Global Information Assurance Certification Paper

Security Measures for Windows 2000 Terminal Server in an Unrestricted University Environment

Douglas McCrea
March 17, 2003
GSEC Practical Assignment v 1.4b

Abstract

Windows 2000 Terminal Services offers a low-cost and relatively high level of security for a mostly unmonitored and unrestricted student work environment. This case study demonstrates the security practices and procedures followed as well as resources used to install Windows 2000 Terminal Server (Application Mode) and corresponding thin clients in a mostly unrestricted university environment.

Before Snapshot

Student employees were using 35 workstations running Windows NT 4.0 SP6a throughout the college. The workstations resided in a Windows 2000 domain and their existence was preventing significant security changes to the existing Windows 2000 domain. Windows NT 4.0 (WinNT) was not capable of accepting Group Policies which were largely used to manage the computers in the college. I wanted to disable NetBIOS over TCP/IP throughout the entire domain which was not possible without stopping communication with the WinNT systems. Additionally, the NT 4.0 systems made rolling out hotfixes, new software, and applying settings changes much more difficult. The computers broke down quite often either due to tampering with the systems, or issues with device drivers. Difficulties were also faced concerning staff members and student staff following security guidelines. The WinNT systems in place significantly detracted from the domain and network security. Windows 2000 Terminal Server provided a low-cost and for a variety of reasons, significantly more secure solution for student staff within the college. The project incorporated a large quantity of techniques and concepts spanning the GSEC course. By drawing on many of the resources and tools provided, a documented plan was created and followed beginning with a risk assessment, continuing with policy development, baseline security, operating system and network hardening, perimeter defense, virus protection, and training.

Risk Assessment

The workstations received less attention by computing staff due to unfamiliarity with the operating system, lack of priority in needing to be repaired compared to a computer outage of a staff member, general state of disrepair, slow computer speeds leading to frustration by computing staff trying to repair the devices and by students working on the computers. This inherently led to more damage to the computers and operating systems.

The IT office of three full-time and four part-time employees was understaffed by one full-time employee, the other full-time staff member had just been hired, and there were only two part-time help desk employees. The Windows 2000 domain allowed nested local administrator rights to all employees by adding their group to the local administrators group on the workstation. This allowed working hour limitations on the part-time helpdesk staff preventing after-hour logins to computers and also allowed the accounts to be disabled if there were any problems with abuse. Part-time employees were not given local administrator passwords. The WinNT systems did not have the group nesting capability of the Windows 2000 workstation meaning that only full-time employees were able to perform fixes on the workstations. This created an expensive and time consuming situation for the IT staff.

Due to a lack of a university-based firewall, the systems were vulnerable to attempted logins using NetBIOS over TCP/IP which happened frequently. Although there was no compromise, this was a situation that added extensive vulnerability to the workstation and the domain.

At the time, the null session attacks[1] existed and were prevented in the Windows 2000 domain by group policy. The necessary settings changes to restrict anonymous[2] had not been applied to the WinNT systems because the systems were about to be replaced.

Floppy drives were accessible and a source of frequent viruses from students trying to work on papers from the university's virus-ridden computer labs. While the systems had virus protection, the systems were potentially vulnerable to unknown viruses and hacks that students could come up with and import in disk as well as on the Web or using Web-based email.

The systems at the time had not had their BIOS's modified to prevent booting from floppy disk or CD and left them vulnerable to multiple hacks such as Offline NT Password & Registry Editor, Bootdisk[3].

While NT policies[4] were used to control access and prevent some tampering, the policies were too restrictive in some cases and not enough in others. Students frequently installed instant messaging software, games, wallpaper, screen savers, GRE test-prep software, and America On-Line software. Many of these installations failed due to restrictions, but left the systems in a larger state of disrepair.

This particular group of computers also had a set of recalled hard drives that failed at a rate of one or two a month. This resulted in a total loss of all local data. Replacing the hard drives and rebuilding the workstations was a lengthy

---

[1] "nt-netbios-nullsession (170)." URL: http://www.iss.net/security_center/static/170.php. (20 Feb. 2003).

[2] "Restricting Information Available to Anonymous Logon Users." 1434748. 1 Aug. 2001. URL: http://support.microsoft.com/default.aspx?scid=KB;en-us;q143474. (20 Feb. 2003).

[3] Nordahl-Hagen, Petter. "Offline NT Password & Registry Editor, Bootdisk." 26 Jan. 2003. URL: http://home.eunet.no/~pnordahl/ntpasswd/. (20 Feb. 2003).

[4] Reilly, Michael D. "Setting NT System Policies." Getting Started with NT. 5621. July 1999. URL: http://www.winnetmag.com/Articles/Index.cfm?ArticleID=5621. (20 Feb. 2003).

process even with drive imaging software and was only done when the failure took place, rather than performing this task with all 35 machines. To solve this issue, all data was saved on shared drives which were backed up. There was a finite amount of space on the shared drives and the student employees amassed large quantities of data, pictures, desktop publishing files and junk files that were never cleaned up. Disk quotas were enforced on the shared drives, but this became a large source of tension between the IT department, student employees, and their supervisors who claimed the students never had enough space to do their work.

Staff represented one of the largest security risks faced. Supervision in some of the offices was extremely poor for both staff and student staff. Staff frequently gave their passwords out to the students or wrote their passwords on pieces of paper or post-it notes. This was out of frustration with the IT staff and with the WinNT workstations which could not handle the desktop publishing software or database software that the staff wanted the students to use; there were additional problem due to staff that were family members working in the same department as student staff; and in at least one case, personal involvement with a student by a staff member. Passwords that were given to the students were immediately shared with other student staff; this was determined during a few late-night, unannounced security walkthroughs of the offices. There was a failure to reprimand students without “proof”, and even when log files were presented or the student was found after working hours on a staff member’s computer, some supervisors stated that it couldn’t be proven which student specifically was using the computer or whether the use was inappropriate and therefore, these serious problems went unaddressed.

