# Global Information Assurance Certification Paper

# Securing Windows GCNT Practical Assignment v3.0

Option 2 - Securing Windows 2000 with Security Templates



Date Prepared:
**November 10, 2001**

Prepared by:
**Jeff Wilkinson**

## Table of Contents

## Introduction

This paper will detail the application, testing and evaluation of a security configuration template for the purpose of securing a Microsoft Windows 2000 Server running Internet Information Server (IIS) version 5.0. The Web Server will be used for distributing information over the public internet. The information will include a business description and mission statement, corporate contacts, shareholder information, job postings and other relevant publicly accessible information. It has been mandated from the executive management that the corporate web site be secured from the possibility of defacement and that the web site should be available at all times.

The security configuration template "web_secure.inf" will be used to secure the production web servers described in this paper. This template was originally created from the sample "highsecweb.inf" template included in the TechNet article "Data Security and Data Availability for End Systems" by Tom Dodds, Warren Kirby and Michael Howard from Microsoft Consulting Services of Southern California. The article is available at the following URL:

http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/bestprac/datavail.asp

The security template was subsequently modified and renamed "web_secure.inf" by Eric Schultze. This updated template includes registry settings that provide an additional level of security. The template also includes the application of restrictive permissions to sensitive registry keys and files. The template used for this paper "web_secure.inf" is available for download at the following URL:

http://www.systemexperts.com/win2k/HardenWin2K.html

Microsoft has also recently published the "hisecweb.inf" security template with the IIS lock down tool. The "hisecweb.inf" template was not chosen for this paper because it does not lockdown registry and file system permissions. The IIS lockdown tool is available for download at the following URL:

http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/downloads/iislock.asp

## Demonstration System (IISPROD01)

The demonstration system IISPROD01 will be used throughout this paper. Two additional servers IISPROD02 and IISTEST01 will be built simultaneously to the same specifications. IISPROD01 and IISPROD02 will be hardware load balanced through an F5 Big IP load balancer. IISTEST01 will reside inside the corporate network and will be accessible to the web development staff. The IISTEST01 server will contain a CD-ROM burner which will be used to transfer site data manually to the production environment. WebDAV is currently being evaluated to provide a channel for updating website content in real-time.

The hardware used for IISPROD01 consists of a Compaq DL360 dual processor Pentium III 1GHz server with 2GB of physical RAM. The Microsoft Select version of Windows 2000 Server with Service Pack 2 was installed using an unattended installation script. All available options in the [components] section of unattend.txt were added and set to "off". This allows for a clean installation with no extraneous services or applications. The system contains two 18.2 GB Ultra SCSI-3 drives configured in a RAID 0 mirror set on the Compaq Smart Array controller. The RAID 0 set was partitioned into 3 logical drives:

Logical partition C: was set to 6GB and labeled "system"
Logical partition D: was set to 9GB and labeled "sites"
Logical partition E: was set to 3GB and labeled "logs"

Following the server installation, the D and E partitions were formatted with NTFS. The following NTFS permissions were set at the root of drives D and E.

- Removed "Everyone"
- Added "IISPROD01\Administrators" (Full Control)
- Added "IISPROD01\SYSTEM" (Full Control)
- Enabled "Reset permissions on all child objects and enable propagation of inheritable permissions"

The following iiscomp.txt text file was created on the D: drive, for the controlled installation of IIS to the logical drive E:

```
[components]
iis_common = on
iis_inetmgr = on
iis_www = on
iis_doc = on
[InternetServer]
PathWWWRoot=d:\websites\default\root
```

The System optional components manager was used from the command line to install IIS as follows:

```
SYSOCMGR /i:%WINDIR%\inf\sysoc.inf /u:d:\iiscomp.txt
```

The following post installation configuration tasks were completed using the Internet Information Services MMC snap-in:

- Removed Virtual Web Sites
  - Scripts d:\websites\default\scripts
  - IISHelp c:\winnt\help\iishelp
  - IISAdmin c:\winnt\system32\inetsrv\iisadmin
  - IISSamples d:\websites\default\iissamples
  - MSADC c:\program files\common files\system\msadc
  - Printers c:\winnt\web\printers
- Removed Script Mappings – some ASP content will be used on the web site, so the script mappings to the asp.dll have been left in place. All unused script mappings have been be removed.
  - .htw c:\winnt\system32\webhits.dll
  - .ida c:\winnt\system32\idq.dll
  - .idq c:\winnt\system32\idq.dll
  - .htr c:\winnt\system32\inetsrv\ism.dll
  - .idc c:\winnt\system32\inetsrv\httpodbc.dll
  - .shtm c:\winnt\system32\inetsrv\ssinc.dll
  - .shtml c:\winnt\system32\inetsrv\ssinc.dll
  - .stm c:\winnt\system32\inetsrv\ssinc.dll
  - .printer c:\winnt\system32\msw3prt.dll
- Removed Execute Permissions (Set to none)
- Removed index this resource
- Enabled only Anonymous Access

The "IUSR_IISPROD01" user account was granted the NTFS permissions Read & List folder contents to the root folder under d:\websites\default. Additionally, the AdminScripts, IISSamples and Scripts directories were deleted from the default directory.

The hfnetchk tool was run from the command line to check the patch status against the mssecure.xml patch database downloaded on November 26th. The following syntax was used to generate the patch report below:

```
hfnetchk.exe -v -z -s 1 -x mssecure.xml
```

---

IISPROD01

---

* WINDOWS 2000 SERVER SP2

Patch NOT Found MS00-077 Q299796
File C:\Program Files\NetMeeting\callcont.dll has an invalid checksum and its file version is equal to or less than what is expected.

Patch NOT Found MS01-007 Q285851
File C:\WINNT\system32\winlogon.exe has an invalid checksum and its file version is equal to or less than what is expected.

Patch NOT Found MS01-013 Q285156
File C:\WINNT\system32\els.dll has an invalid checksum and its file version is equal to or less than what is expected.

Patch NOT Found MS01-025 Q296185
File C:\WINNT\system32\webhits.dll has an invalid checksum and its file version is equal to or less than what is expected.

Patch NOT Found MS01-031 Q299553
File C:\WINNT\system32\tlntsvr.exe has an invalid checksum and its file version is equal to or less than what is expected.

Patch NOT Found MS01-036 Q299687
File C:\WINNT\system32\advapi32.dll has an invalid checksum and its file version is equal to or less than what is expected.

Patch NOT Found MS01-040 Q292435
File C:\WINNT\system32\drivers\tdipx.sys has an invalid checksum and its file version is equal to or less than what is expected.

Patch NOT Found MS01-041 Q298012
File C:\WINNT\system32\catsrv.dll has an invalid checksum and its file version is equal to or less than what is expected.

Patch NOT Found MS01-046 Q252795
File C:\WINNT\system32\drivers\irda.sys has an invalid checksum and its file version is equal to or less than what is expected.

Patch NOT Found MS01-052 Q307454
File C:\WINNT\system32\export\instrdp5.dll has an invalid checksum and its file version is equal to or less than what is expected.

* Internet Information Services 5.0

Patch NOT Found MS01-025 Q296185
File C:\WINNT\system32\webhits.dll has an invalid checksum and its file version is equal to or less than what is expected.

Patch NOT Found MS01-044 Q301625
File C:\WINNT\system32\adsiis.dll has an invalid checksum and its file version is equal to or less than what is expected.

* Internet Explorer 5.01 SP2

Patch NOT Found MS01-051 Q306121
File C:\WINNT\system32\wininet.dll has an invalid checksum and its file version is equal to or less than what is expected.

