Global Information Assurance Certification Paper

Securing a Windows 2000 Server Connected to the Internet

For SANS New Orleans 2001

By: James Oryszczyn

Securing Windows 2000 with IIS 5.0 to use on the Internet.

This paper is a guide on how to harden Windows 2000 for use on the Internet. I will also show steps to on how to make IIS 5.0 more secure. Security is ever changing and policies and procedures will change. This document provides no guaranties and should be used only as a guide. This paper was written to fulfill the requirement for SANS GIAC certification.

These procedures were performed on a standalone Windows 2000 server. All of the steps discussed in this document should be tested in a lab situation before implemented on production systems. This will ensure that production systems stay up and running. Always make sure you test changes on non-production machines.

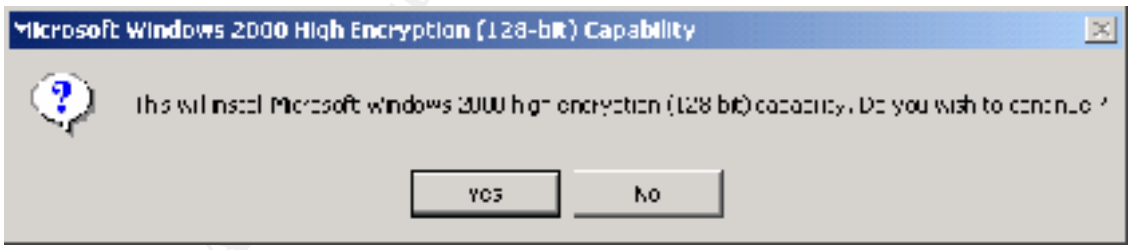
Hot Fixes and Service Packs

Build you Windows 2000 Web server off of the network and not connected to the Internet. This will ensure that the machine has not been tampered with.

Apply Service Pack 1 for Windows 2000. If you are not running the high encryption pack for Windows 2000 you need to update your system to the 128-bit encryption. Go to http://www.microsoft.com/windows2000/downloads/recommended/encryption/default.asp

Use the standard download and download it to your machine

The file you download will be Encpack_Win2000_EN. Double click to run it

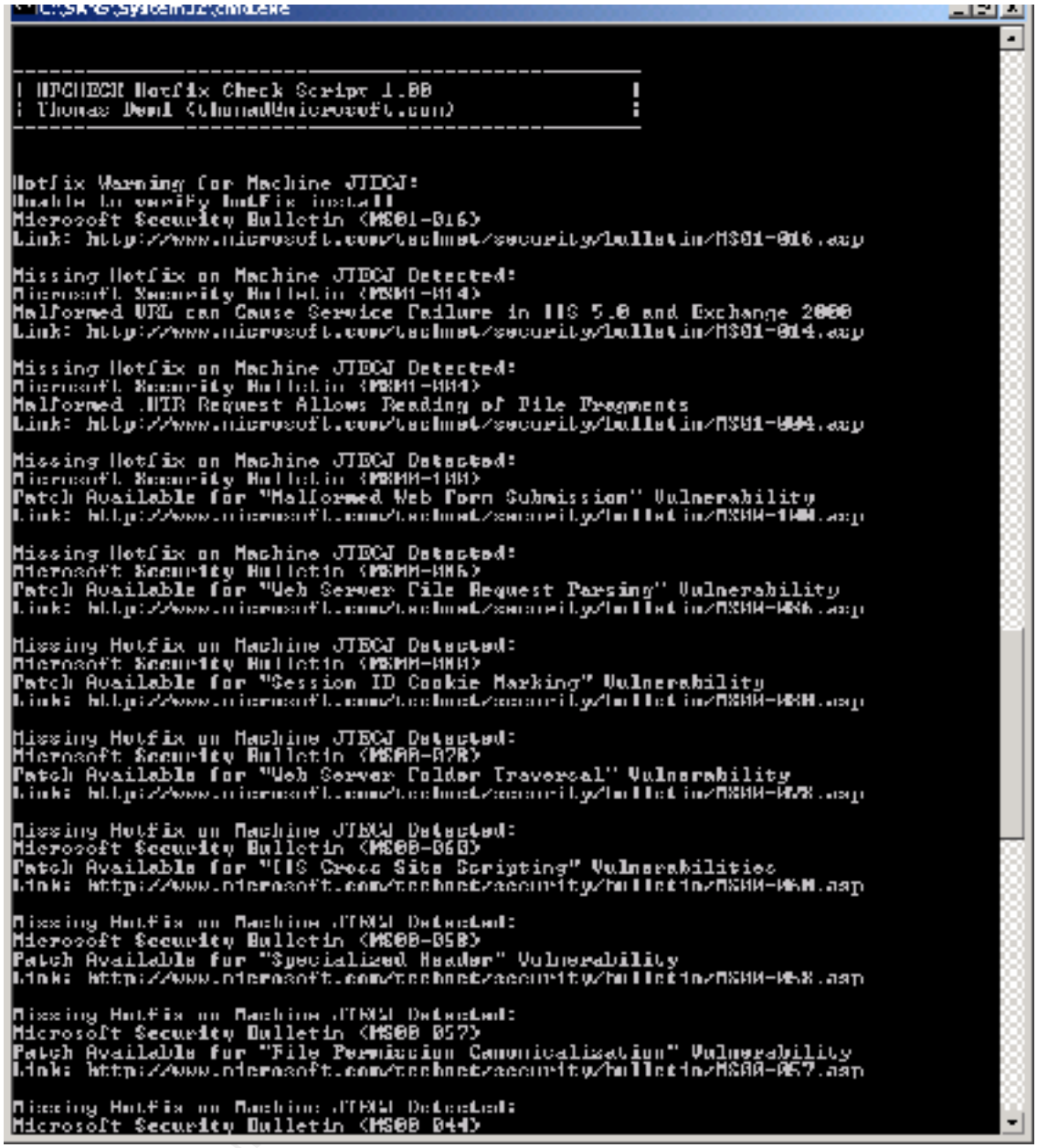


Click on yes to continue and after the High encryption is installed reboot your computer.

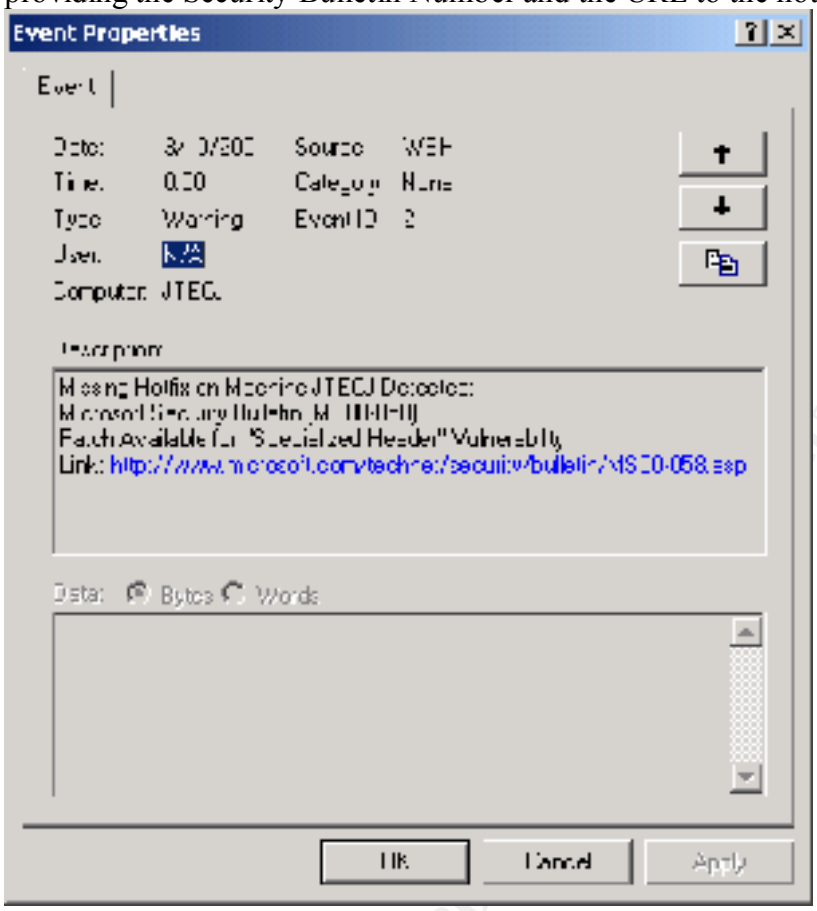
Now you are ready to install Service Pack 1 or greater for Windows 2000(Service Pack 1 was the latest and greatest at the time of this document). You can get this service pack from windowsupdate.microsoft.com. Make sure that you install the lasted and greatest service pack.

You also need to apply some hot fixes to IIS and to Windows 2000. You can automatically check to see what hot fix you need for IIS by downloading the IIS hot fix checking tool http://www.microsoft.com/technet/security/tools.asp.
This tool is a must have for anyone supporting IIS 5.0. It has many useful features like logging missing hot fixes to the event log and you can event customize the script to send you an email on the hot fixes that are missing.

Extract it to a folder of your choice and run it. You may have to run this command cscript.exe //H:Cscript. This will change the default script host to cscript.exe.
Go to a command prompt and change to the directory were the hot fix tool was extracted. Run hfcheck.wsf and it will query a Microsoft server and come back with the hot fixes you need for IIS 5.0. Below is an example of the hot fix tool. **Warning!!!! You still need to check for Windows 2000 Hot fixes.**



Example of the missing hot fix in the event logs. Microsoft has been very helpful by providing the Security Bulletin Number and the URL to the hot fix.



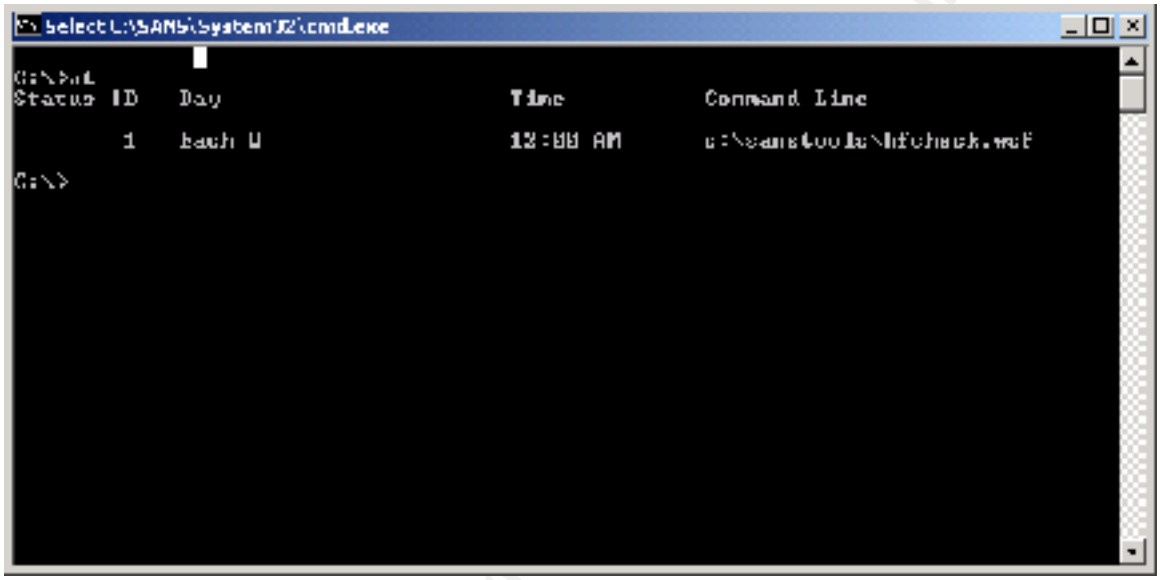
You can modifiy the script that Microsoft created to allow you to send an email to an admin if a hot fix is missing.

