Global Information Assurance Certification Paper

Securing Windows 2000 Server Step-by-Step from an "out-of-the-box" to an "Internet Ready" Configuration.

Author: Alicia Laing
Date: March 28, 2001

Introduction:

This paper was written to fulfill the practical requirement for the SANS GIAC Certified Windows Security Administrator certification.

Windows 2000 "out-of-the-box" is not secure to be configured for connection to the Internet. In order to secure your windows 2000 server there are a series of configuration steps to follow. These security steps pertain to Windows 2000 as a Web Server ready for the Internet.

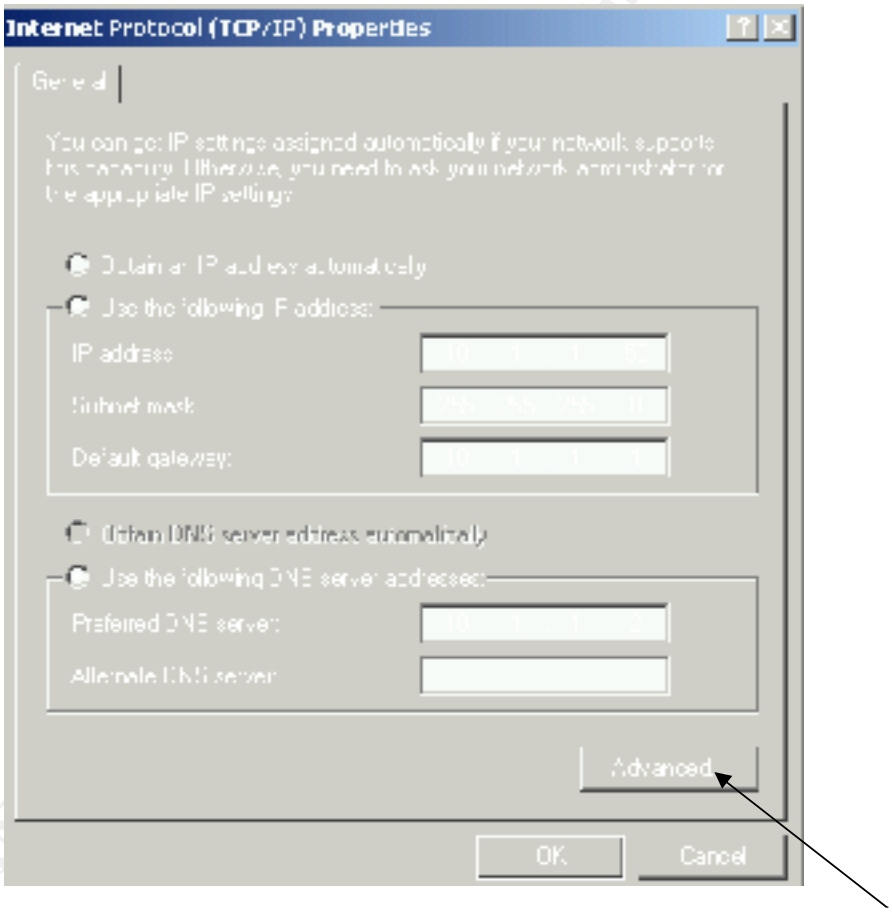
The first security measure is physical security followed by the proper hardening of the Operating System during the initial install. I will make the presumption that this machine is in a secure place, locked away in a room or closet.

Initial Install of Win2k Server:

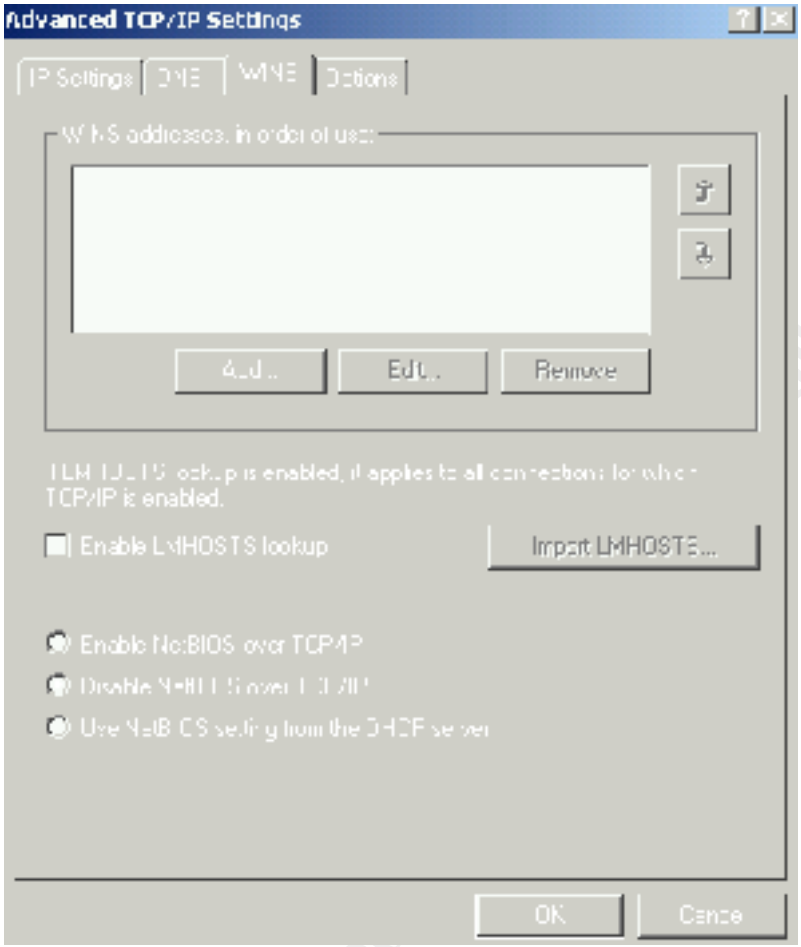
- Install the Operating System from scratch, being that this is mainly for security you should not upgrade from a previous version of Windows NT.
- The installation process begins with the regular routine displaying a number of screens about licensing etc. Accept the defaults they are the standard screens, which are easy to follow.
- At the disk configuration make sure that your hard disk is partitioned in at least 2 partitions, one for the system and OS files and the other for your application and data files. This is to avert applications from accidentally or purposefully accessing the system files.
- Make sure that all your disks are formatted as NTFS. If you choose to format it later, type *convert [drive:] /fs: ntfs* at the command prompt.
- Configure your proper regional settings (e.g. eastern or pacific time zones.) for it is important for the logs. Type your name, company and the license mode, if it is per seat or per server. It is suggested to configure the server for per seat with a large number; if you wish you could always change it to per server at later time.
- Give the computer a name and a difficult password, because it is consequential to choose a strong password for the Administrator.
- At the Windows 2000 components screen you are to uncheck all the options so that the server is at a

minimum install. We will add components as needed at a subsequent time.