During Snapshot

The WinNT systems needed to be converted to Windows 2000 due to the many disadvantages of staying with Windows NT 4.0 in a Windows 2000 domain. All 35 systems were Pentium 100MHz with 32MB of RAM. This configuration is below the minimum system requirements for Windows 2000[5], so a direct upgrade from Windows NT on those systems was not possible. Purchasing and licensing 35 systems would cost well over $20,000 which was not within the budget. Windows 2000 Terminal Services could be housed on a reasonably powerful server for less than $10,000 with all educational licensing. By using a Terminal Services solution, many of the initial workstation security settings would be automatically applied by group policy, and the remaining issues of further locking down the Terminal Server for student use would need to be tested.

Fully testing Terminal Server and a thin-client for the Terminal Server was paramount. Constructing and testing a locked-down thin-client was the first step. If a suitable thin client using Windows NT 4.0 was unavailable, the entire concept wouldn’t be plausible. Testing was performed on the same system. After the

---

[5] “Appendix F - Windows 2000 Server and Professional Systems Requirements.” Windows 2000 Server Deployment Planning Guide. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/reskit/deploy/part7/sdgappf.asp. (21 Feb. 2003).

initial system was set up with Windows NT 4.0 and fully patched, an image was taken using Norton Ghost Enterprise 7.5. Each change and step was reviewed and documented and if an error was made or a settings change did not work the way we wanted, the change was rescinded or the image was reapplied and the process was repeated. This also helped streamline documentation errors as the documentation was reviewed each time the system was brought back from an image. After testing, the following thin client was created:

Windows NT 4.0 Service Pack 6a
32 MB RAM
1.2 GB Hard drive formatted with NTFS

Preliminary workstation installation:

1. NTFS was chosen as the format of the drive to provide the necessary drive security.
2. Custom Setup Options were chosen to minimize software installed.
3. All selected components were unchecked.
4. A network interface card was installed with the latest drivers and configured only with TCP/IP using DHCP, however, the network card was unplugged until Service Pack 6a is installed by CD.
5. All other defaults were kept and the systems is not added to the domain.
6. Service pack 6a was installed by CD and the network card was plugged in.
7. The welcome screen was unchecked and closed.
8. Internet Explorer 6 was installed using the download helper on a floppy disk. This is done ironically because the version of Internet Explorer provided with the original NT 4.0 installation disk is incapable of downloading the software directly from Microsoft's site. The a custom install was performed only downloading IE 6 and visual Basic Scripting support in order to use Windows Update to perform the rest of the updates. This can be a debatable point and updates could be applied if brought in by CD, however, this will not be necessary considering the security changes that will be listed below.
9. Windows Update was used to complete the update and patching process.
10. At this point an image was made using Norton Ghost 7.5 Enterprise so that if any errors took place during Registry Changes or security settings, the system could be easily recovered.

Security Lockdown:

1. BIOS
    a. The BIOS was upgraded to the most recent version.
    b. An administrative BIOS password was added.
    c. Booting from the hard drive was place first in the boot options to prevent users from booting from floppies or CD and launching attacks or using the systems as Linux drones.
2. Terminal Client was installed using a High Encryption enabled installation disk set.

    a. High encryption must be enabled on the Terminal Server before creating the disk set or the default low encryption disk set will be created[6].
    b. We found this out because we changed the setting to High Encryption on the server after the client disks had been created and the clients could no longer connect.
    c. During the Terminal Services client installation, “Yes” must be answered to the question of whether the client should be installed for all user or this thin-client setup will not work.
3. NT Systems Changes
    a. Under My Computer->Properties->Startup/Shutdown Tab-> Show list for X seconds was changed from 30 to 5 to lessen the wait time for student trying to log on.
    b. Users
        i. The administrator and guest accounts were renamed.
        ii. The guest account was verified to be disabled.
        iii. A third user, which would be used as the auto-logon account was created as an administrator. Note that the administrator group membership will be removed once the registry entries are made. This is explained below. This account must also have a different password than the administrator or the workstation could become vulnerable to auto-logon into the administrator account. This actually happened the first time I logged in during testing because I forgot to change the local user password to something other than the local administrator password I was currently using during testing.
        iv. On all accounts, the password does not expire box was checked.
    c. Network settings
        i. WINS and LMHost lookups were not used.
        ii. Under TCP/IP Properties->Advanced Tab->Enable Security Checkbox Checked
            1. ->Configure
            2. Permit only->TCP Ports->no entries required.
            3. Permit only->UDP Ports->port 68 (DHCP) so the workstation can obtain an IP address.
            4. Permit IP Protocols->no entries required.
            5. This locks down the workstation from the majority of network-based attacks by blocking all inbound traffic except ICMP. The only presence that can be detected remotely of the machine is by ICMP such as the use of ping. This is acceptable because the system is of little interest other than being detectable as a possible

---

[6] “Terminal Services Client Cannot Connect to a Server Running 128-bit Encryption.” 257894. 11 Oct. 2002. URL: http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B257894. (22 Feb. 2003).

