Global Information Assurance Certification Paper

SANS/GIAC – Windows NT Security

Practical Assignment for SNAP San Jose – May 8-13, 2000

Version 1.0

Author: Stefan Mititelu

The assignment I have chosen to work on is a step-by-step process of strengthening an NT server chosen to be a Primary Domain Controller, by starting with the initial setup as Microsoft delivers the NT server software, through running some Security/Auditing tools against this servers, all the way to applying needed fixes for decreasing the risks associated to the initial "out-of-the-box" configuration.

1. Initial setup

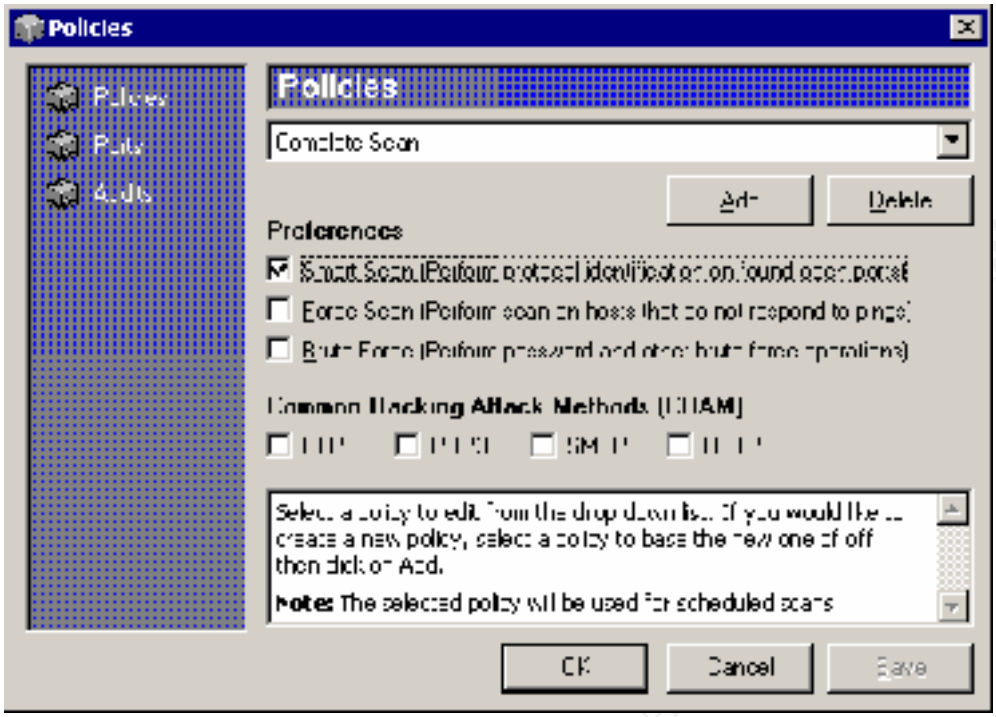
I will skip here the obvious steps taken to install an NT server (use floppies and CD), and I will just specify some specifics related to the default setup:

a. The default NT server delivered in the US is the one with Service Pack 1 – 128-bit encryption;
b. I have chosen to use the whole drive of the PC as one single partition, formatted as NTFS;
c. The address assignment is from the "private" pool (RFC 1918) = 172.16.4.212;
d. The name of the PDC = SANS, and the name of the domain is SANSDOM;
e. I have chosen to start with a strong password from the beginning, and let the tools I was going to use decide if the password was considered strong enough (if able to do so);
f. I have decided to try two of the best tools available as commercial products for the NT users, i.e. Retina var. 2.0 (www.eeye.com) and Webtrends Security Analyzer ver. 3.5 (www.webtrends.com). I have used the evaluation versions of these products, with the most updated patches as of 06/08/2000.

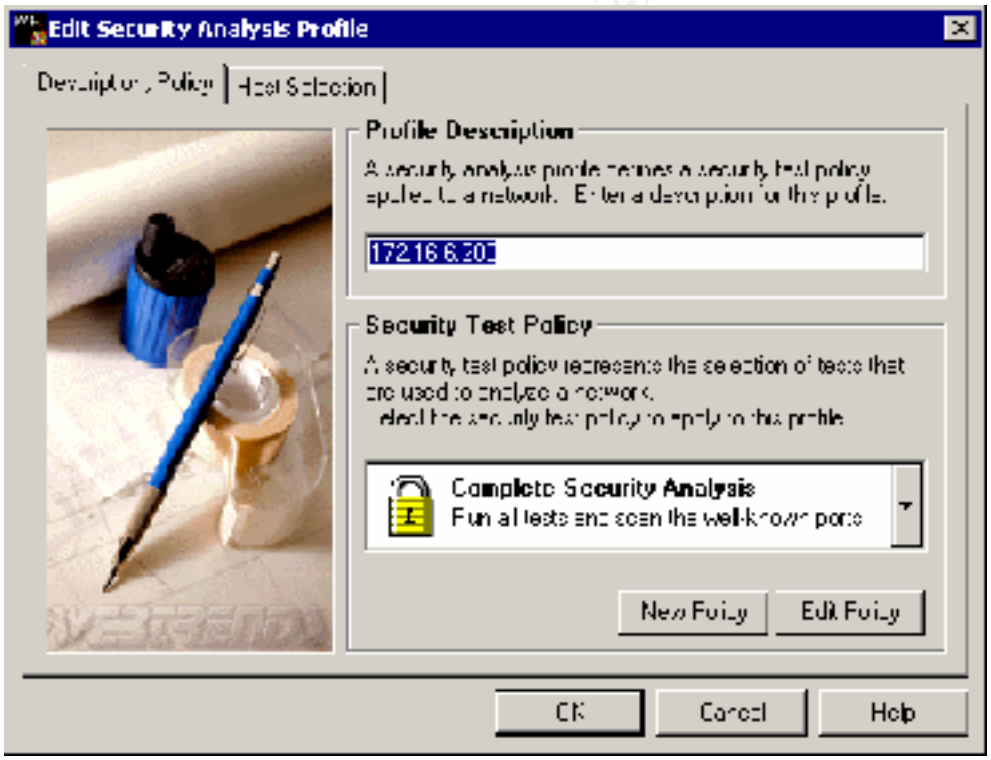
2. First security test

After the installation the first batch of security tests was run. The setup choices for the two test packages were as follows:

Retina:



Webtrends:



Results:

Retina version 2.0 having run on a system having only SP1 installed:

Address: 172.16.4.212
This is the IP (Internet Protocol) address of the machine, a single machine might have multiple IP adresses associated with it.

Report Date: 06/09/00 06:53:17AM
This is the date and time the scanner started to perform the auditing process. The date and time is reported off the machine local time zone.

Domain Name: SANS
This is the domain name of the machine. There can be multiple domain names assigned to a single IP (Internet Protocol) address or one domain name assigned to multiple IP addresses.

Status: Server Alive
No More Details Available

Audits: 172.016.004.212

FTP Servers: Anonymous FTP
Medium Risk Level
It is recommended that you disable anonymous FTP access if it is not needed. Anonymous FTP access can lead to an attacker gaining information about your system that can possibly lead to them gaining access to your system.
How To Fix:
Follow your FTP server instructions on how to disable anonymous FTP.

Accounts: Administrator - Default Administrator Account
Medium Risk Level
The default Windows NT Administrator account exists on this machine. This account can be a basis for brute force attacks, as it cannot be locked out by too many incorrect

password attempts.
How To Fix:
It is suggested to rename the administrator account.
1. Load User Manager
2. Select Administrator
3. Select Rename from under the User menu.

Accounts: IUSR_SANS - Password Does Not Expire
Medium Risk Level
If a users password does not expire you allow a remote attacker endless amount of time to try to figure out your users password. It is recommended that you make all users passwords expire unless the user account is used for a system service.
How To Fix:
Remove the password never expires option from the user account.
1. Open User Manager.
2. Select the user from the list.
3. Select Properties from the User menu.
4. Uncheck "Password Never Expires."
5. Click "Ok".

Accounts: Administrator - Password Does Not Expire
Medium Risk Level
If a users password does not expire you allow a remote attacker endless amount of time to try to figure out your users password. It is recommended that you make all users passwords expire unless the user account is used for a system service.
How To Fix:
Remove the password never expires option from the user account.
1. Open User Manager.
2. Select the user from the list.
3. Select Properties from the User menu.
4. Uncheck "Password Never Expires."
5. Click "Ok".

Accounts: Guest - Password Does Not Expire
Medium Risk Level
If a users password does not expire you allow a remote attacker endless amount of time to try to figure out your users password. It is recommended that you make all users passwords expire unless the user account is used for a system service.
How To Fix:
Remove the password never expires option from the user account.
1. Open User Manager.
2. Select the user from the list.
3. Select Properties from the User menu.
4. Uncheck "Password Never Expires."
5. Click "Ok".

IP Services: gopher service

Medium Risk Level
The gopher service is a rather old unsupported protocol whose predecessor is HTTP.
How To Fix:
Disable the Gopher service.
If you are running a Unix OS disable the gopher service in the /etc/inetd.conf file. Restart inetd so changes will take effect.
If you are running Windows NT then go to Control Panel/Services and disable "Simple TCP/IP services."

Accounts: Guest - Cannot Change Password
Low Risk Level
It is recommended that a machine be set up so that a user has the ability to change their password; otherwise password changes will occur less frequently. However, if this account is one that is used by a system service the ability to change passwords is not something that is required.
How To Fix:
Allow the user to change their password by doing the following:
1. Open User Manager.
2. Select the user from the list box.
3. Select properties from the User menu.
4. Uncheck "User Cannot Change Password."
5. Click "OK".

Accounts: IUSR_SANS - Cannot Change Password
Low Risk Level
It is recommended that a machine be set up so that a user has the ability to change their password; otherwise password changes will occur less frequently. However, if this account is one that is used by a system service the ability to change passwords is not something that is required.
How To Fix:
Allow the user to change their password by doing the following:
1. Open User Manager.
2. Select the user from the list box.
3. Select properties from the User menu.
4. Uncheck "User Cannot Change Password."
5. Click "OK".

Web Servers: IISAdmin
Low Risk Level
The /iisadmin folder is used to remotely administer the Internet Information Server.
How To Fix:
It is recommended that you remove the /iisadmin virtual directory if web based administration of IIS is not needed.

Accounts: Guest - User Never Logged On
Information Risk Level
It is suggested that you review this user account. If it is not needed or was not created by

an administrator of your network, it is suggested that you disable or delete it.
How To Fix:
To delete the account:
1. Open User Manager
2. Select the account to delete
3. Press the "Delete" key
4. Click "Ok"

To Disable the account:
1. Open User Manager
2. Select the account to disable
3. Select Properties from the User menu
4. Check "Account Disabled"
5. Click "Ok"

Machine: 172.016.004.212

File Share Name: SANS
This is the name used for the remote systems file sharing. This is typically the same as the remote netbios name.

MAC Address: 0 10 5A A6 70 20
The MAC (Media Access Control) Address is a number assigned to the remote computers network card. This number can be used to know what type of network card is installed in the remote machine.
NIC Brand: 3COM CORPORATION

Netbios Name: SANS
This is the name assigned to the remote computer. The Netbios name is used when doing file and print sharing across netbios networks.

Netbios Workgroup: SANSDOM
This is the workgroup that the remote computer is apart of. Typically in an office enviornment, workstations are joined together by a workgroup. For instance all of the accounting department might be joined by the workgroup "accounting." This workgroup makes it easier for people within the accounting department to share files with each other.

OS Name: WindowsNT
This is the remote OS (Operating System). For example, Windows, Linux, Solaris etc...

Ports: 172.016.004.212

21: FTP - File Transfer Protocol [Control]
Banner: 220 sans Microsoft FTP Service (Version 2.0).
Protocol: FTP

70: GOPHER - Gopher
No More Details Available

80: WWW-HTTP - World Wide Web HTTP (Hyper Text Transfer Protocol)
Protocol: HTTP
Version: Microsoft-IIS/2.0

135: RPC-LOCATOR - RPC (Remote Procedure Call) Location Service
No More Details Available

139: NETBIOS-SSN - NETBIOS Session Service
No More Details Available

Services: 172.016.004.212

Browser: Computer Browser
Browser (Computer Browser) maintains an up-to-date list of computers on your network and supplied the list to requesting programs.

Browser Service Elections
No More Details Available

Domain Master Browser

No More Details Available

IIS (Internet Information Server)
IIS (Internet Information Server) is a bundled software package that includes, ftp, smtp, and http server software.

LanmanServer: Server
Provides RPC support and file, print, and named pipe sharing.

LanmanWorkstation: Workstation
Provides network connections and communications.

LicenseService: License Logging Service
License Logging Service.

Master Browse
No More Details Available

Messenger Service
No More Details Available

Netlogon: Net Logon
Supports pass-through authentication of account logon events for computers in a domain.

RPCLOCATOR: Remote Procedure Call (RPC) Locator
(RPC) Remote Procedure Call Locator. Manages the RPC name service database.

RpcSs: Remote Procedure Call (RPC)
(RPC) Remote Procedure Call. Provides the endpoint mapper and other miscellaneous RPC services.

Spooler: Print Spooler

Print Spooler. Loads files to memory for later printing.

Shares: 172.016.004.212

ADMIN$: Remote Admin
Default Administration share. The admin$ share is a mapping to \winnt\system32. An attacker could use access to this share to remotely run l0pht crack against your server to find out your passwords.

C$: Default share
This is a default share created when the server first boots. It is a mapping to the root of your C drive.

IPC$: Remote IPC
This is a default share created when the server first boots. Responsible for Inter Process Communications.

NETLOGON: Logon server share
No More Details Available

Users: 172.016.004.212

Administrator: Built-in account for administering the computer/domain
Last logon: Fri Jun 09 05:36:09 2000
Last Logoff: unknown
Password Age: 0 days
Expires: never
Logon Server: *
Max storage: unlimited
Number of Logons: 1
Privilege: Administrator
Password expired: no
RID: 500
Bad PW Count: 0

Country Code: 0

Guest: Built-in account for guest access to the computer/domain
Account Disabled: True
Last logon: never
Last Logoff: unknown
Expires: never
Logon Server: *
Max storage: unlimited
Number of Logons: 0
Privilege: Guest
Password expired: no
RID: 501
Bad PW Count: 0
Country Code: 0

IUSR_SANS: Internet Server Anonymous Access
Full Name: Internet Guest Account
Last logon: Fri Jun 09 05:54:54 2000
Last Logoff: unknown
Password Age: 0 days
Expires: never
Logon Server: *
Max storage: unlimited
Number of Logons: 2
Privilege: User
Password expired: no
RID: 1001
Bad PW Count: 0
Country Code: 0

Webtrends version 3.5 having run on the system with SP1 installed

Detected Vulnerabilities and Fixes
Vulnerabilities/Fixes
High - Microsoft Office VBA shell/Text-ISAM patch Jet is a Microsoft database engine that is used by products such as Microsoft Office 97 and Office 2000. There aretwo serious vulnerabilities in the unpatched versions of the Jet database engine. The first is the VBA Shell vulnerability. The VBA Shell vulnerability affects all versions of Jet except Jet 4.0. An attacker who exploits the VBA shell vulnerability can execute an operating system commandembedded within a database query when the query is processed. This could allow a spreadsheet, database, orother application file containing such a query to take almost any action on the user's computer when thequery is executed. An attacker could read, write or delete files, execute commands, or start and stopservices, as a few examples.

The second is the Text-ISAM vulnerability, which affects all versions of Jet. Jet provides a way to modifythe contents of text files, as a way of allowing data exchange between it and other systems. However, anattacker could use this capability to modify system files via a database query.

Microsoft Office uses the Jet engine, and Office users are particularly at risk from these vulnerabilities.The VBA Shell vulnerability affects all versions of Office prior to Office 2000, and also affects onemember of the Office 2000 suite, Access 2000. The Text I-ISAM vulnerability affects all versions of Office.

The vulnerability poses an especially serious threat to Office users for three reasons:
- Scenarios for exploiting the vulnerabilities via Office documents are publicly known and readily available. Sampleexploit code has been posted on several Internet security sites.
- The widespread use of Office would make it an attractive target for mounting attacks via these vulnerabilities.
- The ability of Office documents to perform Document Object Hosting would permit users to be attacked simplyby visiting a malicious user's web site.

In addition to Office, Jet is used by many other Microsoft products, including but not limited to:
Microsoft Visual Studio
Microsoft Project
Microsoft Publisher
Microsoft Streets & Trips
For a complete listing of Microsoft products that use Jet, consult Microsoft Knowledge Base article Q141796,"Identify the Jet Database Engine Components" at:
http://support.microsoft.com/support/kb/articles/Q141/7/96.asp

Jet also is used by many third-party products. It is difficult to provide a listing of all of these products, becauseJet is freely available for use by third parties.
For more information on these vulnerabilities, please see the Microsoft Security bulletin at:
http://www.microsoft.com/Security/Bulletins/ms99-030.asp

Fix - Apply the Microsoft Office Service Release

The patch for the Microsoft Office VBA shell/Text-ISAM vulnerability has been incorperated into the Microsoft Office service release 4.0.

The fix eliminates the VBA Shell vulnerability by creating and operating in a mode called "sandbox mode". When Jet is insandbox mode, it restricts what operating system commands can be included in database queries.For example, commands that simply report information are still allowed, but commands that could beused to take malicious action on the computer are not.

The fix eliminates the Text-ISAM vulnerability by specifying a list of file types that Jet database queriesmay not write to. This list is configurable, and users can change which file types are on this list.
You can download and apply Microsoft Office service release 4.0 from the following location:
http://download.microsoft.com/download/office2000dev/SP/1/win98/EN-US/jet40sp4.exe

After the patch is applied, the settings for sandbox mode are stored in the registry, in the following registry key:
Hive:HKEY_LOCAL_MACHINE
Key:SOFTWARE\Microsoft\Jet\4.0\Engines
Name:SandboxMode
Type:DWORD
The data in the SandboxMode key indicates the level of permissiveness for sandbox mode.
You can set the key to the following values, with 0 (zero) being most permissive and 3 being least permissive:
0 - Sandbox mode is disabled at all times.
1 - Sandbox mode is used for Access applications, but not for non-Access Applications.
2 - Sandbox mode is used for non-Access applications, but not for Access Applications. (This is the default value.)
3 - Sandbox mode is used at all times.
For more information on sandbox mode, please visit:

http://support.microsoft.com/support/kb/articles/q239/4/82.asp

After the patch is applied, the settings for the Text-ISAM permissible file types for write are stored in the registry, in the following registry key:
Hive:HKEY_LOCAL_MACHINE
Key:Software\Microsoft\Jet\4.0\Engines\Text
Name:DisabledExtensions
Type:REG_SZ
The data in the DisabledExtensions key indicates what file types cannot be written to by Jet database queries. By default,the following values are added to the list:
bat
cmd
ini
sys
inf
vbs
js
You can add additional file types to this list by adding them to the registry key described above.
For more information on this feature, please visit:
http://support.microsoft.com/support/kb/articles/q239/4/71.asp

High - Guest access to application log

Guest users have access to the application log, which records events logged by applications running on the system. The application log can contain crucial information that in the wrong hands presents a security violation.