The patch information listed in the batch script has been updated through November 26th, 2001. The command line options represent quiet mode installation with no reboot. The patches for Internet Explorer have a different syntax for quiet mode with no reboot. This is consistent with the Internet Explorer Administration Kit's (IEAK) installation options but inconsistent with the hotfix syntax. The qchain.exe utility is used at the end to safely chain the hotfixes together without requiring a reboot after each patch. The qchain utility is available from Microsoft and documented in the technet article "Use QChain.exe to Install Multiple Hotfixes with Only One Reboot (Q296861)"

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

**[PATCH.BAT]**

```
@echo off
rem MS00-077 : NetMeeting Desktop Sharing Vulnerability
        Q299796_W2K_SP3_x86_en.EXE -z -m
rem MS00-007 : Recycle Bin Creation Vulnerability
        Q285851_W2K_SP3_x86_en.EXE -z -m
rem MS00-013 : Misordered Windows Media Services Handshake Vulnerability
        Q285156_W2K_SP3_x86_en.EXE -z -m
rem MS01-025 : Index Server Search Function Contains Unchecked Buffer
        Q296185_W2K_SP3_x86_en.EXE -z -m
rem MS01-027 : Flaws in Web Server Certificate Validation Could Enable Spoofing
        IE501sp2-q295106.exe /q:1 /r:n
rem MS01-031 : Predictable Named Pipes Could Enable Privilege Elevation via Telnet
        Q299553_W2K_SP3_x86_en.EXE -z -m
rem MS01-036 : Function Exposed via LDAP over SSL Could Enable Passwords to be Changed
        Q299687_W2K_SP3_x86_en.EXE -z -m
rem MS01-037 : Authentication Error in SMTP Service Could Allow Mail Relaying
        Q302755_W2K_SP3_x86_en.EXE -z -m
rem MS01-040 : Invalid RDP Data Can Cause Memory Leak in Terminal Services
        Q292435_W2K_SP3_x86_en.EXE -z -m
rem MS01-041 : Malformed RPC Request Can Cause Service Failure
        Q298012_W2K_SP3_x86_en.EXE -z -m
rem MS01-046 : Access Violation in Windows 2000 IRDA Driver Can Cause System to Restart
        Q252795_W2K_SP3_x86_en.EXE -z -m
rem MS01-051 : Malformed Dotless IP Address Can Cause Web Page to be Handled in Intranet
Zone
```

```
        IE501sp2-q306121.exe /q:1 /r:n
rem MS01-052 : Invalid RDP Data can Cause Terminal Service Failure
        Q307454_W2K_SP3_x86_en.EXE -z -m
        qchain.exe
```

Following a reboot of the server, the hfnetchk command was run against the server again, which yielded the following output:

```
hfnetchk.exe -v -z -s 1 -x mssecure.xml

---------------------------
IISPROD01
---------------------------

        * WINDOWS 2000 SERVER SP2

        INFORMATION  All necessary hotfixes have been applied

        * Internet Information Services 5.0

        INFORMATION  All necessary hotfixes have been applied

        * Internet Explorer 5.01 SP2

        INFORMATION
        All necessary hotfixes have been applied.
```

The server is now ready to be configured with a security configuration template.

## Security Template Settings and Evaluation

The web_secure.inf template provides the starting point for a medium to high level of security. No security template should be used in a production environment without thorough analysis of the template settings and adequate testing in a lab environment. In most cases, the template will need to be customized to the individual needs of the environment in which it will be applied. Each section and setting of the security template is listed below with a detailed description of the setting and recommendations for where settings should be modified for the demonstration system described in this paper.

### 1.1 Account Policies

#### 1.1.1 Password Policy

**Enforce password history [8 passwords remembered]**

This option is used in conjunction with the Minimum password age option to enforce the use of unique passwords. The possible values for this setting range from 0 (or no passwords remembered) to 24 (passwords remembered). For this option to be effective, the Minimum password age should be set to a value greater than "0". To ensure that passwords are not reused, I would recommend setting this to the maximum value of 24.

**Maximum password age [42 days]**

The maximum password age option determines the amount of time a user can go without changing their password. The possible values for this setting range from 0 (or never expire) to 999 days. Additionally, the maximum password age must be greater than the minimum password age. The default setting of 42 days is a good option.

**Minimum password age [2 days]**

The minimum password age option determines how long a password must be used before it can be changed. The possible values for this setting range from 0 (or allow changes immediately) to 999 days. The setting of 1 day, in conjunction with the maximum password history setting of 24 passwords remembered will greatly reduce the possibility of a user selecting the same password twice.

**Minimum password length [7 characters]**

This option specifies the minimum character length for the user's password. The security template only allows for values between 0 (or no password required) and 14 characters. Windows 2000 supports a maximum password length of 127 characters. Password length is a tricky

subject, the longer the password, the more secure it is. At the same time, the longer the password is, the more likely the user will right it down. Password hashes created for LAN Manager and NTLM v1 are easily cracked via LC3 (l0pht Crack version 3) and other utilities. If LAN Manager or NTLM v1 is required, careful consideration of password length should be used. These password hashes are divided into 2 seven part segments. Either segment of the hash can be cracked independently of the other. In some cases using a password longer than 7 characters can be detrimental. Take for example the password "present4U". This password is 9 characters and follows the windows default complexity requirements. The first 7 characters ("present") are hashed independently from the second 7 characters ("4U"). The first half of the hash will be immediately broken from a standard dictionary password attack. The second half of the hash only requires 2 of the 7 characters be cracked. Even using the brute force password attack in LC3, the second half will be broken is seconds. In this case, the 7 character password "prsnt4U" would be a more secure password. For a web server accepting connections over the public internet, a setting of 14 characters should be used. Only administrative personnel will be logging onto the system using local accounts, so extended password lengths should not be a problem.

**Passwords must meet complexity requirements [Enabled]**

This option determines whether passwords must meet the following complexity requirements.

- Does not contain all or part of the user's account name
- Must be least six characters in length
- Contains characters from three of the following four categories:
  - Upper case characters (A-Z)
  - Lower case characters (a-z)
  - Numbers (0-9)
  - Symbols (!$#% etc.. )

Password complexity is filtered through the passfilt.dll. The passfilt.dll can be replaced with a custom filter. The NSA Security Configuration Tool Set includes the enpasflt.dll which enforces 8 character passwords, requires characters from all 4 character categories and does not allow any part of the user's logon or full name. Adding complexity to the password is extremely important. The additional use of symbols will greatly increase the amount of time it will take to break an exposed password hash.

**Store passwords using reversible encryption [Disabled]**

This option is used to provide compatibility with applications that require

access to the user's password. Some third party SMB servers and applications which utilize Challenge Handshake Authentication Protocol (CHAP) or Digest Authentication may require this setting be enabled. Reversibly encrypted passwords are saved during the change password procedure. If this setting is disabled after having previously been enabled, the passwords must be changed to remove the reversibly encrypted password. This option should only be enabled as a last resort. Before globally enabling this setting, try enabling the option for the specific user account that requires the use of the application.

### 1.1.2 Account Lockout Policy

**Account lockout duration [0 minutes]**

This setting specifies the number of minutes an account will remain locked out when the Account lockout threshold has been exceeded. A value of "0" indicates the account will remain locked out until an administrator unlocks the account. This is an ideal setting for a stand alone web server.

**Account lockout threshold [5 invalid logon attempts]**

A failed logon attempt against a specific user account is tracked in the bad logon counter associated with the user account. When the counter reaches the value specified in the Account lockout threshold, the user's account will be locked. I would recommend the setting be lowered to 3 invalid logon attempts.

**Reset account lockout counter after [30 minutes]**

This setting determines the number of minutes to wait, following a failed logon attempt, before setting the bad logon counter back to "0". If local user accounts are known, the password attempts could be programmatically targeted. A simple formula would be (Account lockout threshold value – 1) password attempts within (Reset account lockout counter after *x* minutes + 1) interval of time. With the above settings, 4 password attempts could be made against every local account every 31 minutes, without triggering an account lockout. That would be 185 password attempts per day against each local user account. If the security logs are not checked regularly, this type of attack could go undetected for a long period of time. The reset account lockout counter should be set to a value "1440" which is equivalent to 24 hours. This setting should deter this type of attack.

### 1.1.3 Kerberos Policy

Kerberos policy is only valid on a Windows 2000 Domain Controller. This template is designed to secure a Windows 2000 Standalone or Member

server.

**Enforce user logon restrictions [Not defined]**

**Maximum lifetime for service ticket [Not defined]**

**Maximum lifetime for user ticket [Not defined]**

**Maximum lifetime for user ticket renewal [Not defined]**

**Maximum tolerance for computer clock synchronization [Not defined]**

## 1.2 Local Policies

### 1.2.1 Audit Policy

**Audit account logon events [Success, Failure]**

This audit policy tracks logon events for local user accounts. This option should be enabled for both success and failure.

**Audit account management [Success, Failure]**

This audit policy tracks changes to objects in the local accounts database.

**Audit directory service access [No auditing]**

This audit policy setting only applies to domain controllers. The demonstration system is a stand alone web server and does not require this option be enabled.

**Audit logon events [Success, Failure]**

This audit policy tracks interactive, network and service logon and logoff events against the local system. This includes accounts from remote systems.

**Audit object access [Failure]**

This audit policy tracks access to any object on the local system that has an Access Control List (ACL) associated with it. Registry keys, files and folders are all examples of objects that can be tracked using this audit policy.

**Audit policy change [Success, Failure]**

This audit policy enables the tracking of changes to the audit or user rights assignment policies.

**Audit privilege use [Failure]**

This audit policy enables the tracking of successful or failed use of a user right. There are a number of rights which are not audited through this setting:

- Bypass traverse checking
- Debug programs
- Create a token object
- Replace process level token
- Generate security audits
- Back up files and directories
- Restore files and directories

**Audit process tracking [No auditing]**

This audit policy allows for the detailed tracking of the following types of events:

- program activation
- process exit
- handle duplication
- indirect object access.