        Windows machine by it’s TTL of 128. This does prevent the use of DNS and so only an IP address can be entered for the Terminal Server when it is configured.
        6. This type of setup also lowers the need for a personal firewall as mentioned in Host Perimeter Defense in the course material.

d. Thin client preparation
    i. After the basic preparation was performed, more drastic changes needed to be made to the registry, start menu, and auto-logon user account.
    ii. The administrator account (let’s call it admin) was logged out of and the terminal client account (let’s call it term_user) was logged into for the first time.
        1. All items that could be deleted from the desktop were deleted.
        2. Under the All User’s start menu, Administrative Tools (common) and Terminal Services Client (TSC) folders were moved to the Administrator’s Start Menu.
        3. A copy of Client Connection Manager from the TSC folder was placed in the Start Menu of term_user.
        4. All extra programs under both All Users and term_user are removed.
        5. Under Client Connection Manager (CCM), a new connection was made to the terminal server (let’s call it term1).
            a. The connection’s name was made to be “Logon to Term1.”
            b. The IP address (not UNC name, because DNS will not resolve host names due to the inbound port restrictions) for the Terminal Server was added.
            c. There was no automatic logon added, user are supposed to log on.
            d. The resolution was set to 1024x768 and the Full Screen check box was checked (this is important as the machine should look and feel like the user is really using the system directly).
            e. At first, I did not enable data compression or cache bitmaps. I found that the bandwidth utilization was unacceptably high with 35 machines all constantly obtaining new bitmaps as well as other network activities (the network was 10Mb at the time). Additionally, there was significant lag because the network was over-utilized between this server and the other 50 or

        so hosts on the same hub. Once these check boxes were checked, there was a very large improvement in the network. A few months later, the network was completely revised, placed on 100Mb switches with a 1 Gb uplink removing almost all lag.

        f. The link for Logon to Term1 was placed in the startup folder so that the application is automatically launched in full-screen mode upon boot up.
        g. A link should also be copied to the All User's Start menu so that it can be access if the client has been logged off without having to reboot the computer.
        h. Once the Shortcuts have been put into place, the system should be rebooted to test how it will look and work. If it works, then the link to CCM should be deleted so that it cannot be altered. Changes can be made to the Client Connection in the future by logging in as Admin and copying the CCM link to the All Users or term_user's start menu.
    6. The term_user's and All User's startup folders' properties were changed to "hidden". Because View Hidden Files and Folders is not selected for the user, the folders disappear from view.
    7. Help cannot be removed from the Start menu. Disable this by creating a text file named Windows.hlp and copying it over the existing file in the Windows NT\System32 folder.
iii. All registry entries were tested either in combination or step-by-step (for the more drastic changes). As each registry key worked, it was added to a .reg file so that it could be automatically run to speed up client production and testing.

The following Registry keys were altered as per Microsoft Knowledgebase article 198771[7] and "NT 4 Lockdown" by Snakegully Computing[8]:

Under
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

---

[7] "How to Lock Down Windows NT and Internet Explorer 4.01 Desktop." 198771. 1 Oct. 2002. URL: http://support.microsoft.com/default.aspx?scid=kb%3ben-us%3b198771. (23 Feb. 2003).
[8] "NT 4 Lockdown" 27 Jan. 2003. URL: http://www.snakegully.nu/tech/nt4lockdown.html. (23 Feb. 2003).

"NoDriveTypeAutoRun"=dword:00000095
This disables the AutoRun function on a CD-ROM allowing programs to automatically run when a CD is placed in the drive.

"NoFind"=dword:00000001
This removes the find command from the start menu.

"NoFolderOptions"=dword:00000001
This removes the folder options item from the settings menu.

"NoFavoritesMenu"=dword:00000001
This removes the favorites menu.

"NoRecentDocsMenu"=dword:00000001
This removes the Documents menu from the start menu.

"NoSetActiveDesktop"=dword:00000001
This removes the Active Desktop item from the settings menu.

"NoDesktop"=dword:00000001
This hides all the items on the desktop.

"NoSetFolders"=dword:00000001
This removes set folders from the start menu.

"NoSetTaskbar"=dword:00000001
This removes the taskbar from the start menu.

"NoSaveSettings"=dword:00000001
This prevents settings from being saved upon exit.

"NoNetHood"=dword:00000001
This hides the network neighborhood.

"NoRun"=dword:00000001
This removes the Run command from the start menu.

"NoDrives"=dword: 0x3fffffff
This hides all drives.

"NoTrayContextMenu"=dword:00000001
This removes context menus from the tray.

"NoViewContextMenu"=dword:00000001
This remove the Desktop and Explorer context menus.

Under
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]

"DisableLockWorkstation"=dword:00000001
This removes the lock workstation option from the menus.

"DisableTaskMgr"=dword:00000001
This disables the use of task manager available from ctrl+alt+del.

"DisableChangePassword"=dword:00000001
This disables the password change option.

Under [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]

"DefaultPassword"="putyourpasswordhere”
This is where you put the autologon password you wish to use.

"AutoAdminLogon"="1"
This turns on autologon which removes multiple logons to the same computer.

iv. During the testing of the registry keys, I found that I needed administrative rights temporarily to import the registry keys. Due to the HKEY_CURRENT_USER entries, the term_user account needed to be made into an administrator. The nature of the registry keys made it so that it would be very difficult to remove the administrative rights after the registry keys were added as well as delete the registry file. The solution was to add the term_user to the Administrators group, pull up the User Manager so that the administrative rights could be taken away once the registry keys had been added, and also have the directory where the recent file links were placed open so that it could be deleted as well.

v. The security on the reg file needed to be set to so that it could not be accessed by the recent Documents file. Despite the setting being in the Registry file to block access to the recent documents, it still appears and so locking this file down prevents it’s use, however the drawback is that the registry file still shows up. Failure to lock down the file results in a failed attempt to import into the registry. If the registry file is deleted, a search for a document results for the link, this is a security problem and so it must be locked down by permission.

vi. Once the registry keys have been added the registry can no longer be modified.

Windows 2000 Terminal Services

This section will include securing Terminal Services from a user's point of view in depth as well as a review of the overall practices used to help secure the Terminal Server on the network. Securing the Terminal Server turned out to be the more difficult portion of this process. Every application could be used to bypass security put into place either by Group Policy, registry entries, or VirusScan. While fully integrating software such as Internet Explorer and Microsoft Office with Windows 20000 can be extremely useful, it opens up vulnerabilities and the potential to sidestep many of the settings put into place on the Terminal Server.

The initial tests were run on a:

Pentium III 933MHz workstation
256MB of RAM
20GB Hard Drive
Windows 2000 SP2 with hotfixes (up to date at the time)
Terminal Services installed

The test platform logic was if multiple clients could work off of this workstation, then a much more powerful platform would be able to accommodate many more clients and allow for expansion when needed.