Fix - Disable Guest access to the NT application log

Disable guest access to the application log.
This is done by setting the following registry key's value:
Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Services\EventLog\Application
Name: RestrictGuestAccess
Type: REG_DWORD
Value: 1
The key described above may not exist by default, and may need to be created.

High - Guest access to security log

Guest users have access to the security log, which records security related events such as logons, policy changes and account management. The security log can contain crucial information that in the wrong hands presents a security violation.

Fix - Disable Guest access to the NT security log

Disable guest access to the security log.
This is done by setting the following registry key's value:
Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Services\EventLog\Security
Name: RestrictGuestAccess
Type: REG_DWORD
Value: 1
The key described above may not exist by default, and may need to be created.

High - Guest access to system log

Guest users have access to the system log, which records system events such as a driver failing to load or changes to component settings. The system log can contain crucial information that in the wrong hands presents a security violation.

Fix - Disable Guest access to the NT system log

Disable guest access to the system log.

This is done by setting the following registry key's value:
Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Services\EventLog\System
Name: RestrictGuestAccess
Type: REG_DWORD
Value: 1
The key described above may not exist by default, and may need to be created.

High - Malformed Resource Enumeration patch

A vulnerability exists in Windows NT 4.0 Server and Workstation that poses a denial of service threat. An invalid argument sent via IPC to the Service Control Manager can cause the named pipes to fail. If the named pipes fail, a variety of services and applications can fail.The computer then must be restarted to resume normal operations.
For more information on this issue, please see the Microsoft Security Bulletin at:
http://www.microsoft.com/security/bulletins/ms99-055.asp

Fix - Install the Resource Enumeration patch

Microsoft has released a patch that fixes this problem. The patch is available for download from the sitelisted below:
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=16382
For more information on this issue, please see the Microsoft Security Bulletin at:
http://www.microsoft.com/security/bulletins/ms99-055.asp

High - Syskey Keystream Reuse

This vulnerability allows a particular cryptanalytic attack to be effective againstSyskey, significantly reducing the strength of the protection it offers.

For more information on this issue, please see the Microsoft Security Bulletin at:
http://http://www.microsoft.com/technet/security/bulletin/ms99-056.asp
or
the FAQ of this bulletin at:
http://www.microsoft.com/technet/security/bulletin/fq99-056.asp

This vulnerability does not affect Windows 2000.

Fix - Install the Syskey Keystream Reuse hotfix

The hotfix patch for this Microsoft Security Bulletin can be found at:
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=16798

High - Check for NT Service Pack 3

Service Packs 3 and above for Windows NT 4.0 fix many security issues, including some important Denial of Service vulnerabilities. It also adds some usefulsecurity features such as the ability to restrict anonymous user sessions. ServicePack 3 is considered by many the minimum requirement for Service Packs to secure your network. Subsequent Service Pack releases address even more security issues.

Fix - Install Windows NT SP3 or greater

To resolve this problem, obtain the latest service pack for Windows NT version 4.0. For information on obtaining the latest Service Pack, please visit:
http://support.microsoft.com/support/kb/articles/Q152/7/34.asp

High - CSRSS worker thread exhaustion hotfix not applied

Windows NT 4.0 Server and Workstation have a threading problem which can cause a denial of servicefor systems that allow interactive logons. The problem exists in the CSRSS.EXE service, the Win32 subsystemprovides Windows NT services to client processes running on the local machine. When a client processrequests a Win32 service, CSRSS generates a worker thread to service the request.
When all worker threads are occupied, the request waits in a queue until one of the threads completesits work and becomes available.
The vulnerability results from the way CSRSS handles requests requiring user input. A worker thread needinguser input will display a message box and wait for the user to provide input. The thread will remain occupieduntil it receives the input. If all CSRSS worker threads in are waiting for user input, no other requests can beserviced. This causes the machine to hang until the user input is provided. Once the input is received, processingreturns to normal.
For more information on this issue, please see the Microsoft Security Bulletin at:
http://www.microsoft.com/security/bulletins/ms99-021.asp

Fix - Install the CSRSS worker thread exhaustion hotfix

Microsoft has supplied a patch for this issue. You can download and apply the hotifx from:
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/Hotfixes-PostSP5/CSRSS-fix/ For more information on this issue, please see the Microsoft Security Bulletin at:
http://www.microsoft.com/security/bulletins/ms99-021.asp

High - GetAdmin privilege elevation

The GetAdmin hotfix has not been applied to the host.
The GetAdmin utility grants administrator rights to normal users. With administrator rights, a normal user can compromise system security.
For more information on the GetAdmin utility, see Knowledge Base article Q146965, at:
http://support.microsoft.com/support/kb/articles/Q146/9/65.asp

Fix - Apply Windows NT GetAdmin hotfix

Apply the getadmin-fix hotfix. See:
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/getadmin-fix/README.TXT
for instructions on how to apply the hotfix.
The download files are located at:
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/getadmin-fix

For more information on the GetAdmin utility, see Knowledge Base article Q146965 at:
http://support.microsoft.com/support/kb/articles/Q146/9/65.asp .

High - Kernal out of date

On a regular basis Microsoft bundles HotFixes and updates for NT4 into Service Packs. By upgrading to the latest Service Pack you are assured of having the latest upgrades and fixes for your NT4 machine.

Fix - Update Kernal

This computer does not have the latest Service Pack installed, and it is recomened that you upgrade your machine to the latest Service Pack.
You can get the latest recomened Service Pack at:
http://www.microsoft.com/ntserver/nts/downloads/default.asp#RecommendedUpdates

High - Malformed LSA hotfix not applied

A vulnerability exists in Windows NT 4.0 Server and Workstation that poses a denial of service threat. Amalformed request to the Local Security Authority (LSA) service can cause the service to stop responding.The computer then must be restarted to resume normal operation.
For more information on this issue, please see the Microsoft Security Bulletin at:
http://www.microsoft.com/security/bulletins/ms99-020.asp
or
Microsoft Knowledge Base (KB) article Q231457, Malformed Request Causes LSA Service to Hang, at:
http://support.microsoft.com/support/kb/articles/q231/4/57.asp

Fix - Install the LSA3 hotfix

Microsoft has released a patch that fixes the problem. The patches are available for download from the sitelisted below:
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP5/LSA3-fix/
For more information on this issue, please see the Microsoft Security Bulletin at:
http://www.microsoft.com/security/bulletins/ms99-020.asp
or
Microsoft Knowledge Base (KB) article Q231457, Malformed Request Causes LSA Service to Hang, at:
http://support.microsoft.com/support/kb/articles/q231/4/57.asp

High - Windows NT SMB denial of service

Windows NT servers (including those with Service Pack 3 and all hotfixesapplied) are vulnerable to a denial of service attack. During the processingof a Server Message Block (SMB) logon request, if the SMBlogon packet is incorrectly processed, memory corruption results in the NTkernel. When this happens, a blue screen error message appears and themachine has to be rebooted.
For more information on this vulnerability, please see the Microsoft Knowledge Base article"Denial of Service Attack Causes Windows NT Systems to Restart" at:
http://support.microsoft.com/support/kb/articles/q180/9/63.asp

Fix - Install Windows NT SP4 or greater to address SMB denial of service

Microsoft provided a fix for this problem in Windows NT Service Pack 4.
For information on obtaining the latest Service Pack, please visit:
http://support.microsoft.com/support/kb/articles/Q152/7/34.asp
For more information on this vulnerability, please see the Microsoft Knowledge Base article"Denial of Service Attack Causes Windows NT Systems to Restart" at:
http://support.microsoft.com/support/kb/articles/q180/9/63.asp

High - Windows NT Telnet to Port 135 denial of service

Telnetting to Port 135 can cause 100% CPU usage. An attacker can use telnet to connectto port 135 on a Windows NT computer, then type ten or more random characters and disconnect. CPUusage on the server will jump to 100% and will not decrease until the server is restarted. This problemis caused by a problem in Microsoft's Remote Procedure Calls (RPC) in Windows NT.
For more information on this vulnerability, please see Microsoft Knowledgebase article Q162567,"Telnet to Port 135 Causes 100% CPU Usage" at:
http://support.microsoft.com/support/kb/articles/q162/5/67.asp

Fix - Install Windows NT SP3 or greater to correct Telnet to port 135 Denial of Service issue

Microsoft has fixed the Telnet to port 135 Denial of Service issue with Service Pack 3. Forinformation on obtaining the latest Service Pack, please visit:
http://support.microsoft.com/support/kb/articles/Q152/7/34.asp

Medium - Anonymous FTP

Anonymous FTP accounts pose security risks unless properly configured and administered.
For more information about anonymous FTP vulnerabilities, see:
ftp://info.cert.org/pub/tech_tips/anonymous_ftp_abuses

Fix - Restrict permissions for anonymous FTP account

Closely monitor anonymous connects to the FTP server. In addition, you may want to reconfigure the FTP Server to disallow anonymous connections.

For information about configuring an anonymous FTP account, see:
ftp://info.cert.org/pub/tech_tips/anonymous_ftp_config

Medium - ASP source download through IIS

Older versions of the IIS server allow the source of an Active Server Page to be downloaded. If a period '.' is appended to the filename, the source will be downloaded (e.g., "http://localhost/default.asp."). The source may contain hard coded usernames and passwords. Many sites have the SQL administrator password hard coded within their scripts.

Fix - Upgrade IIS server to latest version

Upgrade to the latest verion of the IIS Server.

For more information, visit http://www.microsoft.com/iis

Medium - NEWDSN.EXE exploit

The NEWDSN.EXE exploit allows an intruder to create any file within wwwroot using NEWDSN.EXE cgi.
Applies to computers running Microsoft IIS with NEWDSN.EXE installed.

Fix - Disable or remove NEWDSN.EXE

There are two possibilities to resolve this issue.
Set ACLS on the newdsn.exe
or
Remove the newdsn.exe
The newdsn.exe is typically not used - and can safely be removed. This is obviously the most secure. If you use the script - make sure that ACLs are set so that unauthenticated users cannot access it.
Search your hard drives for the file newdsn.exe. The executable could be stored in multiple places - so searching for the file name is the most effective method.

Medium - Fragmented IGMP Packet

Fragmented IGMP packets can cause a variety of problems in Windows 95 and 98, up to and including causing the machine to crash. Windows NT 4.0 contains the same vulnerability, but other system mechanisms make a successful attack much more difficult.

For more information on this issue, please see the Microsoft Security Bulletin at:
http://http://www.microsoft.com/technet/security/bulletin/ms99-034.asp
or
the FAQ of this bulletin at:
http://www.microsoft.com/technet/security/bulletin/fq99-034.asp

Fix - Install the Fragmented IGMP Packet patch

This vulnerability can be easily fixed by downloading and executing the appropriate patch.

- Windows 95:
http://www.microsoft.com/windows95/downloads/contents/WUCritical/vip386/Default.asp

- Windows 98:
http://www.microsoft.com/windows98/downloads/contents/WUCritical/VIP386/Default1.asp

- WindowsNT 4.0 (Workstation and Server):
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP5/IGMP-fix/

Medium - Unidentified TCP ports

Trojans and backdoors typically reside on unidentifiable TCP/UDP ports. The following TCP Ports have been identified.

Fix - Determine source of ports

Determine the source of the ports as they may be backdoors or trojans.

Medium - Administrator account not renamed

The Administrator account should be renamed to a more obscure name to make it more difficult to execute a brute force attempt at password guessing. By renaming the Administrator account, it is harder for a password-seeking intruder to know that they have an account that has an Administrative permission level.

Fix - Rename Administrator Account

To rename the Administrator account on NT 4.0, select the User->Rename menu choice in User Manager.

On Windows 2000:
-Open the Administrative Tools control panel.
-Open the Local Security Policy tool.
-Expand the Local Policies item and select Security Options.
-Double-click on the "Rename administrator account" item in the right window pane and change theadministrator account name.

-Click OK to save the changes.

Medium - Guest account not renamed

The Guest account should be renamed to a more obscure name to make it more difficult to execute a brute force attempt at password guessing.

Fix - Rename Guest Account

To rename the Guest account, select the User->Rename menu choice in User Manager.

On Windows 2000:
-Open the Administrative Tools control panel.
-Open the Local Security Policy tool.
-Expand the Local Policies item and select Security Options.
-Double-click on the "Rename guest account" item in the right window pane and change theguest account name.
-Click OK to save the changes.

Medium - .REG Association modification by non-administrators

This registry key can be used maliciously against users of this system.By default, protections are set on the various components of the registrythat allow work to be done while providing standard-level security. In addition to the considerations for standard security, the administratorof a high-security installation might want to set protections on certainkeys in the registry.
In a secure installation, .REG files should not be associated with REGEDIT, since.REG files can be used to enter information into the registry. If non-administrativeusers have the ability to change this value, they can create this association and enterinformation into the registry.

Fix - Strengthen Registry on key referenced by HKEY_CLASSES_ROOT\.reg

You can set registry permissions through REGEDT32. Select the key to be secured, thenchoose Permissions from the Security menu.
Restrict access to the following registry key:

Hive: HKEY_CLASSES_ROOT
Key: the value under the \\.reg key. For example, if the value under \\.reg key is "regfile", then the KEY would be "regfile"Set the permissions on this key to allow:
- Administrators - Full Access
- System - Full Access
- Everyone - Read Access
KEY = the value under the \\.reg key. For example, if the value under \\.reg key is "regfile", then the KEY should be "regfile"

Medium - Hazardous Registry Permissions: AeDebug

This registry key can be used maliciously against users of this system.By default, protections are set on the various components of the registrythat allow work to be done while providing standard-level security. In addition to the considerations for standard security, the administratorof a high-security installation might want to set protections on certainkeys in the registry.

Fix - Strengthen Registry Permissions: AeDebug

You can set registry permissions through REGEDT32. Select the key to be secured, thenchoose Permissions from the Security menu.
Restrict access to the following registry key:

Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows NT\CurrentVersion\AeDebug

Set the permissions on this key to allow:
- Administrators - Full Access
- System - Full Access
- Everyone - Read Access

Medium - Hazardous Registry Permissions: Compatibility

This registry key can be used maliciously against users of this system.By default, protections are set on the various components of the registrythat allow work to be done while providing standard-level security. In addition to the considerations for standard security, the administratorof a high-security installation might want to set protections on certainkeys in the registry.

Fix - Strengthen Registry Permissions: Compatibility

You can set registry permissions through REGEDT32. Select the key to be secured, thenchoose Permissions from the Security menu.
Restrict access to the following registry key:

Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows NT\CurrentVersion\Compatibility

Set the permissions on this key to allow:
- Administrators - Full Access
- System - Full Access
- Everyone - Read Access

Medium - Hazardous Registry Permissions: Drivers

This registry key can be used maliciously against users of this system.By default, protections are set on the various components of the registrythat allow work to be done while providing standard-level security. In addition to the considerations for standard security, the administratorof a high-security installation might want to set protections on certainkeys in the registry.

Fix - Strengthen Registry Permissions: Drivers

You can set registry permissions through REGEDT32. Select the key to be secured, thenchoose Permissions from the Security menu.
Restrict access to the following registry key:

Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows NT\CurrentVersion\Drivers

Set the permissions on this key to allow:
- Administrators - Full Access
- System - Full Access
- Everyone - Read Access

Medium - Hazardous Registry Permissions: Drivers32

This registry key can be used maliciously against users of this system.By default, protections are set on the various components of the registrythat allow work to be done while providing standard-level security. In addition to the considerations for standard security, the administratorof a high-security installation might want to set protections on certainkeys in the registry.

Fix - Strengthen Registry Permissions: Drivers32

You can set registry permissions through REGEDT32. Select the key to be secured, thenchoose Permissions from the Security menu.
Restrict access to the following registry key:

Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows NT\CurrentVersion\Drivers32

Set the permissions on this key to allow:
- Administrators - Full Access
- System - Full Access
- Everyone - Read Access

Medium - Hazardous Registry Permissions: Embedding

This registry key can be used maliciously against users of this system.By default, protections are set on the various components of the registrythat allow work to be done while providing standard-level security. In addition to the considerations for standard security, the administratorof a high-security installation might want to set protections on certainkeys in the registry.

Fix - Strengthen Registry Permissions: Embedding

You can set registry permissions through REGEDT32. Select the key to be secured, thenchoose Permissions from the Security menu.
Restrict access to the following registry key:

Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows NT\CurrentVersion\Embedding

Set the permissions on this key to allow:
- Administrators - Full Access
- System - Full Access
- Everyone - Read Access

Medium - Hazardous Registry Permissions: HKEY_CLASSES_ROOT

This registry key can be used maliciously against users of this system.By default, protections are set on the various components of the registrythat allow work to be done while providing standard-level security. In addition to the considerations for standard security, the administratorof a high-security installation might want to set protections on certainkeys in the registry.

Fix - Strengthen Registry Permissions: HKEY_CLASSES_ROOT

You can set registry permissions through REGEDT32. Select the key to be secured, thenchoose Permissions from the Security menu.
Restrict access to the following registry key:

Hive: HKEY_CLASSES_ROOT

Set the permissions on this key to allow:
- Administrators - Full Access
- System - Full Access
- Everyone - Read Access

Medium - Hazardous Registry Permissions: MCI

This registry key can be used maliciously against users of this system.By default, protections are set on the various components of the registrythat allow work to be done while providing standard-level security. In addition to the considerations for standard security, the administratorof a high-security installation might want to set protections on certainkeys in the registry.

Fix - Strengthen Registry Permissions: MCI

You can set registry permissions through REGEDT32. Select the key to be secured, thenchoose Permissions from the Security menu.
Restrict access to the following registry key:

Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows NT\CurrentVersion\MCI

Set the permissions on this key to allow:
- Administrators - Full Access
- System - Full Access
- Everyone - Read Access

Medium - Hazardous Registry Permissions: MCI Extensions

This registry key can be used maliciously against users of this system.By default, protections are set on the various components of the registrythat allow work to be done while providing standard-level security. In addition to the considerations for standard security, the administratorof a high-security installation might want to set protections on certainkeys in the registry.

Fix - Strengthen Registry Permissions: MCI Extensions

You can set registry permissions through REGEDT32. Select the key to be secured, thenchoose Permissions from the Security menu.
Restrict access to the following registry key:

Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows NT\CurrentVersion\MCI Extensions

Set the permissions on this key to allow:
- Administrators - Full Access
- System - Full Access
- Everyone - Read Access

Medium - Hazardous Registry Permissions: Ports

This registry key can be used maliciously against users of this system.By default, protections are set on the various components of the registrythat allow work to be done while providing standard-level security. In addition to the considerations for standard security, the administratorof a high-security installation might want to set protections on certainkeys in the registry.

Fix - Strengthen Registry Permissions: Ports

You can set registry permissions through REGEDT32. Select the key to be secured, thenchoose Permissions from the Security menu.
Restrict access to the following registry key:

Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows NT\CurrentVersion\Ports

Set the permissions on this key to allow:
- Administrators - Full Access
- System - Full Access
- Everyone - Read Access

Medium - Hazardous Registry Permissions: ProfileList

This registry key can be used maliciously against users of this system.By default, protections are set on the various components of the registrythat allow work to be done while providing standard-level security. In addition to the considerations for standard security, the administratorof a high-security installation might want to set protections on certainkeys in the registry.

