Global Information Assurance Certification Paper

Security Configuration for Windows 2000 Server Acting as an IIS 5.0 Web Server

August 30,2000

Author: **Robert Millott**
ACS Defense Inc.

Table of Content

Introduction:

This guide is designed to provide the user with step-by-step procedures for installing and configuring Windows 2000 Server when used as an IIS Web Server. Microsoft IIS currently acts as the web server for about 20%[1] of the internet's web sites. With so many servers currently deployed, securing a web site in today's Internet environment is vital. Many instances of penetration into corporate networks use the web server as the launch point from which to gain unauthorized access. Whether the intent is to embarrass the company through defacing their web page, or gain corporate secrets through surreptitious access to their Intranet, a web corporate web server is a popular place to begin. Due to incorrect server settings, failure to apply service packs or hot fixes, or just lack of knowledge of good security practices, IIS is one of the most popular targets for hackers to attack. This guide will take a step-by-step approach to installing and configuring windows 2000 Server and IIS 5.0 to act as a corporate web server, allowing information to be delivered to legitimate customers and clients, while restricting unauthorized access to any other services.

A step-by-step approach is used, because all too often, the person actually setting up a server is not a fully trained individual with years of experience in creating and maintaining a web site. Large corporations often have entire staff's dedicated to creating and maintaining not only their web presence, but also their networks. Unfortunately, smaller companies, as well as government organizations, usually are understaffed and under budgeted, so they must rely on untrained, inexperienced individuals to handle their networks. It is this audience that this paper is directed. Detailed steps will be followed by explanations of why each step is important, and what it is either allowing or preventing.

[1] Information gathered from Netcraft (http://www.netcraft.com/survey/) survey of over 18,000,000 web servers in July, 2000.

Assumptions and Configurations

This web server will be configured as a stand-alone server, providing no other services and not a member of any domain. This is done for a number of reasons. Any service run on a computer is a potential vulnerability. The more services a computer is running, the more likely some un-thought of interaction or configuration setting will open the computer up to vulnerabilities. Since the web server is designed to be accessed by anyone from the Internet, securing it is vital. Running extra services, such as file-serving, application serving, or as a Domain Controller, just opens up more avenues of attack available to a malicious intruder. Although more costly, purchasing a separate computer to act as the web server will allow a much more secure configuration.

Keeping the server outside the domain, with no privileges within the domain serves as a back up security precaution. If the site is successfully attacked and intruder gains unauthorized access, this severely limits what the user can do. The attacker can control the web server and the web pages it offers, but this is often a minor consideration when compared to gaining access to the company's intranet and potentially sensitive information it contains. Payroll information, company proprietary information and trade secrets, which create a company's competitive advantage, should outweigh the public information. Even web based companies who entirely depend upon their web site for income generation, must keep this front end, public information separated from their corporate backbone.

Step-by-Step Installation

This guide shows step by step directions assuming a newly formatted Harddrive and the MSDN Windows 2000 Server (build 2195). Upgrade versions or later releases may differ slightly.

1.1. Format the hard drive. This installation guide assumes a fresh install on a clean machine, not an upgrade.
1.2. Boot from the CD right into the install program.
1.3. Welcome to Setup
  1.3.1. Press Enter to setup windows
1.4. Windows 2000 Server Setup
  1.4.1. Setup has determined your computers H/D is new (will only see if it's a clean or new H/D)
  1.4.2. Press C to continue
1.5. Windows 2000 Licensing Agreement
  1.5.1. Press F8 – I agree
1.6. Disks and partitions – Select the partition to install windows 2000 or create a new partition
  1.6.1. Select Unformatted space
  1.6.2. Press enter to install
1.7. Windows 2000 Server Setup
  1.7.1. Select "Format the partition using NTFS File System"
  1.7.2. Press enter
  1.7.3. Format Status …
  1.7.4. Please wait while setup copies files to the windows 2000 install folder
  1.7.5. This portion of setup has completed successfully – please reboot
1.8. Reboot the system.
1.9. Welcome to the windows 2000 setup wizard
  1.9.1. Click next to continue
  1.9.2. Installing devices, setup is detecting and installing devices on you computer
1.10. Regional Settings
  1.10.1. Change how numbers, currencies and dates appear
  1.10.2. Change keyboard layout
  1.10.3. Click next
1.11. Personalize your software
  1.11.1. Enter your name _____
  1.11.2. Enter your organization _____
  1.11.3. Click next
1.12. Your Product Key
  1.12.1. Enter your product key
  1.12.2. Click Next
1.13. Licensing modes
  1.13.1. Select your licensing mode
  1.13.2. Click Next
1.14. Computer name and administrator password
  1.14.1. Computer Name _____

