Using Auditing to Improve the Security of Microsoft Windows NT Server 4.0, Terminal Server Edition.

SANS GIAC GSNA Practical Assignment (v1.0)

Richard G. Norman

08 August 2001

Table of Contents

1. Objective

This paper was written to satisfy the requirements for the SANS GIAC GSNA Practical Assignment (v1.0) as set for SANS Parliament Square held in London, England during June 2001.

There have been many articles written covering the security (or lack thereof •) of Microsoft Windows NT systems but much less attention appears to have been given to the security of multi-user Windows systems.

These multi-user Windows NT systems (examples include Microsoft Windows NT Server 4.0, Terminal Server Edition and Citrix MetaFrame) present a range of unique security issues and thus require a different approach than Windows NT Server when attempting to secure and audit them.

This paper will attempt to explain these issues; offer some suggestions about how to optimise these tasks using recognised security auditing techniques, and present a consolidated checklist that can be used to audit a Microsoft Windows NT Server 4.0, Terminal Server Edition server.

2. Technology Overview

Microsoft Windows NT 4.0 Terminal Server Edition is a special version of the Microsoft Windows NT Server 4.0 product that incorporates technologies originally developed by Citrix that later became the subject of a cross-licensing deal between Citrix and Microsoft.

One of the key differences between Microsoft Windows NT 4.0 Server (hereinafter referred to as NT4S) and Microsoft Windows NT 4.0 Terminal Server Edition (hereinafter referred to as NT4TSE) is the way access to the server is controlled.

In a typical secure environment the NT4S server machines would be housed in a physically secure environment (e.g. a locked computer room) and only a limited number of users would be granted physical access to the machine (i.e. console logons). By comparison, even if the NT4TSE machine is kept in a physically secure environment the multi-user architecture invites users to establish virtual sessions on the server as though they were logging on to the console. *This can be considered equivalent to opening the computer room door to all users!*

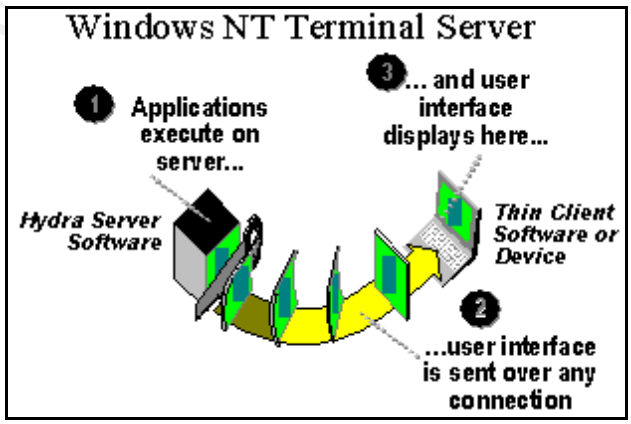


Figure 1. Windows Terminal Server Architecture[1](source **Microsoft TechNet**)

Microsoft acknowledges the security risks inherent to this approach as the following extracts from the Microsoft web site show:

'One of the major problems with Terminal Server is that the default security of the operating system after installation is not nearly sufficient for any production deployment. Although this is exactly the same behavior as Windows NT Server or Workstation, because any user on a Terminal Server is running locally, default security provides even the regular user with far too many security privileges. Couple this with the fact that system auditing, a way of tracking changes or attempted changes in the environment, is not enabled by default, and you could find your Terminal Server in a nonfunctional state shortly after implementation.' [2]

..and..

'When users access a session through a Terminal Server, by default, they have access to all files on the Terminal Server. The actions of one user can have a detrimental effect on other users of the Terminal Server.' [3]

There are a number of other significant factors, but the extracts above should make the potential security vulnerabilities that a badly configured NT4TSE server could introduce abundantly clear.

The Multi-User Windows family incorporates a range of technology variants (e.g. NT4TSE, Citrix MetaFrame, Windows 2000 Server etc.) running on a range of different hardware platforms (from a single server to large multiple-server farms) across any of the supported network infrastructures.

This degree of flexibility makes it possible for almost every business to successfully utilise multi-user Windows technology but also necessitates careful planning when undertaking security audits to ensure that the specific environment has been properly audited and that nothing has been overlooked. Consequently, this investigation will be limited to the combination of hardware and software detailed in section 6 on page 8.

Despite the specific scope of this investigation, it should be possible to utilise this approach and the checklists when investigating any multi-user Windows environment.

3. The Current State of Practice for Auditing NT4TSE

Because NT4TSE is essentially a variant of NT4S, it is essential that the underlying machine be properly secured first before any attempt is made to secure the additional functionality offered by NT4TSE.

There is a wealth of information published covering the procedures necessary to secure and audit the security of NT4S machines but there appears to be very little available concerning securing the combination of NT4S and NT4TSE.

For example, the SANS Reading Room (http://www.sans.org/infosecFAQ/win/win_list.htm) contains numerous papers detailing the steps necessary to secure NT4S machines but has only a few papers covering NT4TSE and/or Citrix MetaFrame.

I spent a considerable amount of time trying to find any existing audit checklists for the combined NT4S and NT4TSE environment, but did not manage to find any. I did find a few articles about securing Citrix MetaFrame and NT4TSE but many of these were of a narrative nature rather than in checklist form – for instance, the article by Mark RiCharde[4] in the SANS InfoSec Reading Room details the enhanced functionality that Citrix MetaFrame offers and discusses some of the security issues regarding this platform but does not make many concrete suggestions for auditing it.

In an attempt to generate a consolidated list for auditing NT4TSE, I decided to combine the applicable portions of the checklists and narrative-style 'how-to' lists detailed in Appendix 1. with additions and edits where necessary. Additional general resources used are listed in the References[5] section. These resources generally cover a common core of pointers and so I have only cross-referenced those which are unique to individual lists.

The security audit checklist is included in section 6 and is very extensive. All the controls need to be checked to audit the NT4TSE system properly.

This checklist includes the audit results of a sample machine named TSETSE, which was built in a test environment for the express purposes of developing this checklist. These sample results are all formatted as hidden text in Microsoft Word so that they can be viewed and printed or hidden as preferred.

Click ¶ on the Standard Word toolbar in Word 2000 to hide or unhide these sample results when viewing this document on screen.

To choose whether to print the checklist with or without these sample results change the state of the 'print hidden text' checkbox in the Word Options applet under the 'Print' tab.

4. General Warning

Please note that the suggestions for changes contained in this document could render your server/s inoperable if implemented in a production environment without being fully tested prior to being applied.

Please do not attempt any changes unless you are sure that they are appropriate for your server and network environment.

The testing techniques suggested below should only be attempted if properly authorised and with sufficient knowledge not to try anything that could break a production system.

Failure to obtain proper authorisation could result in hacking charges being levelled against the person making these tests.

5. Subjective Measurements

There are not many subjective measurements that can be applied to NT4TSE as most of the settings are either *on* or *off* e.g. a binary registry value or a non-existent registry key.

Arguably the only way to audit a NT4TSE system subjectively would be to perform penetration testing on the machine. This would entail working through the objective checklist listed below and then using whatever tools are available to try to circumvent the security measures that have been applied.

NT4TSE does make this type of testing fairly convenient because the tester can establish multiple remote sessions and be logged in as an administrator and a normal user at the same time from a remote PC. It is then possible to attempt something as the normal user then switch sessions and confirm whether the Event Logs etc. have picked up whatever attempt was made. The auditor can then switch to the desktop on his/her host (local) machine and record the results of the test. Screenshots can be easily captured from either NT4TSE session and pasted into the report to provide proof of actions and results.

Example techniques that could be used to subjectively test the security of a NT4TSE server could include:

- Attempting to log in using the Administrator account (which should be a disabled dummy account)
- Attempting to login using an incorrect password (to test account lockout)
- Using third-party tools in an attempt to edit the registry remotely (to test registry security)
- Logging in as a non-administrative user then attempting to access files and folders which should be off-limits to normal users (to test file and folder permissions)
- Attempting to use system utilities (e.g. IPCONFIG or FTP) while logged in as a normal user (to test application security and user rights)
- Attempting to change a password to something that should fail the strong password requirements
- Attempting to enter the secure area housing the server when unauthorised (could anyone slip in behind an administrator? Are strangers questioned when snooping around the server room? etc.)
- Attempting to delete crucial system files while logged in as a normal user (to test file and folder permissions and the audit logs etc.)
- Attempting to edit the UserLogon.cmd file to insert some unauthorised code when logged in as a non-administrative user
- Attempting to use various tools to try to crack the passwords to the machine

6. Objective Measurements (Audit Checklist)

Auditing the objective factors influencing the security of NT4TSE machines is far easier as the steps to be taken are all clearly documented by Microsoft and numerous security organisations. Unfortunately, there appears to be no consolidated checklist for NT4TSE at present so I have attempted to create a checklist that could be used to objectively measure the factors that affect NT4TSE server security.

It really surprised me that there were so many points to check and that there was no easy way to secure a NT4TSE machine other than to do it manually. It also surprised me that the default installation of NT4TSE is so potentially insecure. I had always thought that the NT4TSE servers I had built in the past were reasonably secure but when I audited them against this checklist I became aware of how many vulnerabilities they still had.

NT4TSE contains many of the tools required to do this audit but some tools will need to be obtained from other sources. The Windows NT Resource Kits contain a number of very useful tools and utilities and many of these could be utilised when auditing machines. I have detailed the tools to be used throughout the checklist and, where appropriate, included screenshots in Appendix 2 on page 89 onwards.

The test machine (TSETSE) was built and configured as detailed below:

- NT4TSE was installed onto a Dell Optiplex GXI machine using mostly default settings
- The machine has just one network interface
- The machine has just one hard disk drive (IDE), one IDE CD-ROM drive and one floppy drive.
- The Operating System had been patched and HotFixes had been applied according to the recommendations of the Microsoft Windows Update site for NT4TSE http://www.microsoft.com/ntserver/terminalserver/downloads/default.asp
- The machine was configured as a standalone server on a workgroup

A number of assumptions have been made regarding the machine, the audit process and auditor and the fictitious company environment the machine is operated in. These are:

- The auditor has an administrator-level account as well as a user-level account to use during the audit process
- The auditor has physical access to the server as well as access to a workstation which has the NT4TSE client installed
- The auditor is reasonably proficient with NT4TSE and NT4S
- The auditor has been granted the permission necessary to undertake this specific audit
- The audit will be conducted at a time which minimises any unplanned downtime accidentally caused by the audit process
- The server is housed in a reasonably secure physical environment
- The server is not Internet or public facing and is on a protected company network (i.e. not in a DMZ)

6.1 Physical Security and Server Hardware

This section will attempt to establish whether the server is housed and maintained in accordance with best practice guidelines. An amazingly large percentage of server-class machines are housed in insecure or otherwise inappropriate environments and these controls serve to highlight these vulnerabilities:

Control	Response	Auditor's Comments	General Comments and Guidance Notes
1. Server Name			
2. Date of Audit			
3. Location of machine			*Record the physical location of the machine (e.g. Server room 2, Rack 1).*
4. Auditor's Name			
5. Record the name/s and titles of any other person/s attending the audit.			*This might include the System Administrator etc.*
6. Is the Server kept in a secure room? If No, go to question 8.			
7. Describe the methods used to secure the room.			

8. List the personnel who have access to the secure room.			
9. Is there any evidence of a keystroke capturing device plugged into the keyboard socket?			*Keystroke capturing devices are small devices which are inserted between the keyboard and the computer and which can record every keystroke for later analysis. They can be covertly installed then removed after an administrator has logged in so that the administrator password can be obtained. These devices can store in excess of 2,000,000 keystrokes for less than a one-off cost of $150! An example device is available from KeyGhost (http://www.keyghost.com).*
10. Is there a UPS (Uninterruptible Power Supply) protecting the power supply? If No, go to question 14			*Even small power glitches can be very disruptive to computers. All servers should be protected by a UPS.*
11. Supply make and model of the UPS.			
12. When was the last load test completed?			*A full load test of the UPS should be done regularly (e.g. monthly or quarterly)*

13. When was the battery last checked or tested?			*If the battery condition is sub-optimal then it will not be able to carry the load when the power fails. This often only becomes apparent when the power fails!*
14. Are backups done regularly? If No, go to question 19.			*Having good backups is crucial. Systems fail and if there are no good backups (or if the backups that do exist cannot be restored) then data will be lost.*
15. Record the backup hardware used.			*This is useful information in the event of a disaster (e.g. a fire in the computer room) so that appropriate hardware and software can be obtained to make restoration of the tapes (which were hopefully stored offsite!) possible.*
16. Record the backup software used.			
17. When last was a restore operation tested?			

18. Describe how the backup tapes are stored and handled.			*Backup tapes should be stored offsite in a secure location. They should be handled, transported and stored in a secure manner in accordance with the manufacturer's guidelines.*
19. Is the System Time synchronised to the company time server/s?			*It is important that all the machines and devices within a company use a standard time. Unsynchronised machines make event log consolidation very difficult and can mask suspicious patterns spread across multiple devices.*
20. Are there any environmental control systems in the computer room? If No, go to question 22.			*Lack of proper environmental control could affect the security and availability of the server. High temperature and/or humidity could cause system failures.*
21. Are there any automated alerting procedures to warn of environmental control system failure?			*Environmental controls systems do fail and if there is no alerting system then the failure might go unnoticed until a computer system is affected and fails.*

22. Are there any obvious risk factors in the area immediately surrounding the server that might affect its operation?			*Examples might include water pipes in the computer room or a power supply which is shared with a kettle etc.*
23. Does the machine have fault-tolerant disks?			*Examples include mirrored disks and RAID subsystems. Production servers should have fault-tolerant disks.*
24. Is an Emergency Rescue Disk (ERD) Available?			*An ERD can be useful when trying to recover a failed server.*
25. Is the ERD up-to-date (i.e. was it created or updated within the last month or since the last major system change?			*The ERD should be updated after every major system change (e.g. Service Pack install) and regularly in between such events. It is good practice to update it before doing any maintenance work as a precaution!*

26. Is the ERD kept in a secure location?			*The ERD contains sensitive information about the machine and the users so it should be restricted to authorised personnel.*

6.2 BIOS and start-up settings

An NT machine can be made reasonably secure when actually running the operating system but numerous opportunities for compromising an NT system exist when the operating system is not running (e.g. when booting before NT is running). Most of these opportunities require physical access to the machine to exploit so this further strengthens the argument for installing the machine in a physically secure environment. These controls serve to audit and reduce these risks.

BIOS settings will need to be checked at boot time. Warning – beware of changing any BIOS or system settings without fully understanding the consequences because an incorrect setting could render the machine inoperable!