Fix - Strengthen Registry Permissions: ProfileList

You can set registry permissions through REGEDT32. Select the key to be secured, thenchoose Permissions from the Security menu.
Restrict access to the following registry key:

Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows NT\CurrentVersion\ProfileList

Set the permissions on this key to allow:
- Administrators - Full Access
- System - Full Access
- Everyone - Read Access

Medium - Hazardous Registry Permissions: WOW

This registry key can be used maliciously against users of this system.By default, protections are set on the various components of the registrythat allow work to be done while providing standard-level security. In addition to the considerations for standard security, the administratorof a high-security installation might want to set protections on certainkeys in the registry.

Fix - Strengthen Registry Permissions: WOW

You can set registry permissions through REGEDT32. Select the key to be secured, thenchoose Permissions from the Security menu.
Restrict access to the following registry key:

Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows NT\CurrentVersion\WOW

Set the permissions on this key to allow:
- Administrators - Full Access
- System - Full Access
- Everyone - Read Access

Medium - User access to Performance Monitor data

The HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Perfliballows users to access system performance data. This data may contain sensitivesystem information such as performance counters, and which processes are running. Thisinformation should be available only to Administrators.

Fix - Restrict access to Performance Monitor Data

Change the permissions on the following key to allow only Administrator access.
This is done by performing the following steps:
(1) Run the registry editor (regedt32.exe)
(2) Click on the following registry key name:
Hive: HKEY_LOCAL_MACHINE
Key: SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib
(3) On the Security menu, click Permissions
(4) Remove all users and groups from the list except for Administrators, then click "OK"to save your changes.

Medium - Site Server - Site Wizard Input Validation

Microsoft has released a patch that eliminates a security vulnerability in web applications associated with Microsoft® Site Server 3.0, Commerce Edition. These applications are provided as samples and generated by wizards, but do not follow security best practices. If deployed on a web site, they could allow inappropriate access to a database on the site.
For more information on this issue, please see the Microsoft Security Bulletin at:
http://http://www.microsoft.com/technet/security/bulletin/ms00-010.asp
or
the FAQ of this bulletin at:
http://www.microsoft.com/technet/security/bulletin/fq00-010.asp

Fix - Install the Site Wizard Input Validation patch

You can find the patch at:
http://http://www.microsoft.com/downloads/Release.asp?ReleaseID=18767

Medium - Last username displayed in login dialog

By default Windows NT places the name of the last user to logon to the system in the username field. This can give an intruder a possible account to exploit.

Fix - Suppress display of last username in login dialog

Configure the system to not display the name of the last user that logged in.
This is done by setting the following registry key's value:
Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows NT\CurrentVersion\Winlogon
Name: DontDisplayLastUserName
Type: REG_SZ
Value: 1
The key described above may not exist by default, and may need to be created.

Medium - File type with confirm after download disabled

File types were found with the confirm after download option disabled.
File types handled by the DocObject model are currently configured to download silently and open without any promptto the user. Although this may be useful for many applications, an attacker may use it to download hostile softwareon to a system. It is recommended that every file type has its confirm after download enabled.

Fix - Edit registry setting to confirm after download

Microsoft has provided a utility that will reconfigure this option in Office Documents making the entire process easier. You can obtain this utility from:
http://www.microsoft.com/security/Issues/OfficeDocOpenTool.asp
This program fixes known vulnerabilities for MSOffice Document types only. Although it may be generally safe to allow all reported file types to execute withoutconfimation, for more stringent security you can set all document types to confirm before executing.To manually enable confirmation for all other file types not fixed by the Microsoft Utility follow the directions below:Using a registry editor, you can change the handling of these objects to confirm after download.
- Locate the registry key for the associated object name under the following hive.
Hive:HKEY_CLASSES_ROOT

There are four bytes of data being stored in the EditFlag for each of the keys. Set the third byte to 00 to enable confirm after download.
In particular, you should ensure that you make this change under the following key to protect against known exploits.
Hive:HKEY_CLASSES_ROOT
Key:Excel.Sheet.8
Data:EditFlag

Medium - Internet Explorer: Eyedog ActiveX control

Eyedog is a control used by diagnostic software in Windows. It is currently marked as "safe for scripting" on the host,but should not be because it allows registry information to be queried and machine characteristics to be gathered. Inaddition, one of the control's methods is vulnerable to a buffer overrun attack. For more information on this issue, please see the Microsoft Security Bulletin at:
http://www.microsoft.com/Security/Bulletins/ms99-032.asp

Fix - Apply patch to set "kill bit" for Eyedog ActiveX control

The patch sets the "kill bit", which prevents the Eyedog control from loading within Internet Explorer. You can downloadand apply the patch from:
ftp://ftp.microsoft.com/peropsys/IE/IE-Public/Fixes/usa/Eyedog-fix/

Medium - Misordered Windows Media Services Handshake

Microsoft has released a patch that eliminates a security vulnerability in Microsoft® Windows Media Services. The vulnerability could allow denial of service attacks against a streaming media server.

For more information on this issue, please see the Microsoft Security Bulletin at:
http://http://www.microsoft.com/technet/security/bulletin/ms00-013.asp
or
the FAQ of this bulletin at:
http://www.microsoft.com/technet/security/bulletin/fq00-013.asp

Fix - Install the Misordered Windows Media Services Handshake patch

Windows NT 4.0 Server and Windows 2000 Server have their own unique patch. To get the Windows NT 4.0 patch, you must upgrade to Windows Media Services 4.1. You can get the upgrade at:
http://www.microsoft.com/windows/windowsmedia

After upgrading, get the NT 4.0 Server patch at:
http://download.microsoft.com/download/winmediatech40/Update/4954/NT4/EN-US/WMSU4954_NT4.EXE

To get the Windows 2000 Server patch goto:
http://download.microsoft.com/download/winmediatech40/Update/4954/NT5/EN-US/WMSU4954_Win2000.EXE

Medium - Malformed Hit Highlighting Argument

This test checks for the Malformed Hit-Highlighting patch. This patch eliminates two vulnerabilities whose only relationship is that both occur in Index Server. The first is the "Malformed Hit-Highlighting Argument" vulnerability. The ISAPI filter that implements the hit-highlighting (also known as "WebHits") functionality does not adequately constrain what files can be requested. By providing a deliberately-malformed argument in a request to hit-highlight a document, it is possible to escape the virtual directory. This would allow any file residing on the server itself, and on the same logical drive as the web root directory, to be retrieved regardless of permissions.

The second vulnerability involves the error message that is returned when a user requests a non-existent Internet Data Query file. The error message provides the physical path to the web directory that was contained in the request. Although this vulnerability would not allow a malicious user to alter or view any data, it could be a valuable reconnaissance tool for mapping the file structure of a web server.

For further information:
http://www.microsoft.com/technet/Security/Bulletin/ms00-006.asp
There is also a FAQ for this bulletin at:
http://www.microsoft.com/technet/security/bulletin/fq00-006.asp

Fix - Install the Malformed Hit-Highlighting Argument Patch

Install the patch from Microsoft
Windows2000
http://www.microsoft.com/downloads/release.asp?ReleaseID=17726

WindowsNT 4.0
Intel
http://www.microsoft.com/downloads/release.asp?ReleaseID=17727

Medium - Malformed Resource Enumeration Argument

The vulnerability could cause a Windows NT machine to stop responding to requests for services.

For more information on this issue, please see the Microsoft Security Bulletin at:
http://http://www.microsoft.com/technet/security/bulletin/ms99-055.asp
or
the FAQ of this bulletin at:
http://www.microsoft.com/technet/security/bulletin/fq99-055.asp

This vulnerability does not affect Windows 2000.

Fix - Install the Malformed Resource Enumeration Argument hotfix

The hotfix patch for this Microsoft Security Bulletin can be found at:
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=16382

This is the same hotfix as the Syskey Keystream Reuse vulnerability hotfix.

Medium - Malformed Security Identifier Request

The vulnerability could allow a malicious user to cause a Windows NT machine to stop responding to requests for service.

For more information on this issue, please see the Microsoft Security Bulletin at:
http://http://www.microsoft.com/technet/security/bulletin/ms99-057.asp
or
the FAQ of this bulletin at:
http://www.microsoft.com/technet/security/bulletin/fq99-057.asp

This vulnerability does not affect Windows 2000.

Fix - Install the Malformed Security Identifier Request hotfix

The hotfix patch for this Microsoft Security Bulletin can be found at:
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=16798

This is the same hotfix as the Syskey Keystream Reuse vulnerability hotfix.

Medium - RDISK Registry Enumeration File

The RDISK utility creates a temporary file during execution that can contain security-sensitive information, but does not appropriately restrict access to it. Under certain conditions, it could be possible for a malicious user to read the file as it was being created.

For more information on this issue, please see the Microsoft Security Bulletin at:
http://www.microsoft.com/technet/security/bulletin/ms00-004.asp
or
the FAQ of this bulletin at:
http://www.microsoft.com/technet/security/bulletin/fq00-004.asp

This vulnerability does not affect Windows 2000.

Fix - Install the RDISK Registry Enumeration File hotfix

The hotfix patch for this Microsoft Security Bulletin can be found at:
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=17745

Medium - Recycle Bin Creation

Under a very daunting set of conditions, a malicious user could create, delete or modify files in the Recycle Bin of another user who shared the machine. In most cases, the vulnerability would not allow the malicious user to read the files unless they already had read permission to do so.

For more information on this issue, please see the Microsoft Security Bulletin at:
http://http://www.microsoft.com/technet/security/bulletin/ms00-007.asp

or
the FAQ of this bulletin at:
http://www.microsoft.com/technet/security/bulletin/fq00-007.asp

Fix - Install the Recycle Bin Creation hotfix

Install the Recycle Bin Creation hotfix. It can be found at:
http://www.microsoft.com/downloads/release.asp?ReleaseID=17606

Medium - Spoofed LPC Port Request

This vulnerability could allow a user logged onto a Windows NT 4.0 machine from the keyboard to become an administrator on the machine. For more information on this issue, please see the Microsoft Security Bulletin at:
http://www.microsoft.com/technet/security/bulletin/ms00-003.asp
or
the FAQ of this bulletin at:
http://www.microsoft.com/technet/security/bulletin/fq00-003.asp

This vulnerability does not affect Windows 2000.

Fix - Install the Spoofed LPC Port Request hotfix

The hotfix patch for this Microsoft Security Bulletin can be found at:
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=17382

Medium - Windows NT Initial Sequence Numbers

TCP sequence numbers provide flow control and data integrity for TCP sessions. Each byte in a TCPsession has a unique sequence number.
Windows NT 4.0 has somewhat predictable ISN (Initial Sequence Numbers). These ISNs may make the host vulnerable tospoofing and or session hijacking.
For more information on this issue, please see the Microsoft Security Bulletin at:
http://www.microsoft.com/technet/security/bulletin/ms99-046.aspor
The Microsoft FAQ for this issue at:
http://www.microsoft.com/technet/security/bulletin/fq99-046.asp

Fix - Install TCP/IP Hotfix to improve TCP Initial Sequence Number randomness

Microsoft has provided a patch for this issue.

The patch implements the same algorithm that will be used in Windows 2000. This algorithm produces ISNs with a muchgreater degree of randomness.
Please note, although this patch was made available before Windows NT Service Pack 6 was released, it is not included in Service Pack6, since that Service Pack was too far along in its development to include this patch. It is anticipated that it willbe included in Service Pack 7. This patch will need to be reinstalled after the installation of Service Pack 6 or earlier.

If you are running Service 4 or 5, you can download and apply the patch from:
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=16763
If you are running Service 6, you can download and apply the patch from:
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=16764

Medium - IIS-fix service patch

The IIS-fix service patch is not applied to the host.
The Internet Information Server service stops when it receives a client request (such as URLs and headers) thatcontains between 4 and 8 kilobytes of data from a browser. Microsoft Internet Information Server services willgenerate a Dr. Watson error referencing the Inetinfo.exe process.
For more information on this issue, please visit:
http://support.microsoft.com/support/kb/articles/q143/4/84.asp

Fix - Install IIS-fix Service Patch or update to latest Windows NT 4.0 Service Pack

Microsoft has provided a solution for this issue. You can protect your IIS installation from this issue by downloadingand applying the patch, or by installing the latest Windows NT 4.0 Service Pack. This fix was first available as part ofService Pack 4. It is recommended that you download and apply the latest Windows NT 4.0 Service Pack to resolve this and othersecurity issues.
For information on obtaining the latest Service Pack for Windows NT 4.0, please visit:
http://support.microsoft.com/support/kb/articles/Q152/7/34.ASP
For your convenience, the English version of this post-SP3 hotfix has been posted to the following Internet location. However,Microsoft recommends that you install Windows NT 4.0 Service Pack 4 to correct this problem.
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/iis-fix

Medium - MS Spoofed Route Pointer Vulnerability

This vulnerability, which affects Microsoft® Windows® 95, 98 and Windows NT® 4.0 couldallow source routing to be performed, even if it has ostensibly been disabled.

For more information on this issue, please see the Microsoft Security Bulletin at:
http://www.microsoft.com/technet/security/bulletin/ms99-038.asp
or
the FAQ of this bulletin at:
http://www.microsoft.com/technet/security/bulletin/fq99-038.asp

This vulnerability does not affect Windows 2000.

Fix - Install the hotfix

There is currently no patch for Windows 95/98.

The Windows NT 4.0 hotfix patch for this Microsoft Security Bulletin can be found at:
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/Hotfixes-PostSP5/spoof-fix/

Medium - Priv-fix hotfix

The Priv-fix hotfix is not installed on the computer.
The "sechole.exe" program allows a normal user to become administrator. This exploits a problem with Windows NT's "DEBUG" privilege. This exploit works against all versions of NT, including NT 5.0 betas. This attack may work against NT Domain controllers.
For more information, see Knowledge Base article Q190288, at:
http://support.microsoft.com/support/kb/articles/Q190/2/88.asp

Fix - Apply Windows NT Priv-fix Hotfix

Apply the priv-fix hotfix.See:
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP3/priv-fix/README.TXT
for instructions on how to apply the hotfix.

The download files are located at:
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP3/priv-fix/

For more information, see Knowledge Base article Q190288, at:
http://support.microsoft.com/support/kb/articles/Q190/2/88.asp

Medium - RPC spoof

A vulenrability exists in the RPCSS.EXE service that can be exploited to degrade system performance. The service couldthen consume 100 percent of CPU time. Analyzing the network with a protocol analyzer will show multiple RPC REJECTpackets (addressed to UDP port 135) between two or more systems when an RPC spoofing attack is in progress.
A UDP packet with a destination port of 135 can be spoofed so that it appears as if one datagram RPC server sentbad data to another datagram RPC server. The second server returns a REJECT packet. The first server replies withanother REJECT packet creating a loop that is not broken until a packet is dropped. If this spoofed UDP packet issent to multiple computers, an infinite loop may be created, consuming processor resources and network bandwidth.

Fix - Apply Windows NT RPC Spoofing Hotfix

Microsoft has supplied a patch for this issue in Microsoft Windows NT Service Pack 4. For information on obtaining thelatest Service Pack, please visit:
http://support.microsoft.com/support/kb/articles/Q152/7/34.asp

This hotfix has also been posted as Snk-fixi.exe and Snk-fixa.exe. This post-SP3 hotfix has been posted to thefollowing Internet location. However, Microsoft recommends that you install Windows NT 4.0 Service Pack 4 tocorrect this problem.
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP3/Snk-fix/

Medium - SECHole Vulnerbility Detected

The "sechole.exe" program allows a normal user to become administrator. This exploits a problem with Windows NT's "DEBUG" privilege. This exploit works against all versions of NT, including NT 5.0 betas. This attack may work against NT Domain controllers.

For more information, see Knowledge Base article Q190288, at:
http://support.microsoft.com/support/kb/articles/Q190/2/88.asp

Fix - Apply Windows NT Patch to fix the SECHole Vulnerability

Apply the priv-fix hotfix.See:
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP3/priv-fix/README.TXT
for instructions on how to apply the hotfix.

The download files are located at:
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP3/priv-fix/

For more information, see Knowledge Base article Q190288, at:
http://support.microsoft.com/support/kb/articles/Q190/2/88.asp

Medium - Srv-Fix Hotfix Not Applied

Teardrop is a denial of service attack. It exploits a weakness in the NT TCP/IP stack to crash the machine.

For more information, see Knowledge Base article Q180963, at:
http://support.microsoft.com/support/kb/articles/Q180/9/63.asp

Fix - Apply Windows Srv-fix Hotfix

Install the latest Service Pack. See:
http://www.microsoft.com/ntserver/nts/downloads/default.asp#RecommendedUpdates
for instructions on how to apply the hotfix.

Medium - Unprotected IOCTLs hotfix

The IOCTLs that are used to obtain services from the keyboard and mouse drivers in Windows NT do not requirethe calling program to have administrative privileges. A user-level program can use a program with IOCTL calls todisable the mouse and keyboard. This creates a denial of service situation where the machine would need to berebooted to restore normal service.
For more information on this issue, please see the Microsoft Security Bulletin at:
http://www.microsoft.com/security/bulletins/ms99-024.asp
or
Microsoft Knowledge Base (KB) article Q236359, Denial of Service Attack Using Unprotected IOCTL Function Call, at:
http://support.microsoft.com/support/kb/articles/q236/3/59.asp

Fix - Install the IOCTL hotfix

Microsoft has provided a patch to address this vulnerability. You can download and apply the patch from:
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/Hotfixes-PostSP5/IOCTL-fix/

Medium - WINS Update not Installed

Invalid UDP frames directed to any computer running WINS raises an exception in WINS causing it to terminate silently.When WINS is no longer running, problems such as domain synchronization, browsing, or connectivity may occur.

Fix - Install WINS Update

To resolve this problem it is recomended that you update your system to the latest service pack. You can obtain the latest service pack at:
http://support.microsoft.com/support/kb/articles/Q152/7/34.ASP

If for some reason you can not upgrade your system to the latest service pack MicroSoft also offers a hot fix at:
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postsp3/winsupd-fix/

Medium - Teardrop2 hotfix

Teardrop is a denial of service attack. It exploits a weakness in the Windows NT Server and Workstation 4.0 TCP/IP stack to crash the machine.

For more information, see Knowledge Base article Q179129, at:
http://support.microsoft.com/support/kb/articles/Q179/1/29.asp

Fix - Apply Windows NT 4.0 Teardrop2 Hotfix

Apply the teardrop2-fix hotfix. See:
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP3/teardrop2-fix/README.TXT
for instructions on how to apply the hotfix.

The download files are located at:
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP3/teardrop2-fix/

For more information, see Knowledge Base article Q179129, at:
http://support.microsoft.com/support/kb/articles/Q179/1/29.asp

Medium - Land Attack Possible

Teardrop is a denial of service attack. It exploits a weakness in the NT TCP/IP stack to crash the machine.

For more information, see Knowledge Base article Q179129, at:
http://support.microsoft.com/support/kb/articles/Q179/1/29.asp

Fix - Apply Land-Fix Hotfix

Apply the teardrop2-fix hotfix. See:
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP3/teardrop2-fix/README.TXT
for instructions on how to apply the hotfix.