- At the Network Settings dialog box you would want to choose custom settings and only select Client for Microsoft Network (we will be running IIS, which needs this to start) and Internet Protocol (TCP/IP). Click on the properties of TCP/IP; assign a static IP address, subnet mask, gateway and DNS server. Click on Advanced to setup the DNS and WINS for your nic.



- Disable NetBIOS over TCP/IP and uncheck enable LMHOSTS lookup on your WINS settings, seen here.



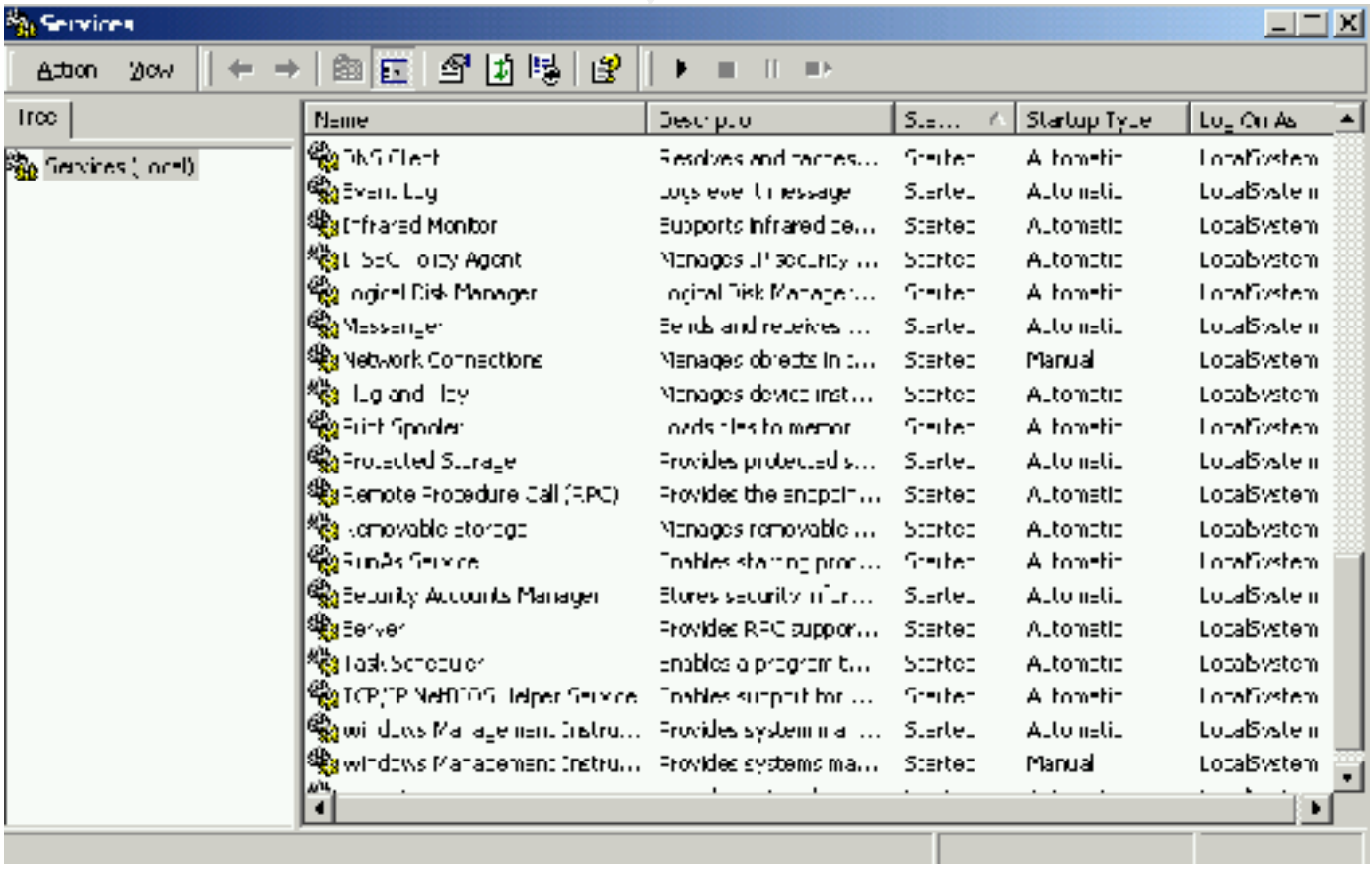
- For security purposes it is wise to configure this machine as part of a workgroup. If the server needs to communicate with other hosts, setup a DMZ where the machine is in a separate domain apart from your trusted network.
- The installation is just about finished you will be required to reboot.

Configure Services:

Disable services on Windows 2000 that you don't need or will not use, to prevent hackers or crackers from capitalizing on any faults those services may contain. To disable the startup options and the account under which the service is running, go to Start/Programs/Administrative Tools/Services. The Local System account is the default way a service is run and basically it has an advantage to the entire system.

Warranted that the services listed are running and started automatically.

- DNS Client
- EventLog
- IPSec Policy Agent
- Logical Disk Manger
- Network Connections Manager
- Plug and Play
- Protected Storage
- Remote Procedure Call
- RunAs Service
- Security Accounts Manager
- Task Scheduler
- Windows Management Instrumentation
- Windows Management Instrumentation Driver Extensions.
- Server
- Workstation

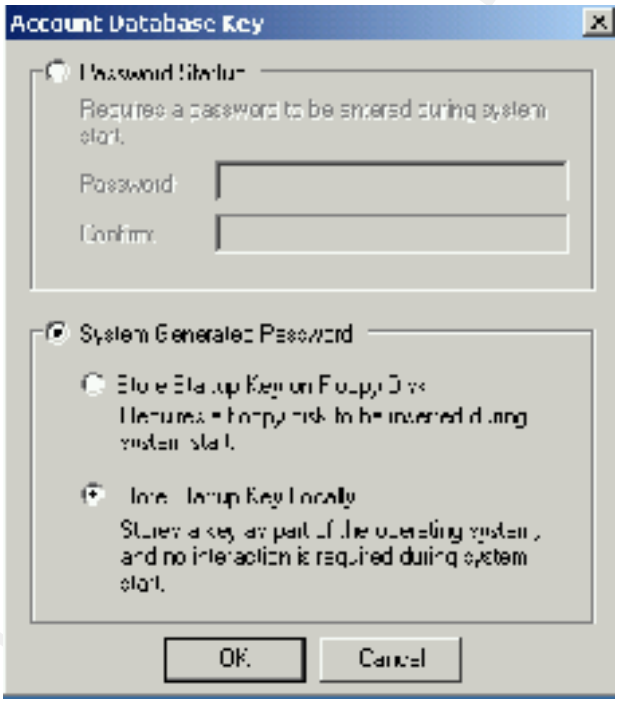


The best rule to secure systems is to disable all services that you are not using, so that if you need them at a later

time you could easily enable them. Also services should be run under an inferior account that can be used to validate to the system like a local account.