**Audit system events [Success, Failure]**

This audit policy allows for the tracking of system events. System events are defined as events which affect the security of the system or the security logs. Additionally, the shutdown or restart of the local computer is considered a system event.

The Audit policies in this template provide and adequate level of detail for the analysis of local security. The security logs should be monitored on a consistent basis for anomalies.

### 1.2.2 User Rights Assignment

**Access this computer from the network [Authenticated Users]**

This user privilege allows the local computer to be accessed through the network interface. The local "Users" group should be removed and specific local groups should be created with appropriate local NTFS permissions for the application or resources that will be shared on the target system.

**Act as part of the operating system [Not defined]**

This user privilege allows a process to take over the identity of any user account on the local system. This privilege should not be granted to an individual user or group. If a service requires this privilege, configure the service to use the local system account which has this right inherently.

### Add workstations to domain [Not defined]

This user privilege grants the user or group the ability to add a computer account to the domain. This setting is only valid when defined on a domain controller.

### Back up files and directories [Backup Operators, Administrators]

This user privilege allows for the bypassing of local NTFS permissions for the purpose of backing up data on local system. The backup process must utilize the NTFS backup API.

### Bypass traverse checking [Users, Power Users, Everyone, Backup Operators, Administrators]

This user privilege allows navigation through the registry or NTFS file system in order to gain access to an object in a sub folder that the user has been explicitly granted access to. The user can not list the contents of folders in the path to the object. The following example demonstrates this concept further:

HKLM\Software\Microsoft\Windows\Current Version\Internet Settings\URL History

If the user account has read access to the object "Directory" in URL History folder, but did not have read access to the folders leading into the URL History folder, the user would need the bypass traverse checking in order to gain access to the object.

### Change the system time [Power Users, Administrators]

This user privilege allows modification to the system's internal clock. The Windows Time service is an SNTP client and can be configured to pull time from an external NTP time source using the following command line:

net time /setsntp:*ntp.domain.com*

David Mills from the University of Delaware maintains an updated list of NTP servers at the following URL:

http://www.eecis.udel.edu/~mills/ntp/servers.html

### Create a pagefile [Administrators]

This user privilege allows for the modification of page file settings. On the demonstration system, the page file initial and maximum values will be modified to equal "2048" which is the value for the amount of installed RAM on the system. This will keep the page file from growing and shrinking which can cause fragmentation on the partition. Once the setting is adjusted, the administrators group can be removed from this user right if desired.

### Create a token object [Not defined]

This user privilege allows the creation of access tokens by processes running under the context of the user account. This privilege should not be granted to an individual user or group. If a service requires this privilege, configure the service to use the local system account which has this right inherently.

### Create permanent shared objects [Not defined]

This user privilege allows for the creation of objects in the kernel mode object manager. Components which run in kernel mode have this right inherently. This privilege should not be granted to an individual user or group.

### Debug programs [Administrators]

This user privilege allows the user or group the ability to attach a debugger to any process running on the local system. This right should only be defined when a debugger will be used on the system for troubleshooting purposes.

### Deny access to this computer from the network [Not defined]

Users defined in this setting will be denied over the network access to the host computer. This option explicitly overrides any permission granting that access.

### Deny logon as a batch job [Not defined]

Users defined in this setting will be denied the ability to log on as a batch process on the host computer. This option explicitly overrides any permission granting that capability.

### Deny logon as a service [Not defined]

Users defined in this setting will be denied the ability to logon as a service on the host computer. This option explicitly overrides any permission granting that capability.

### Deny logon locally [Not defined]

Users defined in this setting will be denied local logon to the host computer. This option explicitly overrides any permission granting local logon.

### Enable computer and user accounts to be trusted for delegation [Not defined]

This user privilege allows the user or group the ability to set the "Trusted for Delegation" option on a user or computer object. This permission can be explicitly overridden by setting the "Account can not be delegated" flag

on a specific user account. This permission allows a system process to access resources on another system under the context of the user or computer that has been trusted for delegation.

**Force shutdown from a remote system [Not Defined]**

This user privilege gives the user or group the permission to shut down the host computer from a remote system.

**Generate security audits [Not defined]**

This user privilege allows a system process running under the context of the user or group member, the ability to write events to the security log.

**Increase quotas [Administrators]**

This user privilege gives the user or group the permission to increase the quota on an object.

**Increase scheduling priority [Administrators]**

This user privilege gives the user or group the permission to change the scheduling priority of a process. The following priorities are available through the task manager:

- RealTime
- High
- AboveNormal
- Normal
- BelowNormal
- Low

**Load and unload device drivers [Administrators]**

This user privilege allows the user or group the permission to load and unload device drivers on the host computer.

**Lock pages in memory [Not defined]**

This user privilege allows a system process running under the context of the user or group member, the ability to keep its data from being paged to disk.

**Log on as a batch job [Not defined]**

This user privilege allows the user or group the permission to log on as a batch process on the host computer.

**Log on as a service [Not defined]**

This user privilege allows the user or group the permission to log on as a service on the host computer.

**Log on locally [Administrators, Authenticated Users, Backup Operators, Power Users, Users]**

This user privilege allows the user or group the permission to interactively logon to the console of the host computer. Logons through terminal services are also considered local logons even though the user is not physically at the console.

**Manage audit and security log [Administrators]**

Users with this privilege can manage audit settings on system objects and have read/write access to the security log.

**Modify firmware environment values [Administrators]**

Users with this privilege can manage system-wide environment values.

**Profile single process [Power Users, Administrators]**

This user privilege allows for monitoring of non-system processes

**Profile system performance [Administrators]**

This user privilege allows for monitoring of system processes

**Remove computer from docking station [Users, Power Users, Administrators]**

This user privilege allows for the removal of a laptop from its docking station. Since we are not running our production web server on a laptop, this setting should be changed to no users.

**Replace a process level token [Not defined]**

This user privilege allows a parent process to replace the access token on any of its spawned processes.

**Restore files and directories [Backup Operators, Administrators]**

This user privilege allows for the bypassing of local NTFS permissions for the purpose of restoring data to the local system. The restore process must utilize the NTFS backup API.

**Shut down the system [Users, Power Users, Backup Operators, Administrators]**

This user privilege allows the user or group the permission to shut down the host computer. At the console, the user must have the local logon right unless the "Allow system to be shut down without having to logon" security option is enabled.

**Synchronize directory service data [Not defined]**

This user privilege allows the synchronization of Active Directory data. This setting is not relevant on a stand-alone server.

**Take ownership of files or other objects [Administrators]**

This user privilege allows the user or group the permission to take ownership of an object with an associated access control list (ACL). This right grants ultimate permission on the host computer. This allows the changing of ACL entries regardless of current permissions.

For the demonstration system, the Users, Power Users, Backup Operators and Everyone groups can safely be removed without affecting anonymous access to the web site.

### 1.2.3 Security Options

**Additional restrictions for anonymous connections [No access without explicit anonymous permissions]**

This setting controls the amount of information an anonymous user can obtain from the host computer through a NULL (unauthenticated) session. By default, the anonymous user is a member of the "Everyone" group. The following options are available for this setting:

- None. Rely on default permissions
- Do not allow enumeration of SAM accounts and names – the "Everyone" group is replaced with the "Authenticated Users" group when accessing resource through a NULL session.
- No access without explicit anonymous permissions – the "Everyone" group is removed from the access token given to a NULL user session.

On a standalone system, "No access without explicit anonymous permissions" is the best choice. The other available options are for backward compatibility in a Windows domain environment.

**Allow server operators to schedule tasks (domain controllers only) [Disabled]**

This option allows the server operators group to schedule tasks on the local computer. Only domain controllers have a server operators group. This security option has no relevance on a stand alone server.

**Allow system to be shut down without having to log on [Disabled]**

This setting allows the bypassing of the "shutdown this computer" user right if the user has physical access to the host computer.

**Allowed to eject removable NTFS media [Administrators]**

This setting allows for the ejection of removable NTFS media. An example

would be an NTFS formatted Iomega Jaz drive or optical disk library. The demonstration system is not outfitted with a removable media drive. No group should be defined for a setting that is not required.

**Amount of idle time required before disconnecting session [15 minutes]**

This setting determines the amount of idle time in minutes that will be allowed for a client connecting through a Server Message Block (SMB) session. The default value is 15 minutes.

**Audit the access of global system objects [Enabled]**

This setting enables the auditing of access to global system objects.

**Audit use of Backup and Restore privilege [Enabled]**

This option is used in conjunction with the "Audit privilege use" user right to enable the auditing of backup and restore user privileges. This also enables the auditing of files backed up or restored through the use of those privileges.