The download files are located at:
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP3/teardrop2-fix/

For more information, see Knowledge Base article Q179129, at:
http://support.microsoft.com/support/kb/articles/Q179/1/29.asp

Medium - SSPing Vulnerability Detected

Teardrop is a denial of service attack. It exploits a weakness in the NT TCP/IP stack to crash the machine.

For more information, see Knowledge Base article Q179129, at:
http://support.microsoft.com/support/kb/articles/Q179/1/29.asp

Fix - Apply Windows NT Teardrop2 Hotfix

Apply the teardrop2-fix hotfix. See:
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP3/teardrop2-fix/README.TXT
for instructions on how to apply the hotfix.

The download files are located at:
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP3/teardrop2-fix/

For more information, see Knowledge Base article Q179129, at:
http://support.microsoft.com/support/kb/articles/Q179/1/29.asp

Medium - Out of Band (OOB) data crash hotfix

The Out of Band (OOB) data crash hotfix is not installed on this computer.
Windows NT may stop responding or hang with a STOP 0x0000000A or 0x00000019 message when it receives intentionallycorrupted UDP packets.
This is a variation of the Teardrop attack which exploits a weakness in the NT TCP/IP stack to crash the machine.
For more information, see Knowledge Base article Q179129, at:
http://support.microsoft.com/support/kb/articles/Q179/1/29.asp

Fix - Apply Windows NT Teardrop2 Hotfix

Apply the teardrop2-fix hotfix. The first Windows NT 4.0 Service Pack release to include the hotfix for this issue wasService Pack 4. You can protect your computers from this issue by applying Windows NT 4.0 Service Pack 4 or higher.

For information on obtaining the latest Service Pack release, please visit:
http://support.microsoft.com/support/kb/articles/Q152/7/34.asp
In the event that you are unable to apply Service Pack 4 or higher, a hotfix from Microsoft is available for this issue as well.See:
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP3/teardrop2-fix/README.TXT
for instructions on how to apply the hotfix.
The hotfix download files are located at:
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP3/teardrop2-fix/
For more information, see Knowledge Base article Q179129, at:
http://support.microsoft.com/support/kb/articles/Q179/1/29.asp

Medium - Windows NT Y2K-fix fix

There are a number of year 2000 issues under Windows NT that require a patch. The issues include the following itemsas documented in Windows NT KnowledgeBase articles:

User Manager Does Not Recognize February 2000 As a Leap Year

After Changing the Time, Windows NT May Skip a Day

Find Files Displays Garbled Date if Year is 2000 or Greater

Shell Doc Property Dialog Custom Date Incorrect after Year 2000

Err Msg: Value Entered Does Not Match with the Specified Type

FPNW Logout.exe Incorrectly Reports Year After Jan. 1, 2000

Date of Print Job May Be Displayed Incorrectly in Print Queue

Problems in Date/Time after Choosing February 29 in a Leap Year

Migration Changes NetWare Accounts Expiration Date

FPNW Client Does Not Get Correct Time or Date After Y2K

IBM PS/1 will not Boot on or After January 1, 2000

NTBACKUP Writes Incorrect Year to Log File

Fix - Apply Windows NT Y2k-fix Hotfix

Apply the Windows NT Y2K-fix hotfix. The first Windows NT 4.0 Service Pack release to include the hotfix for this issue wasService Pack 4. You can protect your computers from this issue by applying Windows NT 4.0 Service Pack 4 or higher.

For information on obtaining the latest Service Pack release, please visit:
http://support.microsoft.com/support/kb/articles/Q152/7/34.asp

In the event that you are unable to apply Service Pack 4 or higher, a hotfix from Microsoft is available for this issue as well.See:
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP3/y2k2-fix/README.TXT
for instructions on how to apply the hotfix.
The download files are located at:
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP3/y2k2-fix/

For more information, see Knowledge Base article Q175093, at:
http://support.microsoft.com/support/kb/articles/Q175/0/93.asp

Low - FTP service enabled

This test determines if the FTP service is active on your network. Since any service can potentially be exploited, you should minimize the number of services running on your network. Many services are installed as part of the default installation.

Fix - Remove Unnecessary Services: FTP

The FTP service has been detected. Since any service can potentially be exploited, you should minimize the number of services running on your network. Many services are installed as part of the default installation. Remove any services that are unnecessary.

Low - HTTP (Web) service enabled

This test determines if the HTTP (Web) service is active on your network. Since any service can potentially be exploited, you should minimize the number of services running on your network. Many services are installed as part of the default installation.

Fix - Remove Unnecessary Services: HTTP (Web)

The HTTP (Web) service has been detected. Since any service can potentially be exploited, you should minimize the number of services running on your network. Many services are installed as part of the default installation. Remove any services that are unnecessary.

Low - User cannot change password

A user was found that is prevented from changing their password. The User Cannot Change Passwordoption should primarily be used when the passwords for user accounts are administered centrally by thenetwork administrator. This option is often used if several users share the same account. If userscannot change their password, there is a risk that if the password is exposed that the user will nottake adequate action to get the password changed.

Fix - Allow user to change password

On Windows NT 4.0:
-Change the user policy to allow the user to change their password
-From the Windows NT User Manager, highlight the user and select "Properties" from the "User" menu.
-In the resulting "User Properties" dialog, uncheck the "User Cannot Change Password" checkbox.
-Click the OK button to save your changes.

On Windows 2000:
-Open the Administrative Tools control panel.
-Open the Computer Management tool.
-Expand the Local Users and Groups item and click on Users.
-Double-click the user on the right window pane and uncheck the "User cannot change password" checkbox.
-Select OK to save changes.

Low - User has not logged on in specified number of days

A user account was detected that has not logged in recently, based on the number of days specified in thetest properties. Dormant user accounts are often excellent targets for intruders, sincethey are not in active use, and unusual activity or changes may go unnoticed.

Fix - Remove unnecessary dormant users

Investigate the account status and usage. If the account is no longer needed, it should be deleted.
Note: Even though a user has never logged in locally, it does not guarantee thatthe account is not used. For example, if you have specific accounts for services, theywill have never logged in. Be sure to investigate the use of any account before deleting it.

Low - User never logged in

A user account was detected that has never logged. Inactive user accounts are often excellent targets for intruders, sincethey are not in active use, and unusual activity or changes may go unnoticed.

Fix - Remove unnecessary inactive users

Investigate the account status and usage. If the account is not needed, it should be deleted.
Note: Even though a user has never logged in locally, it does not guarantee thatthe account is not used. For example, if you have specific accounts for services, theywill have never logged in. Be sure to investigate the use of any account before deleting it.

Low - User's password never expires

The user was found to have a password that will never expire. A strong password policy includesrequiring users to change their passwords regularly. The longer a user retains a password, thehigher the risk of exposure of their password.

Fix - Change account policy to require regular password changes

On Windows NT 4.0:
-From the Windows NT User Manager, highlight the user and select "Properties" from the "User" menu.
-In the resulting "User Properties" dialog, uncheck the "Password Never Expires" checkbox.
-Click the OK button to save your changes.

On Windows 2000:
-Open the Administrative Tools control panel.
-Open the Computer Management tool.
-Expand the Local Users and Groups item and click on Users.
-Double-click the user on the right window pane and uncheck the "Password never expires" checkbox.
-Select OK to save changes.

Low - Logon credential caching

Logon credentials are being cached on the host.
By default, Windows NT caches the last logon credentials of users who log on interactivelyto the system. This is to provide system availability reasons in the event that the computeris disconnected or if none of the domain controllers are available.
Although the cached credentials are protected, in order to provide a highly secure environment,customers may want to disable this feature to protect sensitive logon information.

Fix - Disable caching of logon credentials

To disable caching of logon credentials in NT 4.0, set the following registry key's value:

Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows NT\CurrentVersion\Winlogon
Name: CachedLogonsCount
Type: REG_SZ
Value: 0

To disable caching of logon credentials in Windows 2000:
-Open Control Panel.
-Open Administrative Tools.
-Open Local Security Settings.
-Expand Local Policies and select Security Options.
-Double-click on 'Number of previous logons to cache(in case domain contoller is not available' item policy.
-Select 0 logons and hit OK.

Low - Printer driver installation restrictions

The installation of printer drivers is not restricted on the host.
Normal users can circumvent the security of a workstation by installing a trojan printer driver.

Fix - Restrict printer drivers installation

Allow only NT Administrators and Print Operators to install printer drivers.

This is done by setting the following registry key's value:
Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers
Name: AddPrintDrivers
Type: REG_DWORD
Value: 1

Low - Windows NT legal notice banner

Windows NT can display a logon banner before user logon with a caption and anytext you choose. This banner can be used to display legal notices about authorizeduse or information regarding site policy.
The absence of such a notice could beinterpreted as an invitation to enter and browse the system.

Fix - Display a legal notice before logon

Use the registry editor to create or assign the following registry key values:
Hive:HKEY_LOCAL_MACHINE
Key:Software/Microsoft/Windows NT/CurrentVersion/Winlogon
Type:REG_SZ
Name:LegalNoticeCaption
Value:set this value to what you would like the caption of the legal notice to say
and
Hive:HKEY_LOCAL_MACHINE
Key:Software/Microsoft/Windows NT/CurrentVersion/Winlogon
Type:REG_SZ
Name:LegalNoticeText
Value:set this value to what you would like the text of the legal notice to say.

Low - Allocation of CR-ROM drives

In its default configuration, Windows NT will allow any program to access the files on a CDin your CDROM drive. Sensitive data on a CD, or a malicious program on a CD in your CDROM drivecould be executed by another user or process on the computer.

Fix - Restrict access to CDROM drive to currently logged on users

You can instruct Windows NT to restrict CDROM access to the current interactively loggedon user. When Windows NT operates in this mode, the CDROM is allocated to a user as partof the interactive logon process. The device will be freed for general use for reallocationwhen the user logs off. Therefore, for maximum security, it is important to remove any sensitivedata from the CDROM drive before logging off.
To enable allocation of the CDROM drive during log on for NT 4.0, set the following registry key value:

Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\WindowsNT\CurrentVersion\Winlogon
Name: AllocateCDRoms
Type: REG_SZ
Value: 1

On Windows 2000:
-Open Control Panel.
-Open Administrative Tools.
-Open Local Security Settings.
-Expand Local Policies and select Security Options.
-Double-click on 'Restrict CD-ROM access to locally logged-on user only' item policy.
-Select 'Enabled' and hit OK.

Low - Allocation of floppy drives

In its default configuration, Windows NT will allow any program to access the files on a floppydisk in your floppy drive. Sensitive data on a floppy, or a malicious program on a floppy in yourfloppy disk drive could be executed by another user or process on the computer.

Fix - Restrict access to floppy drive to currently logged on users

You can instruct Windows NT to restrict floppy drive access to the current interactively loggedon user. When Windows NT operates in this mode, the floppy drive is allocated to a user as partof the interactive

logon process. The device will be freed for general use for reallocationwhen the user logs off. Therefore, for maximum security, it is important to remove any sensitivedata from the floppy drive before logging off.
To enable allocation of the floppy drive during log on, set the following registry key value:

Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\WindowsNT\CurrentVersion\Winlogon
Name: AllocateFloppies
Type: REG_SZ
Value: 1

-Open Control Panel.
-Open Administrative Tools.
-Open Local Security Settings.
-Expand Local Policies and select Security Options.
-Double-click on 'Restrict floppy access to locally logged-on user only' item policy.
-Select 'Enabled' and hit OK.

Low - Malformed dialer entry patch

The Dialer.exe application has an unchecked buffer in the section of the program that processes the dialer.inifile. This vulnerability could be used to run arbitrary code via a buffer overrun technique.This vulnerability requires a fairly complicated attack scenario that limits its scope. Dialer.exe runsin the security context of the user, so an attacker cannot simply modify a dialer.inifile and run it, as he or she would not gain additional privileges. Instead, the attacker would need tomodify the dialer.ini file of another user who had higher privileges, then wait for that user to run Dialer.Although the unchecked buffer is present in all versions of Windows NT 4.0, primarily workstations that havedial-out capability are risk.
For more information on this issue, please see the Microsoft Security Bulletin at:
http://www.microsoft.com/security/bulletins/ms99-026.asp
or
A Frequently asked questions document (FAQ) regarding this vulnerability can be found at:
http://www.microsoft.com/security/bulletins/MS99-026faq.asp
or
Microsoft Knowledge Base (KB) article Q237185, Dialer.exe Access Violation with Phone Entry more than 128 Bytes:
http://support.microsoft.com/support/kb/articles/q237/1/85.asp

Fix - Download and apply patch for dialer.exe

Microsoft has provided a patch for this issue. You can download and apply the patch from:
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP5/Dialer-fix/

Low - Malformed Rich Text

RTF files consist of text and control information. The control informationis specified via directives called control words. The default RTF readerthat ships as part of many Windows platforms has an unchecked buffer in theportion of the reader that parses control words. If an RTF file contains aspecially-malformed control word, it could cause the application to crash.Microsoft believes that this is a denial of service vulnerability only, andthat there is no capability to use this vulnerability to run arbitrarycode.

Fix - Install Hotfix Q29973

This vulnerability can be easily fixed by downloading and executing the appropriate patch
- Windows 95:
http://www.microsoft.com/windows95/downloads/contents/WUCritical/rtfcontrol/default.asp
- Window 98:

http://www.microsoft.com/windows98/downloads/contents/WUCritical/rtfcontrol/default.asp
- Windows NT 4.0 Workstation, Windows NT 4.0 Server, and Windows NT 4.0 Server, Enterprise Edition:
Intel:
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=17510

Alpha:
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=17511

Windows 2000 is NOT affected by this vulnerability

Low - WinHlp32 Update

An unchecked buffer exists in the Help utility, and a help file that has been carefully modified could be usedto execute arbitrary code on the local machine via a buffer overrun technique.
This vulnerability affects only the local machine; there is no capability to directly attack a remote machinevia this vulnerability.
For more information on this issue, please see the Microsoft Security Bulletin at:
http://www.microsoft.com/security/bulletins/ms99-015.asp
or
Microsoft Knowledge Base (KB) article Q231605, Malformed Help File Causes Help Utility to Stop Responding
http://support.microsoft.com/support/kb/articles/q231/6/05.asp

Fix - Install WinHlp32 Update

Microsoft has released patches that fix the problem identified. Download and apply the patch from:
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP5/winhlp32-fix/winhlp-i.exe

Low - User does not have logon hours set

You might want to restrict the hours during which an account has access to the network. Forexample, certain workers may be able to access network resources only during normal businesshours-Monday through Friday from 8 AM to 5 PM. If accounts are restricted from logon during off hours, it limits the chancethat an intruder will be able to exploit those accounts. Most hacking attempts occuroutside of regular business hours when there is limited staff on hand to notice unusual activity. Restricting logon hours only affects the ability to connect to a server. It does not restrict usersfrom using a workstation.

Fix - Modify user configuration to restrict logon hours

You can manage logon hours for a user account from User Manager.
Highlight the user in the User Manager window and select "Properties" from the "User" menu.
Click the "Hours" button from the User Properties sheet. Please note that the "Hours" button isonly available if you are managing a domain.
The Logon Hours dialog displays a weekly schedule of times allowed for user logon. The dark areasindicate valid logon times. Logon hours are permitted by selecting the desired hours and clicking"Allow". Similarly, restricted hours are specified by selecting the hours and clicking "Disallow".

You can use any of the following four methods to select logon times in the Logon Hours dialog:
Clicking the day of week label-for example, Sunday-selects the entire day.
Clicking the top of an hour column selects that hour every day of the week.
Clicking the column square above Sunday selects the entire week.
Clicking a specific hour selects that hour.
After the logon hours are set, click OK to save the logon hours for that account.

Low - IIS SSL Error Message patch not applied

A Vulnerability in the SSL protocol allows Internet transaction encrypted with SSL to be decoded. To use this discovered vulnerability as an attack, the attacker must first be able to observe the encrypted transaction between a Web client and a Web server. Once the attacker observes a single encrypted transaction, the attacker would then proceed to send a large number (about a million) of packets to the original Web server and analyze the responses. The attacker would then be able to decode the information contained in the single encrypted transaction he had observed.

Due to the large number of messages needed, a Web site operator could detect an attack through observations such as abnormal network or CPU utilization.
Unlike some vulnerabilities that can be exploited more quickly by dividing the workload between multiple attacking machines, this attack cannot be divided among attackers to reduce the amount of work or time for an attack.
For more information, see:
- Microsoft Knowledge Base article Q148427, Updates in SChannel.DLL, http://support.microsoft.com/support/kb/articles/q148/4/27.asp
- RSA Labs advisory information, http://www.rsa.com/rsalabs/pkcs1
- Bell Labs, http://www.bell-labs.com
- CERT Advisory CA-98.07.PKCS, http://www.cert.org/advisories/CA-98.07.PKCS.html

Fix - Apply IIS SSL Error Message Patch

Only customers that use SSL on their Internet servers need to take action. This issue affects both 40-bit and 128-bit versions of SSL (including SGC). Customers who use the server products listed above, but do not use SSL are not affected and do not need to take action.

Download and Install the IIS SSL Error Message Patcb from:
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP3/ssl-fix

Low - Anonymous users may be able to obtain the password policy

Windows NT 4.0 with Service Pack 3 (SP3) installed provides the capability to restrict anonymous users from obtaining system information. However, error messages returned on failed logon by the Windows NT Server reveal information about the password policy to anonymous users.For more information on this vulnerability, please see the Microsoft KnowledgeBase article at:
http://support.microsoft.com/support/kb/articles/q129/4/57.asp

Fix - Apply NT Service Pack 4 to disable anonymous access to password policy information

Microsoft has a fix available that disables anonymous access to password policy information when the RestrictAnonymous access is enabled. When the hotfix is applied and RestrictAnonymous is enabled, anonymous connections cannot obtain password policy information. Microsoft recommends installing the fix on all domain controllers that have Service Pack 3 installed. To resolve this problem, obtain the latest service pack for Windows NT version 4.0. For information on obtaining the latest Service Pack, please visit:
http://support.microsoft.com/support/kb/articles/Q152/7/34.asp
For more information on this vulnerability, please see the following article in the Microsoft Knowledge Base:
http://support.microsoft.com/support/kb/articles/q129/4/57.asp

Low - Malformed Image Header Hotfix

An executable file with a specially-malformed image header can cause a system failure. The machine will thenneed to be restarted to resume service.

For more information on this issue, please see the Microsoft Security Bulletin at:
http://www.microsoft.com/security/bulletins/ms99-023.asp
or
Microsoft Knowledge Base (KB) article Q234557, Executable with a Specially-Malformed Image Header May Crash Windows NT:
http://support.microsoft.com/support/kb/articles/q234/5/57.asp

Fix - Install Service Pack 5 or install the Malformed Image Header hotfix

This issue was first addressed in Windows NT Service Pack 5, and you can protect your computer by installing the latestService Pack for Windows NT 4.0 Server or Workstation.
For information on obtaining the latest Service Pack for Windows NT 4.0, please visit:
http://support.microsoft.com/support/kb/articles/Q152/7/34.ASP
You can also apply the following hotfix if you are running Windows NT 4.0 with Service Pack 4. You can download andapply the patch from:
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/Hotfixes-PostSP4/Kernel-fix/

Low - Pent-fix (F00F) hotfix

The Pent-fix (F00F) Hotfix is not installed on the computer.
When an Intel Pentium processor receives a specific invalid instruction, known as the "F00F," the computer may hang and must be rebooted.
The "F00F" bug received its name from its instruction encoding, F0 0F C7 C8. This instruction encoding maps to a LOCK CMPXCHG8B EAX instruction.