Protecting the SAM Database:

The local Sam database is encrypted by default using a locally stored startup key. The encryption cannot be disabled, but it can be configured to require a password or prompt for a floppy diskette. This is a problem with how Windows 2000 stores it in the registry, so it is best to reconfigure Syskey (this will require user intervention at start up). Type Syskey at the command prompt to then update that option.



System Policy:

Using Local System Policy tool to set policies for the local machine. Go to Start/Programs/Administrative Tools/Local Security Policy. This is where you would set the Password Policies, Account Lockout Policies, Audit Policies, User rights, security options etc.

Password Policy:

Configure the following to ensure strong password protection.

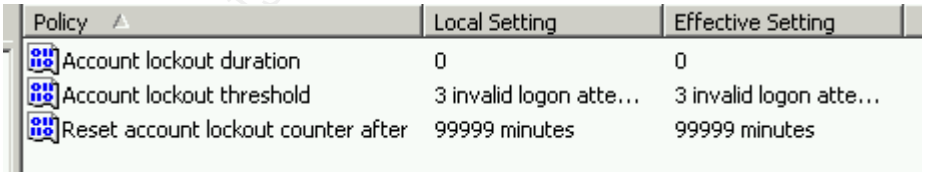
- Enforce Password History; the endorsed value is 5 to prevent passwords from being used repeatedly.
- Maximum Password Age, the recommended value is 60 days. Users are required to change passwords every 60 days, if not the account will be locked out.
- Minimum Password Age, the value should be 5.
- Minimum Password length, the value should be 8 characters. Making the password longer makes it harder to crack.
- Passwords Must Meet Complexity Requirement, this should be enabled. The passwords must be complex, so there should be a mixture of special characters, numbers, and upper and lowercase letters.
- Store passwords using reversible encryption, this should be disabled. If enabled anyone with the highest privilege of Admin can see the password.

Policy	Local Setting	Effective Setting
Enforce password history	5 passwords remembered	5 passwords remem...
Maximum password age	60 days	60 days
Minimum password age	5 days	5 days
Minimum password length	8 characters	8 characters
Passwords must meet complexity r...	Enabled	Enabled
Store password using reversible e...	Disabled	Disabled

Account Lockout Policies:

This should be configured to enable account lockout.

- Account Lockout Threshold. This should be enabled. Once enabled 3 incorrect login attempts will lockout the user.
- Account Lockout Duration. Enabled with a value of 0 such that the Administrator must un-lock the user's account.
- Reset Account Lockout Threshold after 99999 minutes.



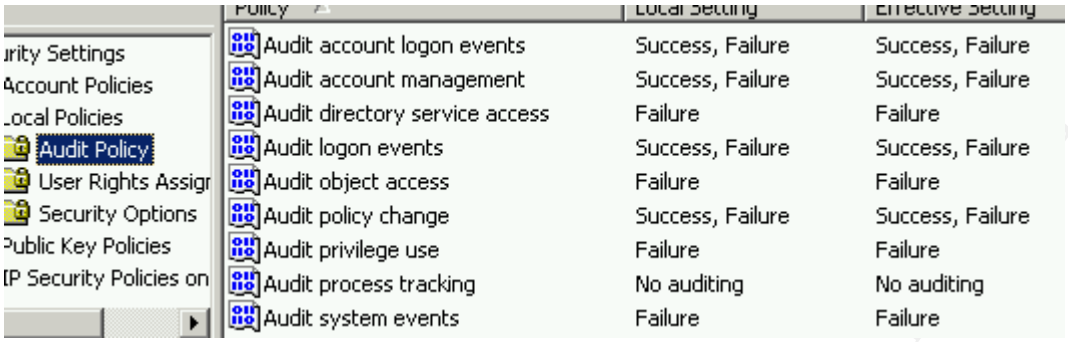
Policy	Local Setting	Effective Setting
Account lockout duration	0	0
Account lockout threshold	3 invalid logon atte...	3 invalid logon atte...
Reset account lockout counter after	99999 minutes	99999 minutes

Audit Policy:

At a minimum you should audit a few events, the success and failures for these policies.