The parameters for this server were:

1. Accommodate up to 35 clients simultaneously.
2. Allow students the feeling of freedom to work, but really placing in extensive restrictions on:
    a. Software installations
    b. Snooping
    c. Hardware access
    d. Printer access
    e. Customization of environment
    f. Drive access
    g. Network share access
    h. Start menu and available programs
3. Allow staff to interact seamlessly with students' work through shared folders.
4. Protect the data on the server.
5. Protect the server from compromise by viruses.
6. Protect the server on the network.
7. Allow multiple levels of student employee to utilize the same server with varying levels of access.

8. Allow mostly unmonitored use by student employees who have demonstrated an aptitude for computing, hacking, and damaging even some of the most restricted environments.

Network Security

Windows 2000 Terminal Server must be protected from outside attack by hardening the operating system. A well devised and well thought-out layered strategy must be adhered to. This paper may cover some strategies listed in the guides listed below; however, the main objective of this paper is to provide the overall techniques used in securing the Terminal Server from attack and the individual techniques used to secure the Terminal Server in reference to the user environment. The following resources have been used to develop a Defense in Depth strategy as defined in the course material for the domain and Terminal Server, analyze potential weaknesses, and can help an administrator choose the options for hardening the defenses of Windows 2000 as an overall strategy:

1. Tools
    a. Microsoft Baseline Security Analyzer[9]
    b. Nessus vulnerability tester[10]. This tool was discussed in the Vulnerability Scanners section of the course material.
    c. Snort Intrusion Detection System[11]. This IDS was discussed in the Network Intrusion Detection with Snort section of the course material.
2. Information
    a. Securing Windows 2000 Terminal Services[12]
    b. National Security Agency Security Recommendation Windows 2000 Guides Download Page[13] (this compilation can be found at http://nsa2.www.conxion.com/win2k/download.htm) is one of the best compilations of security guides available

The Terminal Server was placed behind a Cisco PIX firewall allowing the following:

1. Port 3389 access to the internet. This is the port which Terminal Services listens on. There is a registry key that allows this default port to be

---

[9] "Microsoft Baseline Security Analyzer." Tools and Checklists. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/Security/tools/tools/MBSAHome.ASP. (25 Feb. 2003).

[10] "Nessus." URL: http://www.nessus.org/. (28 Feb. 2003).

[11] Caswell, Brian and Roesch, Marty. "Snort - The Open Source Network Intrusion Detection System." 24 Feb. 2003. URL: http://www.snort.org/. (25 Feb. 2003).

[12] Mackey, David. "Securing Windows 2000 Terminal Services." Windows 2000 Terminal Services. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/win2kts/maintain/optimize/secw2kts.asp. (25 Feb. 2003).

[13] "National Security Agency Security Recommendation Windows 2000 Guides Download Page." 23 Feb. 2003. URL: http://nsa2.www.conxion.com/win2k/download.htm. (25 Feb. 2003).

changed[14] which we are currently considering to further lock down the Terminal Servers from attempted compromise, although there have been no attempted logins to date and only one scan for 3389 into the network. However, we would have to update this immediately on all 35 WinNT systems as well as give this to our home users. This will probably be done through a self-extracting executable that will replace the current entry. This is where standardization has made things easier. All of our users have been given the same instructions to install the terminal client at home, and all of our Terminal Clients have been set up identically with their own configuration for use as thin clients. Instructions and changes can therefore be quickly adapted between platforms as well as between the home user setup and thin client setup.

2. Port 445 for workstations. This is for SMB shares in order to allow file sharing to workstations. This port has been enabled to allow file sharing outside of the firewall to trusted and restricted subnets.
3. Full communication behind the firewall. All servers are behind the firewall and enjoy full communication on a private VLAN.

The network is monitored using the Snort IDS configured on Windows 2000 workstation and monitoring on the interface (rather than with an IP address) in high speed mode. High speed mode allows the interception of suspicious packets with very low packet loss. The IDS monitors the trunk port allowing intrusion detection on multiple VLANS on a 100 Mb Cisco switch. The both the internal and external VLANS are monitored with the same IDS in this manner. Snort 1.9.1 with the current rules files detects logons to the Terminal Server from all external IP addresses. When a new subnet is detected and expected because a new home installation kit has been issued, it is correlated with a login in the security logs in Windows 2000 for the domain. In this manner, new Terminal Client home users can be differentiated from an attacker attempting to log in. This also allows us to keep track of Terminal Clients for licensing reasons. The IDS is also important in identifying any suspicious behavior of users emanating from the Terminal Server to other places on the Internet or local network.

Further efforts have been made to secure the Terminal Server from network intrusion attempts:

1. NetBIOS over TCP/IP has been disabled. This can be disabled by My Network Places->Properties->Interface Name->Properties->Internet Protocol (TCP/IP) Properties->Advanced Button->WINS Tab->Disable NetBIOS over TCP/IP.
2. While Group Policy Settings will be discussed further in the paper, I found that although Show Last Logged on username was disabled in Group Policy, it was not disabled on the Terminal Server. This apparently is a