Control	Response	Auditor's Comments	General Comments and Guidance Notes
27. Is the System Startup Menu List time Delay set to 0 Seconds?			*Use the Control Panel System applet then select Startup/Shutdown. A setting of 0 reduces the risk of interruption. See section 12.2 for a screenshot.*
28. Is the Automatically Reboot option in Control Panel | System | Startup/Shutdown enabled.			*This will automatically reboot the server if it crashes.*

29. If the machine BIOS supports it, is the boot order set to the hard disk only?			*Some machines enable booting from floppy disk or CD-Rom drives. These should be removed from the boot list if at all possible.*
30. If the BIOS supports it, is the floppy disk disabled?			*This prevents anyone working at the console loading files from or saving files to floppy disks.*
31. If the BIOS supports passwords, is there a power-on password set?			*Setting the power-on password does increase security but will prevent the machine from automatically rebooting after a failure (e.g. a power failure) so discretion is advised when setting this. Evaluate the environment the machine is housed in.*
32. If the BIOS supports it, is there a setup password allocated?			*Even if the power-on password is not set the setup (or administrator) password should be set to prevent unauthorised changes to the BIOS setup.*
33. If the BIOS supports it, are all unnecessary devices (e.g. serial ports, printer ports etc.) disabled		• • • •	*This is a continuation of the 'if it is not needed then disable it' approach. For example, a disabled serial port will prevent any attack through a re-directed serial port.*

34. Is there a manufacturer's maintenance or utility partition on the hard disk?			*These partitions are often bootable so could be used to launch an attack. Remove or disable them as appropriate.*
35. Try to boot the machine with a bootable floppy in the floppy drive. Does it boot normally?			*If no, try to establish why.*
36. Try to boot the machine with a bootable CD in the CD-Rom drive. Does it boot normally?			*If no, try to establish why.*

6.3 Server Operating System

This section will attempt to audit the security of the basic server Operating System and will draw heavily on checklists designed for Windows NT 4.0 Server but will have additional questions added for Windows NT 4.0 Server, Terminal Server Edition.

Control	Response	Auditor's Comments	General Comments and Guidance Notes
37. Base Operating System version			*Use Winver.exe to check. WinMSD can also be used to create a report.*
38. Are all partitions formatted as NTFS?			*Use Windows NT Disk Administrator to verify.*
39. Is the machine a PDC/BDC/ Member Server?			
40. Domain/Workgroup name.			

41. Record Service Pack version applied.			*Unless good reasons prevent it, service packs should be applied as soon as they are released. Use Winver.exe to check. Sample screenshots in section 12.3. WinMSD can also be used to create a report.*
42. Is this the latest applicable Service Pack? If Yes go to question 44. (please note that NT4TSE requires special Service Packs which are not the same as the NT4S versions).			*Unfortunately, the **Windows NT 4.0 Post-Service Pack 6a Security Rollup Package** is not suitable for use with Terminal Server, so the patches need to be individually installed. The latest version currently available is SP6 as available at* http://www.microsoft.com /ntserver/terminalserver /downloads/recommended /tsesp6/ *Other downloads for Terminal Server are available from the Microsoft Windows Update for Terminal Server site at* *http://www.microsoft.com /ntserver/terminalserver /downloads/default.asp*
43. List any special reasons why the latest Service Pack has not been applied.			

44. Have any Hotfixes been applied? If No, go to question 46. (Use Control Panel Add/Remove Programs to check).			*Not all Windows NT Server 4.0 Hotfixes are suitable for use on NT4TSE – please consult Microsoft article Q196334[6] 'How to Determine If a Hotfix Is Compatible with Terminal Server' for further information.*
45. List any applied Hotfixes.			*Microsoft does not test Hotfixes as thoroughly as Service Packs and recommends that they be applied only to fix or prevent specific problems.* *The list of installed Hotfixes can also be checked by running any one of them from the command line with the -L (or list) switch e.g. Q25787 –L.*
46. Has SysKey been enabled?			*This should be applied to encrypt the Accounts Database unless company policy dictates otherwise. It is a one-way process initiated (or checked) by running the command-line tool 'Syskey'. The 'Store Startup Key locally' option is usually sufficient to ensure an acceptable level of security.*

47. Is the Registry Size Limit setting appropriate for this system?			*A user profile will not load if the Registry Size Limit is exceeded but Microsoft recommend setting the RSL to only slightly exceed current requirements (Q189119[7], Q176083[8] and Q124594[9] discuss this further).*

6.4 Operating System – Additional Components

There are numerous additional components supplied and installed as part of Windows NT 4.0 and Windows NT 4.0 Terminal Server Edition which do not form part of the core Operating System but which could compromise overall system security if improperly configured. Examples include Internet Explorer, Outlook Express etc. These need to be identified and patched or removed as appropriate to ensure overall security is not compromised.

Control	Response	Auditor's Comments	General Comments and Guidance Notes
48. What version of Internet Explorer is installed? If this is the latest release version go to question 50.			*Latest Release version at time of writing is v5.5 SP2.*
49. List any reasons preventing the latest release of Internet Explorer being applied.			

Internet Explorer v5.5 and above contain numerous optional components each of which might be used to launch an attack against the machine. Check whether the components itemised in the controls below are installed using the Control Panel Add/Remove Applications applet and select Internet Explorer then click the Add/Remove button then select Add a Component. Installed components are highlighted. All components that are not used for any production purpose should be uninstalled.

Control	Is Component Installed?	Auditor's Comments	General Comments and Guidance Notes
50. Microsoft virtual machine.			
51. Internet Connection Wizard.			
52. Dynamic HTML Data Binding.			
53. Internet Explorer Browsing Enhancements.			
54. MSN Messenger Service.			
55. NetMeeting.			
56. Windows Media Player.			
57. Windows Media Player Codecs.			
58. Vector Graphics Rendering (VML).			
59. AOL ART Image Format Support.			
60. Macromedia Shockwave Player.			
61. Macromedia Flash Player.			
62. Web Folders.			
63. Visual Basic Scripting Support.			
64. Additional Web Fonts.			
65. Any components under Multi-Language Support.			
66. Outlook Express.			P*lease note that some applications, e.g. Outlook, require Outlook Express to function.*

6.5 Internet Explorer Security Settings

It is possible to configure the security settings of Internet Explorer and consequently consideration should be given to disabling any scripting features within Internet Explorer. Alternatively, the settings could be set to disabled or to prompt any time a script or applet tries to execute. Although this can be very frustrating for the user it should be considered as part of the strategy towards a highly secure machine.

If possible, consideration should be given to using the Microsoft Internet Explorer Administration Kit (also known as the IEAK and available

from http://www.microsoft.com/Windows/ieak/en/) to enforce the security setting for Internet Explorer for all users. Failure to do so allows each user to reconfigure most of these settings back to insecure levels and any new user profiles will inherit the insecure settings which Internet Explorer uses as a default.

These settings can be configured using the Control Panel Internet Settings applet under the Security Tab then adjusted using the Custom Level button. Components to check for the Internet Zone and any other zones used are listed below:

Control	Response	Auditor's Comments	General Comments and Guidance Notes
67. Download Signed ActiveX Controls.			
68. Download Unsigned ActiveX Controls.			
69. Initialise and script ActiveX controls not marked as safe.			
70. Run ActiveX controls and plugins.			
71. Script ActiveX controls marked safe for scripting.			

72. File Download.			
73. Font Download.			
74. Java Permissions.			
75. Access Data sources across domains.			
76. Don't prompt for client certificate selection when no certificate or only one certificate exists.			
77. Drag and drop or copy and paste files.			
78. Installation of desktop items.			
79. Launching programs and files in an IFRAME.			
80. Navigate sub-frames across different domains.			
81. Software channel permissions.			

82. Submit nonencrypted form data.			
83. Userdata persistence.			
84. Active Scripting.			
85. Allow paste operations via script.			
86. Scripting of Java applets.			
87. Is 'My Briefcase' available on the 'Default User' and 'All Users' Desktop?			*Remove My Briefcase from all profiles unless it is specifically required for production purposes. The NT Search Tool is useful for this.*
88. Is the 'Install Internet Information Server' icon available on any desktop?			*Remove this icon from all profiles if possible.*
89. Is the 'Inbox' icon available on any desktop?			*Remove this icon from all profiles if possible.*
90. Is Microsoft Music Control installed?			*Use the Add/Remove Program applet in Control Panel to uninstall this application unless there is a valid production purpose for it.*
91. Is Outlook Express installed? If No, please go to question 93.			

92. Is Outlook Express required on this machine for any production purpose?			P*lease note that some applications, e.g. Outlook, require Outlook Express to function*
93. Is Microsoft Wallet installed?			
94. Is VDOLive Player installed?			
95. Is Internet Information Server (IIS) installed on this machine? If No please go to question 287.			
96. Is IIS required on this machine for any production purpose?			
97. What version of IIS is installed?			
98. Are the latest Service Packs and Hotfixes for IIS installed?			

6.6 Option Pack Applications

This section is based on the section named 'Install Only Necessary Option Pack Applications' from Chris Young's Windows NT 4.0 Audit Checklist.[10]

The Windows Option Pack contains IIS and a number of additional applications and services which could compromise the security of the machine.

Use Add/Remove Programs in Control Panel to verify whether these components are installed. Investigate whether any are needed for any production function because best practice would recommend disabling or uninstalling those which are not required.

Check this list against the corporate security policy.

Control	Is Component Installed?	Auditor's Comments	General Comments and Guidance Notes
Windows Option Pack Components:			
99. Certificate Server.			
100. FrontPage 98 (or 2000 or later version) Server Extensions.			
101. Internet Connection Service for RAS.			
The following subcomponents under Internet Information Server (IIS):			
102. File Transfer Protocol (FTP) Server.			
103. Internet NNTP Service.			
104. Internet Service Manager (HTML).			
105. SMTP Service.			
106. World Wide Web Sample Site.			
107. Microsoft Index Server.			
108. Microsoft Message Queue.			
109. Microsoft Script Debugger.			
110. Microsoft Site Server Express 2.0 .			
The following subcomponents under Transaction Server:			
111. Transaction Server Development.			
112. Visual InterDev RAD Remote Deployment Support.			
113. Windows Scripting Host.			

6.7 Anti-Virus protection

Viruses pose a severe threat to all Windows systems today so a well-protected server should have anti-virus protection installed.

This section will audit the anti-virus protection installed on the NT4TSE server (if any):

Control	Audited Result	Auditor's Comments	General Comments and Guidance Notes
114. Is any anti-virus software installed? If no, go to control 119.			Use the Control Panel Add/Remove Programs applet to verify.
115. What product and version is installed?			Use the Control Panel Add/Remove Programs applet to verify.
116. What version is the scan engine?			
117. What version is the virus signature file?			
118. What is the date of the virus signature file?			

6.8 User Account Management

User accounts are used to control access to the server and all the resources on the server. Each user account is unique and has a unique SID (Security identifier) so that even if an account is renamed it retains the same SID.

Recommended practice is to create Groups which contain the User accounts then to manage access to resources at Group level wherever possible.

Each user account has a password associated with it, and these can be blank in a default installation so there are many changes that can be made to improve security.

Most of these settings are made using the User Manager (or User Manager for Domains) tool. There are a number of additional tools which can be useful when auditing and editing these settings. The Windows NT Resource Kits contain a number of very useful utilities and most of these may be downloaded from Microsoft.

Control	Response	Auditor's Comments	General Comments and Guidance Notes

119. Are strong passwords required?			*Obvious it may be, but strong passwords are more difficult to crack and the NT Resource Kit tool PassProp.exe allows the minimum length and complexity of the passwords to be set. Please consult company policy for minimum requirements.*
120. Is Lockout enabled on the Administrator account?			*PassProp.exe also allows the Administrator account to be locked out when too many incorrect password attempts are made (this does not affect interactive Administrator logins from the console).*
121. Is a maximum password age set?			*This is set in User Manager under Policies. Forcing password expiration is usually considered a good thing, but check company policy.*
122. Is Password Uniqueness set?			*Remembering old passwords is useful to prevent the user simply cycling through a small number of passwords when forced to change his/her password. Check company policy for number to record.*

123. Is a minimum password age set?			*Minimum password age is really only useful in conjunction with password uniqueness. It prevents the user from cycling through his small group of passwords to get back to his/her favourite one. Once again, check company policy.*
124. Is Account Lockout set?			*When enabled, Account Lockout will lock an account if too many incorrect login attempts are made in a preset time. Please consult the company policy for this setting and the sub-sections within it.*
125. Has the Administrator account been renamed to something less obvious?			*The Administrator account cannot be disabled, so good practice would be to rename the account to something less obvious and set a very long and difficult password for it – this password is then typically locked away in a secure place and only used in an emergency. A copy of the Administrator account is then usually used for normal day-to-day maintenance and this should also have a nondescript name and a good password. Check company policy.*

126. Has the Administrator account description been amended or deleted?			*The default description can be useful in identifying the new Administrator account name.*
127. Has a decoy Administrator account been set up?			*If the system has no Administrator account, this confirms to an attacker that the account has been renamed. Creating a decoy makes it more difficult for an attacker to verify which account he is attacking.*
128. Has the decoy Administrator account been disabled?			*Disabling the account prevents any potential login to the account. Check the Event Log frequently for login attempts to this account.*
129. Has the Guest account been disabled?			*The Guest account cannot be deleted, so it should be disabled.*
130. Has the Guest account been renamed to something less obvious?			*As the Guest account cannot be disabled, good practice would recommend renaming it as well as disabling it. This can be thought of as enhancing security through obscurity!*

131. List all members of the Administrators group.			*Every member of the Administrators group is a potentially severe security hole. The number of Administrator logins should be strictly controlled and these should only be created when absolutely necessary. Good practice would recommend that users authorised to do administrative tasks use a 'normal' user login for their normal logins then use the RUNAS or SU NT Resource Kit utilities to conduct Administrative tasks. Please check company policy.*

6.9 Registry Access

The Windows NT registry contains a vast amount of information, from device settings to application specific settings. Incorrect or inappropriate changes to the registry can cause system failure and/or system compromise while insufficiently tight permission settings could enable an unauthorised person to access sensitive data stored in the registry.

This section is based on information contained in the Microsoft TechNet NT Resource Kit[11]

It is possible to access the registry of a remote machine across the network but a registry edit can prevent this or limit which users can do this. Confirm whether this change has been made as follows.

Control	Response	Auditor's Comments	General Comments and Guidance Notes

132. Has the HKEY_LOCAL_MACHINE\ System\CurrentControlSet\Control\ SecurePipeServers\winreg entry been added?			*This entry allows access to the registry to be restricted.* *When a users connects over the network to the registry on a Windows NT computer, the Server Service on the target computer checks for the existence of the **winreg** key. If **winreg** is not present, the connection is allowed. If **winreg** exists, the **ACL** on **winreg** is checked for read or write access, either of which will allow the connection.*
133. List all users and groups which have access to the registry key in control 132.			*This should be limited to the administrators and any other trusted users on an as-needed basis.*

NT provides a method for securing the registry based on Access Control Lists. Use Regedt32.exe to manage the access control lists for the registry.