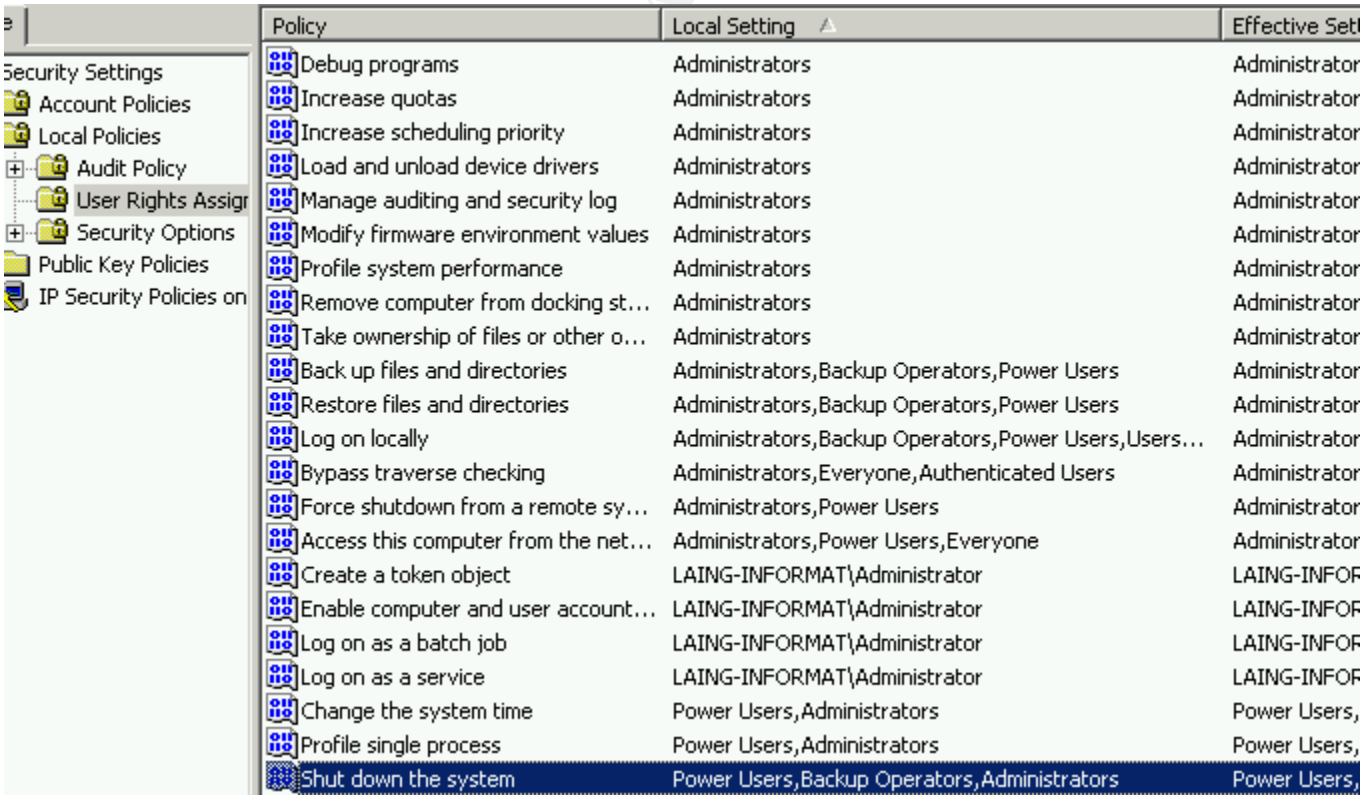
- Audit Account Logon Events
- Audit Account Management
- Audit Logon Events
- Audit Policy change

- Audit System Events



User Rights:

Configure the following options for user rights; take note of the users and groups who will be performing some action on the system. Administrator should be in most of them. The settings below should be applied in a secure environment.



Security Options:

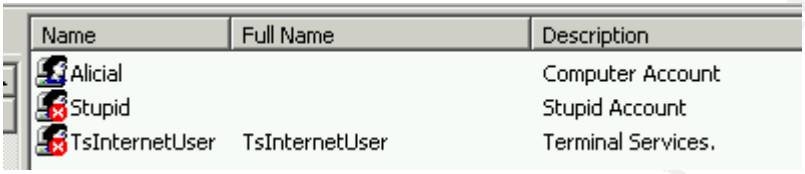
These security policy settings create and set registry keys. Apply all of these settings appropriately for your secure environment.

Policy	Local Setting	Effective Setting
Additional restrictions for anonymous connecti...	No access without e...	No access without e...
Allow server operators to schedule tasks (do...	Disabled	Disabled
Allow system to be shut down without having ...	Disabled	Disabled
Allowed to eject removable NTFS media	Administrators	Administrators
Amount of idle time required before disconnec...	15 minutes	15 minutes
Audit the access of global system objects	Disabled	Disabled
Audit use of Backup and Restore privilege	Enabled	Enabled
Automatically log off users when logon time e...	Enabled	Enabled
Clear virtual memory pagefile when system sh...	Enabled	Enabled
Digitally sign client communication (always)	Enabled	Enabled
Digitally sign client communication (when possi...	Enabled	Enabled
Digitally sign server communication (always)	Enabled	Enabled
Digitally sign server communication (when pos...	Disabled	Disabled
Disable CTRL+ALT+DEL requirement for logon	Disabled	Disabled
Do not display last user name in logon screen	Disabled	Disabled
LAN Manager Authentication Level	Send LM & NTLM re...	Send LM & NTLM re...
Message text for users attempting to log on	This is a Secure Net...	This is a Secure Net...
Message title for users attempting to log on	Authorized Users Only	Authorized Users Only
Number of previous logons to cache (in case d...	0 logons	0 logons
Prevent system maintenance of computer acc...	Disabled	Disabled
Prevent users from installing printer drivers	Enabled	Enabled
Prompt user to change password before expir...	14 days	14 days
Recovery Console: Allow automatic administra...	Disabled	Disabled
Recovery Console: Allow floppy copy and acc...	Disabled	Disabled
Rename administrator account	Not defined	Not defined
Rename guest account	Not defined	Not defined
Restrict CD-ROM access to locally logged-on u...	Enabled	Enabled
Restrict floppy access to locally logged-on use...	Enabled	Enabled
Secure channel: Digitally encrypt or sign secur...	Enabled	Enabled
Secure channel: Digitally encrypt secure chan...	Enabled	Enabled
Secure channel: Digitally sign secure channel ...	Enabled	Enabled
Secure channel: Require strong (Windows 20...	Disabled	Disabled
Send unencrypted password to connect to thi...	Disabled	Disabled
Shut down system immediately if unable to log...	Enabled	Enabled
Smart card removal behavior	No Action	No Action
Strengthen default permissions of global syst...	Enabled	Enabled
Unsigned driver installation behavior	Do not allow installa...	Do not allow installa...
Unsigned non-driver installation behavior	Do not allow installa...	Do not allow installa...

Account Policy:

These polices are set for logon security. Three default users are created when Windows 2000 is installed: Administrator, Guest, and TSInternetUser. The