For more information, see Knowledge Base article Q163852 at:
http://support.microsoft.com/support/kb/articles/Q163/8/52.asp

Fix - Apply Windows NT Pent-fix (F00F) Hotfix

Apply the pent-fix hotfix. See:
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP3/pent-fix/README.TXT for instructions on how to apply the hotfix.

The download files are located at:
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP3/pent-fix/

For more information, see Knowledge Base article Q163852 at:
http://support.microsoft.com/support/kb/articles/Q163/8/52.asp

Fixes Required by Host

Hosts/Fixes

172.16.4.212 (SANS)

- Remove Unnecessary Services: FTP
- Restrict permissions for anonymous FTP account
- Upgrade IIS server to latest version
- Disable or remove NEWDSN.EXE
- Remove Unnecessary Services: HTTP (Web)
- Install the Fragmented IGMP Packet patch
- Determine source of ports
- Rename Administrator Account
- Rename Guest Account

- Allow user to change password
- Remove unnecessary dormant users
- Remove unnecessary inactive users
- Change account policy to require regular password changes
- Strengthen Registry on key referenced by HKEY_CLASSES_ROOT\.reg
- Strengthen Registry Permissions: AeDebug
- Strengthen Registry Permissions: Compatibility
- Strengthen Registry Permissions: Drivers
- Strengthen Registry Permissions: Drivers32
- Strengthen Registry Permissions: Embedding
- Strengthen Registry Permissions: HKEY_CLASSES_ROOT
- Strengthen Registry Permissions: MCI
- Strengthen Registry Permissions: MCI Extensions
- Strengthen Registry Permissions: Ports
- Strengthen Registry Permissions: ProfileList
- Strengthen Registry Permissions: WOW
- Restrict access to Performance Monitor Data
- Apply the Microsoft Office Service Release
- Install the Site Wizard Input Validation patch
- Disable Guest access to the NT application log
- Disable Guest access to the NT security log
- Disable Guest access to the NT system log
- Suppress display of last username in login dialog
- Disable caching of logon credentials
- Restrict printer drivers installation
- Display a legal notice before logon
- Edit registry setting to confirm after download
- Apply patch to set "kill bit" for Eyedog ActiveX control
- Install the Misordered Windows Media Services Handshake patch
- Install the Resource Enumeration patch
- Install the Syskey Keystream Reuse hotfix
- Install the Malformed Hit-Highlighting Argument Patch
- Install the Malformed Resource Enumeration Argument hotfix
- Install the Malformed Security Identifier Request hotfix
- Install the RDISK Registry Enumeration File hotfix
- Install the Recycle Bin Creation hotfix
- Install the Spoofed LPC Port Request hotfix
- Install TCP/IP Hotfix to improve TCP Initial Sequence Number randomness
- Restrict access to CDROM drive to currently logged on users
- Restrict access to floppy drive to currently logged on users
- Download and apply patch for dialer.exe
- Install Hotfix Q29973
- Install WinHlp32 Update
- Modify user configuration to restrict logon hours
- Install IIS-fix Service Patch or update to latest Windows NT 4.0 Service Pack
- Apply IIS SSL Error Message Patch
- Install Windows NT SP3 or greater
- Install the CSRSS worker thread exhaustion hotfix
- Apply Windows NT GetAdmin hotfix
- Update Kernal
- Install the LSA3 hotfix
- Install Windows NT SP4 or greater to address SMB denial of service
- Install the hotfix
- Apply Windows NT Priv-fix Hotfix
- Apply Windows NT RPC Spoofing Hotfix
- Apply Windows NT Patch to fix the SECHole Vulnerability
- Apply Windows Srv-fix Hotfix
- Install the IOCTL hotfix
- Install WINS Update
- Apply NT Service Pack 4 to disable anonymous access to password policy information
- Install Service Pack 5 or install the Malformed Image Header hotfix
- Apply Windows NT Pent-fix (F00F) Hotfix

- Install Windows NT SP3 or greater to correct Telnet to port 135 Denial of Service issue
- Apply Windows NT 4.0 Teardrop2 Hotfix
- Apply Land-Fix Hotfix
- Apply Windows NT Teardrop2 Hotfix
- Apply Windows NT Y2k-fix Hotfix

Required Fixes
Fix/Host
Remove Unnecessary Services: FTP 172.16.4.212 (SANS)
Restrict permissions for anonymous FTP account 172.16.4.212 (SANS)
Upgrade IIS server to latest version 172.16.4.212 (SANS)
Disable or remove NEWDSN.EXE 172.16.4.212 (SANS)
Remove Unnecessary Services: HTTP (Web) 172.16.4.212 (SANS)
Install the Fragmented IGMP Packet patch 172.16.4.212 (SANS)
Determine source of ports 172.16.4.212 (SANS)
Rename Administrator Account 172.16.4.212 (SANS)
Rename Guest Account 172.16.4.212 (SANS)
Allow user to change password 172.16.4.212 (SANS)
Remove unnecessary dormant users 172.16.4.212 (SANS)
Remove unnecessary inactive users 172.16.4.212 (SANS)
Change account policy to require regular password changes 172.16.4.212 (SANS)
Strengthen Registry on key referenced by HKEY_CLASSES_ROOT\.reg 172.16.4.212 (SANS)
Strengthen Registry Permissions: AeDebug 172.16.4.212 (SANS)
Strengthen Registry Permissions: Compatibility 172.16.4.212 (SANS)
Strengthen Registry Permissions: Drivers

172.16.4.212 (SANS)
Strengthen Registry Permissions: Drivers32 172.16.4.212 (SANS)
Strengthen Registry Permissions: Embedding 172.16.4.212 (SANS)
Strengthen Registry Permissions: HKEY_CLASSES_ROOT 172.16.4.212 (SANS)
Strengthen Registry Permissions: MCI 172.16.4.212 (SANS)
Strengthen Registry Permissions: MCI Extensions 172.16.4.212 (SANS)
Strengthen Registry Permissions: Ports 172.16.4.212 (SANS)
Strengthen Registry Permissions: ProfileList 172.16.4.212 (SANS)
Strengthen Registry Permissions: WOW 172.16.4.212 (SANS)
Restrict access to Performance Monitor Data 172.16.4.212 (SANS)
Apply the Microsoft Office Service Release 172.16.4.212 (SANS)
Install the Site Wizard Input Validation patch 172.16.4.212 (SANS)
Disable Guest access to the NT application log 172.16.4.212 (SANS)
Disable Guest access to the NT security log 172.16.4.212 (SANS)
Disable Guest access to the NT system log 172.16.4.212 (SANS)
Suppress display of last username in login dialog 172.16.4.212 (SANS)
Disable caching of logon credentials 172.16.4.212 (SANS)
Restrict printer drivers installation 172.16.4.212 (SANS)
Display a legal notice before logon 172.16.4.212 (SANS)
Edit registry setting to confirm after download 172.16.4.212 (SANS)
Apply patch to set "kill bit" for Eyedog ActiveX control

172.16.4.212 (SANS)
Install the Misordered Windows Media Services Handshake patch 172.16.4.212 (SANS)
Install the Resource Enumeration patch 172.16.4.212 (SANS)
Install the Syskey Keystream Reuse hotfix 172.16.4.212 (SANS)
Install the Malformed Hit-Highlighting Argument Patch 172.16.4.212 (SANS)
Install the Malformed Resource Enumeration Argument hotfix 172.16.4.212 (SANS)
Install the Malformed Security Identifier Request hotfix 172.16.4.212 (SANS)
Install the RDISK Registry Enumeration File hotfix 172.16.4.212 (SANS)
Install the Recycle Bin Creation hotfix 172.16.4.212 (SANS)
Install the Spoofed LPC Port Request hotfix 172.16.4.212 (SANS)
Install TCP/IP Hotfix to improve TCP Initial Sequence Number randomness 172.16.4.212 (SANS)
Restrict access to CDROM drive to currently logged on users 172.16.4.212 (SANS)
Restrict access to floppy drive to currently logged on users 172.16.4.212 (SANS)
Download and apply patch for dialer.exe 172.16.4.212 (SANS)
Install Hotfix Q29973 172.16.4.212 (SANS)
Install WinHlp32 Update 172.16.4.212 (SANS)
Modify user configuration to restrict logon hours 172.16.4.212 (SANS)
Install IIS-fix Service Patch or update to latest Windows NT 4.0 Service Pack 172.16.4.212 (SANS)
Apply IIS SSL Error Message Patch 172.16.4.212 (SANS)
Install Windows NT SP3 or greater 172.16.4.212 (SANS)
Install the CSRSS worker thread exhaustion hotfix 172.16.4.212 (SANS)

Apply Windows NT GetAdmin hotfix 172.16.4.212 (SANS)
Update Kernal 172.16.4.212 (SANS)
Install the LSA3 hotfix 172.16.4.212 (SANS)
Install Windows NT SP4 or greater to address SMB denial of service 172.16.4.212 (SANS)
Install the hotfix 172.16.4.212 (SANS)
Apply Windows NT Priv-fix Hotfix 172.16.4.212 (SANS)
Apply Windows NT RPC Spoofing Hotfix 172.16.4.212 (SANS)
Apply Windows NT Patch to fix the SECHole Vulnerability 172.16.4.212 (SANS)
Apply Windows Srv-fix Hotfix 172.16.4.212 (SANS)
Install the IOCTL hotfix 172.16.4.212 (SANS)
Install WINS Update 172.16.4.212 (SANS)
Apply NT Service Pack 4 to disable anonymous access to password policy information 172.16.4.212 (SANS)
Install Service Pack 5 or install the Malformed Image Header hotfix 172.16.4.212 (SANS)
Apply Windows NT Pent-fix (F00F) Hotfix 172.16.4.212 (SANS)
Install Windows NT SP3 or greater to correct Telnet to port 135 Denial of Service issue 172.16.4.212 (SANS)
Apply Windows NT 4.0 Teardrop2 Hotfix 172.16.4.212 (SANS)
Apply Land-Fix Hotfix 172.16.4.212 (SANS)
Apply Windows NT Teardrop2 Hotfix 172.16.4.212 (SANS)
Apply Windows NT Y2k-fix Hotfix 172.16.4.212 (SANS)

2. First step for securing the server + second step of security test

The next step is the most obvious one: applying the latest available service pack. In our case, at the present date (06/2000) the available one is SP6a. This step is also obvious in terms of running the setup, thus no need for a full description of the process. I will rather concentrate on running the same security tests as before, on this newly patched environment:

Results:

Retina version 2.0 having run on a system having SP6a installed:

Address: 172.16.4.212
This is the IP (Internet Protocol) address of the machine, a single machine might have multiple IP adresses associated with it.

Report Date: 06/09/00 14:41:12PM
This is the date and time the scanner started to perform the auditing process. The date and time is reported off the machine local time zone.

Domain Name: SANS
This is the domain name of the machine. There can be multiple domain names assigned to a single IP (Internet Protocol) address or one domain name assigned to multiple IP addresses.

Status: Server Alive
No More Details Available

Audits: 172.016.004.212

FTP Servers: Anonymous FTP
Medium Risk Level
It is recommended that you disable anonymous FTP access if it is not needed. Anonymous FTP access can lead to an attacker gaining information about your system that can possibly lead to them gaining access to your system.
How To Fix:

Follow your FTP server instructions on how to disable anonymous FTP.

Accounts: Administrator - Default Administrator Account

Medium Risk Level

The default Windows NT Administrator account exists on this machine. This account can be a basis for brute force attacks, as it cannot be locked out by too many incorrect password attempts.

How To Fix:

It is suggested to rename the administrator account.

1. Load User Manager
2. Select Administrator
3. Select Rename from under the User menu.

Accounts: IUSR_SANS - Password Does Not Expire

Medium Risk Level

If a users password does not expire you allow a remote attacker endless amount of time to try to figure out your users password. It is recommended that you make all users passwords expire unless the user account is used for a system service.

How To Fix:

Remove the password never expires option from the user account.

1. Open User Manager.
2. Select the user from the list.
3. Select Properties from the User menu.
4. Uncheck "Password Never Expires."
5. Click "Ok".

Accounts: Administrator - Password Does Not Expire

Medium Risk Level

If a users password does not expire you allow a remote attacker endless amount of time to try to figure out your users password. It is recommended that you make all users passwords expire unless the user account is used for a system service.

How To Fix:

Remove the password never expires option from the user account.

1. Open User Manager.
2. Select the user from the list.
3. Select Properties from the User menu.
4. Uncheck "Password Never Expires."
5. Click "Ok".

Accounts: Guest - Password Does Not Expire

Medium Risk Level

If a users password does not expire you allow a remote attacker endless amount of time to try to figure out your users password. It is recommended that you make all users passwords expire unless the user account is used for a system service.

How To Fix:

Remove the password never expires option from the user account.

1. Open User Manager.

2. Select the user from the list.
3. Select Properties from the User menu.
4. Uncheck "Password Never Expires."
5. Click "Ok".

IP Services: gopher service

Medium Risk Level

The gopher service is a rather old unsupported protocol whose predecessor is HTTP.

How To Fix:

Disable the Gopher service.
If you are running a Unix OS disable the gopher service in the /etc/inetd.conf file. Restart inetd so changes will take effect.
If you are running Windows NT then go to Control Panel/Services and disable "Simple TCP/IP services."

Accounts: Guest - Cannot Change Password

Low Risk Level

It is recommended that a machine be set up so that a user has the ability to change their password; otherwise password changes will occur less frequently. However, if this account is one that is used by a system service the ability to change passwords is not something that is required.

How To Fix:

Allow the user to change their password by doing the following:
1. Open User Manager.
2. Select the user from the list box.
3. Select properties from the User menu.
4. Uncheck "User Cannot Change Password."
5. Click "OK".

Accounts: IUSR_SANS - Cannot Change Password

Low Risk Level

It is recommended that a machine be set up so that a user has the ability to change their password; otherwise password changes will occur less frequently. However, if this account is one that is used by a system service the ability to change passwords is not something that is required.

How To Fix:

Allow the user to change their password by doing the following:
1. Open User Manager.
2. Select the user from the list box.
3. Select properties from the User menu.
4. Uncheck "User Cannot Change Password."
5. Click "OK".

Web Servers: IISAdmin

Low Risk Level

The /iisadmin folder is used to remotely administer the Internet Information Server.

How To Fix:

It is recommended that you remove the /iisadmin virtual directory if web based administration of IIS is not needed.

Accounts: Guest - User Never Logged On

Information Risk Level

It is suggested that you review this user account. If it is not needed or was not created by an administrator of your network, it is suggested that you disable or delete it.

How To Fix:

To delete the account:

1. Open User Manager
2. Select the account to delete
3. Press the "Delete" key
4. Click "Ok"

To Disable the account:

1. Open User Manager
2. Select the account to disable
3. Select Properties from the User menu
4. Check "Account Disabled"
5. Click "Ok"

Machine: 172.016.004.212

File Share Name: SANS

This is the name used for the remote systems file sharing. This is typically the same as the remote netbios name.

MAC Address: 0 10 5A A6 70 20

The MAC (Media Access Control) Address is a number assigned to the remote computers network card. This number can be used to know what type of network card is installed in the remote machine.

NIC Brand: 3COM CORPORATION

Netbios Name: SANS

This is the name assigned to the remote computer. The Netbios name is used when doing file and print sharing across netbios networks.

Netbios Workgroup: SANSDOM

This is the workgroup that the remote computer is apart of. Typically in an office enviornment, workstations are joined together by a workgroup. For instance all of the accounting department might be joined by the workgroup "accounting." This workgroup

makes it easier for people within the accounting department to share files with each other.

OS Name: WindowsNT
This is the remote OS (Operating System). For example, Windows, Linux, Solaris etc...

Ports: 172.016.004.212

21: FTP - File Transfer Protocol [Control]
Banner: 220 sans Microsoft FTP Service (Version 3.0).
Protocol: FTP

70: GOPHER - Gopher
No More Details Available

80: WWW-HTTP - World Wide Web HTTP (Hyper Text Transfer Protocol)
Protocol: HTTP
Version: Microsoft-IIS/3.0

135: RPC-LOCATOR - RPC (Remote Procedure Call) Location Service
No More Details Available

139: NETBIOS-SSN - NETBIOS Session Service
No More Details Available

Services: 172.016.004.212

Browser: Computer Browser
Browser (Computer Browser) maintains an up-to-date list of computers on your network and supplied the list to requesting programs.

Browser Service Elections
No More Details Available

Domain Master Browser
No More Details Available

IIS (Internet Information Server)
IIS (Internet Information Server) is a bundled software package that includes, ftp, smtp, and http server software.

LanmanServer: Server
Provides RPC support and file, print, and named pipe sharing.

LanmanWorkstation: Workstation
Provides network connections and communications.

LicenseService: License Logging Service
License Logging Service.

Master Browse
No More Details Available

Messenger Service
No More Details Available

Netlogon: Net Logon
Supports pass-through authentication of account logon events for computers in a domain.

RPCLOCATOR: Remote Procedure Call (RPC) Locator
(RPC) Remote Procedure Call Locator. Manages the RPC name service database.

RpcSs: Remote Procedure Call (RPC)

(RPC) Remote Procedure Call. Provides the endpoint mapper and other miscellaneous RPC services.

Spooler: Print Spooler
Print Spooler. Loads files to memory for later printing.

Shares: 172.016.004.212

ADMIN$: Remote Admin
Default Administration share. The admin$ share is a mapping to \winnt\system32. An attacker could use access to this share to remotely run l0pht crack against your server to find out your passwords.

C$: Default share
This is a default share created when the server first boots. It is a mapping to the root of your C drive.

IPC$: Remote IPC
This is a default share created when the server first boots. Responsible for Inter Process Communications.

NETLOGON: Logon server share
No More Details Available

Users: 172.016.004.212

Administrator: Built-in account for administering the computer/domain
Last logon: Fri Jun 09 13:36:23 2000
Last Logoff: unknown
Password Age: 1 days
Expires: never
Logon Server: *

Max storage: unlimited
Number of Logons: 2
Privilege: Administrator
Password expired: no
RID: 500
Bad PW Count: 0
Country Code: 0

Guest: Built-in account for guest access to the computer/domain
Account Disabled: True
Last logon: never
Last Logoff: unknown
Expires: never
Logon Server: *
Max storage: unlimited
Number of Logons: 0
Privilege: Guest
Password expired: no
RID: 501
Bad PW Count: 0
Country Code: 0

IUSR_SANS: Internet Server Anonymous Access
Full Name: Internet Guest Account
Last logon: Fri Jun 09 13:42:49 2000
Last Logoff: Fri Jun 09 10:50:30 2000
Password Age: 1 days
Expires: never
Logon Server: *
Max storage: unlimited
Number of Logons: 2
Privilege: User
Password expired: no
RID: 1001
Bad PW Count: 0
Country Code: 0

Webtrends version 3.5 having run on the system having SP6a installed

Detected Vulnerabilities and Fixes
Vulnerabilities/Fixes
Medium - Anonymous FTP Anonymous FTP accounts pose security risks unless properly configured and administered.