Control Registry HKEY	Audited Permissions match recommended permissions	Recommended Permissions	Auditor's Comments	General Comments and Guidance Notes

134. HKCR (all subkeys)		Everyone: Special (Query Value, Enumerate Subkeys, Notify, Read Control)		
135. HKLM\SOFTWARE		Everyone: Special (Query Value, Enumerate Subkeys, Notify, Read Control)		

136. HKEY_LOCAL_MACHINE\SOFTWARE\ MICROSOFT\RPC (and all subkeys) \WindowsNT\CurrentVersion\ \WindowsNT\CurrentVersion\AeDebug \WindowsNT\CurrentVersion\Compatibility \WindowsNT\CurrentVersion\Drivers \WindowsNT\CurrentVersion\Embedding \WindowsNT\CurrentVersion\Fonts \WindowsNT\CurrentVersion\FontSubstitutes \WindowsNT\CurrentVersion\FontDrivers \WindowsNT\CurrentVersion\FontMapper \WindowsNT\CurrentVersion\FontCache \WindowsNT\CurrentVersion\GRE_Initialize \WindowsNT\CurrentVersion\MCI \WindowsNT\CurrentVersion\MCI Extensions \WindowsNT\CurrentVersion\Port (all subkeys) \WindowsNT\CurrentVersion\Type1Installer \WindowsNT\CurrentVersion\ProfileList \WindowsNT\CurrentVersion\ Windows3.1MigrationStatus(all subkeys) \WindowsNT\CurrentVersion\WOW (all subkeys)		Modify Everyone: Special (Query Value, Enumerate Subkeys, Notify, Read Control)		
137. HKLM\SOFTWARE\MICROSOFT \WindowsNT\CurrentVersion\PerfLib		Remove Everyone: Read, Add Interactive: Read		
138. HKLM\SOFTWARE\Microsoft \Windows\CurrentVersion\Run		Modify Everyone: Special (Query Value, Enumerate Subkeys, Notify, Read Control)		

139. HKLM\SOFTWARE\Microsoft Windows\CurrentVersion\RunOnce		Modify Everyone: Special (Query Value, Enumerate Subkeys, Notify, Read Control)		
140. HKLM\Software\Microsoft \WindowsNT\CurrentVersion \Winlogon		Creator Owner: Full Control, Administrator: Full Control, System: Full Control, Everyone: Read		
141. HKLM\SYSTEM \CurrentControlSet \Control\LSA		Creator Owner: Full Control, Administrator: Full Control, System: Full Control, Everyone: Read		
142. HKLM\System \CurrentControlSet\Services\ LanManServer\Shares\UPS		Modify Everyone: Special (Query Value, Enumerate Subkeys, Notify, Read Control)		
143. HKEY_USERS\.default		Modify Everyone: Special (Query Value, Enumerate Subkeys, Notify, Read Control)		

6.10 Other Restrictions configured in the Registry

While checking the registry, check the following permissions as they control access to the devices, services and resources listed below.

Control Registry Key	Value Name & (Data Type)	Audited value matches recommended value	Recommended value	Auditor's Comments	General Comments and Guidance Notes
144. HKLM\SOFTWARE \Microsoft\WindowsNT \CurrentVersion \Winlogon	AutoAdminLogon (Binary)		0		*A 0 value disables Automatic Logon*
145. HKLM\SOFTWARE \Microsoft\WindowsNT \CurrentVersion \Winlogon	CachedLogonsCount (String)		0		*A 0 value disables Caching of Logon Credentials*
146. HKLM\SOFTWARE \Microsoft\WindowsNT \CurrentVersion \Winlogon	DontDisplay LastUserName (Binary)		1		*A 1 value will suppress the name of the last user to Log In*
147. HKLM\SOFTWARE \Microsoft\WindowsNT \CurrentVersion \Winlogon	LegalNoticeCaption (String)		See company policy		*This field should contain the message box caption portion of the legal notice shown before login*

148. HKLM\SOFTWARE \Microsoft\WindowsNT \CurrentVersion \Winlogon	LegalNoticeText (String)		See company policy		*This field should contain the message portion of the legal notice shown before login*
149. HKLM\SOFTWARE \Microsoft\WindowsNT \CurrentVersion \Winlogon	ShutdownWith outLogon (String)		0		*A 0 value disables Shut Down without Logging On*
150. HKLM\SYSTEM \CurrentControlSet \Control\Lsa	CrashOnAuditFail (DWORD)		0		*See company policy as this is a trade-off between security and availability. A 0 value disables Shutdown on Full Audit Log*
151. HKLM\SYSTEM \CurrentControlSet \Control\LSA	FullPrivilege Auditing (Binary)		1		*A 1 value enables auditing of Rights*
152. HKLM\System \CurrentControlSet \Control\LSA	LMCompatibility Level (DWORD)		See company policy (valid 0 - 5)		*LanManager Pass-word Hash Support (see Q147706[12])*

153. HKLM\SYSTEM \CurrentControlSet \Control\LSA	Notification Packages (Multi String)		Passfilt		*This enables strong password filtering*
154. HKLM\System \CurrentControlSet \Control\LSA	Restrict Anonymous (DWORD)		1		*A 1 value restricts Null Credentials Logon.*
155. HKLM\SYSTEM \CurrentControlSet \Control\LSA	SubmitControl (DWORD)		0		*A 0 value restricts the AT schedule service.*
156. HKLM\SYSTEM \CurrentControlSet \Control\SessionManager \MemoryManagement	ClearPageFile-AtShutdown (DWORD)		1		*A 1 value clears the Page File during shutdown.*
157. HKLM\SYSTEM \CurrentControlSet \Services\CDROM	Autorun (DWORD)		0		*A 0 value disables Autorun for CD-Rom drives.*

158. HKLM\System \CurrentControlSet \Services\EventLog \logname	RestrictGuest Access (DWORD)		1		*There is one of these keys for each log. A 1 value secures the associated Event Log from Guest account viewing.*

6.11 Event Logs

The Windows NT Event logs contain an astounding amount of information about the machine. There are three event logs, an Application Log, a System Log and a Security Log.

Good practice recommends that only authorised users be given access to these logs, and this is achieved by setting the NTFS ACL for the three log files (AppEvent.evt, SysEvent.evt and SecEvent.evt).

Use Explorer to navigate to C:\WTSRV\System32\config then check the security of these three files against the controls below.

Control Event Log File	Audited Permissions match recommended permissions	Recommended Permissions	Auditor's Comments	General Comments and Guidance Notes
159. AppEvent.EVT		Administrators – Full System – Special Access (RO)		*Access to these files should be restricted as per company policy.*
160. SysEvent.EVT		Administrators – Full System – Special Access (RO)		

161. SecEvent.EVT		Administrators – Full System – Special Access (RO)		

It is possible to set the size and overwrite attributes for the Event log files in NT Server and NT4TSE. The default setting is to overwrite events older than 7 days with a maximum log size of 512kB.

Best security practice recommends that the logs are not automatically overwritten, but this could cause loss of data and/or system crashes when the logs fill up. An approach which combines reasonable security with less chance of downtime is to allow the log files to be very big (e.g. big enough to hold 3 months of normal data) then to set the '*Overwrite Events as needed*' flag to allow them to be overwritten as needed. Settings of 10MB are usually sufficient to meet this requirement.

This does require that the logs are reviewed frequently and reviews should preferably be done daily, but at least weekly.

To audit the size limits and overwrite settings for the log files, open Event Viewer, click Log on the menu, then click Log Settings.

Control	Audited value	Recommended value	Auditor's Comments	General Comments and Guidance Notes
162. System Log Maximum size		10MB		*Check company policy. A reasonable starting point is 10MB, but this needs to be refined in line with company policy and actual usage.*
163. System Log – overwrite policy		As Needed		*Check company policy.*

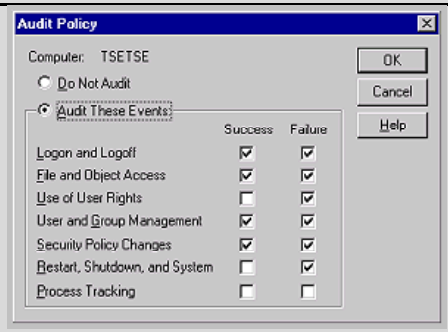
164. Security Log Maximum size		10MB		*Check company policy. A reasonable starting point is 10MB, but this needs to be refined in line with company policy and actual usage.*
165. Security Log – overwrite policy		As Needed		*Check company policy.*
166. Application Log Maximum size		10MB		*Check company policy. A reasonable starting point is 10MB, but this needs to be refined in line with company policy and actual usage.*
167. Application Log – overwrite policy		As Needed		*Check company policy.*

6.12 Security Logging

By default, security logging is not enabled on NT4TSE servers and has to be manually enabled. Auditing access and other failure events can often be more informative than auditing successful events because they will show unsuccessful login attempts and unsuccessful attempts to access the registry and event log files. Use the User Manager Policies menu to check the following.

Much of this section is based on the work of Sherri Heckendorn[13].

Control	Audited value	Recommended value	Auditor's Comments	General Comments and Guidance Notes

168. Is auditing enabled?		Enabled		*If auditing is not enabled here then no auditing will be allowed anywhere on the machine.*
169. Attach a screenshot				
170. Logon and Logoff – Success		Enabled		
171. Logon and Logoff – Failure		Enabled		
172. File and Object Access - Success		Disabled		*Enabling this can cause the logs to fill up very quickly.*
173. File and Object Access – Failure		Enabled		*This will alert when a user fails to open an object or file – too many of these could indicate a break-in attempt or password guessing.*
174. Use of User Rights – Success		Disabled		
175. Use of User Rights – Failure		Enabled		

176. User and Group Management – Success		Disabled		
177. User and Group Management - Failure		Enabled		*This will alert if a user attempts to change group membership or user rights etc.*
178. Security Policy Changes – Success		Enabled		
179. Security Policy Changes – Failure		Enabled		
180. Restart, Shutdown and System – Success		Enabled		
181. Restart, Shutdown and System – Failure		Enabled		
182. Process Tracking – Success		Disabled		
183. Process Tracking – Failure		Disabled		

6.13 Security Logging (File and Folder access)

Access to files and folders can be restricted on an NTFS volume using ACLs and this will prevent unauthorised access but to have these access attempts logged auditing has to be turned on for these objects. This requires that security logging has been enabled on the system (see the section on Security Logging on page 43).

Once again, it is important to selectively audit successful as well as failed access attempts as this information could prove very useful.

It is important to recognise that auditing these activities places a heavy processing load on the server so the actions and objects to audit should be carefully selected.

Use Explorer then select Properties then Auditing to audit these controls.

Folder or File	Audited Permissions	Recommended User Permissions	Auditor's Comments	Comments and Guidance Notes
184. C:\ directory and files		Everyone R		
185. C:\IO.SYS		N		
186. MSDOS.SYS		N		

187. BOOT.INI		N		
188. NTDETECT.COM		N		
189. NTLDR		N		
190. AUTOEXEC.BAT		N		

191. CONFIG.SYS		N		
192. C:\WTSRV files and folders (%systemroot%)		R		
193. C:\WTSRV \config		R		
194. C:\WTSRV \inf		R		
195. *.ADM		R		
196. *.PNF		R		

197. C:\TEMP		N		***Note: this may cause applications hard coded to use C:\TEMP as the temporary folder to fail but this problem should be increasingly rare as the environment variable %temp% is more frequently used.***
Each user who logs on to NT4TSE has a special directory created for them by the system as their Temp directory. This folder is created in C:\TEMP and has an alphanumeric name corresponding to the session number on the server (e.g. session number 6 will have C:\TEMP\6 created for them but the console session always uses the C:\Temp\0 folder). The %TEMP% variable for the user is then set to this folder. Allowing the users permissions to C:\TEMP would allow them to view and potentially to edit the files in the temp folders of other users. The temporary folders created for each remote logon (C:\TEMP\X) are deleted after logout, but the console temporary folder C:\TEMP\0 is not deleted – this could enable a user logging on to the console to see files created by previous console logon sessions including the Administrator. These files even survive a reboot. Restrict physical console logons to Administrators only, if possible. The command-line NT4TSE utility named FLATTEMP.EXE allows this default behaviour to be altered and all user temporary folders to be created at the same level. This is not recommended and the state of this should be checked by running FLATTEMP /query .				
198. C:\WTSRV \media		R		
199. *.RMI		C		
200. C:\WTSRV \profiles		(RWX)* (NotSpec)		
201. C:\WTSRV \Profiles \All Users		R		

202. C:\WTSRV \Profiles \Default User		R		
203. C:\WTSRV \Repair		N		
204. C:\WTSRV \System		R		
205. C:\WTSRV \System32		R		
206. C:\WTSRV \System32*.*		R		

207. C:\WTSRV \System32 \$winnt$.inf		R		
208. C:\WTSRV \System32 \Autoexec.nt		R		
209. C:\WTSRV \System32 \config.nt		R		
210. C:\WTSRV \System32 \cmos.ram		C		
211. C:\WTSRV \System32 \midimap.cfg		C		
212. C:\WTSRV \System32 \localmon.dll		R		
213. C:\WTSRV \System32 \decpsmon.*		R		
214. C:\WTSRV \System32 \hpmon.*		R		
215. C:\WTSRV \System32 \config\		L		
216. C:\WTSRV \System32 \drivers\		R		

217. C:\WTSRV \System32\ drivers\etc\		R		
218. C:\WTSRV \System32 \viewers\		R		
219. C:\...*.EXE, *.BAT, *.COM, *.CMD, *.DLL		X		

6.14 File and Folder Permissions

This section investigates the security of the crucial sections of the hard disk/s on the machine. This only applies if the partitions have been formatted with NTFS (see control 38.)

This section is based upon the work of Chris Young[10] but has been amended to reflect the disk and folder structure of a NT4TSE server.

It is assumed that only members of the 'Administrators' (A) group will do software installations and that all other authorised users will be members of the 'Users' (U) group. The 'System' user will need enhanced rights to the disk for system tasks – this user usually has full control to all disk drives.

Another assumption is that the server has only one disk (C:) – in the event that there is more than one disk mounted on the server, the files and folders listed below need to be checked against all disks as appropriate (e.g. all disks may have a Temp folder but only the drive on which the Operating System is installed should have a WTSRV folder.)

A further assumption is that the server is a stand-alone or member server and it is not a domain controller.