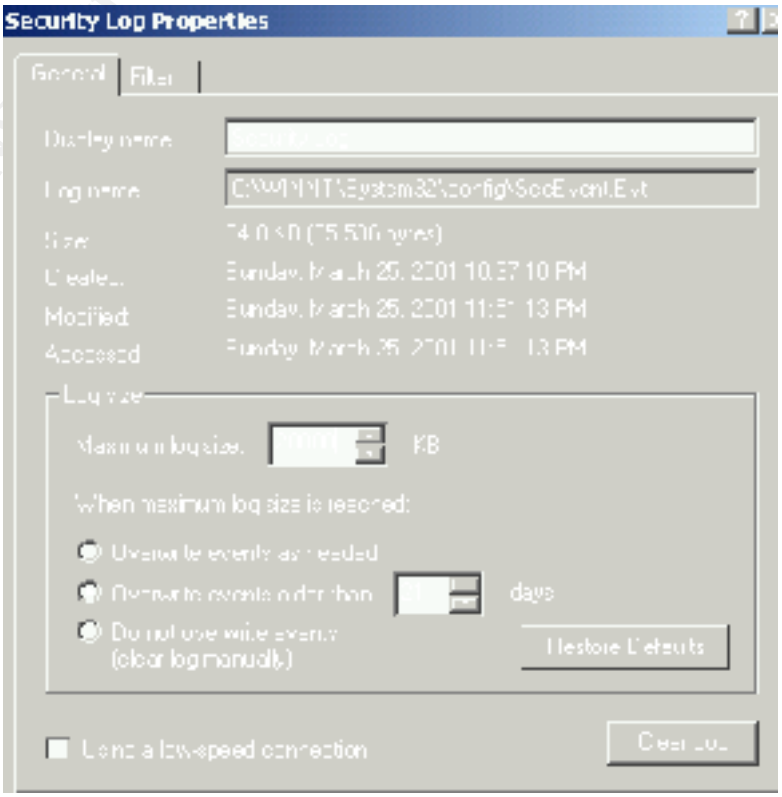
Administrator account should be renamed. Going to Start/Programs/Administrative Tools/ Local Security Settings/Security options can do this. Click on Rename Administrator account; this provides protection from hackers easily recognizing your Administrator account. The Guest account is disabled by default, and it can also be renamed as suggested above, and a password should be set for that account. The TSInternetUser account is for terminal services, to remotely run applications on the server, it should also be disabled because we are not using it. See below, I renamed the Administrator account to Alicial and I renamed the Guess account to Stupid. All accounts have been disabled.



Event Log Settings:

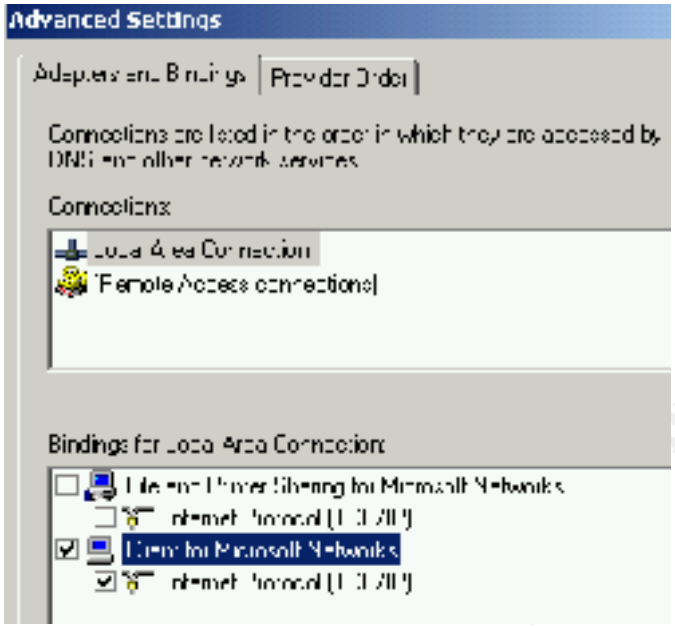
After the series of auditing are enabled, you need to make sure that adequate space is available. Now it's time to configure the log size. Go to Start/Programs/Administrative Tools/Event Viewer/(Application, System, and Security Log) and then right click on the log and click on properties. Log Settings recommendations for Web Server:

- Log-Size: Security Log = 2-4MB, System Log = 1-2MB, Application Log = 1-2MB.
- Log Overwrite: Security Log = older than 21 days, System Log = older than 14 days and Application Log = as necessary.



Unbinding Services:

To unbind services go into Network and Dial-up connections and click on local area network. This is done through the start/setting menu. Next highlight Local Area Network and click on Advanced/Advanced Settings, then clear the checkboxes with the network services.

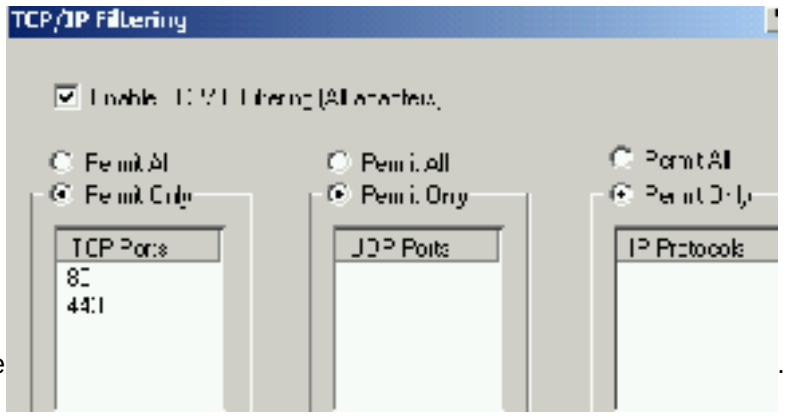


This configuration is for a web server. In order for IIS to run "Client for Microsoft Networks" should also be checked, because it needs NTLM SSP (NT/LanMan Security Support Provider).

TCP/IP Security Settings:

Access control on incoming networks to windows 2000 servers is another security issue. TCP/IP filters and IPSec filters are two ways to perform access control on an incoming network connection.

- Setting up TCP/IP filtering go to Start/Network and dial-up connections/ Local area connection / TCP/IP / Properties/Advanced/Options/ TCP/IP Filtering/Properties. As shown below, all inbound TCP connections to ports 80(http) 443(https), no UDP and IP ports allowed.



IPSec Filtering: This is managed from the local security policy; you will need to add the IPSec filter lists, filter actions, and policy rules. Create a policy say for Web server and then add IPSec filter actions to the policy so that traffic will be monitored. Once the policy is created you could right click and assign the policy to filter packets.

An alternative to filtering traffic is to install a firewall that will block any access to unauthorized ports and only allow packets for authorized ports. You could try third part firewalls such as ZoneAlarm (http://www.zonelabs.com), which is free for personal use, but there is a fee for business use or BlackICE defender (http://www.networkice.com). You could also check Microsoft website for other well-known full feature firewall vendors. (e.g. Checkpoint, Cisco, Gauntlet, etc.)

Tightening TCP/IP Network Attacks:

Change Registry settings to increase resistance of the NT stack for maximum protection from denial of service attack.

Warning:

Inappropriate change of the registry can cause serious problems that may result in the need to re-install your operating system. Please refer to Microsoft knowledge Base about how to edit the registry.

SynAttackProtect: This will reduce the time the system will wait for SYN-ACKs and safekeeping itself in the mean time.

Hive:	HKEY_LOCAL_MACHINE
Key:	System\CurrentControlSet\Services\Tcpip\Parameters
Name:	SynAttackProtect
Type:	REG_DWORD
Value:	2

TcpMaxHalfOpen: This holds the number of connections in the SYN-RCVD state allowed before SYN-ATTACK protection starts to operate.