1.14.2. Administrator password_____
1.14.3. Confirm password _____
1.14.4. Click next

1.15. Windows 2000 components
1.15.1. Uncheck Accessories & Utilities
1.15.1.1. As a stand alone web server, none of these components are required
1.15.2. Uncheck Index Service
1.15.3. Select Internet Information Services (IIS)
1.15.4. Click Details
1.15.4.1. Uncheck Documentation
1.15.4.2. Uncheck Front Page 2000 Server Extensions (unless required by your web site)
1.15.4.3. Uncheck SMTP – this turns off the mail
1.15.4.4. Click OK
1.15.5. Uncheck Script Debugger
1.15.6. Click Next

1.16. Date and Time Settings
1.16.1. Set date and time settings and time zone information
1.16.2. Click Next

1.17. Network settings
1.17.1. Wait while it installs components
1.17.2. Chose custom settings
1.17.3. Click Next

1.18. Network components
1.18.1. Uncheck Client for Microsoft Networks
1.18.2. Uncheck File and printer sharing for Microsoft Network
1.18.3. Select TCP/IP
1.18.4. Click properties
1.18.4.1. Enter IP Address, Network Mask, Default Gateway and DNS Address
1.18.4.2. Click on "Advanced" button
1.18.4.3. Select "WINS" Tab
1.18.4.4. Check "Disable NetBIOS over TCP/IP"
1.18.4.5. Select Options Tab
1.18.4.6. Select "TCP/IP Filtering"
1.18.4.7. Click on Properties
1.18.4.7.1. Check "Enable TCP/IP Filtering (All Adapters)
1.18.4.7.2. Select "Permit only" on TCP Ports
1.18.4.7.3. Click Add button
1.18.4.7.4. Enter "80" and click OK
1.18.4.7.4.1. This allows web access only. If using Secure connections, also enable port 443
1.18.4.8. Click OK
1.18.5. Click OK

1.18.6. Click Yes when Window's warns, "This connection has an empty Primary WINS. Do you want to continue"
1.18.7. Click OK
1.18.8. Click Next
1.19. Workgroup or Computer Domain
1.19.1. Use default "No, this computer is not on a network or is on a network without a domain"
1.19.2. Click Next
1.20. Installing components …
1.21. Completing the Windows 2000 setup wizard
1.21.1. Remove CD
1.21.2. Click Finish
1.21.3. Reboot
1.22. Login
1.22.1. Windows 2000 configure your server pops up DO **NOT RUN THIS,** as this will configure your server to run DNS, DHCP, KDC etc.
1.22.2. Click on "I will configure this server later"
1.22.3. Click next
1.22.4. Uncheck "Show this screen on startup"
1.22.5. Click Next

User Accounts

The changes to the Local Security Policy will direct the renaming of the administrator and Guest accounts. This is a good start. Other User Policies should include:

Administrator has no network access to the computer. This is inconvenient for some administrators to have to physically logon to the computer, but it restricts what an unauthorized user can accomplish. Even if an intruder gains the administrator password, it is not useable, except locally, which should be protected by physical security measures.

IUSR_Computername and IWAM_Computername have only network access to the computer. This will be the account used by anonymous web surfers; thus they should have no local access

No other accounts exist on the computer. The only accounts should be the administrator and the IIS account, IUSR_Computername & IWAM_Computername. These are the only people who should be accessing this computer.