Abbreviations used:

C	Change
R	Read
W	Write
X	Execute
A	Add
N	None
L	List
F	Full Control

Folder or File	Audited Permissions	Recommended User Permissions	Auditor's Comments	Comments and Guidance Notes
220. C:\ directory and files		R		
221. Boot files				
222. IO.SYS		N		
223. MSDOS.SYS		N		
224. BOOT.INI		N		
225. NTDETECT.COM		N		
226. NTLDR		N		
227. AUTOEXEC.BAT		N		
228. CONFIG.SYS		N		
229. C:\TEMP		N		*Please see the full discussion of the implications of this in control 197.*

230. NETLOGON.CHG		N		*This file only exists on PDC or BDC machines (member servers and stand-alone servers do not have this file).*
231. C:\WTSRV\config		R		
232. C:\WTSRV files and folder (%systemroot%)		R		
233. C:\WTSRV\help		AR		
234. *.GID, *.FTG, *.FTS files		C		
235. C:\WTSRV\inf		R		
236. *.ADM		R		
237. *.PNF		R		
238. C:\WTSRV\media		R		
239. *.RMI		C		
240. C:\WTSRV\profiles		(RWX)* (NotSpec)		
241. C:\WTSRV\Profiles \All Users		R		
242. C:\WTSRV\Profiles \Default User		R		

243. C:\WTSRV\Repair		N		*This folder contains the SAM database and this could be used by an attacker to attempt to get the passwords and other security information.*
244. C:\WTSRV\System		R		
245. C:\WTSRV\System32		R		
246. C:\WTSRV \System32*.*		R		
247. C:\WTSRV \System32\ $winnt$.inf		R		
248. C:\WTSRV \System32\ Autoexec.nt		R		
249. C:\WTSRV \System32\ config.nt		R		
250. C:\WTSRV \System32\ cmos.ram		C		
251. C:\WTSRV \System32\ midimap.cfg		C		
252. C:\WTSRV \System32\ localmon.dll		R		

253. C:\WTSRV \System32\ decpsmon.*		R		
254. C:\WTSRV \System32\ hpmon.*		R		
255. C:\WTSRV \System32\config\		L		
256. C:\WTSRV \System32\drivers\		R		
257. C:\WTSRV \System32\ drivers\etc\		R		
258. C:\WTSRV \System32\viewers\		R		
259. C:\...*.EXE, *.BAT, *.COM, *.CMD, *.DLL		X		

6.15 User Rights Management

The default user rights allocated by the setup process need to be tweaked to improve security on any Windows NT machine. The User Rights are set using the 'User Manager' applet – click Policies then User Rights.

To view all the rights detailed below, please ensure that the 'Show Advanced User Rights' checkbox is selected. These advanced user rights are typically only used by programmers and when debugging applications and normally would not be allocated to any user or group on a production server. They do need to be audited, however, to ensure that they have not been set accidentally or by someone intent on compromising the system security.

Because complexity can allow configuration errors to be masked, and because common practice recognises only two levels of user (Administrator and all others), the other higher-level groups (backup operators, power users etc.) are not often used. Consult company policy

when auditing user rights if these groups are used in the company environment.

Best practice recommends that these rights are allocated on a group basis and are limited to the minimum required for each group. This section is based upon the work of Chris Young.[10]

Control (User Right)	Response (List groups and users granted this right)	Auditor's Comments	General Comments and Guidance Notes
260. Access this computer from Network			*Remove this right from all users and groups for optimum security but arguments exist for allowing the Administrators group to access the machine remotely. Check company policy.*
261. Act as part of the Operating System			*This right should never normally be granted to any user or group.*
262. Add workstations to domain			*This is not applicable on a member server but on a domain controller should be limited to domain administrators.*
263. Back up files and directories			*Trusted users (e.g. the Administrators and Backup Operators groups).*
264. Bypass traverse checking			*Best practice recommends that only Authenticated Users be allocated this right.*

265. Change the system time			*Usually allocated to Administrators only.*
266. Create a pagefile			*Usually allocated to Administrators only.*
267. Create a token object			*Not usually allocated to any user or group.*
268. Create permanent shared objects			*Not usually allocated to any user or group.*
269. Debug Programs			*No one should be allocated this right as it is not auditable.*
270. Force shutdown from a remote system			*Usually allocated to Administrators only.*
271. Generate security audits			*No one should be allocated this right.*
272. Increase quotas			*Usually allocated to Administrators only.*
273. Increase scheduling priority			*Usually allocated to Administrators only.*
274. Load and unload device drivers			*Usually allocated to Administrators only.*

275. Lock pages in memory			*No one should be allocated this right.*
276. Log on as a batch job			*Usually allocated to Administrators only and then only when required.*
277. Log on as a service			*Usually allocated to Administrators only and then only when required.*
278. Log on locally			*This is required for all Authenticated Users on a NT4TSE server because logically the users are logging in locally. This is a distinct change from the normal NT Server setting.*
279. Manage auditing and security log			*Usually allocated to Administrators only.*
280. Modify firmware environment values			*Usually allocated to Administrators only.*
281. Profile single process			*Usually allocated to Administrators only.*
282. Profile system performance			*Usually allocated to Administrators only.*
283. Replace a process level token			*No one should be allocated this right.*

284. Restore files and directories			*Usually allocated to Administrators only.*
285. Shut down the system			*Usually allocated to Administrators only.*
286. Take ownership of files or other objects			*Usually allocated to Administrators only.*

6.16 Server Operating System (Services)

The Microsoft setup procedures used to build servers typically installs services to cover the widest possible range of uses for the server. Almost every server will have one or more services installed by the setup utility which is not required in the production configuration. Best practice recommends removing or disabling these services.

Other services (e.g. EventLog) are required to help ensure the highest level of security is maintained.

The services actually required will depend on the configuration of the server. Consult the corporate security policy, if available, to help determine which services are required and which are unused.

In addition, there are some services which are not included in the standard build which can be added to improve security. Consideration should be given to installing these services.

An added advantage of disabling unused services is better server performance!

Use the Control Panel Services applet to audit the following controls (the NT Resource Kit utility named SCList.exe can be used to produce a list

of installed services and their states):

Service Name	Audited State (circle as appropriate)	Recommended Setting	Auditor's comments	General Comments and Guidance Notes
287. Is the FLOPLOCK service installed, running and set to automatically start?		Automatic Started		*FlopLock.exe is an additional component available in the Microsoft NT Server Resource Kit. It runs as a service and restricts floppy disk access to the Administrators group on NT Server by hiding the drive/s from all other users. See Q185704*[14]
288. Alerter		Disabled Stopped		*This service is not required in most configurations and may usually be disabled.*
289. Com+ Event System		Disabled Stopped		*This service is usually not required and may be disabled in most configurations.*
290. Computer Browser		Disabled Stopped		*This service is usually not required and may be disabled in most configurations.*
291. DHCP Client		Disabled Stopped		*This service is usually not required and may be disabled unless the server uses DHCP.*
292. Directory Replicator		Disabled Stopped		*This service is usually not required and may be disabled in most configurations.*

293. EventLog		Automatic Started		*The EventLog service is used to maintain the event logs which record security and auditing information.*
294. License Logging Service		Disabled Stopped		*This service is generally required only to manage software licensing and can be disabled if other methods are used to prevent copyright and license infringements.*
295. Messenger		Disabled Stopped		*This service is not required by most installations.*
296. Net Logon		This will depend on Server role (PDC, BDC or member server)		*This service is used to authenticate logons to a domain and to publish the Netlogon share – it is not needed for most installations unless the server needs to process logons.*
297. Network DDE DSDM		Disabled Stopped		*This service is not required by most installations.*
298. NTLM Security Support Provider		Automatic Started		*This is an essential service and should not be disabled.*
299. Plug and Play		Disabled Stopped		*This service is recommended but not required by Microsoft in their TechNet[15] article.*
300. Protected Storage		Automatic Started		*This is an essential service and should not be disabled.*
301. Remote Procedure Call (RPC) Locator		Disabled Stopped		*This service is only required if remote administration is required and may be disabled in some configurations.*

302. Remote Procedure Call (RPC) Service		Automatic Started		*This is an essential service and should not be disabled.*
303. SAP Agent		Disabled Stopped		*This service is only required if IPX networking is used so may be disabled in TCP/IP only configurations.*
304. Server Service		Automatic Started		*This service can be stopped but it is required to run User Manager so is usually left running.*
305. Spooler Service		Automatic Started		*This service can be stopped but it is required for printing so is usually left running.*
306. Task Scheduler		Disabled Stopped		*This service is only required if Task Scheduling is required on the server so may be disabled in most configurations.*
307. TCP/IP NetBios Helper		Disabled Stopped		*This service is usually not required and may be disabled in most configurations.*
308. Telephony Service		Disabled Stopped		*This service is usually not required and may be disabled unless dial-up communications is used.*
309. Terminal Server		Automatic Started		*This service is essential for Terminal Server to run!*
310. Terminal Server Licensing		Disabled Stopped		*This service is generally required only to manage Terminal Server software licensing and can be disabled if other methods are used to prevent copyright and license infringements.*

311. UPS		Automatic Started		*This service is essential if a UPS is attached and properly configured.*
312. Workstation		Automatic Started		*This service not essential but is best left enabled to enable the machine to access the network.*

6.17 Server Operating System (Network Protocols)

The Microsoft setup procedures used to build servers typically installs network protocols to cover the widest possible range of uses for the server. If TCP/IP is the only protocol needed then the others should be removed.

The services actually required will depend on the configuration of the network. Consult the corporate security and network configuration policies, if available, to help determine which protocols are required and which are unused.

An added advantage of disabling unused protocols is better network performance!

Use the Network applet in Control Panel to audit the following controls:

Control	Audited Value	Recommended Setting	Auditor's Comments	General Comments
313. Record the Computer Name alongside				*This should be a unique name on the network. Check that it adheres to the corporate naming convention, if applicable.*
314. Record the Workgroup or Domain name alongside.				*Verify that this is appropriate for the organisation and location of this server.*

315. NWLink IPX/SPX Compatible Transport		Not Installed		*These protocol is not required in a TCP/IP-only network*
316. NWLink NetBIOS		Not Installed		
317. TCP/IP Protocol		Installed		
318. IP address is static or DHCP-assigned		Static		*Static IP addresses are recommended for servers.*
319. Record the IP address details		IP Address Subnet Mask Gateway		*Please enter the IP address, Subnet mask and Default Gateway address alongside.*
320. Record the Host Name alongside				
321. Record the Domain alongside				
322. Record the DNS Server addresses alongside				*Verify that these DNS Server addresses are appropriate for the organisation and location of this server.*
323. Record the entries in the Domain Suffix Search Order field alongside				
324. Record the address of the Primary and secondary WINS servers alongside				*Verify that these DNS Server addresses are appropriate for the organisation and location of this server.*
325. Record the state of the Enable DNS for Windows Resolution checkbox		Enabled		*This allows the server to use DNS to resolve WINS queries.*

326. Record the state of the Enable LMHOSTS Lookup checkbox		Disabled		*This allows the server to use the LMHOSTS file to resolve name queries.*
327. Record the Scope ID (if present)				*This is usually left blank – verify that this is appropriate for the organisation and network.*
328. Record the Seconds Threshold value alongside		Default is 4		*These are normally left at default and are only applicable if the DHCP Relay service is installed and running.*
329. Record the Maximum Hops value alongside		Default is 4		
330. Enter the names of the DHCP servers entered alongside				
331. Record the state of the Enable IP Forwarding checkbox		Disabled		*This allows or disallows the server from acting as a router but is only applicable in a multi-homed system (one with more than one NIC). It should normally be disabled.*

6.18 Server Operating System (Network Services)

As with network protocols, the setup routine installs numerous network services, many of which are not usually needed. Audit these and disable any unnecessary ones as for protocols.

Use the Services tab for the controls in this section:

Control	Audited Value	Recommended Setting	Auditor's Comments	General Comments
332. Computer Browser		Installed		*This is required by the workstation service.*
333. NetBIOS interface		Not Installed		*This is not required in a TCP/IP-only network and can normally be removed.*
334. RPC Configuration		Not Installed		*This is required by applications written to utilise Remote Procedure Calls – check company policy and remove if unnecessary.*
335. SAP Agent		Not Installed		*This is not required in a TCP/IP-only network and can normally be removed.*
336. Server		Installed		*This is required to run the server and should not normally be removed.*
337. Workstation		Installed		*This is required by the workstation function and should not normally be removed.*
338. Record the details of the network adapter			Screenshot attached in section 12.8	*Repeat this for each adapter.*
339. Record the information listed for each network adapter. TCP/IP is most likely the only protocol				*TCP/IP is usually the only protocol and the WINS client has the workstation and server service bound to it normally. Repeat this for each adapter.*

Record the IPCONFIG information.

Control	Audited Value	Auditor's Comments	General Comments and Guidance Notes
340. IPCONFIG report created?			Use a Command Window (DOS box) to run IPCONFIG /ALL then print this or save to a file and attach to report.

6.19 Hide potentially dangerous files

NT comes complete with a number of files which are useful administrator tools but which could be used by an attacker to gather knowledge about the system. These files are usually installed in publicly accessible folders and can usually be run by any user from any current directory location because the folders are usually included in the search path.

While it is possible for a determined attacker to provide his or her own copies of these files, best practice recommends moving these files to an alternate location which is only accessible to Administrators and adding this folder to the path of the administrator group only. This folder can then be added to the path so that authorised users can access and run these files.

NT4TSE includes a tool named Appsec.exe which can also be used to control access to applications not authorised. This will be covered in a later section.

The files listed below should be moved from their default locations to a common secure location (e.g. C:\WTSRV\System32\UserUtils) and auditing should be configured to record access to these files.

Please note that these changes can cause some applications (especially 16-bit applications) to cease functioning properly so all these changes should be tested on a non-production server before being applied to a production server machine.

The NT Find utility can be used for this, and the list below can be copied into the find tool then the results sorted by folder – this will allow any discrepancies to be quickly spotted.

APPSEC.* ; ARP.EXE ; AT.EXE ; ATSVC.EXE ; CACLS.EXE ; CMD.EXE ; COMMAND.COM ; CSCRIPT.EXE ; DEBUG.EXE ; EDIT.EXE ; EDLIN.EXE ; FINGER.EXE ; FTP.EXE ; IPCONFIG.EXE ; ISSYNC.EXE ; NBTSTAT.EXE ; NET.EXE ; NETSH.EXE ; NETSTAT.EXE ; NSLOOKUP.EXE ; PING.EXE ; POLEDIT.EXE ; POSIX.EXE ; QBASIC.EXE ; RCP.EXE ; RDISK.EXE ; REGEDIT.EXE ; REGEDT32.EXE ; REGINI.EXE ; REGSRV32.EXE ; REXEC.EXE ; ROUTE.EXE ; RSH.EXE ; RUNAS.EXE ; RUNONCE.EXE ; SECFIXUP.EXE ; SYSKEY.EXE ; TELNET.EXE ; TFTP.EXE ; TRACERT.EXE ; TSKILL.EXE ; WSCRIPT.EXE ; XCOPY.EXE

Figure 2 File list for pasting into the NT Find tool

This section is based upon the work of Chris Young[10] but has been amended to reflect the differences between NT4TSE and NT Server 4.0.