**Automatically log off users when logon time expires [Enabled]**

For users that have logon restrictions configured for their user account, this option will forcibly log off the account when the servers time matches the users restricted time.

**Clear virtual memory pagefile when system shuts down [Enabled]**

If this option is enabled, the pagefile will be erased before the system shuts down. If physical access was gained to a server, it would be possible to gain access to the NTFS partition from a boot floppy or CD-ROM. If sensitive data (i.e. transactional data destined for another system) was in the pagefile when the system was shutdown, that data could be gleamed from the pagefile. However, this does not prevent someone from unplugging the system which would leave the pagefile intact.

**Digitally sign client communication (always) [Not Defined]**

**Digitally sign client communication (when possible) [Enabled]**

**Digitally sign server communication (always) [Not Defined]**

**Digitally sign server communication (when possible) [Enabled]**

These options allow for the forced or attempted digital signing of SMB data sent over the network between the workstation and server services. The workstation and server services on the demonstration system have been disabled through this template, so these setting have no purpose.

**Disable CTRL+ALT+DEL requirement for logon [Disabled]**

This setting enables a user to bypass the CTRL+ALT+DEL requirement for logon. Malicious applications designed to intercept a user name and password can be disguised as a logon screen. The CTRL+ALT+DEL sequence will display the windows secure logon and terminate any running application.

**Do not display last user name in logon screen [Enabled]**

This setting will keep the user name of the last logged on user from appearing automatically in the user logon prompt.

**LAN Manager Authentication Level [Send NTLM response only]**

This setting configures the default challenge/response authentication for network logons. The following options are the available:

- Send LM & NTLM responses.
- Send LM & NTLM - use NTLMv2 session security if negotiated.
- Send NTLM response only.
- Send NTLMv2 response only.
- Send NTLMv2 response only\refuse LM.
- Send NTLMv2 response only\refuse LM & NTLM.

**Message text for users attempting to log on [This is a private computer system.]**

This setting allows for the configuration of a text message to be displayed before a user logs on to the host computer.

**Message title for users attempting to log on [A T T E N T I O N !]**

This setting allows for the configuration of the title bar text for the dialog window used to display the "Message text for users attempting to log on".

**Number of previous logons to cache (in case domain controller is not available) [1 logons]**

This setting determines the number of domain logons to cache in the event a domain controller is unavailable. The demonstration system is a stand-alone server which is not a member of a domain. This setting should be set to "0" which effectively disables the setting.

**Prevent system maintenance of computer account password [Disabled]**

If this setting is enabled on a domain member server, the Netlogon

service will not negotiate password changes for the local computer account with the domain controller. The demonstration server is not a domain member, therefore will not utilize this setting.

**Prevent users from installing printer drivers [Enabled]**

Enabling this setting will limit the installation of printer drivers to the Local Administrators and Power Users groups.

**Prompt user to change password before expiration [14 days]**

This setting determines the number of days prior to password expiration to begin notifying the user to change their password.

**Recovery Console: Allow automatic administrative logon [Disabled]**

Enabling this option will allow anyone with physical access the host computer, the capability to boot into the recovery console and gain unauthenticated administrative access the system. This setting should never be enabled. This setting should not exist.

**Recovery Console: Allow floppy copy and access to all drives and all folders [Disabled]**

This setting is safe to enable as long as the "Allow automatic administrative logon" is disabled.

**Rename administrator account [Not defined]**

This option will automatically rename the local "Administrator" account to the specified value. If this option is not used, the local "Administrator" account should be renamed manually.

**Rename guest account [Not defined]**

This option will automatically rename the local "Guest" account to the specified value. The guest account is disabled by default and should remain disabled. By practice, I generally rename the local "Guest" account "Administrator".

**Restrict CD-ROM access to locally logged-on user only [Enabled]**

**Restrict floppy access to locally logged-on user only [Enabled]**

These settings are used to restrict access the local CD-ROM and/or floppy drive on the host computer. Enabling these options will restrict access to users who are logged on interactively. This policy does not prevent access to the device over the network if the device is shared. If no users are logged on locally, the device will be available over the network.

**Secure channel: Digitally encrypt or sign secure channel data (always) [Not Defined]**

**Secure channel: Digitally encrypt secure channel data (when possible) [Enabled]**

**Secure channel: Digitally sign secure channel data (when possible) [Enabled]**

**Secure channel: Require strong (Windows 2000 or later) session key [Not Defined]**

The netlogon service is responsible for the establishment of a secure channel between the domain member server and a domain controller. These settings control the use of digital signatures and encryption when setting up the RPC tunnel for a secure channel connection. The demonstration system is not a domain member and will not utilize these settings.

**Secure system partition (for RISC platforms only) [Not defined]**

This setting only applies to RISC platform servers which are no longer supported by Windows 2000.

**Send unencrypted password to connect to third-party SMB servers [Disabled]**

This setting allows the SMB redirector to send clear text passwords to third party SMB servers.

**Shut down system immediately if unable to log security audits [Not Defined]**

This setting will determine if the system will shut down if it can no longer write audit events to the security log. This option should only be enabled when auditing is more important than availability.

**Smart card removal behavior [Not Defined]**

This setting defines the default action when a smart card is removed from an attached reader. The available options are:

- No Action
- Lock Workstation
- Force Logoff

**Strengthen default permissions of global system objects (e.g. Symbolic Links) [Enabled]**

If this option is enabled, a local user will not be able to modify a global system object not created by them.

**Unsigned driver installation behavior [Do not allow installation]**

This setting determines what policy to use when a user attempts to install a driver that was not digitally signed by Microsoft's Hardware Quality Lab.

The following policies are available:

- Silently succeed
- Warn but allow installation
- Do not allow installation

## 1.3 Event Log

### 1.3.1 Settings for Event Logs

When possible, event logs should be forwarded in real time from the target system to a dedicated logging server for analysis. This can be accomplished through the use of third party software. Alternatively, the event logs can be pulled at specified intervals through scripting or resource kit tools.

**Maximum application log size [Not Defined]**

**Maximum security log size [10240 kilobytes]**

**Maximum system log size [Not Defined]**

The maximum log size settings determine the amount of space available for each event log. The combination of the 3 event logs should not exceed 80% of the available disk space if left on the system partition. By default, the event logs are stored in **%SystemRoot%\System32\Config**. If a log consolidation tool can not be used, move the event logs to an alternate drive. Detailed instructions for moving the event logs can be found in the Microsoft Knowledge Base article "Q175386" listed below:

http://support.microsoft.com/support/kb/articles/Q175/3/86.ASP.

**Restrict guest access to application log [Enabled]**

**Restrict guest access to security log [Enabled]**

**Restrict guest access to system log [Enabled]**

This option restricts guest and NULL user read access to the specified log file. By default, the security log is restricted and the Application and System logs are viewable by anyone. All logs should be restricted from viewing by non administrative personnel. Information about running services, applications and user and service accounts can be gathered by viewing the system and application logs.

***Retain application log [Not defined]***

***Retain security log [14 days]***

***Retain system log [Not defined]***

Event log retention specifies the number of days an event log will be retained before it is allowed to be overwritten. Possible values range from 1 – 365 days. If this setting is not defined, the logs will be retained indefinitely if the retention method is set to manual.

***Retention method for application log [Not Defined]***

***Retention method for security log [By Days]***

***Retention method for system log [Not Defined]***

There are three possible retention methods. If the retention is set by days, it will not overwrite the log until the value specified in the retain log setting is exceeded. If retention is set by size, it will not overwrite the log until the log reaches the size specified in the maximum log size setting. The final option is the manual option which does not allow the logs to be automatically overwritten.

***Shut down the computer when the security audit log is full [Not Defined]***

This setting should never be enabled on a production server. For medium to high security systems, a log dumping agent should be installed. There are many third party tools for dumping the event logs to a dedicated logging server. Enabling the above option opens up the server to a possible denial of service attacks in which the server is flooded with failed access attempts.

## 1.4 Restricted Groups

The web_secure.inf security configuration template specifies the following restricted groups:

- Power Users
- TelnetClients

## 1.5 System Services

Each available service can be configured as Automatic, Manual or Disabled. Additionally, permissions can be set on each service. It good security practice to disable all unnecessary services. Many of the default running services are only required for Windows NT/2000 domain controllers or member servers.