Service Packs, Patches and Hot Fixes

Keeping a constant watch on Microsoft's web site for the latest Service Packs, patches and Hot Fixes is vital. Microsoft constantly updates and patches the operating system and applications. Many of these Service Packs or Hot Fixes have security implications, fixing vulnerabilities discovered in different applications. Keeping abreast of the latest changes and performing updates in a timely manner minimizes the chances of a security breach.

Virus Scanner

Running a virus scanner on the web server can also provide protection. If the server is attacked and broken into, one of the first things an intruder will usually do is to install a backdoor. Virus scanners now recognize most common backdoor programs, such as Netbus or BackOrfice and can prevent an intruder from installing such programs.

Post Installation Modifications

1. Event Logs
   - 1.1. Modify the way Microsoft saves logs. Default settings are to overwrite logs after 7 days. This erases all audit logs, which is a bad security practice. Recommendation is to not overwrite logs, requiring an administrator to manually review and clear the logs.
   - 1.2. Start => Programs => administrative tools => Event Viewer
   - 1.3. Select Security Logs, right click on it and select properties
   - 1.4. Click on "do not overwrite events (clear logs manually)".
   - 1.5. Increase size of logs, settings depend upon local policy, but minimum should be 1024
   - 1.6. This requires the system administrator to clear the logs. Combined with security option of shutting system down if unable to log security audits, it forces administrators to review logs occasionally. This is the strongest and best means of controlling Audits, especially security logs, although some sites might not want their machine to shutdown if security logs are filled, due to Denial of Service possibilities.
2. Various Services
   - 2.1. Turning off unneeded services prevents their possible exploitation. Microsoft defaults to running many services, as a single purpose web server, are not needed. Below is a list of services to turn off. To turn them off, go to the services tool, right click on the service, then select "Disable" for startup type, and "Stop" for Service Status.
   - 2.2. Start => Programs => administrative Tools => Services
   - 2.3. Select the following services and disable them:
     - 2.3.1. DHCP Client
       - 2.3.1.1. Since the Web server has a static IP and will not be a DHCP client, disable this service
     - 2.3.2. Distributed Link tracking Client
       - 2.3.2.1. This service is used for Distributed file system. Unless you are distributing your web pages across other remote Windows 2000 computers, this is an unneeded service
     - 2.3.3. Distributed Transaction Coordinator
       - 2.3.3.1. Transaction service is used my IIS 5.0 and COM+ to help with distributed transactions such as e-commerce functions where and entire function must complete, or none of it is completed. Unless there is a need for this capability in the web site, disable it.
     - 2.3.4. IPSec Policy Agent
       - 2.3.4.1. IPSec can be used for Virtual Private Networks (VPNs). Since this is a stand alone web server, not VPNs needed
     - 2.3.5. Messenger
       - 2.3.5.1. Allows sending and receiving popup messages across the network. Not needed for a web server
     - 2.3.6. Network Connections

2.3.6.1. Manages object in the Network and Dial-up connections folder. Not needed for a Web Server

2.3.7. Print Spooler

2.3.7.1. Spools all print jobs. The web server should not be acting as a print server, so disable it

2.3.7.2. Remote Access Connection Manager

2.3.7.2.1. Controls remote Access network connections

2.3.7.3. Remote Registry Service

2.3.7.3.1. Allows remote registry manipulation.

2.3.7.4. RunAs

2.3.7.4.1. Allows upgrading of security credentials to enable executing processes under different credentials

2.3.7.5. Task Scheduler

2.3.7.5.1. Task Scheduler allows the executing of any script or program at a scheduled time. Windows 2000 also allows remote scheduling of events, via DCOM. Unless absolutely needed by the administrator, disable this ability.