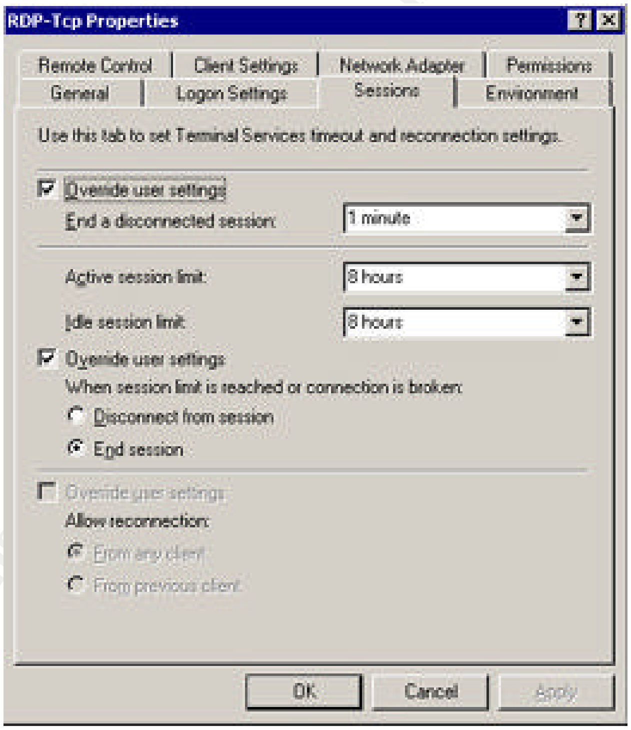
---

[14] "How to Change Terminal Server's Listening Port." 187623. 14 Oct. 2002. URL: http://support.microsoft.com/?kbid=187623. (26 Feb. 2003).