Sample:

```
Set objMsg = CreateObject("CDONTS.NewMail")
'Set the properties of the Message
objMsg.From = "HotfixNotification@YourCompany.com"
objMsg.To = "Administrators@YourCompany.com"
objMsg.Subject = "Missing Hotfix Detected!"
objMsg.Body = "Microsoft Security Bulletin _
(" + sBulletin + ") " + sTitle + " Link:
_http://www.microsoft.com" + sLink
objMsg.Send
```

You can also schedule the hot fix tool to run with the at schedule command. I recommend scheduling this script to run at least once a week to make sure that all updates have been applied. This tool can also be run remotely. You could run this tool from a management workstation allowing to checking of all the web servers in the enterprise and allowing the tool to log in a central location below is a sample command to schedule the script.

AT.EXE 12:00am /INTERACTIVE /every:Wednesday c:\sanstools\hfcheck.wsf



Below is a URL to the current hot fixes needed to secure IIS 5.0 and Windows 2000. You should apply all of these hot fixes until Windows 2000 SP2 becomes available. Make sure that you install the hot fixes in order. Start with the oldest hot fix and work you way to the latest hot fix.

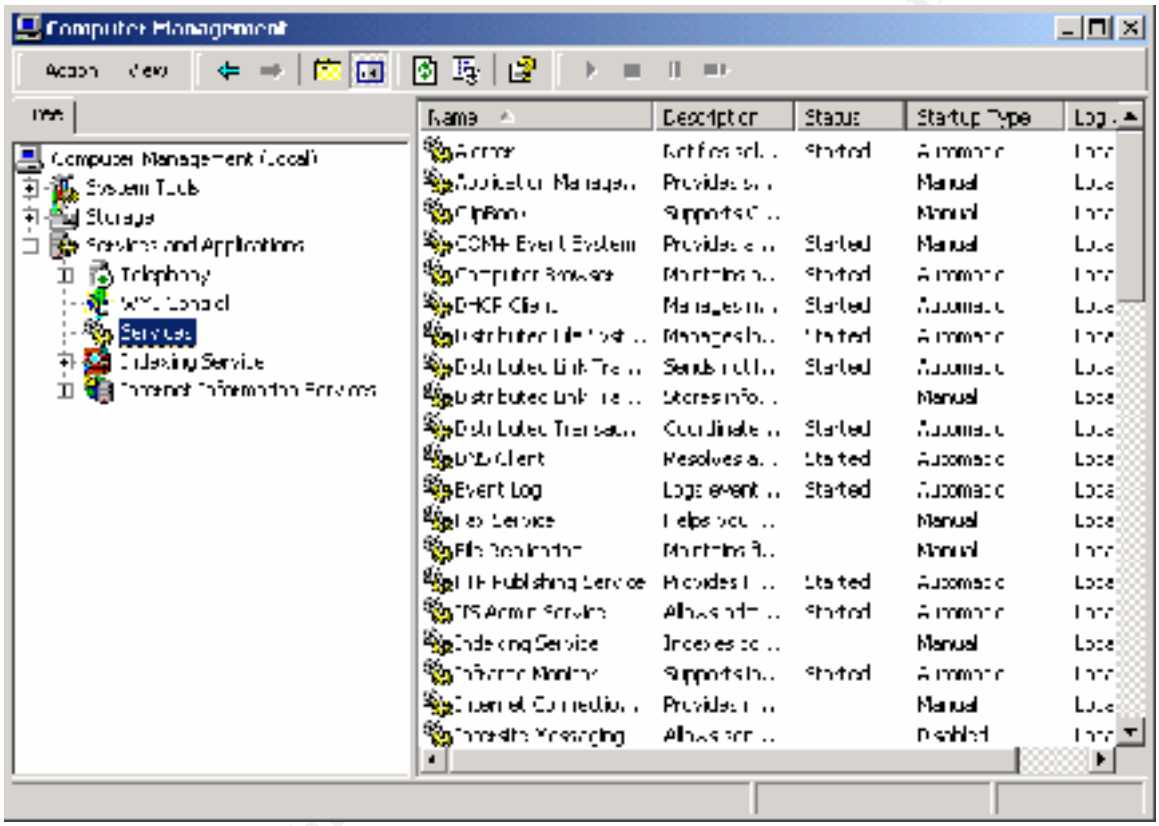
IIS Link :
http://www.microsoft.com/technet/security/current.asp?productID=15

Windows 2000 Link:
http://www.microsoft.com/technet/security/current.asp?productID=43

OS Hardening

Disabling Services

Windows 2000 comes default with a slew of services enabled. Most of these services are unneeded. They either take up server memory or make a web server vulnerable. You need to go to computer management and then services and applications. Expand Services and Applications and click on services.



As you can see that by default many services are enabled by default. Most of these services are needed when the 2000 Server is part of a domain, but not needed on a web server. When you disable the Server, Workstation and TCP/IP Netbios Helper you can prevent a hacker from pulling information remotely using netbios and null sessions. Below is a list of services and there explanation that can be disabled. I recommended disabling as many services as you can. **Warning**, **Some services like the server service or workstation might need to be enabled if you are using a commercial backup product**

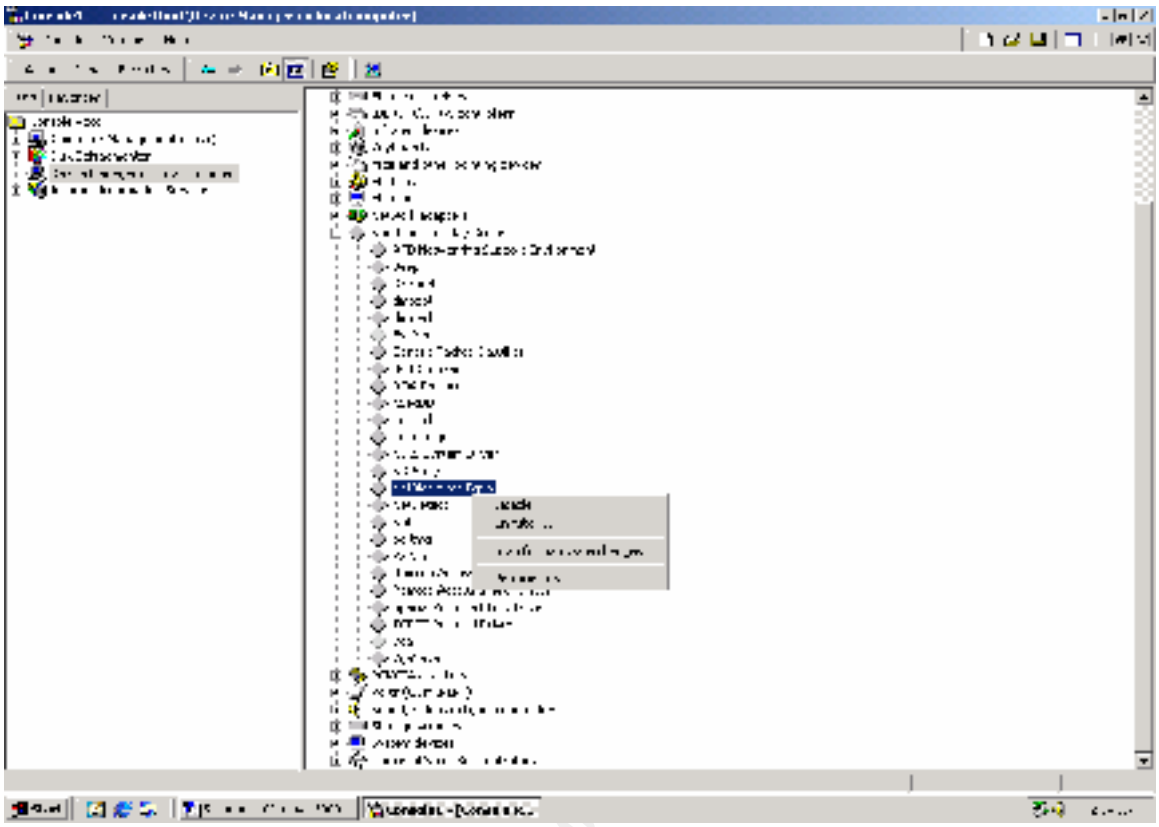
Alerter	Used to Send Administrative alerts to a list of Netbios names	Disable
Computer	Builts and maintains a list of computers and domains in	Disable

Browser	Network Neighbor Hood	
Distributed File System	Manages logical volumes distributed across a local or wide area network.	Disable
Distributed Link Tracking Client	Sends notifications of files moving between NTFS volumes in a network domain.	Disable
Distributed Link Tracking Server	Stores information so that files moved between volumes can be tracked for each volume in the domain.	Disable
DNS Client	Resolves and caches Domain Name System (DNS) names.	*Disable
Messenger	Sends and receives messages transmitted by administrators or by the Alerter service.	Disable
Print Spooler	Loads files to memory for later printing.	Disable
Remote Registry Service	Allows remote registry manipulation.	Disable
RunAs Service	Enables starting processes under alternate credentials	Disable
Server	Provides RPC support and file, print, and named pipe sharing.	Disable
System Event Notification	Notifies COM+ Event System subscribers of these events.	Disable
TCP/IP Net BIOS Helper Service	Enables support for Net BIOS over TCP/IP (Nest) service and Net BIOS name resolution.	Disable
Telephony	Local computer and, through the LAN, on servers that are also running the service.	Disable
Workstation	Provides network connections and communications.	Disable

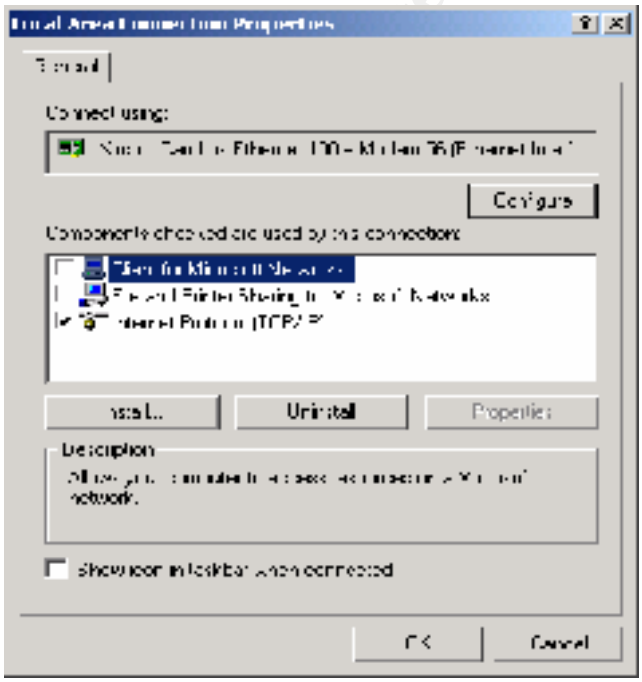
*Disable if DNS Name resolution is not needed