2.3.7.6. TCP/IP NetBIOS Helper Service

2.3.7.6.1. Enables NetBIOS over TCP/IP. Not needed for Web Server

2.3.7.7. Telephony

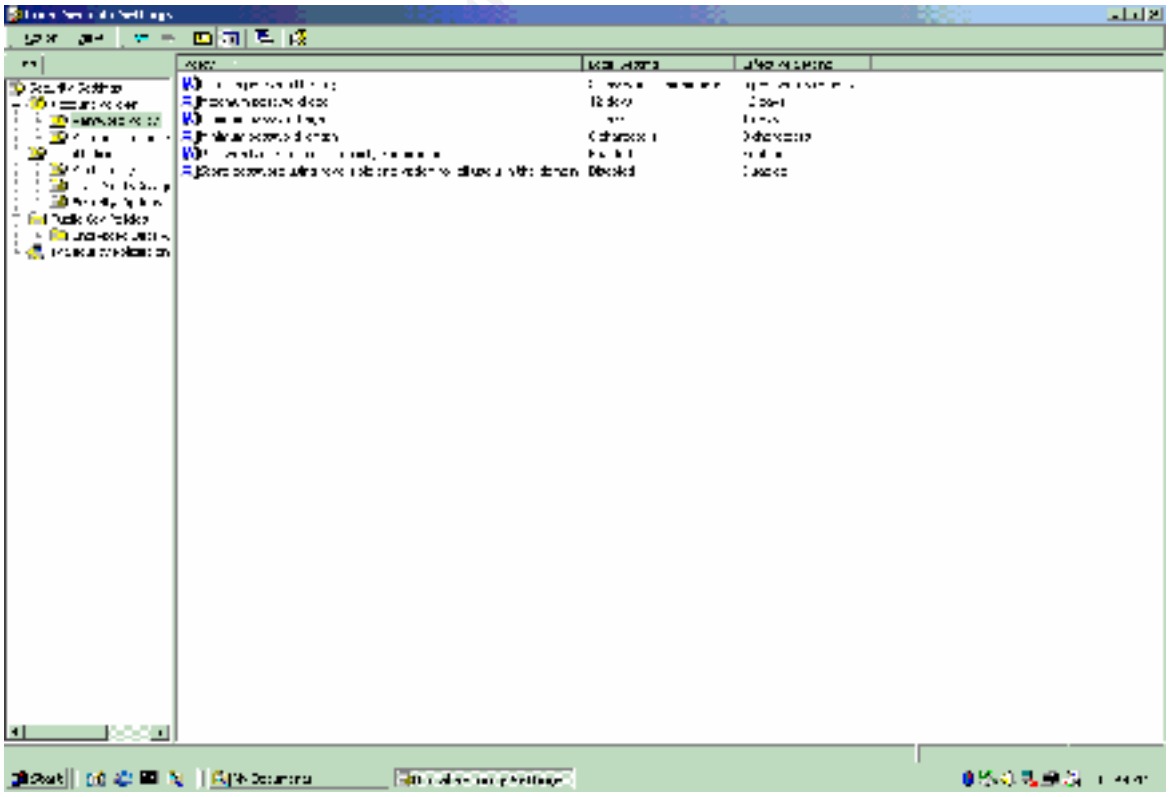
2.3.7.7.1. Provides TAPI support

Manual Configuration of the Local Security Policy:

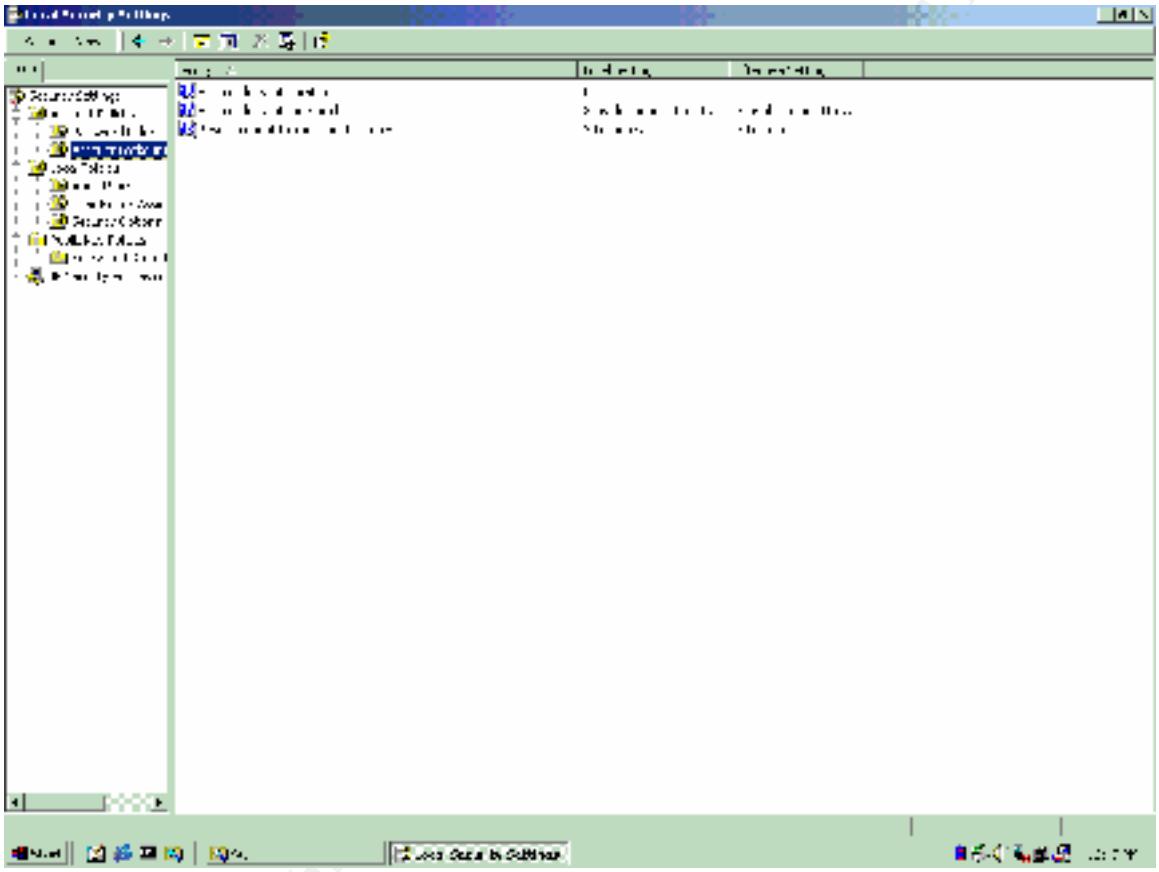
The Local Security Policy settings allow an administrator to control many facets of the security of the local machine. Most settings provide adequate control, but the ones listed below should be changed. The Local Security Policy Editor can be reached through the Administrative Tools, Click Start => Programs => Administrative Tools => Local Security Policy

This starts the policy editor. Select the policy folder from the left half of the screen; select the individual policy you want to modify on the right. Right click on the policy to modify it, then select its new value.