function by design[15]. I created a registry key file (.reg) that should be run after the installation of any Terminal Server to avoid the last logged on username from being displayed. If the registry key is not added, an attacker can see the last logged in user, giving them a starting point for a password guessing attack. The following registry key prevents the last logged on username from being displayed:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon]
"DontDisplayLastUserName"="1"
```

3. Terminal Server connections
    a. In order to keep data as private as possible, High encryption is enforced on the Terminal Server by Administrative Tools->Terminal Services Configuration->Connections->RDP-TCPIP Properties->General Tab->Encryption Level set to high.
    b. I found the following settings were used for Sessions after students and supervisors complained about session timeouts and I found a lot of sessions were disconnnected:



Use this tab to set Terminal Services timeout and reconnection settings.

☑ Override user settings
End a disconnected session: 1 minute

Active session limit: 8 hours
Idle session limit: 8 hours
☑ Override user settings
When session limit is reached or connection is broken:
○ Disconnect from session
● End session

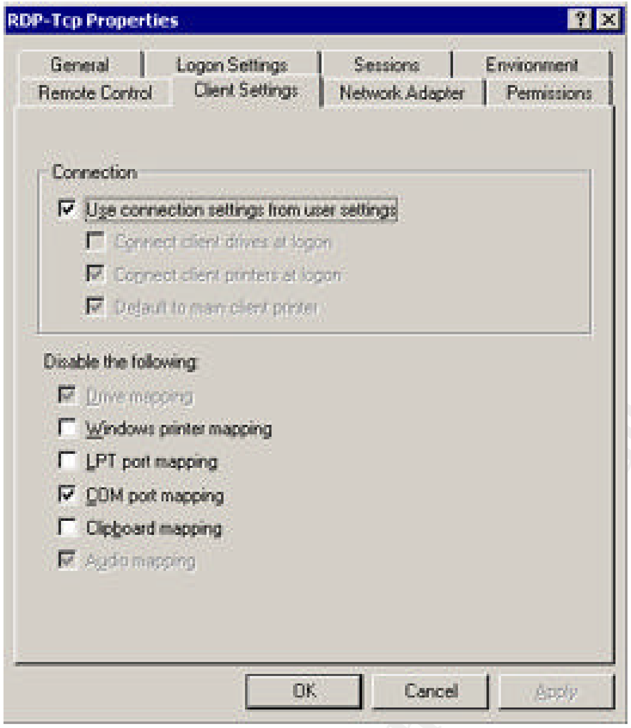
☐ Override user settings
Allow reconnection:
● From any client
○ From previous client

    c. The following client settings were used. These settings were modified because three of the thin clients required the use of a local printer. Terminal Server allows the use of a local printer by mapping

---

[15] “PRB: Policy to Not Display Last Username on RDP Client.” 193353. 14 Oct. 2002. URL: http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B193353. (26 Feb. 2003).

LPT ports. COM port mapping was uneceesary and so was disabled :



Connection

☑ Use connection settings from user settings

☐ Connect client drives at logon

☑ Connect client printers at logon

☑ Default to main client printer

Disable the following:

☑ Drive mapping

☐ Windows printer mapping

☐ LPT port mapping

☑ COM port mapping

☐ Clipboard mapping

☑ Audio mapping

d. The remainder of the settings were kept as default.

4. Microsoft's Baseline Security Analyzer was used to verify security settings on the server and to help make sure there were no points of exposure.

Terminal Server Lockdown

Terminal Services in Application mode is easily exploitable with no further settings changes. The modifications provided below eliminate many of the vulnerabilities that are faced by the Terminal Server. Using a combination of Group Policy and some of my student IT employees that have a strong ability to find weaknesses in controlled environments, I was able to come up with a minimally exploitable user environment that still felt friendly to students.

The first major concern was available software. The following software was installed:

1. Microsoft Office 2000 Premium Disk 1 and 2. This was installed using the termsrvr.mst Microsoft Transform File[16]. Unfortunately, Outlook 2000 has the ability to view the file system even when Group Policy restrictions on

---

[16] "OFF2000: How to Install Office 2000 on Windows 2000 Terminal Server." 224313. 6 Aug. 2002. URL: http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B224313. (28 Feb. 2003).

viewing drives are in place. Therefore, use of Microsoft Outlook is restricted to the "Student Outlook Users Group" on the Desktop and Start Menu and the default Everyone Read and Execute permissions are removed. The installation of this software was performed from the College's Office 2000 Administrative Share so that any changes made to the workstations or any security updates that required the installation point could be performed automatically without having to refer back to the original installation CDs.

2. Adobe Acrobat Reader. This software was installed because of its constant use on the Internet. Although it shows that it may remain incompatible with Windows 2000 Terminal Server if it is installed on the Windows 2000 prior to the installation of Terminal Services in Application mode, it functions well in the environment. This software did pose a considerable problem with users trying to install it (all be it unsuccessfully) because they were unaware of its existence due to customized Start Menus and Desktops. I ended up putting a shortcut to Acrobat Reader on the desktop so that the students would recognize that it was installed on the Server and stop trying to install it themselves.
3. Virus Protection. The University has a site license for McAfee anti-virus software. Because the machine in question is a server, NetShield, rather than a more appropriate desktop virus scanner was installed. The settings for this software cannot be modified. NetShield was configured for:
    a. Heuristics scanning to detect unknown viruses.
    b. Hourly virus DAT signatures updates were set up to keep the high-use system up to date.
    c. Connection to Alert Manager to make me aware of any virus detection.
    d. Automatic cleaning of infected files with deletion upon failure.
    e. Nightly virus scanning during off hours.
    f. Scanning of inbound, outbound, boot sector, and network drives.
    g. Scanning of compressed and archive files.
4. Macromedia Shockwave/Flash Player. This software was installed because it allowed students to play games during long evening hours. There was a noticeable difference in attempted software installations after this plug-in was installed. Many times I've found that by steering the direction of use and advertising software's existence, I can manipulate users into less damaging solutions. This was also the case with instant messaging (IM) software. IM software has had many vulnerabilities and installing the software would add greatly to the administrative overhead of having to keep the software up to date. Instead, I had directions written for using JAVA-based IM software and distributed it too all of my users, not just on the Terminal Server users. The direction included how to create a link to the JAVA-based IM software and most users found this was an acceptable solution to locally installed IM software. Yahoo IM required a plug-in be installed. I installed this on the server to avoid exclusion of any single IM package.

5. Building Management software was also installed which functions on a local front-end and a SQL Server 2000 backend. The directory was locked down from changes and the desktop icon was only made accessible to a group called “Building Database Students”.
6. While WinZip is present on our workstations, it is noticeably absent from the Terminal Server. I intentionally did not install the software because the only data that is needed for students to perform their jobs is on our shared drives in an uncompressed form. The only use the students would have for an unzipping program in this case would be to download installable files. While this is not a restriction that would totally prevent the download and attempted installation, I’ve found countless Zip files for software in the Recycle Bin on the student’s desktops. This policy acts as more of a deterrent than a complete block. Additional blocks listed below act far more comprehensively than not having unzipping software.
7. Disabling the automatic updating of the software also prevents some issues where the software may ask the user to update.

Group Policy

I used Group Policy to perform many of the restrictions that were put into place. Group Policy is an excellent platform for distributing controlled settings because it allows and administrator to literally add a new system under the same organizational unit, and with some small changes that have been and will be described, enjoy the same extensive restrictions on the machine with no further effort. This allows for a very quick expansion of services as well as a platform for disaster recovery and contingency. The sections of Group Policy that will be described were specifically altered for the Terminal Server from our standard domain Group Policy Settings to further restrict the user environment. The settings for the domain’s Group Policy for workstations follow very closely to the Secure Workstation template[17]. In cases where there is a difference, the Group Policy settings for the domain are actually more restrictive than the template. The Group Policy settings that are pertinent to the Terminal Server lockdown that are different than the standard securews.inf template are listed below.

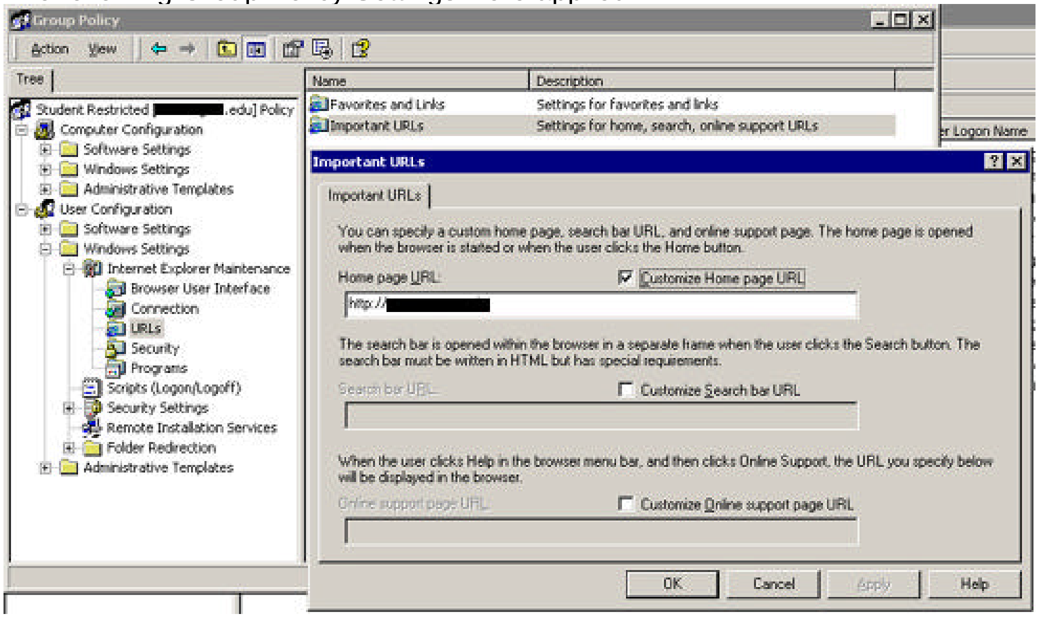
An organizational unit was created called “Terminal Servers”. Underneath that organizational unit, two more organizational units were created call “Users” and “Computers”. A process called policy filtering exists where a top level organizational unit has a Group Policy attached to it and that policy applies down to all organizational units within it. A Group Policy is then applied on a subordinate organizational unit with more restrictive settings and the top level settings plus the more restrictive settings are then applied to the objects in the lower level organizational unit. In this case, I wanted to use the Computer settings from our domain, but use a different set of User settings than supplied by the domain. I created and attached a Group Policy to the “Users” organizational

---

