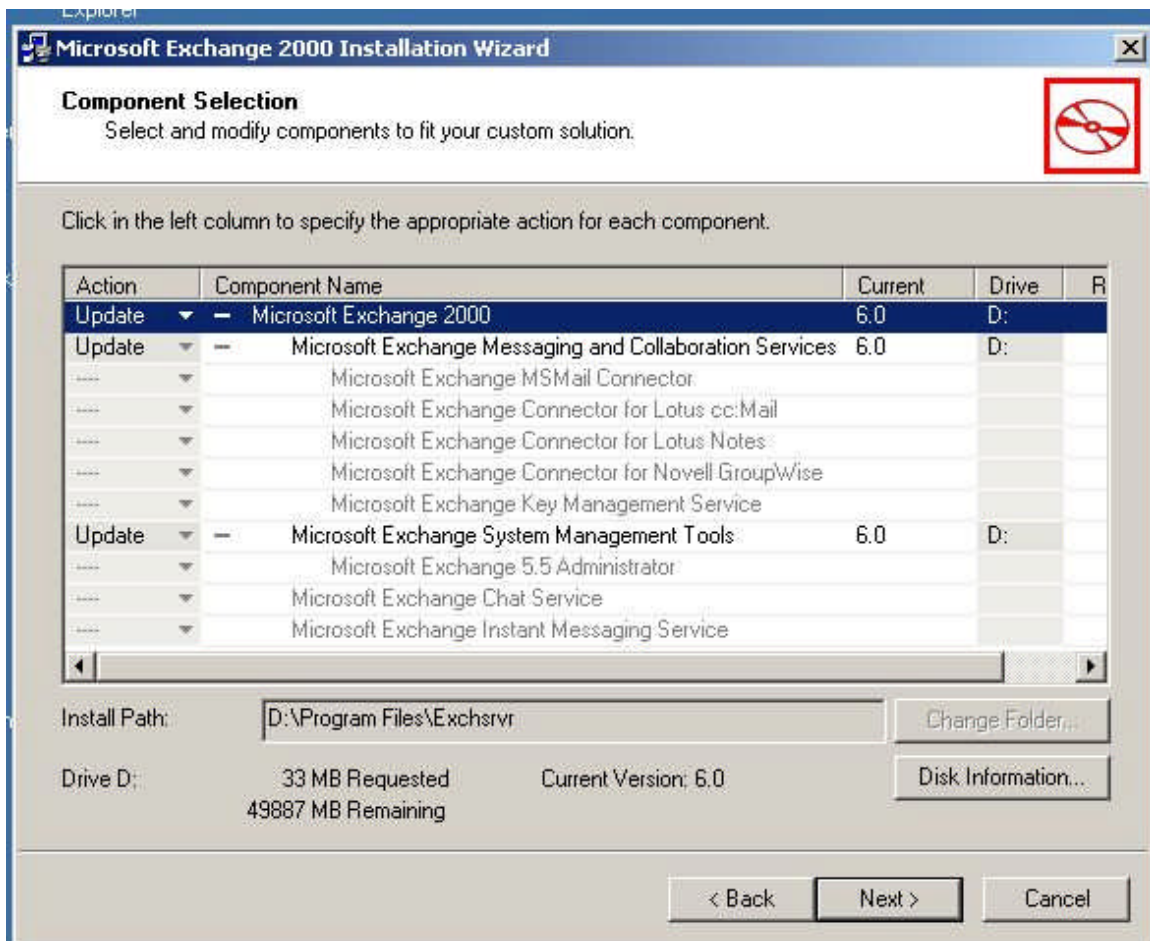
is allowing the NTP traffic. You can then restart the time service with the net start w32time command. More information about this subject and locating a time server that would be appropriate for your specific situation can be found at <http://www.ntp.org/>⁵. It is considered proper protocol to contact the administrator of a public time server via email before syncing with them.

The next step is to apply the Small Business Server service pack 1 or 1a. The main difference between 1 and 1a is that 1 includes Windows 2000 service pack 3 and 1a includes Windows 2000 service pack 4. The service pack includes a set of 3 CD's.



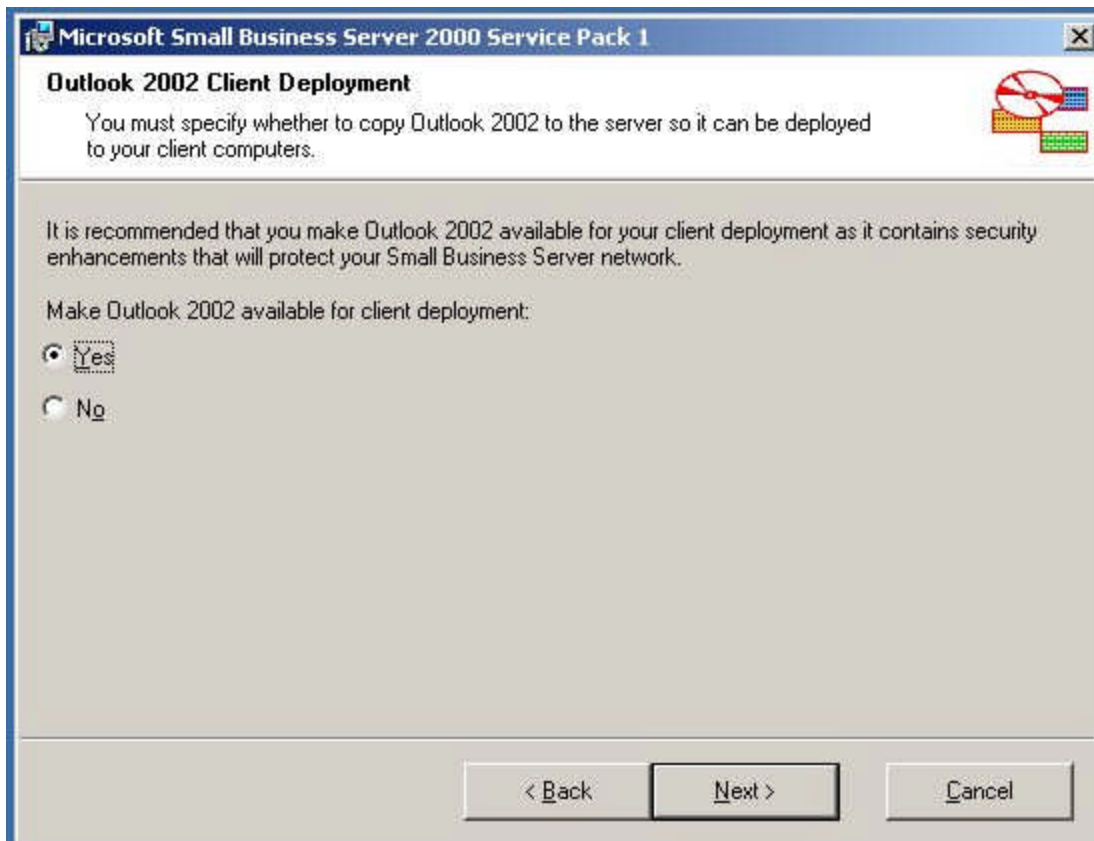
Here is the Welcome screen for the service pack. Click 'Next' to continue.

The process will first apply Windows 2000 service pack 4 and requires a restart.



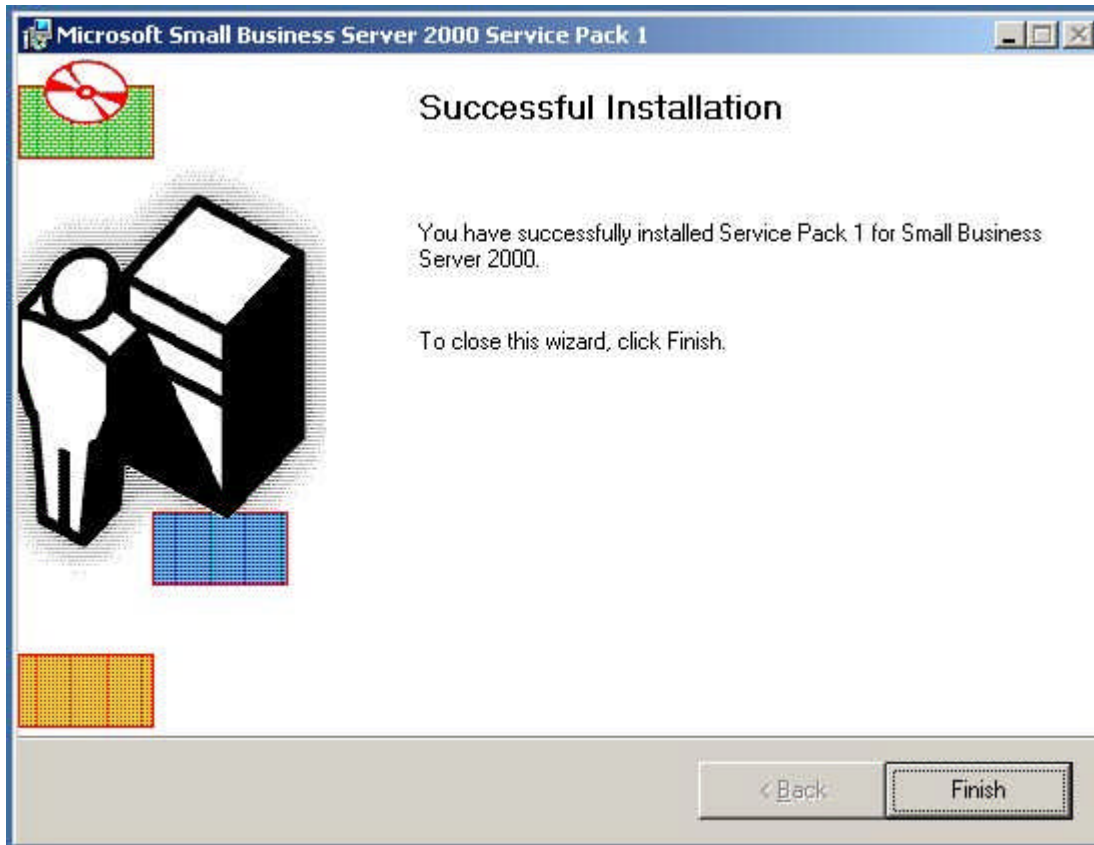
Then the process will apply service pack 3 for Exchange 2000.

© SANS Institute 2004



Once Exchange has been updated and the PC had been restarted you are prompted to update Outlook 2000 to 2002. Click 'Next' to continue.

© SANS Institute 2004

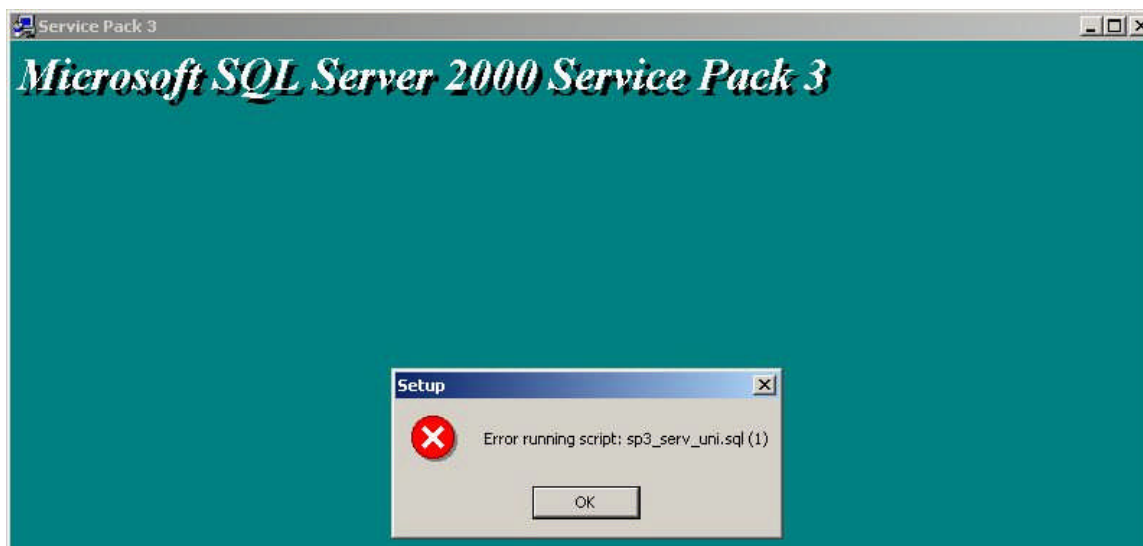


Once Outlook has been updated the update process completes successfully with the screen as shown above.

Interestingly there are also service packs for SQL 2000, service pack 3 and ISA Server service pack 1 but they are not included in the update process. To apply those updates the CD entitled 'Additional Service Packs' is placed in the drive and you can navigate to their perspective folders and double click to apply.

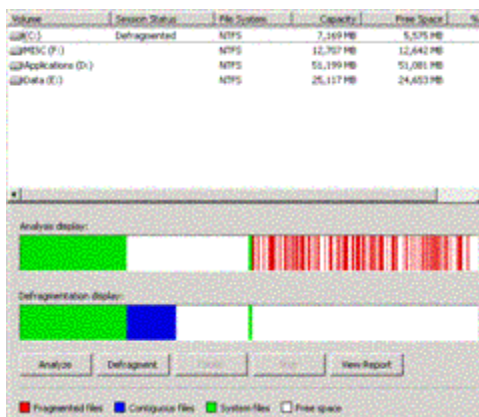
I did experience one error during the SQL update as shown below.

© SANS Institute 2004



I did find this error mentioned in the included Readme file and the solution of a reboot of the PC and then another start of the update. Following that recommendation it did complete successfully on the second go around. ISA updated with no issues to service pack 1.

The next step was to do a little house keeping on the PC. Most people don't realize the condition of the partition just after a fresh install but here is a snapshot of the Windows partition at this point in setup process.



Pretty dramatic before and after don't you think?

To complete this phase of the install I then did a backup of the Systemstate and then a backup of the complete OS partition. This will provide a snapshot in case I encounter a problem later and can return to this point of the install.

To summarize where we are at this point of the process we have a Small Business Server running Windows 2000 at service pack level 4, Exchange Server 2000 running at service

pack level 3, SQL Server 2000 running at service pack level 3 and Internet and Security Acceleration Server running at service pack level 1.

Before I proceed further I went ahead and updated Internet Explorer to 6.0 SP1.

The next step is to apply any updates to the Windows 2000 OS that have come out since Service Pack 4 and any updates for the other components as well. Microsoft provides different options that allow you to go through this process. The update web site is probably the easiest providing you can get to it from a protected network. If that is not possible then you can use their Security website to query what updates are available. I use the [Microsoft TechNet: Home](#) and then click the Security bulletin search link. This link will take you to the web page that looks like the screen shot below.

From here you can select the product and current state as I did; Windows 2000 Service Pack 4. Click the Go button and you will get a list back of the available updates.

Bulletins 1 - 11 of total 11 Bulletins found				Page	1 of 1
▲ Date	Bulletin Description	Affected Software Service Packs	Max Bulletin Severity		
Nov 11, 2003	<u>Buffer Overrun in the Workstation Service Could Allow Code Execution (828749): MS03-049</u> Affected Software: Windows 2000 Server	Windows 2000 Service Pack 2, Windows 2000 Service Pack 3, Windows 2000 Service Pack 4	Critical		
Oct 15, 2003	<u>Buffer Overrun in the ListBox and in the ComboBox Control Could Allow Code Execution (824141): MS03-045</u> Affected Software: Windows 2000 Server	Windows 2000 Service Pack 3, Windows 2000 Service Pack 4	Important		
Oct 15, 2003	<u>Buffer Overrun in Windows Help and Support Center Could Lead to System Compromise (825119): MS03-044</u> Affected Software: Windows 2000 Server	Windows 2000 Service Pack 3, Windows 2000 Service Pack 4	Critical		
Oct 15, 2003	<u>Buffer Overrun in Messenger Service Could Allow Code Execution (828035): MS03-043</u> Affected Software: Windows 2000 Server	Windows 2000 Service Pack 3, Windows 2000 Service Pack 4	Critical		
Oct 15, 2003	<u>Buffer Overflow in Windows Troubleshooter ActiveX Control Could Allow Code Execution (826232): MS03-042</u> Affected Software: Windows 2000 Server	Windows 2000 Service Pack 3, Windows 2000 Service Pack 4	Critical		
Oct 15, 2003	<u>Vulnerability in Authenticode Verification Could Allow Remote Code Execution (823182): MS03-041</u> Affected Software: Windows 2000 Server	Windows 2000 Service Pack 3, Windows 2000 Service Pack 4	Critical		
Sep 10, 2003	<u>Buffer Overrun in RPCSS Service Could Allow Code Execution (824146): MS03-039</u> Affected Software: Windows 2000 Server	Windows 2000 Service Pack 2, Windows 2000 Service Pack 3, Windows 2000 Service Pack 4	Critical		

As you can see above there were several bulletins listed for the OS. I also searched on Exchange and got one, ISA which resulted in 6 and SQL 2000 which resulted in two. Once the updates are downloaded you can use the qchain.exe utility to install most of these only having to do one reboot. Qchain⁷ and information on using it can be found at <http://www.microsoft.com/downloads/details.aspx?FamilyID=a85c9cfa-e84c-4723-9c28-f66859060f5d&displaylang=en>.

Here is the list of updates that are needed to be applied:

-Windows 2000 Server-

[KB837001 - MS04-014](#)

[KB828741 - MS04-012](#)

[KB835732 - MS04-011](#)

[KB832359 - MS04-008](#)

[KB828028 - MS04-007](#)

[KB830352 - MS03-006](#)

[KB828749 - MS03-049](#)

[KB824141 - MS03-045](#)

[KB825119 - MS03-044](#)

[KB828035 - MS03-043](#)

[KB826232 - MS03-042](#)

[KB823182 - MS03-041](#)

[KB824146 - MS03-039](#)

[KB824105 - MS03-034](#)

[KB823559 - MS03-023](#)

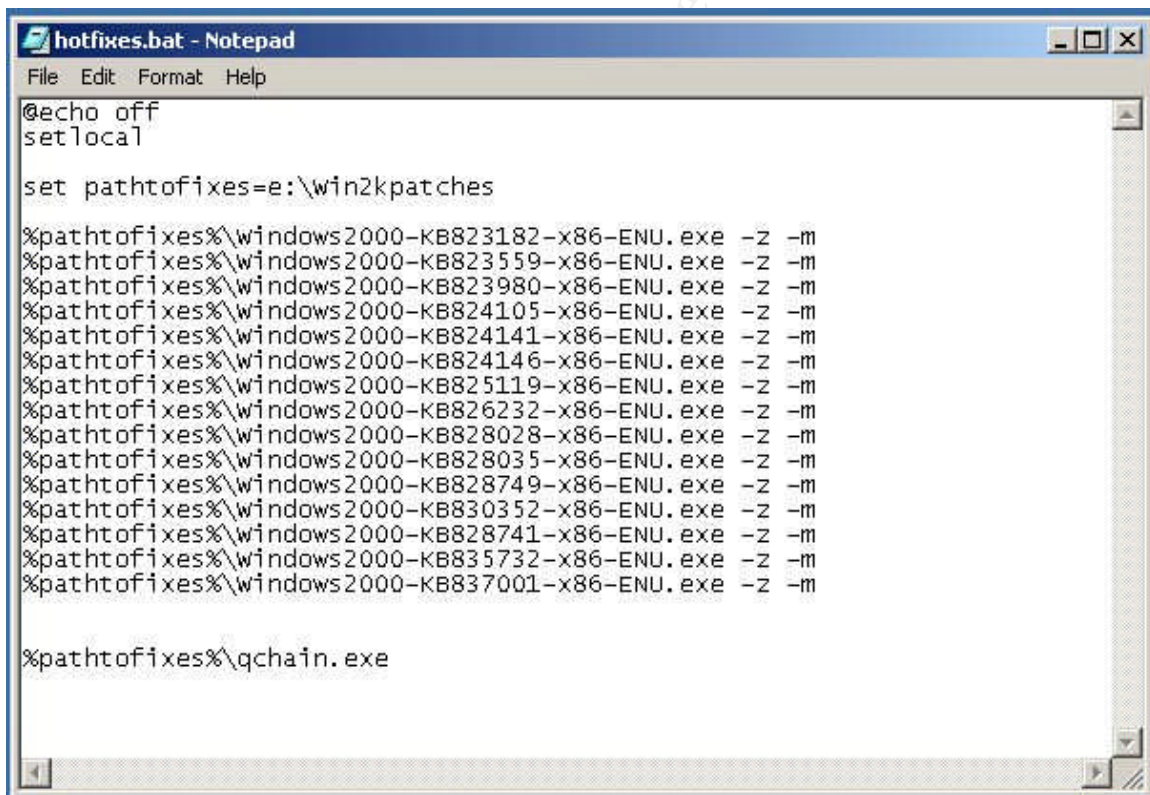
[KB822343 - MS03-022](#)

-Exchange 2000-
[829436 - MS03-046](#)

-ISA Server-
[KB816458 - MS04-001](#)
[KB816456 - MS03-028](#)
[331066 - MS03-012](#)
[331065 - MS03-009](#)
[328130 - MS02-044](#)
[Q323889 - MS02-027](#)

-SQL Server 2000-
[832483 - MS04-003](#)
[815495 - MS03-031](#)

I created a batch for called hotfixes.bat which is shown below.



```
hotfixes.bat - Notepad
File Edit Format Help
@echo off
setlocal

set pathtofixes=e:\win2kpatches

%pathtofixes%\windows2000-KB823182-x86-ENU.exe -z -m
%pathtofixes%\windows2000-KB823559-x86-ENU.exe -z -m
%pathtofixes%\windows2000-KB823980-x86-ENU.exe -z -m
%pathtofixes%\windows2000-KB824105-x86-ENU.exe -z -m
%pathtofixes%\windows2000-KB824141-x86-ENU.exe -z -m
%pathtofixes%\windows2000-KB824146-x86-ENU.exe -z -m
%pathtofixes%\windows2000-KB825119-x86-ENU.exe -z -m
%pathtofixes%\windows2000-KB826232-x86-ENU.exe -z -m
%pathtofixes%\windows2000-KB828028-x86-ENU.exe -z -m
%pathtofixes%\windows2000-KB828035-x86-ENU.exe -z -m
%pathtofixes%\windows2000-KB828749-x86-ENU.exe -z -m
%pathtofixes%\windows2000-KB830352-x86-ENU.exe -z -m
%pathtofixes%\windows2000-KB828741-x86-ENU.exe -z -m
%pathtofixes%\windows2000-KB835732-x86-ENU.exe -z -m
%pathtofixes%\windows2000-KB837001-x86-ENU.exe -z -m

%pathtofixes%\qchain.exe
```

In the batch file I listed all the patches that could be applied in this manner. The syntax being:

pathtofixes\patch_name -z -m.

The `-m` switch tells the update utility to use the unattended setup mode and the `-z` switch is to keep the update utility from restarting the system. This utility can only be used on updates that were created after December of 2002.

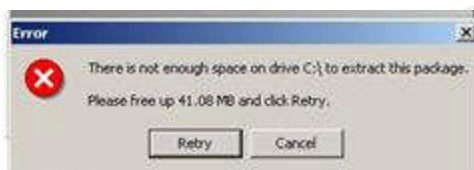
Here is a list of all the switches:

Switch Description

/f Forces other programs to close at shutdown.
/n Does not back up files for removing hotfixes.
/z Does not restart the computer after the installation is completed.
/q Uses quiet mode; no user interaction is required.
/m Uses unattended Setup mode (Windows 2000).
/u Uses unattended Setup mode (Windows XP).
/l Lists installed hotfixes.

Once this was completed a reboot was needed to allow the OS to update.

Then ISA was updated, Exchange and Finally SQL Server 2000. I did encounter an interesting symptom when attempting to update SQL with the KB815495 fix. When attempting to run it from a partition other than the 'C' it produced an error shown in the screen shot below.



The error basically states that there is not enough room on drive C:\ to extract the package and states that more space needs to be provided. There was actually plenty of space on the C partition. I resolved this problem by moving the update to the 'C' partition and running it from there.

Once the Server was rebooted I used the Microsoft HFNETCHK tool to verify where the system was as far as updates. This tool is no longer available as a stand alone product but has been incorporated into the Microsoft Baseline Security Analysis Tool ([MBSA v1.2](#))⁸. Details about the tool can be found [here](#)⁹. MBSA is a very robust tool and analyzes many aspects of the PC beyond just the service pack and Hotfix levels. We will use this tool later in the process to finish up the hardening process on the SBS server. We are currently interested in specifically evaluating the service pack and hot fix level. To use the hfnetchk tool included in the MBSA tool it can be accessed from a cmd window by typing `mbsacli.exe /hf`. To display the syntax of the hfnetchk tool add a `/?` to the end of the exe as shown below.

C:\Networking\HFCHKR>hfnetchk /?
Microsoft Network Security Hotfix Checker, 3.32
Copyright (C) Shavlik Technologies, 2001-2002
Developed for Microsoft by Shavlik Technologies, LLC
info@shavlik.com (www.shavlik.com)

hfnetchk.exe [-h hostname] [-i ipaddress] [-d domainname] [-n] [-b]
[-r range] [-history level] [-t threads] [-o output]
[-x datasource] [-z] [-v] [-s suppression] [-nosum]
[-u username] [-p password] [-f outfile] [-about]
[-fh Hostfile] [-fip ipfile]

Description:

The HFNETCHK tool assesses a machine or group of machines for security hotfixes that have either been installed and/or need to be installed. For more information on this tool, please refer to Microsoft Knowledge Base Article Q303215.

Parameter List:

-about About hfnetchk.

-h hostname Specifies the NetBIOS machine name to scan.
 Default is the localhost.

-fh hostfile Specifies the name of a file containing
 NetBIOS machine names to scan. One name per
 line, 256 max per file.

-i ipaddress Specifies the IP address of a machine to scan.

-fip ipfile Specifies the name of a file containing
 addresses to scan. One IP address per
 line, 256 max per file.

-r range Specifies the IP address range to be scanned,
 starting with ipaddress1 and ending with
 ipaddress2 inclusive. <ipaddress1-ipaddress2>

-d domain_name Specifies the domain_name to scan. All
 machines in the domain will be scanned.

-n network All systems on the local network will be
 scanned. (i.e., all hosts in Network
 Neighborhood)

- history level Displays hotfixes that are:
(1) explicitly installed
(2) explicitly not installed
(3) explicitly installed and not installed
This switch is not necessary for normal operation. Do not use this switch unless you've read -history usage in Q303215.
- t threads Number of threads used for executing scan.
Possible values are from 1 to 128. Default is 64
- o output Specifies the desired output format.
(tab) outputs in tab delimited format.
(wrap) outputs in a word wrapped format.
Default is wrap.
- x datasource Specifies the xml datasource containing the hotfix information. Location may be an xml filename, compressed xml cab file, or URL.
Default is mssecure.cab from the Microsoft website.
- s suppress Suppresses NOTE and WARNING messages
1 = Suppress NOTE messages only
2 = Suppress both NOTE and WARNING messages
Default is to show all messages
- z reg checks Do not perform registry checks.
- nosum checksum Do not evaluate file checksum.
The checksum test calculates the checksum of files. This can use up large amounts of bandwidth. Using this option will speed up a scan and use less bandwidth. File version checks will be still done.
- b baseline Display the status of hotfixes required to meet minimum baseline security standards.
- v verbose Displays the details for Patch NOT Found, WARNING and NOTE messages. Enabled by default in tab mode.
- f outfile Specifies name of the file to save the results.
Default is to display to screen.

- u username Specifies optional user name for login to remote computer.
- p password Specifies password to be used with user name.
- ? help Displays this menu.

Examples:

```
HFNETCHK.exe
HFNETCHK.exe -v -z -b
HFNETCHK.exe -h hostname
HFNETCHK.exe -h hostname -f out.txt
HFNETCHK.exe -d domainname -u domainname\username -p password
HFNETCHK.exe -d domainname -u username -p password
HFNETCHK.exe -h h1,h2,h3
HFNETCHK.exe -i 192.168.1.1 -s 2 -t 10 -v
HFNETCHK.exe -i 192.168.1.1,192.168.1.8 -h hostname -x mssecure.xml
HFNETCHK.exe -d domain_name -s 1 -o tab -x c:\temp\mssecure.xml
HFNETCHK.exe -r 192.168.1.1-192.168.1.254 -history 1 -t 20
HFNETCHK.exe -x http://www.xyz.abc/mssecure.xml
HFNETCHK.exe -x "c:\Space In Path\mssecure.xml"
HFNETCHK.exe -fh d:\MyHostFile.txt
HFNETCHK.exe -fip d:\MyIPFile.txt
HFNETCHK.exe -about
```

Here is a screen shot of the tool running on the SBS server at this point of the process the syntax that was used was `hfnetchk -v` which runs the tool with verbose output giving specifics about any Patch Not Found, Warning or Note messages. If the system did not have Internet access the `mssecure.xml` file could be placed on the system locally and then you would include the `-x /pathto/mssecure.xml` option to the command.

© SANS Institute 2004, Author retains full rights.


```
C:\WINNOT\system32\cmd.exe
Scanning SBSSERVER01
.....
Done scanning SBSSERVER01
-----
SBSSERVER01 <10.1.250.1>
-----

* WINDOWS 2000 SERVER SP4

Patch NOT Found MS04-011      835732
File C:\WINNOT\system32\kernel32.dll has an invalid checksum and
its file version is equal to or less than what is expected.

* INTERNET INFORMATION SERVICES 5.0

Information
All necessary hotfixes have been applied.

* INTERNET EXPLORER 6 SP1

Information
All necessary hotfixes have been applied.

* SQL SERVER 2000 SP3

Note      MS03-031      815495
Please refer to Q306460 for a detailed explanation.
```

The HFNETCHK.EXE tools output displays a couple of Note messages which state to refer to [Q306460](#). This type of message can be displayed when MBSA or HFNETCHK cannot determine the status of the software update. It does this by checking information in registry keys, file versions and file checksums. When this information is not available this can result in a 'Note' or 'Warning' message. This can happen when there may be more than one appropriate update to the fix, for example two versions of a dll that resolves the same issue therefore a 'Note' message is generated since the XML file does not compare all available variations. The follow up on the 'Note' listed in this output would be to refer back to the security bulletin about this update and find the file version listing and compare against the files on the local system.

During some investigation of this issue I came across documentation that stated that the stand alone hfnetchk.exe tool was soon to be deprecated and would no longer work properly with the down loaded XML file.

To address the issue the Microsoft Baseline Security Analyzer was installed (which will be discussed later) and the command line tool mbsaccli.exe with the /hf -v switches was used to scan the system producing the output below.

* SMALL BUSINESS SERVER 2000 SP4

Note MS03-030 819696
Please refer to 306460 for a detailed explanation.

* INTERNET INFORMATION SERVICES 5.0 SP4
Information

There are no security updates available for this product.

* INTERNET EXPLORER 6 SP1
Information

All necessary hotfixes have been applied.

* WINDOWS MEDIA PLAYER 6.4 FOR WINDOWS 2000 SP4
Information

There are no security updates available for this product.

* EXCHANGE 2000 SP3
Information

All necessary hotfixes have been applied.

* MDAC 2.7 SP1
Information

All necessary hotfixes have been applied.

* MICROSOFT VIRTUAL MACHINE (VM) GOLD

Patch NOT Found MS03-011 816093
File version is less than expected.
[C:\WINNOT\system32\msjava.dll, 5.0.3310.0 < 5.0.3810.0]

* MSXML 2.6 GOLD
Warning

The latest service pack for this product is not installed.
Currently Gold is installed. The latest service pack is SP3.

Patch NOT Found MS02-008 318202
File version is less than expected.
[C:\WINNOT\system32\msxml2.dll, 8.0.6518.2 < 8.2.8307.0]

* MSXML 3.0 SP3
Information

There are no security updates available for this product.

Warning

The latest service pack for this product is not installed.
Currently SP3 is installed. The latest service pack is SP4.

* SQL SERVER 2000 SP3
Information

All necessary hotfixes have been applied.

As you can see from the output above this tool can produce a lot of output and exposes many more issues than the HFNETCHK.EXE tool. Based on the results above the appropriate updates were applied and the mbsaccli.exe tool was rerun after another reboot of the system.

* SMALL BUSINESS SERVER 2000 SP4

Note MS03-030 819696
Please refer to 306460 for a detailed explanation.

* INTERNET INFORMATION SERVICES 5.0 SP4

Information
There are no security updates available for this product.

* INTERNET EXPLORER 6 SP1

Information
All necessary hotfixes have been applied.

* WINDOWS MEDIA PLAYER 6.4 FOR WINDOWS 2000 SP4

Information
There are no security updates available for this product.

* EXCHANGE 2000 SP3

Information
All necessary hotfixes have been applied.

* MDAC 2.7 SP1

Information
All necessary hotfixes have been applied.

* MICROSOFT VIRTUAL MACHINE (VM) GOLD

Information
All necessary hotfixes have been applied.

* MSXML 2.6 SP3

Information
There are no security updates available for this product.

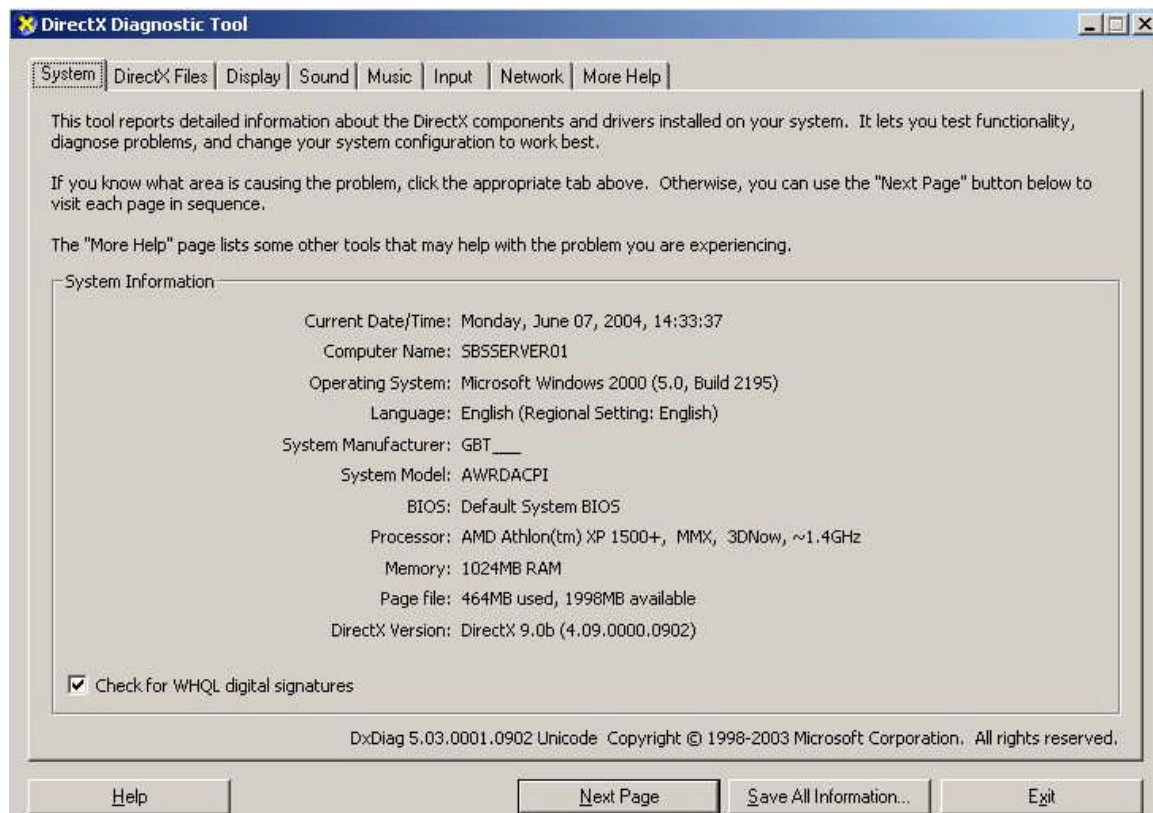
* MSXML 3.0 SP4

Information
There are no security updates available for this product.

* SQL SERVER 2000 SP3

Information
All necessary hotfixes have been applied.

The output above now shows that all the updates have been applied just leaving the one Note message. In reviewing the security article [KB819696](#) it deals with an unchecked buffer in DirectX which was installed when the ATI video drivers were installed. You can check for the specific version on the PC by running the dxdiag.exe tool which produces a tabbed screen like the screen shot below.



Based on the articles recommendation I was running version 8.0 and could install the patch for 8.0 but Microsoft recommends installing version 9.0b which is what I did. Once that has been completed the Note message was still appearing and so to verify the update had been applied properly I checked the file version against the security article as shown below.

DirectX 9.0b and DirectX 9.0a patch (32-Bit) for Windows 2000:

Date	Time	Version	Size	File name
30-May-2003	09:00	6.5.1.902	1,136,640	Quartz.dll (end user)
30-May-2003	09:00	6.5.1.902	1,962,496	Quartz.dll (redist)

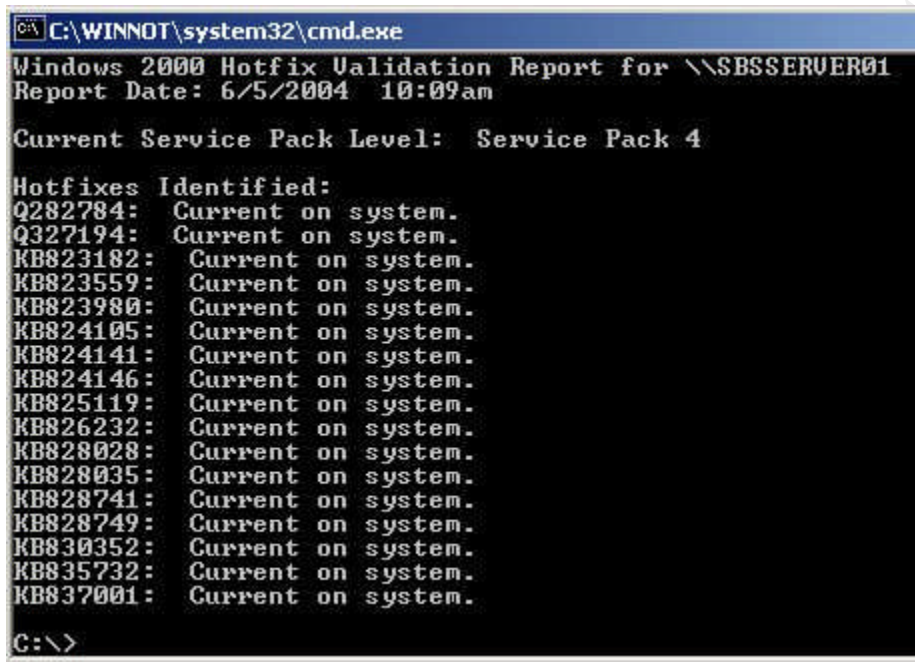
The screenshot shows the DirectX Diagnostic Tool window with the 'DirectX Files' tab selected. It displays a list of files with the following columns: Name, Version, Attributes, Language, Date, and Size.