Netbios/SMB

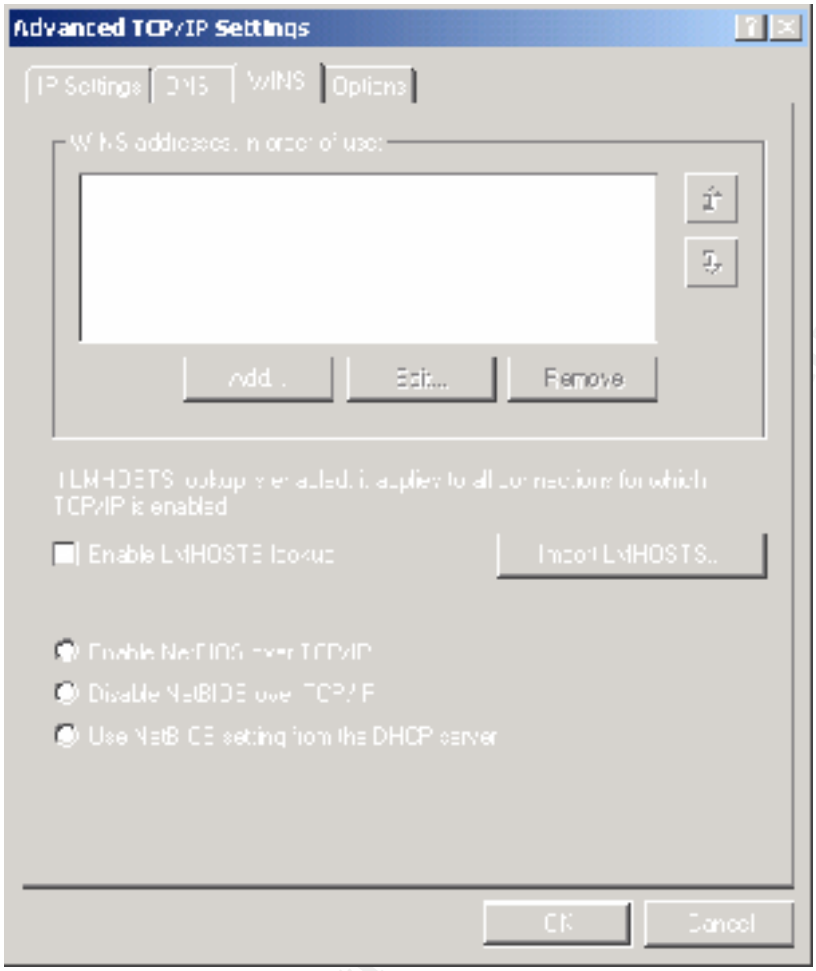
To disable direct host (445 using SMB) go to Computer Management → System Tools → Device Management → View → Show Hidden Devices → Non Plug and Play Drivers Go to NetBios over TCP/IP right click and disable. This will disable the direct host listener on port 445/tcp. (Windows 2000 uses 445 called direct host to do SMB without having to use netbios. IT uses port 445 instead of port 139 for communication.)



To disable Netbios over TCP/IP, right click on my network places and go to properties. Right click properties on local area connection. Uncheck Client for Microsoft Networks and File and Print Sharing for Microsoft Networks as shown in figure and click ok. This will disable Netbios and will disable access to the web server using file sharing.



You can also disable netbios over TCP/IP by going to Local Area Connection Properties and then go to TCP/IP and then advanced. Got to the wins tab and select disable Netbios over TCP/IP as shown in figure



Event Logs

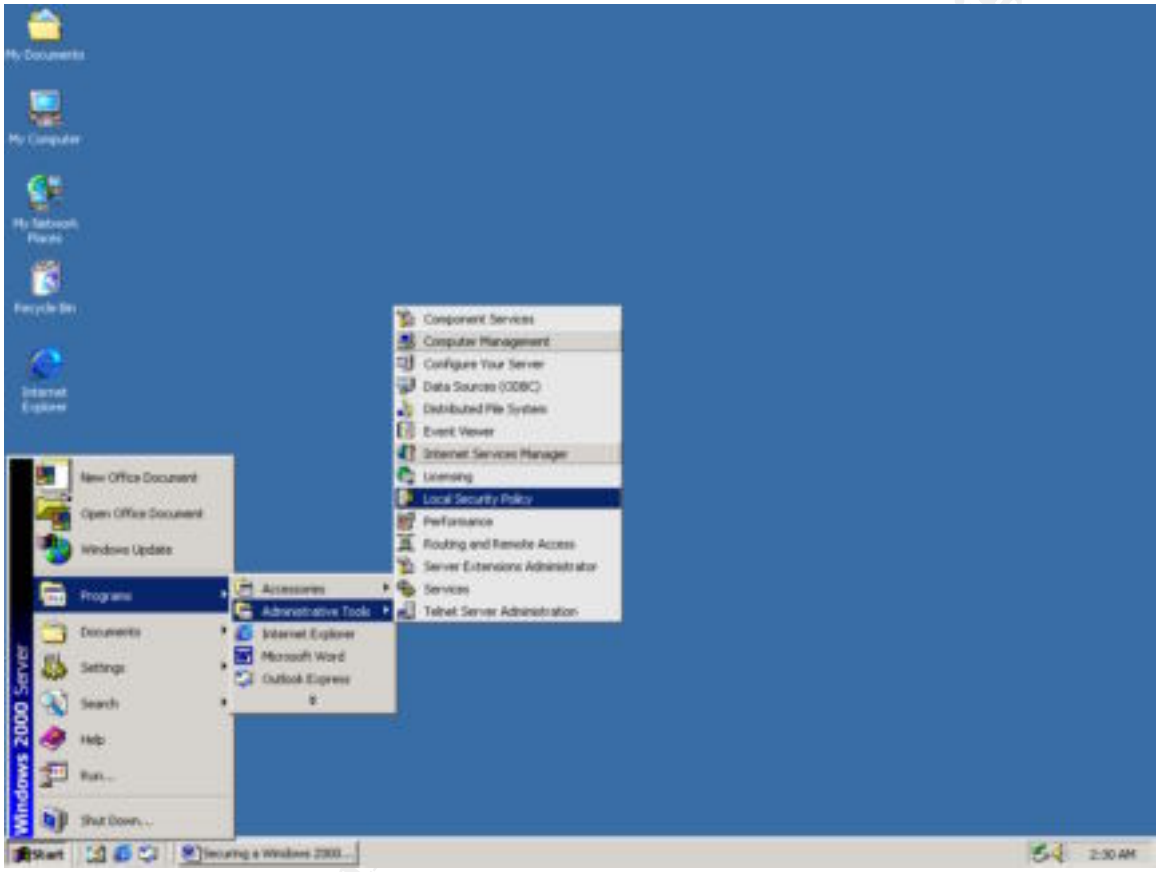
The event logs by default only log 512KB of events before they start to over write. I recommend that you make the event logs size at least 10MBif not 20MB. I would also recommend that you change the overwrite setting to 30 days. This will allow you to look at the logs up to a month back. To change this go to Computer Management, then event viewer. Right Click on each of the logs and set the size. You may also want to secure the event logs by changing permissions on the c:\winnt\system32\config\logname.evt. I recommend setting the access to administrators and local system to Full control and deny everyone else access. You can also change the location of the log files by changing the following registry keys.

- Applicaton Log HKEY LOCAL MACHINE \SYSTEM\CurrentControlSet\Services\Eventlog\Application
- System Log HKEY LOCAL MACHINE \SYSTEM\CurrentControlSet\Services\Eventlog\System

- Security log HKEY LOCAL MACHINE \SYSTEM\CurrentControlSet\Services\Eventlog\Security

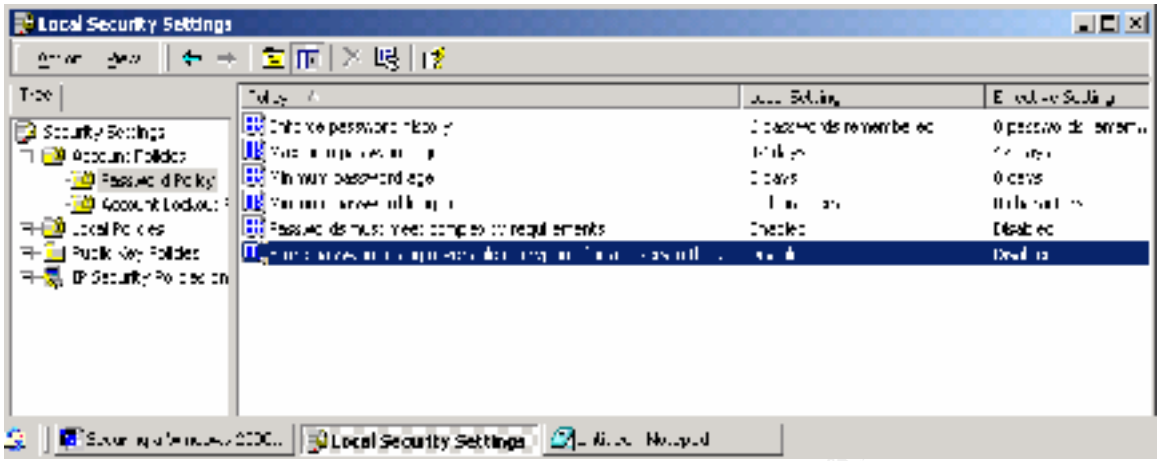
Audit and Policy Settings

Go to start → program files→ Administrative tools→ Local security policy



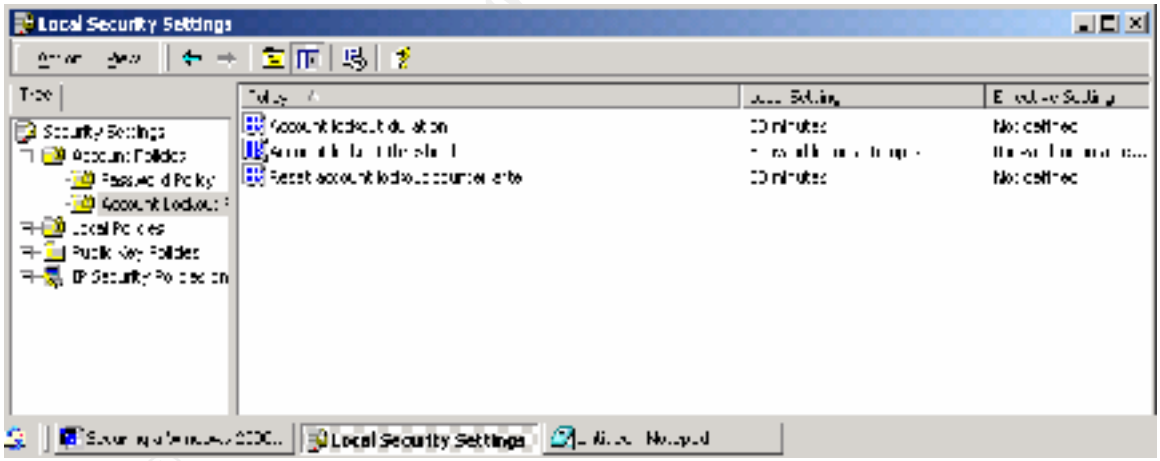
Go to password policy and set the following to your desired setting. I recommend enabling Passwords must meet complexity requirements. Below are the default setting and what I recommend.