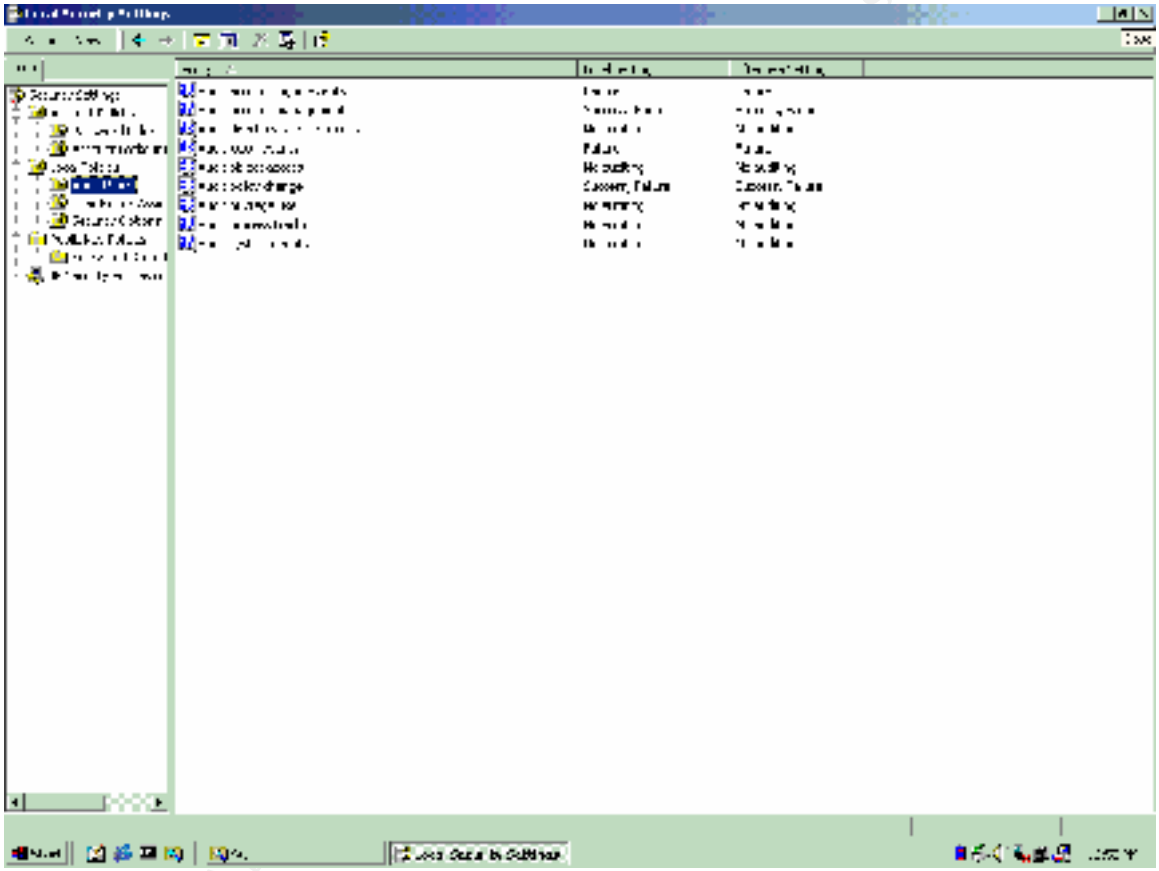
Password Policy	**Setting**	**Explanation**
Enforce Password History	5	Users cannot reuse same password when changing them. This policy sets how many new passwords must be used before you can reuse one
Maximum Password Age:	42 days	How many days a user may use a password before they are forced to change it
Minimum password Age:	1 day	How many days a password must be used before it can be changed. Prevents a user from changing his password multiple times in one day to defeat the password history setting
Minimum Password Length:	8 char	Longer password makes guessing it much harder
Password must meet complexity requirements	Enabled	Password cannot contain any part of the user or account name Must contain 3 of the following 4 parts English uppercase (A-Z) English lowercase (a-z) Numbers (0-9) Special characters, such as punctuation
Store passwords using reversible encryption	Disabled	Someone, someday will figure out how to exploit a reversible encryption scheme