Name	Version	Attributes	Language	Date	Size
quartz.dll	6.05.0001.0902	Final Retail	English	5/30/2003 09:00:02	1136640
strmdll.dll	4.01.0000.3928	Final Retail	English	6/19/2003 12:05:04	246544
iac25_32.ax	2.00.0005.0053	Final Retail	English	7/26/2000 07:00:00	199680
ir41_32.ax	4.51.0016.0003	Final Retail	English	7/26/2000 07:00:00	848384

I have overlaid the dxdiag.exe tool screen on the top of the security article that lists the file version for Quartz.dll and verified that the file version did in fact match. To suppress the note message(s) in the future you can add the -s1 switch (EX:mbsacli.exe /hf -v -s1).

Another tool that can be used in validating the software updates is the Microsoft [QFE](#) check tool that verifies the installation of Windows 2000 and Windows XP Hotfixes.

Once it has been installed it is just a simple matter of running it from the command line.



```
C:\WINNOT\system32\cmd.exe
Windows 2000 Hotfix Validation Report for \\SBSSERVER01
Report Date: 6/5/2004 10:09am

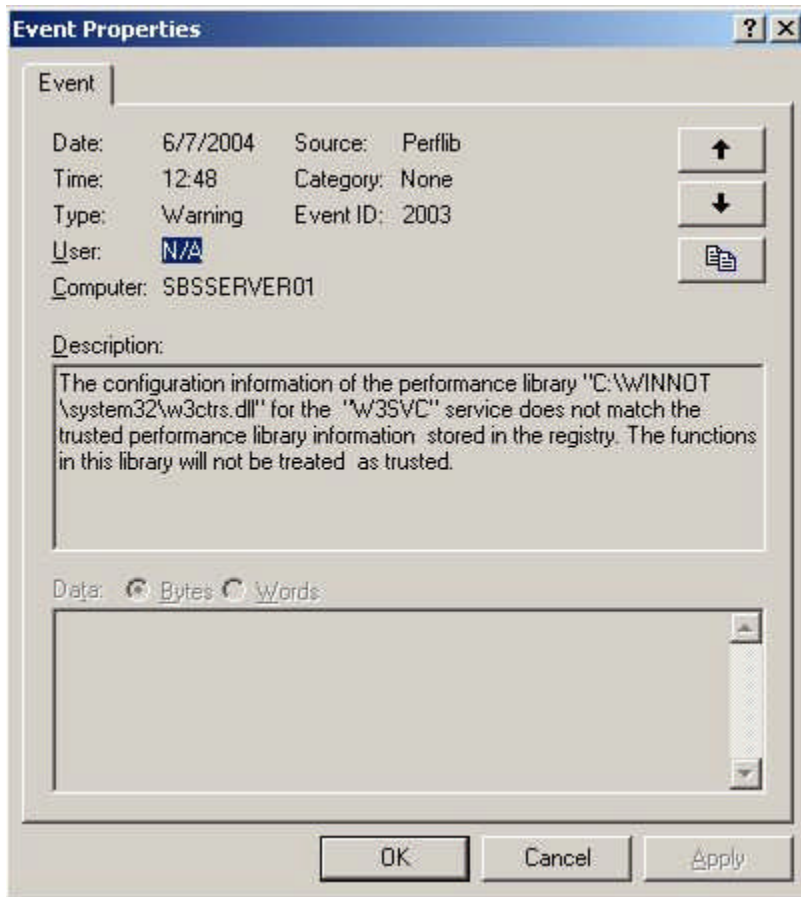
Current Service Pack Level: Service Pack 4

Hotfixes Identified:
Q282784: Current on system.
Q327194: Current on system.
KB823182: Current on system.
KB823559: Current on system.
KB823980: Current on system.
KB824105: Current on system.
KB824141: Current on system.
KB824146: Current on system.
KB825119: Current on system.
KB826232: Current on system.
KB828028: Current on system.
KB828035: Current on system.
KB828741: Current on system.
KB828749: Current on system.
KB830352: Current on system.
KB835732: Current on system.
KB837001: Current on system.

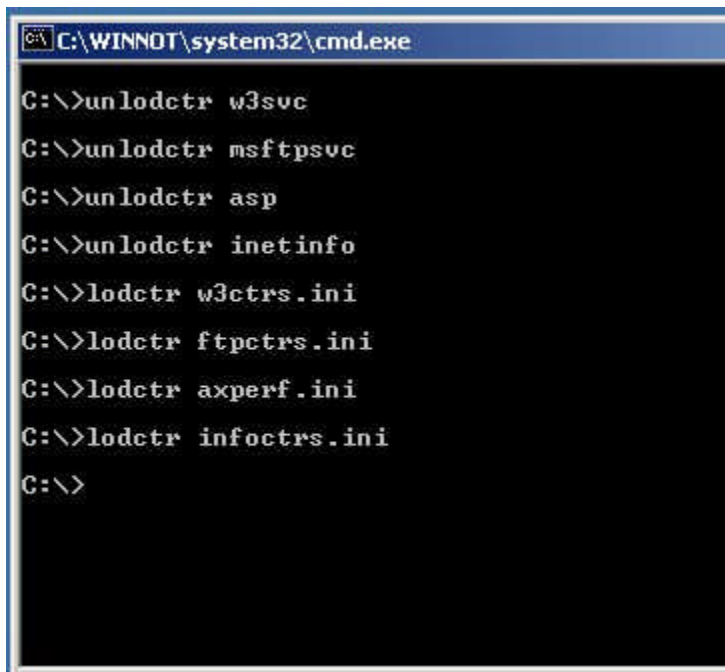
C:\>
```

Above is the output of the tool. We can see that we are at Service Pack Level 4 and it lists the 17 updates that have been installed. Now would be a good time to do a system state backup and a backup of the operating system before proceeding.

In reviewing the event logs at this point I noticed multiple Event ID 2003 entries showing up like the screen shot below.



In researching this issue I found a knowledge base article [KB267831](#) that described the symptom and the resolution. Interestingly the article states that this symptom can be caused by installing Windows 2000 on a drive that uses the FAT or FAT32 file system and then installing IIS in the same setup process which I had not done.



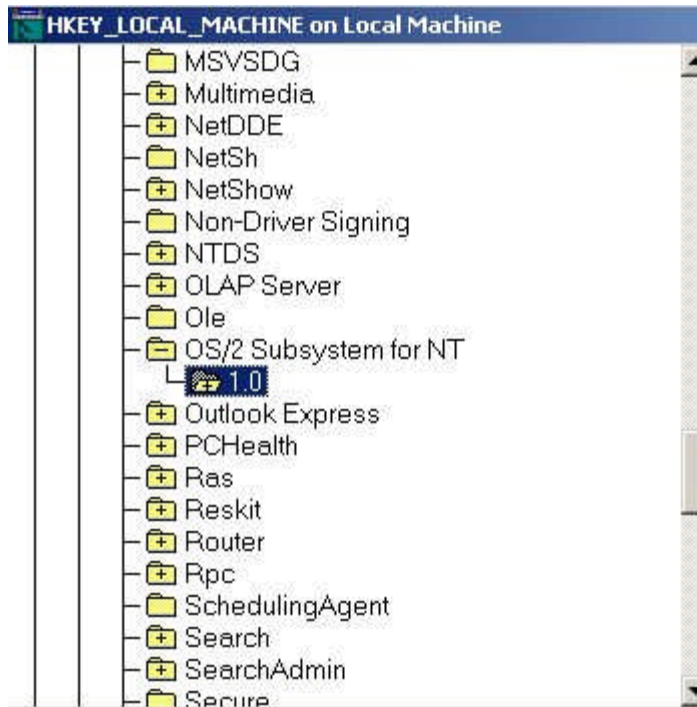
```
C:\WINNOT\system32\cmd.exe

C:\>unlodctr w3svc
C:\>unlodctr msftpsvc
C:\>unlodctr asp
C:\>unlodctr inetinfo
C:\>lodctr w3ctrs.ini
C:\>lodctr ftpctrs.ini
C:\>lodctr axperf.ini
C:\>lodctr infoctrs.ini
C:\>
```

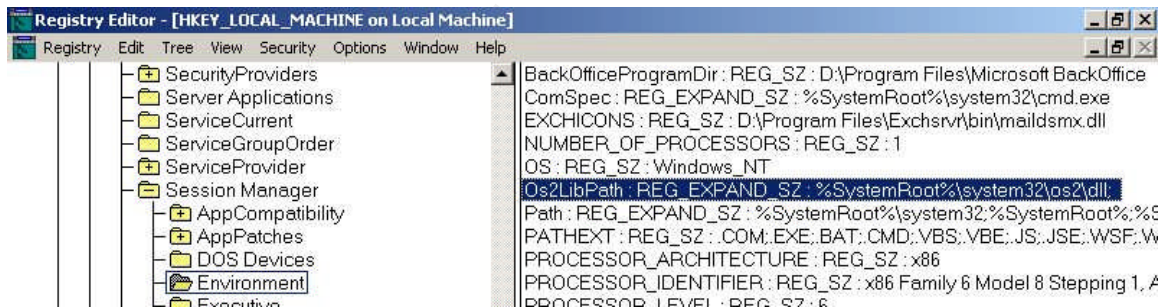
I applied the resolution which was to unload and reload the performance counters and reboot. This did in fact resolve the issue and I was no longer seeing the Event ID 2003 entries.

The next area to focus on is the OS/2 and POSIX subsystems that are included in the OS for legacy compatibility. These can and should be removed since they are not needed in most environments. The procedure requires using a registry editing tool and it is strongly advised in the Microsoft article [Q320869](#) to use regedt32.exe and not regedit.exe since it could potentially corrupt the registry during this process. There are better instructions that can be found in the SANS Securing Windows 2000 professional¹⁰ or in the NSA documentation that can be downloaded with the security templates. As described by the information in the SANS documentation ‘The steps presented here are a slight departure from the Microsoft recommended steps based on some real world experience.’ Which I can also personally affirm experiencing an infamous blue screen of death during a reboot after incorrectly performing this procedure. Here is the excerpt from the SANS publication which will be used to complete this procedure with some screen shots added for clarity.

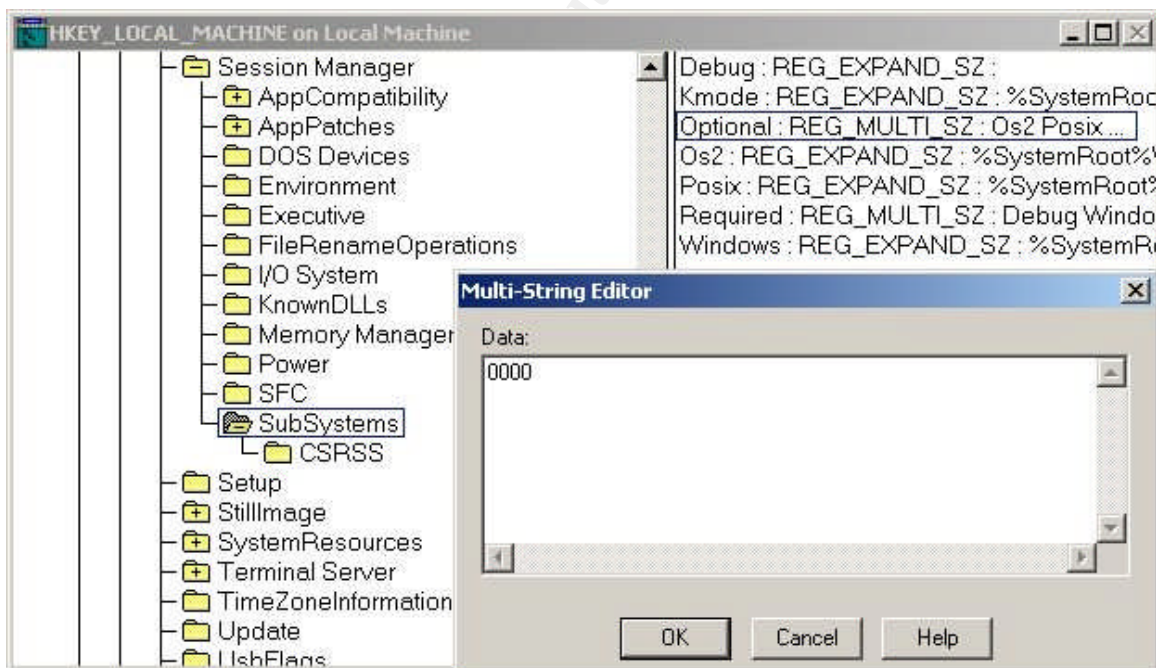
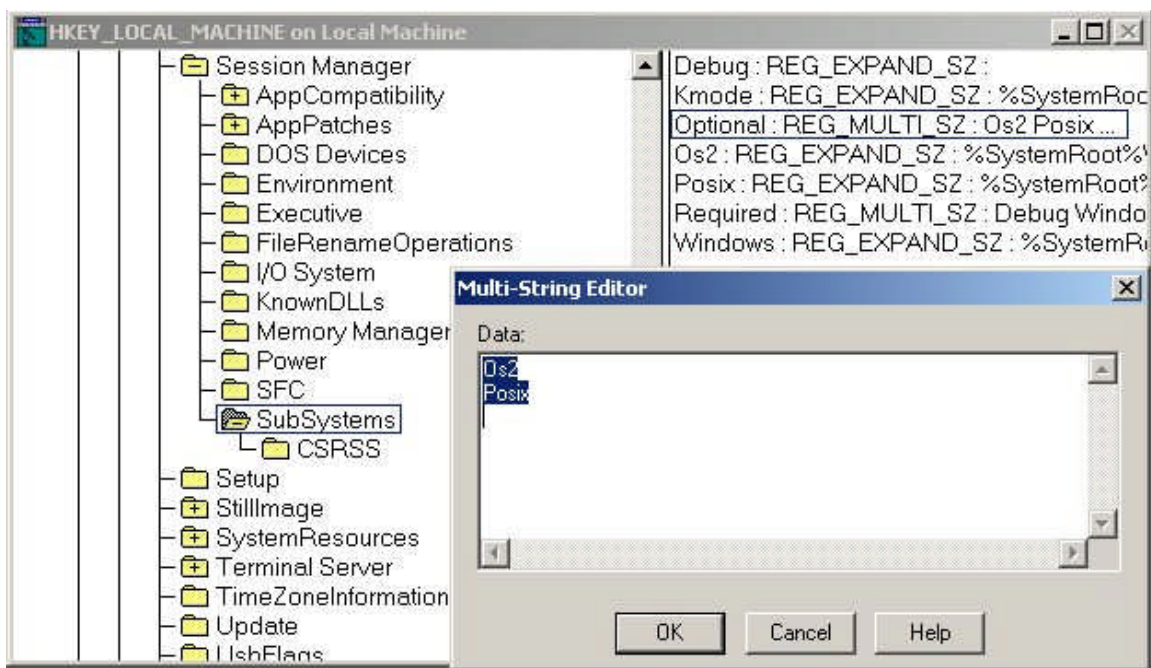
“To remove OS/2 and POSIX completely:
Delete all sub-keys of HKLM\SOFTWARE\Microsoft\OS/2 Subsystem
for NT



Delete the value HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Environment\Os2LibPath



Replace all values of OS/2 and POSIX in
HKLM\CurrentControlSet\Control\Session\Manager\Subsystems\Optional



With a string of 4 zeros (simply emptying the string can lead to a Blue Screen in some cases)

Delete the files DOSCALLS.DLL, NETAPI.OS2, OS2.EXE, OS2SRV.EXE and OS2SS.EXE from the % SystemRoot% \ System32\DllCache folder. This is where backup copies are stored for use

by Windows File Protection.

Reboot THE SYTEM, and delete all files, NOT FOLDERS OR DIRECTORIES, from the %systemroot%\system32\os2 folder and its subfolders.”

If you are prompted by the Windows File Protection to replace missing files just click Cancel. You may also want to review these settings if you ever have a need to reapply a service pack.

The next step in the process is to harden the IP stack of the operation system. This can be done by following the recommendations in the Microsoft article entitled ‘Security Considerations for Network Attacks’¹¹ found at - <http://www.microsoft.com/technet/security/topics/network/secdeny.msp>

Here is an excerpt that provides the guideline that could be followed. (NOTE: as always a cautionary note when modifying the registry bad things can happen. You should always back up before you proceed.)

“Registry Settings for Maximum Protection from Network Attack

The following registry settings will help to increase the resistance of the NT or Windows 2000 network stack to network denial of service attacks.

SynAttackProtect

Key: Tcpip\Parameters

Value Type: REG_DWORD

Valid Range: 0, 1, 2

0 (no synattack protection)

1 (reduced retransmission retries and delayed RCE (route cache entry) creation if the TcpMaxHalfOpen and TcpMaxHalfOpenRetried settings are satisfied.)

2 (in addition to 1 a delayed indication to Winsock is made.)

Note When the system finds itself under attack the following options on any socket can no longer be enabled : Scalable windows (RFC 1323) and per adapter configured TCP parameters (Initial RTT, window size). This is because when protection is functioning the route cache entry is not queried before the SYN-ACK is sent and the Winsock options are not available at this stage of the connection.

Default: 0 (False)

Recommendation: 2

Description: Synattack protection involves reducing the amount of retransmissions for the SYN-ACKS, which will reduce the time for which resources have to remain allocated. The allocation of route cache entry resources is delayed until a connection is made. If synattackprotect = 2, then the connection indication to AFD is delayed until the three-way handshake is completed. Also note that the actions taken by the protection mechanism only occur if TcpMaxHalfOpen and TcpMaxHalfOpenRetried settings are exceeded.

TcpMaxHalfOpen**Key:** Tcpip\Parameters**Value Type:** REG_DWORD—Number**Valid Range:** 100–0xFFFF**Default:** 100 (Professional, Server), 500 (advanced server)**Recommendation:** default

Description: This parameter controls the number of connections in the SYN-RCVD state allowed before SYN-ATTACK protection begins to operate. If SynAttackProtect is set to 1, ensure that this value is lower than the AFD listen backlog on the port you want to protect (see Backlog Parameters for more information). See the SynAttackProtect parameter for more details.

TcpMaxHalfOpenRetried**Key:** Tcpip\Parameters**Value Type:** REG_DWORD—Number**Valid Range:** 80–0xFFFF**Default:** 80 (Professional, Server), 400 (Advanced Server)**Recommendation:** default

Description: This parameter controls the number of connections in the SYN-RCVD state for which there has been at least one retransmission of the SYN sent, before SYN-ATTACK attack protection begins to operate. See the SynAttackProtect parameter for more details.

EnablePMTUDiscovery**Key:** Tcpip\Parameters**Value Type:** REG_DWORD—Boolean**Valid Range:** 0, 1 (False, True)**Default:** 1 (True)**Recommendation:** 0

Description: When this parameter is set to 1 (True) TCP attempts to discover the Maximum Transmission Unit (MTU or largest packet size) over the path to a remote host. By discovering the Path MTU and limiting TCP segments to this size, TCP can eliminate fragmentation at routers along the path that connect networks with different MTUs. Fragmentation adversely affects TCP throughput and network congestion. Setting this parameter to 0 causes an MTU of 576 bytes to be used for all connections that are not to hosts on the local subnet.

NoNameReleaseOnDemand**Key:** Netbt\Parameters**Value Type:** REG_DWORD—Boolean**Valid Range:** 0, 1 (False, True)**Default:** 0 (False)**Recommendation:** 1

Description: This parameter determines whether the computer releases its NetBIOS name when it receives a name-release request from the network. It was added to allow the administrator to protect the machine against malicious name-release attacks.

EnableDeadGWDetect**Key:** Tcpip\Parameters

Value Type: REG_DWORD—Boolean

Valid Range: 0, 1 (False, True)

Default: 1 (True)

Recommendation: 0

Description: When this parameter is 1, TCP is allowed to perform dead-gateway detection. With this feature enabled, TCP may ask IP to change to a backup gateway if a number of connections are experiencing difficulty. Backup gateways may be defined in the Advanced section of the TCP/IP configuration dialog in the Network Control Panel. See the "Dead Gateway Detection" section in this paper for details.

KeepAliveTime

Key: Tcpip\Parameters

Value Type: REG_DWORD—Time in milliseconds

Valid Range: 1–0xFFFFFFFF

Default: 7,200,000 (two hours)

Recommendation: 300,000

Description: The parameter controls how often TCP attempts to verify that an idle connection is still intact by sending a keep-alive packet. If the remote system is still reachable and functioning, it acknowledges the keep-alive transmission. Keep-alive packets are not sent by default. This feature may be enabled on a connection by an application.

PerformRouterDiscovery

Key: Tcpip\Parameters\Interfaces\

Value Type: REG_DWORD

Valid Range: 0,1,2

0 (disabled)

1 (enabled)

2 (enable only if DHCP sends the router discover option)

Default: 2, DHCP-controlled but off by default.

Recommendation: 0

Description: This parameter controls whether Windows 2000 attempts to perform router discovery per RFC 1256 on a per-interface basis. See also SolicitationAddressBcast.

EnableICMPRedirects

Key: Tcpip\Parameters

Value Type: REG_DWORD

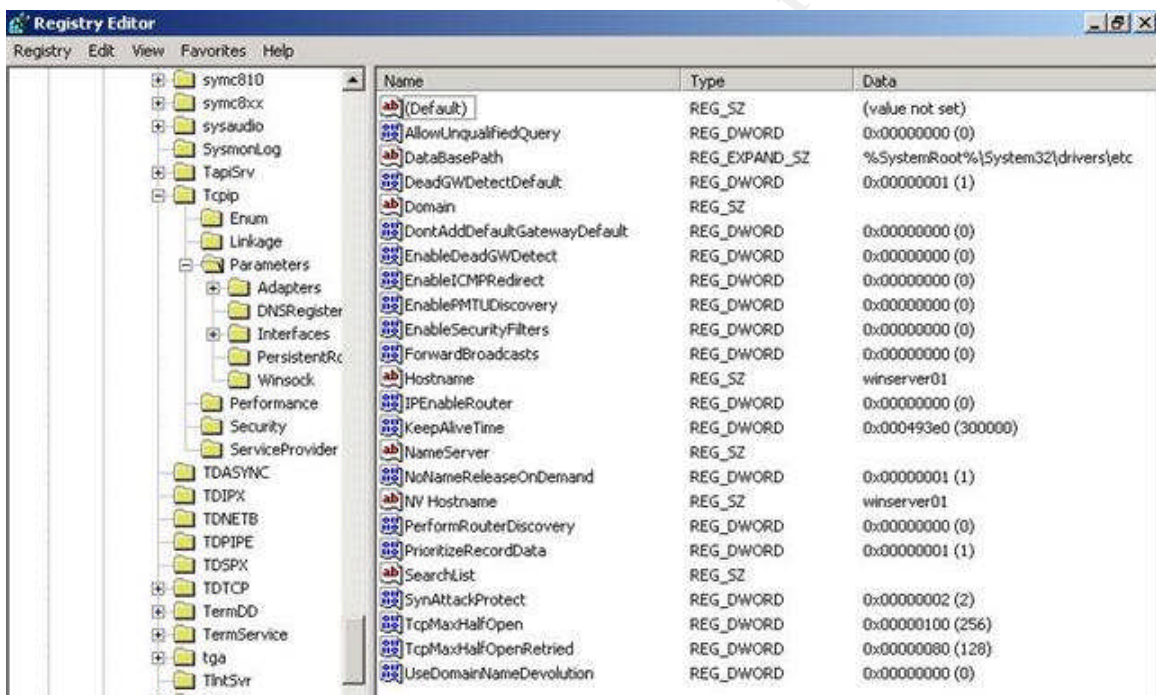
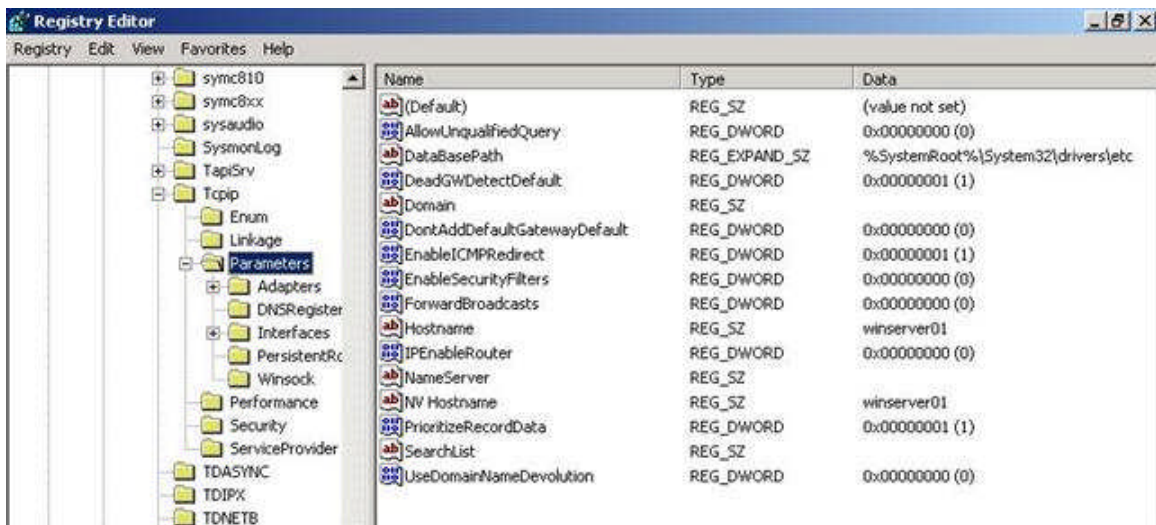
Valid Range: 0, 1 (False, True)

Default: 1 (True)

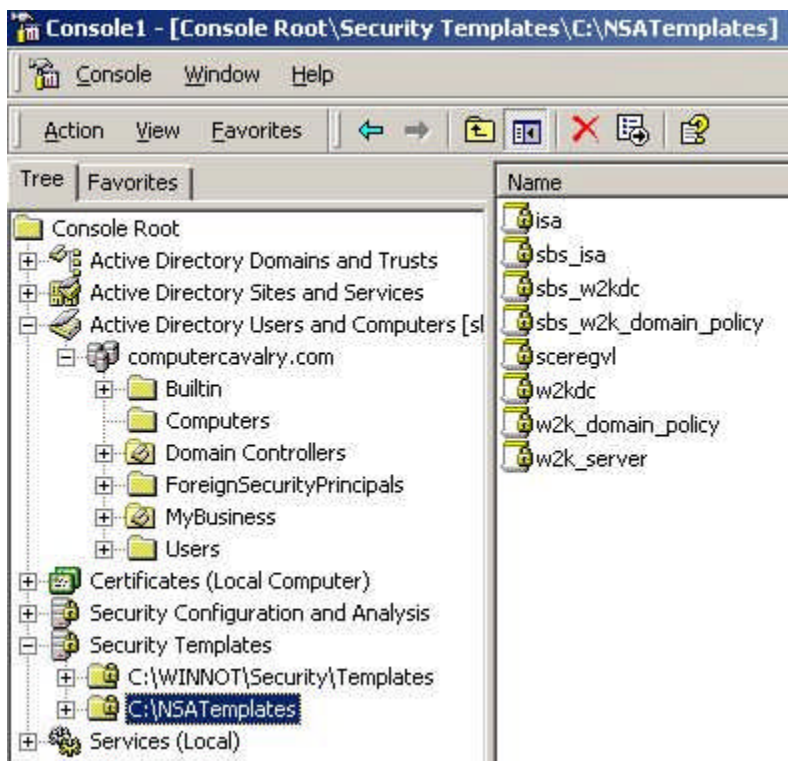
Recommendation: 0 (False)

Description: This parameter controls whether Windows 2000 will alter its route table in response to ICMP redirect messages that are sent to it by network devices such as a routers. “

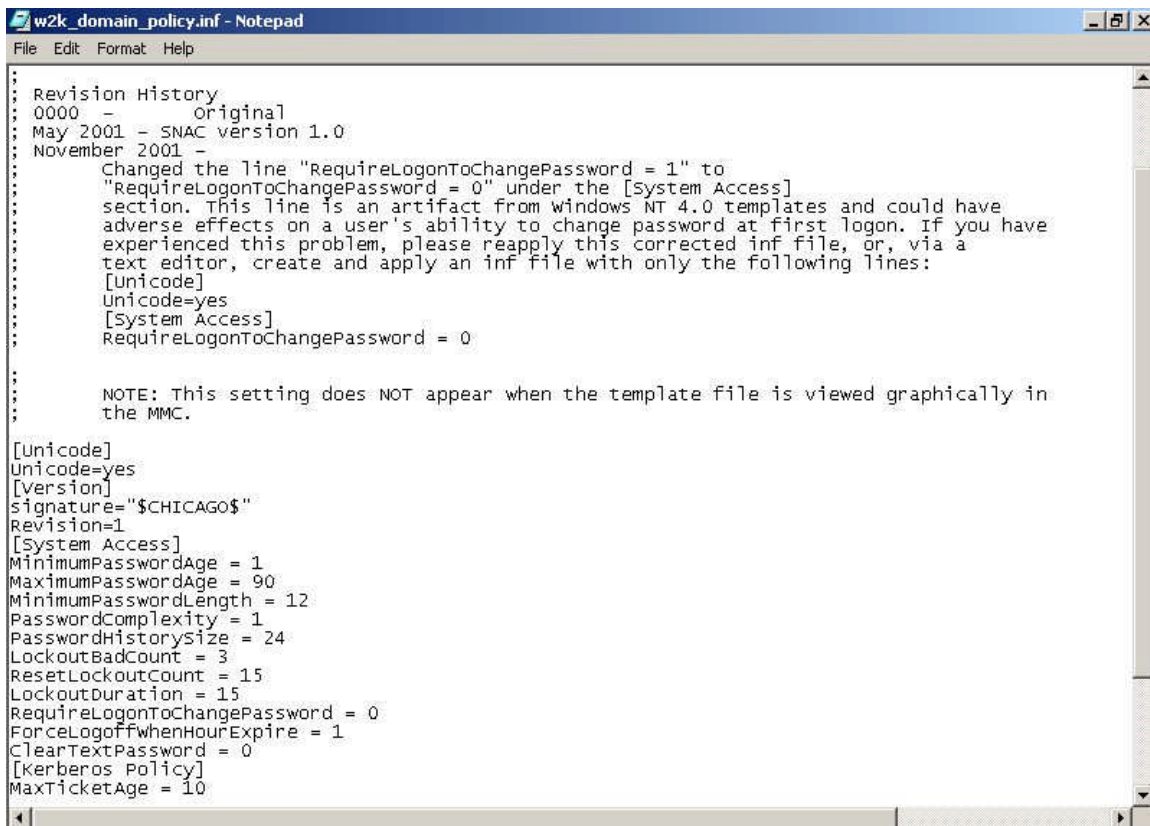
Below are screen shots of the registry before and after the additions were made.



The results above can also be achieved by utilizing the Security Configuration and Analysis snap-in that can be added to a Microsoft Management Console along with the Security Templates snap-in and template files that can be down loaded from the [NSA website](#)¹² or the Center for Internet Security [website](#)¹³. Some of these security templates include the above settings along with many more.



Above is a screen shot of a Microsoft Management Console (MMC) with a few snap-ins added including the Security Configuration and Analysis Editor and the Security Template snap-in. Windows 2000 includes several templates by default. They are located at `%systemroot%\Security\Templates`. The screen shot also shows the template files that were downloaded from the NSA website which were copied adding 'sbs' to the file names as to leave the originals in tact.



```
File Edit Format Help

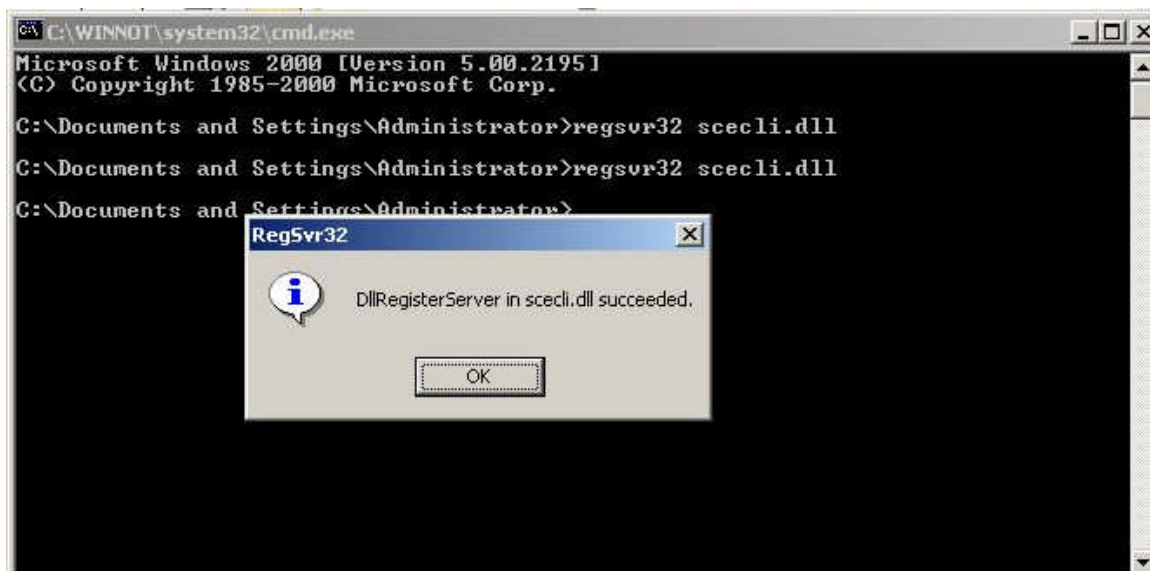
;
; Revision History
; 0000 - Original
; May 2001 - SNAC version 1.0
; November 2001 -
;   Changed the line "RequireLogonToChangePassword = 1" to
;   "RequireLogonToChangePassword = 0" under the [System Access]
;   section. This line is an artifact from windows NT 4.0 templates and could have
;   adverse effects on a user's ability to change password at first logon. If you have
;   experienced this problem, please reapply this corrected inf file, or, via a
;   text editor, create and apply an inf file with only the following lines:
;   [Unicode]
;   Unicode=yes
;   [System Access]
;   RequireLogonToChangePassword = 0
;
; NOTE: This setting does NOT appear when the template file is viewed graphically in
; the MMC.
;
[Unicode]
Unicode=yes
[Version]
Signature="$CHICAGO$"
Revision=1
[System Access]
MinimumPasswordAge = 1
MaximumPasswordAge = 90
MinimumPasswordLength = 12
PasswordComplexity = 1
PasswordHistorySize = 24
LockoutBadCount = 3
ResetLockoutCount = 15
LockoutDuration = 15
RequireLogonToChangePassword = 0
ForceLogoffWhenHourExpire = 1
ClearTextPassword = 0
[Kerberos Policy]
MaxTicketAge = 10
```

The template file or 'inf' file is actually a Unicode text file. The formatting is done in sections. Each section begins with a header that is enclosed in brackets (EX: [System Access]). The files can be opened and edited with notepad or any text editor but it is recommended that modifications are made using the Security Configuration and Analysis GUI. Template files provide a way to modify several areas of the system including account policies, user rights, file and folder permissions, registry permissions, services, etc. Template files are incremental not cumulative and great care must be taken when applying templates to a system because there is no true roll back process. So before applying any type of changes using this process it is imperative to do a system back up that can be used in case things get 'broken'. The NSA download also includes a modified sceregl.inf file that exposes several new options including the ones that harden the TCP/IP stack. The original Windows file is located in the %systemroot%\inf folder. This folder is not visible by default.

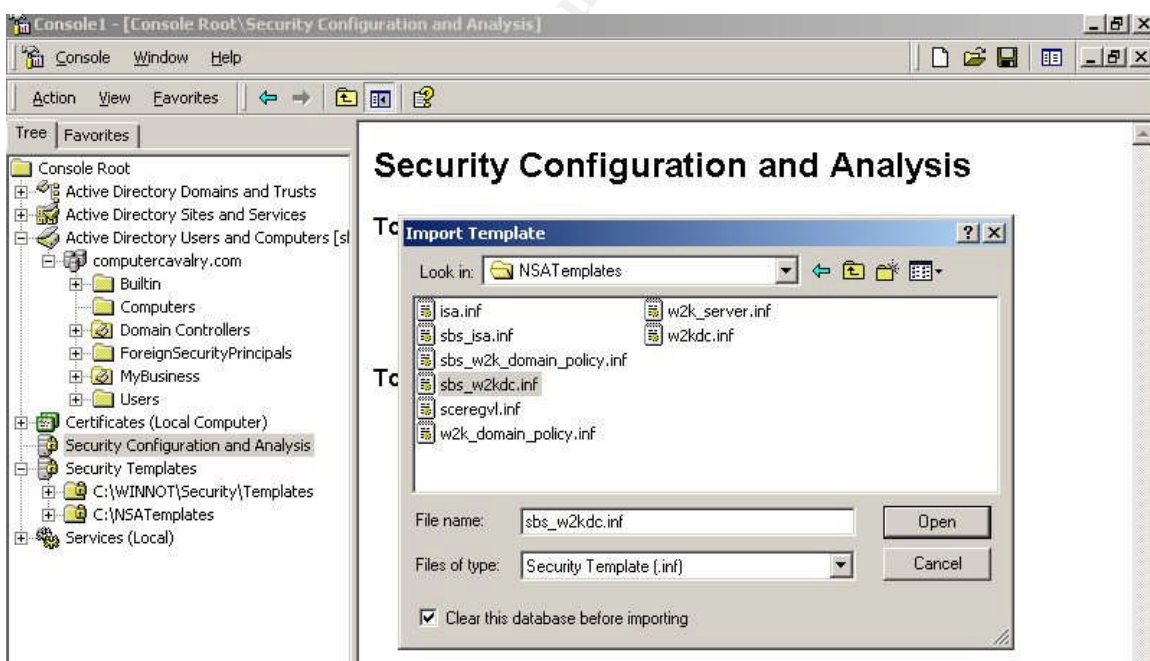




To expose this folder in explorer – select the Tools -> Folder Options -> View and select 'Show Hidden Files and Folders' as shown above. Next it is suggested that you rename the current file to something else and then copy the new sciregvl.inf file to the inf folder. To expose the new options in the Security Configuration and Analyses Editor you must re-register the scecli.dll.