Policy	Default Setting	Recommended setting
Enforce password history	0 passwords remembered	6 passwords remembered
Maximum password age	42 days	30 or 42 days
Minimum password age	0 days	0 days
Minimum password length	0 characters	10 or more characters
Passwords must meet complexity requirements	Disabled	Enabled
Store passwords using reversible encryption for all users in the domain	Disable	Disabled



Then go to account lockout policy. By default accounts will not lock out after bad logon attempts. This is a dangerous setting as hackers could keep banging away with cracking utilities until they crack the accounts. The lock out setting can help prevent that and make them work harder.

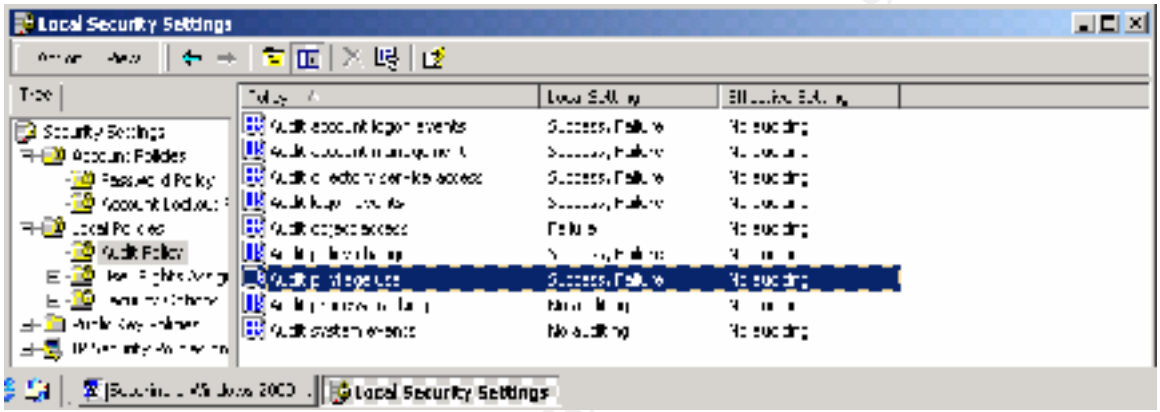
Policy	Default Setting	Recommended Setting
Account Lockout Duration	Not defined	30 minutes
Account Lockout Threshold	Account will not lock out	5 invalid logon attempts
Reset account lockout counter after	Not defined	30 minutes



Then go to local policies → Audit policy. I recommend auditing on everything except Audit systems events and audit process tracking. If you audit these events you security log can fill with events that are non-important. Auditing these events will give you enough information of people trying to break in. You can now track when security policies are changed and when people log on and off. This will leave you a very good audit trail latter on.

Policy	Default Setting	Recommended Setting

Audit account logon events	No auditing	Audit Success and Failure
Audit account management	No auditing	Audit Success and Failure
Audit directory service access	No auditing	Audit Success and Failure
Audit logon events	No auditing	Audit Success and Failure
Audit object access	No auditing	Audit Failure
Audit policy change	No auditing	Audit Success and Failure
Audit privilege use	No auditing	Audit Success and Failure
Audit process tracking	No auditing	No auditing
Audit system events	No auditing	No auditing

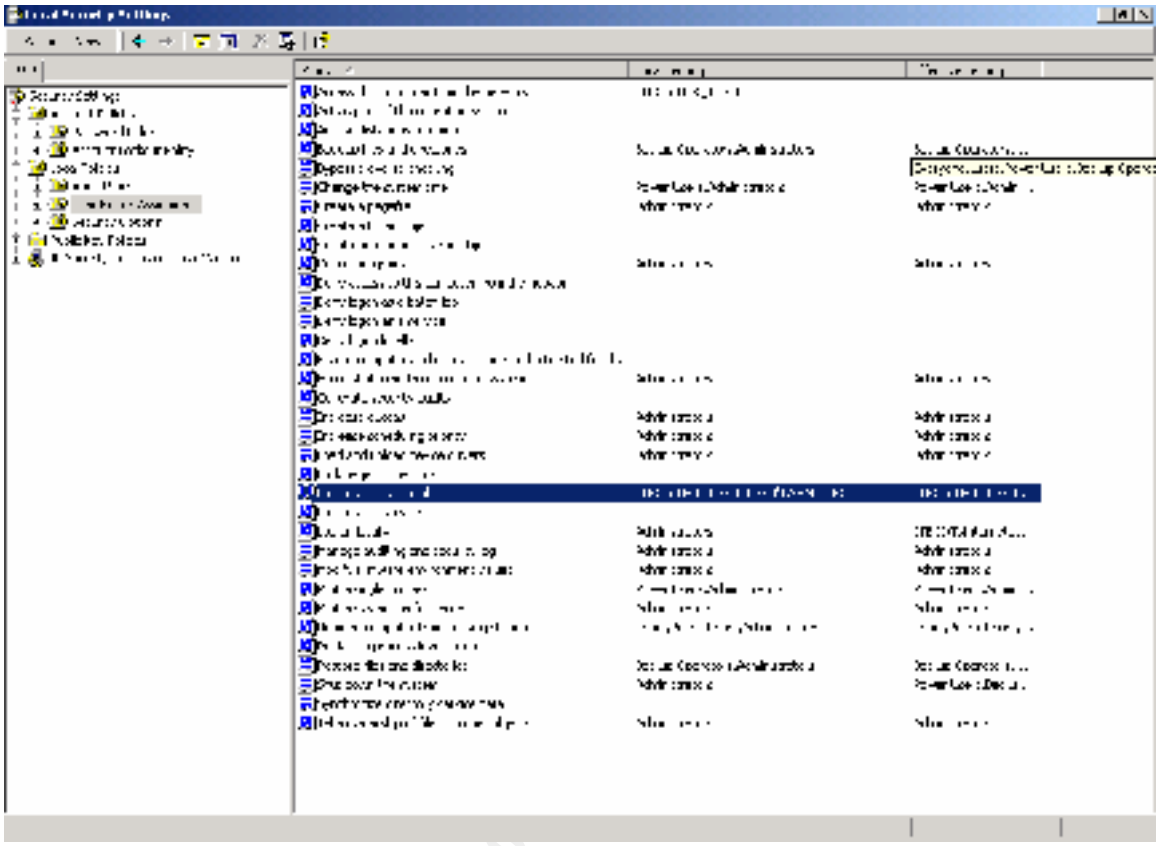


Users Rights Assignments

Then go to Users Rights Assignment as show in figure 2-B. I have listed below what rights to change. By default everyone can log on locally. This is dangerous as anyone could log on. Even Guest if it got enabled accidentally. I recommend that all users get removed except Webmasters and Administrative Users that need console access. The Access this computer from the network also has the everyone group in it by default. I recommend removing all user accounts except the anonymous user. If you have IIS control the anonymous users password, than you need to allow Access this Computer from the Network. If you don't allow IIS to control the password than you need to allow the anonymous user to log on Locally. I recommend having IIS control the password.

Policy	Default Setting	Recommend Setting
Access this Computer from the network	Everyone and all the default install Groups	Remove all users accounts and groups except the anonymous IIS user
Bypass transverse Checking	Everyone	Remove all user accounts
Log on locally	Everyone	Remove all accounts except User accounts that need to log on to the web server.
Shut down the system	Power Users, Backup Operators, Administrators	Remove all groups except administrators.

Figure 2-B



Security Options

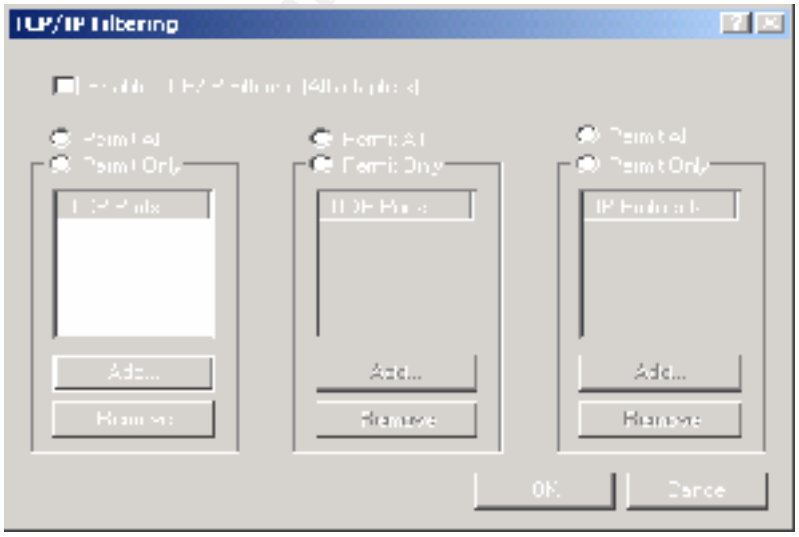
Go to start → program files→ Administrative tools→ Local security policy. Then go to Security options. Below I have listed the default setting and what the setting should be set to.

Policy	Default Setting	Recommended Setting
Additional restrictions for anonymous connections	None. Rely on Default permissions	Do not allow enumeration of SAM accounts and shares
Do not display last user name in logon screen	Disabled	Enabled
LAN Manager Authentication Level	Send LM & NTLM responses	Send NTLMv2 response only/refuse LM & NTLM
Message text for users attempting to log on	None	You choice EX (This system is subject to usage logging and monitoring. Authorized Access only)
Message tile for users attempting to log on	None	Warning!!!!!
Prevent System maintence of	Disabled	Enabled

computer account password		
Recovery Console: Allows automatic Administrative logon	Disabled	Enabled
Restrict CD-ROM access to locally logged-on user only	Disabled	Enabled
Restrict Floppy Access to locally logged-on user only	Disabled	Enabled

Packet Filtering

In Windows 2000 there are ways to control which ports users can access. You can right click on My Network Places → Go to Properties →Right click on Local Area Connection →Go to Properties→ Highlight TCP/IP Protocol and chick on properties→ Go to advanced settings and double click on TCP/IP Filtering. This will block all ports except what you have defined in the Permit only List. I recommend only Allowing Port 80 (HTTP), and if need 443 (SSL) and FTP (21). This will stop people from probing other ports.



Routing and Remote Access

You can also use the routing and remote access service to control packet filtering. I don't like to use this and I don't recommend it. You need to have the workstation service enabled to use it. It is also a service so if someone was able to crash the service or stop the service the benefits of Using Routing and Remote Access are defeated. I recommend using IPSEC policies instead. It is also another service that would need to be running.

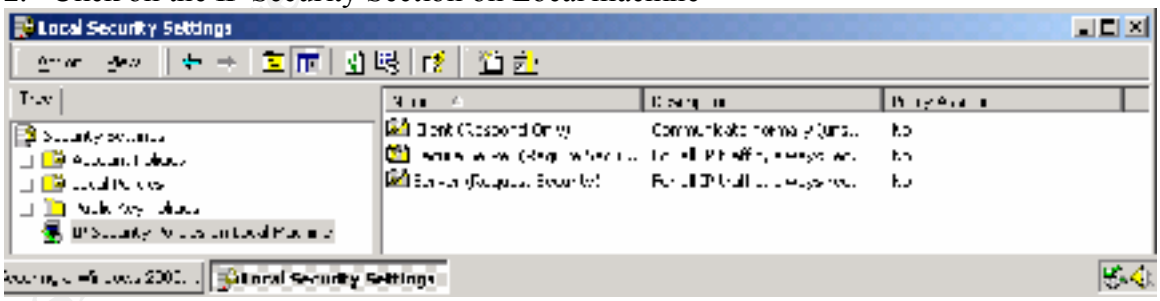
IPSEC Polices

IPSEC is the framework and a standard for IP Security. IPSEC provides an authenticated, secure channel with the following protocols and standards.