**Alerter [Disabled]**

**Application Management [Not Defined]**
**ClipBook [Disabled]**
**COM+ Event System [Not Defined]**
**Computer Browser [Disabled]**
**DHCP Client [Disabled]**
**Distributed File System [Disabled]**
**Distributed Link Tracking Client [Not Defined]**
**Distributed Link Tracking Server [Not Defined]**
**Distributed Transaction Coordinator [Not Defined]**
**DNS Client [Not Defined]**
**Event Log [Not Defined]**
**Fax Service [Disabled]**
**File Replication [Not Defined]**
**IIS Admin Service [Automatic]**
**Indexing Service [Disabled]**
**Internet Connection Sharing [Disabled]**
**Intersite Messaging [Not Defined]**
**IPSEC Policy Agent [Automatic]**
**Infrared Monitor [Disabled]**
**Kerberos Key Distribution Center [Not Defined]**
**License Logging Service [Not Defined]**
**Logical Disk Manager [Not Defined]**
**Logical Disk Manager Administrative Service [Not Defined]**
**Net Logon [Disabled]**
**NetMeeting Remote Desktop Sharing [Disabled]**
**Network Connections [Not Defined]**
**Network DDE [Not Defined]**
**Network DDE DSDM [Not Defined]**
**NT LM Security Support Provider [Not Defined]**
**Performance Logs and Alerts [Not Defined]**
**Plug and Play [Not Defined]**
**Print Spooler [Disabled]**
**Protected Storage [Not Defined]**
**QoS RSVP [Not Defined]**
**Remote Access Auto Connection Manager [Disabled]**
**Remote Access Connection Manager [Disabled]**

**Remote Procedure Call (RPC) [Not Defined]**
**Remote Procedure Call (RPC) Locator [Disabled]**
**Remote Registry Service [Disabled]**
**Removable Storage [Not Defined]**
**RunAs Service [Not Defined]**
**Security Accounts Manager [Not Defined]**
**Server [Disabled]**
**Smart Card [Not Defined]**
**Smart Card Helper [Not Defined]**
**System Event Notification [Not Defined]**
**Task Scheduler [Disabled]**
**TCP/IP NetBIOS Helper Service [Not Defined]**
**Telephony [Disabled]**
**Telnet [Disabled]**
**Terminal Services [Disabled]**
**TermServLicensing [Disabled]**
**Uninterruptible Power Supply [Not Defined]**
**Utility Manager [Not Defined]**
**Windows Installer [Not Defined]**
**Windows Management Instrumentation [Not Defined]**
**Windows Management Instrumentation Driver Extensions [Not Defined]**
**Windows Time [Not Defined]**
**Workstation [Disabled]**
**World Wide Web Publishing Service [Automatic]**

The web_secure.inf template does an excellent job of identifying and disabling services that are not required in a standalone server configuration. Microsoft has detailed information on each of the available Windows 2000 services at the following URL:

http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/deploy/prodspecs/win2ksvc.asp

This information can aid in determining which services can be safely disabled and what dependencies exist between those services.

## 1.6 Registry

A number of entries were added to the [Registry Values] section of the web_secure.inf file. Of special notice are the entries which do not have corresponding values when viewed through the GUI. The following keys aid significantly in the protection of the TCP/IP stack and the avoidance of denial of service attacks.

```
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxDataRetransmissions=4,3
;see reskit regentry.chm
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxConnectResponseRetransmissions=4,2
;MS KB Q142641
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpen=4,500
;see reskit regentry.chm
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpenRetried=4,400
;see reskit regentry.chm
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxPortsExhausted=4,1
;see reskit regentry.chm
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting=4,1
;see reskit regentry.chm
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime=4,300000
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnablePMTUDiscovery=4,0
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableDeadGWDetect=4,0
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect=4,1
;MS KB Q142641
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableSecurityFilters=4,1
;see reskit regentry.chm
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirects=4,0
;MS KB Q225344
```

## 1.7 File System

The web_secure.inf template added restrictions to many of the executables in the %WINROOT%\System32 directory and other locations. Of special mention are the restriction of the files that make up the OS/2 and Posix subsystems and MSC files which represent the administration tools available through the Microsoft Management Console. Overall, the template did an excellent job of identifying and locking down dangerous executables and subsystem components.

## Security Template Application and Testing

The security configuration template will be applied to the system using the secedit.exe command line utility. Secedit has the following syntax (from the online help) for the "analyze" and "configure" options:

**Syntax**

**secedit /analyze /db** *FileName* [/**cfg** *FileName*] [/**log** *FileName*] [/**quiet**]

**secedit /configure /db** *FileName* [/**cfg** *FileName* ] [/**overwrite**][/**areas** *area1 area2...*] [/**log** *FileName*] [/**quiet**]

**Parameters**

**/db** *FileName*
Required. Provides the file name of a database that contains the security template that should be applied.

**/cfg** *FileName*
Specifies the file name of the security template that will be imported into the database and applied to the system. This command-line option is only valid when used with the **/db** parameter. If this is not specified, the template that is already stored in the database is applied.

**/overwrite**
Specifies whether the security template in the **/cfg** parameter should overwrite any template or composite template that is stored in the database instead of appending the results to the stored template. This command-line option is only valid when the **/cfg** parameter is also used. If this is not specified, the template in the **/cfg** parameter is appended to the stored template.

**/areas** *area1 area2...*
Specifies the security areas to be applied to the system. If an area is not specified, all areas are applied to the system. Each area should be separated by a space.

| Area name | Description |
|---|---|
| SECURITYPOLICY | Local policy and domain policy for the system, including account policies, audit policies, and so on. |
| GROUP_MGMT | Restricted group settings for any groups specified in the security template |
| USER_RIGHTS | User logon rights and granting of privileges |
| REGKEYS | Security on local registry keys |
| FILESTORE | Security on local file storage |
| SERVICES | Security for all defined services |

**/log** *FileName*
Specifies the file name of the log file for the process. If it is not specified, the default path is used.

**/quiet**
Suppresses screen and log output.

The web_secure.inf security template has been copied to the root of drive E.

The following command has been run to apply the template to the local computer:

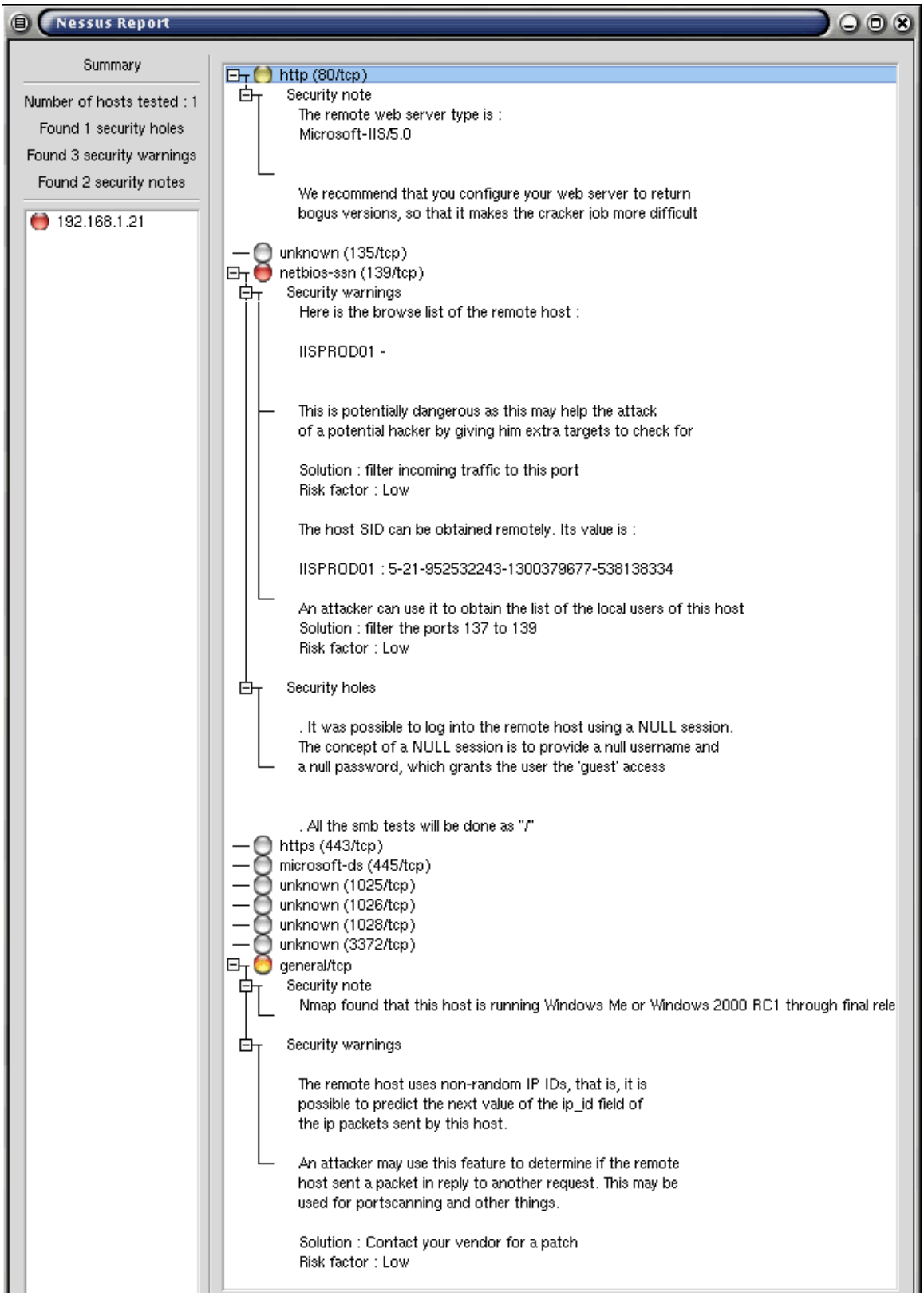
```
secedit /configure /db e:\web_secure.sdb /cfg e:\web_secure.inf /log e:\web_secure.log
```

The resulting web_secure.log file is reviewed to determine the successful application of the template file. Any errors in the process are recorded in the log file. Several errors were logged due to the non-existence of files and services on the demonstration system. These errors can be safely ignored if in fact the files and services are not installed.