Hive:	HKEY_LOCAL_MACHINE
Key:	System\CurrentControlSet\Services\Tcpip\Parameters
Name:	TcpMaxHalfOpen
Type:	REG_DWORD-Number
Value:	100-0xFFFF

TcpMaxHalfOpenRetried: This holds the numbers of connections in the SYN-RCVD state where at least one retransmission of the SYN is sent, before SYN-ATTACK protection starts.

Hive:	HKEY_LOCAL_MACHINE
Key:	System\CurrentControlSet\Services\Tcpip\Parameters
Name:	TcpMaxHalfOpenRetried
Type:	REG_DWORD-Number
Value:	80-0xFFFF

EnablePMTUDiscovery: This controls whether TCP will try to discover the MTU over the passage to a remote host.

Hive:	HKEY_LOCAL_MACHINE
Key:	System\CurrentControlSet\Services\Tcpip\Parameters
Name:	EnablePMTUDiscovery
Type:	REG_DWORD-Boolean
Value:	0

NoNameReleaseOnDemand: When the computer receives a name release request from the network, it is dependent upon the computer releasing its NetBIOS name.

Hive:	HKEY_LOCAL_MACHINE
Key:	System\CurrentControlSet\Services\Netbt\Parameters
Name:	NoNameReleaseOnDemand
Type:	REG_DWORD-Boolean
Value:	1

KeepAliveTime: TCP will send a keep alive packet to verify that an idle connection is still there.

Hive:	HKEY_LOCAL_MACHINE
Key:	System\CurrentControlSet\Services\Tcpip\Parameters
Name:	KeepAliveTime
Type:	REG_DWORD-Time in milliseconds
Value:	300000

PerformRouterDiscovery: This controls whether TCP will try to perform a router discovery per interface.

Hive:	HKEY_LOCAL_MACHINE
Key:	System\CurrentControlSet\Services\Tcpip\Parameters
Name:	PerformRouterDiscover
Type:	REG_DWORD
Value:	0

EnableICMPRedirects: This controls whether the server will change its route table in response to ICMP redirect messages sent by network devices.

Hive:	HKEY_LOCAL_MACHINE
Key:	System\CurrentControlSet\Services\Tcpip\Parameters
Name:	EnableICMPRedirects
Type:	REG_DWORD
Value:	0

Disable DirectDraw: Prevents accesses to the video hardware and memory.

Hive:	HKEY_LOCAL_MACHINE
Key:	System\CurrentControlSet\Control\GraphicsDrivers\DCI
Name:	DirectDraw
Type:	REG_DWORD
Value:	0

Disable the default shares:
At initial installation, windows 2000 creates default shares for use of the system account, which creates a security threat. Type Net Share at the command prompt to delete all shares.

```
C:\>net share

Share name   Resource                        Remark

------------------------------------------------------------------------------
ADMIN$       C:\WINNT                        Remote Admin
C$           C:\                             Default share
IPC$                                         Remote IPC
The command completed successfully.


C:\>net share admin$ /d
admin$ was deleted successfully.
```

Hidden Shares	Path
C$ D$ E$	Root of each partition
ADMIN$	%SYSTEMROOT% (C:\WINNT)
IPC$	Temporary connections between servers
PRINT$	\SPOOL\DRIVERS

Removing OS/2 and POSIX Subsystems: This will increase system performance in the long run.

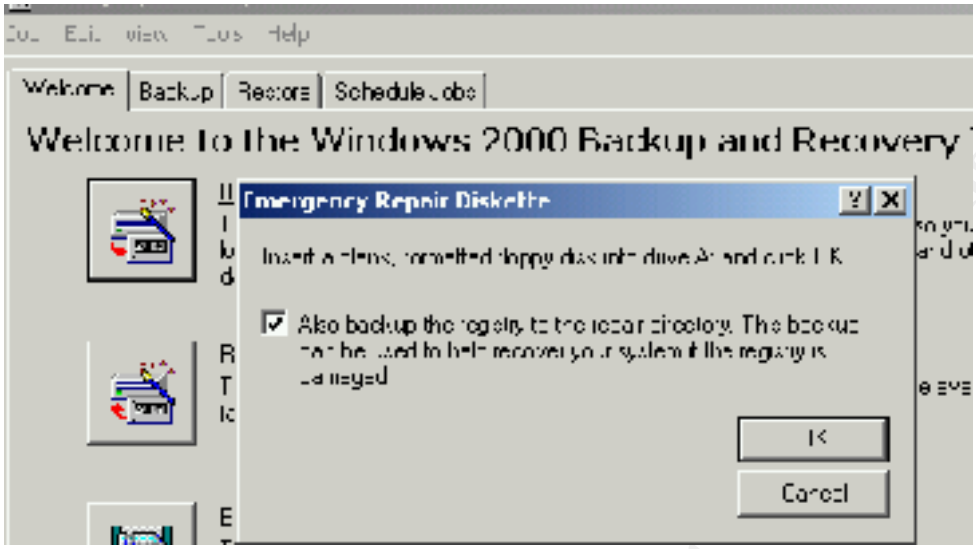
- HKLM\System\CurrentControlSet\Control\Session Manager\SubSystems, remove the corresponding registry values for POSIX and OS/2.
- HKLM\Software\Microsoft\OS/2 Subsystem for NT, delete all the sub keys.
- HKLM\System\CurrentControlSet\Control\Session Manager\Environment, remove Os2LibPath value.
- Then delete the files os2*, posix*, and psx* in %systemroot%\system32.

Installing Service Packs and Hot-fixes:

After all the applications and services are installed you will need to install the latest service packs and hot-fixes for the operating system and IIS. Only install hot-fixes for services that you need, or you will be creating more security holes within your OS. Refer to Microsoft's web site for the latest service pack (http://www.microsoft.com/windows2000/downloads/default.asp). The latest service pack to date for Windows 2000 is Service Pack 1.

Finishing up:

- ***Anti-Virus software:*** Install virus software on your production systems and make sure that the update runs every week or you could manually update the virus pattern. Well known virus protection software can be found at: http://www.symantec.com or http://www.MacFee.com or for a list of vendors search for Knowledge Base Article Q49500 at http://search.support.microsoft.com.
- ***Secure Backup Tapes:*** Protect your tapes by encrypting or putting them away at secure sites. Create ERD Diskettes and lock them away. Go to Start/Program/ Accessories/ System Tools/Backup, and then click on Tools/Create an ERD. See the following screen below.