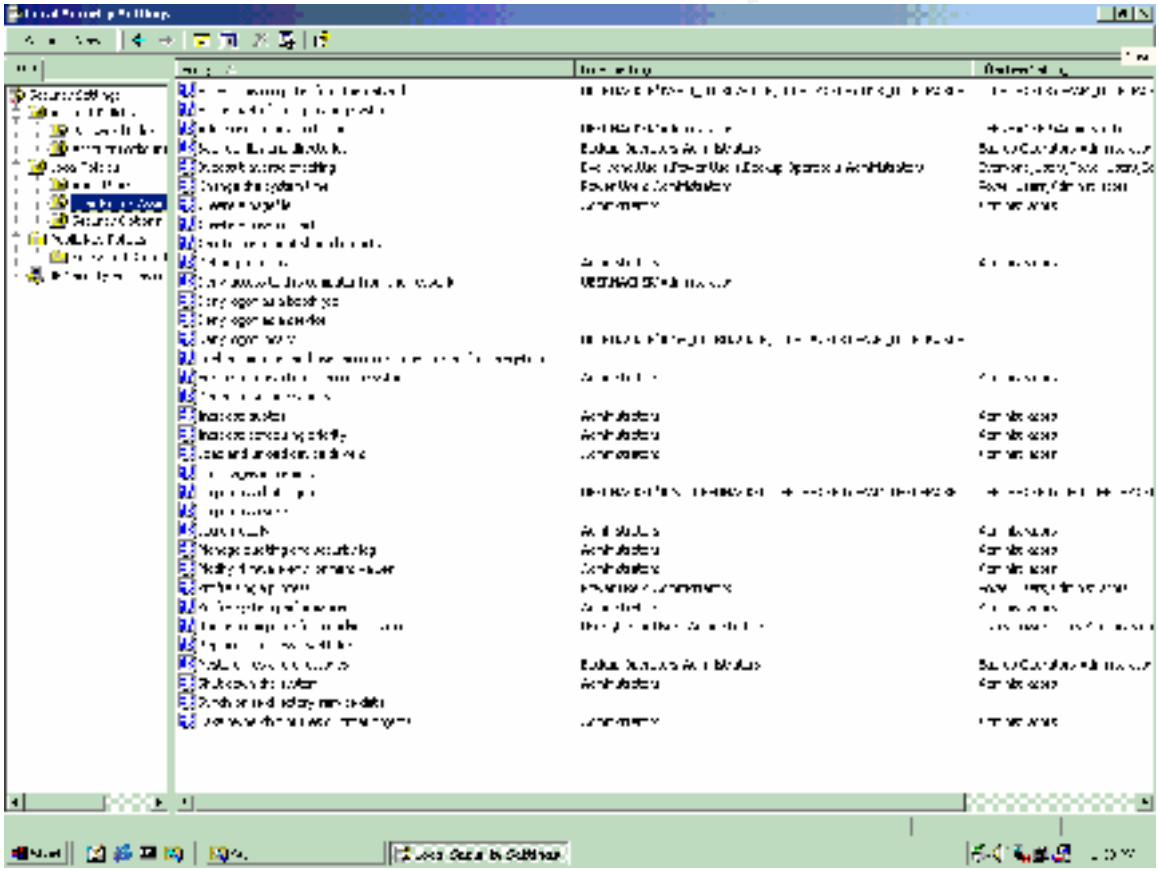
Account Lockout		
Account Lockout Duration	0	Administrator must re-instate locked out accounts
Account Lockout Threshold	3	Number of tries until account is locked out
Reset account Lockout counter after	30 min	Time till lockout counter resets back to zero