For more information about anonymous FTP vulnerabilities, see:
ftp://info.cert.org/pub/tech_tips/anonymous_ftp_abuses

Fix - Restrict permissions for anonymous FTP account

Closely monitor anonymous connects to the FTP server. In addition, you may want to reconfigure the FTP Server to disallow anonymous connections.

For information about configuring an anonymous FTP account, see:
ftp://info.cert.org/pub/tech_tips/anonymous_ftp_config

Medium - NEWDSN.EXE exploit

The NEWDSN.EXE exploit allows an intruder to create any file within wwwroot using NEWDSN.EXE cgi. Applies to computers running Microsoft IIS with NEWDSN.EXE installed.

Fix - Disable or remove NEWDSN.EXE

There are two possibilities to resolve this issue.
Set ACLS on the newdsn.exe
or
Remove the newdsn.exe
The newdsn.exe is typically not used - and can safely be removed. This is obviously the most secure. If you use the script - make sure that ACLs are set so that unauthenticated users cannot access it.
Search your hard drives for the file newdsn.exe. The executable could be stored in multiple places - so searching for the file name is the most effective method.

Medium - Fragmented IGMP Packet

Fragmented IGMP packets can cause a variety of problems in Windows 95 and 98, up to and including causing the machine to crash. Windows NT 4.0 contains the same vulnerability, but other system mechanisms make a successful attack much more difficult.

For more information on this issue, please see the Microsoft Security Bulletin at:
http://http://www.microsoft.com/technet/security/bulletin/ms99-034.asp
or
the FAQ of this bulletin at:
http://www.microsoft.com/technet/security/bulletin/fq99-034.asp

Fix - Install the Fragmented IGMP Packet patch

This vulnerability can be easily fixed by downloading and executing the appropriate patch.

- Windows 95:
http://www.microsoft.com/windows95/downloads/contents/WUCritical/vip386/Default.asp

- Windows 98:
http://www.microsoft.com/windows98/downloads/contents/WUCritical/VIP386/Default1.asp

- WindowsNT 4.0 (Workstation and Server):
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP5/IGMP-fix/

Medium - Unidentified TCP ports

Trojans and backdoors typically reside on unidentifiable TCP/UDP ports. The following TCP Ports have been identified.

Fix - Determine source of ports

Determine the source of the ports as they may be backdoors or trojans.

Medium - Administrator account not renamed

The Administrator account should be renamed to a more obscure name to make it more difficult to execute a brute force attempt at password guessing. By renaming the Administrator account, it is harder for a password-seeking intruder to know that they have an account that has an Administrative permission level.

Fix - Rename Administrator Account

To rename the Administrator account on NT 4.0, select the User->Rename menu choice in User Manager.

On Windows 2000:
-Open the Administrative Tools control panel.
-Open the Local Security Policy tool.
-Expand the Local Policies item and select Security Options.
-Double-click on the "Rename administrator account" item in the right window pane and change theadministrator account name.
-Click OK to save the changes.

Medium - Guest account not renamed

The Guest account should be renamed to a more obscure name to make it more difficult to execute a brute force attempt at password guessing.

Fix - Rename Guest Account

To rename the Guest account, select the User->Rename menu choice in User Manager.

On Windows 2000:
-Open the Administrative Tools control panel.
-Open the Local Security Policy tool.
-Expand the Local Policies item and select Security Options.
-Double-click on the "Rename guest account" item in the right window pane and change theguest account name.
-Click OK to save the changes.

Low - FTP service enabled

This test determines if the FTP service is active on your network. Since any service can potentially be exploited, you should minimize the number of services running on your network. Many services are installed as part of the default installation.

Fix - Remove Unnecessary Services: FTP

The FTP service has been detected. Since any service can potentially be exploited, you should minimize the number of services running on your network. Many services are installed as part of the default installation. Remove any services that are unnecessary.

Low - HTTP (Web) service enabled

This test determines if the HTTP (Web) service is active on your network. Since any service can potentially be exploited, you should minimize the number of services running on your network. Many services are installed as part of the default installation.

Fix - Remove Unnecessary Services: HTTP (Web)

The HTTP (Web) service has been detected. Since any service can potentially be exploited, you should minimize the number of services running on your network. Many services are installed as part of the default installation. Remove any services that are unnecessary.

Low - User cannot change password

A user was found that is prevented from changing their password. The User Cannot Change Passwordoption should primarily be used when the passwords for user accounts are administered centrally by thenetwork administrator. This option is often used if several users share the same account. If userscannot change their password, there is a risk that if the password is exposed that the user will nottake adequate action to get the password changed.

Fix - Allow user to change password

On Windows NT 4.0:
-Change the user policy to allow the user to change their password
-From the Windows NT User Manager, highlight the user and select "Properties" from the "User" menu.
-In the resulting "User Properties" dialog, uncheck the "User Cannot Change Password" checkbox.
-Click the OK button to save your changes.

On Windows 2000:
-Open the Administrative Tools control panel.
-Open the Computer Management tool.
-Expand the Local Users and Groups item and click on Users.
-Double-click the user on the right window pane and uncheck the "User cannot change password" checkbox.
-Select OK to save changes.

Low - User has not logged on in specified number of days

A user account was detected that has not logged in recently, based on the number of days specified in thetest properties. Dormant user accounts are often excellent targets for intruders, sincethey are not in active use, and unusual activity or changes may go unnoticed.

Fix - Remove unnecessary dormant users

Investigate the account status and usage. If the account is no longer needed, it should be deleted. Note: Even though a user has never logged in locally, it does not guarantee thatthe account is not used. For example, if you have specific accounts for services, theywill have never logged in. Be sure to investigate the use of any account before deleting it.

Low - User never logged in

A user account was detected that has never logged. Inactive user accounts are often excellent targets for intruders, sincethey are not in active use, and unusual activity or changes may go unnoticed.

Fix - Remove unnecessary inactive users

Investigate the account status and usage. If the account is not needed, it should be deleted.
Note: Even though a user has never logged in locally, it does not guarantee thatthe account is not used. For example, if you have specific accounts for services, theywill have never logged in. Be sure to investigate the use of any account before deleting it.

Low - User's password never expires

The user was found to have a password that will never expire. A strong password policy includesrequiring users to change their passwords regularly. The longer a user retains a password, thehigher the risk of exposure of their password.

Fix - Change account policy to require regular password changes

On Windows NT 4.0:
-From the Windows NT User Manager, highlight the user and select "Properties" from the "User" menu.
-In the resulting "User Properties" dialog, uncheck the "Password Never Expires" checkbox.
-Click the OK button to save your changes.

On Windows 2000:
-Open the Administrative Tools control panel.
-Open the Computer Management tool.
-Expand the Local Users and Groups item and click on Users.
-Double-click the user on the right window pane and uncheck the "Password never expires" checkbox.
-Select OK to save changes.

Low - User does not have logon hours set

You might want to restrict the hours during which an account has access to the network. Forexample, certain workers may be able to access network resources only during normal businesshours-Monday through Friday from 8 AM to 5 PM. If accounts are restricted from logon during off hours, it limits the chancethat an intruder will be able to exploit those accounts. Most hacking attempts occuroutside of regular business hours when there is limited staff on hand to notice unusual activity. Restricting logon hours only affects the ability to connect to a server. It does not restrict usersfrom using a workstation.

Fix - Modify user configuration to restrict logon hours

You can manage logon hours for a user account from User Manager.
Highlight the user in the User Manager window and select "Properties" from the "User" menu.
Click the "Hours" button from the User Properties sheet. Please note that the "Hours" button isonly available if you are managing a domain.
The Logon Hours dialog displays a weekly schedule of times allowed for user logon. The dark areasindicate valid logon times. Logon hours are permitted by selecting the desired hours and clicking"Allow". Similarly, restricted hours are specified by selecting the hours and clicking "Disallow".

You can use any of the following four methods to select logon times in the Logon Hours dialog:
Clicking the day of week label-for example, Sunday-selects the entire day.
Clicking the top of an hour column selects that hour every day of the week.
Clicking the column square above Sunday selects the entire week.
Clicking a specific hour selects that hour.
After the logon hours are set, click OK to save the logon hours for that account.

Fixes Required by Host
Hosts/Fixes
172.16.4.212 (SANS) • Remove Unnecessary Services: FTP • Restrict permissions for anonymous FTP account • Disable or remove NEWDSN.EXE • Remove Unnecessary Services: HTTP (Web) • Install the Fragmented IGMP Packet patch • Determine source of ports • Rename Administrator Account • Rename Guest Account • Allow user to change password • Remove unnecessary dormant users • Remove unnecessary inactive users • Change account policy to require regular password changes • Modify user configuration to restrict logon hours

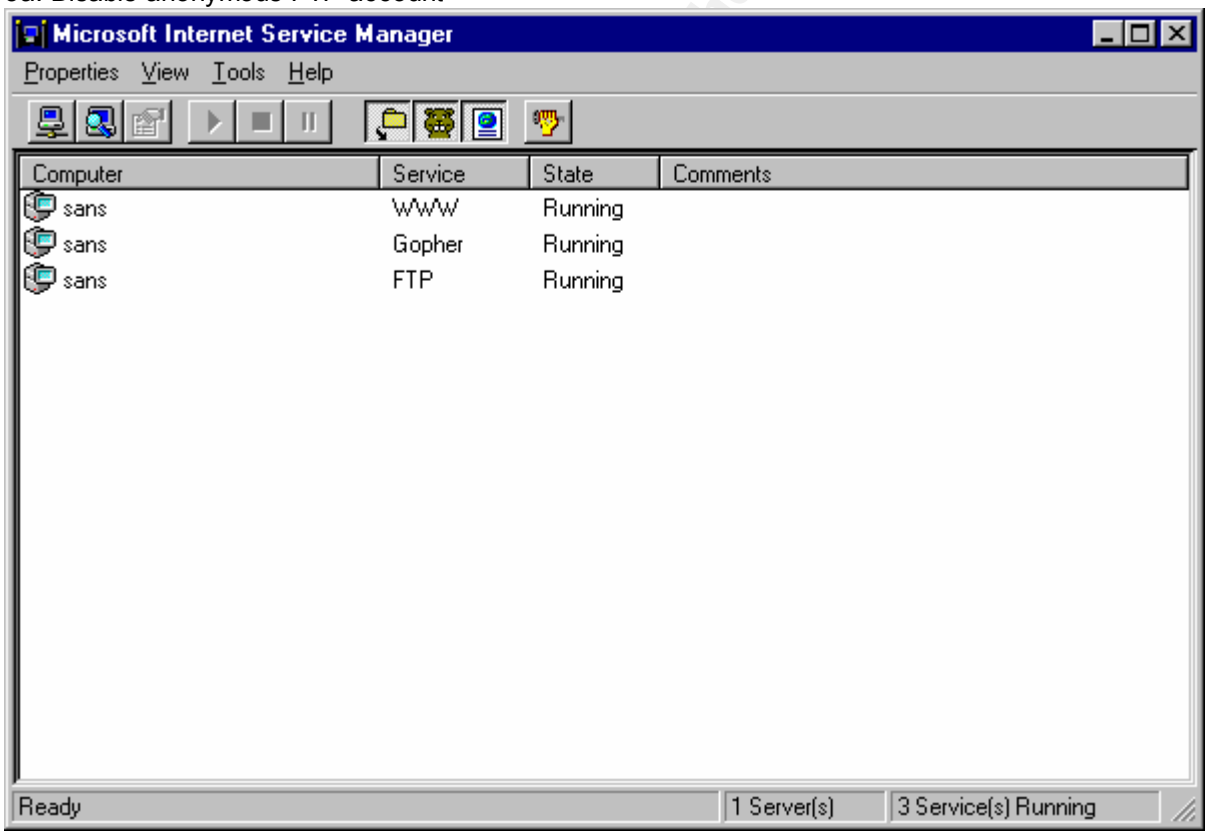
Required Fixes
Fix/Host
Remove Unnecessary Services: FTP 172.16.4.212 (SANS)
Restrict permissions for anonymous FTP account 172.16.4.212 (SANS)
Disable or remove NEWDSN.EXE 172.16.4.212 (SANS)
Remove Unnecessary Services: HTTP (Web) 172.16.4.212 (SANS)
Install the Fragmented IGMP Packet patch 172.16.4.212 (SANS)
Determine source of ports 172.16.4.212 (SANS)
Rename Administrator Account 172.16.4.212 (SANS)
Rename Guest Account 172.16.4.212 (SANS)
Allow user to change password 172.16.4.212 (SANS)
Remove unnecessary dormant users 172.16.4.212 (SANS)
Remove unnecessary inactive users 172.16.4.212 (SANS)
Change account policy to require regular password changes

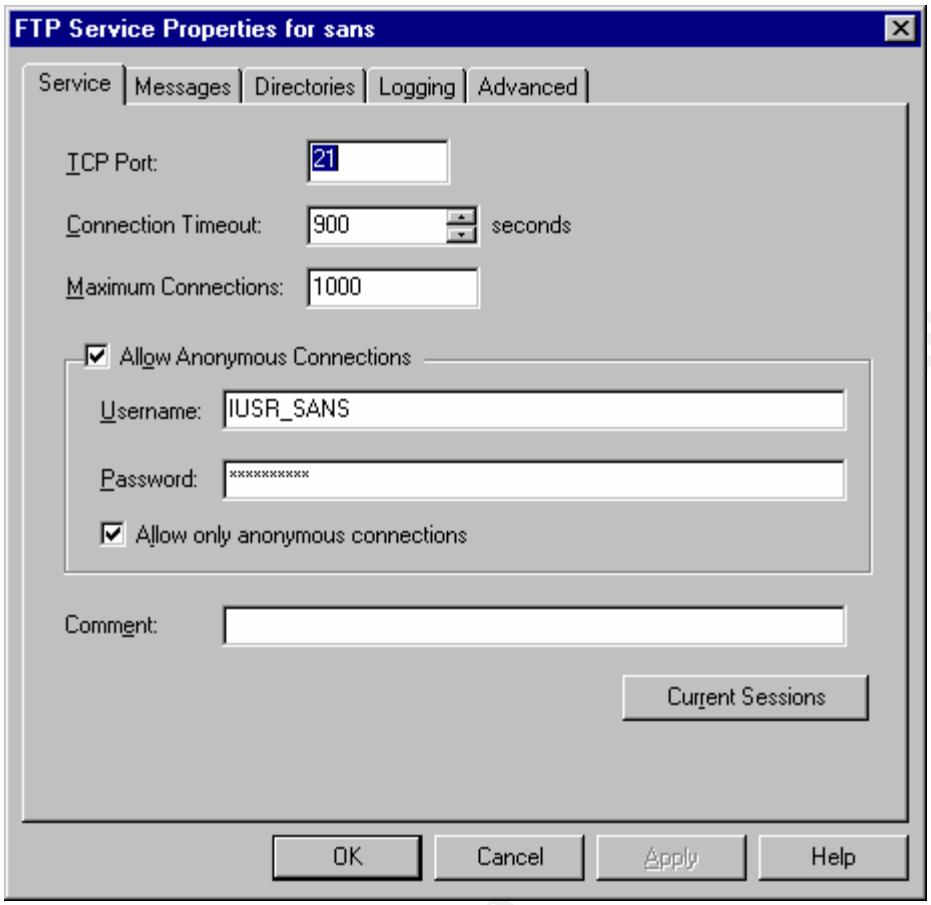
172.16.4.212 (SANS)
Modify user configuration to restrict logon hours 172.16.4.212 (SANS)

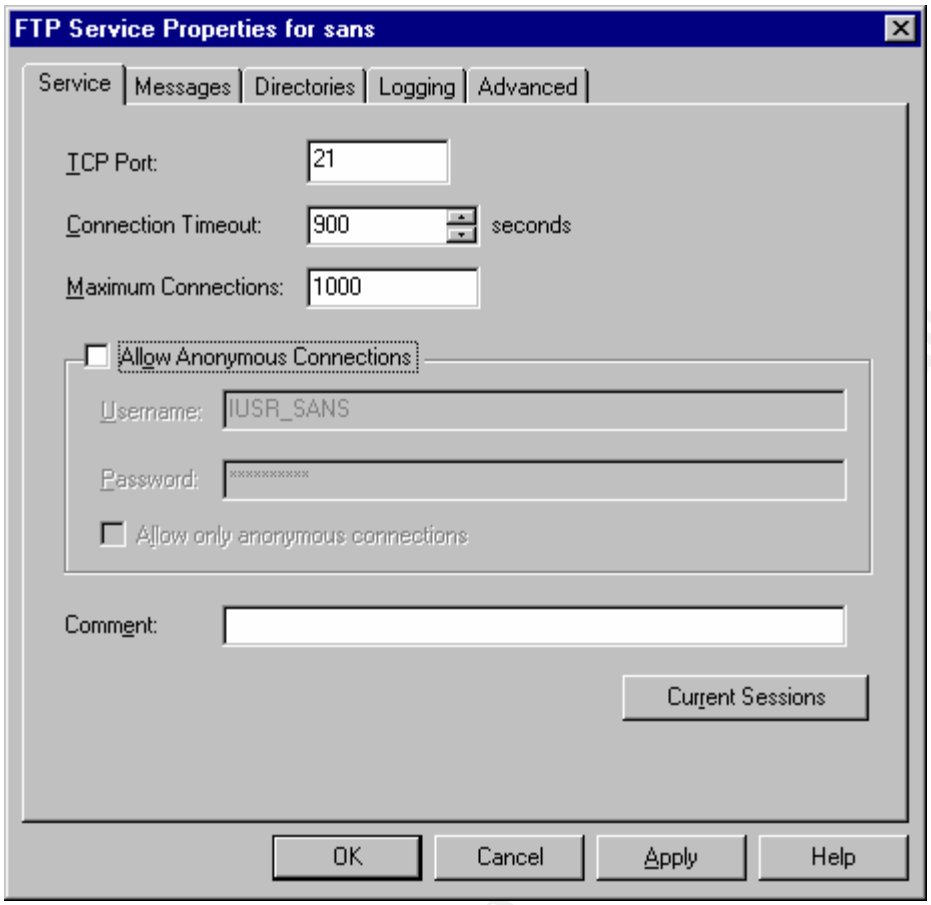
3. Second step for securing the server + third step of security test

At this stage I will try to address the findings of the tools and “manually” produce the changes necessary to strengthen even further our PDC server, based on the recommended fixes. I will try to picture here the needed steps, first, by combining the findings and coming up with a unitary view of what is to done. The following table represents the steps I consider necessary to apply some of the recommended fixes, as well as brief explanation on why (if anything) was not addressed.