- ***Setting Permissions on the Security event log:***

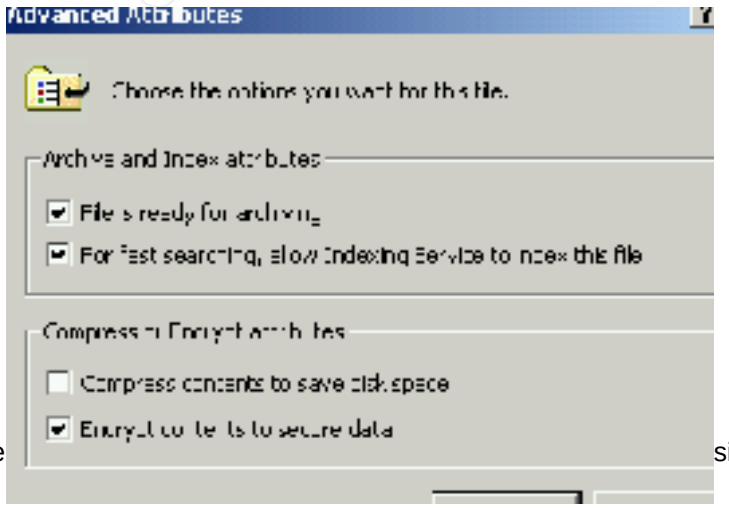
Permissions should be set on the three event logs AppEvent.Evt, SecEvent.Evt, and SysEvent.Evt to allow only the Administrator and the System account access.

- ***Disable Dump File Creation:***

To disable the dump file, go to the Control Panel/System Properties/ Advanced/Startup and Recovery and change "Write Debugging Information" to NONE. Configure the system to boot straight to the OS click on Control Panel/System Properties/ Advanced/Startup and Recovery/System Startup and set the boot time to 0.

- ***Enable EFS (Encrypting File System)***

This encryption system is an extra layer of security for files and folder; it will prevent hackers from getting into your sensitive files. Go to Windows Explorer, right click on the file or folder you wish to encrypt and choose Properties. On the General Tab, in the EFS properties click on Advanced then you select Encrypt contents to secure data.



- ***Protecting System Utilities:***

Create an admin group. Let's call it ToolsForAdmin. Add authorized users to this group. Change the ACL on the tools to remove local system and the administrator group. Next remove the tools from the system root and add a separate directory and place the tools in the new directory. ToolsForAdmin should then be given ownership and the ability to read and execute on the following tools. Arp.exe, at.exe, atsvc.exe, cacls.exe, cmd.exe, debug.exe, edit.com, edlin.exe, finger.exe, ftp.exe, xcopy.exe, ipconfig.exe, net.exe, nsloolup.exe, posix.exe, rcp.exe, regedit.exe, rexec.exe, rsh.exe, secfixup.exe, telnet.exe, Nbtstat.exe, Netstat.exe, ping.exe, qbasic.exe, rdisk.exe, regedt32.exe, route.exe, Runonce.exe, syskey.exe and tracert.exe.

Protecting Files and Directories:

By default the "Everyone" group is given access to the system root drive. Administrators and local System should have full control while "everyone group" should have read access. Or better yet give authorization to the "Authenticated Users" group to prevent users from accessing your machine without the proper rights. Apply all these changes to the following files and directories system root: e.g. C:\Winnt, c:\temp, c:\winnt\system32, c:\winnt\repair, c:\winnt\system32\config, c:\winnt\system32\drivers, c:\autoexe.bat. Then only add the Administrators and the system as full control to c:\boot.ini, c:\ntdetect.com, c:\ntldr, c:\config.sys.

- **Protect the Registry:**

For the following registry subkeys give Full control to Administrator and System and Authenticated users read access.

1. HKEY_LOCAL_MACHINE\Hardware
2. HKEY_LOCAL_MACHINE\Software
3. HKEY_LOCAL_MACHINE\System
4. HKEY_USERS\. Default

Restrict Remote Access to the registry; only Administrators must have full control. Add the following key, winreg then click on Security menu and click on Permissions, only set Administrator to Full control.

Hive:	HKEY_LOCAL_MACHINE
Key:	System\CurrentControlSet\Control\SecurePipeServers
Name:	Winreg

IIS 5.0 SERVER SECURITY:

- Limit the number of user accounts on the web server.
- Remove all default install directories for www root.
- Web files should be on a second partition not on the boot or the system partitions.
- Put restrictions on the IUSR_computername and IWAM_computername.
- Apply hot-fixes and service packs from the Microsoft website.
- Monitor your logs on a regular basis to see what users are doing on your website.

IIS Services:

- Event Log
- License logging service
- Windows NTLM Security Support Provider
- Remote Procedure Call service
- Windows NT Server
- IIS Admin Service
- MSDTC
- World Wide Web Publishing Service
- Protected Storage

Authentication Methods:

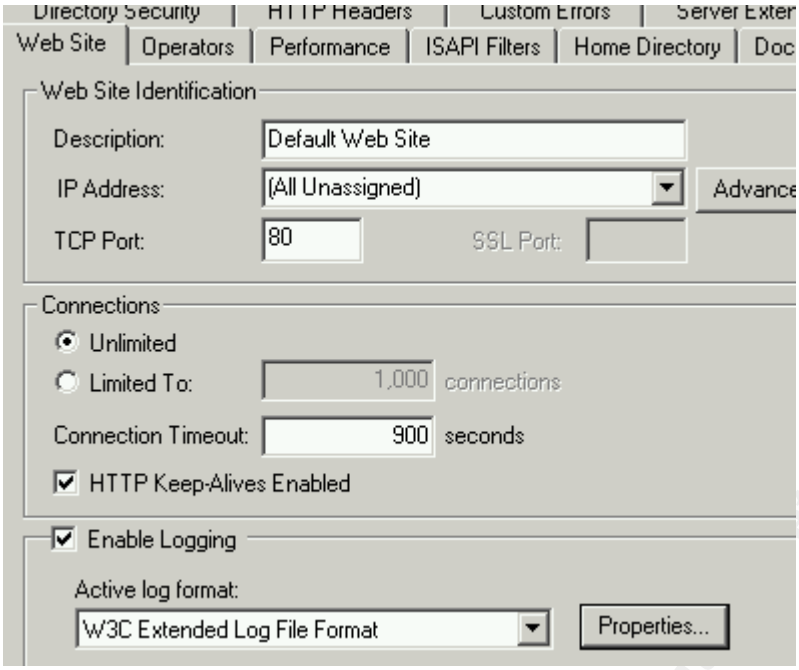
- Anonymous (no user name or password required)
- Basic (password sent over in clear text)
- Windows NT Challenge/Response (Stronger authentication with your domain)
- Client Certificates (Need a certificate on your browser to authenticate with the webserver)

ACL on Virtual Directories: *Set Administrators and System to full control and everyone write permissions.*

- CGI (. exe, .dll, .cmd, .pl)
- Script files (.asp)
- Include files (.inc, .shtm, .shtml)
- Static content (.txt, .gif, .jpg, .html, .htm)

IIS Log File:

Enable logging to check for attacks on your server. Choose the properties of your default web site, click on the web site tab, check enable logging and choose W3C Extended log file format from the Active log format list. See below.