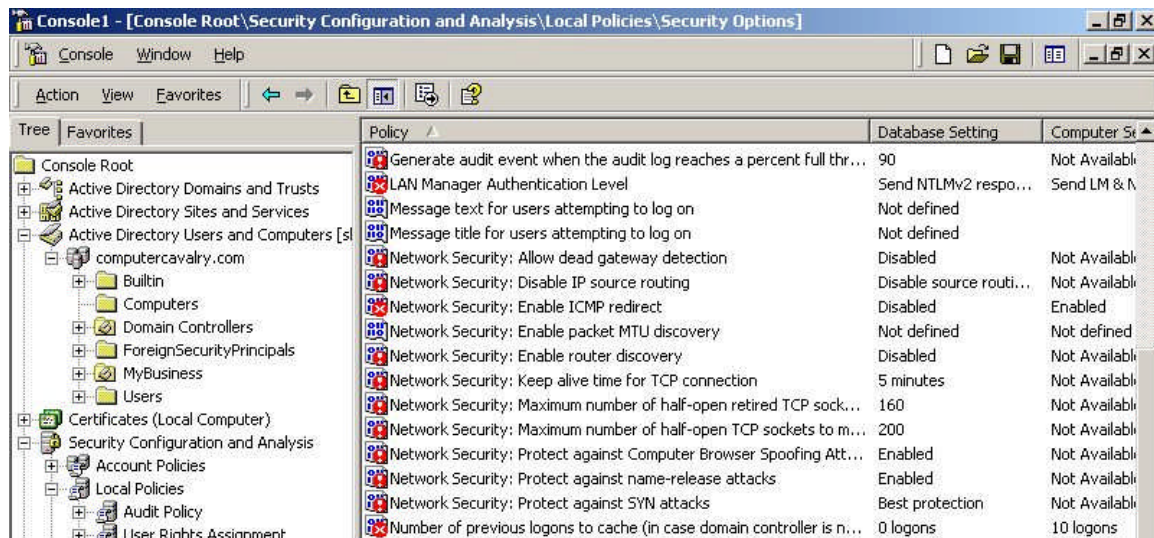


This is done by opening a command window and typing 'regsvr32 scecli.dll' and should result in a succeeded message like the screen shot above. The next step is to import a template into the configuration editor and analyze the system's current settings. This is done by right clicking on the SCA snap-in, selecting open database, providing a database name and selecting a template to import.



Something to pay attention to is the 'Clear this database before importing' check box located on the bottom left of the above window. This box allows you to clear any existing settings if an existing database is being used or also allows you to merge templates into a single database. Notice in the list of templates above there is an 'isa.inf'

template file. After importing the current template file that has been selected we can repeat the steps and make sure the check box is not checked and select the isa.inf template file to add those settings incrementally to the current settings. Once they have been incorporated the new combined settings can be exported to a new template file. The next step is to analyze the system. This is a non-invasive procedure which produces a comparison report of the database settings versus the current system settings.



Here is a screen shot of the results after the analysis was done also showing some of the new values starting with the 'Network Security: Allow dead gateway detection' that were exposed from the new sceregvl.inf file.

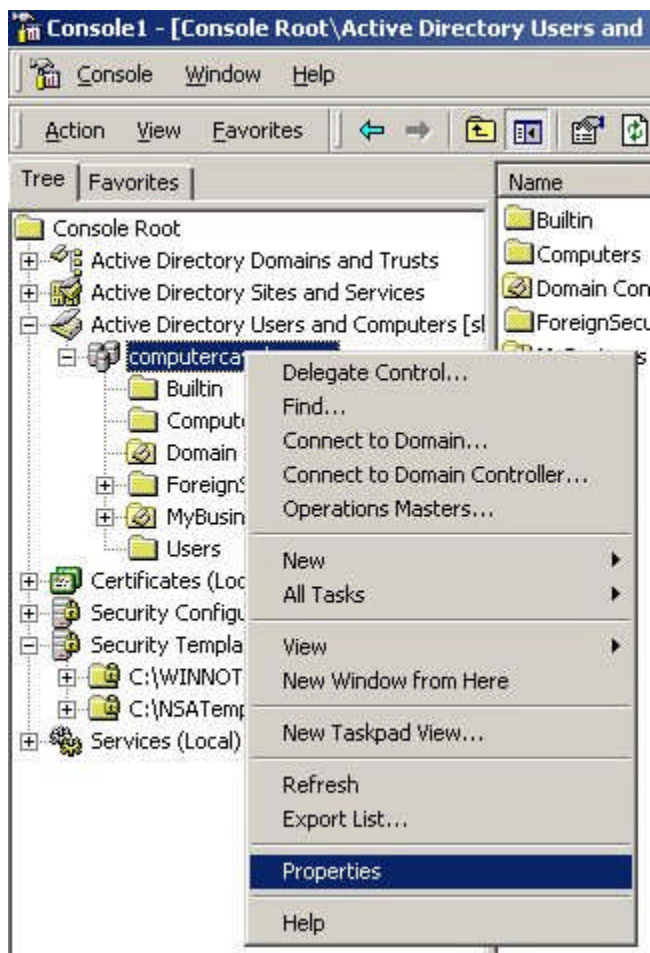
Since this is a Small Business Server which means it is also a Domain Controller there are some settings that need special attention. These specifically have to do with the account policies and information about this subject is discussed in detail in Microsoft's Q article [Q259576](#) "Group Policy Application Rules for Domain Controllers"¹⁴. A brief excerpt from the article explains –

"Domain controllers pull some security settings only from group policy objects linked to the root of the domain. Because domain controllers share the same account database for the domain, certain security settings must be set uniformly on all domain controllers..."

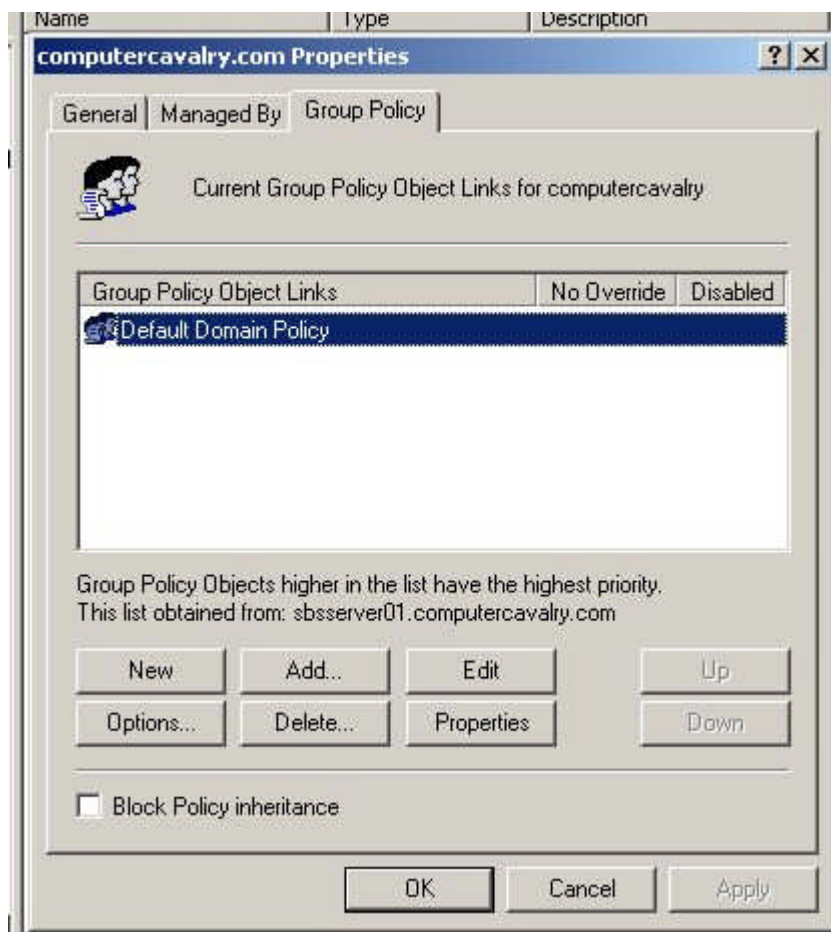
The template for the domain policy can be imported into the GPO object that is linked to the domain. The steps to do this can be found in Microsoft's Q article [Q321679](#)¹⁵ and are explained below.

The first step is to create an MMC with the Active Directory Users and Computers snap-in included or use the Small Business Administrator Console located on the menu. Once this is done we can expose the GPO for the domain by following the steps below.

- 1) Expand Active Directory Users and Computers and right click on the domain object.

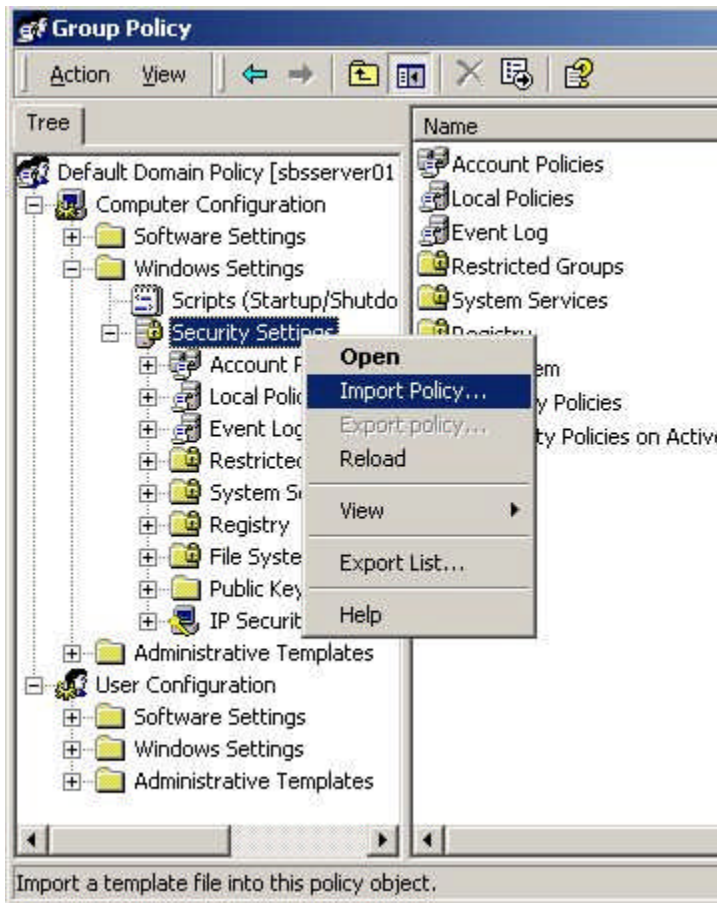


2) Select the Group Policy Tab and then the Default Domain Policy Object



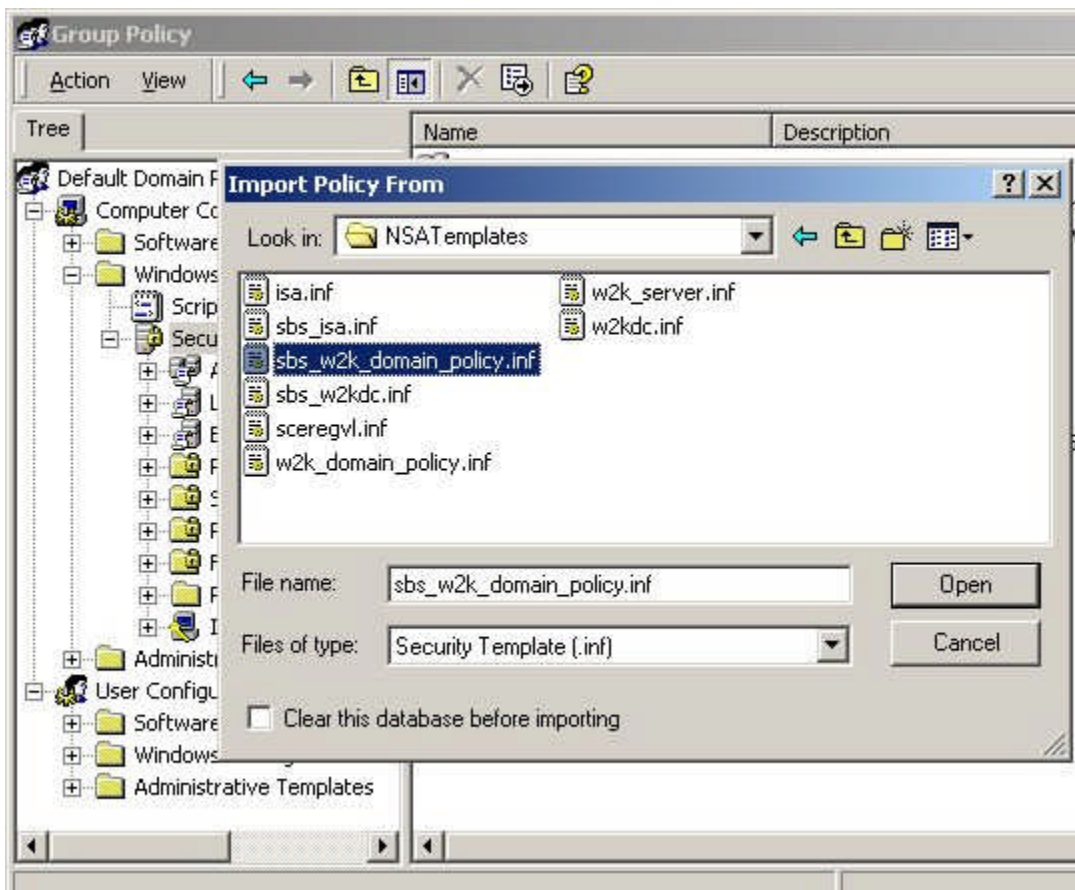
3) Click the Edit button

© SANS Institute 2004

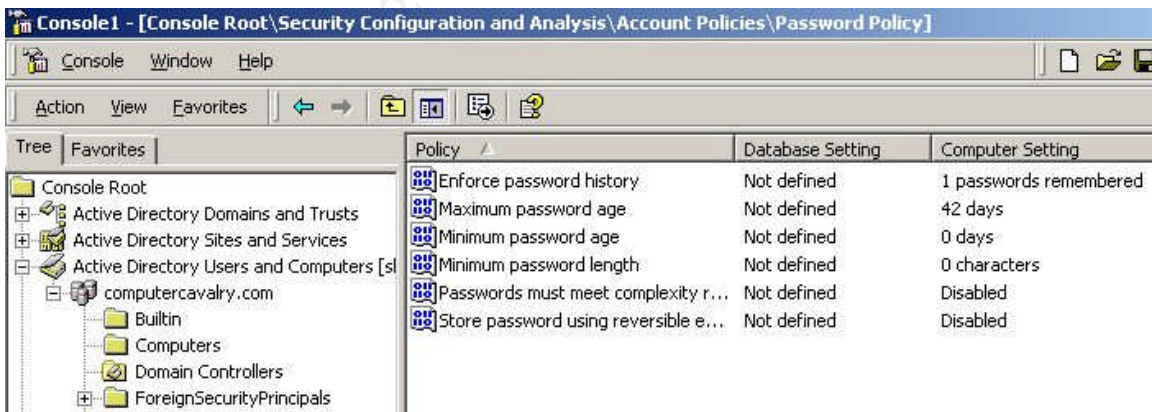


4) Expand Computer Configuration-> Windows Settings-> Security Settings – you can see that this is where the account policies are located.

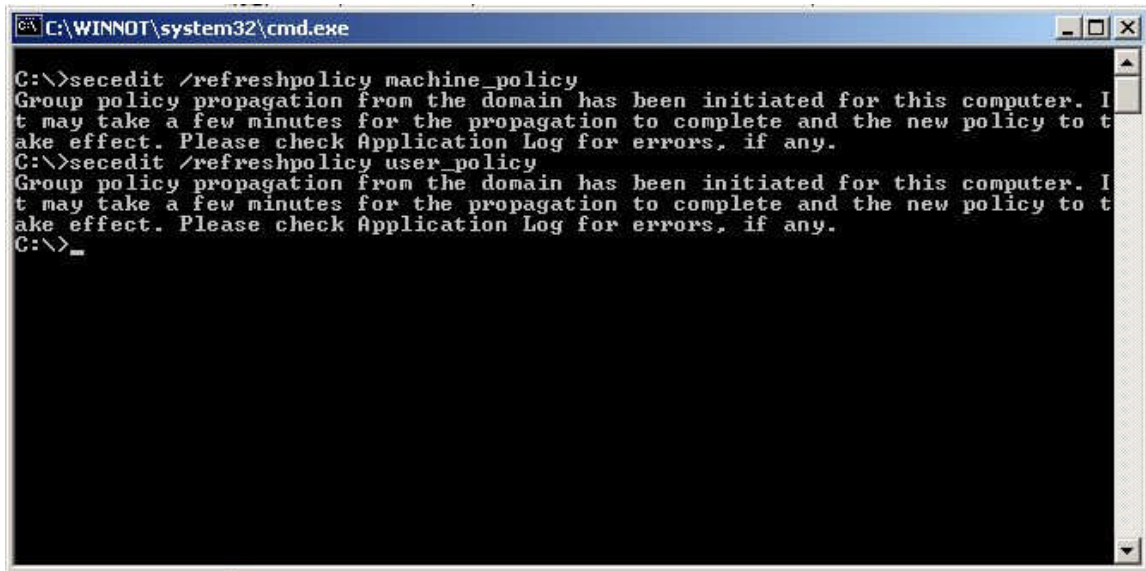
5) Right click Security Settings and select Import Policy from the context menu



6) Locate the domain policy template – make sure and do not check the ‘Clear this database before importing’ check box and click the open button.



Back in the Security Configuration and Analysis tool we can see the current settings listed under Computer Settings and the Database Settings are ‘Not defined’.



```
C:\WINNOT\system32\cmd.exe

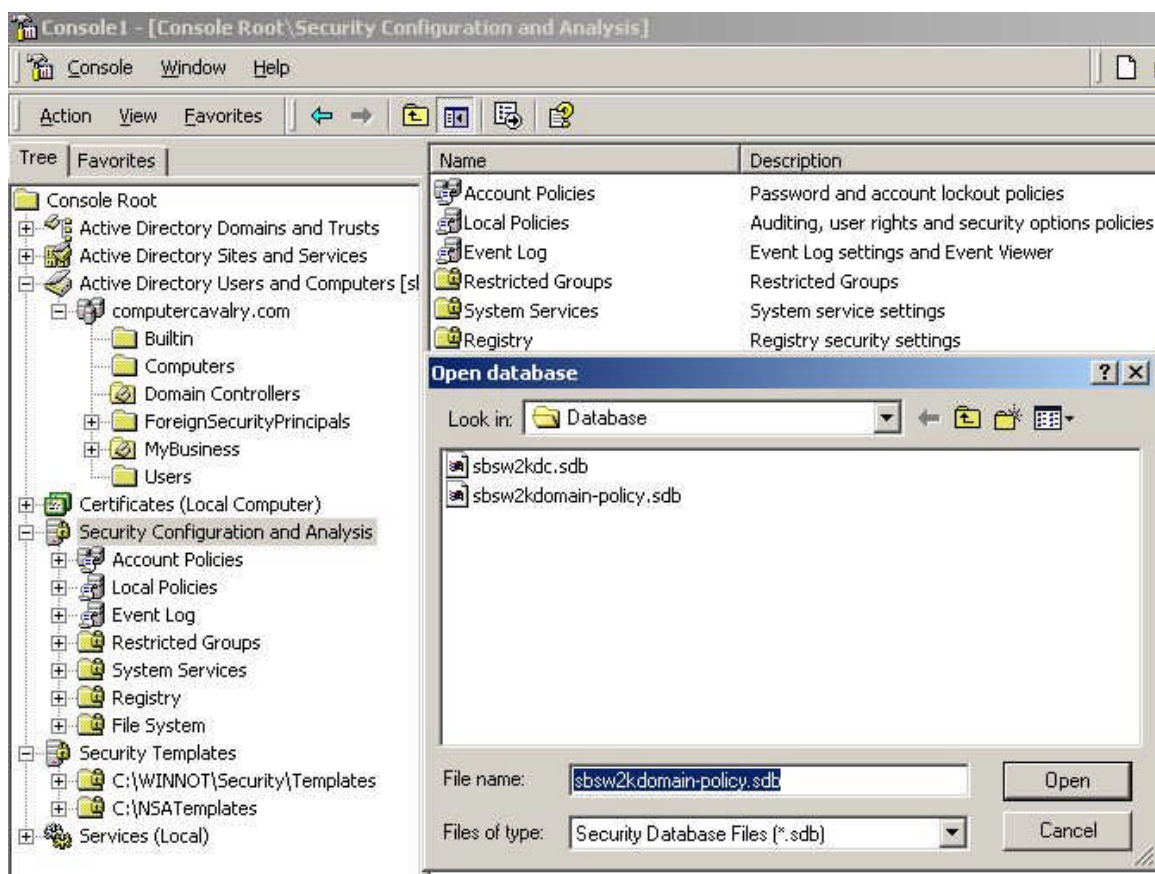
C:\>secedit /refreshpolicy machine_policy
Group policy propagation from the domain has been initiated for this computer. I
t may take a few minutes for the propagation to complete and the new policy to t
ake effect. Please check Application Log for errors, if any.
C:\>secedit /refreshpolicy user_policy
Group policy propagation from the domain has been initiated for this computer. I
t may take a few minutes for the propagation to complete and the new policy to t
ake effect. Please check Application Log for errors, if any.
C:\>_
```

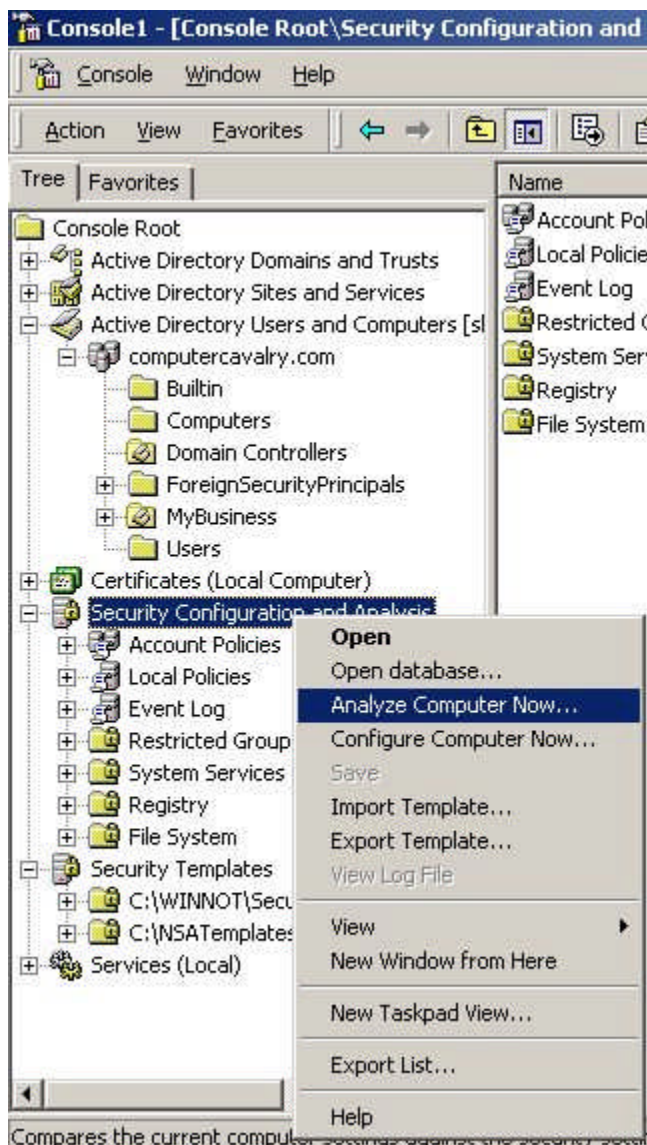
We could wait for the policy to update which is 90 minutes on a workstation or member server or 5 minutes on a domain controller. We can manually force the update by using the secedit.exe command line tool as illustrated above. We force the update by typing

```
C:\>secedit /refreshpolicy machine_policy
```

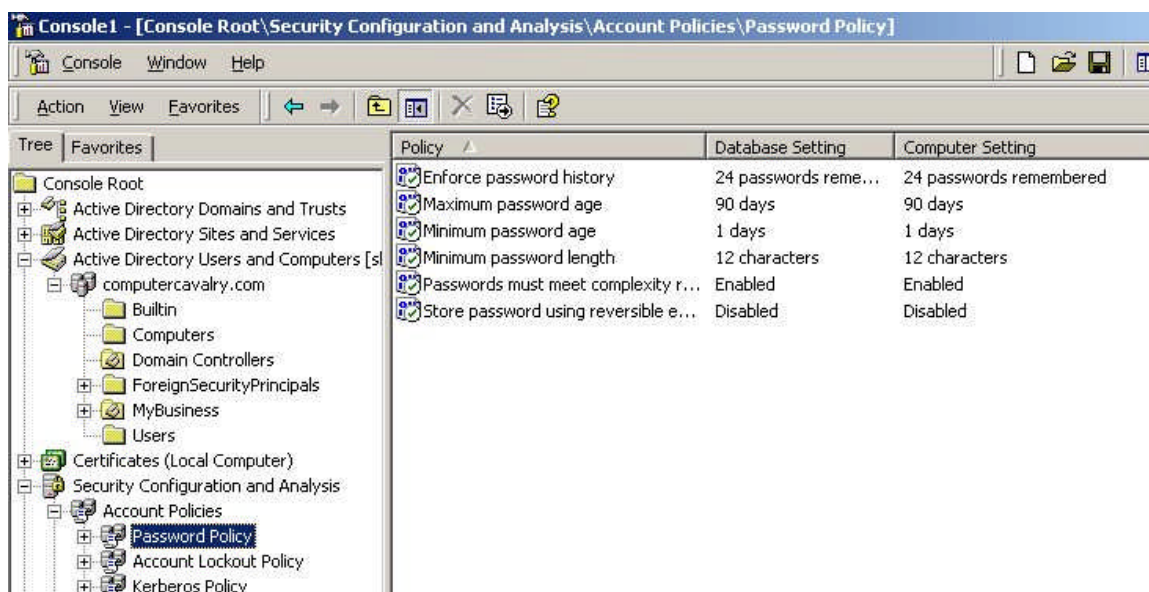
```
C:\>secedit /refreshpolicy user_policy
```

© SANS Institute 2004, Author retains full rights.





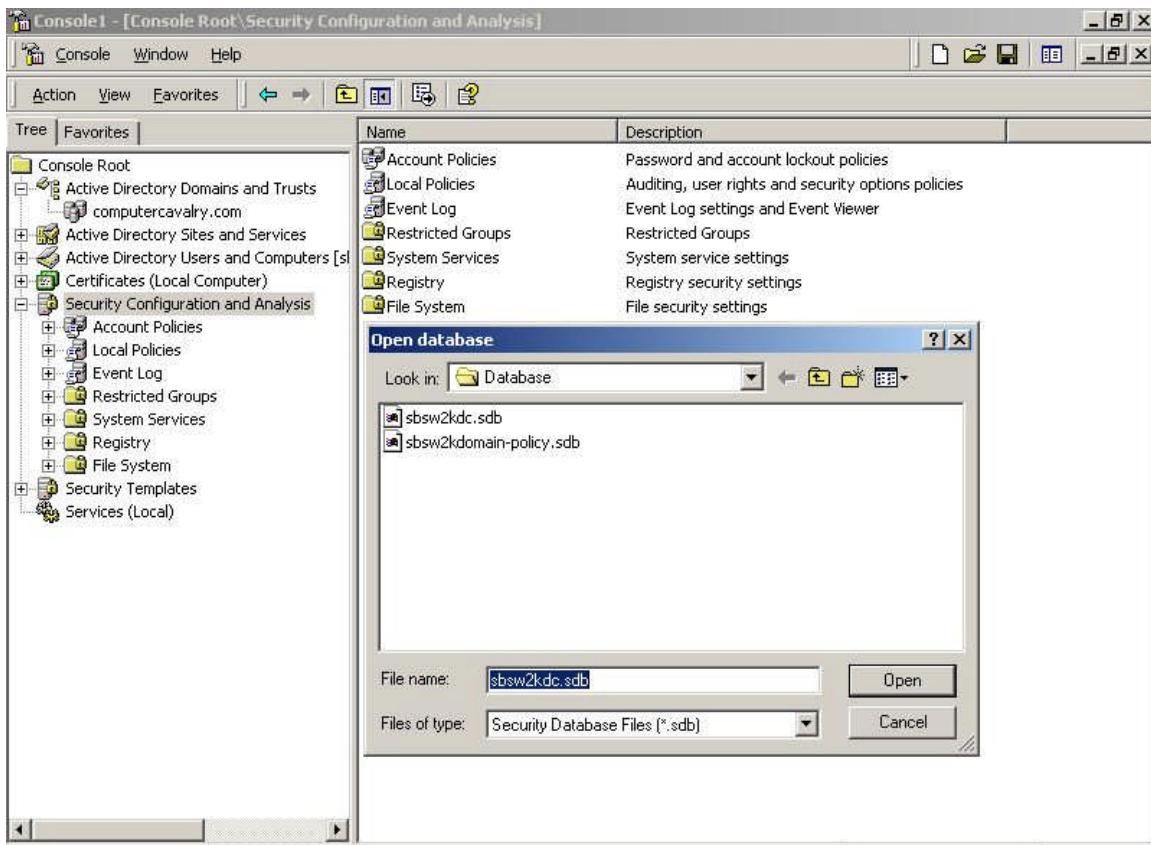
Back to the Security and Configuration tool we can open the policy domain database back up and run the 'Analyze Computer Now' option to verify that the changes have actually been made.



The results as expected do reflect the updated values from the policy domain template and match the Database settings from that template inf file.

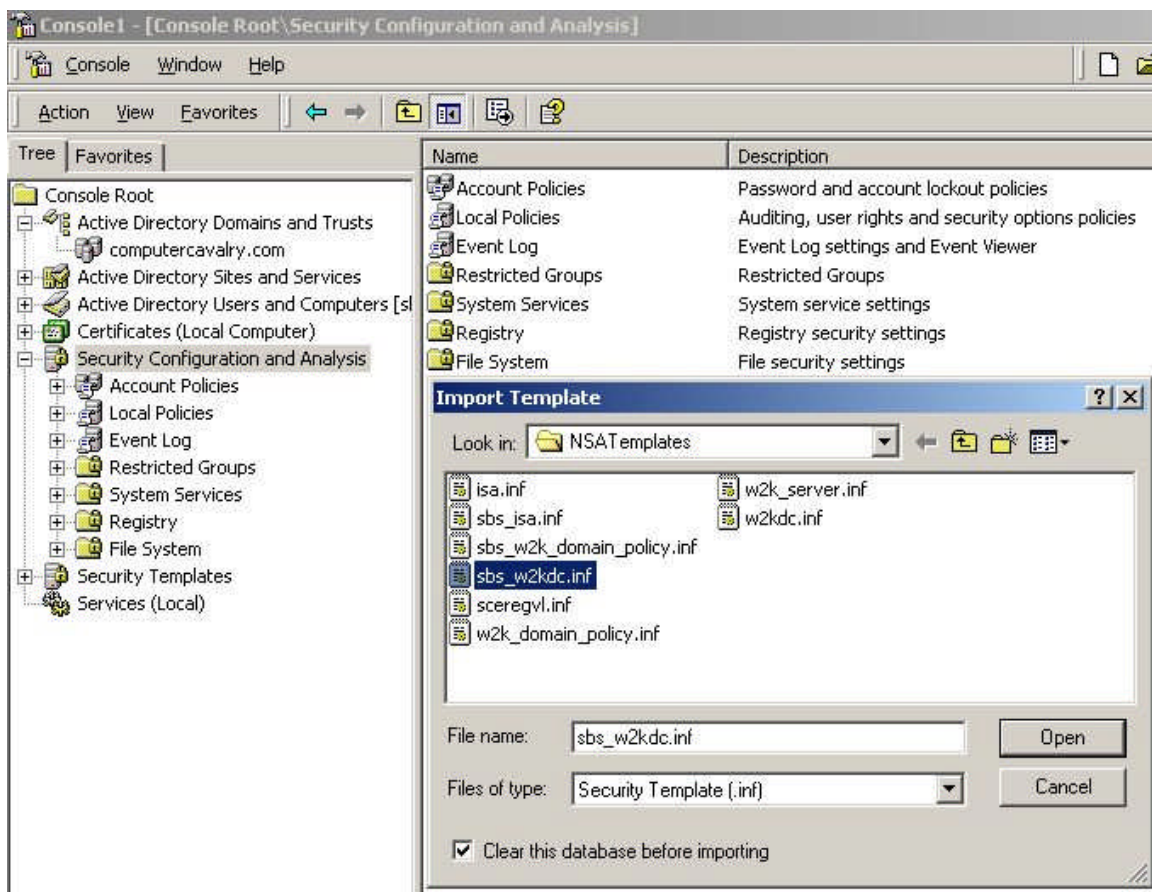
The next step is to merge the sbs_w2kdc.inf and sbs_isa.inf template files into one security database to apply to the Small Business server. This way we can take advantage of the settings included in both. The first step is to open our existing database file that was created earlier.

© SANS Institute 2004, Author retains full rights.



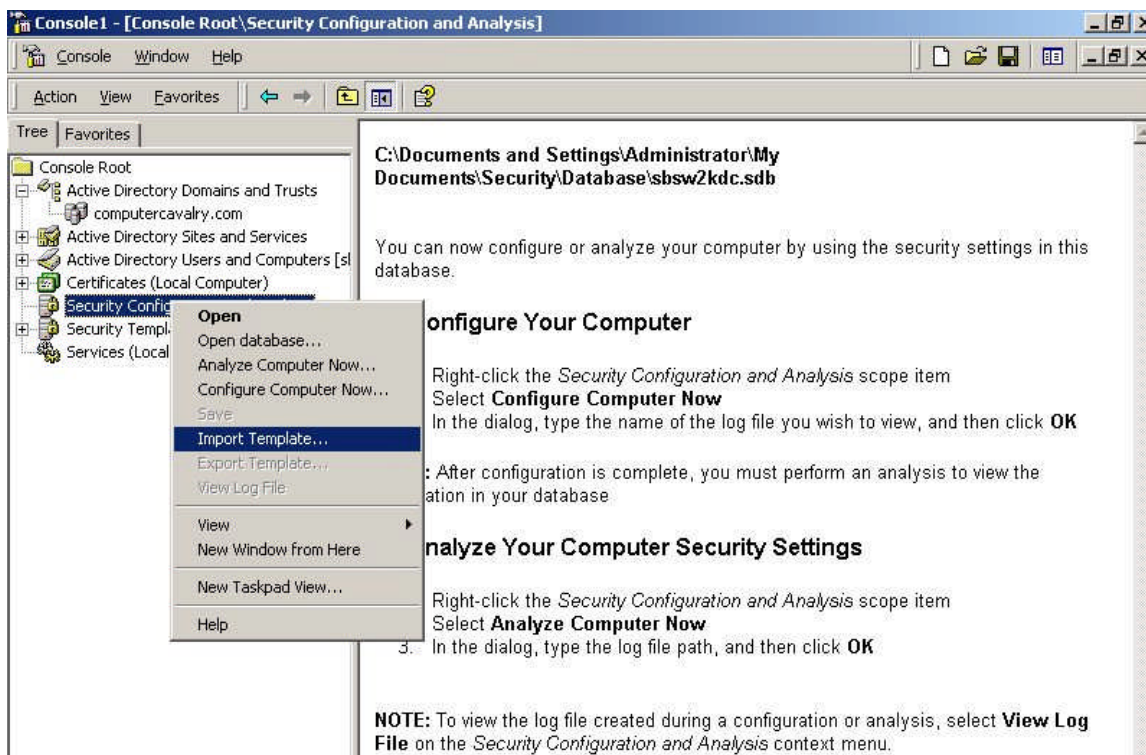
Once the database is open the first template is imported.