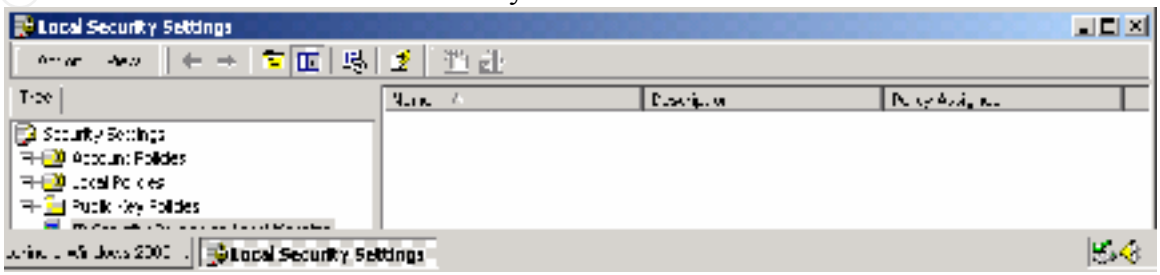
- Authentication using the Internet Key Exchange Protocol (IKE, RFC 2409)
- Integrity Protection using the Authentication Header (AH, RFC 2402)
- Encryption Using the Encapsulating Security Payload (ESP, RFC 2406)

Before two hosts can establish a secure connection they must authenticate one another. They negotiate a set of encryption parameters called a security association (SA). Windows 2000 uses IKE (Internet Key Exchange) to establish these parameters. IPSEC is a good way to secure the server, as the packet will be dropped even before it makes it up the OSI model, which makes it very secure. To set up an IPSEC policy you need to follow the steps below

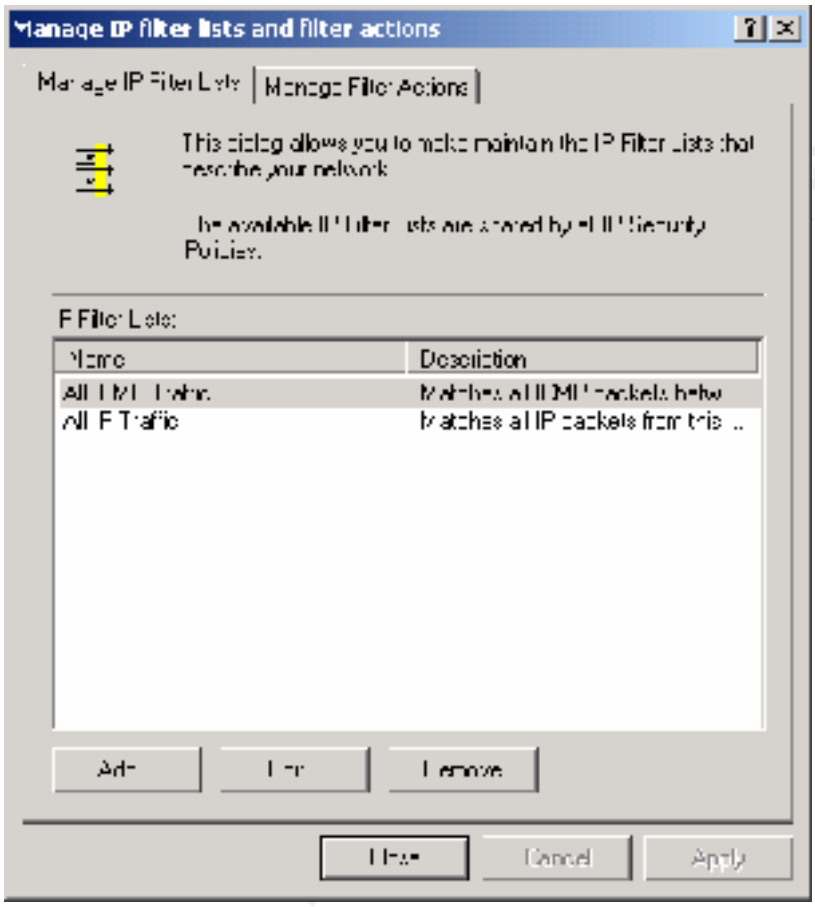
1. Go to Start → Program Files → Administrative Tools → Local Security Policy.
2. Click on the IP Security Section on Local machine



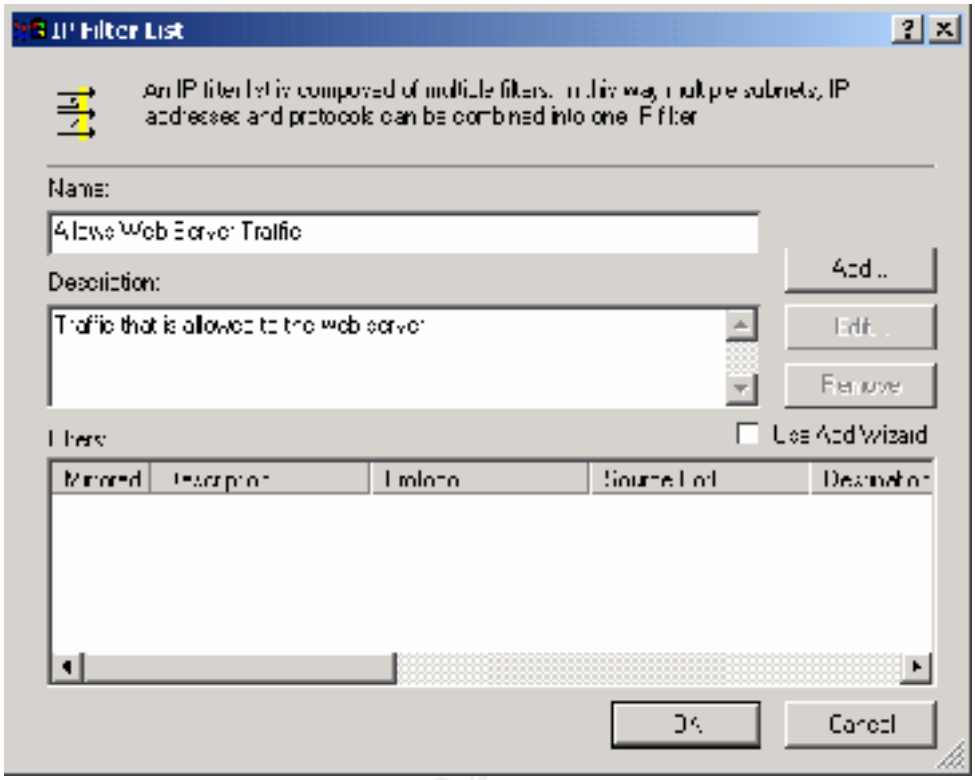
3. Remove the three default IP Security Polices.



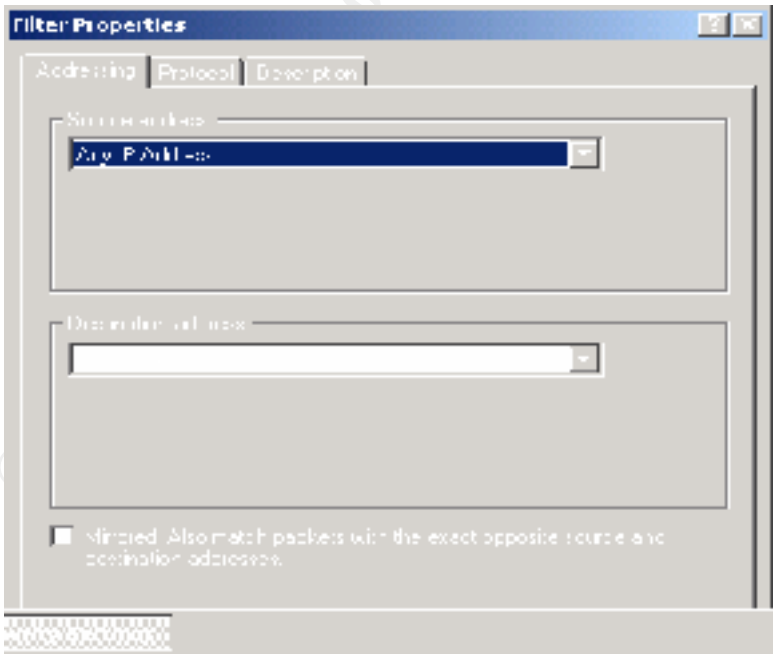
4. Right Click on IP Security Policies on the Local machine and select manage IP filter lists and filter actions.



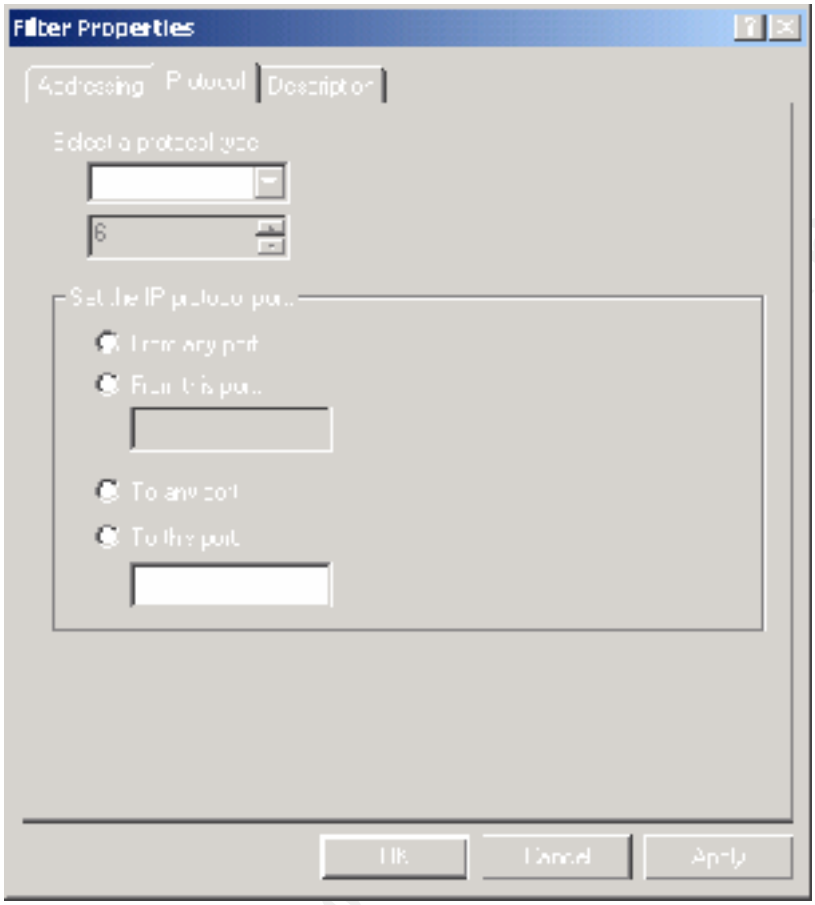
5. Create an IP Security Policy called allowed web server traffic and uncheck use add wizard.