Control (File Name)	Audited Location/s	Comments and Guidance Notes
341. APPSEC.EXE (and .*)		*This file and associated files (appsec.*) are used on NT4TSE to control which applications can be run by users. It can only be run by administrators, but hiding it is recommended anyway. See the dedicated APPSEC section on page 79 for more information.*
342. ARP.EXE		*Displays and modifies the IP-to-Physical address translation tables used by address resolution protocol (ARP).*
343. AT.EXE		*The AT command schedules commands and programs to run on a computer at a specified time and date. The Schedule service must be running to use the AT command.*
344. ATSVC.EXE		*This is the executable which runs as the AT service.*
345. CACLS.EXE		*Displays or modifies access control lists (ACLs) of files.*
346. CMD.EXE		*Starts a new instance of the Windows 2000 command interpreter.*
347. COMMAND.COM		*Starts a new instance of the MS-DOS command interpreter.*
348. CSCRIPT.EXE		*Windows Script Host.*
349. DEBUG.EXE		*A program testing and editing tool.*
350. EDIT.EXE		*MS-DOS Editor.*
351. EDLIN.EXE		*A line-oriented text editor.*
352. FINGER.EXE		*This connectivity command displays information about a user on a specified host running the Finger service.*

353. FTP.EXE		*This connectivity command transfers files to and from a host running an FTP server service. Passwords are normally sent unencrypted.*
354. IPCONFIG.EXE		*This diagnostic command displays all current TCP/IP network configuration values.*
355. ISSYNC.EXE		*This is a Site Server/SQL Server file and may not be present on all servers.*
356. NBTSTAT.EXE		*Displays protocol statistics and current TCP/IP connections using NBT (NetBIOS over TCP/IP).*
357. NET.EXE		*This tool allows viewing and/or editing the current network configuration. (e.g. NET VIEW).*
358. NETSH.EXE		*A utility to configure interfaces, routing protocols, filters, routes, and remote access behaviour.*
359. NETSTAT.EXE		*Displays protocol statistics and current TCP/IP network connections.*
360. NSLOOKUP.EXE		*A utility to resolve DNS queries.*
361. PING.EXE		*A utility to check connectivity on a TCP/IP network.*
362. POLEDIT.EXE		*The graphical Policy Editor.*
363. POSIX.EXE		*The POSIX subsystem file.*
364. QBASIC.EXE		*The Quick Basic editor and compiler.*
365. RCP.EXE		*Copies files to and from computer running the RCP service.*
366. RDISK.EXE		*The utility used to create the Emergency Recovery Disk (ERD).*
367. REGEDIT.EXE		*A Registry editor.*
368. REGEDT32.EXE		*A Registry editor which allows setting security on registry keys.*
369. REGINI.EXE		*Adds, removes, or changes keys based on a command script.*
370. REGSRV32.EXE		*You can use the Regsvr32 tool (Regsvr32.exe) to register and unregister object linking and embedding (OLE) controls such as dynamic-link library (DLL) or ActiveX Controls (OCX) files that are self-registerable.*
371. REXEC.EXE		*Runs commands on remote hosts running the REXEC service.*
372. ROUTE.EXE		*Manipulates network routing tables.*
373. RSH.EXE		*Runs commands on remote hosts running the RSH service.*
374. RUNAS.EXE		*Allows a user to run a program as another user.*

375. RUNONCE.EXE		*This file is not always included on NT4TSE – it is used to configure a task to run once at startup.*
376. SECFIXUP.EXE		*This is an IIS file used to configure security.*
377. SYSKEY.EXE		*Enables encrypting the accounts database.*
378. TELNET.EXE		*Telnet allows running remote interactive command shells. Passwords are sent in clear text!*
379. TFTP.EXE		*Transfers files to and from a remote computer running the TFTP service*
380. TRACERT.EXE		*A utility used to trace the route between two machines.*
381. TSKILL.EXE		*A utility to kill processes.*
382. WSCRIPT.EXE		*A scripting host.*
383. XCOPY.EXE		*Extended file copy utility.*

The folder used for these utilities (C:\WTSRV\System32\UserUtils is recommended) needs to be protected and audited. Check these settings in the following section.

Control	Audited Response	Comments and Guidance Notes
384. Is auditing set for UserUtils folder?	Yes / No	*The recommended setting is to audit on file access failure – this will provide a record of attempted unauthorised access to the utilities.*
385. Is the UserUtils folder set to deny access to all but administrators?	Yes / No	
386. Record any files not included in the list above which have been added to the UserUtils folder.		

6.20 C2 Security Compliance and C2Config

The Windows NT Resource Kit contains a utility named C2Config, which can assist in configuring a machine to be C2 compliant[16]. While a computer configured to be C2 compliant is secure, it is not always very useful (one of the conditions for C2 security is that the machine has no network interface!) so this standard will only be used as a guide and only some of the settings will be necessary on a production server.

The C2Config utility will report the status of the controls as follows:

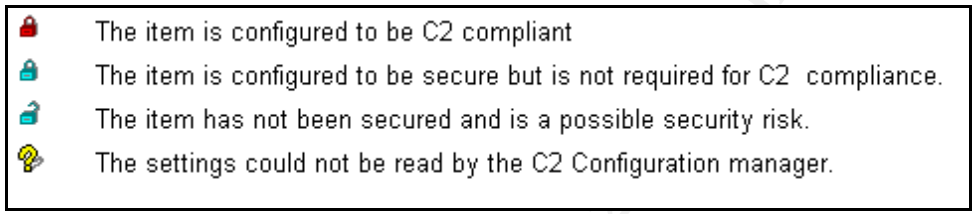


Figure 3 Screenshot from C2Config.HLP

A screenshot of a default NT4TSE server configuration is available in section 12.11.

Run C2CONFIG.EXE to audit controls 387 to 403:

Control	Audited Value	Recommended Setting	Auditor's Comments	General Comments
387. File Systems		C2 Compliant		
388. OS Configuration		C2 Compliant		*It is not possible to set this to be secure until the OS/2 and POSIX subsystems are removed.*
389. OS/2 Subsystem		C2 Compliant		*Uninstall the OS/2 subsystem unless there is a valid reason to keep it.*

390. POSIX Subsystem		C2 Compliant		*Uninstall the POSIX subsystem unless there is a valid reason to keep it.*
391. Security Log		Policy dependent		*The C2 requirement is for the Security Log to be manually cleared and this is the ideal setting but practical considerations usually require that the log is automatically overwritten. Ensure that the log is large enough to prevent valuable data being overwritten.*
392. Halt on Audit Failure		Policy dependent		*The C2 requirement will stop the system if the Security Log reaches full capacity. This is the most secure setting but can reduce reliability because the system will stop if the log is not cleared frequently enough. The ideal setting for this control and for control 391 will depend on company policy.*
393. Display Logon Message		Policy dependent		*This is not a C2 requirement, but is good policy as it provides some measure of legal protection in the event of unauthorised use.*

394. Last Username Display		Policy dependent		*This is not a C2 requirement, but is good policy as it provides some measure of obscurity to prevent unauthorised use.*
395. Shutdown button		Policy dependent		*This is not a C2 requirement, but is good policy as it provides some measure of legal protection in the event of unauthorised use.*
396. Password Length		Policy dependent		*C2 compliance requires non-blank passwords and good practice recommends password length be at least 8 characters but this minimum length is not required for C2 compliance.*
397. Guest Account		Secure		*It is strongly recommended that the Guest account be disabled and, if possible, renamed.*
398. Networking		Not Secure		*This C2 requirement will, if implemented, render the NT4TSE server useless!*
399. Drive Letters and Printers		Policy dependent		*This is not a C2 requirement, but is good policy as it provides enhanced protection.*

400. Removable Media Drives		Policy dependent		*This is not a C2 requirement, but is good policy as it provides enhanced protection.*
401. Registry Security		Secure		*This C2 requirement controls the permissions required to access the registry. Please see Q221766[17] for an essential edit to C2regacl.inf prior to applying.*
402. File System Security		Secure		*This C2 requirement sets the file and directory permissions to the system directories by setting the ACL lists according to the settings contained in C2NTFACL.INF.*
403. Other Security Items				*This is a reminder or help item only and these items are checked elsewhere.*

6.21 APPSEC

APPSEC.exe is a NT4TSE tool which allows the administrator to restrict access to a defined list of executables. Once security is enabled with AccSec, non-administrators will not be able to run applications not listed in the AppSec list. See section 12.11 for a sample AppSec screenshot.

Control	Audited Value	Recommended Setting	Auditor's Comments	General Comments
404. Is security in AppSec enabled? If No, go to control 406		Yes		*Please note that enabling security in AppSec will prevent users from running any applications not specifically listed in AppSec. This can cause problems with certain applications installed by default in NT4TSE – please see Q230338[18], Q186609[19] and Q186500[20] for more information.*
405. List all applications enabled in AppSec		As per company policy.		*Only applications with essential production business purposes should be enabled under AppSec because each application which users are able to run is one more potential vulnerability which may be utilised to attack the system.*

6.22 Policies in NT4TSE

Policies can be used to enforce controls upon the users of the computer and help to control unauthorised access to applications and resources but, as the quotation below indicates, policies can create numerous problems if incorrectly applied.

'*Policies can be implemented in a Microsoft Windows NT Server 4.0, Terminal Server Edition environment to control and limit the access that each user has while connected to a Terminal Server session. When implementing policies in a Terminal Server environment, additional planning and consideration is necessary to accommodate the multiuser environment presented by Terminal Server.*' Microsoft Corporation, Implementing Policies in Terminal Server[21]

The Microsoft White Paper, *Implementing Policies in a Terminal Server Environment* (IMPLPOL.DOC[22]) discusses the application of policies on Terminal Server and anybody tasked with securing NT4TSE machines would be well advised to study this document.

Unlike the policies in NT4 which have to be applied slightly differently depending on the client machine (NT or Windows 9X), the policies in NT4TSE can be applied to NT4TSE sessions only and thus can be client-independent so user sessions from any type of client machine will be affected by the policy.

When implemented in a domain environment the policy files should be saved to the Netlogon share of the domain controllers but in the member server environment these must be saved to a special directory on each server.

Use the tools indicated within each control below to audit whether policies have been enabled for users and sessions on this server (this is for member servers or stand-alone servers and will need to be modified for a Windows domain environment):

Control	Audited Value	Recommended Setting	Auditor's Comments	General Comments

406. Use Regedit to check the value of the HKLM\SYSTEM \CurrentControlSet \Control\Update \NetworkPath registry key. Does it exist? If yes, note the path stored in the value, if No then continue at control 411		Yes		*If the key exists and the value is valid and the UpdateMode value is set to 2 and the permissions for the folder are set so that the user can read the NTConfig.pol file in the folder then the policy will be applied to the user – if applicable to the user.* *Alternatively, the policy will be applied if it exists in the User Profile directory but this is not recommended!*
407. What is the value of the HKLM\SYSTEM \CurrentControlSet \Control\Update \UpdateMode		2		*This determines where the NTConfig.pol file is stored.* *This behaviour is controlled by using the System Policy Editor and opening the registry for the NT4TSE server. It is then changed by editing the value as shown in section 12.13.*
408. Does the folder referred to in HKLM\SYSTEM \CurrentControlSet \Control\Update \NetworkPath exist?		Yes		

409. Does NTConfig.Pol exist in the folder referred to in HKLM\SYSTEM \CurrentControlSet \Control\Update \NetworkPath?		Yes		
410. Does everyone have read access to the folder referred to in HKLM\SYSTEM \CurrentControlSet \Control\Update \NetworkPath?		Yes		
411. Search the system for NTCONFIG.POL files using the NT find files utility. If any are found, record the locations of the files alongside.		These should only exist in the folder referenced in control 406.		

6.23 Zero Administration Kit for Terminal Server

Microsoft have released a Zero Administration kit for Terminal Server which will help reduce support calls and increase security by reducing the user access to system files and utilities. It is highly recommended that consideration be given to applying this kit to the NT4TSE machine if this is appropriate for the organisation.

According to Microsoft, '*The ZAK for Terminal Server applies security ACLs to the local file system and hides most of the local file system. This minimizes user access to parts of the operating system outside the scope of their line of business applications. The ZAK for Terminal Server also includes several policy templates for applying Windows NT policies to manage (lock down) the user's permissions on the desktop.*' Microsoft Corporation, Zero Administration Kit for Terminal Server[23]

The white paper covering the ZAK can be downloaded from http://www.microsoft.com/ntserver/zipdocs/zakfortswp.exe and the actual kit is available from http://www.microsoft.com/ntserver/downloads/bin/nts/ZAK4WTS2.EXE.

The ZAK should only be run when all applications have been installed and a member of the administrators group should run it. When run, the ZAK will create a folder named ZAK under C:\WTSRV. More details can be found in the white paper[24].

The following control checks whether the ZAK has been run:

Control	Audited Value	Recommended Setting	Auditor's Comments	General Comments
412. Does the C:\WTSRV\ZAK folder exist?		Yes		

7. AutoLogon and RDP Security

NT4TSE allows clients to connect to remote desktop sessions using Remote Desktop Protocol (RDP). By default, when the client connects to the NT4TSE session a valid username and password pair will be required. This feature makes it easy for users to use NT4TSE sessions, but does open up a potential security vulnerability.

When AutoLogon is enabled in NT4TSE, all sessions established through the connection type (e.g. RDP-TCP) will be logged-on with the same credentials as specified in the Terminal Server Connection Configuration utility as shown in section 12.14. If the client machine is insecure or compromised then the possibility exists that the person using the remote machine will be able to logon to the NT4TSE server using the default connection without any credential checking.

Because of the security problems this can cause, it is strongly advised that AutoLogon should not be used. If it is used, then the Initial Program should be set to prevent user sessions presenting a virtual desktop. When the Initial Program option is used the application will run immediately the user session is established and will log the user off when the application is closed.

Control	Audited Value	Recommended Setting	Auditor's Comments	General Comments
413. Is AutoLogon enabled?		No		Use the Terminal Server Connection Utility to confirm whether AutoLogon is enabled as shown in section 12.14
414. What security level is set for remote sessions?		High		Ideally this should be high but this is dependent on company policy and hardware and network configuration.

415. Is the 'Use default Windows NT Authentication' checkbox selected?		Checked		It is possible to install third-party authentication tools on NT by installing DLLs. This checkbox will force the logons to be authenticated using the standard msgina.dll even if a replacement DLL has been loaded..

8. Audit Evaluation

Because there are so many factors that affect the security of a NT4TSE machine, it is difficult for anyone to state that a machine is secure.

Many system administrators, when confronted by the sheer number of potential vulnerabilities and the wide range of techniques that could be used to attack a NT4TSE or NT Server machine, seem to be overwhelmed and do not know where to start. This checklist was designed to help these administrators evaluate their servers against the best practice guidelines using an easy step-by-step approach.

Unfortunately, this checklist and the techniques suggested in this document cannot guarantee a secure machine, but if all the controls are checked and any shortfalls are rectified it should ensure that the resultant configuration is more secure than the default 'out-of-the-box' configuration.

Areas that are very difficult (or impossible) to audit would include, amongst others, the threats posed by social engineering, administrator error or an administrator 'going rogue'. In addition, it is almost impossible to audit and verify whether there are any 'back-doors' into the system left (or purposely inserted) by the operating system developer.

Formal, well-documented procedures should help contain the risk posed by these difficult-to-measure threats and should help any abnormal activity to be spotted in the logs etc. – if these have been configured correctly and they are reviewed regularly!

9. Suggested Improvements and Future Enhancements

This audit checklist is dynamic and should be subject to continuous review and improvement.

The hackers and other attackers are continually developing new tools and techniques to use against systems and in addition Microsoft and other developers are continually developing and releasing patches to thwart these threats so the checklist needs to be continually updated to remain effective.