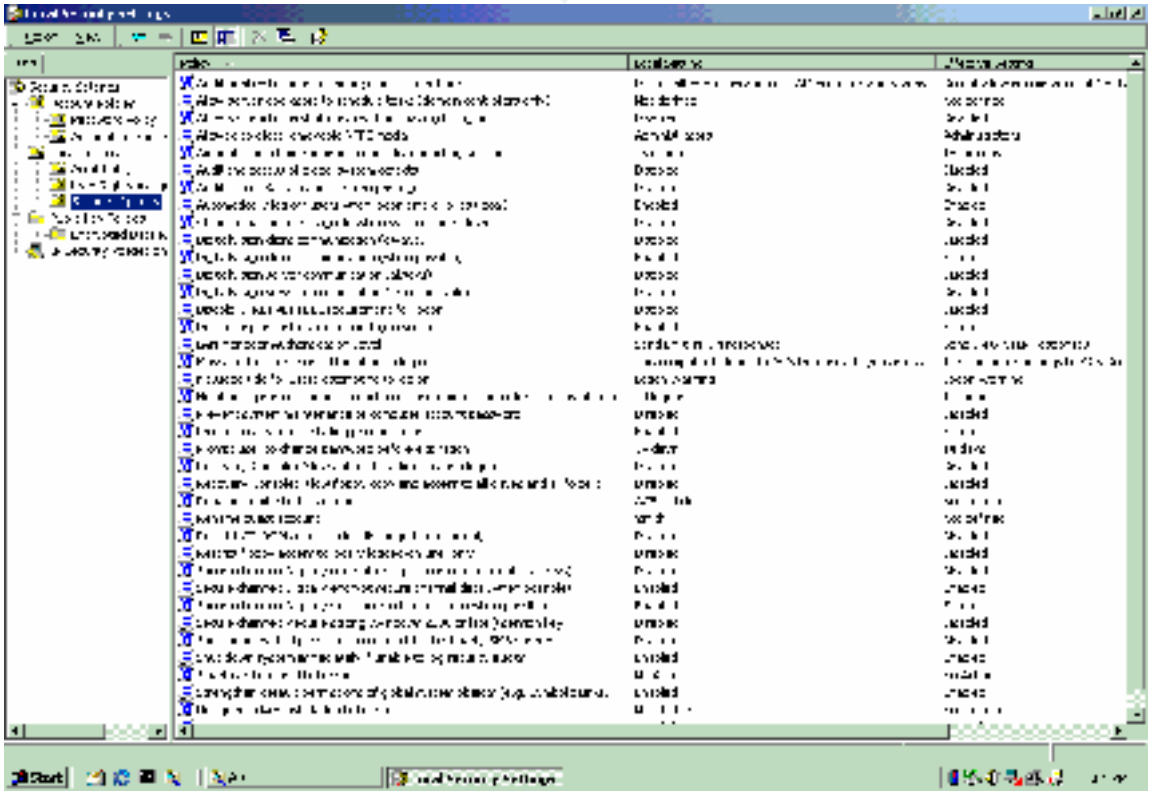
Audit Policy		
Audit account logon events	Failure	Log all account logon failures
Audit Account management	Success/Failure	Log the creation or deletion of accounts
Audit logon events	Failure	Log all account logon failures
Audit Policy change	Success/failure	Log when auditing policy is changed



User rights Assignment		
Access this computer from the network	IUSR_*computername* *IWAM_computername*	Only account allowed to remotely access this computer is the default web browser account
Add Workstations to domain	Administrator	Self explanatory
Deny access to this computer from the network	Administrator	Requires Administrators to perform all work locally
Deny Logon Locally	IUSR_computername IWAM_computername	Deny IIS Accounts from being used to log on locally
Log on Locally	Administrator	Self explanatory
Shutdown the System	Administrator	Self explanatory



Security Options		
Additional restrictions for anonymous connections	Do not allow enumeration of SAM accounts and shares	Do not allow enumeration of SAM accounts and shares
Allow system to be shutdown without having to logging on.	Disabled	Prevents unauthorized shutdown of system
Do not display last user name in logon screen	Enable	Hides the name of the last user to login
Message text for users attempting to login	Enter one	Local Security Policy should direct the text here
Message title for user attempting	Enter one	"Logon Warning"
Rename Administrator Account	Create new name	A Login requires a valid username and password, why give an attacker half of what they need
Rename Guest Account	Create new name	This account should be disabled
Shutdown System immediately if unable to log security audits	Enable	If you cannot log the security logs, shutdown the machine



Conclusion

Configuring the web server using the above as a guide will provide a relatively secure server. Obviously, no site is completely secure. If you are allowing unknown users to access your information, which is what most web servers do, there is some risk involved. Keeping up with the latest security information, and following some basic security settings will prevent all but the most determined attackers out of the web server.

References

The following materials were drawn upon in the creation of this document

Hacking Exposed, Network Security Secrets & Solutions by Stuart McClure, Joel Scambray & George Kurtz, Osborne/McGraw-Hill, ISBN 0-07-212127-0,

Windows 2000 Server Security for Dummies by Paul Sanna, IDG Books Worldwide Inc. ISBN 0-7645-0470-3

Mastering Windows 2000 Server by Mark Minasi, Christa Anderson, Brian M. Smith & Doug Toombs, Sybex Inc. ISBN 0-7821-2774-6,

Sans DC2000 Track 5 .5 Internet Information Server by Jason Fossen