© SANS Institute 2004

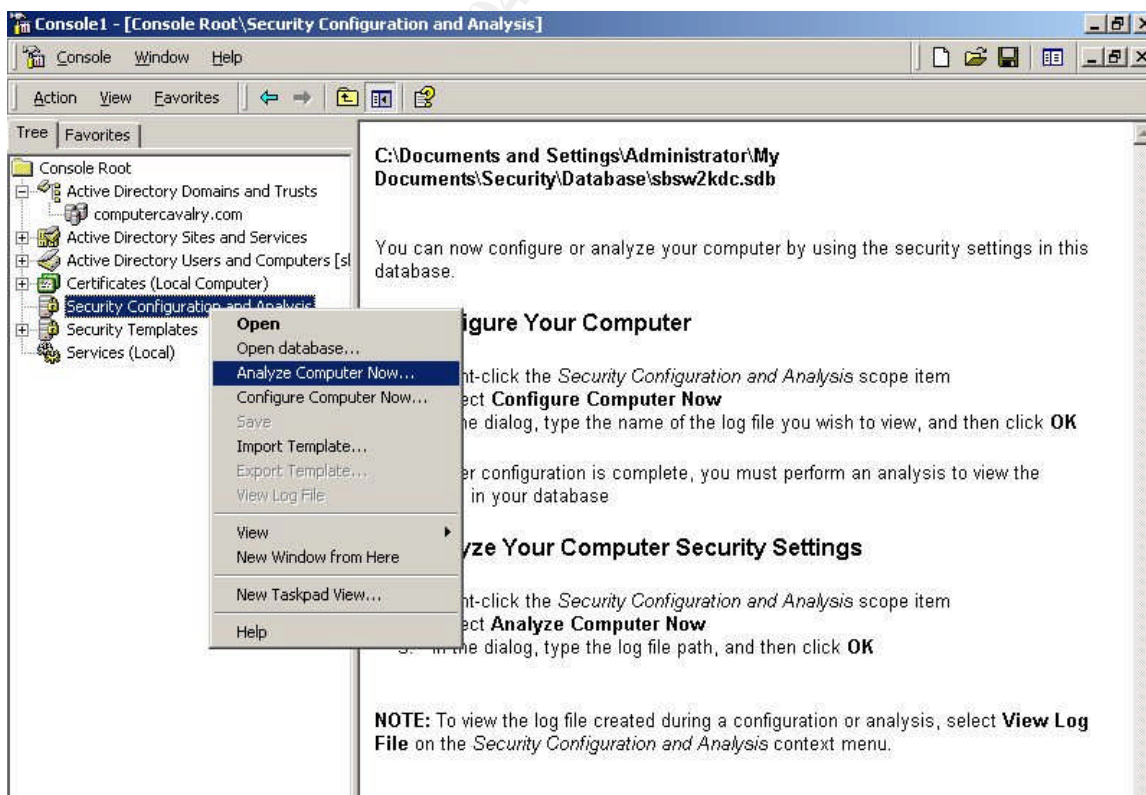


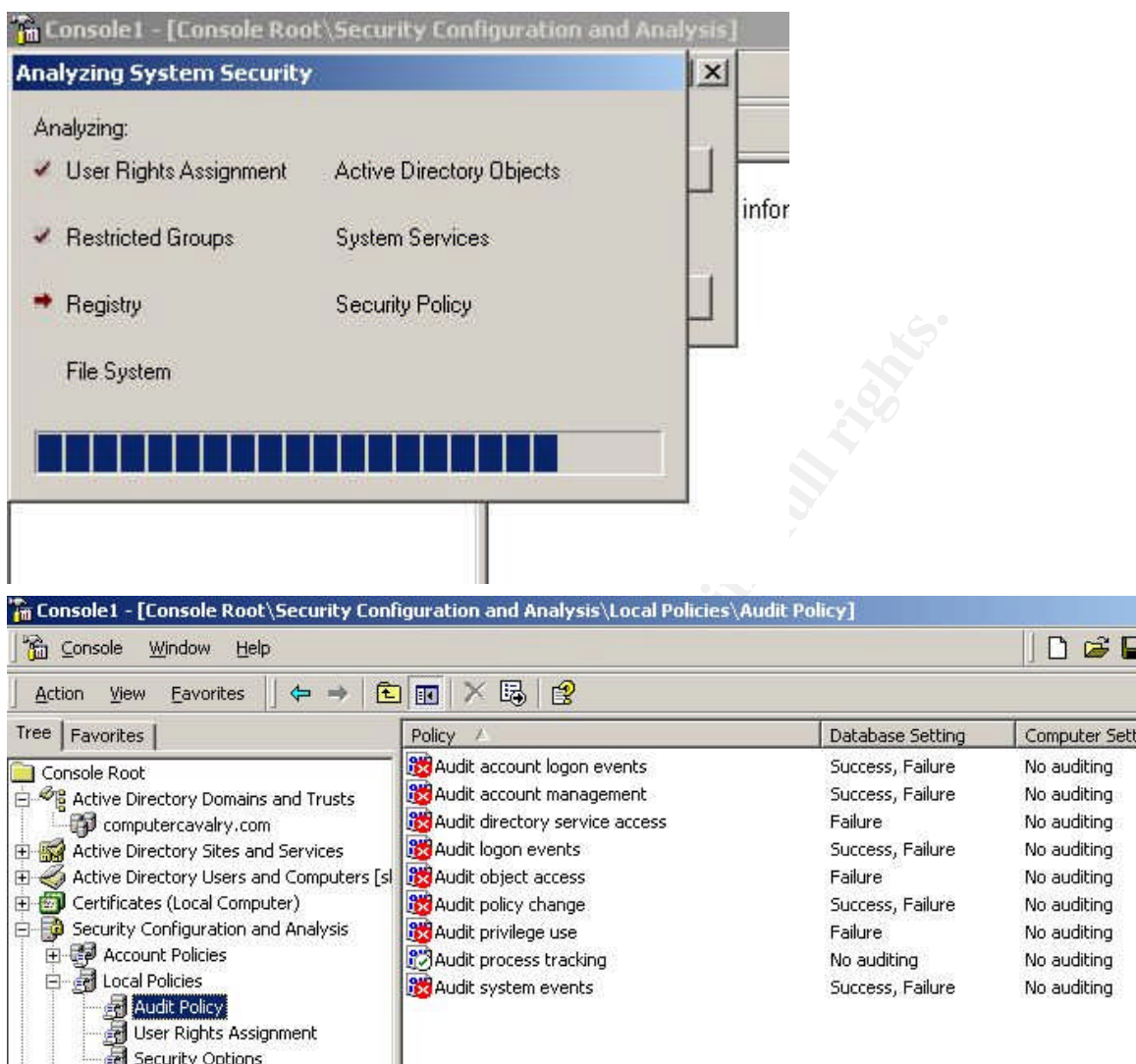
Since we are using an existing database it is important to check the 'Clear this database before importing' check box to remove any existing settings that may exist.

© SANS Institute 2004



Next the Import Template option is selected again this time selecting the sbs_isa.inf template file and confirming that the check box is NOT selected since the goal is to merge the two template files. Then next step is to analyze the computer and review the results.

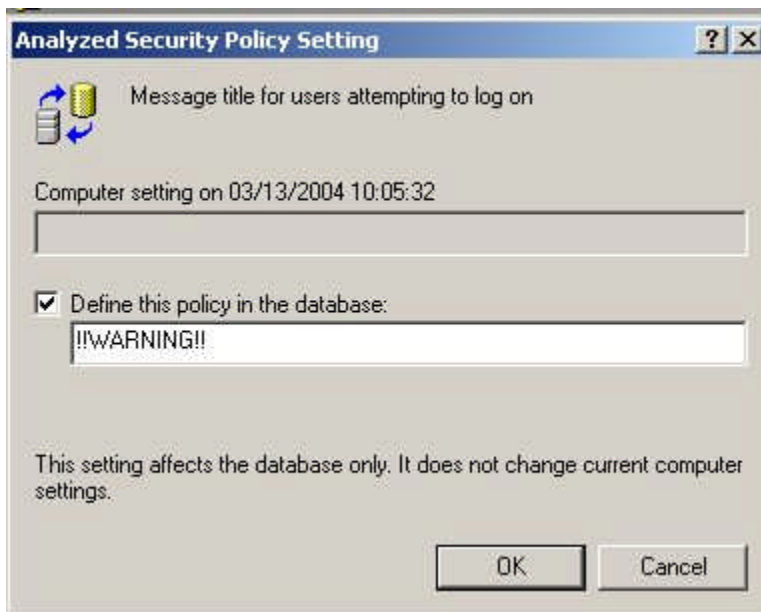




The red x's shown in the example above is a result of a mismatch between the Database setting and the local computer setting. It should be pointed out that mismatches do not necessarily mean that the computer setting is less secure. As an example, if the template file or database setting for password expiration was 90 days and the local security setting on the PC is 45 days a mismatch would occur but obviously having passwords expire every 45 days instead of every 90 days would be more secure if in fact this policy was being followed. A green check mark represents a match between the local setting and the database setting and an exclamation point represents a setting that is available in the database but not on the local system. The NSA documentation that accompanies the templates goes into great detail about each setting and emphasizes 'not to blindly apply the settings to a production machine'.

All the settings should be reviewed for each specific environment. Remember that there is always a delicate balance between security and functionality. Some of the settings can potentially break things particularly in environments that contain down level clients such as Windows 9x machines. There are some settings that are not complete because they are

considered 'local'. For example under the Security Options section the 'Message text for users attempting to log on' and the 'Message title for users attempting to log on' or empty and need information that would be appropriate for your specific situation.



An example of a simple warning title above and below is an example of text that could be used. The text is actually applied as a single line and only broken up here for display purposes.

“This system is for the use of authorized users only.

Individuals using this computer system with authority, without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.”

This is only meant as an example and the wording should be phrased to meet your needs and be appropriate for your specific environment.

Again to re-emphasize the point of not just acquiring templates and blindly applying them I have listed a few of the settings below as examples that come with warning messages in the NSA documentation. These specific settings can be found under the Security Configuration and Analysis snap-in -> Local Policies -> Security Options

- 1) Additional restrictions for Anonymous connections – NSA recommendation for Domain Controllers – ‘No access without explicit anonymous permissions’ (registry value = 2).³⁰

This setting is accompanied by a warning that states that applying the recommended value could potentially cause a negative impact on setting up trust relationships, authentication in a ‘mixed’ environment, running certain services or applications. It references Microsoft Knowledge Base article [Q246261](#).

- 2) Lan Manager Authentication level – ‘Sets the challenge/response authentication level for network logons with non-Windows 2000 Windows clients.’ NSA recommendation for domain controllers – ‘Send NTLMv2 response only/refuse LM and NTLM’.³¹

This setting is accompanied by a warning that includes several areas of concern –

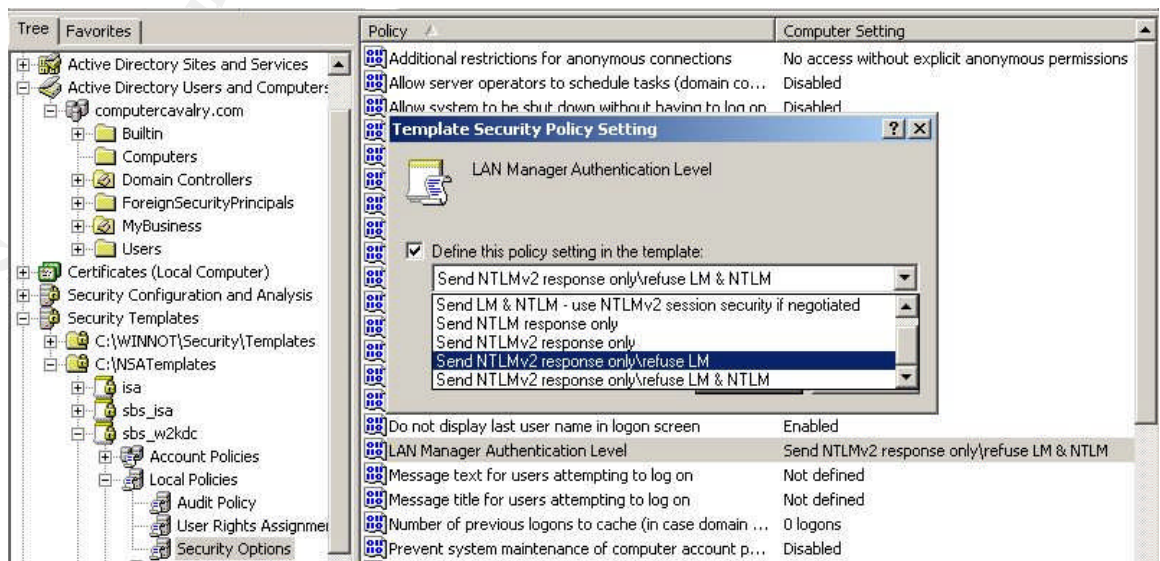
- 1) Some Windows 2000 services use NTLM for authentication, as an example the Cluster Service. Using the recommended setting would cause these services to fail.
 - 2) Using a setting higher than 2 could cause connection issues with down-level clients like Win9x or NT 4.0 prior to service pack 4. Some of this can be overcome by installing the Active Directory Services client found on the Windows 2000 server CD or that can be downloaded from Microsoft’s web site (preferred) on any Win9x clients.
 - 3) If you are adding a Windows 2000 machine to a Windows NT 4.0 domain this value may need to be set to 4 or lower on the Windows NT 4.0 domain controller.
 - 4) Access to a an Exchange server via IMAP or POP may not work from either Outlook 2000 or Outlook Express if this setting is set to 5 the highest. The recommendation would then be to set it to ‘Send NTLMv2 response only/refuse LM’, value=4. It also states that service pack 2 fixes this known issue.
- 3) Rename administrator account – This is one of the settings that is not actually set because it is considered to be ‘environment specific’. My preference is to do this manually and have actually completed this step earlier in the process. I am listing it here because it does come with a ‘gotcha’ and you should be aware of this. If you decide to use this setting and start seeing event ID 1000 and 1202 in the event logs you can refer to Microsoft Knowledge Base article [Q260715](#) for the fix. Basically what has happened is that an existing name was used to rename the administrators account.³²
 - 4) Network Security: Protect against SYN attacks – This setting adjusts the retransmission of TCP-SYN-ACKS, which is the second phase of the TCP 3-Way Hand Shake and can potentially cause a denial of service by exhausting resources on the server. This setting changes the default behavior of this phase of the TCP

3-Way Hand Shake by causing the connection responses to time out more quickly in the event of a SYN denial of service attack. The NSA recommended setting is 'Better Protection' (registry value = 2) but interestingly the template comes configured with 'Best Protection' enabled and is also accompanied by a warning messages about using this specific setting that could lead to network performance degradation.³³

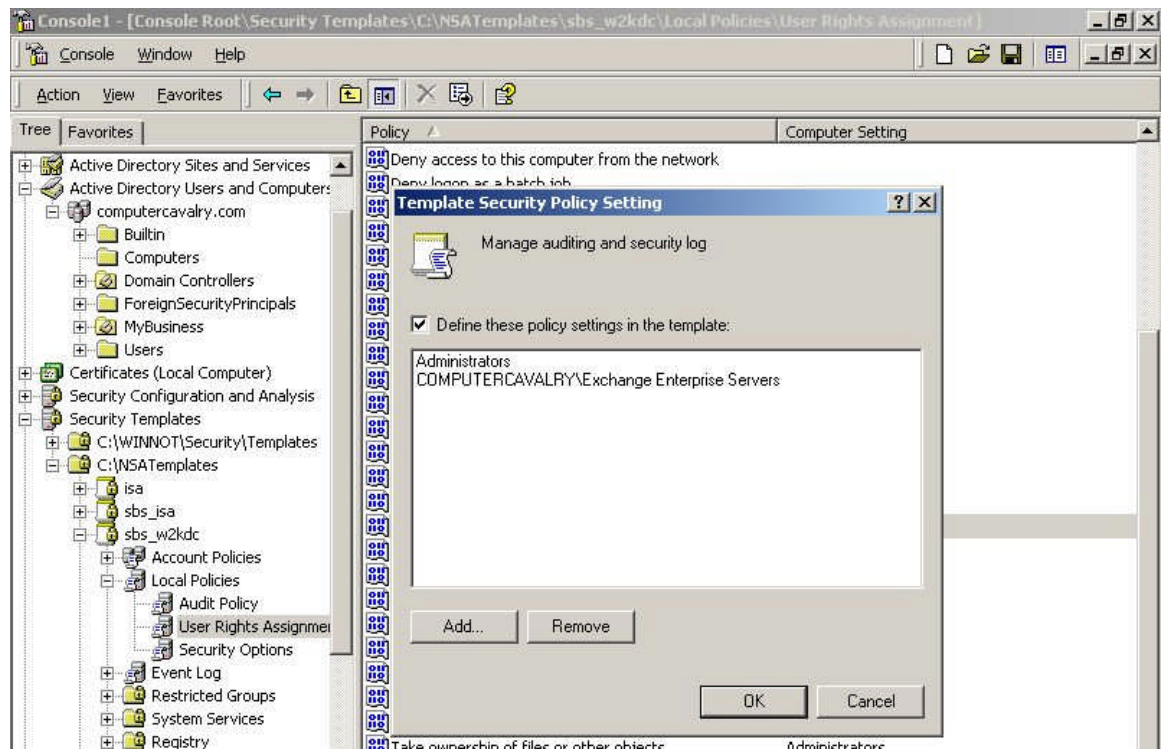
- 5) Restrict CD-ROM access to locally logged on user only – this setting is enabled by default but is also accompanied by a warning message that states that there is a known bug when installing Office 2000 from a CD which causes an error – “Error 1311: Source file not found: E:\OFFICE1.CAB verify that the file exists and that you have access to it.” It goes on to say that a similar error could occur with the Windows 2000 Resource Kit which I have confirmed. More details and workarounds can be found in Microsoft Knowledge Base article [Q230895](http://support.microsoft.com/kb/q230895).³⁴

Since these settings are being applied to a Small Business Server which is a domain controller and is running Exchange Server 2000 the NSA documentation includes a document entitled “Instructions for configuring Microsoft Exchange to work with the Windows 2000 Security Recommendations Guides”. It includes additional changes that need to be made to eliminate possible errors that could be encountered when a client attempts to log on using IMAP or POP3. The recommendation states that to avoid this problem one of two actions may be taken.

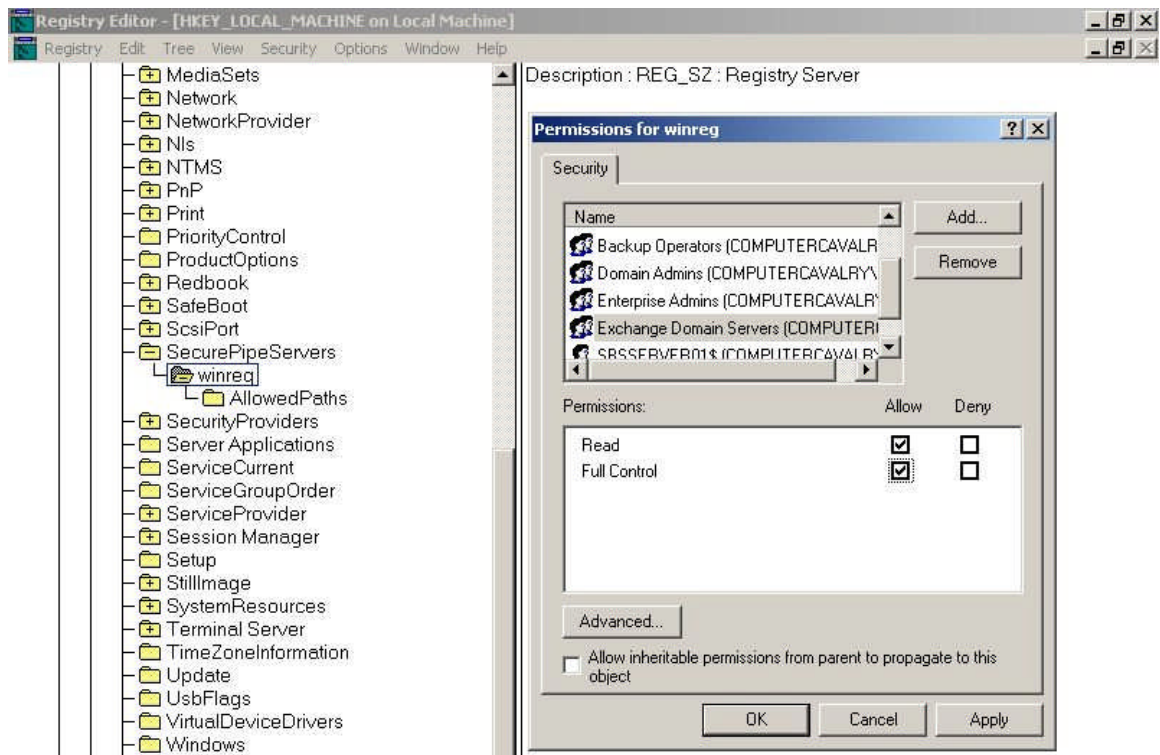
- 1) 'Set the client to use Secure Password Authentication (preferred)'
- 2) OR
 - a) On both the Exchange servers and Domain Controllers, set the LAN Manager Auth Level to 'send NTLMv2 response only/refuse LM'



- b) Ensure that the Exchange Servers group is given the right to manage audit and security logs on the security policy applied to Domain Controllers.

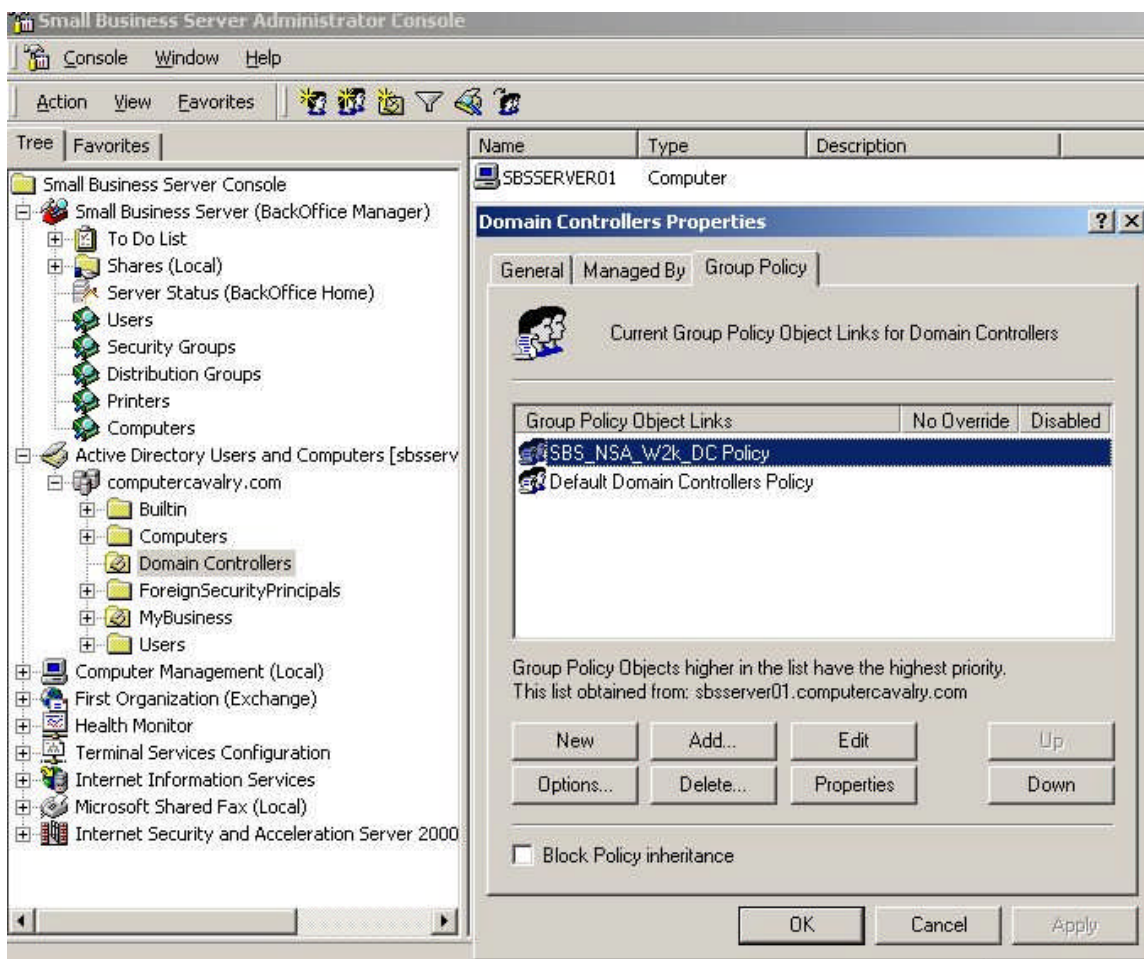


- c) Allow Exchange Domain Servers group full control access to the HKLM\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg key.



These settings are also added to the current database in the Security Configuration and Analysis snap-in so that when we export to a template file it will be included.

© SANS Institute 2004, All rights reserved.



Once we are satisfied with all the settings we can export the database to a template file which can then be imported into a new GPO object linked to the Domain Controllers OU.

The screen shot is used to illustrate that when there are multiple GPO's linked to a container object they are applied from bottom to top and that if there are settings that conflict then the last one written 'wins'. Since we are wanting to just apply these settings to the local PC the Security Configuration and Analysis snap-in was actually used by selecting the 'Configure Computer Now...' option.

Before leaving the area of security templates the subject of deleting customized options should be addressed. To permanently remove customized options from the sceregl.inf file is not as simple as just removing them. This is actually a multiple step process which is listed below and can be found with an example in chapter 3 on page 59 of the NSA documentation.

- 1) "Open sceregl.in in a text editor (Notepad)
- 2) Remove the specific security option from the inf file under the [Registry Registry Values] section

- 3) Under the section labeled 'delete these values from current system', add the registry key to be removed from the template.
- 4) Save and close sceregvl.inf file
- 5) At the command prompt re-register the dll – regsvr32 scecli.dll
- 6) Open the Security Template snap-in and verify the option no longer appears in the Local Policies ->Security options section.
- 7) To clean up, edit the sceregvl.inf file, remove the entry added under the 'delete' section, save and close and re-register the scecli.dll again.”

The next task at hand would be the Windows services. A detailed description of most of the Windows services and their function can be found [here](#). Again the goal is to eliminate unnecessary services without breaking any required functionality. The first step is to inventory the current services that are running on the system. Utilizing a script from the [Small Business Server 2000 Resource Kit](#)¹⁶ called service.vbs we can collect a list of the current services on the SBS system. From a command line type: cscript service.vbs > services.txt which will pipe the output to the text file services.txt. Here is the output below:

Microsoft (R) Windows Script Host Version 5.6

Copyright (C) Microsoft Corporation 1996-2001. All rights reserved.

NAME	STATE	DISPLAY NAME
Alerter	Running	Alerter
AppMgmt	Stopped	Application Management
BITS	Stopped	Background Intelligent Transfer Service
Browser	Running	Computer Browser
cisvc	Stopped	Indexing Service
ClipSrv	Stopped	ClipBook
Dfs	Running	Distributed File System
Dhcp	Running	DHCP Client
dmadmin	Stopped	Logical Disk Manager Admin Service
dmserver	Running	Logical Disk Manager
DNS	Running	DNS Server
Dnscache	Running	DNS Client
Eventlog	Running	Event Log
EventSystem	Running	COM+ Event System
Fax	Stopped	Fax Service
Fwsrv	Running	Microsoft Firewall

GKSVc	Running	Microsoft H.323 Gatekeeper
IISADMIN	Running	IIS Admin Service
IMAP4Svc	Running	Microsoft Exchange IMAP4
isactrl	Running	Microsoft ISA Server Control
IsmServ	Running	Intersite Messaging
kdc	Running	Kerberos Key Distribution Center
lanmanserver	Running	Server
lanmanworkstation	Running	Workstation
LicenseService	Running	License Logging Service
LmHosts	Running	TCP/IP NetBIOS Helper Service
Messenger	Running	Messenger
mnmsrvc	Stopped	NetMeeting Remote Desktop Sharing
ModemSharingServer	Running	Shared Modem Services
MSDTC	Running	Distributed Transaction Coordinator
MSExchangeES	Stopped	Microsoft Exchange Event
MSExchangeIS	Running	Microsoft Exchange Information Store
MSExchangeMGMT	Running	Microsoft Exchange Management
MSExchangeMTA	Running	Microsoft Exchange MTA Stacks
MSExchangeSA	Running	Microsoft Exchange System Attendant
MSExchangeSRS	Stopped	Microsoft Exchange Site Repl Service
MSFTPSVC	Running	FTP Publishing Service
MSIServer	Running	Windows Installer
MSPOP3Connector	Stopped	Microsoft Connector for POP3 Mailboxes
MSSEARCH	Running	Microsoft Search
MSSQLSERVER	Running	MSSQLSERVER
MSSQLServerADHelper	Stopped	MSSQLServerADHelper
MSSQLServerOLAPServ	Running	MSSQLServerOLAPService
NetDDE	Stopped	Network DDE
NetDDEdsdm	Stopped	Network DDE DSDM
Netlogon	Running	Net Logon
Netman	Running	Network Connections
NntpSvc	Running	Network News Transport Protocol (NNTP)
NtFrs	Running	File Replication Service
NtLmSsp	Running	NT LM Security Support Provider

NtmsSvc	Running	Removable Storage
PlugPlay	Running	Plug and Play
PolicyAgent	Running	IPSEC Policy Agent
POP3Svc	Running	Microsoft Exchange POP3
ProtectedStorage	Running	Protected Storage
RasAuto	Stopped	Remote Access Auto Connection Manager
RasMan	Running	Remote Access Connection Manager
RemoteAccess	Stopped	Routing and Remote Access
RemoteRegistry	Running	Remote Registry Service
RESvc	Running	Microsoft Exchange Routing Engine
RpcLocator	Running	Remote Procedure Call (RPC) Locator
RpcSs	Running	Remote Procedure Call (RPC)
RSVP	Stopped	QoS RSVP
SamSs	Running	Security Accounts Manager
SCardDrv	Stopped	Smart Card Helper
SCardSvr	Stopped	Smart Card
Schedule	Running	Task Scheduler
seclogon	Running	RunAs Service
SENS	Running	System Event Notification
SharedAccess	Stopped	Internet Connection Sharing
SharedFax	Running	Microsoft Shared Fax
SMTPSVC	Running	Simple Mail Transport Protocol (SMTP)
Spooler	Running	Print Spooler
SQLSERVERAGENT	Stopped	SQLSERVERAGENT
SysmonLog	Stopped	Performance Logs and Alerts
TapiSrv	Running	Telephony
TermService	Running	Terminal Services
TlntSvr	Stopped	Telnet
TrkSvr	Running	Distributed Link Tracking Server
TrkWks	Running	Distributed Link Tracking Client
UPS	Stopped	Uninterruptible Power Supply
UtilMan	Stopped	Utility Manager
W32Time	Running	Windows Time
W3Proxy	Running	Microsoft Web Proxy

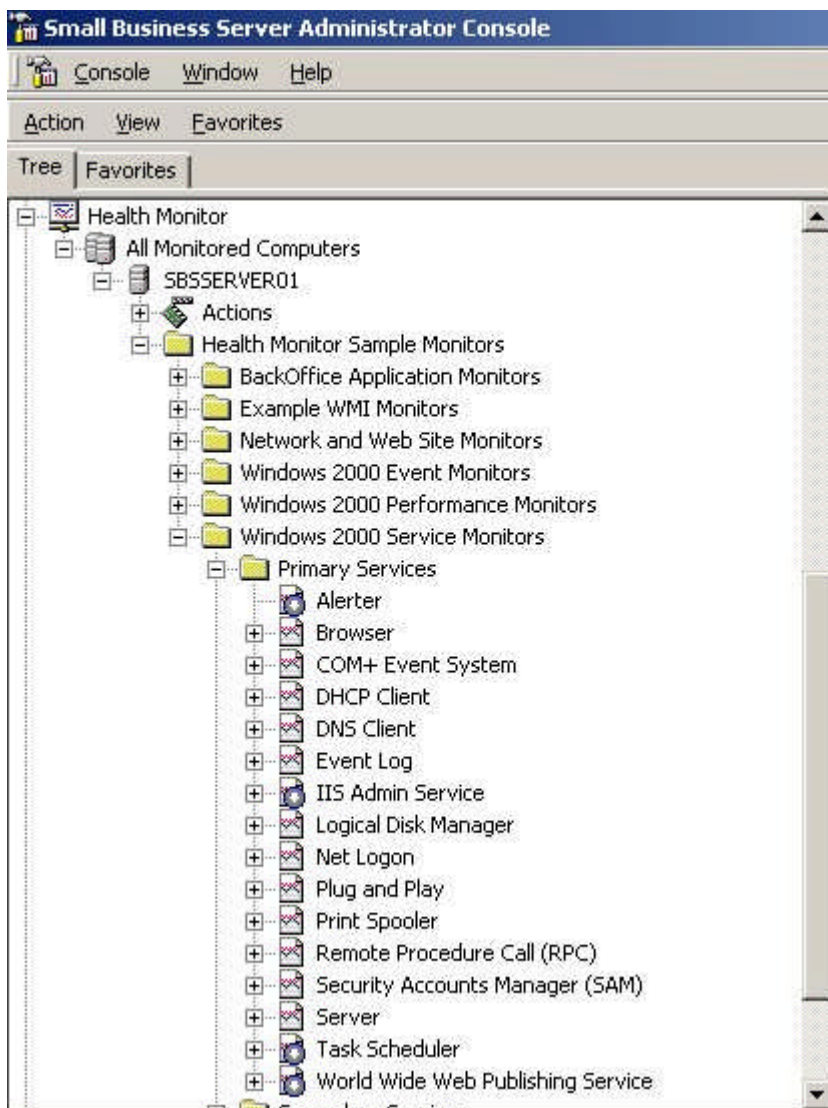
w3schdwn	Running	MS Scheduled Cache Content Download
W3SVC	Running	World Wide Web Publishing Service
WinMgmt	Running	Windows Management Instrumentation
WINS	Running	Windows Internet Name Service (WINS)
Wmi	Running	Windows Mgmt Instr Driver Exten
wuauserv	Running	Automatic Updates
WZCSVC	Stopped	Wireless Configuration

Next another list was compiled from the list above along with some trial and error. It lists the default setting for each service and a recommendation to either maintain the current state or disable the service. A decision was made to turn off all the SQL services since they will not be needed at this time. This process is environment specific and may require lots of 'tweaking' to get it right and could need to change as the environment changes.

NAME	DISPLAY NAME	Default Recommendation	
Alerter	Alerter	Auto	Disabled
AppMgmt	Application Management	Manual	Manual
BITS	Background Intel Transfer Srvc	Manual	Manual
Browser	Computer Browser	Auto	Auto
cisvc	Indexing Service	Manual	Manual
ClipSrv	ClipBook	Manual	Disabled
Dfs	Distributed File System	Auto	Auto
Dhcp	DHCP Client	Auto	Auto
dmadmin	Logical Disk Manager Admin Service	Manual	Manual
dmserver	Logical Disk Manager	Auto	Auto
DNS	DNS Server	Auto	Auto
Dnscache	DNS Client	Auto	Auto
Eventlog	Event Log	Auto	Auto
EventSystem	COM+ Event System	Manual	Manual
Fax	Fax Service	Manual	Manual
Fwsrv	Microsoft Firewall	Auto	Auto
GKSV	Microsoft H.323 Gatekeeper	Auto	Disabled
IISADMIN	IIS Admin Service	Auto	Auto
IMAP4Svc	Microsoft Exchange IMAP4	Auto	Auto
isactrl	Microsoft ISA Server Control	Auto	Auto
IsmServ	Intersite Messaging	Auto	Disabled
kdc	Kerberos Key Distribution Center	Auto	Auto
lanmanserver	Server	Auto	Auto
lanmanworkstation	Workstation	Auto	Auto
LicenseService	License Logging Service	Auto	Auto
LmHosts	TCP/IP NetBIOS Helper Service	Auto	Auto
Messenger	Messenger	Auto	Disabled
mnmsrvc	NetMeeting Remote Desktop Sharing	Manual	Disabled
ModemSharingServer	Shared Modem Services	Auto	Auto
MSDTC	Distributed Transaction Coordinator	Auto	Disabled
MSExchangeES	Microsoft Exchange Event	Manual	Disabled
MSExchangeIS	Microsoft Exchange Information Store	Auto	Auto
MSExchangeMGMT	Microsoft Exchange Management	Auto	Auto
MSExchangeMTA	Microsoft Exchange MTA Stacks	Auto	Auto
MSExchangeSA	Microsoft Exchange System Attendant	Auto	Auto
MSExchangeSRS	Microsoft Exchange Site Repl Srvc	Auto	Disabled
MSFTPSVC	FTP Publishing Service	Auto	Disabled
MSIServer	Windows Installer	Manual	Manual
MSPOP3Connector	MS Connector for POP3 Mailboxes	Manual	Disabled
MSSEARCH	Microsoft Search	Auto	Disabled
MSSQLSERVER	MSSQLSERVER	Auto	Disabled
MSSQLServerADHelper	MSSQLServerADHelper	Manual	Disabled

MSSQLServerOLAPServ	MSSQLServerOLAPService	Auto	Disabled
NetDDE	Network DDE	Manual	Disabled
NetDDEdsdm	Network DDE DSDM	Manual	Disabled
Netlogon	Net Logon	Auto	Auto
Netman	Network Connections	Manual	Manual
NntpSvc	Network News Transport Protocol (NNTP)	Auto	Disabled
NtFrs	File Replication Service	Manual	Manual
NtLmSsp	NT LM Security Support Provider	Manual	Manual
NtmsSvc	Removable Storage	Auto	Auto
PlugPlay	Plug and Play	Auto	Auto
PolicyAgent	IPSEC Policy Agent	Auto	Auto
POP3Svc	Microsoft Exchange POP3	Auto	Auto
ProtectedStorage	Protected Storage	Auto	Auto
RasAuto	Remote Access Auto Connection Manager	Manual	Manual
RasMan	Remote Access Connection Manager	Manual	Manual
RemoteAccess	Routing and Remote Access	Disabled	Disabled
RemoteRegistry	Remote Registry Service	Auto	Auto
RESvc	Microsoft Exchange Routing Engine	Auto	Auto
RpcLocator	Remote Procedure Call (RPC) Locator	Auto	Auto
RpcSs	Remote Procedure Call (RPC)	Manual	Manual
RSVP	QoS RSVP	Manual	Disabled
SamSs	Security Accounts Manager	Auto	Auto
SCardDrv	Smart Card Helper	Manual	Disabled
SCardSvr	Smart Card	Manual	Disabled
Schedule	Task Scheduler	Auto	Disabled
seclogon	RunAs Service	Auto	Auto
SENS	System Event Notification	Auto	Auto
SharedAccess	Internet Connection Sharing	Manual	Disabled
SharedFax	Microsoft Shared Fax	Auto	Auto
SMTPSVC	Simple Mail Transport Protocol (SMTP)	Auto	Auto
Spooler	Print Spooler	Auto	Auto
SQLSERVERAGENT	SQLSERVERAGENT	Manual	Disabled
SysmonLog	Performance Logs and Alerts	Manual	Manual
TapiSrv	Telephony	Manual	Manual
TermService	Terminal Services	Auto	Auto
TlntSvr	Telnet	Manual	Disabled
TrkSvr	Distributed Link Tracking Server	Manual	Disabled
TrkWks	Distributed Link Tracking Client	Auto	Disabled
UPS	Uninterruptible Power Supply	Manual	Manual
UtilMan	Utility Manager	Manual	Disabled
W32Time	Windows Time	Auto	Auto
W3Proxy	Microsoft Web Proxy	Auto	Auto
w3schdwn	Microsoft Sched Cache Content Download	Auto	Auto
W3SVC	World Wide Web Publishing Service	Auto	Auto
WinMgmt	Windows Management Instrumentation	Manual	Manual
WINS	Windows Internet Name Service (WINS)	Auto	Disabled
Wmi	Windows Management Instr. Driver Exten	Manual	Manual
wuauserv	Automatic Updates	Auto	Disabled
WZCVC	Wireless Configuration	Manual	Disabled

Once the changes were made a reboot of the system was done to evaluate any problems that might occur as a result of those changes. The first issue was a couple of counters in the SBS Health Monitor that reported errors because specific services had been disabled. This was resolved by disabling the Alerter and Task Scheduler services as seen below.