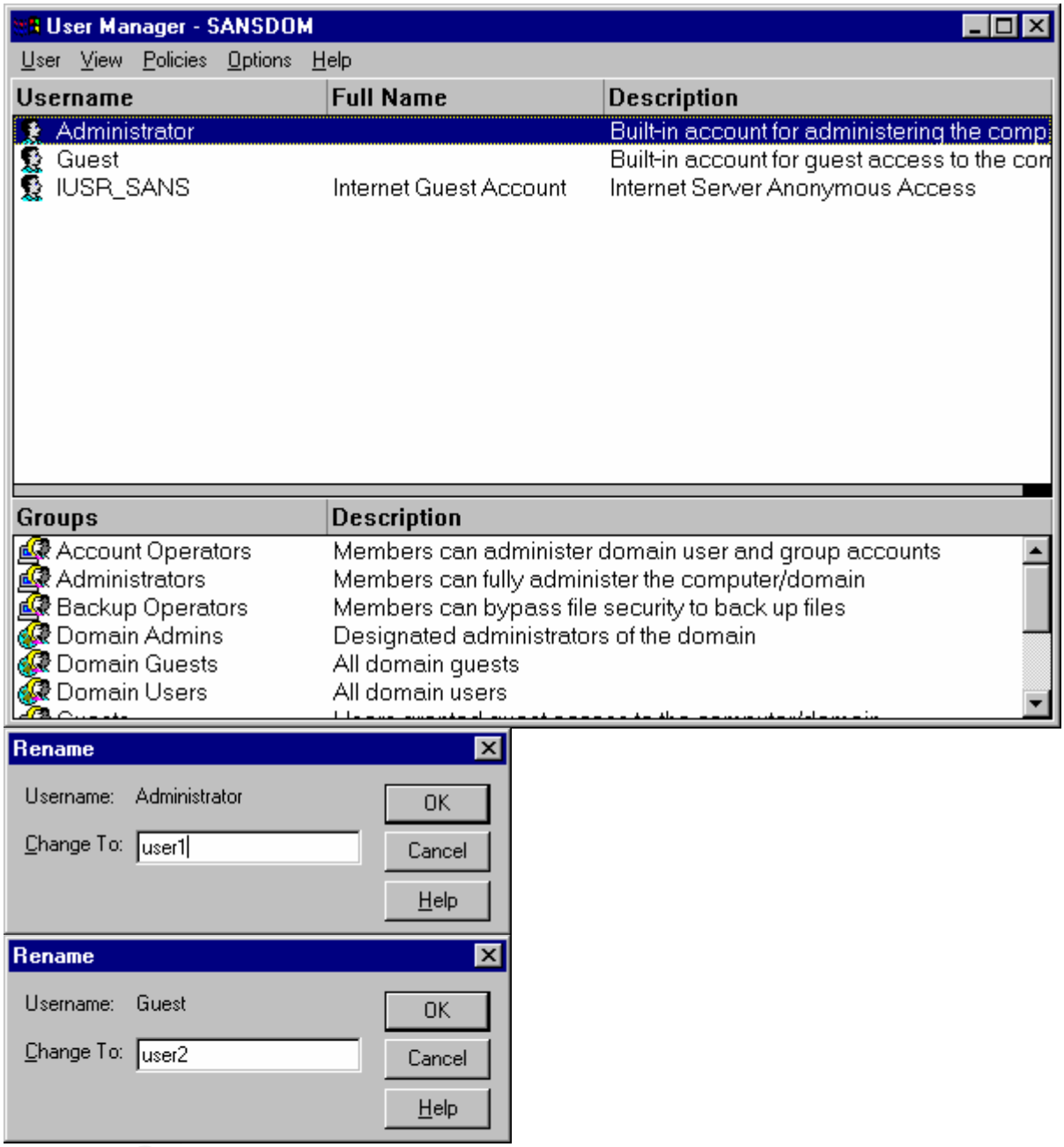
3a. Disable anonymous FTP account



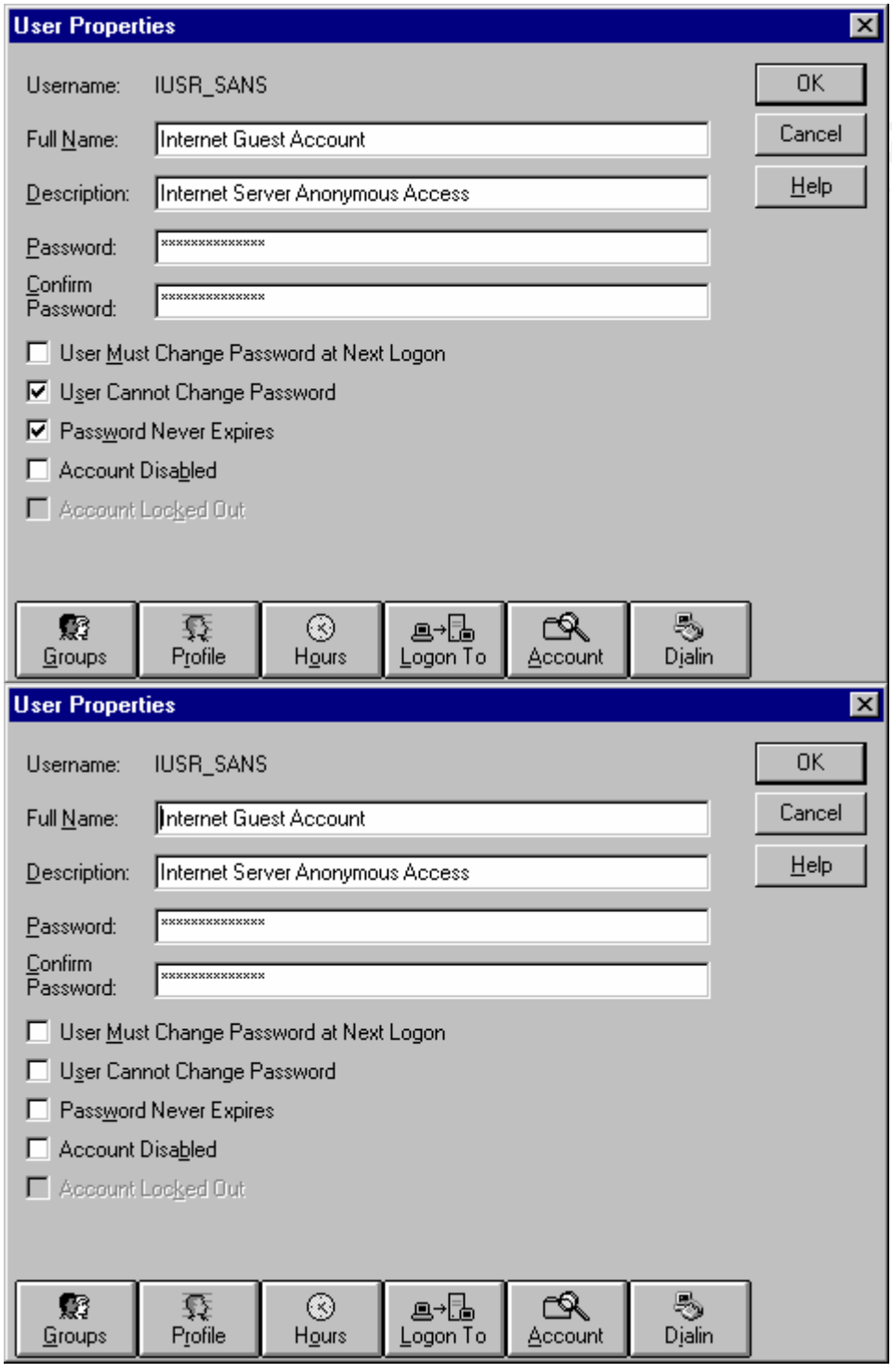




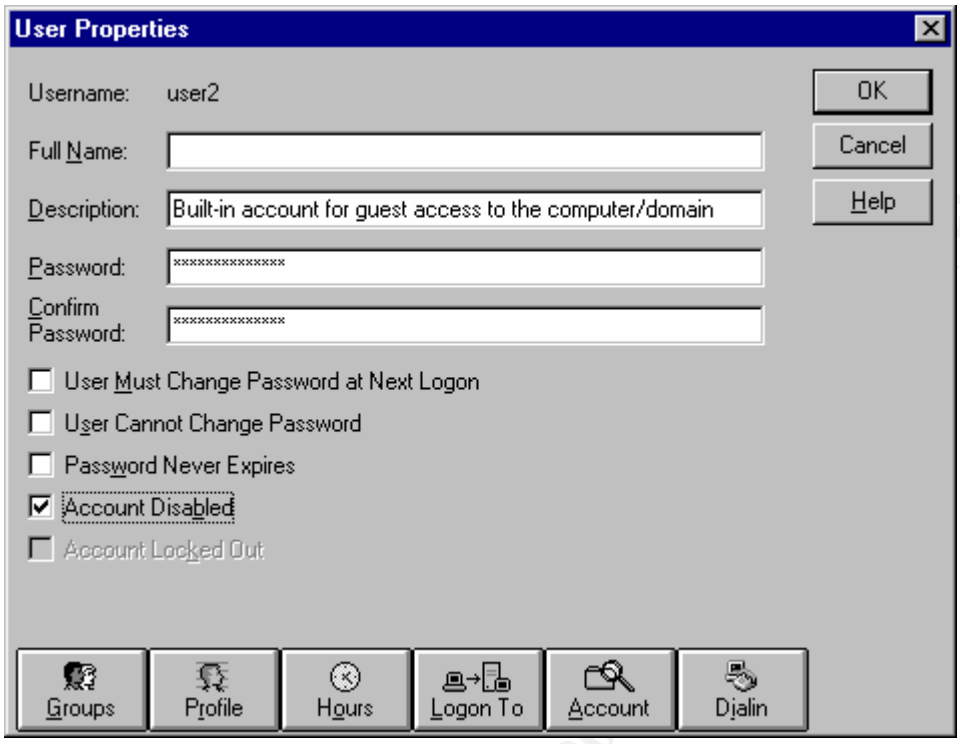
3b. Rename the administrator and guest accounts:



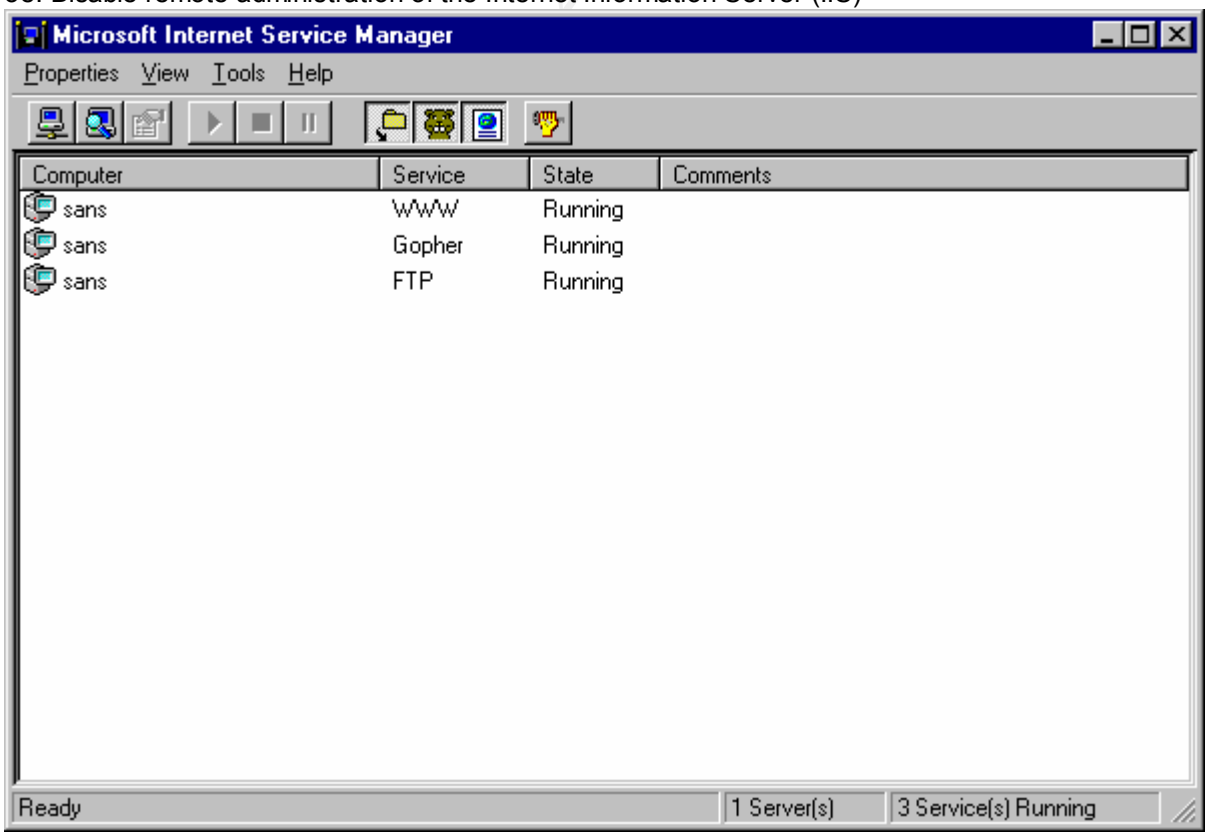
3c. Setup password expiration for guest, administrator and IUSR_SANS accounts, as well as allowing them to change password (I will use IUSR_SANS as example – the others are the same):

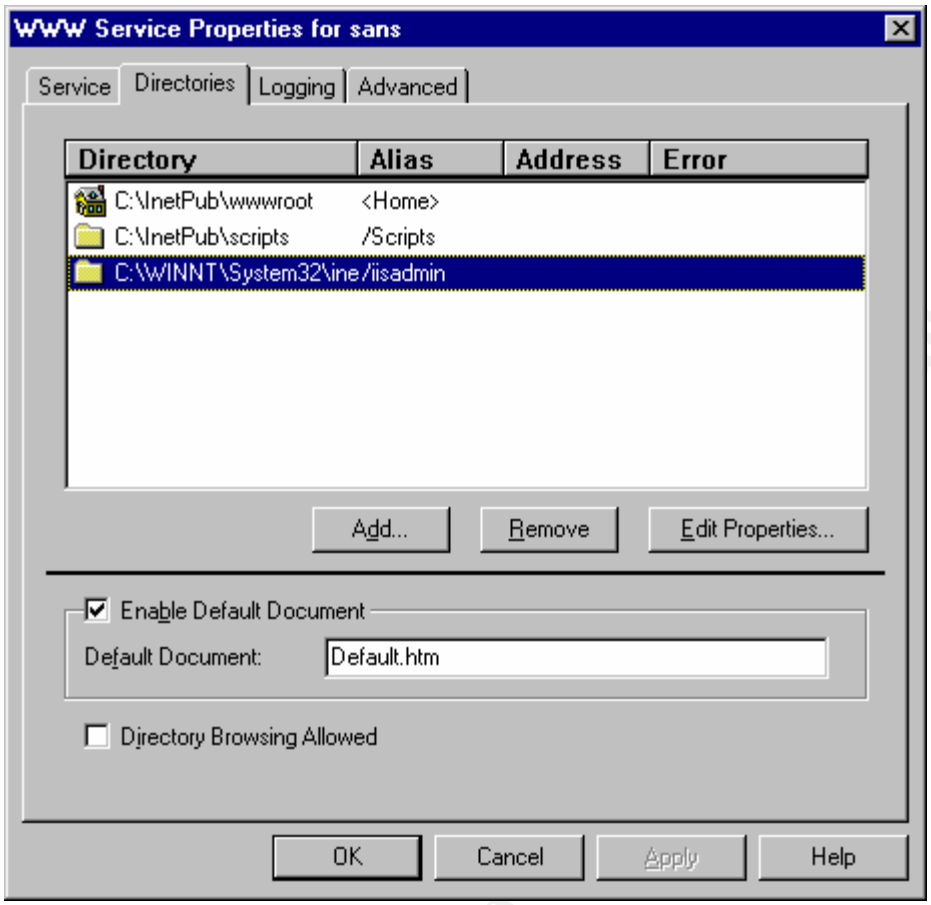


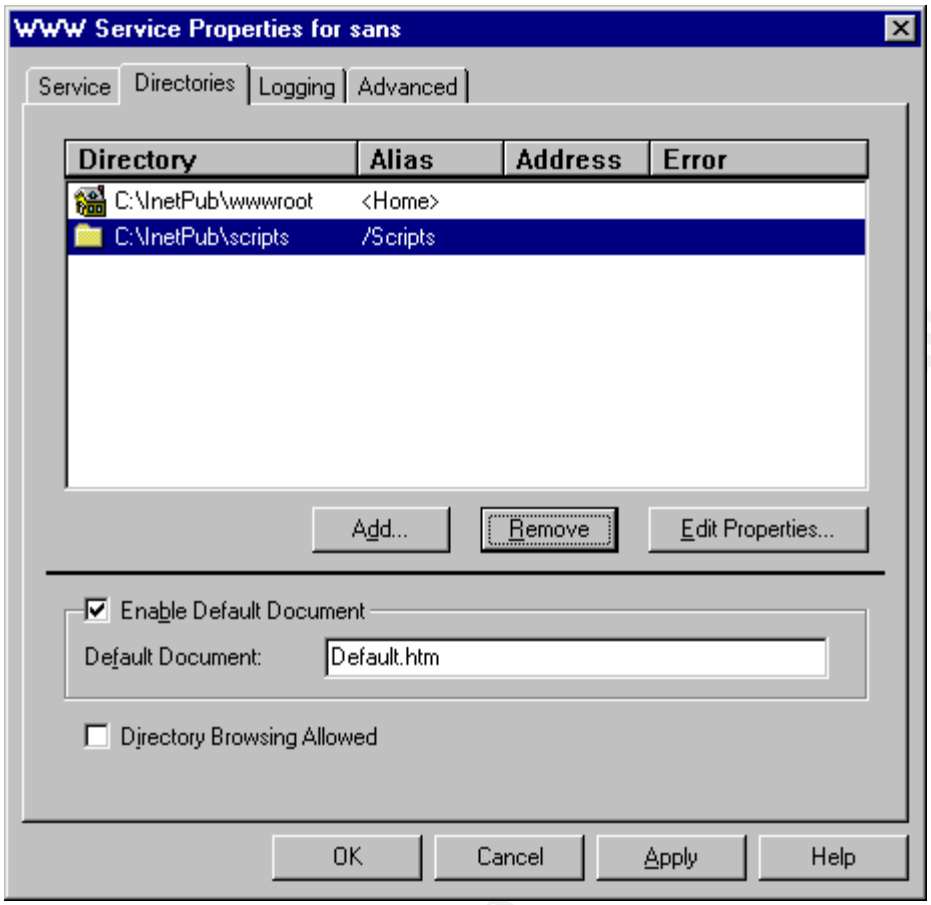
3d. Disable the guest account (for now) – can re-enable, if ever found to be needed:



3e. Disable remote administration of the Internet Information Server (IIS)