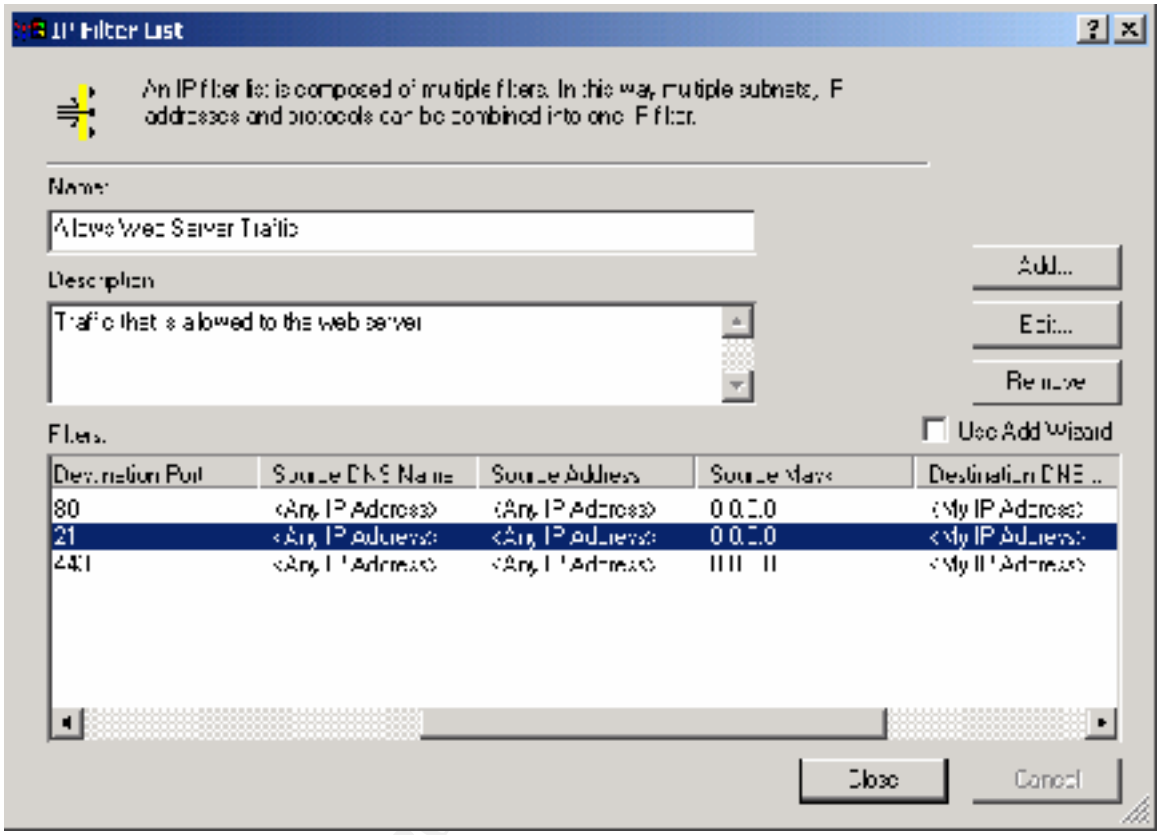
6. Click on add and select source address any IP address, destination IP address my IP address.



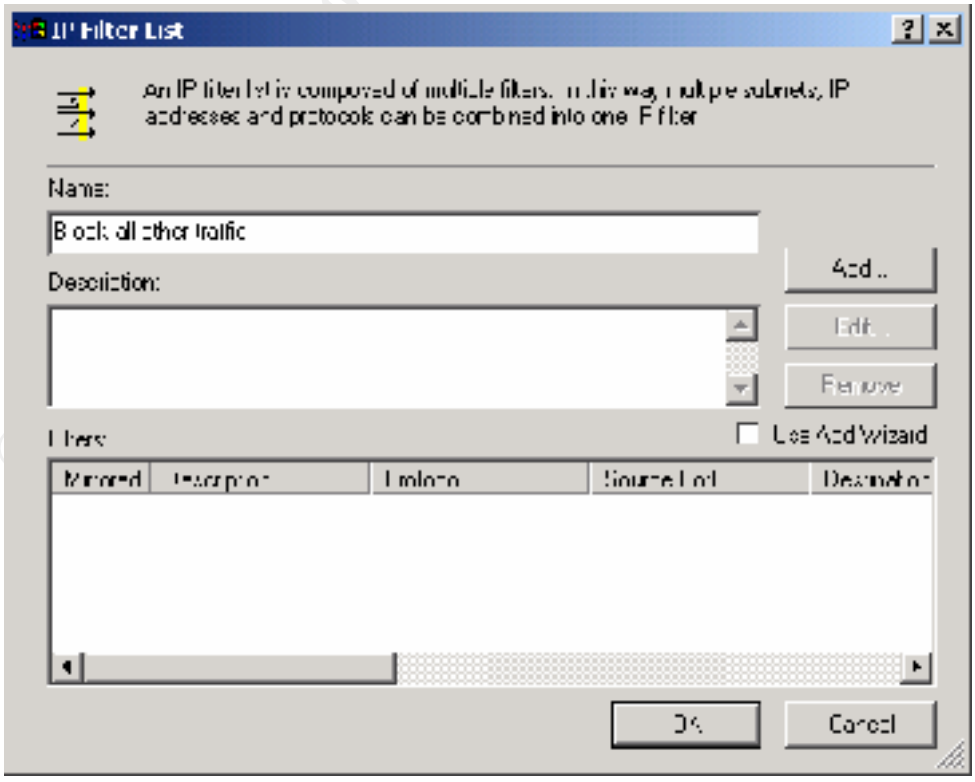
7. Go to protocol and Select TCP as the protocol type. Select from any IP port to local port 80. Repeat Steps 6 and 7 for FTP (TCP 21) and HTTPS (443).



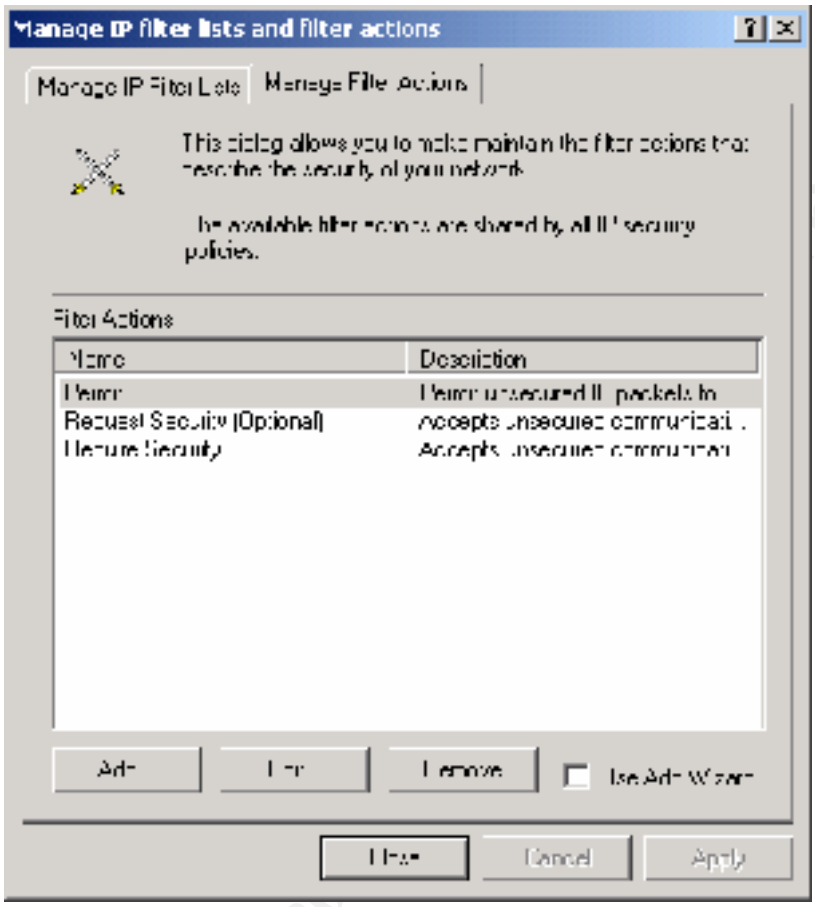
8. It should look like the example below. Click on close



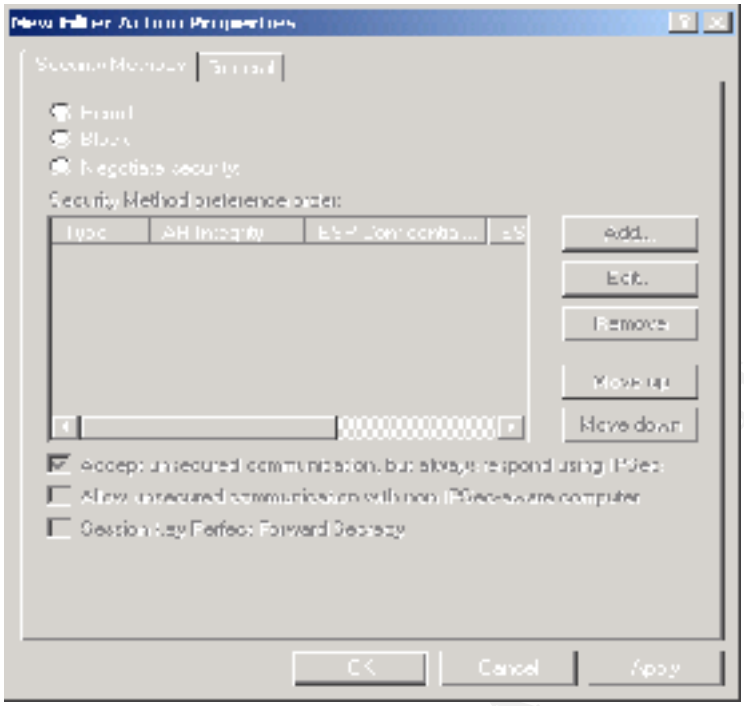
9. Click on add and Give this filter a name of block all other traffic



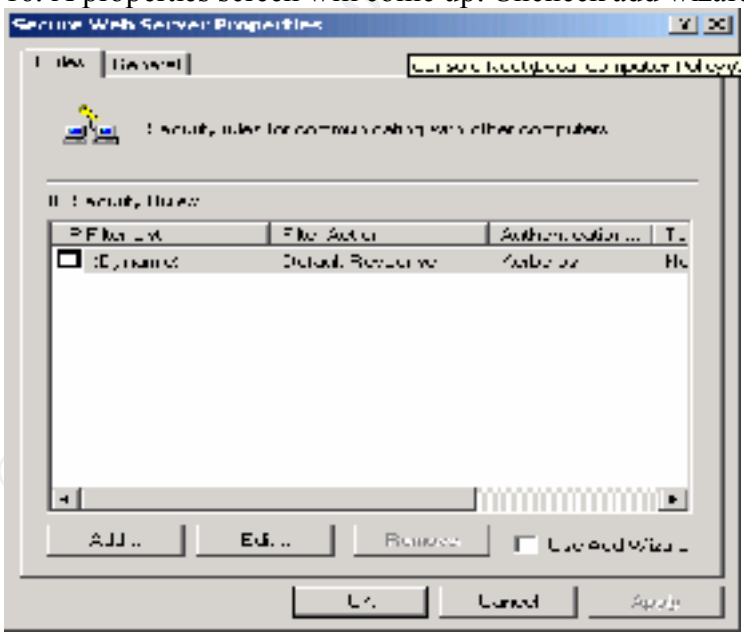
10. Go to manage filter actions, uncheck use add wizard and click on add.