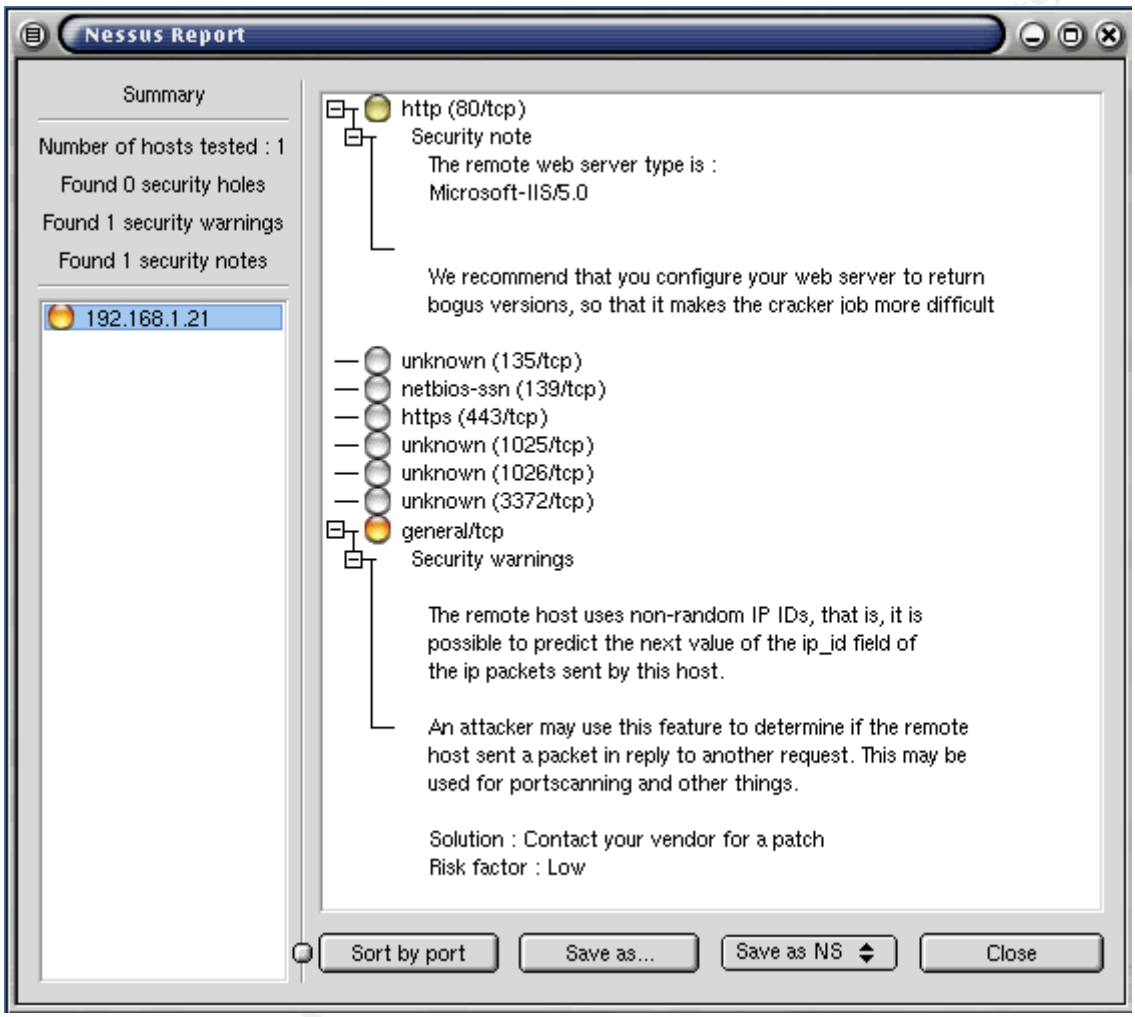
Prior to the application of the web_secure.inf template, the demonstration system was scanned using the Nessus security scanner version 1.0.9 running on RedHat Linux version 7.2. Nessus is freely available at the following URL:

http://www.nessus.org

The output of the security scan is listed on the next page. Note the security hole listed under netbios-ssn (139/tcp) specifying it was possible to log into the remote host using a NULL session. Also note the host name, SID and operating system information were available as well. The security template setting "Additional restrictions for anonymous connections [No access without explicit anonymous permissions]" will block the unauthenticated access to sensitive information. See the follow up scan on page 32.



Following the application of the security configuration template, nessus was run again yielding the following results:

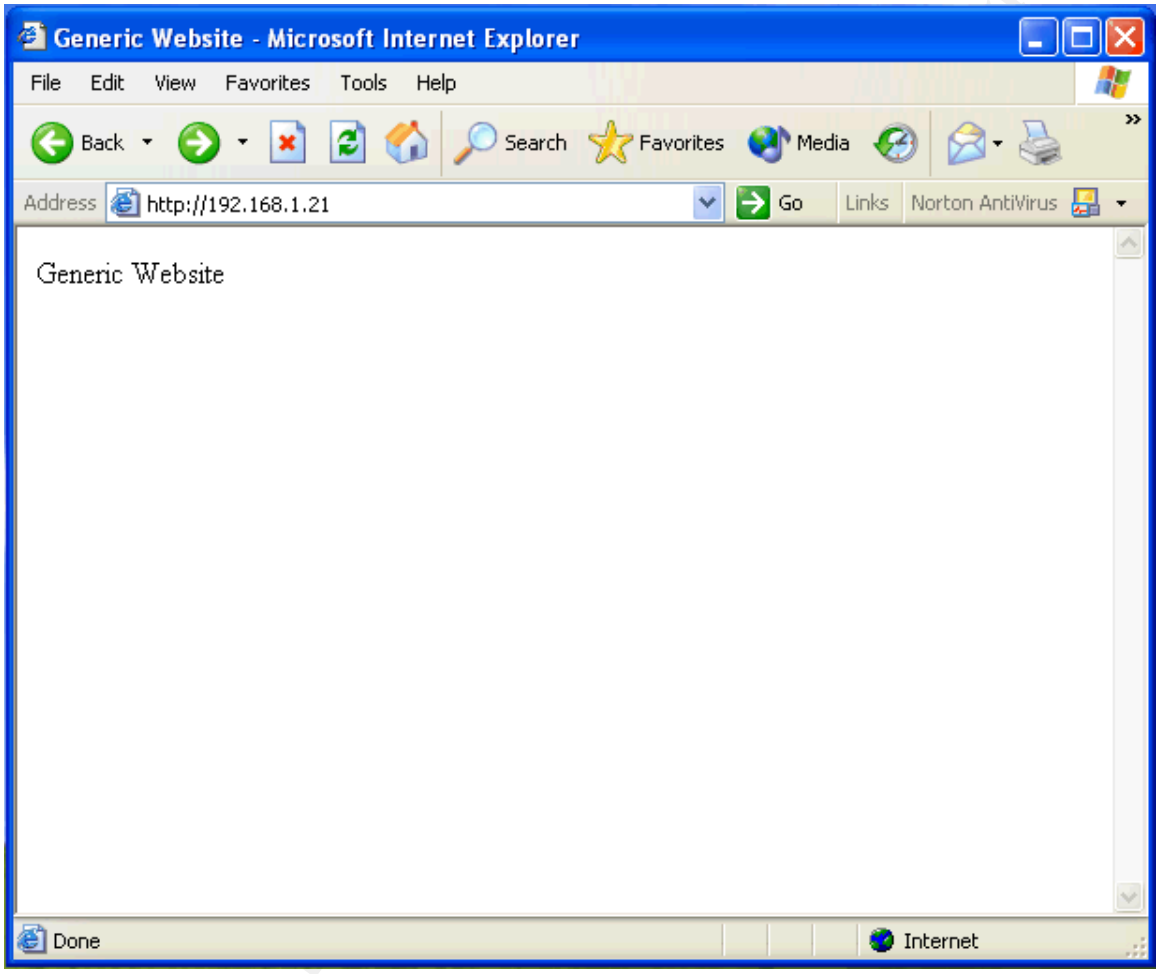



The security issues around unauthenticated access have been accommodated by the security configuration template. We can verify that the web server is functional by connecting through Internet Explorer. The following simple html code was placed in the default.htm file to test the functionality of the web server:

```
<html>
<head>
<meta http-equiv="Content-Language" content="en-us">
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
<title>Generic Website</title>
</head>
```