Other issues observed were error messages in the Application log that referenced the ftp counters and WINS statistics. The solution for the FTP message was to add a new DWORD value 'Disable Performance Counters' (note the spaces in the value) to the HKLM\SYSTEM\CurrentControlSet\Services\MSFTPSVC\Performance\ key. And since we had disabled the WINS service since our environment will not contain any down level clients the WINS service was uninstalled from the system and eliminated further occurrences of those error messages.

A template file was created using the combination of the domain policy template file and the revised sbs_w2kdc.inf file (which included the isa.inf template file) to be used with the CIS scoring tool. This tool which also includes template files can be down loaded from the Center for Internet Security [website](#). The web site offers tools for Windows 2000, Linux, Solaris and Cisco routers. This scoring tool can be used in creating a baseline for different systems on a network and can be used for future auditing of those systems. The template file that we created is placed with the other template files that accompany the CIS scoring tool at driveletter\program files\CIS\templates.

Windows Security Scoring Tool v2.1.9

File Scoring Reporting Benchmarks Help

THE CENTER FOR INTERNET SECURITYSM

Computer: OVERALL SCORE:

Scan Time:

Scoring

Select Security Template:

HFNetChk Options

☐ Use Local HFNetChk Database.

☐ Do not evaluate file checksum.
☐ Do not perform registry checks.
☐ Verbose output.

Compliance Verification

Group Policy - Domain Users Only

Service Packs and Hotfixes

Service Pack Level: Score:
 Security Hotfixes Missing: Score:

Account and Audit Policies

Passwords over 90 Days: Score:
 Policy Mismatches: Score:
 Event Log Mismatches: Score:

Security Settings

Restrict Anonymous: Score:
 Security Options Mismatches: Score:

Additional Security Protection

Available Services Mismatches: Score:
 User Rights Mismatches: Score:
 NoLMHash: NTFS: Score:
 Registry and File Permissions: Score:

Reporting

Here is a screen shot of the tool using the template file that was created. The highest score that can be achieved is 10. The score we achieved here was 7.3. Points were missed because the system is missing 5 Security Hotfixes, has 1 Event Log mismatch and 14 Registry and File Permissions mismatches. When you click the Hotfix Report button a web page is displayed.

* SQL SERVER 2000 SP3

Information

All necessary hotfixes have been applied.

* EXCHANGE 2000 SP3

Information

All necessary hotfixes have been applied.

Security Hotfix Download URL's on the Microsoft Support Site:

Q329115 - <http://support.microsoft.com/default.aspx?scid=kb;en-us;Q329115>

Q327522 - <http://support.microsoft.com/default.aspx?scid=kb;en-us;Q327522>

Q816093 - <http://support.microsoft.com/default.aspx?scid=kb;en-us;Q816093>

Q833330 - <http://support.microsoft.com/default.aspx?scid=kb;en-us;Q833330>

Q330994 - <http://support.microsoft.com/default.aspx?scid=kb;en-us;Q330994>

Q320920 - <http://support.microsoft.com/default.aspx?scid=kb;en-us;Q320920>

Q828026 - <http://support.microsoft.com/default.aspx?scid=kb;en-us;Q828026>

**The CIS Scoring Tool uses the Microsoft Network Security
Hotfix Checker (HfNetChk), which is licensed to CIS by Shavlik
Technologies**

<http://www.shavlik.com>

The report also provides the URL links to the individual items. The Hotfixes were downloaded and applied and the tool was rerun with the results below.

© SANS Institute 2004

THE CENTER FOR INTERNET SECURITYSM

Computer: OVERALL SCORE:

Scan Time:

Scoring

SCORE

Select Security Template:

Refresh Template Directory

HFNetChk Options

☐ Use Local HFNetChk Database.

☒ Do not evaluate file checksum.

☐ Do not perform registry checks.

☐ Verbose output.

HFNetChk was developed by
Shavlik Technologies LLC.
For more information go to
<http://www.shavlik.com>

Compliance Verification

INF File Comparison Utility

Group Policy - Domain Users Only

Export Effective Group Policy

Service Packs and Hotfixes

Service Pack Level:	<input type="text" value="4"/>	Score:	<input type="text" value="1.25"/>
Security Hotfixes Missing:	<input type="text" value="0"/>	Score:	<input type="text" value="1.25"/>

Account and Audit Policies

Passwords over 90 Days:	<input type="text" value="0"/>	Score:	<input type="text" value="0.8333"/>
Policy Mismatches:	<input type="text" value="0"/>	Score:	<input type="text" value="0.8333"/>
Event Log Mismatches:	<input type="text" value="0"/>	Score:	<input type="text" value="0.8333"/>

Security Settings

Restrict Anonymous:	<input type="text" value="2"/>	Score:	<input type="text" value="1.25"/>
Security Options Mismatches:	<input type="text" value="0"/>	Score:	<input type="text" value="1.25"/>

Additional Security Protection

Available Services Mismatches:	<input type="text" value="0"/>	Score:	<input type="text" value="0.625"/>
User Rights Mismatches:	<input type="text" value="0"/>	Score:	<input type="text" value="0.625"/>
NoLMHash:	<input type="text"/>		
Local Drives not NTFS:	<input type="text" value="0"/>		
Internet Connection Firewall:	<input type="text"/>		
NetBIOS over TCP/IP:	<input type="text"/>	Score:	<input type="text" value="0.625"/>
Registry and File Permissions:	<input type="text" value="13"/>	Score:	<input type="text" value="0"/>

Results from applying the updates have moved the score to 9.4 just missing the 10 mark because of some mismatches found on Registry and File Permissions. We could continue to pursue but we going to move on.

The next item on the list was to configure the Windows File Protection system. Windows 2000 and XP provide a system that monitors critical system files and their versions. Running as a background process missing or damaged files can be quietly replaced. This process is attempting to maintain a more stable environment for the operating. Microsoft refers to this as a 'self healing' OS and also attempts to eliminate the old 'dll hell syndrome' that was caused by installs replacing system dll's that would then break some functionality. The protected files are kept in a hidden folder located at %systemroot%\system32\dlcache. The system file checker or [sfc.exe](#) is a command line

tool that can be used to manipulate the WFP system. The sfc.exe command line tool has several options. The syntax is shown below:

**SFC [/SCANNOW] [/SCANONCE] [/SCANBOOT] [/REVERT] [/PURGECACHE]
[/CACHESIZE=x]**

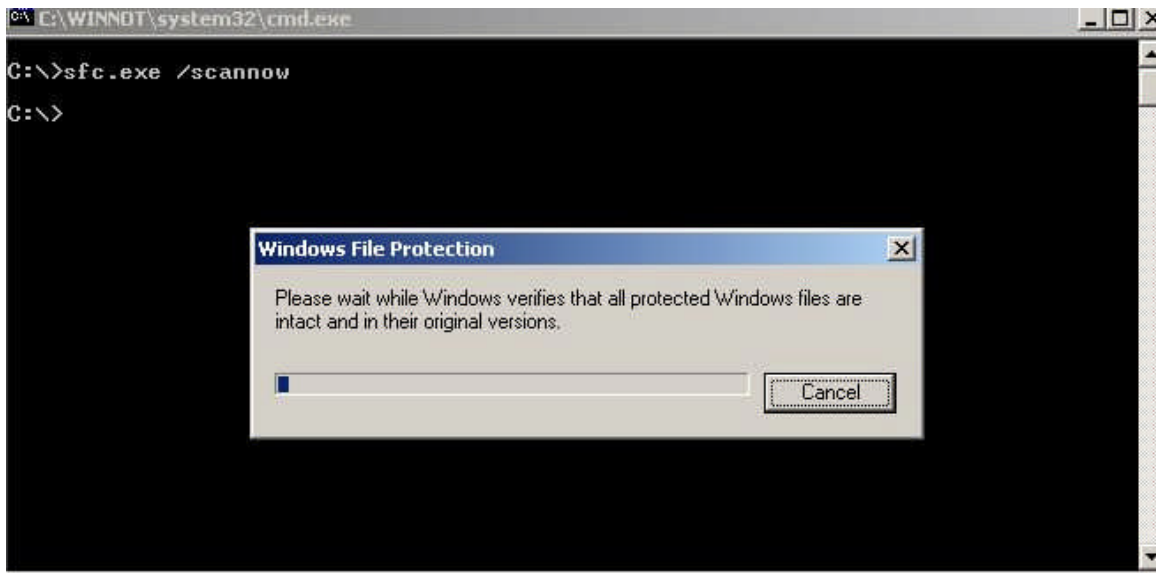
/SCANNOW Scans all protected system files immediately.
/SCANONCE Scans all protected system files once at the next boot.
/SCANBOOT Scans all protected system files at every boot.
/REVERT Return scan to default setting.
/PURGECACHE Purges the file cache.
/CACHESIZE=x Sets the file cache size.

You can control the size of the cache with the /cache=x switch; have the system do a scan on every boot with the /scanboot switch or just on the next boot with the /scanonce switch. Once this process is started with the sfc /scannow command it will evaluate each critical file and may prompt for the Windows 2000 CD or current service pack CD. This can be eliminated by slip streaming the current service pack into the Windows system files (service pack 4 since that is the last service pack that has been applied). The process is fairly simple. 1) Copy the i386 folder from the Windows CD to the system partition. 2) use the update.exe -s: <path to folder> to [slipstream](#)¹⁷ or incorporate the service pack files into the Windows i386 folder. For example if the i386 folder is located on the drive as C:\i386 then the syntax would be update.exe -s:c:\. You do not add the i386 to the path. Once that is done then a change needs to be made to two registry keys –

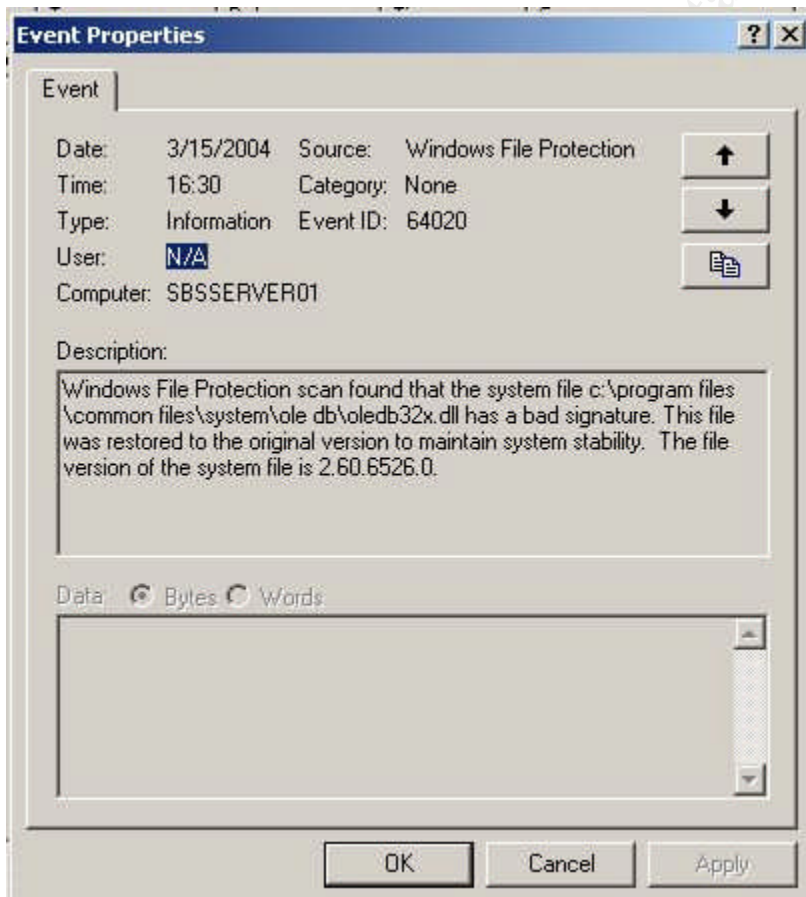
HKLM\Software\Microsoft\Windows\CurrentVersion\Setup\SourcePath

HKLM\Software\Microsoft\WindowsNT\Current\Version\SourcePath.

Based on the example given above the new value would be C:\, again you do not add the i386 to the path value. Once this step is completed the PC needs a reboot and you can then run the sfc.exe tool to populate the dllcache folder.



As you can see above the process is running and it will no longer prompt for needed files.

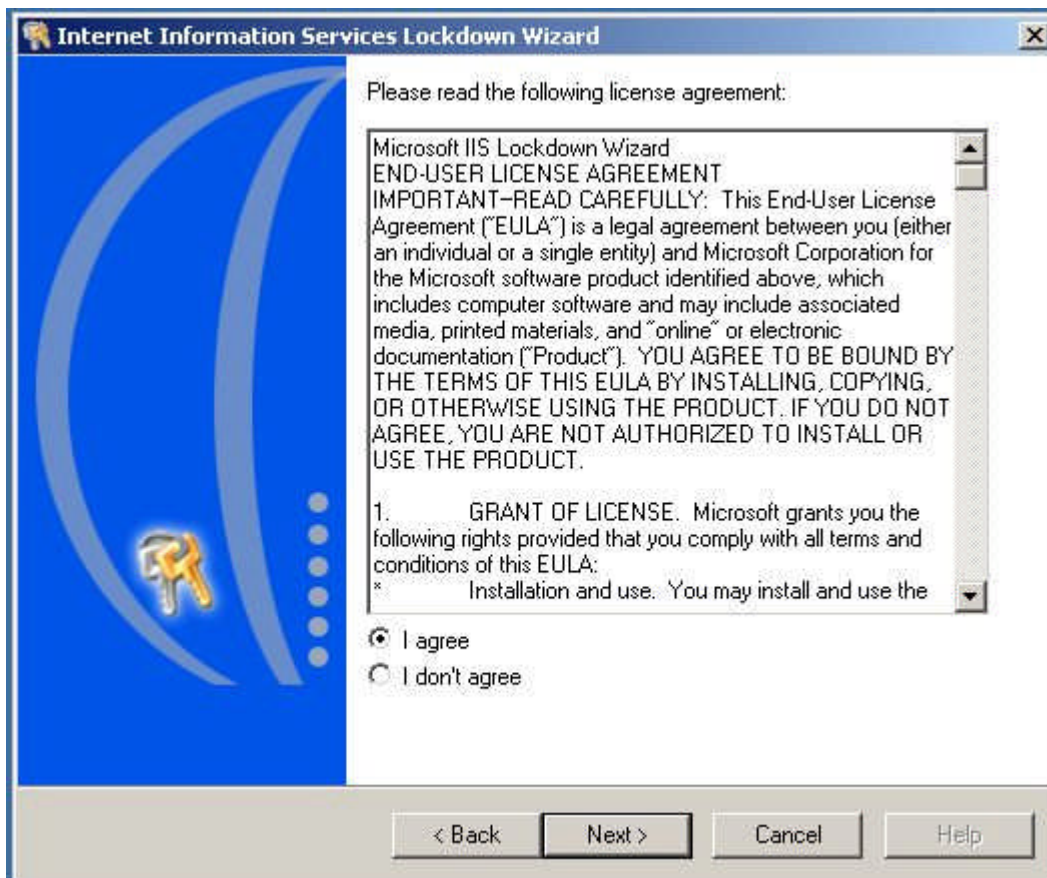


Once system file checker is done you can check the Eventlog and may find an entry like the one above that reflects a file replacement.

Next the Microsoft IIS Lockdown tool can be used to further enhance the security settings on the Small Business server. According to Microsoft “a web server configured with the Express lockdown (one mode of the tool) would be completely protected against known vulnerabilities affecting IIS 4.0 and 5.0 even without the patches for these vulnerabilities.” Of course they also add that it is very important to keep patches and security fixes up to date. The current version 2.1 which can be found [here](#)¹⁸ includes Server roles which are driven by supplied templates and include templates for several of the Microsoft products such as Exchange 5.5, Exchange 2000, Small Business Server 4.5 and 2000, etc. It also includes URLscan integration with customized templates for each supported server role. This allows the administrator to design a custom URLscan filter for the specific server role that is being applied. IIS Lockdown also includes the ability to turn off services such as HTTP, FTP, SMTP, etc. which we have already attended too. The tool can be run in either Express mode or Advanced mode. Advanced mode provides the detail of the changes and the opportunity to tune to your specific situation.

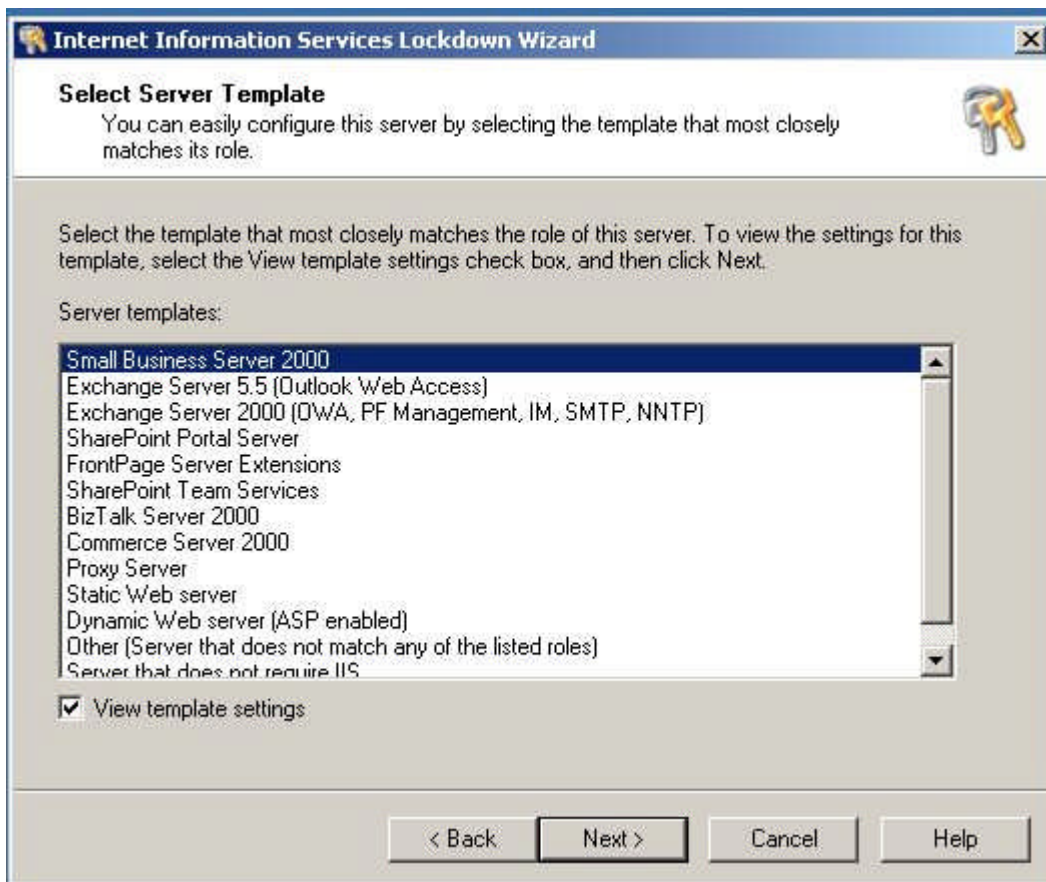


When you start the IIS Lockdown tool you first get a welcome screen which gives a brief description. Click next to continue.



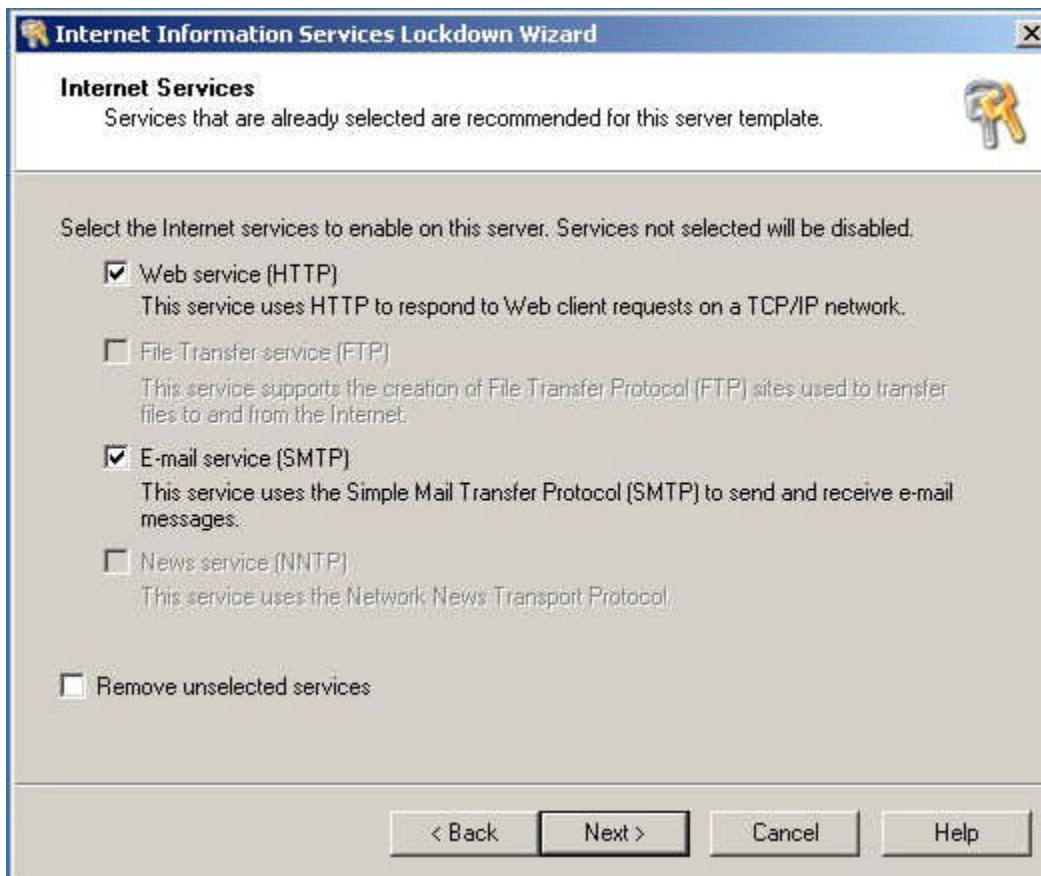
Next is the EULA. Select 'I agree' to continue.

© SANS Institute 2004



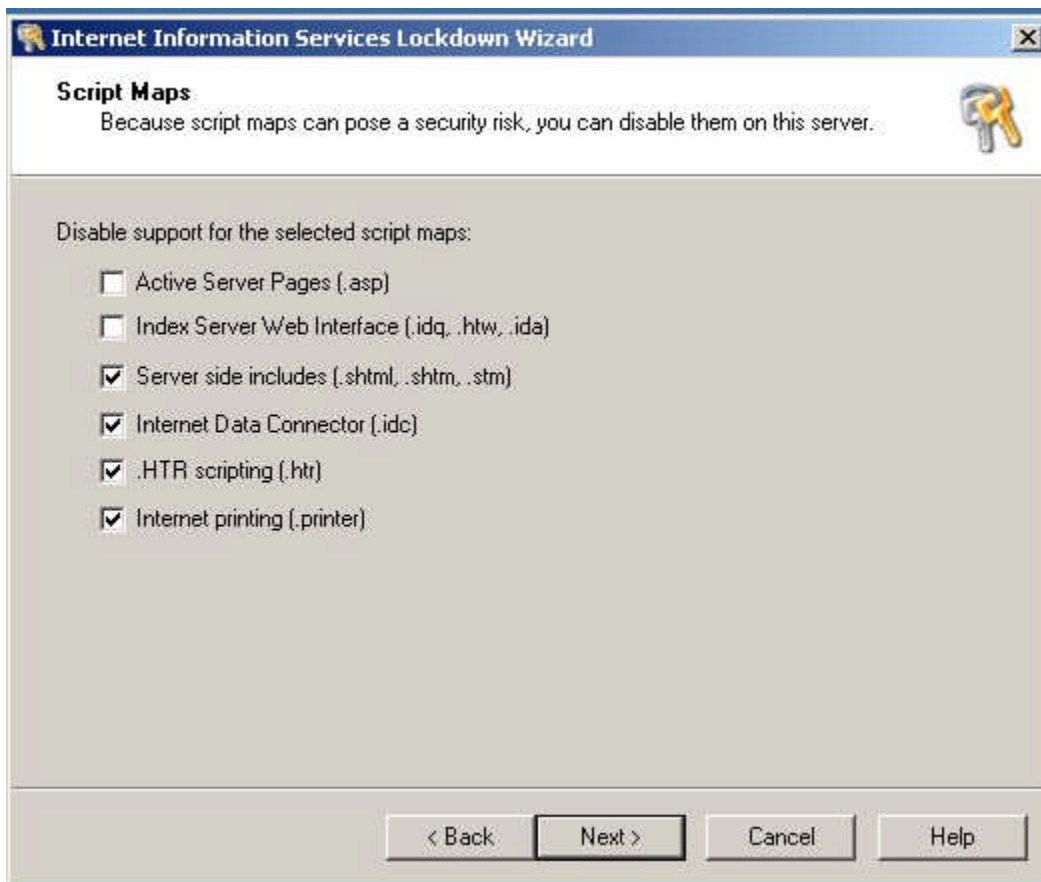
The next screen displays the available templates and a check box if we want to view the settings as we proceed. We select Small Business Server 2000 and click the check box and then Next to continue.

© SANS Institute 2004



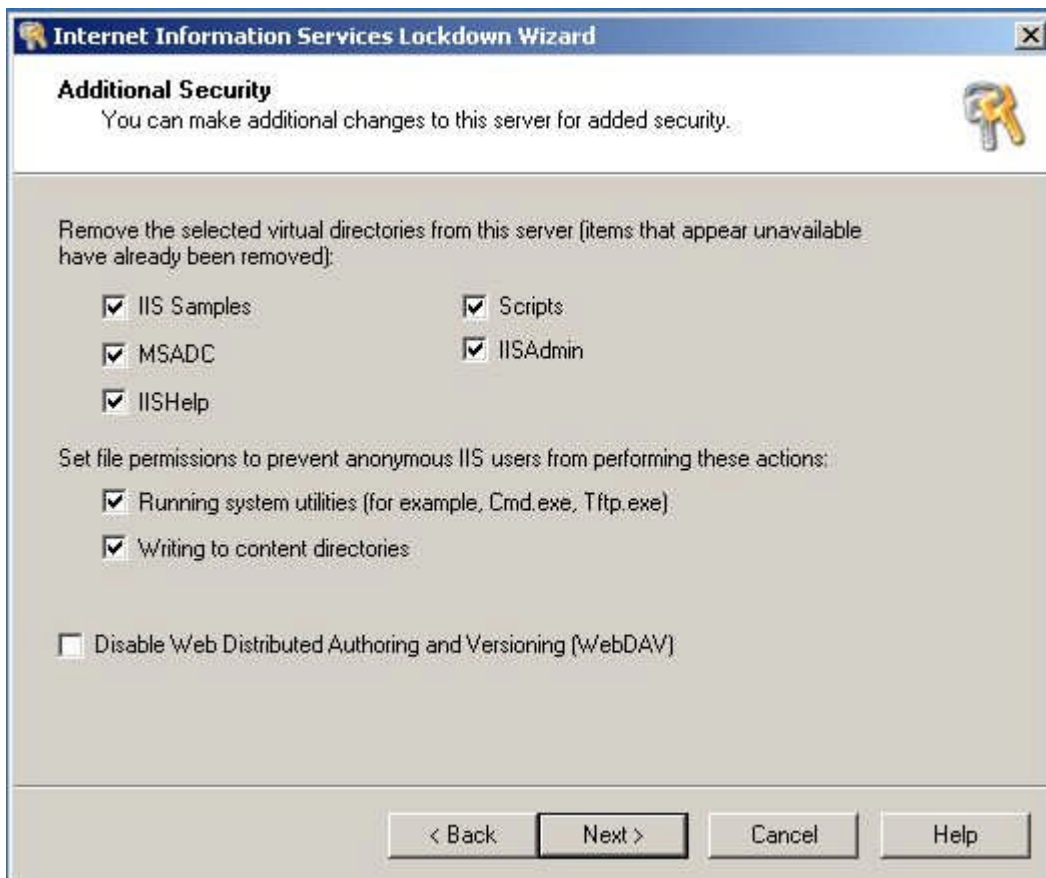
The next screen is where services can be selected to be turned off. Notice the FTP and NNTP services are disabled since we had disabled those earlier.

© SANS Institute 2004



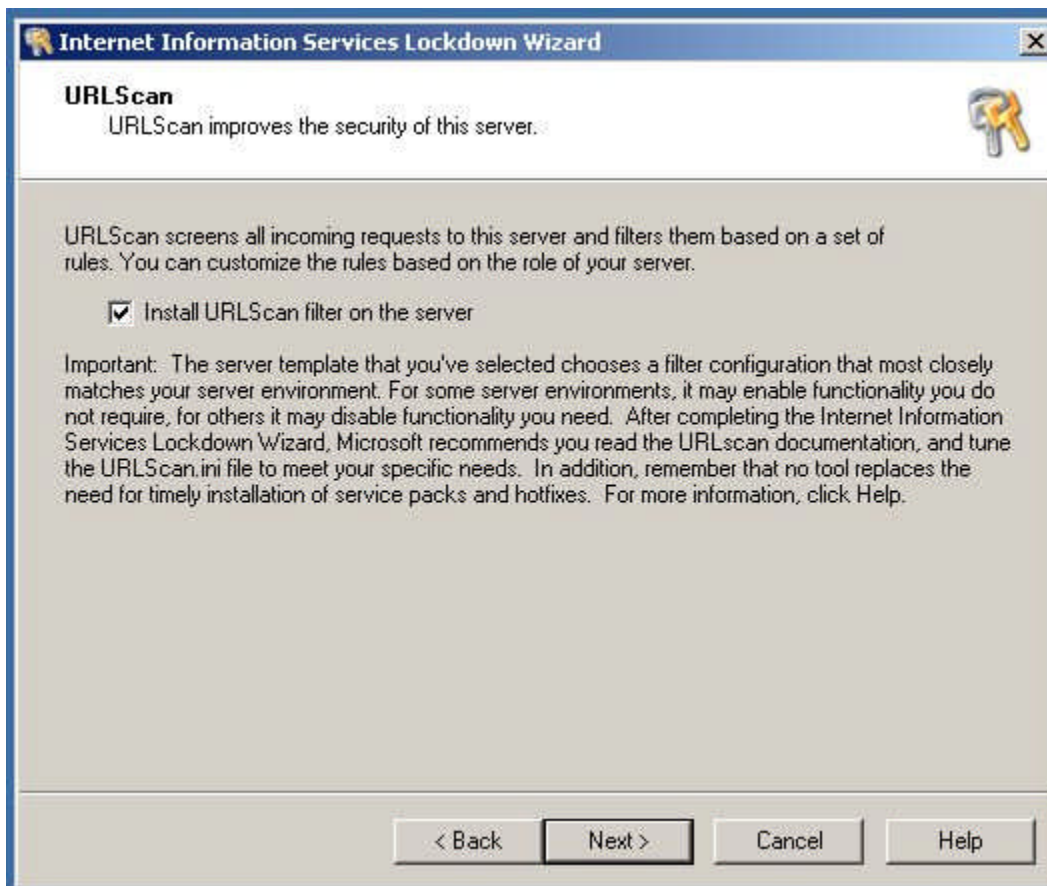
Here is where the ISAPI extension mappings can be selected to be unmapped so they will not be available for potential exploits. On a Small Business Server if Outlook Web Access is going to be made available then the Active Server Pages check box needs to be unchecked as it uses these for functionality. The check boxes above reflect the default settings for the Small Business Server template being applied.

© SANS Institute



The additional security screen will remove virtual directories that were installed by default that are not needed for functionality and could possibly be used for exploits. The screen also reflects changes to permissions on files such as cmd.exe and tftp.exe which in the past have been used by hackers to exploit a web server. Also notice that the WebDAV check box is cleared. Exchange 2000 components use Web Distributed Authoring and Versioning (WebDAV) verbs that are normally disabled by the IIS Lockdown wizard but changes its default behavior here because the Small Business Server template was selected which includes Exchange 2000 that needs these enabled to function correctly. More information about this can be found in Microsoft's Knowledge Base article [Q309508](http://support.microsoft.com/kb/q309508).

© SANS



The URLScan filter is installed by default which can protect the web server against known vulnerabilities like directory traversal, double encoding exploit, etc. The filter is controlled by the urlscan.ini file located at %systemroot%\System32\inet_srv\urlscan\ and may need to be reviewed for specific tweaking.

```
[options]
UseAllowVerbs=1           ; if 1, use [Allowverbs] section, else use [Denyverbs] section
UseAllowExtensions=0      ; if 1, use [AllowExtensions] section, else use [DenyExtensions] s
NormalizeUrlBeforeScan=1  ; if 1, canonicalize URL before processing
VerifyNormalization=1     ; if 1, canonicalize URL twice and reject request if a change occur
AllowHighBitCharacters=1  ; if 1, allow high bit (ie. UTF8 or MBCS) characters in URL
AllowDotInPath=1          ; if 1, allow dots that are not file extensions
RemoveServerHeader=0      ; if 1, remove "Server" header from response
EnableLogging=1           ; if 1, log URLScan activity
PerProcessLogging=0       ; if 1, the urlscan.log filename will contain a PID (ie. urlscan.1
AllowLateScanning=0       ; if 1, then UrlScan will load as a low priority filter.
PerDayLogging=1           ; if 1, UrlScan will produce a new log each day with activity in tl
RejectResponseUrl=        ; UrlScan will send rejected requests to the URL specified here. D
UseFastPathReject=0       ; If 1, then UrlScan will not use the RejectResponseUrl or allow I

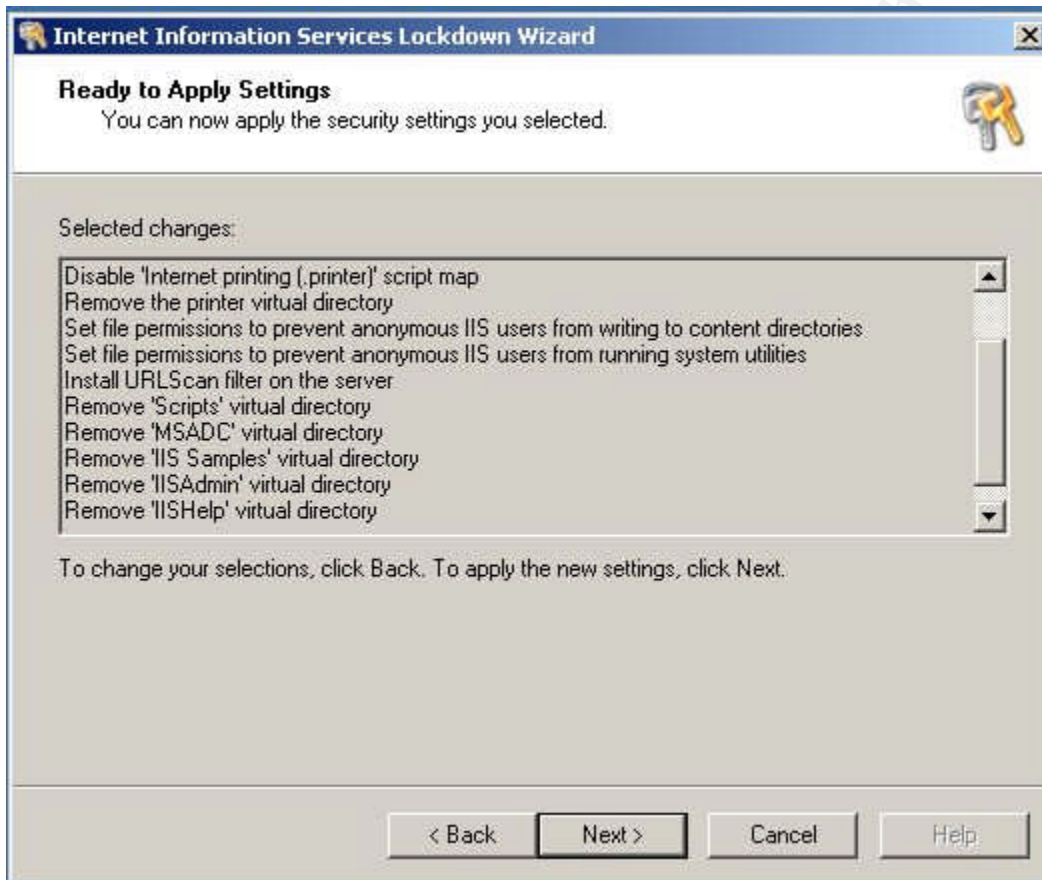
; If RemoveServerHeader is 0, then AlternateServerName can be
; used to specify a replacement for IIS's built in 'Server' header
AlternateServerName=Apache 1.3.32

[Allowverbs]
```

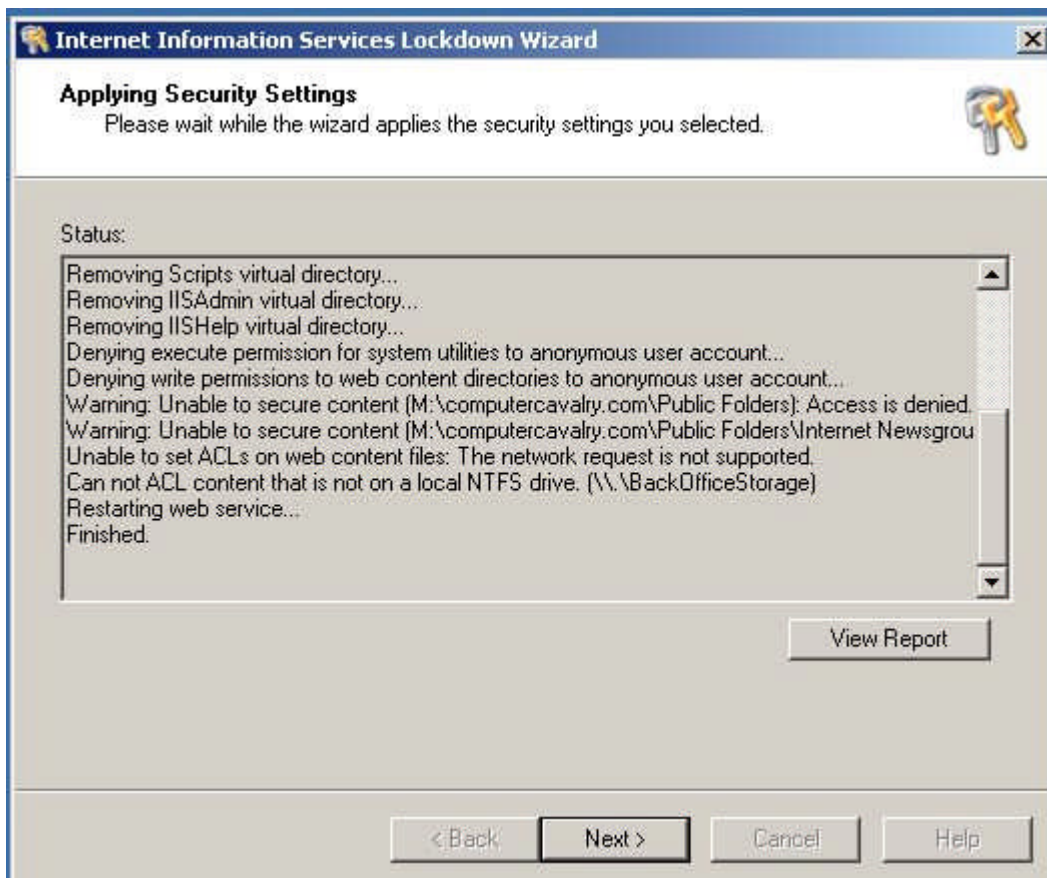
The ini file is set up with sections similar to other ini files. The first section is the [options] section and sets the precedence of other sections. For example if the UseAllowVerbs is set to 1 the the [AllowVerbs] section is used and only the verbs listed will be allowed. Or if the UseAllowVerbs is set to 0 then the [DenyVerbs] section is used and all verbs will be allowed except those that are specifically listed here. One interesting setting is the AlternateServerName=. You can actually get the HTTP server to return

what ever is listed here. I have set this value to Apache 1.3.32. This goes back to the banner section that was described earlier that uses Security by Obscurity. This is not going to make the server more secure but might confuse some that are searching for perhaps a specific platform or version of server to exploit.