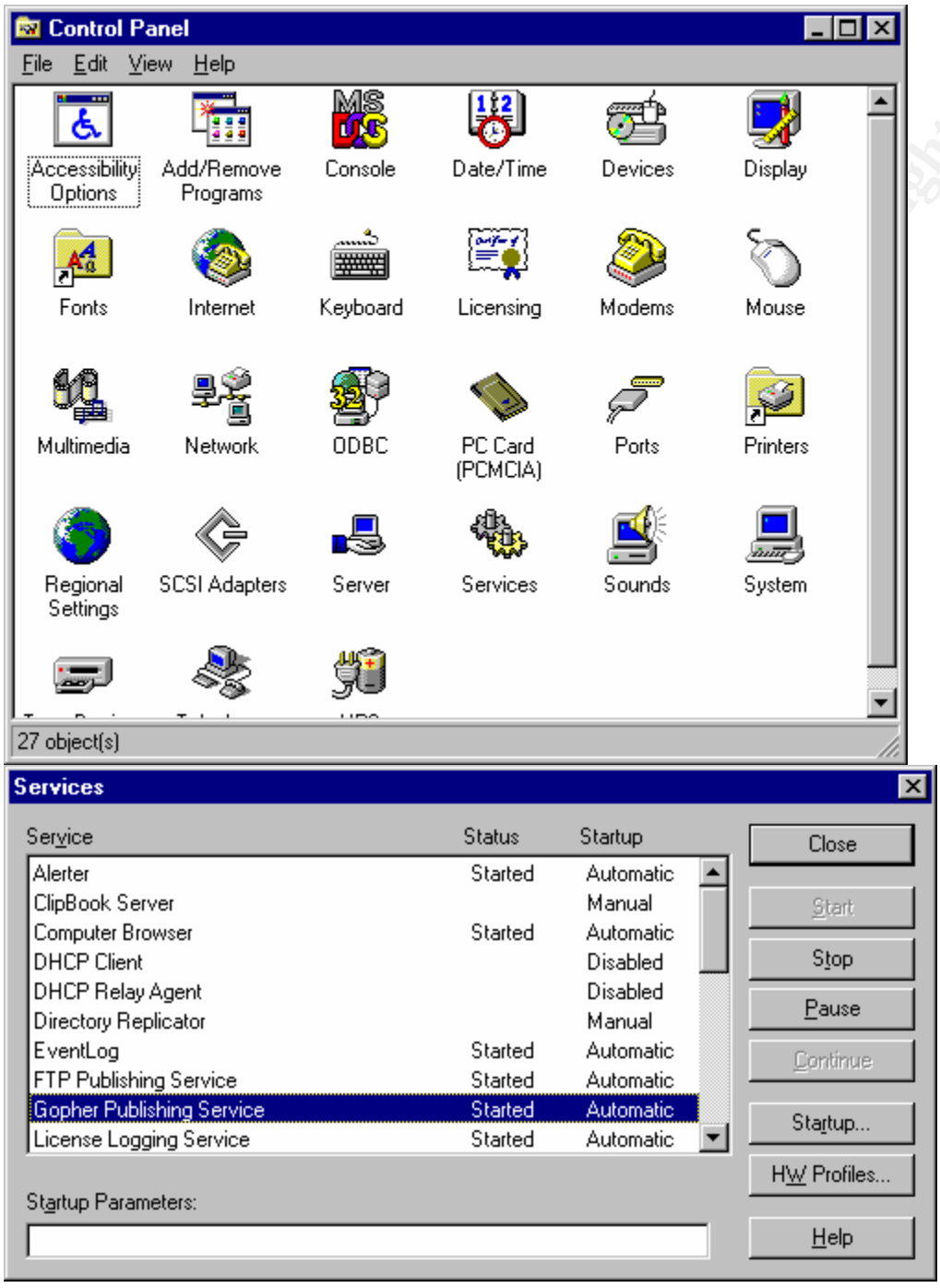


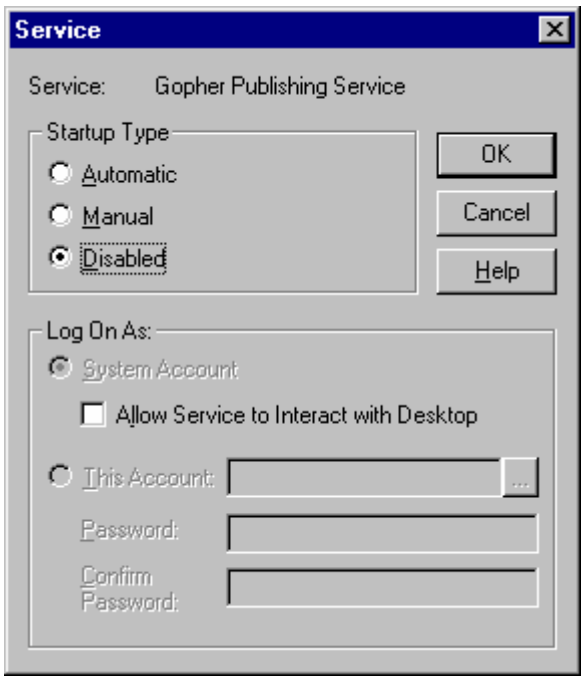


3f. Remove the NEWDSN.EXE

Delete the file NEWDSN.EXE (in the tools folder)

3g. Remove the GOPHER service, if not used:





4. Final step of security test

We will run again the Retina and Webtrends security tests, and we will identify the remaining problems:
Results:

Retina version 2.0 having run on the system with fixes manually applied:

Address: 172.16.4.212
This is the IP (Internet Protocol) address of the machine, a single machine might have multiple IP adresses associated with it.

Report Date: 06/12/00 08:57:15AM
This is the date and time the scanner started to perform the auditing process. The date and time is reported off the machine local time zone.

Domain Name: SANS
This is the domain name of the machine. There can be multiple domain names assigned to a single IP (Internet Protocol) address or one domain name assigned to multiple IP addresses.

Status: Server Alive
No More Details Available

Audits: 172.016.004.212

Web Servers: IISAdmin
Low Risk Level
The /iisadmin folder is used to remotely administer the Internet Information Server.
How To Fix:
It is recommended that you remove the /iisadmin virtual directory if web based administration of IIS is not needed.

Machine: 172.016.004.212

File Share Name: SANS
This is the name used for the remote systems file sharing. This is typically the same as the remote netbios name.

Logged on user: USER1
This is the username of the person currently logged in at the remote machines console. I.E. They are physically sitting infront of the machine.

MAC Address: 0 10 5A A6 70 20
The MAC (Media Access Control) Address is a number assigned to the remote computers network card. This number can be used to know what type of network card is installed in the remote machine.
NIC Brand: 3COM CORPORATION

Netbios Name: SANS
This is the name assigned to the remote computer. The Netbios name is used when doing file and print sharing across netbios networks.

Netbios Workgroup: SANSDOM
This is the workgroup that the remote computer is apart of. Typically in an office enviornment, workstations are joined together by a workgroup. For instance all of the accounting department might be joined by the workgroup "accounting." This workgroup makes it easier for people within the accounting department to share files with each other.

OS Name: WindowsNT
This is the remote OS (Operating System). For example, Windows, Linux, Solaris etc...

Ports: 172.016.004.212

21: FTP - File Transfer Protocol [Control]
Banner: 220 sans Microsoft FTP Service (Version 3.0).
Protocol: FTP

80: WWW-HTTP - World Wide Web HTTP (Hyper Text Transfer Protocol)
Protocol: HTTP
Version: Microsoft-IIS/3.0

135: RPC-LOCATOR - RPC (Remote Procedure Call) Location Service
No More Details Available

139: NETBIOS-SSN - NETBIOS Session Service
No More Details Available

Services: 172.016.004.212

Browser: Computer Browser
Browser (Computer Browser) maintains an up-to-date list of computers on your network and supplied the list to requesting programs.

Browser Service Elections
No More Details Available

Domain Master Browser
No More Details Available

IIS (Internet Information Server)
IIS (Internet Information Server) is a bundled software package that includes, ftp, smtp, and http server software.

LanmanServer: Server
Provides RPC support and file, print, and named pipe sharing.

LanmanWorkstation: Workstation
Provides network connections and communications.

LicenseService: License Logging Service
License Logging Service.

Master Browse
No More Details Available

Messenger Service
No More Details Available

Netlogon: Net Logon
Supports pass-through authentication of account logon events for computers in a domain.

RPCLOCATOR: Remote Procedure Call (RPC) Locator
(RPC) Remote Procedure Call Locator. Manages the RPC name service database.

RpcSs: Remote Procedure Call (RPC)

(RPC) Remote Procedure Call. Provides the endpoint mapper and other miscellaneous RPC services.

Spooler: Print Spooler
Print Spooler. Loads files to memory for later printing.

Shares: 172.016.004.212

ADMIN$: Remote Admin
Default Administration share. The admin$ share is a mapping to \winnt\system32. An attacker could use access to this share to remotely run l0pht crack against your server to find out your passwords.

C$: Default share
This is a default share created when the server first boots. It is a mapping to the root of your C drive.

IPC$: Remote IPC
This is a default share created when the server first boots. Responsible for Inter Process Communications.

NETLOGON: Logon server share
No More Details Available

Users: 172.016.004.212

IUSR_SANS: Internet Server Anonymous Access
Full Name: Internet Guest Account
Last logon: Mon Jun 12 07:36:26 2000
Last Logoff: Fri Jun 09 14:49:09 2000
Password Age: 3 days
Expires: never

Logon Server: *
Max storage: unlimited
Number of Logons: 2
Privilege: User
Password expired: no
RID: 1001
Bad PW Count: 0
Country Code: 0

---

user1: Built-in account for administering the computer/domain
Last logon: Mon Jun 12 07:35:47 2000
Last Logoff: Mon Jun 12 07:29:41 2000
Password Age: 3 days
Expires: never
Logon Server: *
Max storage: unlimited
Number of Logons: 3
Privilege: Administrator
Password expired: no
RID: 500
Bad PW Count: 0
Country Code: 0

---

user2: Built-in account for guest access to the computer/domain
Account Disabled: True
Last logon: Mon Jun 12 06:52:17 2000
Last Logoff: Mon Jun 12 06:52:27 2000
Password Age: 0 days
Expires: never
Logon Server: *
Max storage: unlimited
Number of Logons: 0
Privilege: Guest
Password expired: no
RID: 501
Bad PW Count: 4
Country Code: 0

Webtrends version 3.5 having run on the system with fixes manually applied:

Detected Vulnerabilities and Fixes
Vulnerabilities/Fixes
Medium - Fragmented IGMP Packet Fragmented IGMP packets can cause a variety of problems in Windows 95 and 98, up to and including causing the machine to crash. Windows NT 4.0 contains the same vulnerability, but other system

mechanisms make a successful attack much more difficult.

For more information on this issue, please see the Microsoft Security Bulletin at:
http://http://www.microsoft.com/technet/security/bulletin/ms99-034.asp
or
the FAQ of this bulletin at:
http://www.microsoft.com/technet/security/bulletin/fq99-034.asp

Fix - Install the Fragmented IGMP Packet patch

This vulnerability can be easily fixed by downloading and executing the appropriate patch.

- Windows 95:
http://www.microsoft.com/windows95/downloads/contents/WUCritical/vip386/Default.asp

- Windows 98:
http://www.microsoft.com/windows98/downloads/contents/WUCritical/VIP386/Default1.asp

- WindowsNT 4.0 (Workstation and Server):
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP5/IGMP-fix/

Medium - Unidentified TCP ports

Trojans and backdoors typically reside on unidentifiable TCP/UDP ports. The following TCP Ports have been identified.

Fix - Determine source of ports

Determine the source of the ports as they may be backdoors or trojans.

Medium - Guest account enabled

The Guest account is enabled on the host.
The Guest account can be used by anonymous users to connect to the computer.

Fix - Disable the Guest account

On Windows NT 4.0:
-the Guest account should be disabled by starting Windows NT User Manager,double clicking on the Guest Account and checking the "Account Disabled" checkbox.
On Windows 2000:
-Open Control Panel.
-Open the Administrative Tools control panel.
-Open Computer Management tool.
-Expand the Local Users and Groups item.
-Click on the Users item.
-On the right pane of the windows, double-click on the Guest account and check the "Account is disabled" checkbox.

Medium - Unidentified UDP ports

Trojans and backdoors typically reside on unidentifiable TCP/UDP ports. The following UDP Ports have

been identified.

Fix - Determine source of ports

Determine the source of the ports as they may be backdoors or trojans.

Low - FTP service enabled

This test determines if the FTP service is active on your network. Since any service can potentially be exploited, you should minimize the number of services running on your network. Many services are installed as part of the default installation.

Fix - Remove Unnecessary Services: FTP

The FTP service has been detected. Since any service can potentially be exploited, you should minimize the number of services running on your network. Many services are installed as part of the default installation. Remove any services that are unnecessary.

Low - HTTP (Web) service enabled

This test determines if the HTTP (Web) service is active on your network. Since any service can potentially be exploited, you should minimize the number of services running on your network. Many services are installed as part of the default installation.

Fix - Remove Unnecessary Services: HTTP (Web)

The HTTP (Web) service has been detected. Since any service can potentially be exploited, you should minimize the number of services running on your network. Many services are installed as part of the default installation. Remove any services that are unnecessary.

Low - User has not logged on in specified number of days

A user account was detected that has not logged in recently, based on the number of days specified in thetest properties. Dormant user accounts are often excellent targets for intruders, sincethey are not in active use, and unusual activity or changes may go unnoticed.

Fix - Remove unnecessary dormant users

Investigate the account status and usage. If the account is no longer needed, it should be deleted. Note: Even though a user has never logged in locally, it does not guarantee thatthe account is not used. For example, if you have specific accounts for services, theywill have never logged in. Be sure to investigate the use of any account before deleting it.

Low - User never logged in

A user account was detected that has never logged. Inactive user accounts are often excellent targets for intruders, sincethey are not in active use, and unusual activity or changes may go unnoticed.

Fix - Remove unnecessary inactive users

Investigate the account status and usage. If the account is not needed, it should be deleted. Note: Even though a user has never logged in locally, it does not guarantee thatthe account is not used. For example, if you have specific accounts for services, theywill have never logged in. Be sure to investigate the use of any account before deleting it.

Low - User does not have logon hours set

You might want to restrict the hours during which an account has access to the network. Forexample, certain workers may be able to access network resources only during normal businesshours-Monday through Friday from 8 AM to 5 PM. If accounts are restricted from logon during off hours, it limits the chancethat an intruder will be able to exploit those accounts. Most hacking attempts occuroutside of regular business hours when there is limited staff on hand to notice unusual activity. Restricting logon hours only affects the ability to connect to a server. It does not restrict usersfrom using a workstation.

Fix - Modify user configuration to restrict logon hours

You can manage logon hours for a user account from User Manager.
Highlight the user in the User Manager window and select "Properties" from the "User" menu.
Click the "Hours" button from the User Properties sheet. Please note that the "Hours" button isonly available if you are managing a domain.
The Logon Hours dialog displays a weekly schedule of times allowed for user logon. The dark areasindicate valid logon times. Logon hours are permitted by selecting the desired hours and clicking"Allow". Similarly, restricted hours are specified by selecting the hours and clicking "Disallow".

You can use any of the following four methods to select logon times in the Logon Hours dialog:
Clicking the day of week label-for example, Sunday-selects the entire day.
Clicking the top of an hour column selects that hour every day of the week.
Clicking the column square above Sunday selects the entire week.
Clicking a specific hour selects that hour.
After the logon hours are set, click OK to save the logon hours for that account.

Fixes Required by Host

Hosts/Fixes
172.16.4.212 (SANS) • Remove Unnecessary Services: FTP • Remove Unnecessary Services: HTTP (Web) • Install the Fragmented IGMP Packet patch • Determine source of ports • Disable the Guest account • Remove unnecessary dormant users • Remove unnecessary inactive users • Modify user configuration to restrict logon hours

Required Fixes

Fix/Host
Remove Unnecessary Services: FTP 172.16.4.212 (SANS)
Remove Unnecessary Services: HTTP (Web) 172.16.4.212 (SANS)
Install the Fragmented IGMP Packet patch 172.16.4.212 (SANS)
Determine source of ports

172.16.4.212 (SANS)
Disable the Guest account 172.16.4.212 (SANS)
Remove unnecessary dormant users 172.16.4.212 (SANS)
Remove unnecessary inactive users 172.16.4.212 (SANS)
Modify user configuration to restrict logon hours 172.16.4.212 (SANS)

5. Conclusions

We have gone through an multi-phase analysis of an NT system, setup as a Primary Domain Controller (PDC):

1. Phase 1: default installation from an original Microsoft CD (the latest version available for the US had the NT server with Service Pack 1 – 128-bit);
2. Phase 2: identified two different tools for NT security audit – after going through different tools available for this purpose, the ones I found to qualify both from an NT user community recognition, and as they had evaluation versions available, were: Retina version 2.0 (developed by Eeye – www.eeye.com) and Webtrends Security Analyzer version 3.5 (developed by Web trends – www.wbetrends.com);
3. Phase 3: run the two tools against the system mentioned above. The results will be summarized in a table at the end;
4. Phase 4: as the first rule of securing an NT system, I have downloaded and applied the latest service pack available at the time of this analysis (June 2000), i.e. SP6a;
5. Phase 5: run the two tools against the newly patched system, and record the results;
6. Phase 6: analyzed the recommended problems still found by the security analyzers, and manually applied the needed fixes;
7. Phase 7: run the security tools against the newly fixed system, and recorded the results.

After all of the above tests, the results (see all the material above for details) are as follows (**R** – Retina, **W** – Webtrends):

System status	Number of problems by level of severity and by security tool			Notes
	Major	Medium	Low	
Windows NT server – SP1 – 128-bit	R = 0 W = 13	R = 6 W = 45	R = 3 W = 19	Retina also reported 1 (one) information risk level
Windows NT server – SP6a – 128-bit	R = 0 W = 0	R = 6 W = 6	R = 3 W = 7	
Windows NT server – SP6a and fixes manually applied	R = 0 W = 0	R = 0 W = 4	R = 1 W = 5	

Retina still reported 1 (one) low risk level issue (IISAdmin), even after I applied its own recommended fix (removal of the /iisadmin virtual directory) ?!?

Webtrends still reported the followings:

- fragmented IGMP packets – the recommened fix was not applicable, though, as it detects a Service Pack level higher than the one it was designed for (SP6a, instead of the expected SP5) – one would expect for Microsoft to have incorporated the IGMP fix in the SP6a, so – hopefully – that was the case (and we can assume Webtrends wasn't updated yet);
- guest account enabled – actually the guest account WAS disabled (see the steps above ?!?
- unidentified UDP ports – almost impossible to determine what Webtrends identified (the only UDP ports open on that server – via "netstat –na" – where the well known "Microsoft ports", i.e. 135, 137, 138);
- FTP service enabled – we assumed we would need this on a server, so I decided not to remove it (the only precautionary measure was disabling anonymous logon);
- HTTP service enabled – same as above;
- User not logged on in a specified number of days – most likely it identified the ex-guest (now user2) account, which I had no reason to login as, and whose account I disabled anyway;
- Same for user never logged one;
- User not having established logon hours – this is easy to remedy upon deployment in real production environment, when the appropriate time will be determined

The conclusion is that – with a minimal investment of time and with some financial investment on one of the tools available on the market for security audit – it is safe to assume that an NT server can be secured in a very straightforward manner. One thing to always remember: start any security step for NT by **applying the latest Service Pack, or recommended Microsoft security patches.**

Last Updated: July 26th, 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**