<body>
Generic Website

</body>
</html>

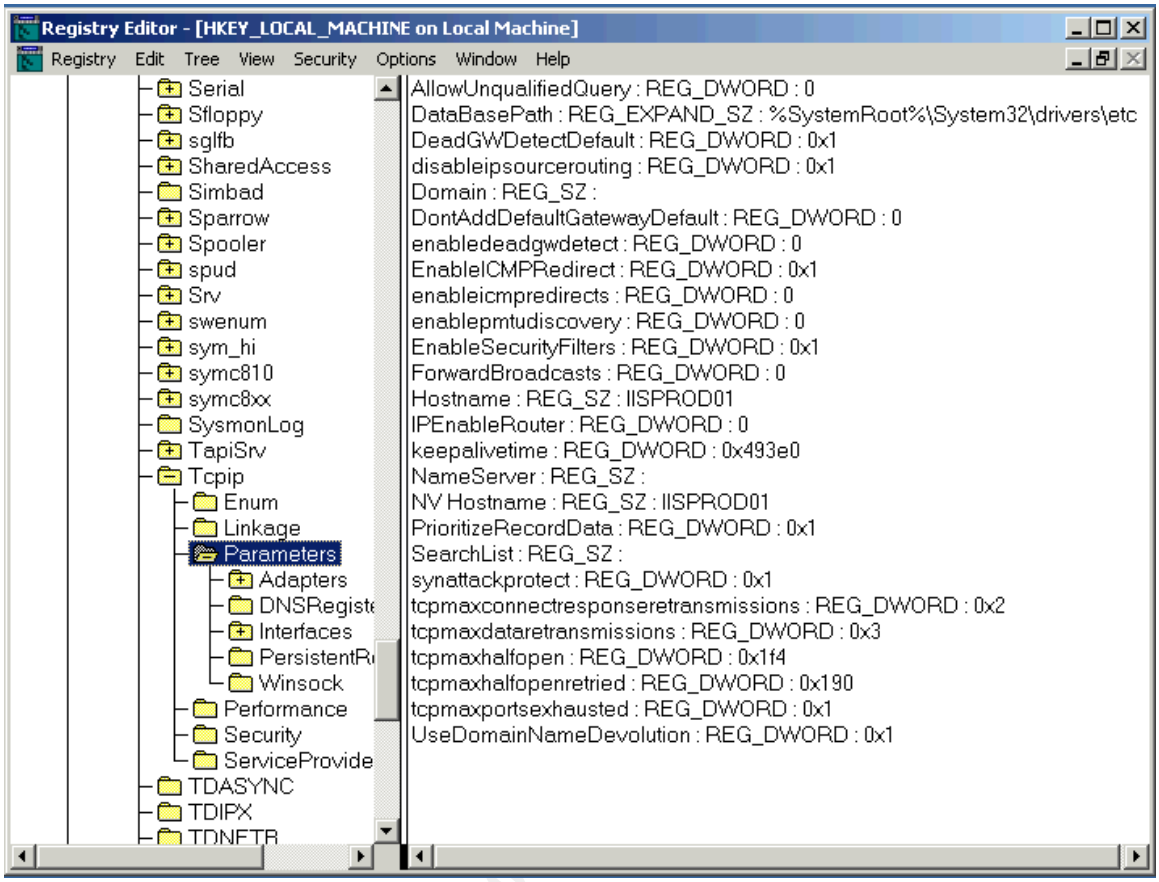



Following the application of the web_secure.inf template, the web site is still available and responding to requests on port 80. Also, note that this is an anonymous connection utilizing the permissions granted to the IUSR_IISPROD01 account which has been granted NTFS permissions Read and List folder contents to the root web directory.

The following screen shot shows the Registry Key:

HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

This demonstrates the successful application of the [Registry Values] section of the web_secure.inf template.

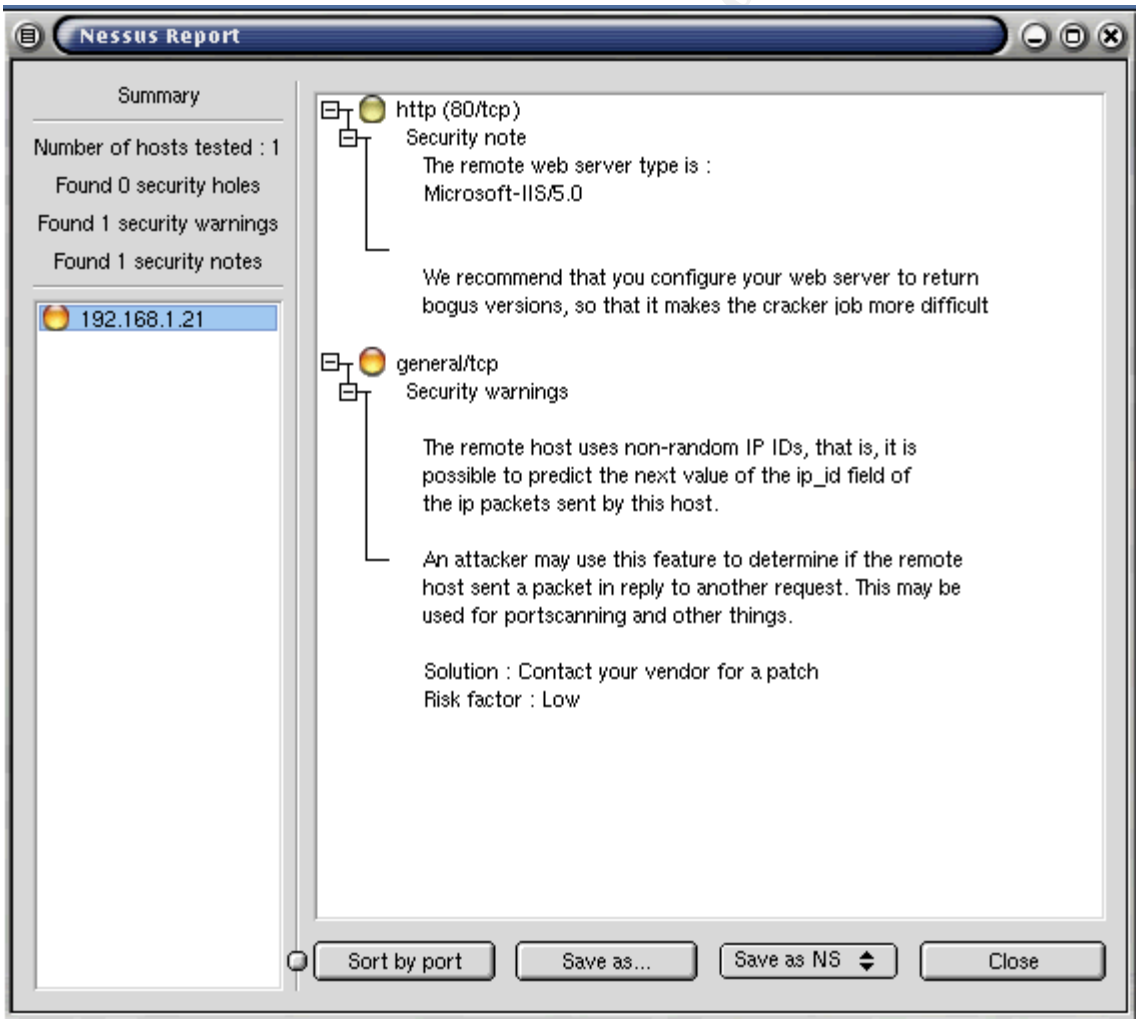


## Additional Security using IPSec Port Filters

For an additional level of security on our production web servers, IPSec static port filters will be configured to block all traffic to the server not destined to TCP port 80. This is accomplished through the following command lines:

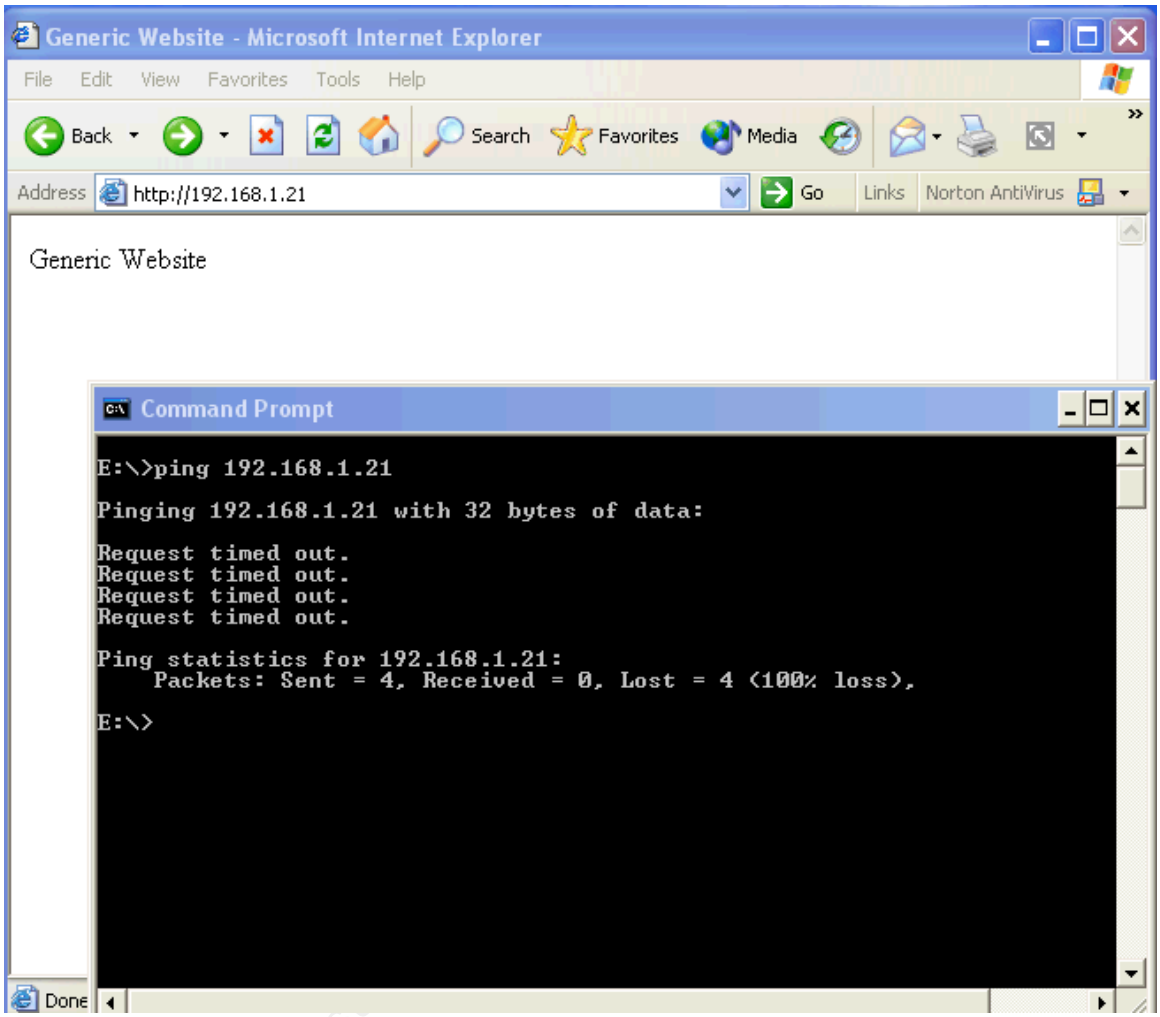
ipsecpol –w REG –p "Secure Web Server" –r "All IP Traffic" –n BLOCK –x –f 0+*
ipsecpol –w REG –p "Secure Web Server" –r "Web Traffic" –n PASS –x –f 0:80+*::TCP

Following the port filtering configuration, nessus was run again yielding the following results:




The port scan shows that all the previously available ports are no longer

responding. Additionally, ICMP ping requests are not responding, but the website is still available.

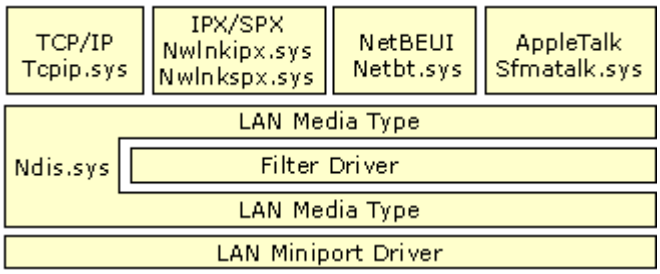



Internet Protocol Security (IPSec) is primarily known for authentication and encryption; it is also designed for static packet filtering. IPSec is defined in RFC 2401 "Security Architecture for the Internet Protocol". The term "selector" in the RFC is equivalent to the term "filter" in the Microsoft IPSec implementation. Section 4.4.2 of the RFC defines the use of selectors in IPSec.

http://www.faqs.org/rfcs/rfc2401.html

When a local IPSec Policy is assigned, the IPSec Policy Agent Service uses the policy information stored in the registry to configure the IPSec Driver. The IPSec Driver (ipsec.sys) does the packet filtering work. The IPSec "filter driver" sits between the NDIS driver at the data link layer (layer 2) and the TCPIP driver at the network layer (layer 3).

**Table 1**




The IPSECPOL.EXE is a command line tool for working with IPSec rules and filters. The tool is available in the Windows 2000 Resource Kit or in the IIS Lockdown Tool Kit:

http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/downloads/iislock.asp

Required files:

ipsecpol.exe
text2pol.dll
ipsecutil.dll

The IPSECPOL.EXE has numerous command line options. The following is a summary of the command line options that were used for the lockdown of the web server:

| | Source IP Destination IP |
|---|---|
| -f | Filter List [A.B.C.D/mask:port+A.B.C.D/mask:port:protocol] Wildcards are accepted and mask and port are optional. |
| -p | Policy name in quotes "" |
| -x | Assigns the policy specified by –p |
| -n | Filter action (PASS or BLOCK) for dynamic rules, the filter is surrounded by parenthesis () for PASS and brackets [] for BLOCK. |
| -w | Write the policy to (REG or DC) Registry or Domain. |
| -r | Rule name in quotes "" |

There is no limit on the number of policies that can be created. However, only one policy can be assigned at one time.

Entries in the IP filter list define packet matching criteria for different types of protocol traffic. Custom filters can be created to handle just about any scenario. Filters can match packets based on the following packet components:

- Source IP address, DNS name or subnet
- Destination IP address, DNS name or subnet
- Source port

- Destination port
  Protocol type (Any, EGP, HMP, ICMP, RAW, RDP, RCD, TCP, UDP, XNS-IDP, and Other)

Each filter can be also be mirrored. Mirroring duplicates the source and destination address, for the filter, in the opposite direction. When multiple filters are used, filter lists which have more specific information take precedence over filter lists that have less specific information. For example, **TCP port 80** is more specific than **All IP traffic**.

ipsecpol –w REG –p "Secure Web Server" –r "Web Traffic" –n PASS –x **–f 0:80+*::TCP**

Filter actions define what the rule will do when a packet match occurs. The following three actions can be taken:

- Permit the packet
- Block the packet
- Negotiate Security

The permit option will pass the packet up the stack to the TCPIP driver. If the block option is selected, the packet will be placed into the bit bucket. The negotiate security option gets into the authentication and encryption capabilities of IPSec.

ipsecpol –w REG –p "Secure Web Server" **–r "Web Traffic" –n PASS** –x –f 0:80+*::TCP

Security rules are created when an IP filter list is associated with a filter action. This is the glue that binds all the components together. There are a few filter exemptions built into the IPSec driver. The following traffic types will not be filtered no matter how the security rules are configured:

- Kerberos (Port 88, TCP/UDP)
- IKE (Port 500, UDP)
- RSVP (Protocol 46)
- IP Broadcast
- IP Multicast

The configuration information is stored in the registry key:
HKLM\Software\Policies\Microsoft\Windows\IPSec\Local

Ipsecpol **–w REG –p "Secure Web Server"** –r "Web Traffic" –n PASS –x –f 0:80+*::TCP

## References

Fossen, Jason. Windows 2000 IPSec & VPNs (version 3.0.1, 08 Aug 2001). SANS Institute.

Fossen, Jason. Securing Internet Information Server 5.0 (version 10.2, 09 Aug 2001). SANS Institute.

Cox, Philip. Hardening Windows 2000. (version 1.2, 25 May 2001). System Experts Corporation,

Windows 2000 Server Resource Kit. Redmond: Microsoft Press, 2001.

Microsoft Corporation TechNet Knowledge Base, Multiple Articles, http://www.microsoft.com/technet, November 2001.