More information on the URLscan filter can be found at Microsoft's website [here](#)¹⁹.



The IIS Lockdown wizard displays all the changes that are going to be made. Click next to continue.



Here we can see the wizard has completed the process. A report is generated and can be viewed and 2 logs are created. One is located at %systemroot%\system32\inetssrv\oblt-log.log with uninstall information and the other is located at %systemroot%\system32\inetssrv\oblt-rep.log. This first log is very important in that it will be needed if a decision is made to re-run the tool which would allow you to undo the changes that were made, if the log is removed or damaged you will no longer be able to undo those changes.

The next area for discussion is socket pooling. Socket Pooling is described in ISA Server and Beyond²⁰ as “an IIS feature that allows IIS services to listen on all interfaces, regardless of the IP address you set the service to listen on.” According to Microsoft’s Q article [Q310155](#)²¹, this was a feature added to IIS 5.0 so that multiple sites hosted on the same server that use different IP addresses but the same port could reduce the number of resources that IIS would consume as a matter of efficiency. Socket pooling on a unihomed PC is considered a good thing but can cause potential problems particularly with what is called port contention if enabled on a multihomed server like the Small Business Server in this scenario. Port contention happens when the same service (i.e. HTTP, SMTP, etc.) is running on the Small Business Server (ISA server) and you try and publish that same service on a server located on the internal network. Small Business Server (ISA server) will not allow that to happen. Another problem is that with socket pooling enabled you have to use packet filters if you want to expose any services running locally on the Small Business Server to the outside world, you are not able to publish

those services. Packet filters are not bad, in some camps they are just considered not quite as secure as publishing since a packet filter is static, meaning it is a service that is always listening on the public interface of the Small Business Server versus a published service that will dynamically become available for a request and then be closed once the connection has been terminated. Packet filters also only look at the IP header while Web publishing can expose the traffic to an application filter which looks at the content.

Socket pooling can be observed by opening a shell window and using the netstat -an command.

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:25	0.0.0.0:0	LISTENING
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING
TCP	0.0.0.0:88	0.0.0.0:0	LISTENING
TCP	0.0.0.0:110	0.0.0.0:0	LISTENING
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:143	0.0.0.0:0	LISTENING
TCP	0.0.0.0:389	0.0.0.0:0	LISTENING
TCP	0.0.0.0:443	0.0.0.0:0	LISTENING
TCP	0.0.0.0:464	0.0.0.0:0	LISTENING
TCP	0.0.0.0:593	0.0.0.0:0	LISTENING
TCP	0.0.0.0:636	0.0.0.0:0	LISTENING
TCP	0.0.0.0:691	0.0.0.0:0	LISTENING
TCP	0.0.0.0:993	0.0.0.0:0	LISTENING
TCP	0.0.0.0:995	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1026	0.0.0.0:0	LISTENING

Here is some output from that command. Notice under the Local Address column the addresses listed as 0.0.0.0:tcpport. This means that these specific services are listening on all available addresses.

E:\ResourceTools>netstat -an find ":25"			
TCP	0.0.0.0:25	0.0.0.0:0	LISTENING
E:\ResourceTools>netstat -an find ":80"			
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING
TCP	127.0.0.1:8080	0.0.0.0:0	LISTENING
TCP	192.168.101.10:8080	0.0.0.0:0	LISTENING
E:\ResourceTools>netstat -an find ":110"			
TCP	0.0.0.0:110	0.0.0.0:0	LISTENING
E:\ResourceTools>netstat -an find ":143"			
TCP	0.0.0.0:143	0.0.0.0:0	LISTENING

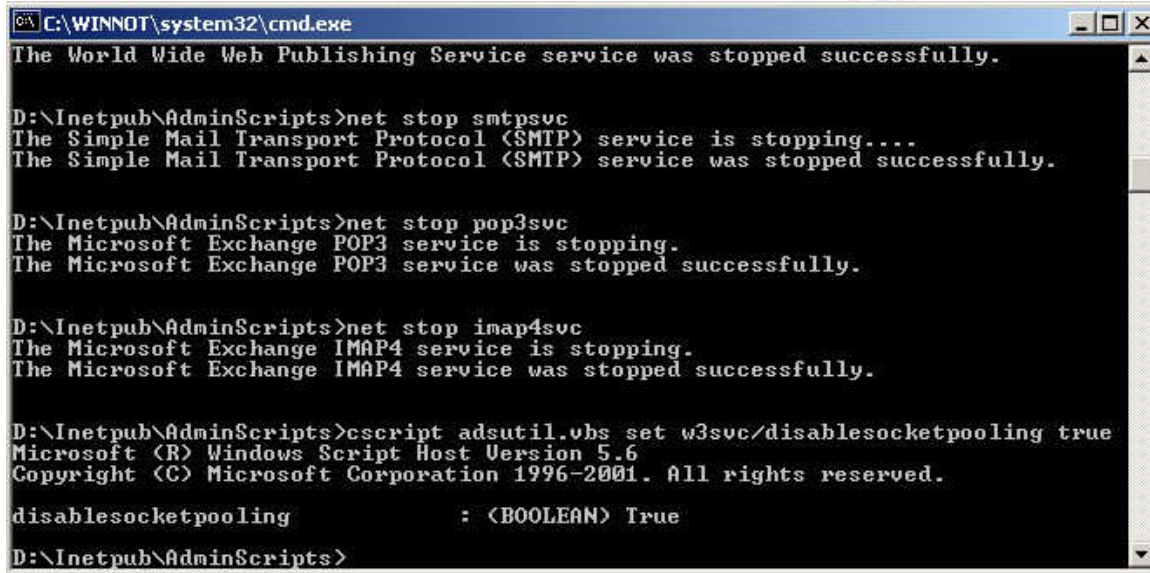
Here is a list of services that use socket pooling from IIS and Exchange. The complete list would be HTTP, HTTPS, FTP, SMTP, NNTP, POP3 and IMAP4. The utilities that are needed to disable socket pooling are; adsutil.vbs located in the \Inetpub\Adminscripts folder and the mdutil.exe which can be found in the i386 folder on the Windows 2000 CD-ROM or on the i386 folder on the PC if you have completed the slipstream process mentioned earlier. The mdutil.exe file will need to be uncompressed by opening a command window where the compressed file is located and typing

expand mdutil.ex_mdutil.exe.

Next the services need to be stopped. This can be done from the same command window using the net stop command.

```
C:\>net stop w3svc
C:\>net stop msftpsvc (if not already disabled)
C:\>net stop nntpsvc (if not already disabled)
C:\>net stop smtpsvc
C:\>net stop pop3svc
C:\>net stop imap4svc
```

To disable the www services go to the \Inetpub\AdminScripts folder and type
D:\Inetpub\Adminscripts>cscript adsutil.vbs set w3svc/disablesocketpooling true



```
C:\WINNOT\system32\cmd.exe
The World Wide Web Publishing Service service was stopped successfully.

D:\Inetpub\AdminScripts>net stop smtpsvc
The Simple Mail Transport Protocol (SMTP) service is stopping...
The Simple Mail Transport Protocol (SMTP) service was stopped successfully.

D:\Inetpub\AdminScripts>net stop pop3svc
The Microsoft Exchange POP3 service is stopping.
The Microsoft Exchange POP3 service was stopped successfully.

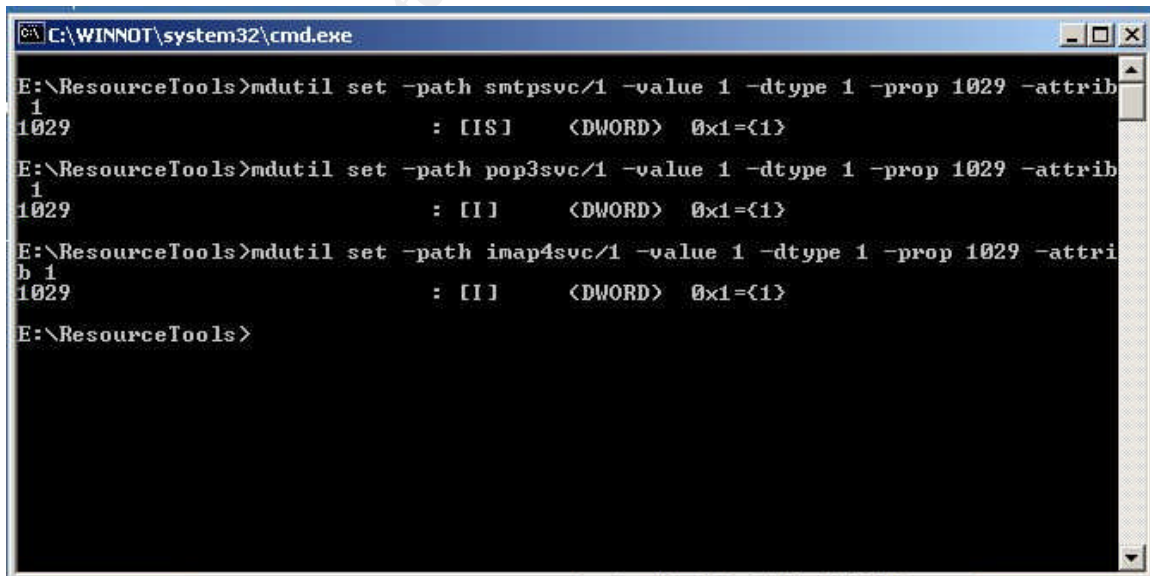
D:\Inetpub\AdminScripts>net stop imap4svc
The Microsoft Exchange IMAP4 service is stopping.
The Microsoft Exchange IMAP4 service was stopped successfully.

D:\Inetpub\AdminScripts>cscript adsutil.vbs set w3svc/disablesocketpooling true
Microsoft (R) Windows Script Host Version 5.6
Copyright (C) Microsoft Corporation 1996-2001. All rights reserved.

disablesocketpooling           : <BOOLEAN> True

D:\Inetpub\AdminScripts>
```

Next place the focus of the command window where the mdutil.exe file is located.



```
C:\WINNOT\system32\cmd.exe

E:\ResourceTools>mdutil set -path smtpsvc/1 -value 1 -dtype 1 -prop 1029 -attrib
1
1029                        : [IS]      <DWORD>  0x1={1}

E:\ResourceTools>mdutil set -path pop3svc/1 -value 1 -dtype 1 -prop 1029 -attrib
1
1029                        : [I]       <DWORD>  0x1={1}

E:\ResourceTools>mdutil set -path imap4svc/1 -value 1 -dtype 1 -prop 1029 -attrib
b 1
1029                        : [I]       <DWORD>  0x1={1}

E:\ResourceTools>
```

At the prompt type:

```
mdutil set -path smtpsvc/1 -value 1 -dtype 1 -prop 1029 -attrib 1
```

You should see output like the screen shot above. Repeat the process for the msftpsvc, nntpsvc, pop3svc, imap4svc. If you have multiple instances of any of these services running you will need to run this command for each instance. If you are not sure if you have multiple instances you can use the mdutil.exe utility to find out.

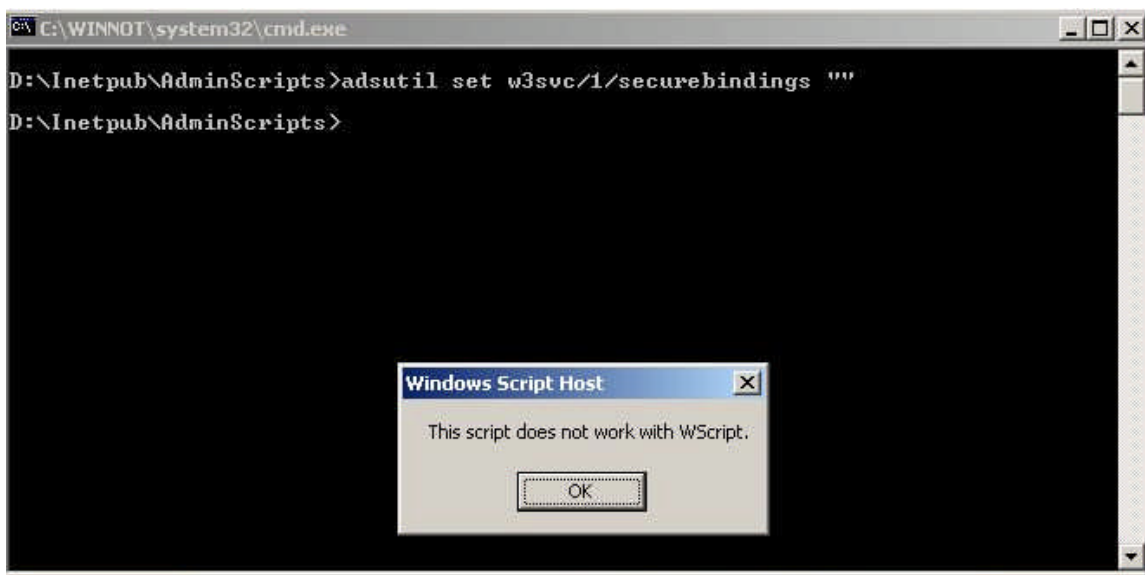
```
C:\WINNOT\system32\cmd.exe
E:\ResourceTools>mdutil.exe enum -path:smtpsvc
```

```
C:\WINNOT\system32\cmd.exe
Key Type
AnonymousPwd
36908
com"
36935
com"
36987
n\phatq.dll"
36950
36953
49875
36970
00 00 80 44 00 00 80 01 0
01 00 00 00 02 00 00 00
0 00 00 00 00 00 00 00 00
LogFileDirectory
s"
36919
36920
61536
B8A1404129)"
[/smtpsvc/Info]
[/smtpsvc/1]
E:\ResourceTools>
```

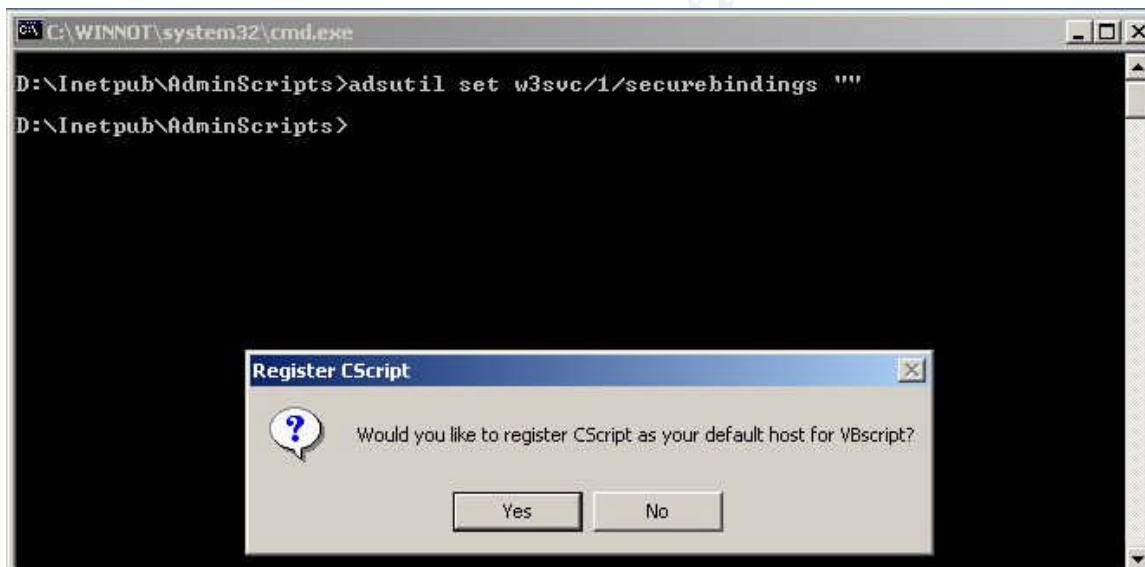
In the first screen shot above we are enumerating the SMTP service to discover if there are multiple instances. The second screen shot reflects only one instance of the SMTP service on this system seen in the last line of the output '[/smtpsvc/1]'. If there were more instances there would be additional lines such as smtpsvc/2, smtpsvc/3, etc.

The last service to disable socket pooling for is the secure web service (SSL listener). Go to the \inetpub\Adminscripts folder and run:

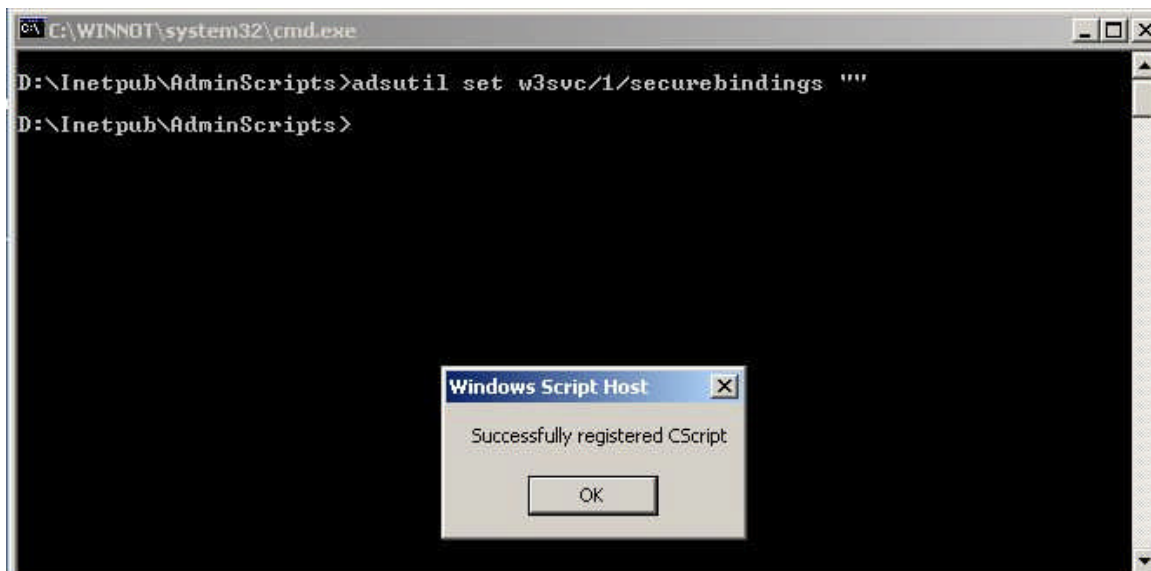
Adsutil set w3svc/1/securebindings ""



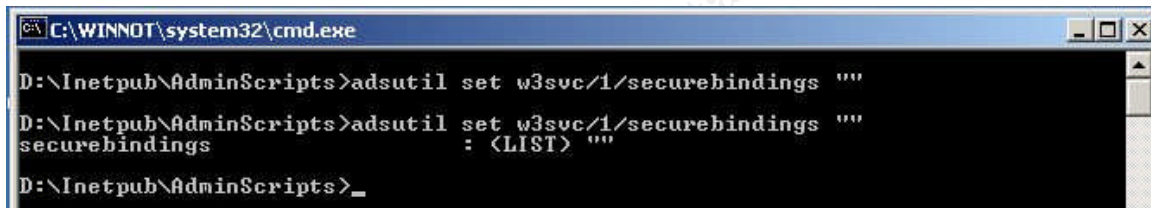
You will get a prompt that states the script does not work with WScript. Click OK.



The next box will ask if you would like to register CScript as your default host for VBScript? Click Yes.



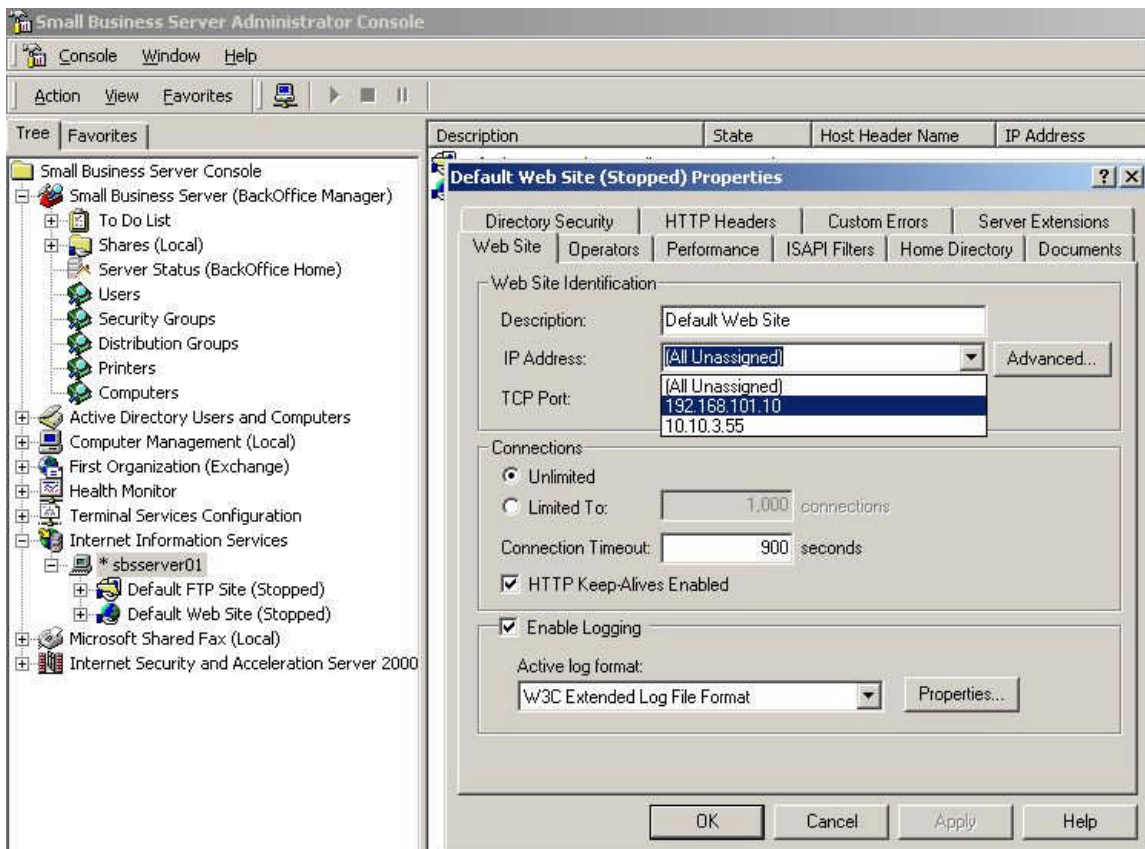
You should then see a successfully registered box. Click OK and run the script again.



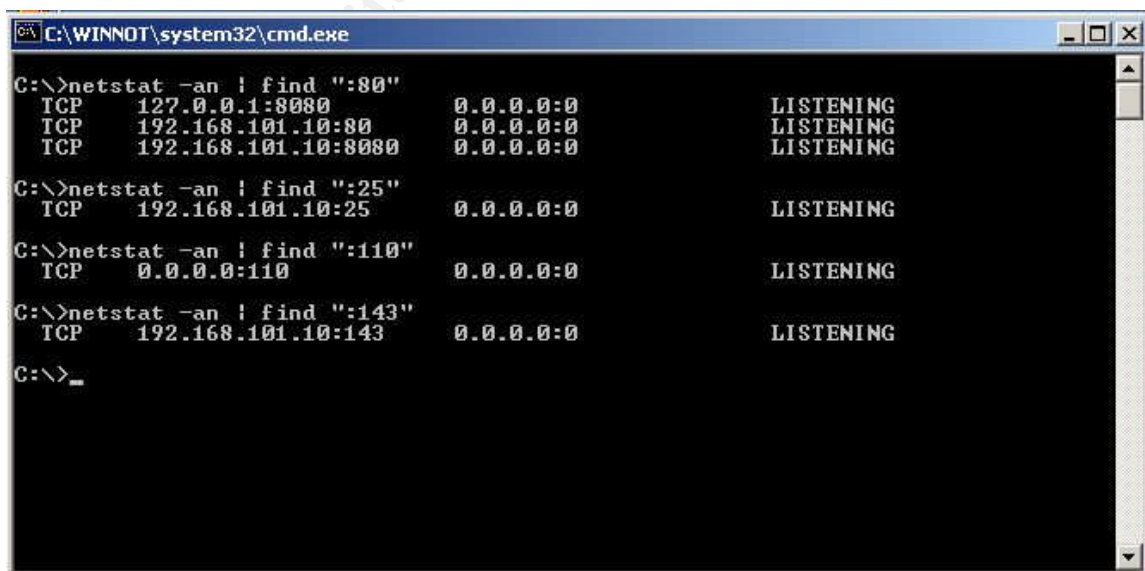
The script should run successfully with the output like above.

Now that socket pooling has been disabled the services are still listening on all available addresses because that is their default configuration.

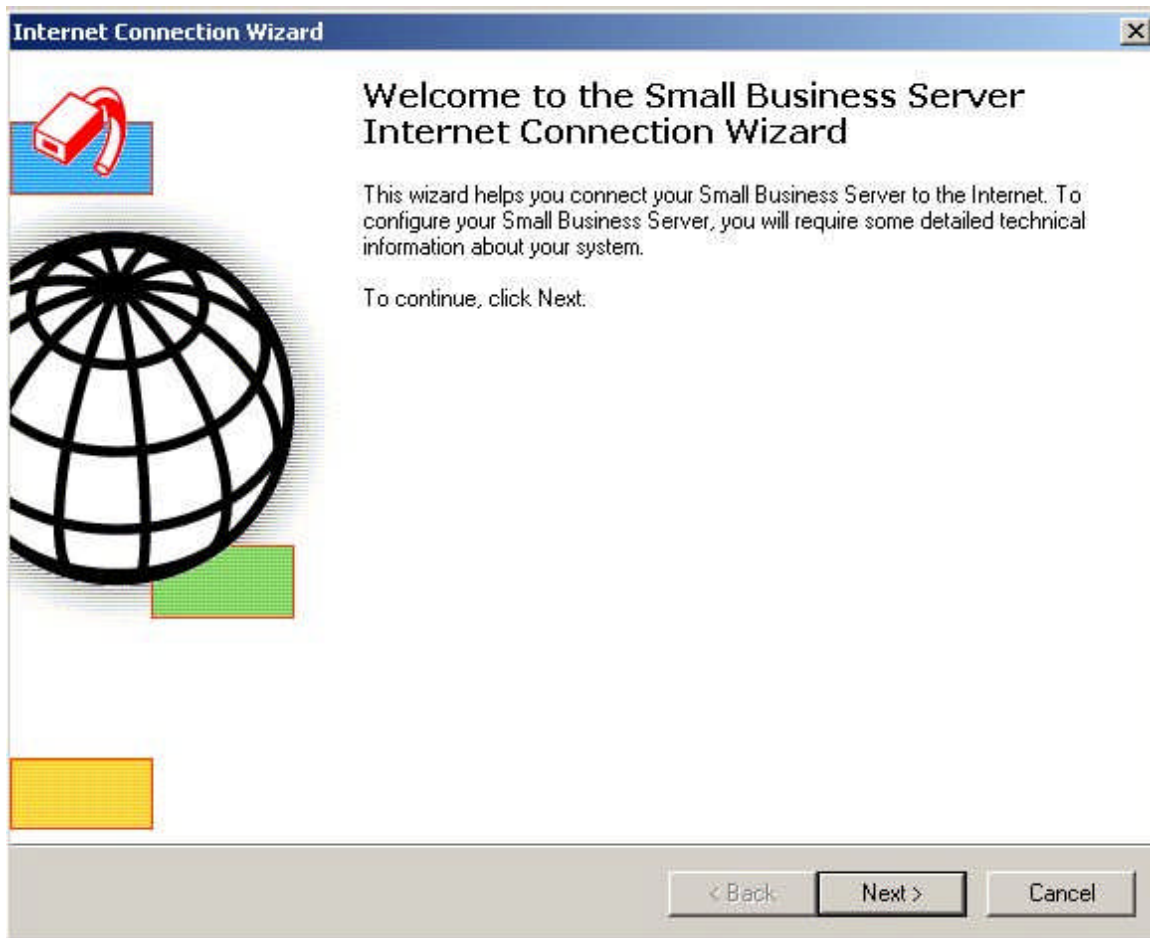
© SANS Institute 2004



To change this you will need to go to the Internet Information Services, right click on the default web site and click properties. Use the drop down box and change the IP address setting from "All Unassigned" to the internal address of the Small Business server. This will need to be done for all the services. Use the Exchange System Manager to make changes to the SMTP, NNTP, POP3 and IMAP4 protocols. Once this step has been completed the services can be restarted using a net start <service name> for each service.

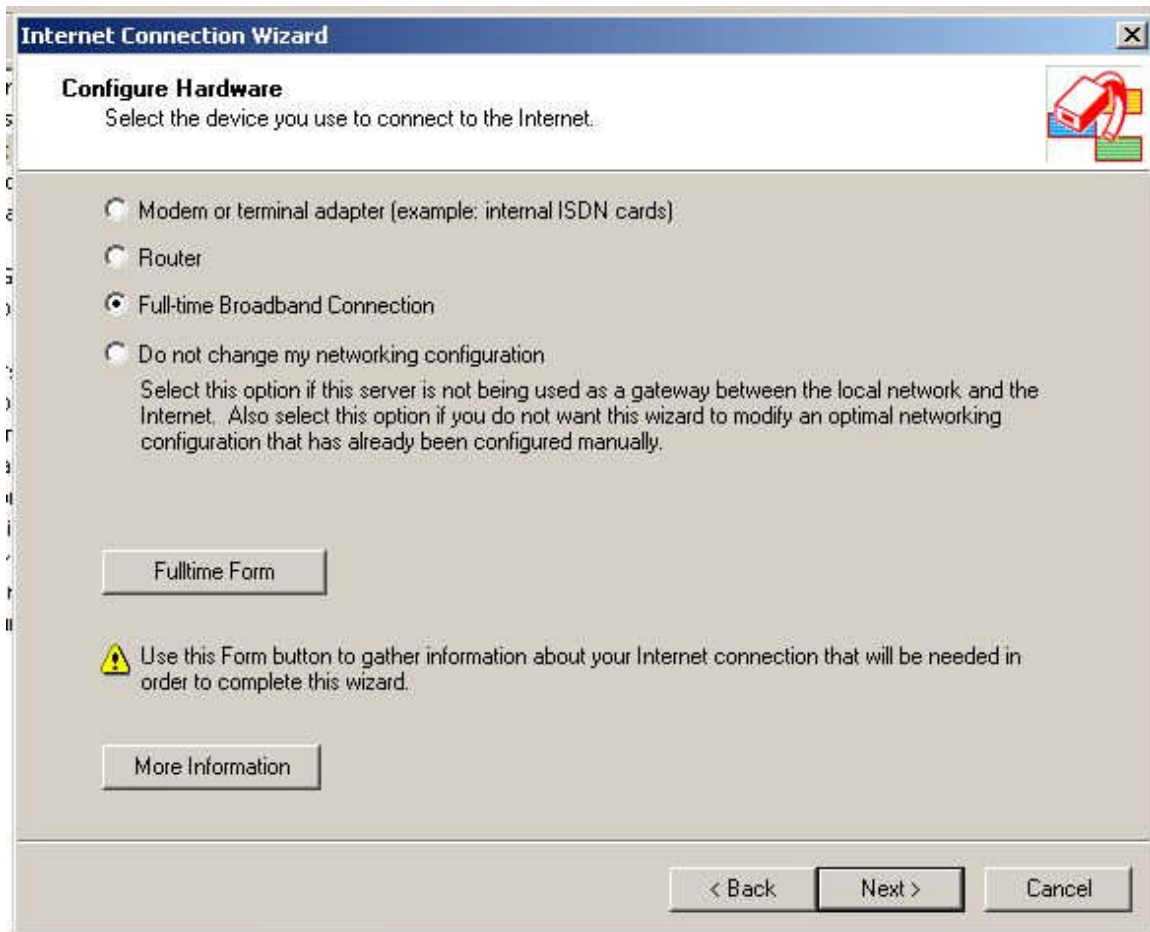


You can then check your work using the same netstat command again. As you can see in the screen shot above the services are now listed on the internal address of the Small Business Server...well almost...just goes to show you should always verify your work!



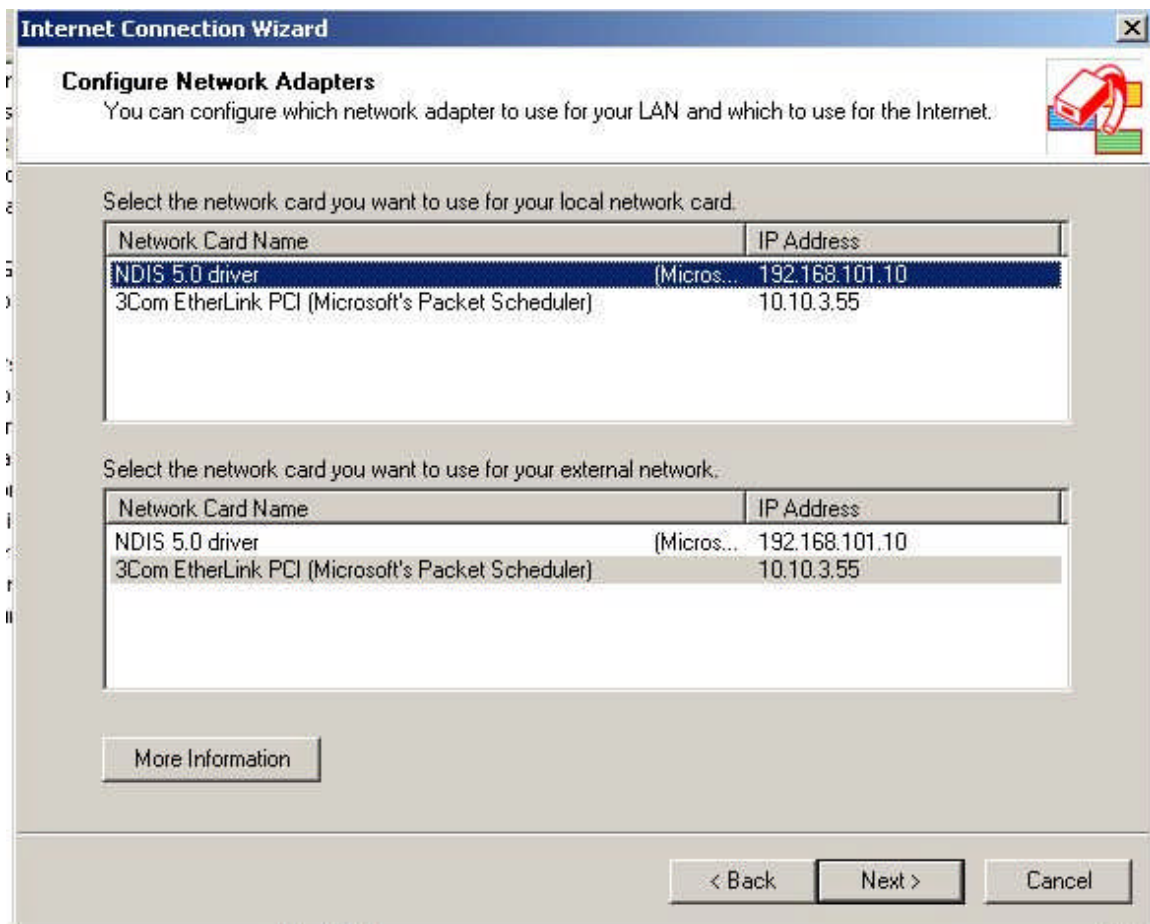
Most tasks on the Small Business Server can be accomplished using Wizards, including adding users, adding a printer, add client licenses, configure remote access, etc. An item to note here is that during the SBS install on a multihomed PC the process disables any network adapters present except the one defined as the internal NIC. Before proceeding we would verify that the public NIC was enabled. Next we run the Internet Connection Wizard to connect the Small Business Server to the Internet.