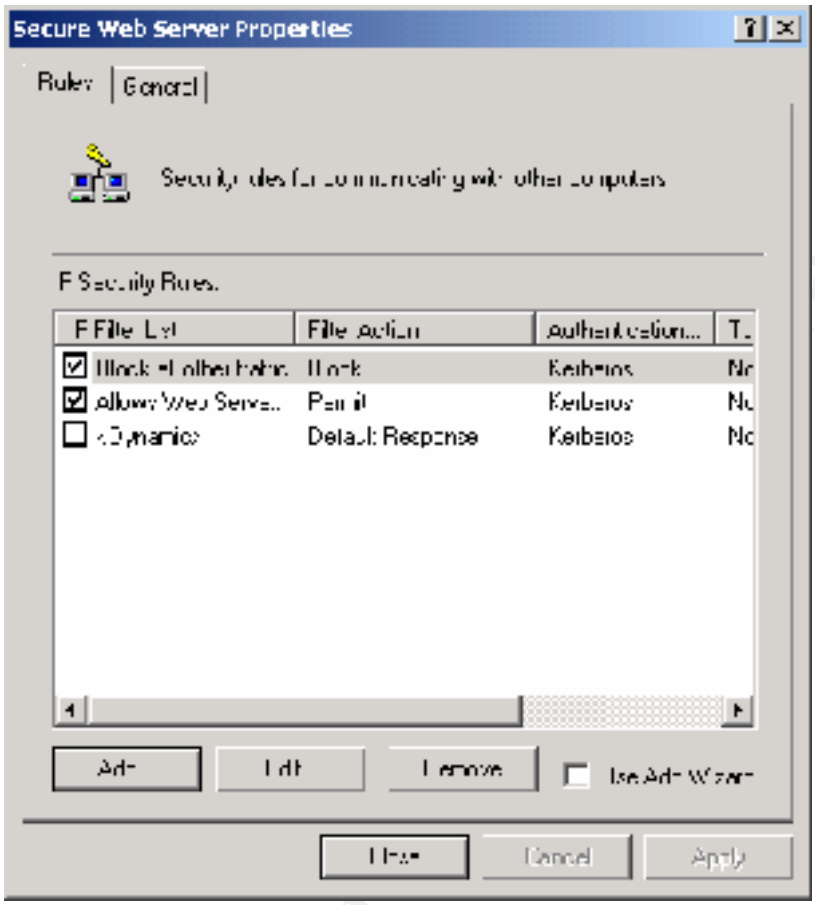
11. You need to create a block security policy. On the general tab give this filter name block. Then go to the security methods and select block. Then select ok. A permit policy is already defined.



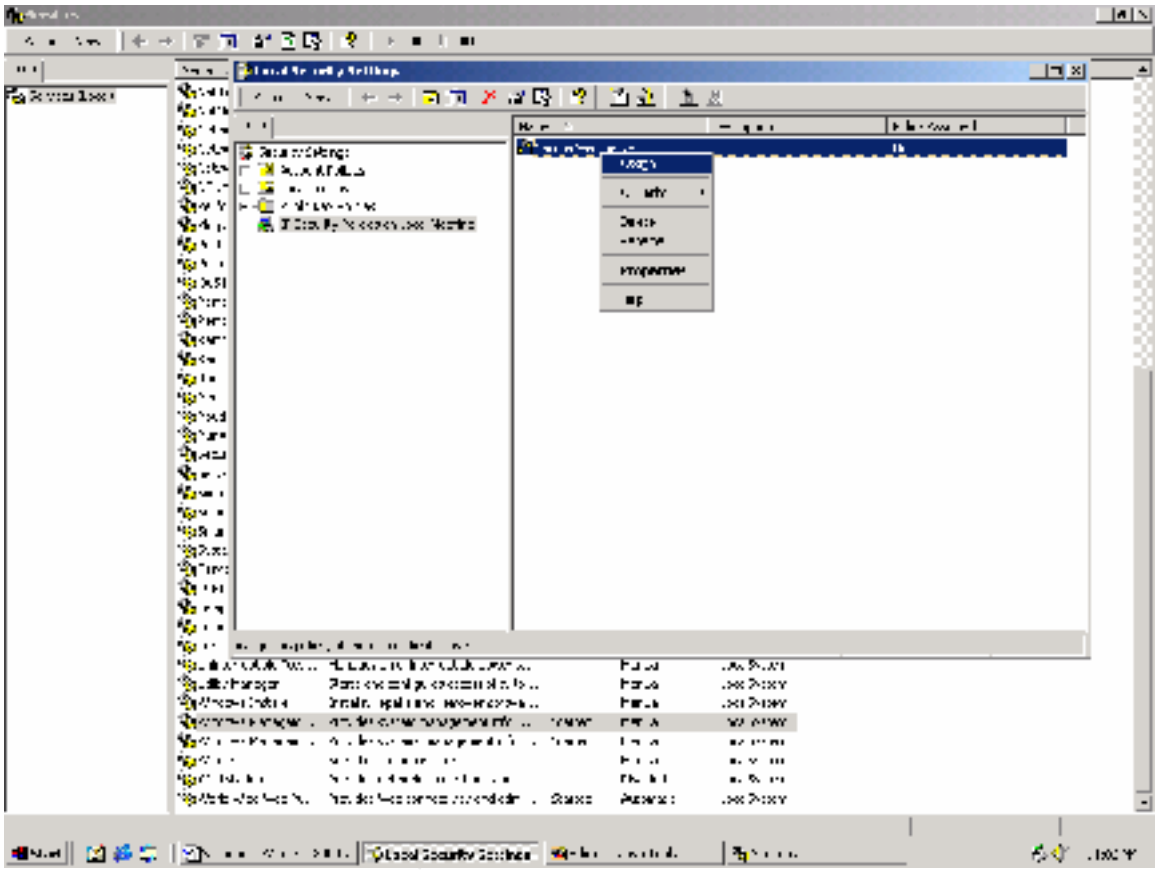
12. Right click on IP Security Policies on local machine and select create IP Security Policy.
13. A policy Wizard will come up. Select Next.
14. For an IP Security Policy Name Give It Secure Web Server. Select Next
15. Uncheck the Activate the default response rule and click next than finish.
16. A properties screen will come up. Uncheck add wizard and click on add



17. Go to the IP Filter list and Select Allows Web Server Traffic, then go to filter action and select permit. Then click on add. Click on add again and select block all other traffic. Then go to filter action and select block. Then select OK.



18. Then select close. Then Right Click on the Secure Web Server policy and Click Assign.



You now have a secure web server. Remember if you want to browse the web, ftp or do DNS lookups from the web server you need to make sure that you create a policy to allow that traffic out. By using an IP Sec Policy you also prevent some one from putting a listener on the web server and binding to a high port. You will still be vulnerable if the hacker binds it to port 80.

User Accounts

You should always rename the Administrator account. All hackers know that Administrator is the default admin account. I recommend renaming this account. Then create another account called administrator with no rights. This account is called the honey-pot or jail admin account. I also recommend creating user accounts for all administrative users and give them only the rights that they need. You could then come up with a very complex administrative password and lock it away until you need it. This will also let you create an audit trail of the administrative users. I also recommend that you create a new IIS anonymous user account. Again, all hackers know that the IIS anonymous account is IUSR_machine name. Leave the old anonymous account on the server but disable it. This will create a jail anonymous account. This is good practice and will go a long way in securing your web server.

Moving Dangerous File
Windows 2000 has some potentially dangerous files that are located in the system path. Examples of these files are tftp.exe, cmd.exe, etc. These files should be moved to a different folder with auditing enabled on the folder and with permissions for only administrators. I recommend creating a secure folder.

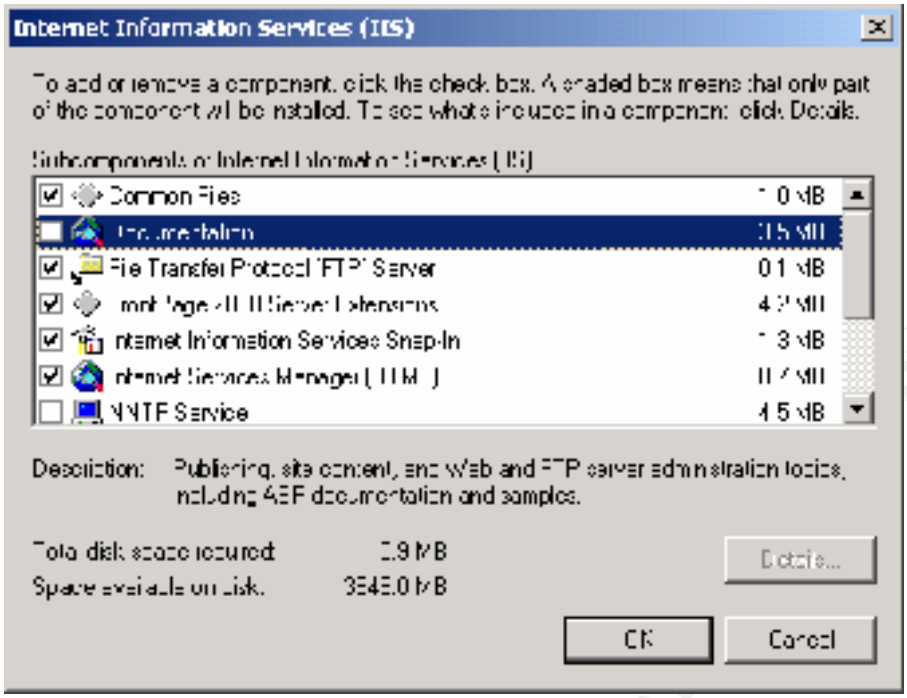
Here is a partial list of the dangerous files.

- At.exe
- Calcs.exe
- Cmd.exe
- Csript.exe
- ftp.exe
- tftp.exe
- regedit.exe
- regedit32.exe
- runas.exe
- nbtstat.exe
- telnet.exe
- net.exe

Securing IIS
The steps below will go threw the steps needed to secure IIS. A create document that will list some to most of these steps is at http://www.microsoft.com/technet/security/iis5chk.asp. This is a very good security checklist from Microsoft's web site.

Installation
The default install off IIS installs a bunch of services and samples applications. I recommend running IIS setup again and removing what you do not need. Go to start → setting → control panel → add/remove programs. Double click on add remove programs and go to add /remove windows components. Select Internet Information Services and click on details. I recommend removing the following,

- Documentation
- Internet Server Manager HTML (Could allow a hacker easy access to hack the web site)
- FrontPage server ext.
- SMTP service.