Auditing the 415 controls contained in this checklist proved to be extremely time-consuming and with such a large number of checks it is very easy to overlook something. It would be a great help if a tool existed that could be scripted to run through the controls in the checklist and generate a report automatically but creating this would be extremely time consuming and might, in itself, lead to complacency.

Doing the audit manually tends to increase awareness of the vulnerabilities uncovered and should help the auditor and the system administrators to understand the systems better. It also encourages them to think about 'the big picture' and consider things that they might not have considered before. For example, no automated system would be able to audit the physical security of the server and the auditors and system administrators might not have considered this before.

Possibly the most important development work that needs to be done on this checklist is to add support for Domain Controllers, Citrix and Windows 2000 Terminal Server.

10. Conclusions

Unfortunately most systems administrators build NT systems, consult the Microsoft Update site to install any Service Packs or hotfixes recommended by Microsoft and then assume the machine is stable and secure without confirming that the patches and fixes are appropriate for their particular environment or that they have been applied correctly.

These systems are then presumed to be secure and are not updated, patched or audited until the Microsoft Update reminder causes the administrator to review the settings. The vast majority of systems are never audited at all, and certainly do not have the security audited.

Hopefully the checklist and methodologies included in this document will provide a means to improve the security of these machines.

11. Appendix 1. Resources used to generate checklist.

Ref.	Document Title	Author	Source
1.	Sherri_Heckendorn.doc	Sherri Heckendorn	http://www.sans.org /y2k/practical /Sherri_Heckendorn.doc
2.	Windows NT 4.0 Audit Checklist	Chris Young	http://www.sans.org /infosecFAQ/audit/NT40.htm
3.	The Hardening of Microsoft Windows NT Operating System Version 4.0	Michael Espinola Jr.	http://www.networkcommand.com /docs/HardNT40rel1.pdf
4.	Windows NT Security Audit Program	Manuel Pimentel	http://www.auditnet.org /docs/winnt.pdf
5.	Windows NT General Application Audit	Nafiza Mohamed	http://www.auditnet.org /docs/WinNTAuditProgram.pdf
6.	Windows NT Server Checklist	Peter Davis and Associates	http://www.pdaconsulting.com /winnts.htm
7.	Windows NT Checklist		http://www.geocities.com /SiliconValley/Lab/7378/ntcheck.htm
8.	Microsoft Windows NT Security Checklist	University of Cambridge Computing Service Technical User Services	http://www-tus.csx.cam.ac.uk /pc_support/WinNT/ntsecchk.html
9.	Windows NT Configuration Guidelines	CERT® Coordination Center	http://www.cert.org/tech_tips /win_configuration_guidelines.html
10.	Sample Security Configuration	Microsoft TechNet	Microsoft TechNet July 2001 - Deploying MS Windows NT Server 4.0 Terminal Server Edition and TSDEPLOY.EXE which contains numerous Word DOC files including *Sample Security Configuration.doc* (Also available at http://www.microsoft.com /TechNet/prodtechnol /termsrv/deploy/tsdepsg.asp But the link to tsdeploy.exe is broken!)
11.	Citrix Systems' Metaframe Offers Enhanced Functionality fo (sic) MS Windows Terminal Server	Mack RiCharde	http://www.sans.org/infosecFAQ /win/metaframe.htm

12. Appendix 2. Audit Screenshots and supporting evidence

12.1 WinMSD screenshot

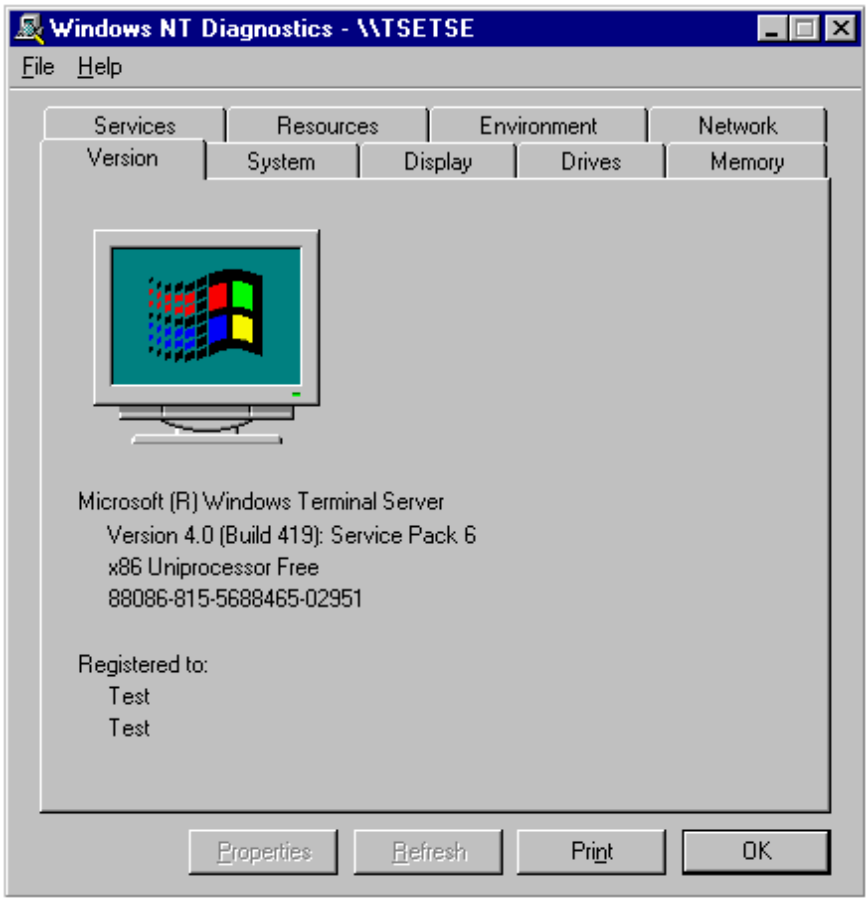


Figure 4 WinMSD screenshot

12.2 System Properties screenshot

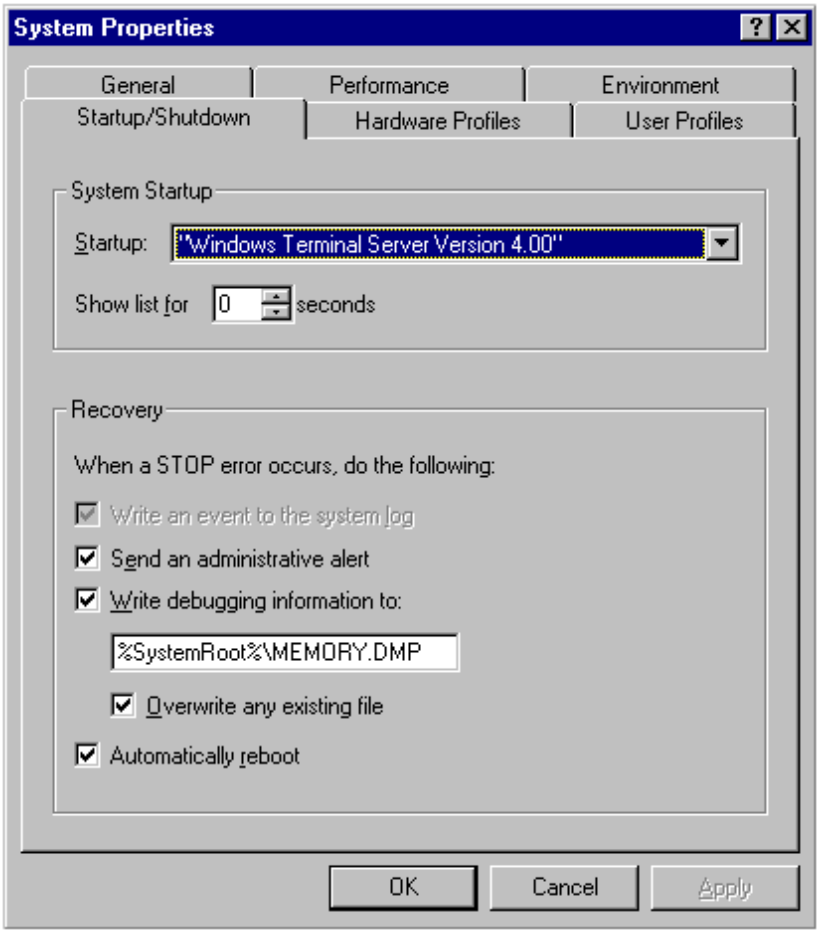


Figure 5 Startup delay and Auto Reboot settings

12.3 WinVer screenshot

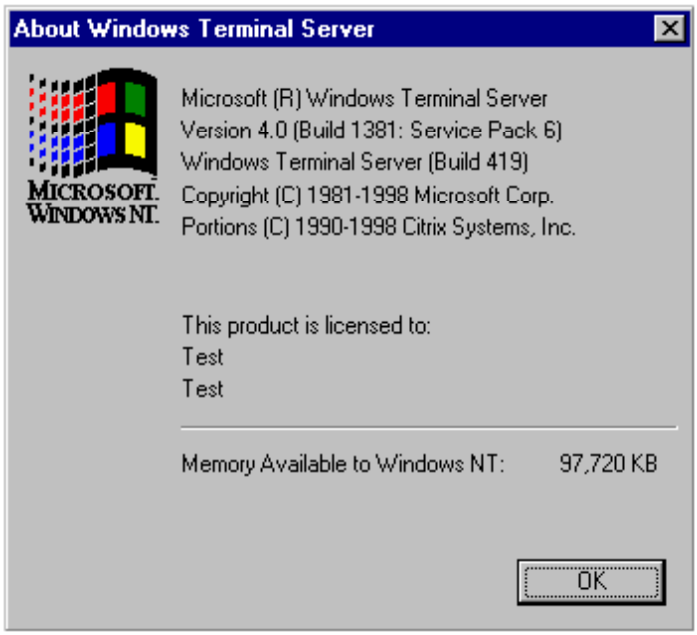


Figure 6 WinVer.exe screenshot from TseTse on 27 July 2001.

12.4 WinMSD Report

A copy of the summary report produced by WinMSD on TseTse on 27 July 2001 follows:

```
Microsoft Diagnostics Report For \\TSETSE
---------------------------------------------------------------------------

OS Version Report
---------------------------------------------------------------------------
Microsoft (R) Windows Terminal Server
Version 4.0 (Build 419): Service Pack 6 x86 Uniprocessor Free
Registered Owner: Test, Test
Product Number: 88086-815-5688465-02951
---------------------------------------------------------------------------

System Report
---------------------------------------------------------------------------
System: AT/AT COMPATIBLE
Hardware Abstraction Layer: PC Compatible Eisa/Isa HAL
BIOS Date: 09/24/97
BIOS Version: Phoenix ROM BIOS PLUS Version 1.

Processor list:
   0:  x86 Family 5 Model 2 Stepping 12 GenuineIntel ~199 Mhz
---------------------------------------------------------------------------

Video Display Report
---------------------------------------------------------------------------
BIOS Date: 09/24/97
BIOS Version: S3 TrioV+ Enhanced Video BIOS Version 1.03-02

Adapter:
   Setting: 1024 x 768 x 256
            75 Hz
   Type: s3 compatible display adapter
   String: S3 Compatible
   Memory: 2 MB
   Chip Type: S3 765
   DAC Type: S3
Driver:
   Vendor: Microsoft Corporation
   File(s): s3.sys, s3.dll
   Version: 4.00, 4.0.0


Drives Report
---------------------------------------------------------------------------
C:\  (Local - NTFS)  Total: 2,060,320 KB, Free: 1,556,518 KB

Memory Report
---------------------------------------------------------------------------
Handles: 1,832
Threads: 184
Processes: 25

Physical Memory (K)
   Total: 97,720
   Available: 41,600
   File Cache: 15,956



Services Report
---------------------------------------------------------------------------
Alerter                                          Running   (Automatic)
```

```
Computer Browser                                Running   (Automatic)
EventLog (Event log)                            Running   (Automatic)
Server                                          Running   (Automatic)
Workstation (NetworkProvider)                   Running   (Automatic)
License Logging Service                         Running   (Automatic)
TCP/IP NetBIOS Helper                           Running   (Automatic)
Messenger                                       Running   (Automatic)
NT LM Security Support Provider                 Running   (Automatic)
SAP Agent                                       Running   (Automatic)
Plug and Play (PlugPlay)                        Running   (Automatic)
Protected Storage                               Running   (Automatic)
Remote Procedure Call (RPC) Service             Running   (Automatic)
Spooler (SpoolerGroup)                          Running   (Automatic)
Terminal Server                                 Running   (Automatic)
Terminal Server Licensing                       Running   (Automatic)
COM+ Event System (Network)                     Running   (Manual)


Drivers Report
----------------------------------------------------------------------
AFD Networking Support Environment (TDI)        Running   (Automatic)
atapi (SCSI miniport)                           Running   (Boot)
Beep (Base)                                     Running   (System)
Cdfs (File system)                              Running   (Disabled)
Cdrom (SCSI CDROM Class)                        Running   (System)
Disk (SCSI Class)                               Running   (Boot)
3Com 3C90x Adapter Driver (NDIS)                Running   (Automatic)
Floppy (Primary disk)                           Running   (System)
i8042 Keyboard and PS/2 Mouse Port Driver (Keyboard Port) Running   (System)
Keyboard Class Driver (Keyboard Class)          Running   (System)
KSecDD (Base)                                   Running   (System)
Mouse Class Driver (Pointer Class)              Running   (System)
Msfs (File system)                              Running   (System)
Mup (Network)                                   Running   (Manual)
Microsoft NDIS System Driver (NDIS)             Running   (System)
NetBIOS Interface (NetBIOSGroup)                Running   (Manual)
WINS Client(TCP/IP) (PNP_TDI)                   Running   (Automatic)
Npfs (File system)                              Running   (System)
Ntfs (File system)                              Running   (Disabled)
Null (Base)                                     Running   (System)
NWLink IPX/SPX Compatible Transport Protocol (PNP_TDI) Running   (Automatic)
NWLink NetBIOS (PNP_TDI)                        Running   (Automatic)
NWLink SPX/SPXII Protocol (PNP_TDI)             Running   (Automatic)
Parallel (Extended base)                        Running   (Automatic)
Parport (Parallel arbitrator)                   Running   (Automatic)
ParVdm (Extended base)                          Running   (Automatic)
Rdr (Network)                                   Running   (Manual)
s3 (Video)                                      Running   (System)
Serial (Extended base)                          Running   (Automatic)
Srv (Network)                                   Running   (Manual)
TCP/IP Service (PNP_TDI)                        Running   (Automatic)
Terminal Device Driver                          Running   (Automatic)
VgaSave (Video Save)                            Running   (System)


IRQ and Port Report
----------------------------------------------------------------------
Devices                        Vector Level  Affinity
----------------------------------------------------------------------
i8042prt                            1     1 0xffffffff
i8042prt                           12    12 0xffffffff
Serial                              4     4 0x00000000
El90x                              11    11 0x00000030
Floppy                              6     6 0x00000000
atapi                               0    14 0x00000000
atapi                               0    15 0x00000000
----------------------------------------------------------------------
```

```
Devices                        Physical Address  Length
-----------------------------------------------------------------------
i8042prt                         0x00000060  0x0000000001
i8042prt                         0x00000064  0x0000000001
Parport                          0x00000378  0x0000000003
Serial                           0x000003f8  0x0000000007
El90x                            0x0000dcc0  0x0000000040
Floppy                           0x000003f0  0x0000000006
Floppy                           0x000003f7  0x0000000001
atapi                            0x000001f0  0x0000000008
atapi                            0x000003f6  0x0000000001
atapi                            0x00000170  0x0000000008
atapi                            0x00000376  0x0000000001
s3                               0x000003c0  0x0000000010
s3                               0x000003d4  0x0000000008
s3                               0x000042e8  0x0000000002
s3                               0x00004ae8  0x0000000002
s3                               0x000082e8  0x0000000004
s3                               0x000086e8  0x0000000004
s3                               0x00008ae8  0x0000000004
s3                               0x00008ee8  0x0000000004
s3                               0x000092e8  0x0000000004
s3                               0x000096e8  0x0000000004
s3                               0x00009ae8  0x0000000004
s3                               0x00009ee8  0x0000000004
s3                               0x0000a2e8  0x0000000004
s3                               0x0000a6e8  0x0000000004
s3                               0x0000aae8  0x0000000004
s3                               0x0000aee8  0x0000000004
s3                               0x0000b6e8  0x0000000004
s3                               0x0000bae8  0x0000000004
s3                               0x0000bee8  0x0000000004
s3                               0x0000e2e8  0x0000000004
s3                               0x0000c2e8  0x0000000004
s3                               0x0000c6e8  0x0000000004
s3                               0x0000cae8  0x0000000004
s3                               0x0000cee8  0x0000000004
s3                               0x0000d2e8  0x0000000004
s3                               0x0000d6e8  0x0000000004
s3                               0x0000dae8  0x0000000004
s3                               0x0000dee8  0x0000000004
s3                               0x0000e6e8  0x0000000004
s3                               0x0000eae8  0x0000000004
s3                               0x0000eee8  0x0000000004
s3                               0x0000f6e8  0x0000000004
s3                               0x0000fae8  0x0000000004
s3                               0x0000fee8  0x0000000004
VgaSave                          0x000003b0  0x000000000c
VgaSave                          0x000003c0  0x0000000020
VgaSave                          0x000001ce  0x0000000002


DMA and Memory Report
-----------------------------------------------------------------------
Devices                          Channel    Port
-----------------------------------------------------------------------
Floppy                              2     0
-----------------------------------------------------------------------
Devices                          Physical Address  Length
-----------------------------------------------------------------------
s3                               0x000a0000  0x00010000
s3                               0xf8000000  0x04000000
s3                               0x000c0000  0x00008000
VgaSave                          0x000a0000  0x00020000


Environment Report
```

```
---------------------------------------------------------------------


System Environment Variables
   ComSpec=C:\WTSRV\system32\cmd.exe
   Os2LibPath=C:\WTSRV\system32\os2\dll;
   Path=C:\WTSRV\system32;C:\WTSRV
   windir=C:\WTSRV
   OS=Windows_NT
   PROCESSOR_ARCHITECTURE=x86
   PROCESSOR_LEVEL=5
   PROCESSOR_IDENTIFIER=x86 Family 5 Model 2 Stepping 12, GenuineIntel
   PROCESSOR_REVISION=020c
   NUMBER_OF_PROCESSORS=1



Environment Variables for Current User
   TEMP=C:\TEMP
   TMP=C:\TEMP



Network Report
---------------------------------------------------------------------
Your Access Level: Admin & Local
Workgroup or Domain: TESTLAN
Network Version: 4.0
LanRoot: TESTLAN
Logged On Users: 1
Current User (1): Superman
  Logon Domain: TSETSE
  Logon Server: TSETSE

Transport: NetBT_El90x1, 00-C0-4F-C9-07-5B, VC's: 0, Wan: Wan
Transport: NwlnkNb, 00-C0-4F-C9-07-5B, VC's: 0, Wan: Wan

Character Wait: 3,600
Collection Time: 250
Maximum Collection Count: 16
Keep Connection: 600
Maximum Commands: 5
Session Time Out: 45
Character Buffer Size: 512
Maximum Threads: 17
Lock Quota: 6,144
Lock Increment: 10
Maximum Locks: 500
Pipe Increment: 10
Maximum Pipes: 500
Cache Time Out: 40
Dormant File Limit: 45
Read Ahead Throughput: 4,294,967,295
Mailslot Buffers: 3
Server Announce Buffers: 20
Illegal Datagrams: 5
Datagram Reset Frequency: 60
Bytes Received: 261
SMB's Received: 3
```