© SANS



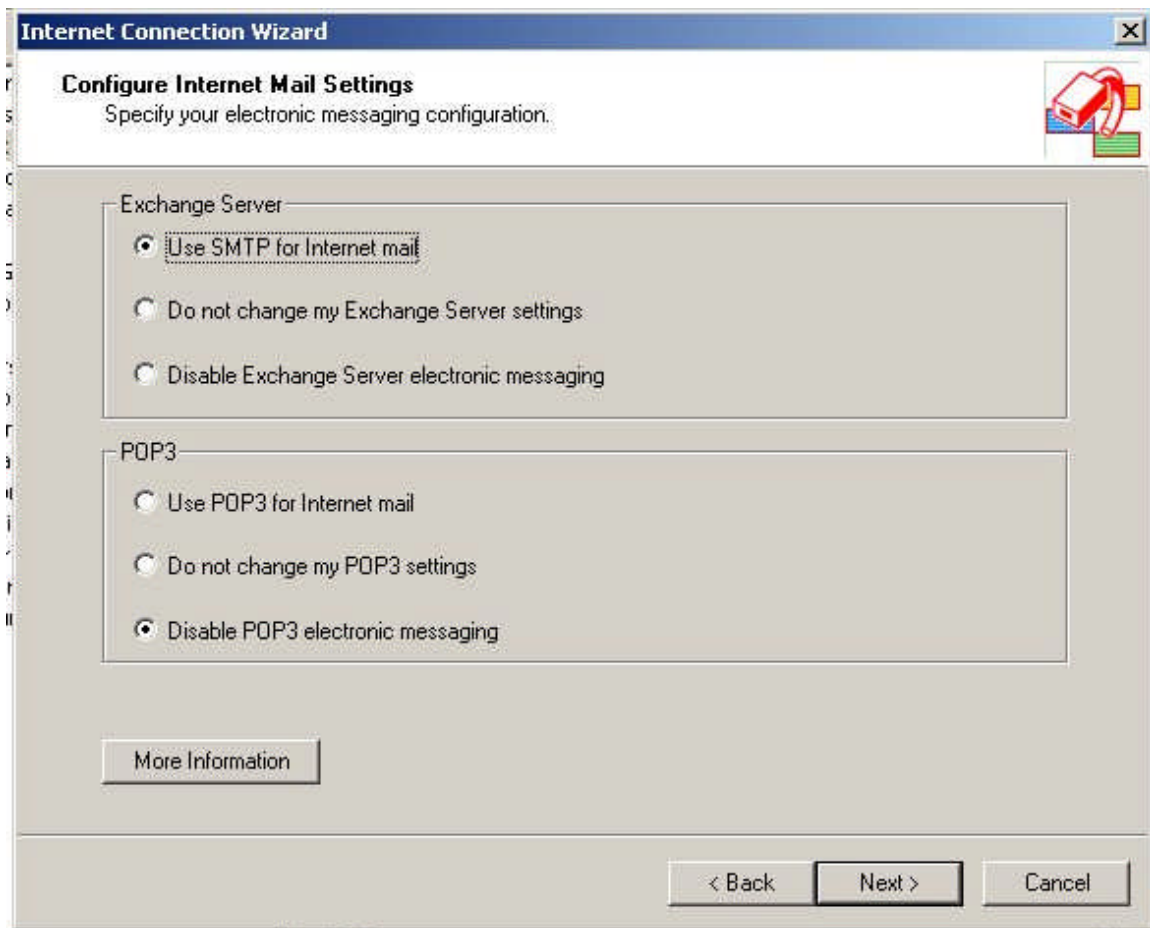
Select the type of connection to be used. Since this server will be connected to a cable modem we select the 'Full-time Broadband Connection' option and click Next.

© SANS Institute



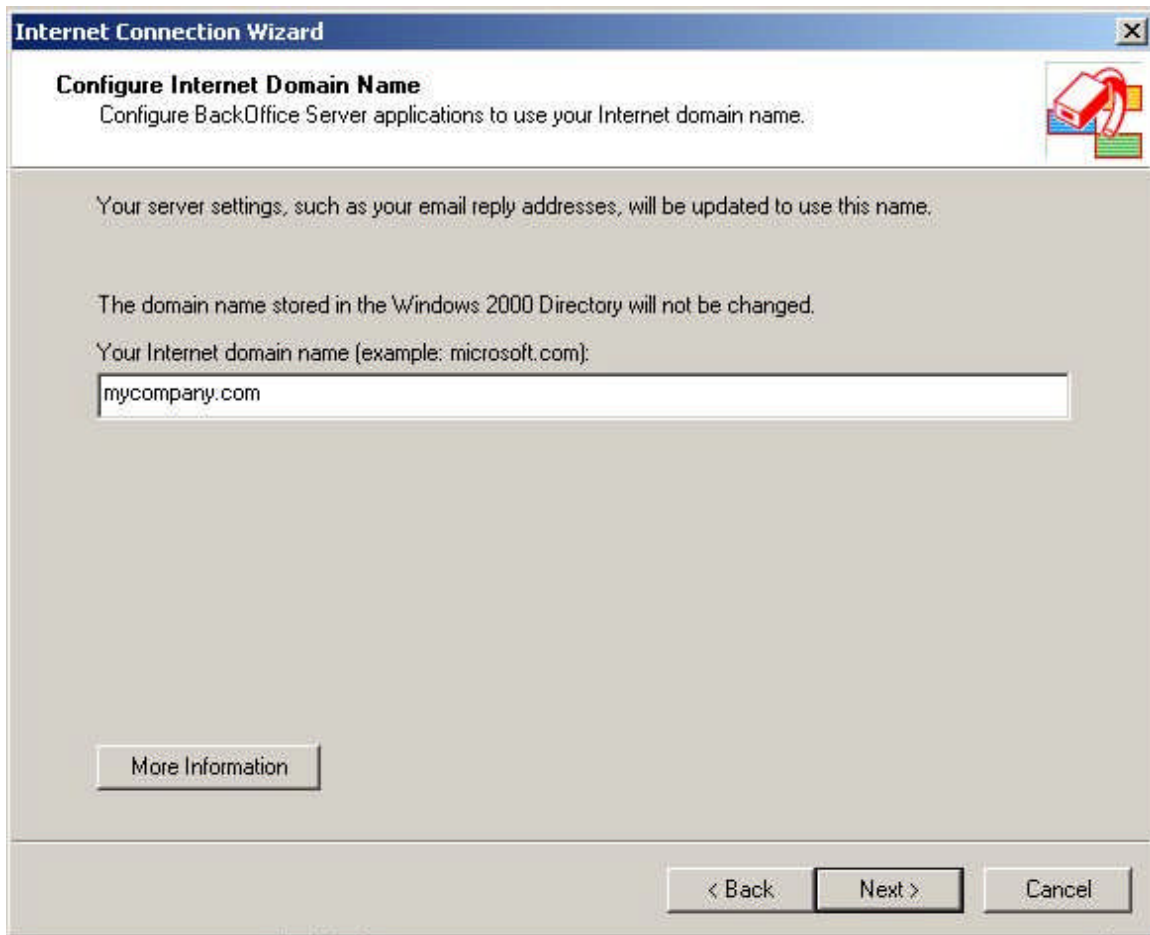
Next the local area network card and external network card are selected. The next screen is where the ISP info is entered including gateway, DNS servers, etc. for the public interface. Since this has already been set up we just click Next to continue.

© SANS Institute



Here we just use the defaults that are provided since we will be doing SMTP mail and not POP3.

© SANS Institute 2004



The FQDN of the company is entered here. Since we had used the FQDN of mycompany.local when we installed Active Directory this is changed here to mycompany.com which is the actual registered domain name of our company. Our ISP is hosting our public name and has a MX record pointing to the public interface of the Small Business Server.

© SANS Institute

Internet Connection Wizard

Configure SMTP Server Address
Enter the name of the ISP SMTP server.

☐ Forward all mail to host. You will forward (queue) all SMTP mail to a mail server at your ISP. Your ISP will provide you with the name or IP address of this mail server.

Mail server:

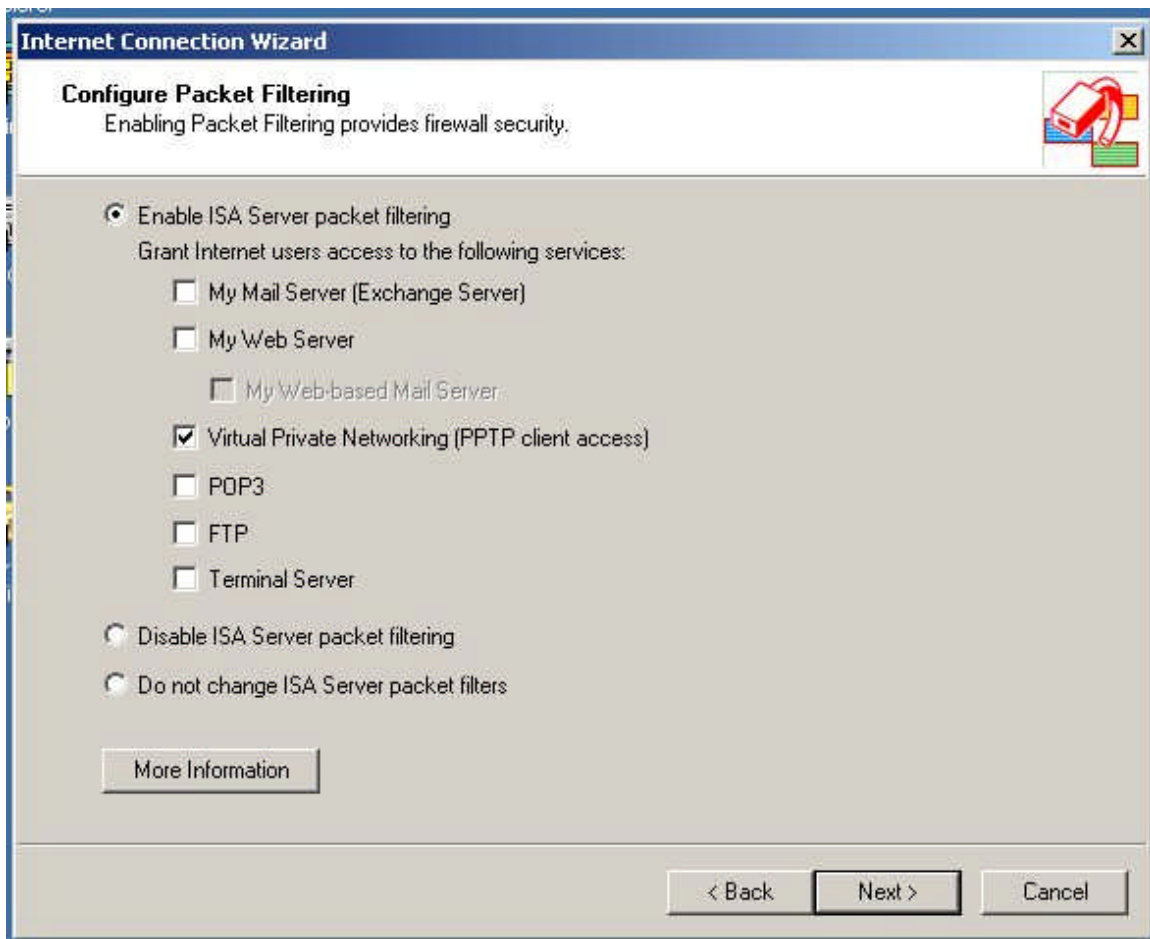
☒ Use domain name system (DNS) for mail delivery.

[More Information](#)

< Back Next > Cancel

In this specific scenario there is no email gateway or smart host, the Exchange Server on the SBS 2000 will be accepting mail and sending mail on behalf of our domain.

© SANS Institute



Here we are configuring packet filters to be created that will allow remote clients to initiate a VPN connection to the server. Since we have disabled socket pooling on the Small Business Server 2000 we will use publishing rules to publish the mail services and Terminal Services for remote management.



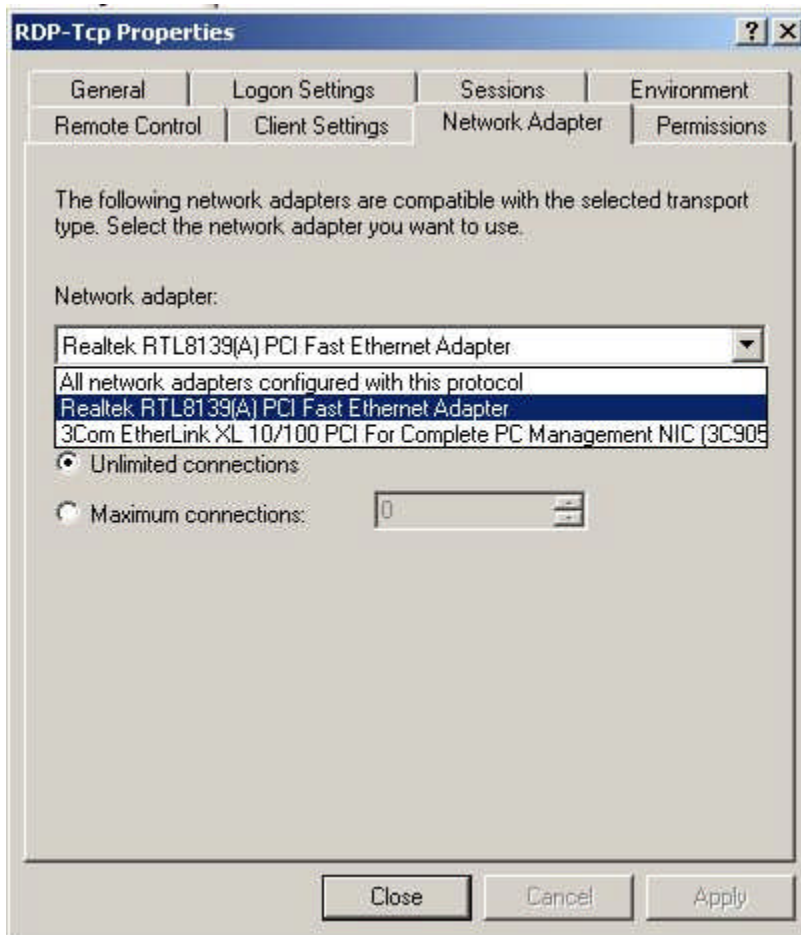
You are prompted that existing filters will be disabled. Click OK to continue. A summary is presented which can be copied and pasted into a document and printed out for record keeping purposes.



Finally a Status window provides feedback as each task is completed.

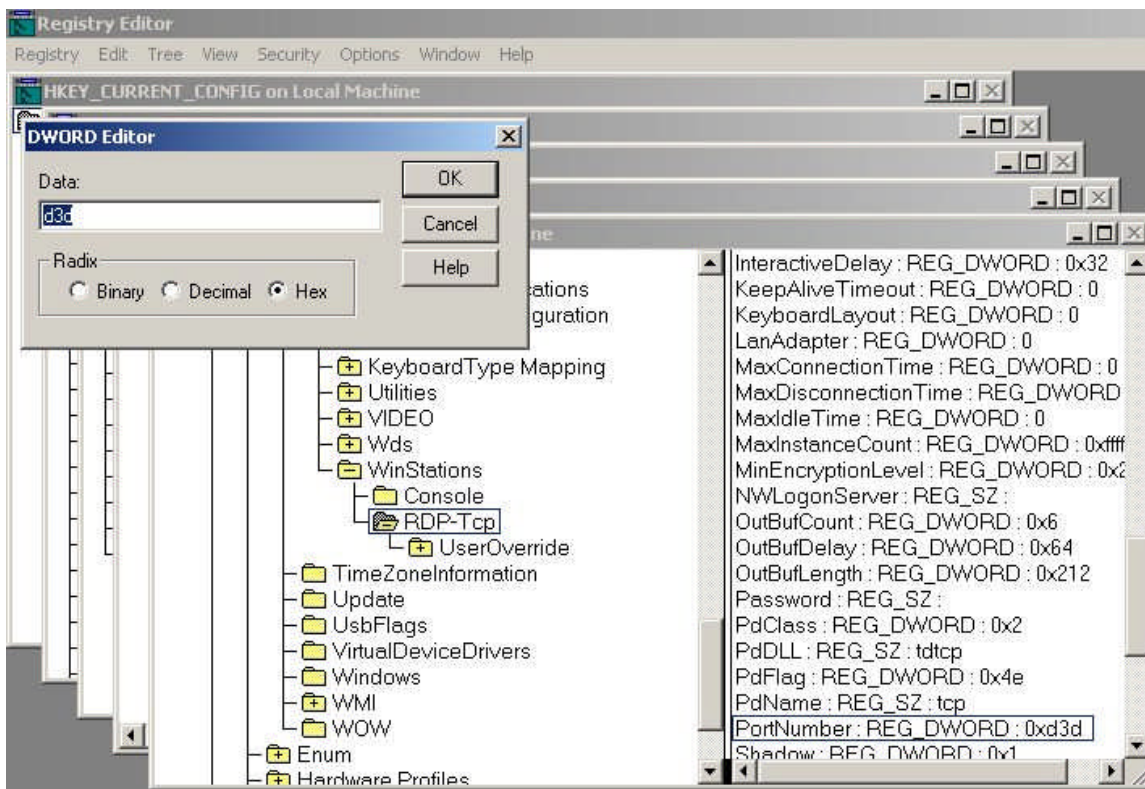
Terminal Services runs on Windows 2000 either in Application Mode or Remote Administration Mode. Configuring Terminal Services to run in Remote Administration Mode provides the ability to connect to the server from a remote client and manager the server. There are no licensing issues that come with this configuration and up to two simultaneous connections can be made. There are two approaches that can be taken when configuring this Small Business Server. One approach is to have Terminal Services only listen on the internal NIC.

© SANS Institute 2004



This is done basically like the other services that were changed. Now to connect to the SBS Server via Terminal Services the client would either have to be on the internal LAN or utilize a VPN connection. This approach keeps the service from being exposed on the public interface.

The second approach would be to publish the service and only allow specific clients to connect. Since it is common knowledge that Terminal Services listens on TCP 3389 this could be changed to something else (Michael's World O'Tips)²². This would not be a great deterrent for the persistent hacker but at least it would not show up in a scan that someone might do specifically looking for this service.



To change the listening port on the server requires a registry change located at –
 HKLM\System\CurrentControlSet\Control\TerminalServer\WinStations\RDP-
 Tcp\PortNumber

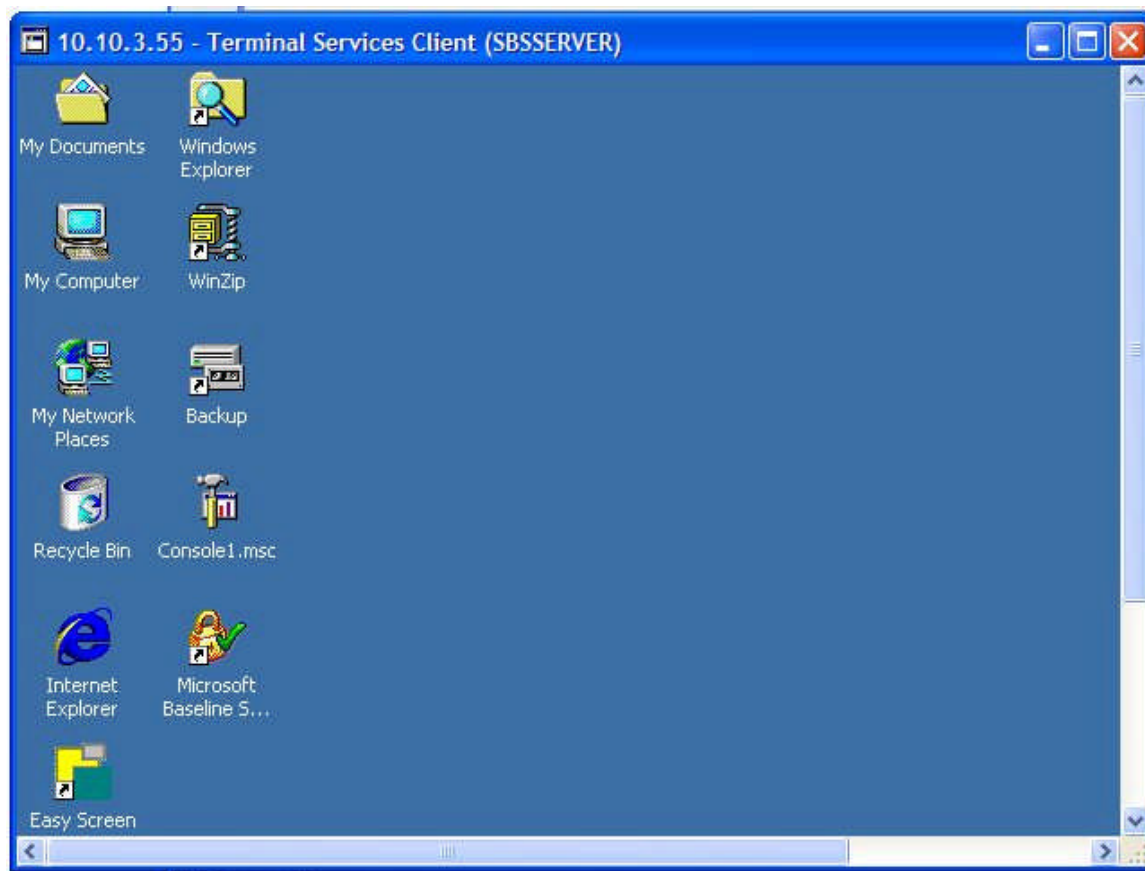
The value is displayed in HEX. Change this value to something else like 8282 (decimal) and restart the server. A new protocol definition will need to be created with the port value that was used in the registry. Once this is completed create a publishing rule using that protocol definition and the client set that includes the IP addresses of the external PC's that will be allowed to connect. (Note: Publishing services on the Small Business Server is beyond the scope of this paper. Details on this subject can be found in the additional resources section at the end of this paper.)

Then to change the Terminal Services client create a new connection in the connection manager. Once the new connection has been created highlight and click Export under the File menu. Save the file with the .cns file extension and open with notepad.

```
sbsserver.cns - Notepad
File Edit Format View Help
[SBSSERVER]
winPosStr=0,1,0,0,640,480
Expand=1
Smooth Scrolling=0
Shadow Bitmap Enabled=1
Dedicated Terminal=0
Server Port=8282
Enable Mouse=1
Disable CTRL+ALT+DEL=1
DoubleClick Detect=0
Full Screen Hotkey=3
Icon Index=0
Desktop Size ID=1
Screen Mode ID=1
Compression=0
BitmapCachePersistEnable=0
Desktop=1
Auto Connect=1
Icon File=
Progman Group=Terminal Services Client
MRU0=10.10.3.55
AutoLogon 50=0
UserName 50=00
MaximizeShell 50=1
Password 50=7368448183FEE2C58646D8334A26C231FE44819CD417E8D50658431453DB6D4700
Salt 50=EC09BC41088626B6F4EC401589F71F43B70E1AA100
Domain 50=00
Alternate Shell 50=00
Shell working Directory 50=00
AutoLogon=0
UserName=00
MaximizeShell=1
Password=A2E2D4F2E53086058B1CB2353858663688FF9AAA6BA84B5F666A8C4F6231B96C00
Domain=00
Alternate Shell=00
Shell working Directory=00
[SBSSERVER\Hotkey]
CtrlEsc=36
AltEsc=45
AltTab=33
AltShiftTab=34
AltSpace=46
CtrlAltDelete=35
[Private Reserved Section]
SBSSERVER=
```

Change the Server Port=3389 to the value that you used in the registry. Save and import back into the Client Connection Manager. You may be prompted to overwrite the existing connection, click yes.

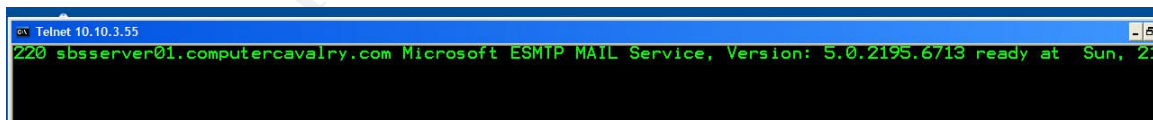
© SANS Institute



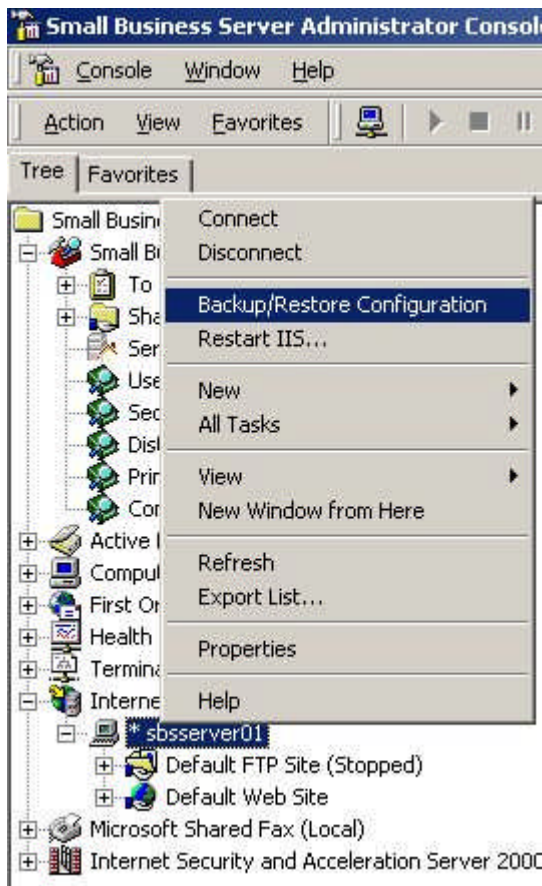
Double click the session icon and you should be prompted for a user name and password and be able to log on to the desktop as I have done.

Once we have published the SMTP service we can test to see if the Small Business Server will accept mail by using the telnet command and replacing the default TCP port 22 with TCP 25 (SMTP) –

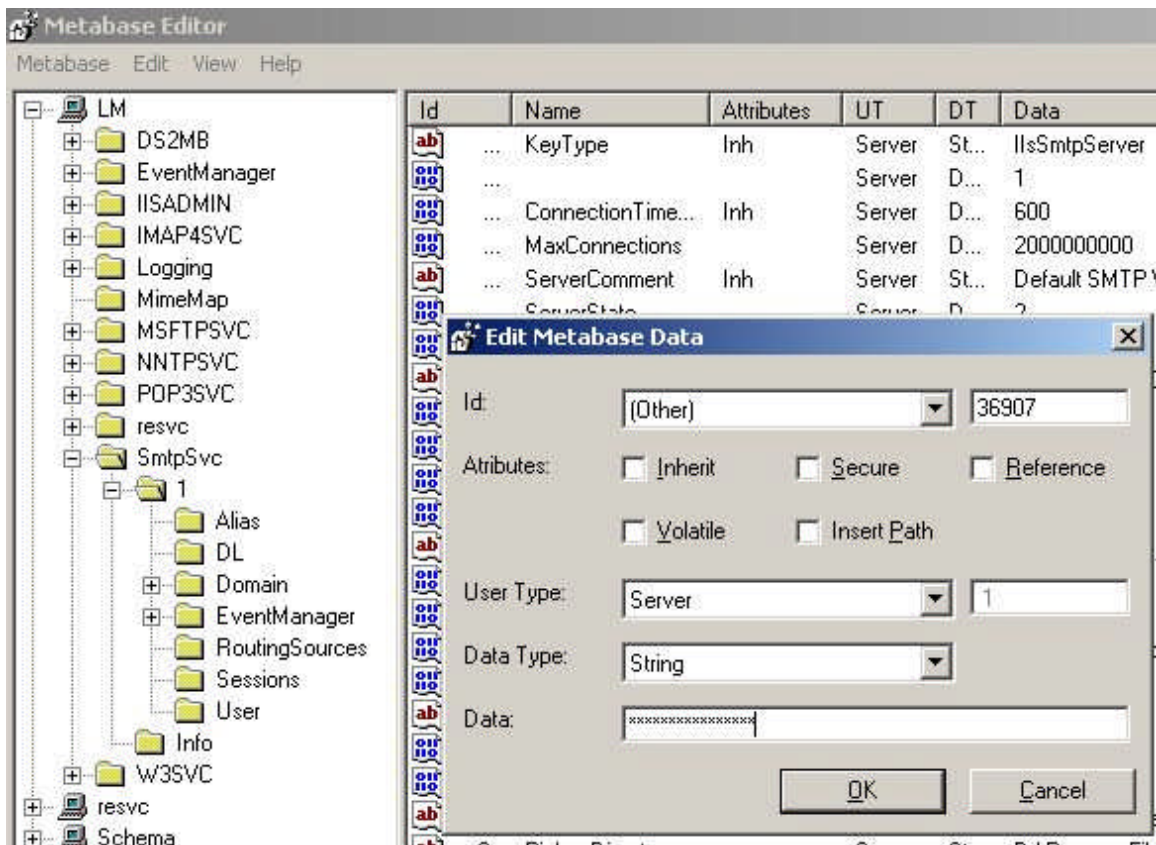
C:\>telnet <external interface IP address> 25



The server not only accepts the connection but as you can see also informs us that it is Microsoft ESMTP mail version 5.0.2195.6713. Probably more information than we would like given that fact that if an exploit were discovered for a specific version of this service it would be an easy task to go out looking for servers running this version to exploit. The banner information that is being displayed above can be modified using the [Metaedit](#)²³ tool. The procedure to accomplish this is described in the Microsoft Q article [Q281224](#)²⁴ 'How to Modify the SMTP Banner'. As with any type of editing that is going to be done a cautionary note – always start by backing up the current data in this instance it is the Metabase for IIS.



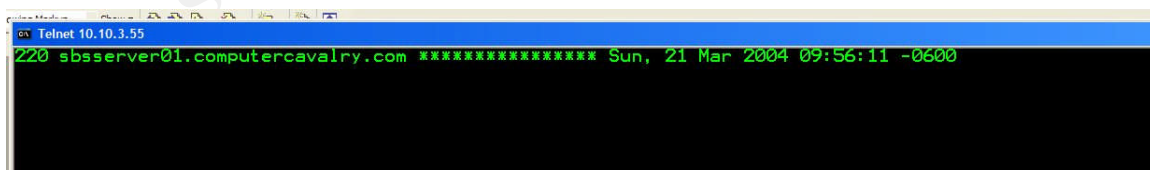
This can be done from the Internet Services Manager by right clicking and selecting the Backup/Restore Configuration option from the context menu.



Next simply start the Metabase editing tool and then per the instructions –

- ‘Click Edit, Click New, and then click String.
- Verify that the entry in the ID box is Other, and then type 36907 (decimal) on the right side of the ID box.
- In the Value box, type the banner that you want to be displayed. (We are using asterisks in the example)
- Stop, and then restart the SMTP virtual server or the SMTP service.’

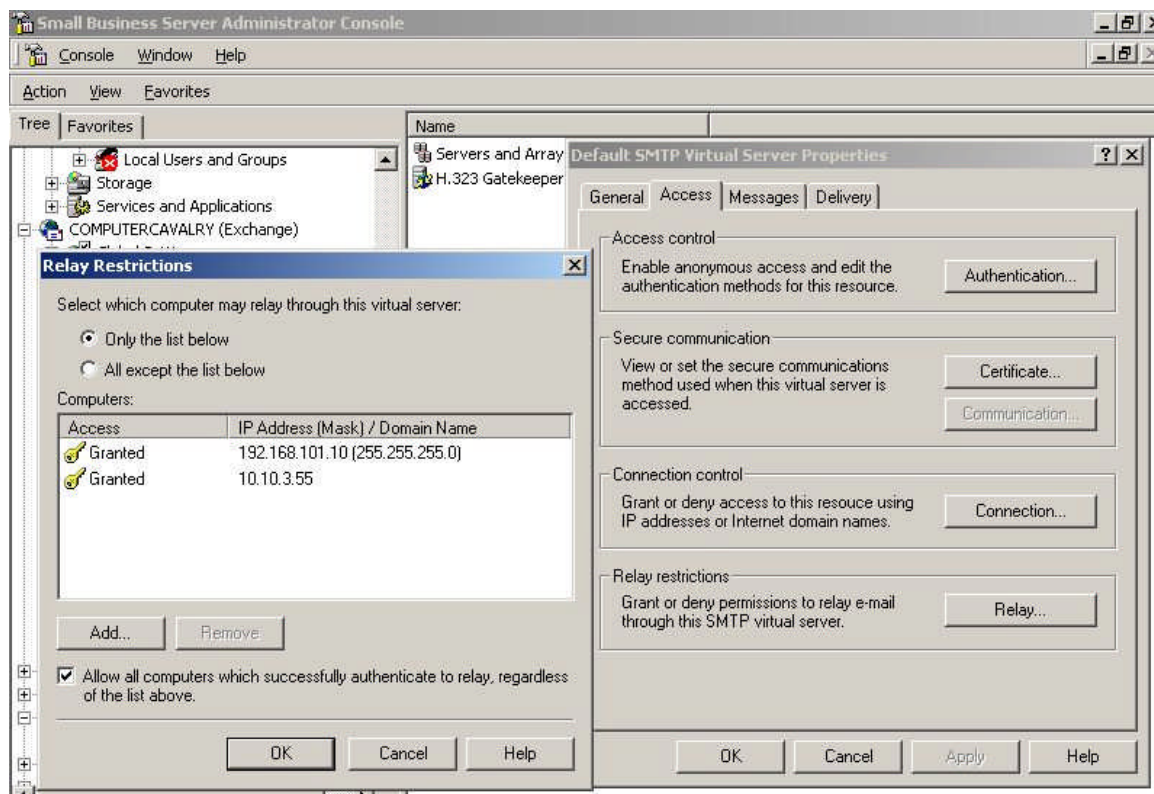
Once this has been completed just attempt the telnet connection again to display the results.



The information that had been displayed previously has been replaced with the asterisks. Information on applying this same strategy to the POP3 and IMAP4 services can be found in Microsoft’s Knowledge Base article [Q303513](#).

Another important item in regards to the mail service is to verify that we are not allowing relaying through our server. Exchange does not allow relaying when installed but it is

always a good idea to confirm that the setting is in fact correct. The setting is accessed from the Exchange System Manager, expanding protocols, SMTP, selecting the virtual server, right click and select properties.



Click on the Relay tab to display the Relay Restrictions page as seen above. As illustrated the only addresses that are listed that are allowed to relay are the IP addresses of the public and private network adapters of the Small Business server. You can also test this using the telnet command.

```

Telnet 10.10.3.55
220 sbsserver01.computercavalry.com ***** Sun, 21 Mar 2004 11:31:31 -0600
ehlo mazzios.com
250-sbsserver01.computercavalry.com Hello [127.0.0.1]
250-TURN
250-ATRN
250-SIZE
250-ETRN
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-8bitmime
250-BINARYMIME
250-CHUNKING
250-VRFY
250-X-EXPS GSSAPI NTLM LOGIN
250-X-EXPS=LOGIN
250-AUTH GSSAPI NTLM LOGIN
250-AUTH=LOGIN
250-X-LINK2STATE
250-XEXCH50
250 OK
mail from:lloyd_ardoin@mazzios.com
250 2.1.0 lloyd_ardoin@mazzios.com...Sender OK
rcpt to:user@spam.com
550 5.7.1 Unable to relay for user@spam.com
  
```

The last line of the telnet session above is the output that should be expected if relaying is not allowed – ‘Unable to relay for user@spam.com’. Information on using the procedure

can be found in the Microsoft Q article [Q324958](#)²⁵ ‘How To: Block Open SMTP Relaying and Clean Up Exchange Server SMTP Queues on SBS’.

Since we have validated that the SMTP service is accepting connections it would be a good time to verify what other ports are listening. A good tool to use that I prefer is NMAP. Using NMAP is well beyond the scope of this paper but there is lots of information that can be found on the Internet. A great place to start is at the [insecure.org website](#)²⁶. There are versions available for Windows NT and there may also be one for Windows 2000 or XP that I am not aware of. You can also find Windows based port scanners available if that is your preference.