Then click on Properties to the right of the Active log format and click on Extended Properties tab and set

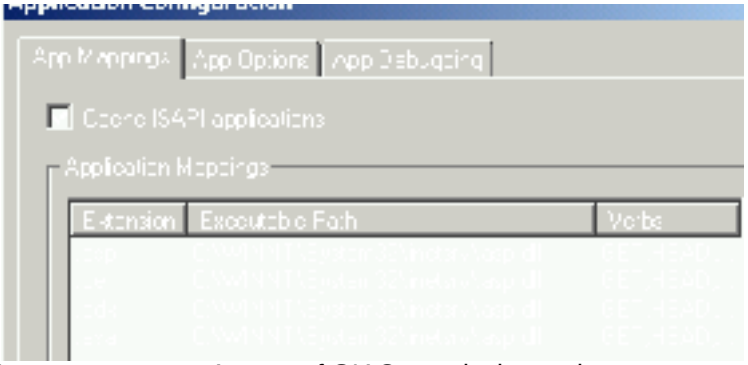
- Client IP address
- User name
- Method
- URI Stem
- HTTP Status
- Win32 Status
- User Agent

Remove or Disable Sample Applications:

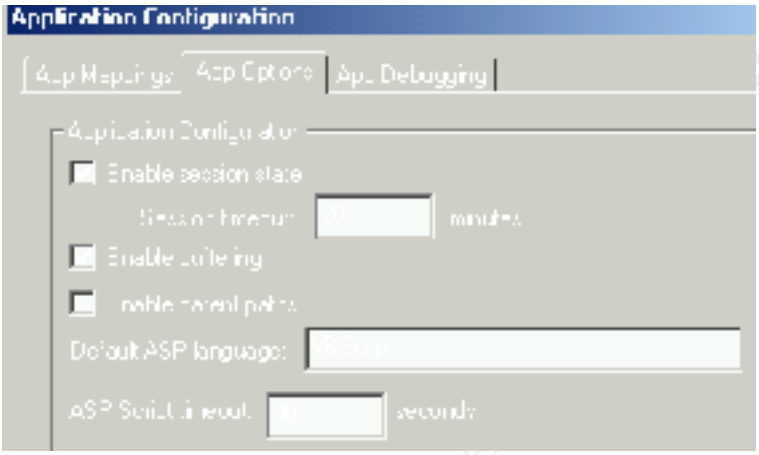
- IIS Samples in C:\inetput\issamples
- IIS Documentation in c:\winnt\help\isshelp
- Data Access in c:\program files\common files\system\msadc

Items to be removed or disabled:

- Unneeded COM Components type at command regsvr32 scrrun.dll /u
- Remove unused scripts mappings, go to IIS Manager and choose properties by right clicking on the Web Server. Click on Home Directory Tab/Configuration to remove these mappings you are not using.



- Parent Paths should be disabled. It is enabled by default which allows you to use ".." in calls to function. Go to IIS Manager and then choose properties by right clicking on the web server. Click on HomeDirectory Tab/ Configuration/ App Options tab and uncheck Enable Parent Paths.



These are a few considerations to help prevent attacks to your IIS web site.

Mailing Lists:
You should be Abreast of the most up-to-date security breaches. Windows 2000 exploits are emerging daily. The mailing list enables you to immediately recognize and patch these vulnerabilities. A few well-known mailing lists are:
Microsoft (http://www.microsoft.com/security)
SANS (http://www.sans.org/newlook/digests/ntdigest.htm)
NTBugtraq (http://www.ntbugtraq.com)
Security Focus (http://www.securityfocus.com)

Credits and References:

- Sheldon, Tom & Cox, Philip. Windows 2000 Security Handbook.California.McGraw-Hill Professional Book Group, July 2000
- Norberg, Stefan. Securing Windows NT/2000 Servers for the Internet. California. O'Reilly & Associates, Inc, November 2000
- Schultz, E. Eugene. Windows NT/2000 Network Security. California. New Riders Publishing U.S.A, July 2000
- Schambray, Joel & McClure, Stuart & Kurtz, George. Hacking Exposed: Network Security Secrets & Solutions Second Edition. California. McGraw-Hill Professional Book Group, October 2000
- Fossen, Jason. Securing Windows NT Step-by-Step. The SANS Institute GIAC Training, 2001
- Fossen, Jason. Securing Internet Information Server 5.0. The SANS Institute GIAC Training, 2001
- Bernie. "Windows 2000 Installation Security Checklist". http://www.labmice.net/articles/securingwin2000.htm
- "Security Considerations for Network Attacks". http://www.microsoft.com/TechNet/Security/dosrv.asp
- "Secure Internet Information Services 5 Checklist". http://www.microsoft.com/technet/Security/iss5chk.asp
- "Risk Assessment for Windows 2000". http://www.nswc.navy.mil/ISSEC/Form/AccredForms/acc_part2_2000.html
- "Windows NT C2 Configuration Checklist". http://www.microsoft.com/technet/security/C2config.asp

Last Updated: July 22nd, 2017

Upcoming Training

SANS Virginia Beach 2017	**Virginia Beach, VA**	**Aug 21, 2017 - Sep 01, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS vLive - SEC505: Securing Windows and PowerShell Automation	**SEC505 - 201709,**	**Sep 18, 2017 - Nov 13, 2017**	**vLive**
Secure DevOps Summit & Training	**Denver, CO**	**Oct 10, 2017 - Oct 17, 2017**	**Live Event**
SANS San Francisco Winter 2017	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**vLive**
SANS Cyber Defense Initiative 2017	**Washington, DC**	**Dec 12, 2017 - Dec 19, 2017**	**Live Event**
SANS Southern California- Anaheim 2018	**Anaheim, CA**	**Feb 12, 2018 - Feb 17, 2018**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**