12.5 HotFixes applied screenshot

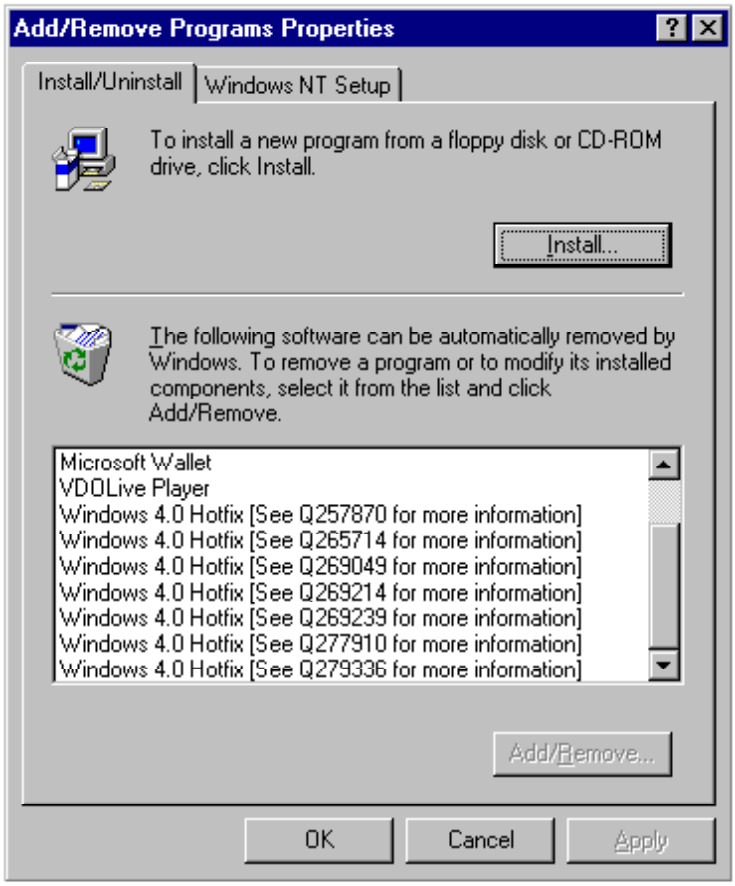


Figure 7 Screenshot from Control Panel showing HotFixes applied to TseTse

12.6 SysKey screenshot

Figure 8 Screenshot from SysKey on TseTse

12.7 Internet Explorer Version Screenshot

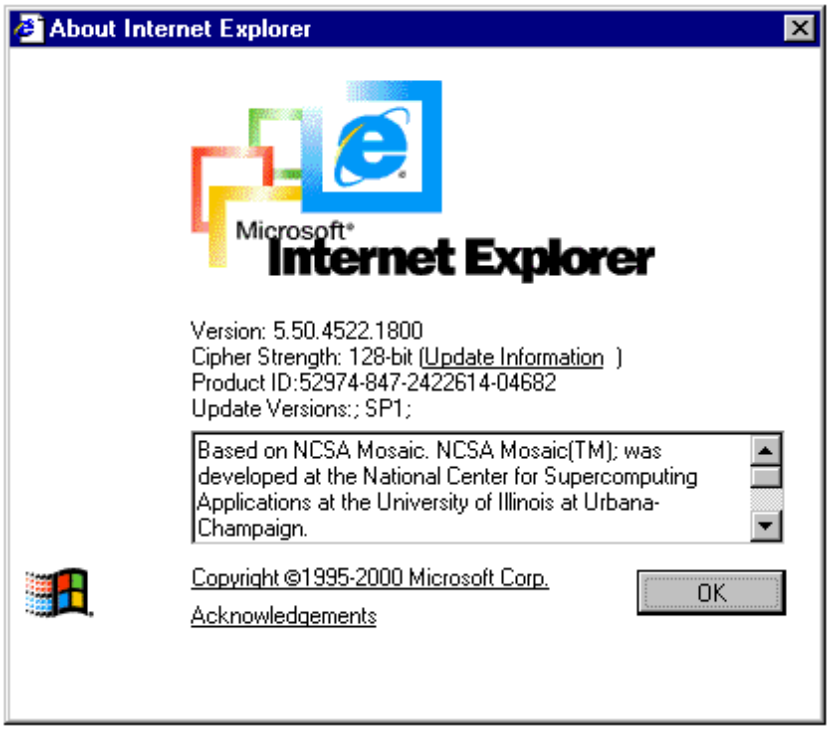
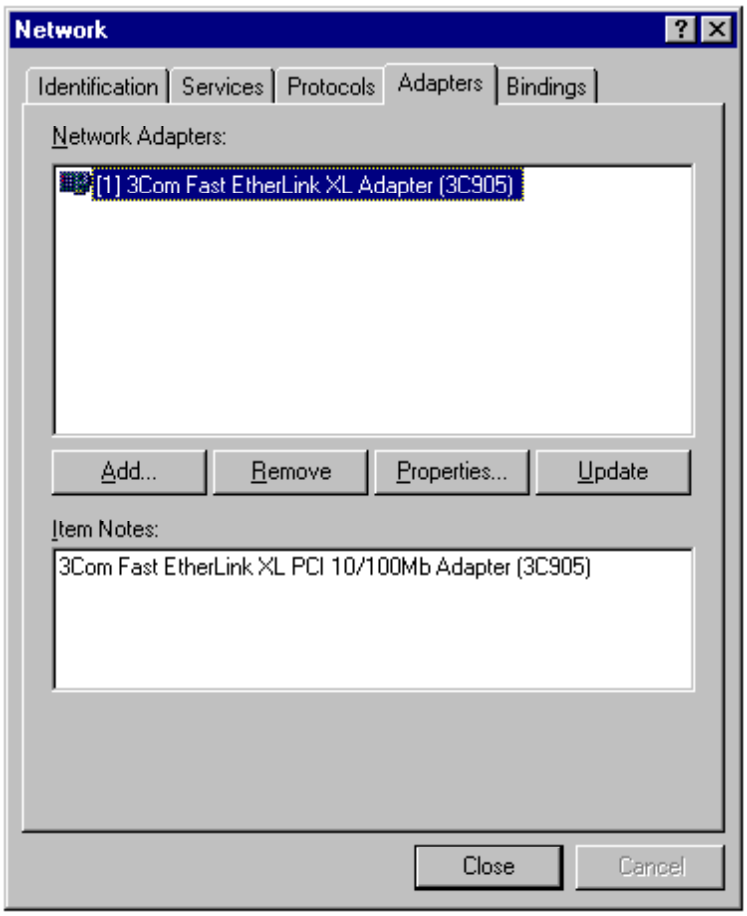


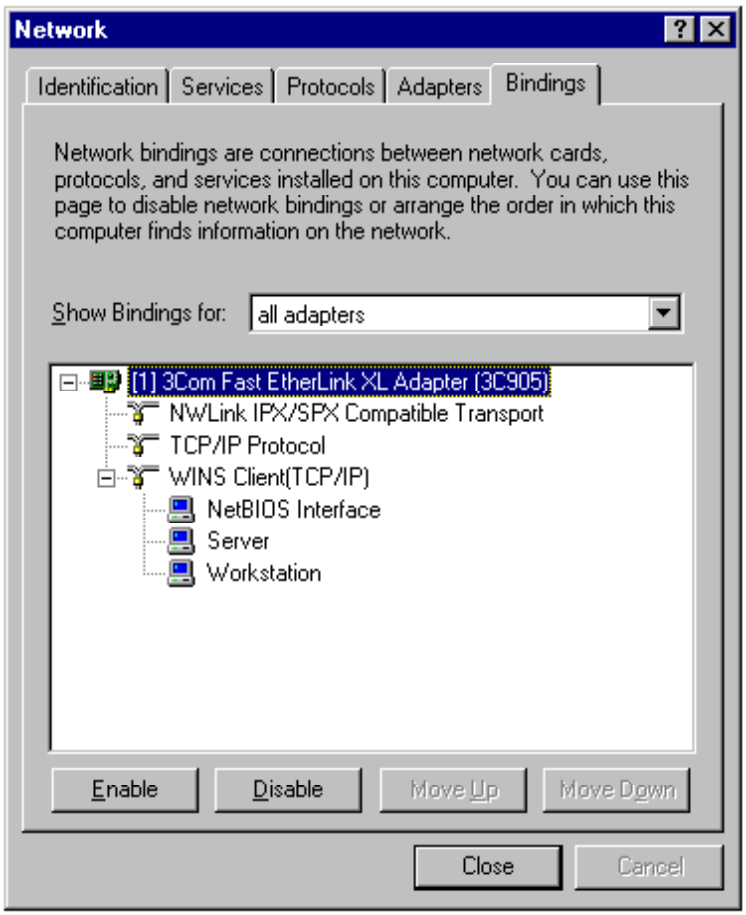
Figure 9 Internet Explorer version screenshot

12.8 Network Adapter Screenshot



10 Network Adapter screenshot

12.9 Network Adapter bindings screenshot



11 Network Adapter bindings on TseTse

12.10 IPCONFIG Report

```
Windows NT IP Configuration

     Host Name . . . . . . . . . . : tsetse.acme.com
     DNS Servers . . . . . . . . . : 192.168.0.252
                                     192.168.0.253
     Node Type . . . . . . . . . . : Hybrid

     NetBIOS Scope ID. . . . . . . :
     IP Routing Enabled. . . . . . : No
     WINS Proxy Enabled. . . . . . : No
     NetBIOS Resolution Uses DNS : Yes

Ethernet adapter El90x1:
     Description . . . . . . . . . : 3Com 3C90x Ethernet Adapter
     Physical Address. . . . . . . : 00-C0-4F-C9-07-5B
     DHCP Enabled. . . . . . . . . : No
     IP Address. . . . . . . . . . : 192.168.0.45
     Subnet Mask . . . . . . . . . : 255.255.255.0
     Default Gateway . . . . . . . : 192.168.0.251
     Primary WINS Server . . . . . : 192.168.0.252
```