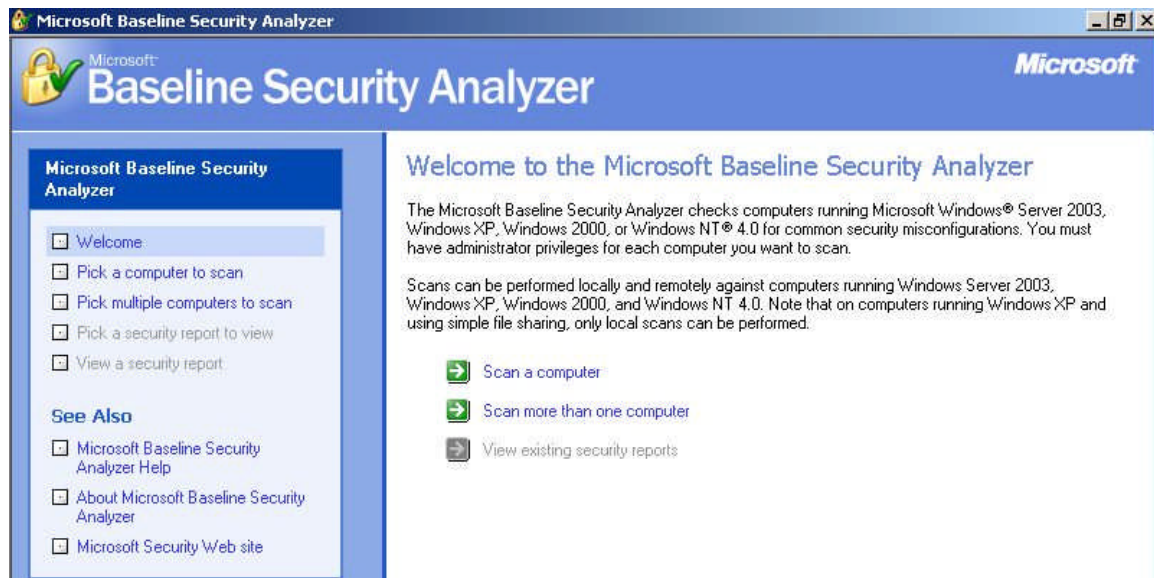
NMAP not only does TCP and UDP port scanning but it has the capability to do OS fingerprinting. The results of the scan for the Small Business Server are shown below.

```
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Host (10.10.3.55) appears to be up ... good.
Initiating SYN Stealth Scan against (10.10.3.55)
Adding open port 7777/tcp
Adding open port 143/tcp
Adding open port 110/tcp
Adding open port 25/tcp
Adding open port 443/tcp
Adding open port 80/tcp
The SYN Stealth Scan took 730 seconds to scan 8000 ports.
Warning: OS detection will be MUCH less reliable because we
did not find at least 1 open and 1 closed TCP port
For OSScan assuming that port 25 is open and port 32769 is
closed and neither are firewalled
Interesting ports on (10.10.3.55):
(The 7994 ports scanned but not shown below are in state:
filtered)
Port      State      Service
25/tcp    open       smtp
80/tcp    open       http
110/tcp   open       pop-3
143/tcp   open       imap2
443/tcp   open       https
7777/tcp   open       unknown
Remote OS guesses: FreeBSD 2.2.1 - 4.1, Windows Millennium
Edition (Me), Win 2000, or WinXP
TCP Sequence Prediction: Class=random positive increments
                        Difficulty=11223 (Worthy challenge)
IPID Sequence Generation: Incremental

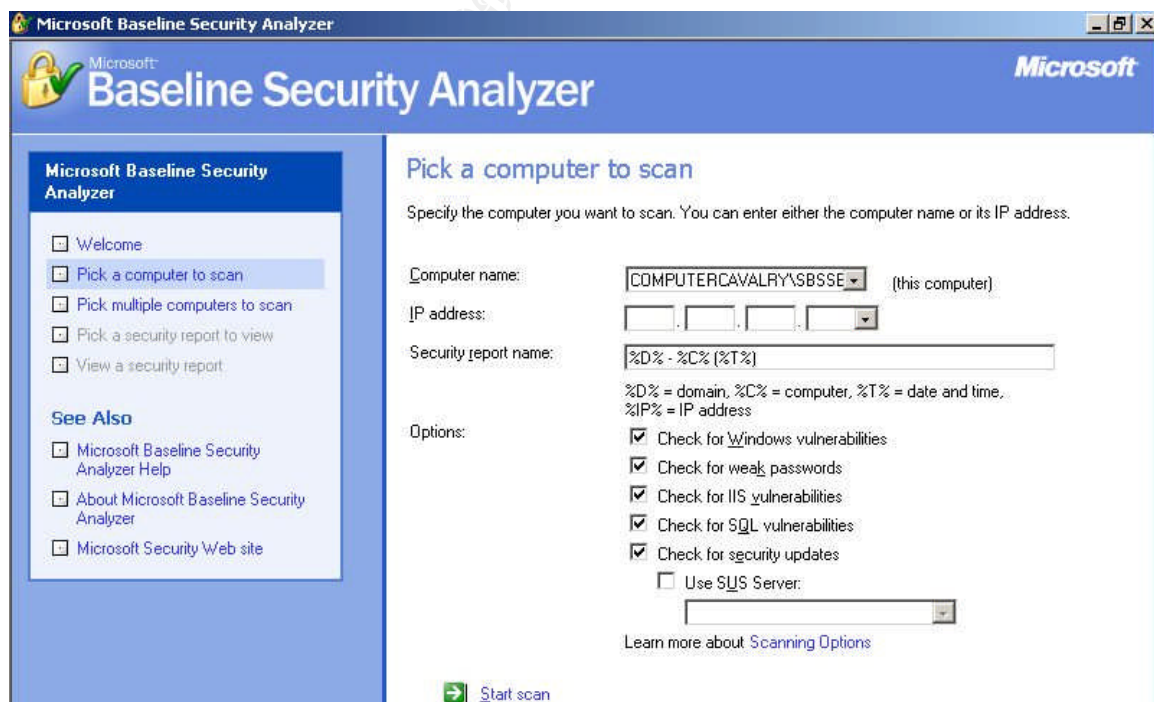
Nmap run completed -- 1 IP address (1 host up) scanned in 735
```

The results show that the HTTP, HTTPS, SMTP, POP3, IMAP4 and the newly configured Terminal Services port –TCP 7777 ports are listening on the Small Business Server which verifies our publishing rules configuration.

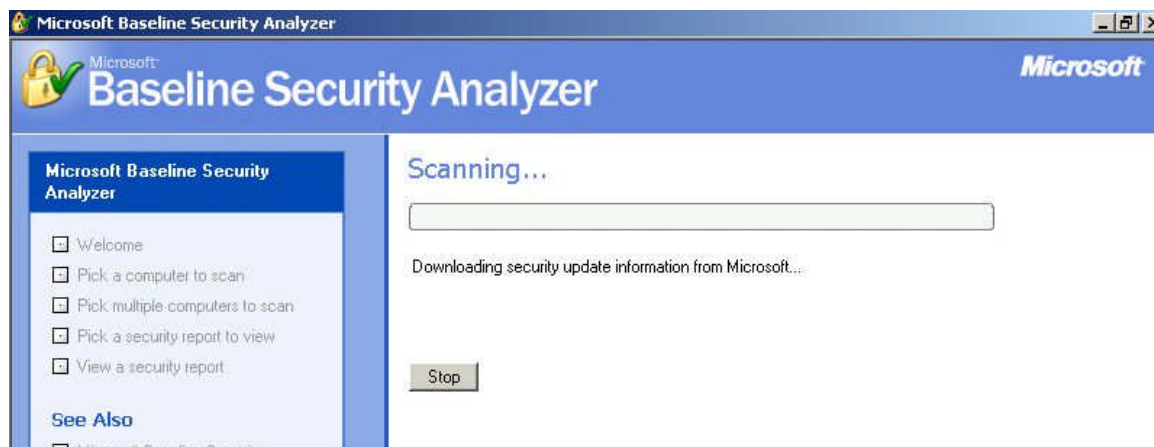
The Microsoft [Baseline Security Analyzer v1.2](#)²⁷ is the last tool that we will use locally on this server. It is free and can be downloaded from the Microsoft website. This tool includes a graphical and command line interface and as mentioned earlier has the HFNETCHK tool included. It runs on Windows XP, Windows 2000 and Windows 2003. It can do a local scan and also scan remote systems for common system misconfigurations as well as missing security updates.



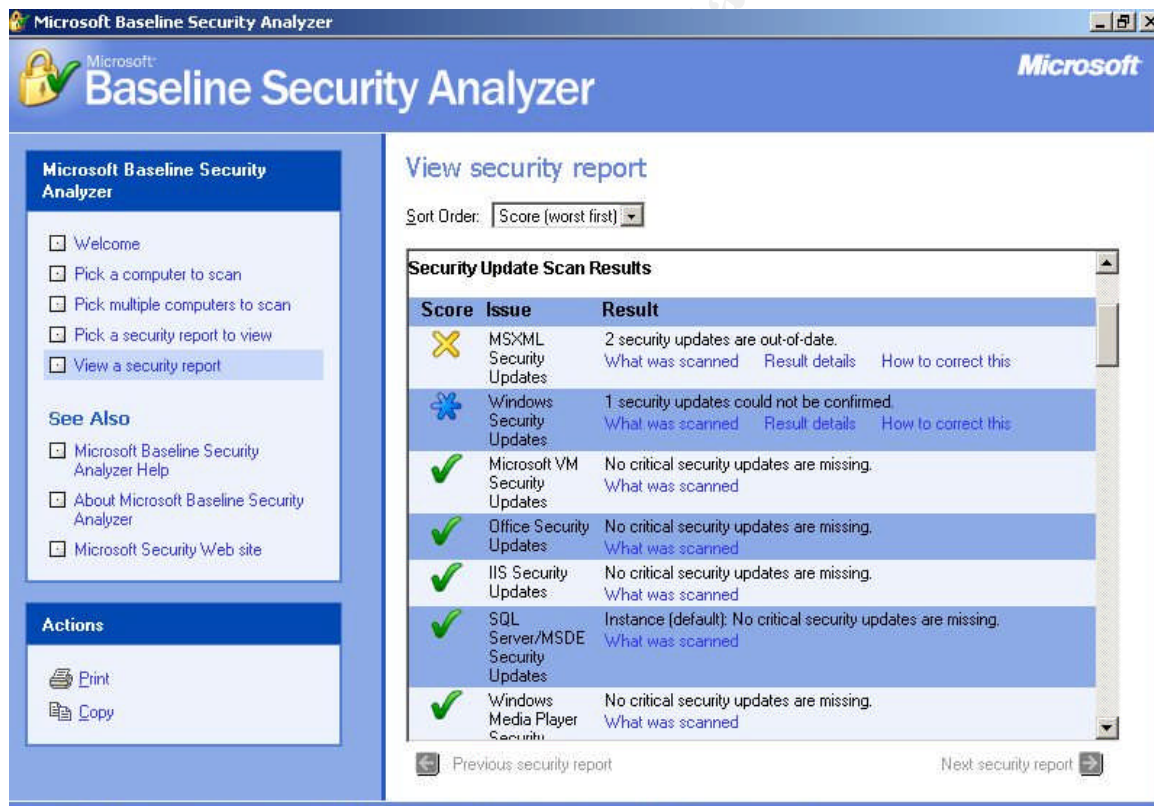
Once it is installed just double click the shortcut on the desktop to start. The look is similar to the Microsoft Security Update website. Click the scan computer link to continue.



Here is where you can select the local or remote system to scan by name or IP address and check which options to specifically check. There is also an option to use a SUS server if there is one on your network.



A progress bar is displayed as the MBSA performs the scan.



Once the scan has been completed a report is generated like the screen shot above. The report is broken into several categories – Security Updates, Windows, Internet Information Server (IIS), SQL Server, and Desktop Application. Each category lists results sorted worst first (default) but can be sorted differently by using the drop down box at the top.

The screenshot displays the Microsoft Baseline Security Analyzer (MBSA) application window. The title bar reads "Microsoft Baseline Security Analyzer". The main header area features the Microsoft logo and the text "Baseline Security Analyzer".

Left Navigation Panel:

- Microsoft Baseline Security Analyzer**
 - Welcome
 - Pick a computer to scan
 - Pick multiple computers to scan
 - Pick a security report to view
 - View a security report**
- See Also**
 - Microsoft Baseline Security Analyzer Help
 - About Microsoft Baseline Security Analyzer
 - Microsoft Security Web site
- Actions**
 - Print
 - Copy

Main Content Area: View security report

Sort Order: **Score (worst first)**

Sysadmins	Could not perform this check because SQL Server and/or MSDE was not running.
Sysadmin role members	Could not perform this check because SQL Server and/or MSDE was not running.
SQL Server/MSDE Account Password Test	The check was skipped because SQL Server and/or MSDE is operating in Windows Only authentication mode. What was scanned
Guest Account	Could not perform this check because SQL Server and/or MSDE was not running.

Desktop Application Scan Results

Vulnerabilities

Score	Issue	Result
	IE Zones	Internet Explorer zones do not have secure settings for some users. What was scanned Result details How to correct this
	Macro Security	No Microsoft Office products are installed

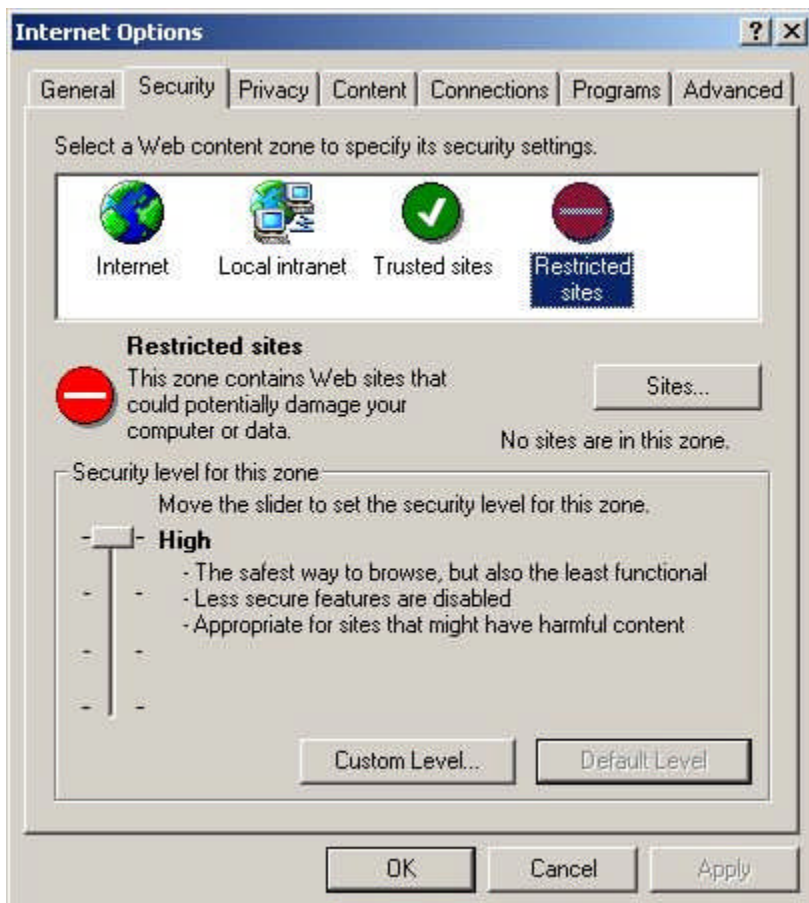
Navigation buttons at the bottom: [Previous security report](#) and [Next security report](#).

Copyright notice at the bottom: © 2002-2004 Microsoft Corporation. © 2002-2004 Shavlik Technologies, LLC. All rights reserved.

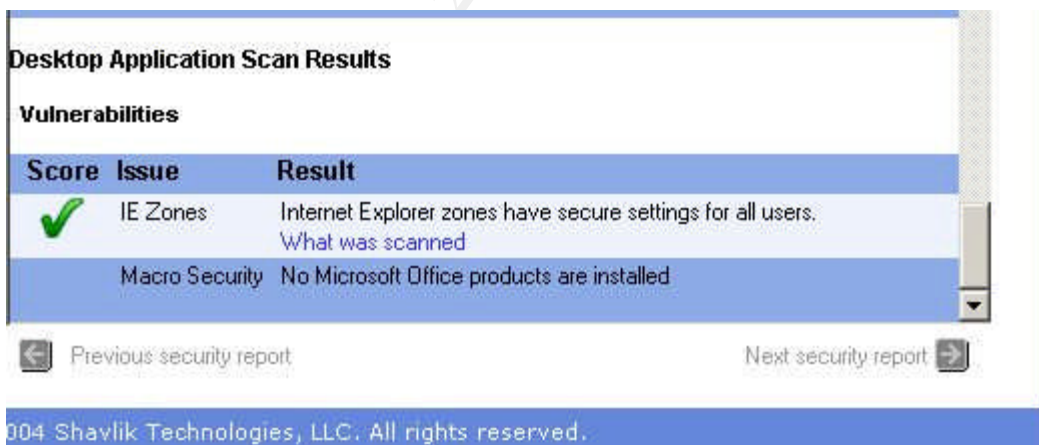
The look and feel of the tool is quite intuitive. In this example under 'Desktop Application Scan result', the red 'X' notates a critical item. You can click on the What was scanned link to get details about this specific line item criteria, click the Result details to see why it is rated as critical and click the How to correct this link for a resolution to the problem.



The configuration that caused the critical result is the current setting on Internet Explorer located on the Security Tab of the browser's properties. Notice that the Restricted Sites zone is set to 'Custom settings'.

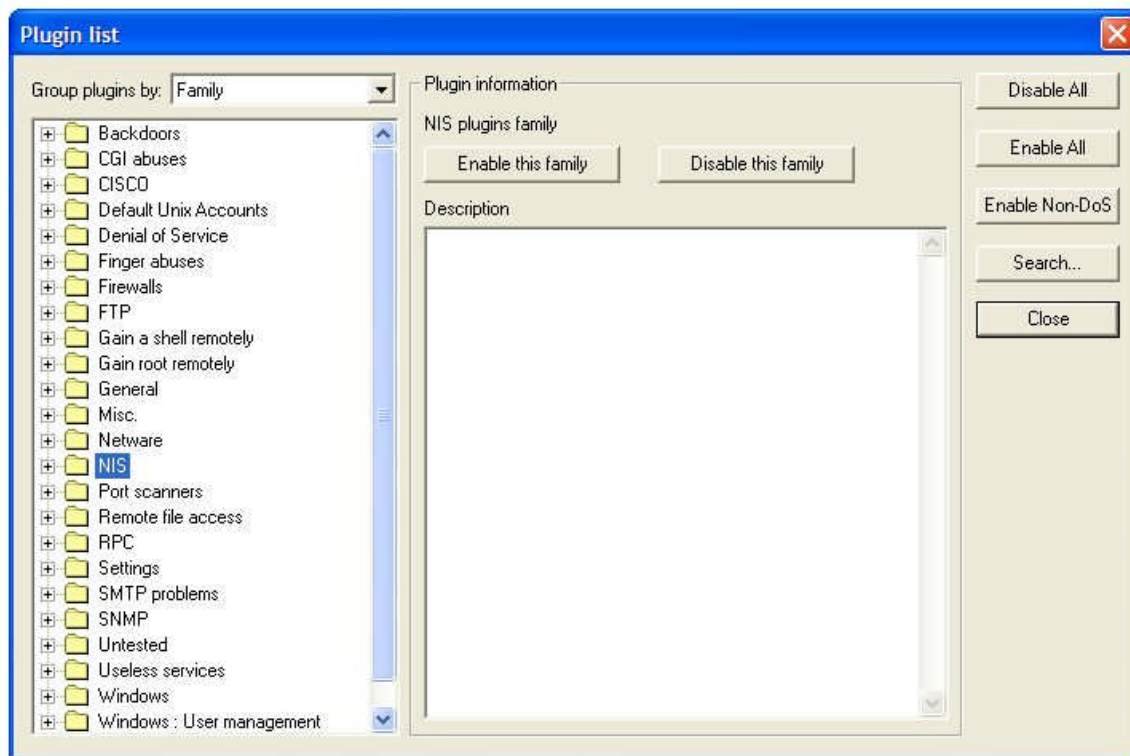


The resolution to this configuration problem is to click the Default Level button and then the Apply button which sets the zone's level to 'High'.

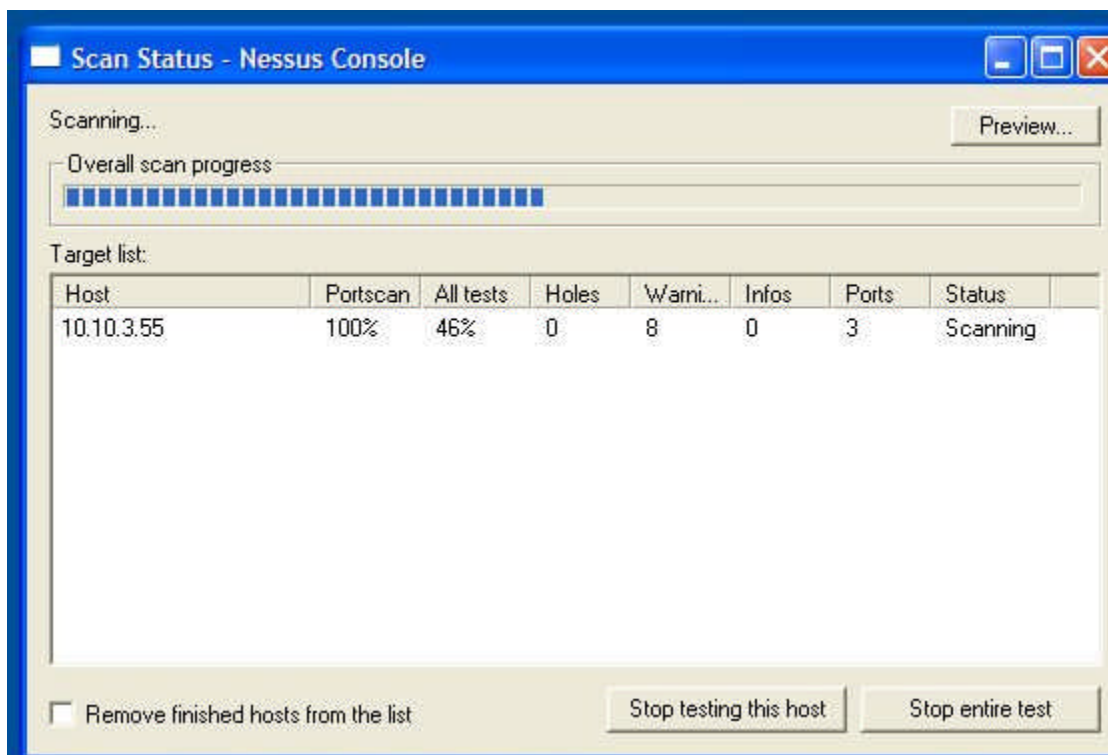


Once this change has been made and a rescan was done the results have changed to reflect that the setting is now in compliance.

The last tool that will be used to check the configuration of the Small Business Server is another Linux tool called Nessus. Nessus is written as a client server application and is a vulnerability scanner. The server daemon must run on a Linux box but there are Windows clients available. Installing and using Nessus is well beyond the scope of this document, Nessus and its documentation can be found at the Nessus.org²⁸ web site. Nessus uses what are called plug-ins. Once the tool is installed it even provides the ability to check for updated or new plug-ins that may be available. Currently there are over 2100 plug-ins available.

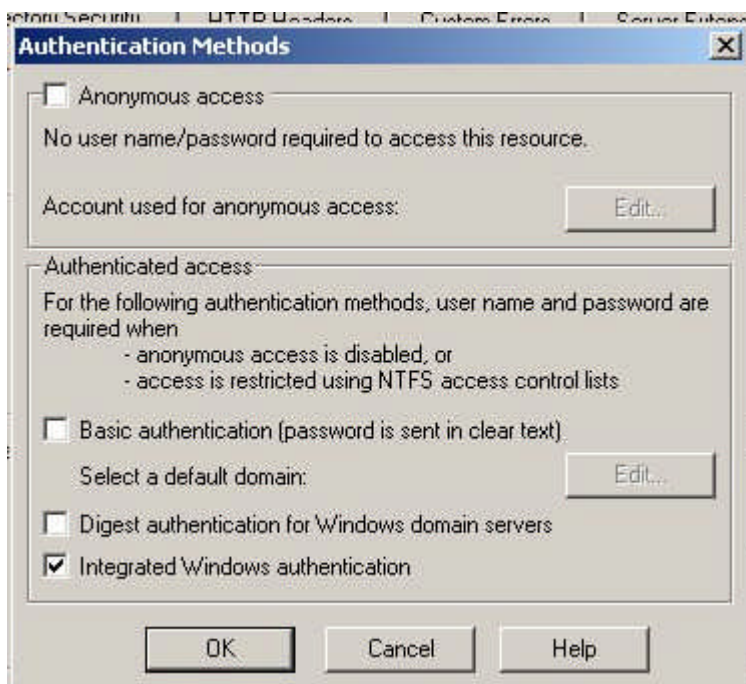


Each plug-in provides the ability to test for a specific type of vulnerability so you can tune Nessus for the specific host that is being tested. Nessus can scan either in a type of safe mode where it relies on banners instead of actually attempting the exploit. A good course of action is to do this type of scan initially and then once satisfied with the results attempt a full scan. Attempting this type of scan should be done with caution as it can cause the host or specific services to stop responding, cause the CPU to go into 100% utilization, or even blue screen. Based on these facts this is a great test to perform on a system that is getting ready to go into a production environment.

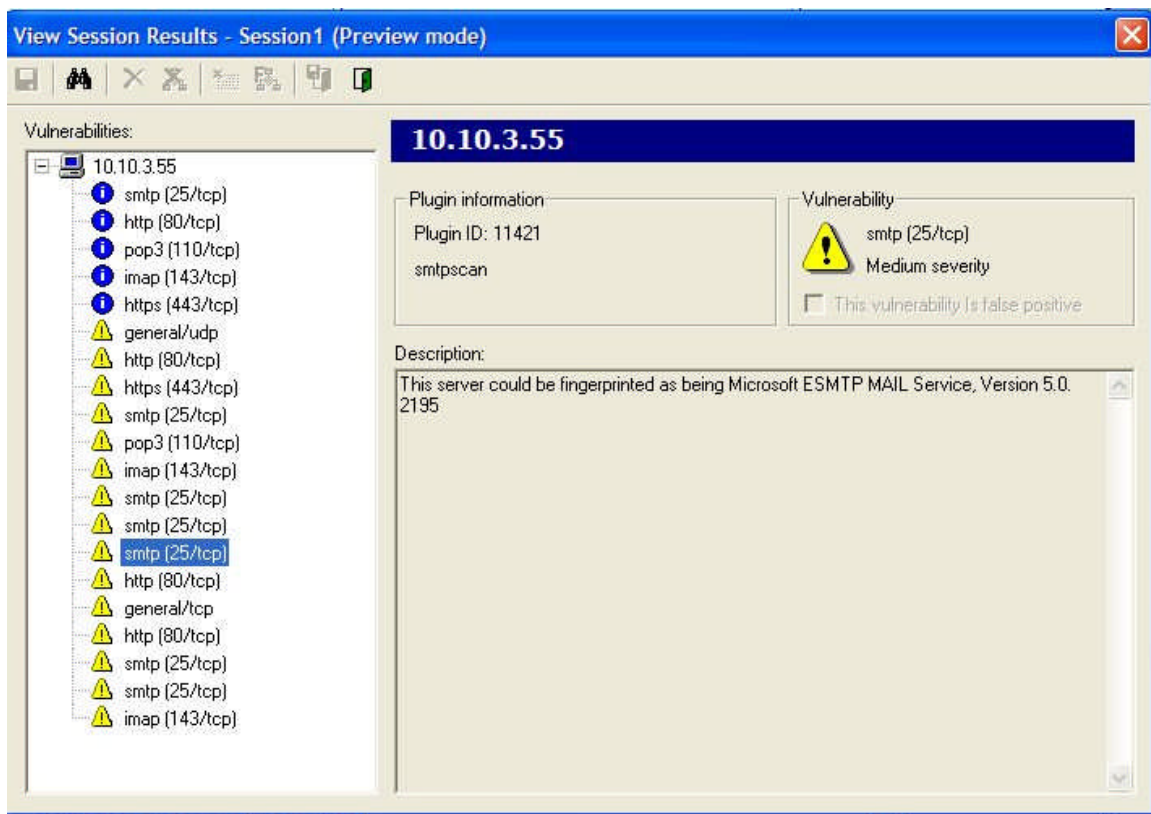


Here is the Windows client running on my XP PC. We are scanning the public interface of the SBS server and have configured Nessus to enable all plug-ins including the ones that are considered dangerous. It provides a progress bar and some stats to keep you informed of the scan.

© SANS Institute 2004, All Rights Reserved



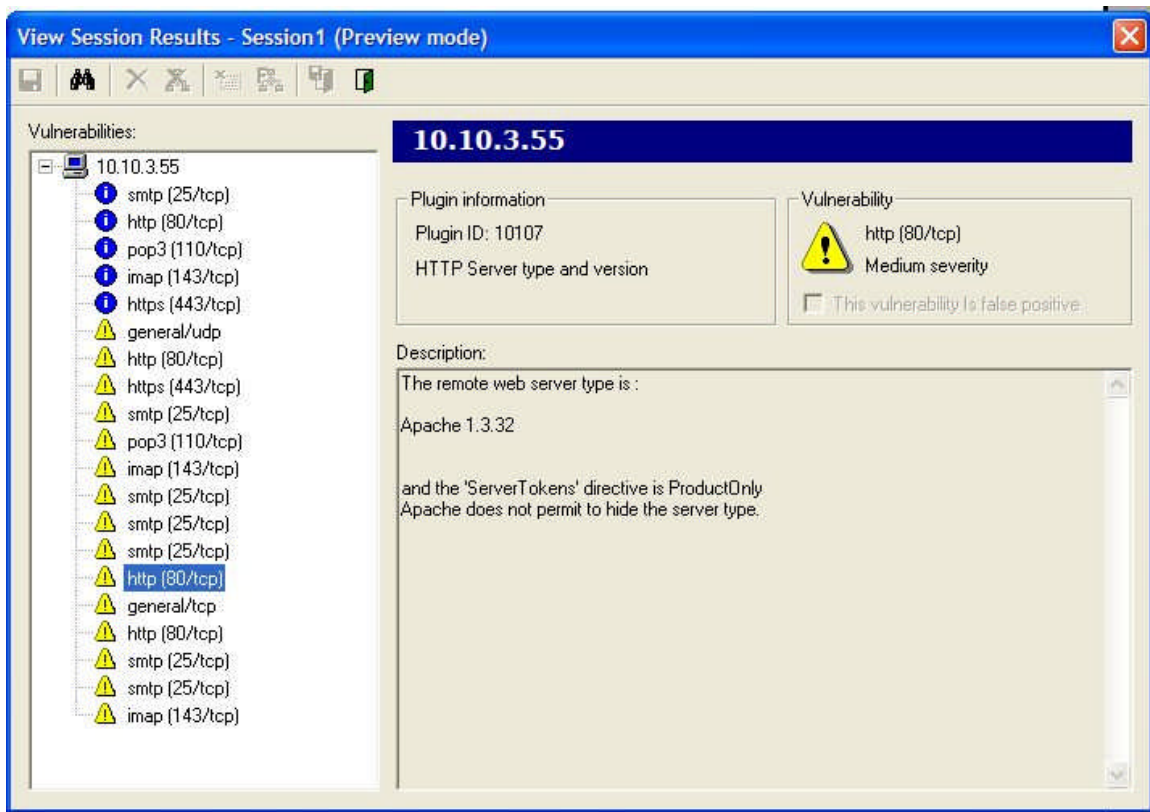
During the initial scan Nessus was able to glean the IUSR_Computername account because of the default authentication setting on the default web site which is Anonymous and Windows Integrated authentication enabled. The Anonymous authentication is not necessary since this server will not be providing public web services and only domain users should be accessing this server for mail services via OWA, POP3 or IMAP4 and will be using Windows Integrated authentication. This does require the client to use Internet Explorer 2.0 or higher which should not be an issue. As shown in the screen shot Anonymous access has been disabled.



Once a scan has completed you can click the preview button to get a glimpse of what it found. One item I found interesting was that even with the SMTP banner change that was done earlier Nessus was able to glean the SMTP version information; I think a good point about security through obscurity only goes so far.

The items on the left are listed as informational – blue circle, warnings – yellow triangle and holes – red circle.

© SANS Institute 2004



Here you can see the results of setting the AlternateServerName=Apache 1.3.32 value in the urlscan.ini file that was discussed earlier.

This report can be saved in several different formats including text and html.

Satisfied with the results, the last item to complete before the Small Business Server is placed in its production environment is to install a virus scanning engine for the mail service – two products being currently evaluated or from Trend Micro and Symantec.

In conclusion - the process described in this document has shown that with readily available tools and information specific steps can be applied during an install of Small Business Server 2000 and immediately thereafter that when combined will result in a much more hardened system. This process has also shown that the order of these additional steps is important to the overall success since initial variations caused some processes to fail and also that part of the process should include some type of verification or validation of the work. Small Business Server 2000 is a complex system, a compromise between cost, functionality and security, but with careful planning and implementation a successful deployment can be achieved.

References:

- ¹Microsoft – ‘System Requirements for Small Business Server 2000’ – URL - <http://www.microsoft.com/sbserver/techinfo/sysreqs/default.asp>
- ²Microsoft Knowledge Base – ‘Cannot Access Group Policy Objects’ – URL - <http://support.microsoft.com/default.aspx?scid=kb;en-us;258296>
- ³Microsoft Knowledge Base – ‘Active Directory Communication Fails on Multihomed Domain Controllers’ – URL - <http://support.microsoft.com/default.aspx?scid=kb;en-us;272294>
- ⁴DNS Poisoning – URL - http://www-personal.umd.umich.edu/~jhayek/Exploits/dns_poisoning.htm
- ⁵NTP.org – URL - <http://www.ntp.org/>
- ⁶Microsoft TechNet Home – URL - <http://www.microsoft.com/technet/default.mspx>
- ⁷Qchaine.exe – URL - <http://www.microsoft.com/downloads/details.aspx?FamilyID=a85c9cfa-e84c-4723-9c28-f66859060f5d&displaylang=en>
- ⁸Microsoft Baseline Security Analyzer v1.2 download – URL - <http://www.microsoft.com/technet/security/tools/mbsahome.mspx>
- ⁹White Paper: Microsoft Baseline Analyzer v1.2 – URL – <http://www.microsoft.com/technet/security/tools/mbsawp.mspx>
- ¹⁰SANS – “Securing Windows 2000 Professional” pg 20-21
- ¹¹Microsoft TechNet – ‘Security Consideration for Network Attacks’ – URL - <http://www.microsoft.com/technet/security/topics/network/secdeny.mspx>
- ¹²NSA Security Recommendation Guides download – URL - <http://nsa2.www.conxion.com/win2k/download.htm>
- ¹³The Center for Internet Security Website – <http://www.cisecurity.org/>
- ¹⁴Microsoft Knowledge Base – “Group Policy Application Rules for Domain Controllers” – URL - <http://support.microsoft.com/default.aspx?scid=kb;en-us;259576&Product=win2000>
- ¹⁵Microsoft Knowledge Base – “How To: Manage Security Templates in Windows 2000” <http://support.microsoft.com/default.aspx?scid=kb;en-us;321679&Product=win2000>

- ¹⁶Microsoft – The Small Business Server 2000 Resource Kit –
<http://www.microsoft.com/resources/documentation/sbs/2000/all/reskit/en-us/default.mspx>
- ¹⁷Slipstreaming Services packs with Windows 2000’ -
<http://www.eits.uga.edu/nt2000/slipstream.html>
- ¹⁸IIS Lockdown Tool 2.1 – URL -
<http://www.microsoft.com/downloads/details.aspx?FamilyID=dde9efc0-bb30-47eb-9a61-fd755d23cdec&displaylang=en>
- ¹⁹Microsoft Knowledge Base – How To: Configure the URLScan Tool –
<http://support.microsoft.com/default.aspx?scid=kb;%5bLN%5d;326444>
- ²⁰ISA Server and Beyond – Dr. Thomas Shinder, Debra Shinder, Martin Grasdal
Disable Socket Pooling Pg. 386-389
- ²¹Microsoft Knowledge Base – How To: Disable IIS 5.0 SMTP service socket pooling in Windows 2000 - <http://support.microsoft.com/default.aspx?scid=kb;en-us;310155>
- ²²Michael’s World O’Tips – How to Change Terminal Server’s Listening Port
<http://www.mike-tech.com/article.php?gif=win2k&article=204>
- ²³Microsoft How To: Download, Install, and Remove the IIS MetaEdit 2.2 Utility
<http://support.microsoft.com/default.aspx?scid=kb;en-us;232068>
- ²⁴Microsoft – How to modify the SMTP Banner –
<http://support.microsoft.com/default.aspx?scid=kb;en-us;281224>
- ²⁵Microsoft – ‘How To: Block Open SMTP Relaying and Clean Up Exchange Server SMTP Queues on SBS’ – URL -
<http://support.microsoft.com/default.aspx?scid=kb;en-us;324958>
- ²⁶NMAP – URL - <http://www.insecure.org/nmap/>
- ²⁷Microsoft TechNet – Microsoft Baseline Security Analyzer –
URL - <http://www.microsoft.com/technet/security/tools/mbsahome.mspx>
- ²⁸Nessus – URL - <http://www.nessus.org/>
- ²⁹Microsoft Knowledge Base – How TO: Configure the Simple Network Time Protocol On ISA Server – URL - <http://support.microsoft.com/default.aspx?scid=kb;en-us;323621>
- ³⁰NSA - Guide to Securing Microsoft Windows 2000 Group Policy Security Configuration Tool Set (Chapter 3 page 38 of the NSA pdf documentation)

³¹NSA - Guide to Securing Microsoft Windows 2000 Group Policy Security Configuration Tool Set (Chapter 3 page 44 of the NSA pdf documentation)

³²NSA - Guide to Securing Microsoft Windows 2000 Group Policy Security Configuration Tool Set (Chapter 3 page 21 of the NSA pdf documentation)

³³NSA - Guide to Securing Microsoft Windows 2000 Group Policy Security Configuration Tool Set (Chapter 3 page 49 of the NSA pdf documentation)

³⁴NSA - Guide to Securing Microsoft Windows 2000 Group Policy Security Configuration Tool Set (Chapter 3 page 53 of the NSA pdf documentation)

Additional Resources –

Download of the Windows 2000 Hardening Guide – w2khg.exe – URL

<http://www.microsoft.com/downloads/details.aspx?displaylang=en&familyid=15e83186-a2c8-4c8f-a9d0-a0201f639a56>

Brelsford, Harry; Clough, Bob. “Small Business Server 2000 Best Practices”

Shinder, Dr. Thomas, Shinder, Debra, Grasdal, Martin. “Configuring ISA Server 2000”