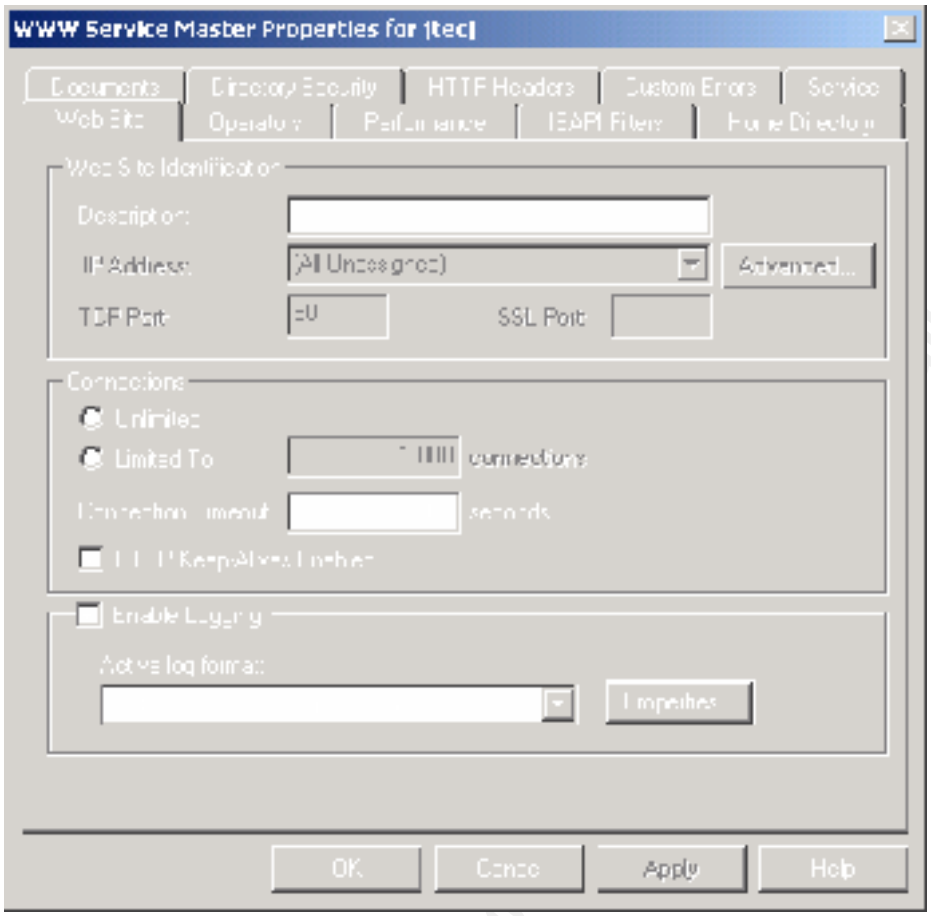


File security
Below is a table that outlines the file security needed on the web pages and scripts. Remember that some asp pages might need read and write.

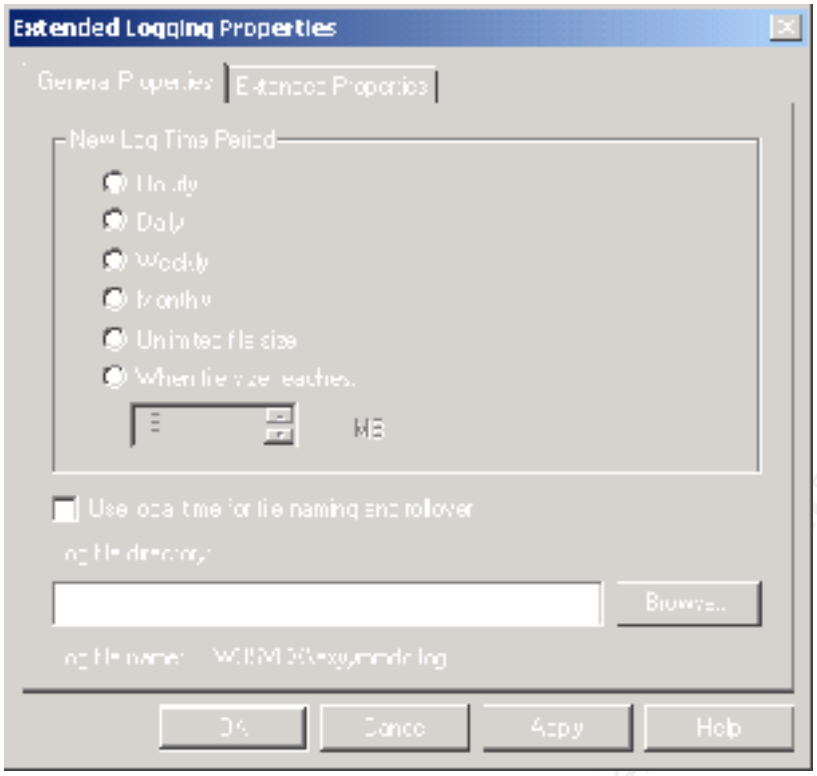
File Type	Access Control Lists
CGI (exe dll cmd pl)	Administrators and System (Full Control) System (Full Control) Everyone (Read)
Script files (asp)	Administrators and System (Full Control) System (Full Control) Everyone (Read)
Static files (html, htm, gif, jpeg)	Administrators and System (Full Control) System (Full Control) Everyone (Read)

A better option would be to creating directories for the different files types and but the ACLs on the directory. EX (d:\inetpub\wwwroot\script, d:\inetpub\wwwroot\static)

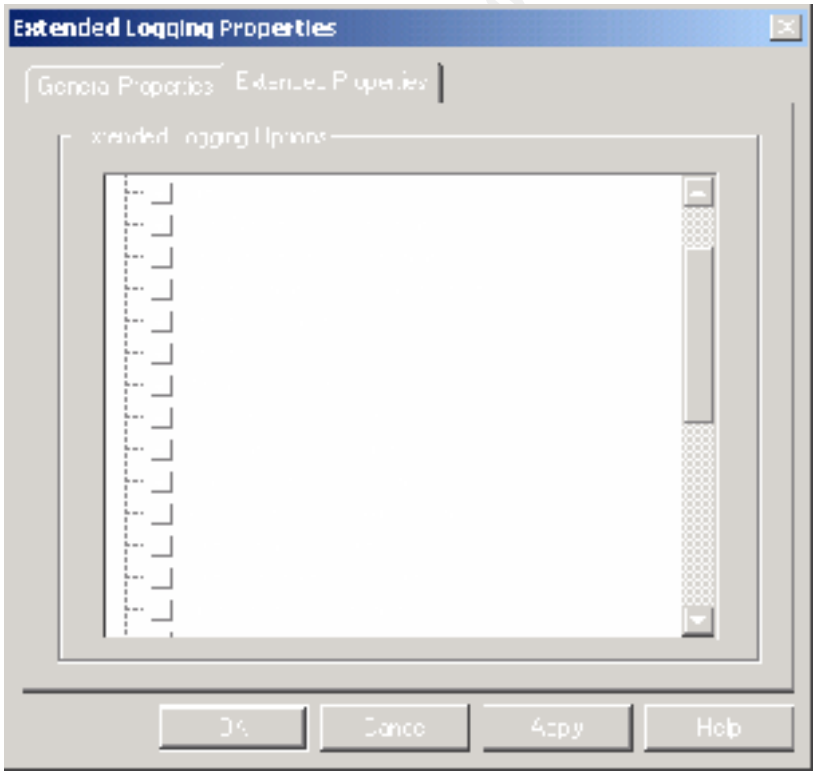
Log Files
Log files are written to %systemroot%\system32\Logfiles. I like to move these files to a different drive. This keeps them off the operating system drive and prevents the hacker from easily removing or modifying the log files. Do change the directory open the Internet Information Services and got to the name of your web server and click on properties.



Go to the active log format and click on properties.



Change the log file directory. You can enable additional logging by going to the extended properties tab. I recommend turning on bytes send and received.



Sample Applications
IIS comes default with some sample applications and documentation installed. These sample applications and documentation have been known to have bugs and reveal information. I recommend removing the sample applications. Below are the paths to the sample applications. I suggest deleting these directories.

- IIS Samples- C:\inetpub\iissamples
- IIS documentation- c:\winnt\help\iishelp
- Data Access – c:\program files\common files\system\msadc
- Admin Scripts – c:\inetpub\admin scripts.

Default Web Site
I recommend removing the default web site and creating a new web site. The default web site has been known to have a bunch off vulnerabilities in it. It is better to create a new web site.

Remove the IISADMPWD Virtual Directory
The IISADMPWD allows users to change passwords. This is dangerous as it could allow someone to try and change your admin password. I recommend removing this virtual directory.

Script mappings
IIS by default has a bunch of script mappings enable. I recommend removing the script mapping you do not need. To remove these script mappings

1. Right-Click the the root of the web site and choose properties
2. Click the home directory tab
3. Click Configuration
4. Remove the mappings that you do not want.

Bellow is a list of the script mappings.

If you don not need this	Then remove this
Web password reset	.htr
Internet Database connector	.idc
Internet printing	.printer
Index Server	.ida .idq .htw
Server Side Includes	.stm, .shtm, shtml
Certificate Request	.cer
Active Server Pages	.asp .asa

Parent Paths
The Parent Paths option allows you to use ".." in calls to functions such as *MapPath*. By default, this option is enabled, and you should disable it. Follow this procedure to disable the option:

1. Right-click the root of the web site, and choose properties

2. Click the Home Directory tab.
3. Click Configuration.
4. Click the App Options tab.
5. Uncheck the Enable Parent Paths check box.

Web Server Root Directory
By default the web server's root directory is c:\inetpub\wwwroot. I recommend that you move this path to a different volume. This would prevent someone from jumping off this directory to get to the root of the OS.

FTP Service
If you use the FTP service to update your website you might want to use IP address restrictions on the ftp site. To get to IP address restrictions go to the FTP site and right click and go to properties. Then go to directory security. Put only the addresses needed to update the web site.

Maintaining Security
To maintain security on the web site you need to setup good policies and procedures. Some examples of policies and procedures are backup polices, polices when the web site gets hacked. If you put polices in place early, you can avoid disaster latter.

Security Scan
Run a third party tool like IIS Internet Scanner to get a look at the security from the Internet. This would allow you to test your web server for over 800 vulnerabilities and to fix any holes that are left open. This scan should be run yearly if not quarterly to check against any new security developments.

Intrusion Detection
Consider getting an intrusion detection system. This system could provide you with an early warning alarm of someone trying to hack you. You can get two types of IDS systems, host based and network based. You might want to consider both for extra protection. Some IDS systems even work with firewalls changing firewall rules to block access.

Security Mailing Lists
Consider subscribing to security related mailing lists to keep on top of the latest developments. Here is are some links to mailing lists

- www.ntbugtraq.com
- www.securityfocus.com
- www.microsoft.com/security
- http://www.securityfocus.com

Web Server Placement
If you are running a public web site you should consider putting it in a DMZ. A DMZ is a packet screened and filtered subnet. When you put your web server on the DMZ you can

limit the services coming in to the DMZ to what is needed to access the web site. You can also limit what goes out from the DMZ. This will prevent a hacker from using the web server to jump into the production network. It will also limit were a hacker can go and prevent him from using you server to hack other Internet web servers.

References:

1. Securing Windows NT/2000 Servers for the Internet by Stefan Norberg, O'Reilly ISBN 1-56592-768-0

2. Microsoft TechNet Security Web Site, http://www.microsoft.com/technet/security/default.asp

3. Hacking Exposed 2nd Edition by Joel Scambray, Stuart McClure, George Kurtz, Osborne ISBN 0-07-212748-1

4. Securing Internet Information Server 5.0 by Jason Fossen, SANS Institute