12.11 C2Config Screenshot

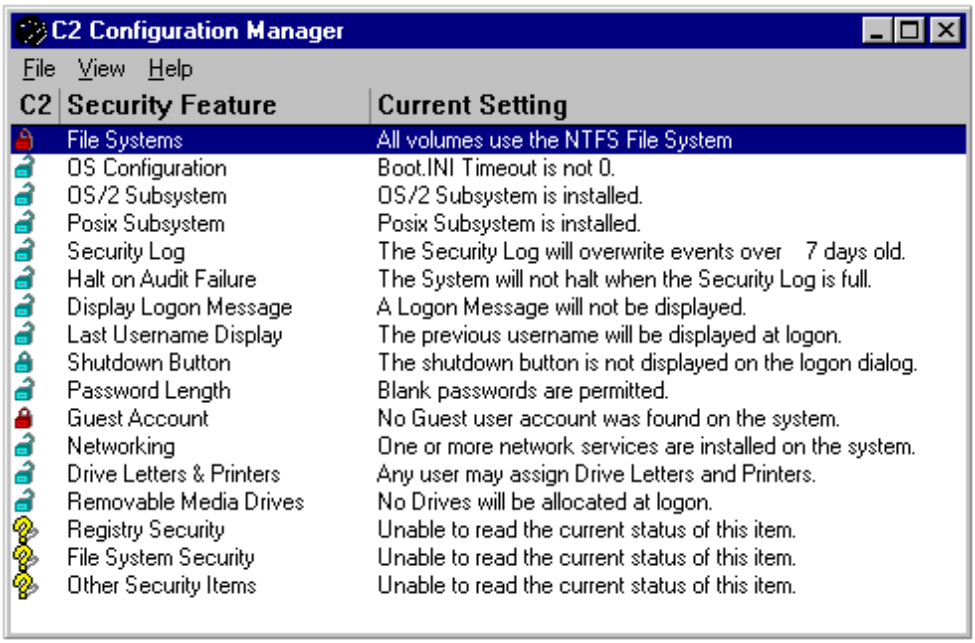


Figure 12 Default Terminal Server C2Config Screenshot

12.12 AppSec Screenshot

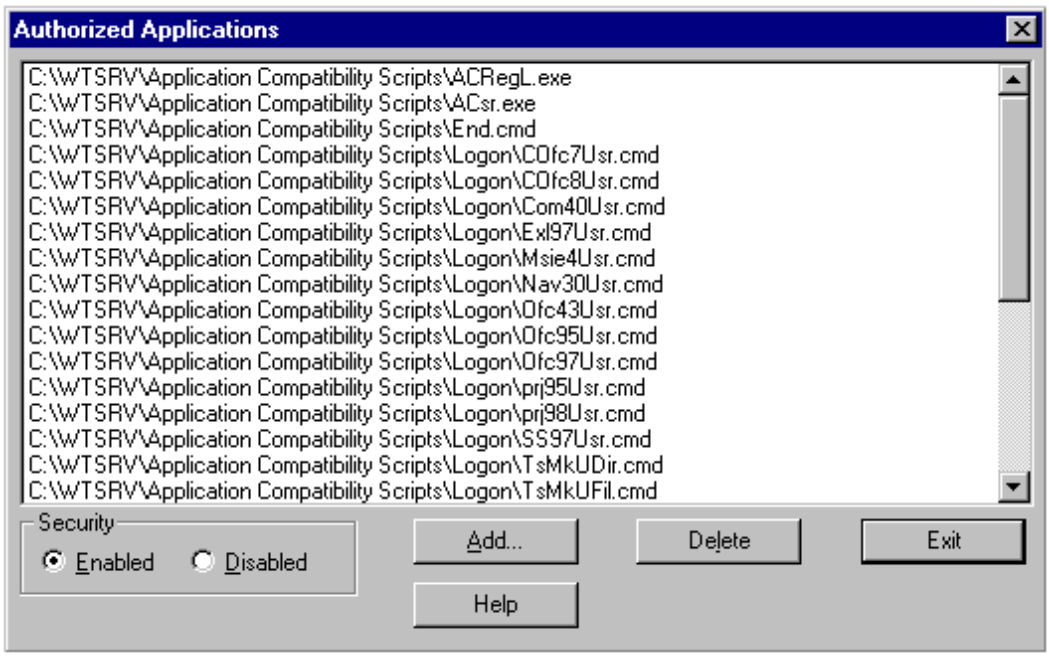


Figure 13 Screenshot of APPSEC.exe

12.13 PolEdit screenshot

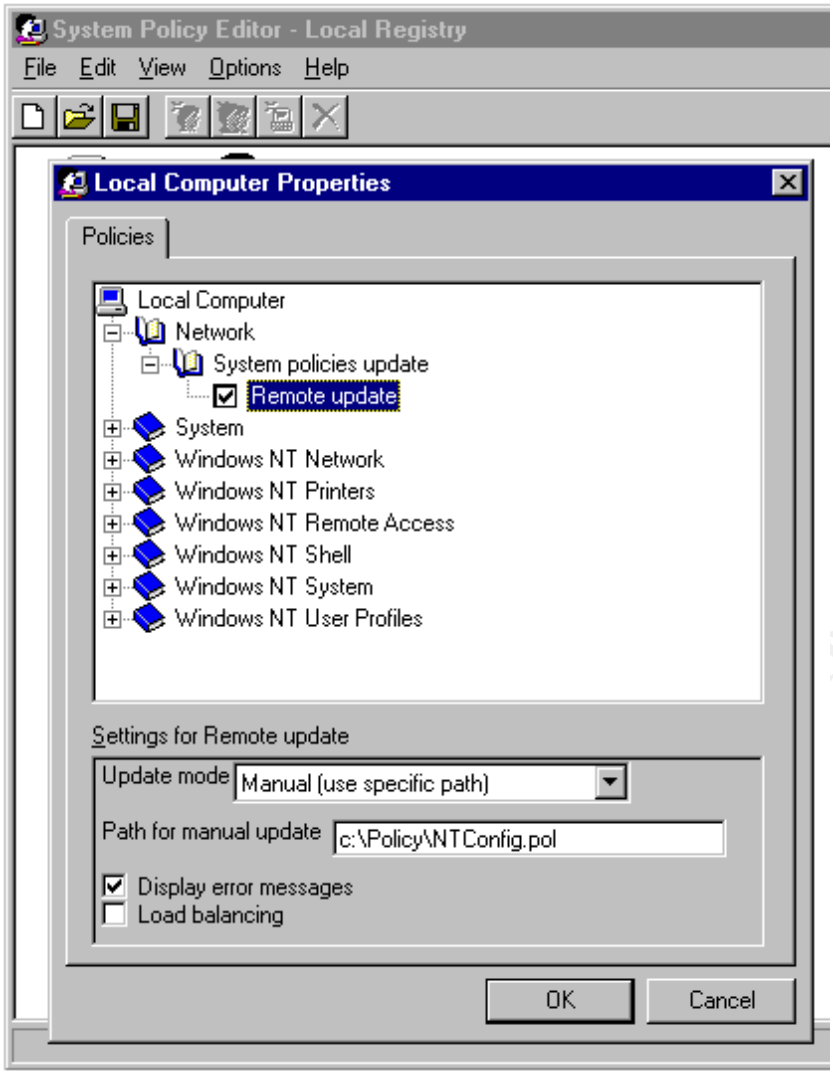


Figure 14 System Policy Editor – NTConfig.pol location

12.14 AutoLogon

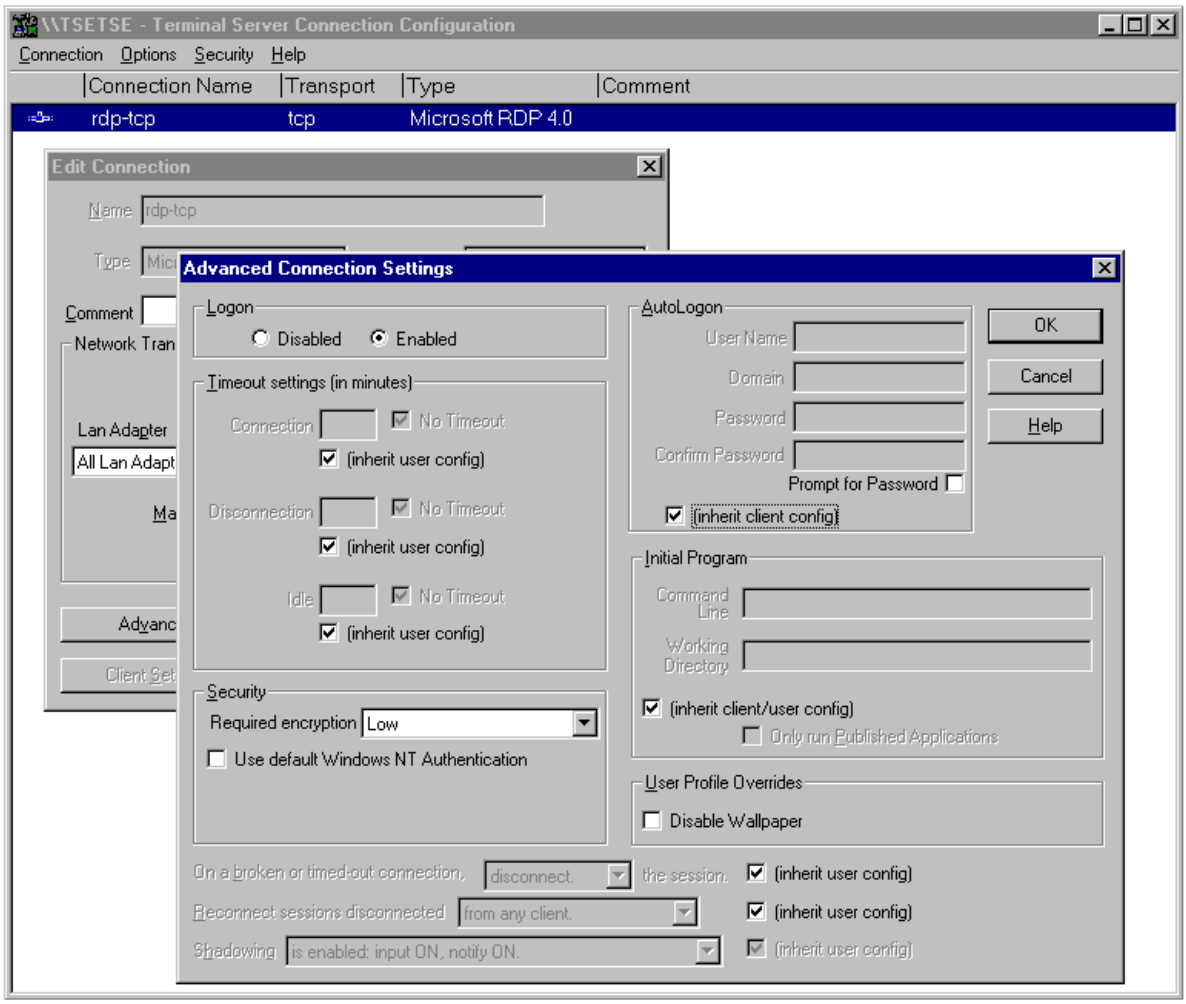


Figure 15 AutoLogn and RDP Configuration.

13. References

1 Microsoft TechNet Microsoft Corporation 1998, *MS Windows NT Server, Terminal Server Edition, version 4.0: An Architectural Overview White Paper*, http://www.microsoft.com/ntserver/terminalserver/techdetails/prodarch/tsarchitecture.asp

2 Microsoft Corporation, *MS Windows NT Server, Terminal Server Edition, Security and Auditing*, http://www.microsoft.com/technet/producttechnol/termserv/maintain/wtspolcy.asp

3 Microsoft Corporation, *MS Windows NT Server, Terminal Server Edition, 'Implementing Policies in a Terminal Server Environment'*, http://www.microsoft.com/technet/prodtechnol/termsrv/maintain/wtspolcy.asp

4 Mark RiCharde, *Citrix Systems' Metaframe Offers Enhanced Functionality fo (sic) MS Windows Terminal Server*, http://www.sans.org/infosecFAQ/win/metaframe.htm

5 Other resources used for general research include:
- Microsoft TechNet CD
- Microsoft Web site
- Citrix web site

6 Microsoft Corporation, *How to Determine If a Hotfix Is Compatible with Terminal Server*, http://support.microsoft.com/support/kb/articles/Q196/3/34.ASP

7 Microsoft Corporation, *Q189119 UserEnv Returns Corrupted Profile for All Failures Including RSL Exceeded,* http://support@microsoft.com/support/kb/articles/q189/1/19.asp

8 Microsoft Corporation, *Q176083 System Is Running Low on Registry Quota*, http://support.microsoft.com/support/kb/articles/q176/0/83.asp

9 Microsoft Corporation, *Q124594 Understanding and Configuring Registry Size Limit (RSL)*, http://support.microsoft.com/support/kb/articles/q124/5/94.asp

10 Chris Young, *Windows NT 4.0 Audit Checklist*, http://www.sans.org/infosecFAQ/audit/NT40.htm

11 Microsoft Corporation, *Microsoft TechNet DVD July 2001*, Windows Product Family, Windows NT Server, Technical Notes, Implementation and Integration, Windows NT 4 Security, Audit and Control, Chapter 13 – Auditing Windows NT Security Features and Controls

12 Microsoft Corporation, *Q147706 How to Disable LM Authentication on Windows NT,* http://support.microsoft.com/support/kb/articles/q147/7/06.asp

13 Sherri Heckendorn, *Auditing Windows NT GIAC Practical*, http://www.sans.org/y2k/practical/Sherri_Heckendorn.doc

14 Microsoft Corporation, *Q185704 How to Restrict Floppy Disk Drive Access Using Floplock Service*, http://support.microsoft.com/support/kb/articles/q185/7/04.asp

15 Microsoft Corporation, *Internet Information Server 4.0 Resource Guide*, http://www.microsoft.com/technet/prodtechnol/iis/reskit/iis40rg/iisrkc08.asp

16 Microsoft Corporation, *Terminal Server Commands: C2CFG or C2CONFIG*, http://support.microsoft.com/support/kb/articles/Q186/6/21.ASP

17 Microsoft Corporation, *Registry Permissions Not Inherited Properly After Securing the Registry with C2Config*, http://support.microsoft.com/support/kb/articles/q221/7/66.asp

18 Microsoft Corporation, *Q230338 Inbox and Internet Explorer Icons Disabled with Appsec.exe,* http://support.microsoft.com/support/kb/articles/Q230/3/38.ASP

19 Microsoft Corporation, *Q186609 Terminal Server's Application Security*,

http://support.microsoft.com/support/kb/articles/Q186/6/09.ASP
20 Microsoft Corporation, *Q186500 Terminal Server Commands: APPSEC,* http://support.microsoft.com/support/kb/articles/Q186/5/00.ASP
21 Microsoft Corporation, *Implementing Policies in Terminal Server,* http://www.microsoft.com/ntserver/techresources/deployment/terminal/implpol.asp
22 Microsoft Corporation, *Implementing Policies in a Terminal Server Environment White Paper*, http://www.microsoft.com/ntserver/zipdocs/implpol.exe
23 Microsoft Corporation, *Zero Administration Kit for Terminal Server*, http://www.microsoft.com/ntserver/terminalserver/downloads /admintools/TermServzak.asp
24 Microsoft Corporation, *Microsoft® ZAK for Windows NT® Server, Terminal Server Edition, version 4.0*, http://www.microsoft.com/ntserver/zipdocs/zakfortswp.exe