[17] “Predefined security templates.” Windows Server 2003 Product Documentation. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/sag_SCEdefaultpols.asp. (28 Feb. 2002).

unit under “Terminal Server”. I blocked policy inheritance to the “Users” organizational unit so that the domain Group Policy would not affect the Terminal Server Users and the Group Policy I attached “Student Restricted” could not be overridden by our domain policy. Because “Student Restricted” was attached to the “Users” folder, it did not affect the Terminal Server which inherited the default domain policy. The “Student Restricted” Group Policy made this entire process possible by giving me direct control over all aspects of the user’s environment.

The following Group Policy Settings were applied:



Name	Description
Favorites and Links	Settings for favorites and links
Important URLs	Settings for home, search, online support URLs

Important URLs

You can specify a custom home page, search bar URL, and online support page. The home page is opened when the browser is started or when the user clicks the Home button.

Home page URL: ☑ Customize Home page URL

http://[redacted]

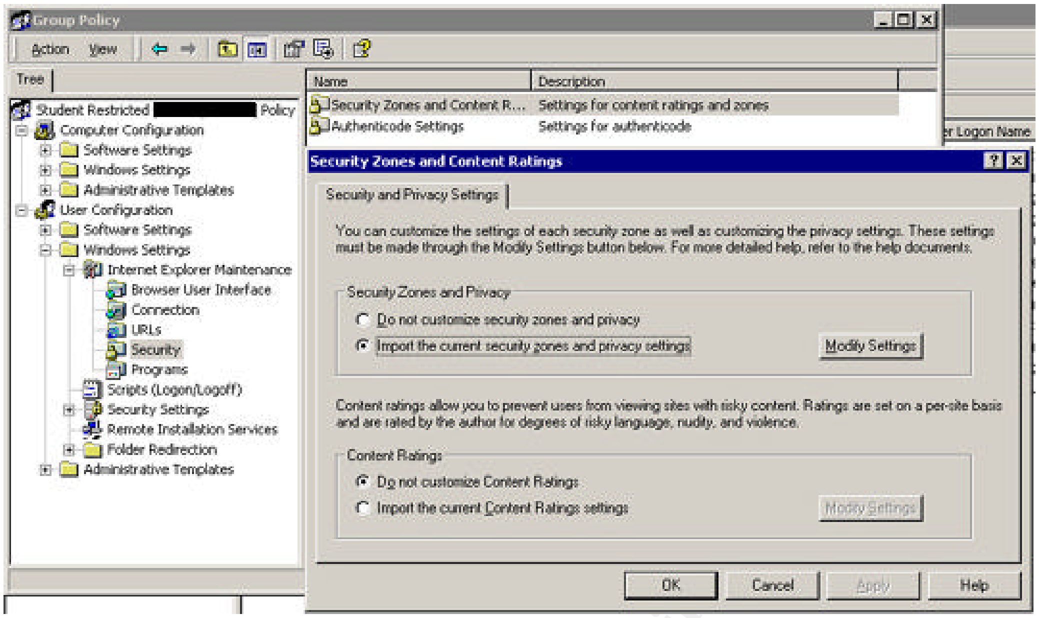
The search bar is opened within the browser in a separate frame when the user clicks the Search button. The search bar must be written in HTML but has special requirements.

Search bar URL: ☐ Customize Search bar URL

When the user clicks Help in the browser menu bar, and then clicks Online Support, the URL you specify below will be displayed in the browser.

Online support page URL: ☐ Customize Online support page URL

1. The homepage was set to the University’s main page. This became necessary because students unintentionally (or intentionally) set the default homepage to pornographic websites and gambling sites. A supervisor called and asked me to reset the homepage to that account. I did it through Group Policy making the change permanent rather than having to redo it every time it was changed in the future.



Name	Description
Security Zones and Content R...	Settings for content ratings and zones
Authenticode Settings	Settings for authenticode

Security Zones and Content Ratings

Security and Privacy Settings

You can customize the settings of each security zone as well as customizing the privacy settings. These settings must be made through the Modify Settings button below. For more detailed help, refer to the help documents.

Security Zones and Privacy

○ Do not customize security zones and privacy

● Import the current security zones and privacy settings

Modify Settings

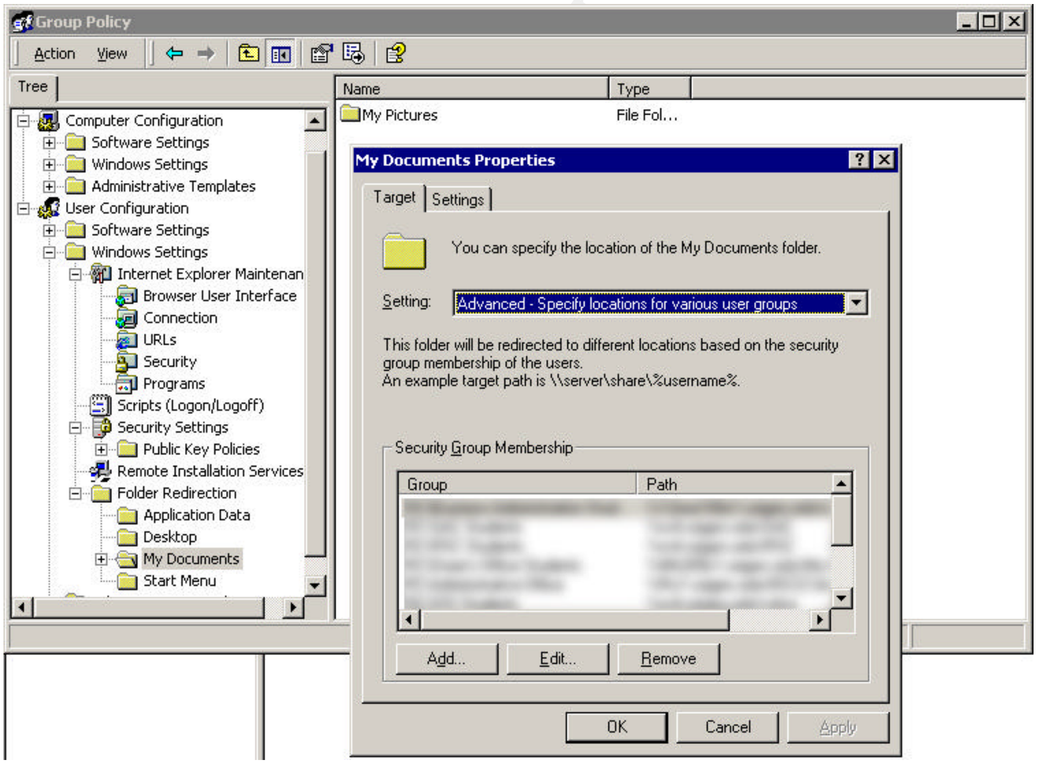
Content ratings allow you to prevent users from viewing sites with risky content. Ratings are set on a per-site basis and are rated by the author for degrees of risky language, nudity, and violence.

Content Ratings

● Do not customize Content Ratings

○ Import the current Content Ratings settings

2. Under Security Zones and Content Ratings. I imported the current security zone information from our domain. The is the typical "Medium" setting with some intranet trusts.



Name	Type
My Pictures	File Fol...

My Documents Properties

Target | Settings

You can specify the location of the My Documents folder.

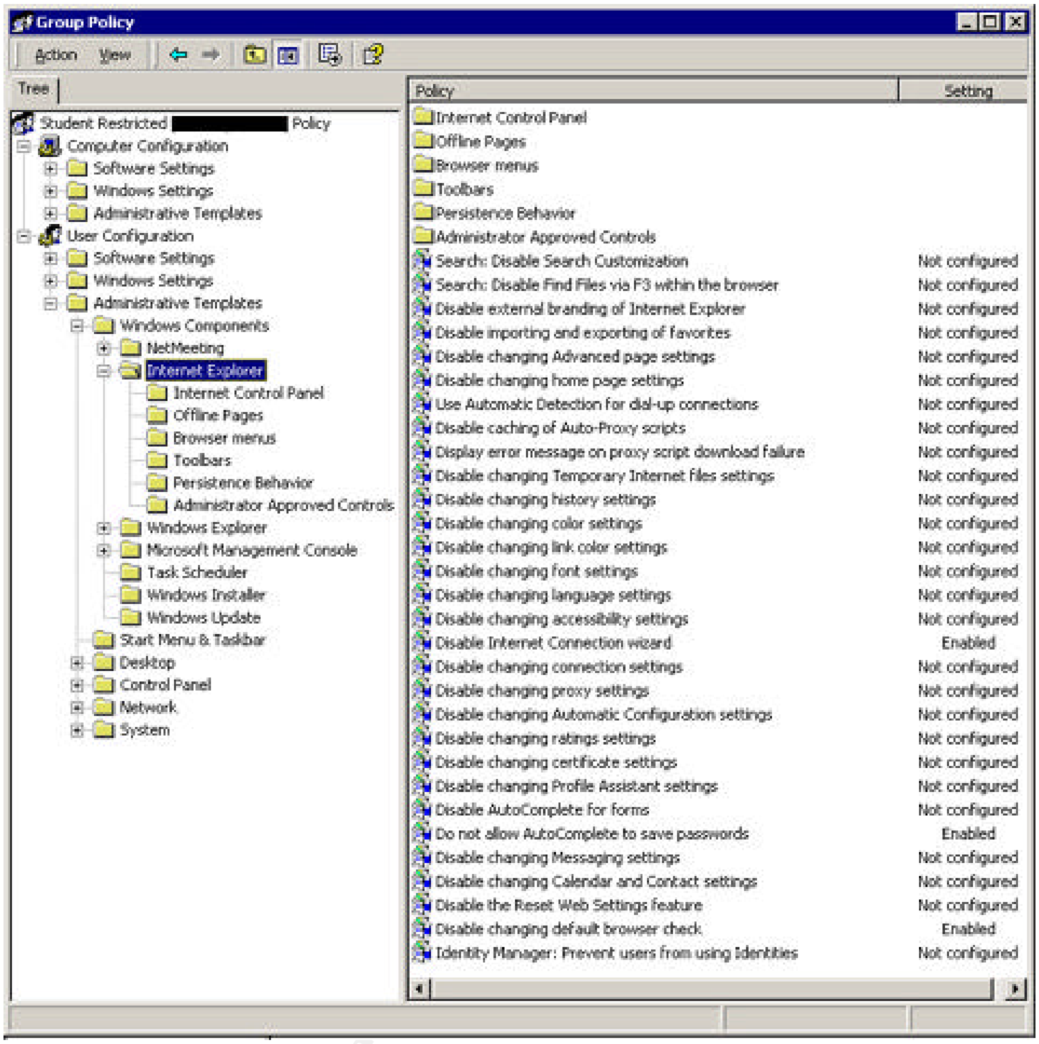
Setting: Advanced - Specify locations for various user groups

This folder will be redirected to different locations based on the security group membership of the users.
An example target path is \\server\share\%username%.

Security Group Membership

Group	Path
[redacted]	[redacted]

3. Under My Documents properties, I set in place the first of the crucial settings that makes this entire setup possible. I selected the pull down menu “Advanced – Specify Locations for Various User Groups”. I redirected the students’ My Documents folders to specific shares on the Terminal Server (or elsewhere) based on group membership. This was done because I would eventually lock out access to both drives on the server through Group Policy preventing any drive access, but enabling access to the correct folders by using network shares. This also allowed me the freedom to move the folder off the server to another server if space became an issue, prevented users traversing up from directories, and removed the necessity of using Explorer or My Computer to work with files.
    a. Under the settings tab, it was very important to uncheck “Grant the user exclusive rights to My Documents”. At first this remained checked and caused undesirable results.
    b. It was also important to “Leave the folder in the new location when the policy is removed or the folders would be redirected and copied to bizarre locations in the domain if any mistake was made with the policy.

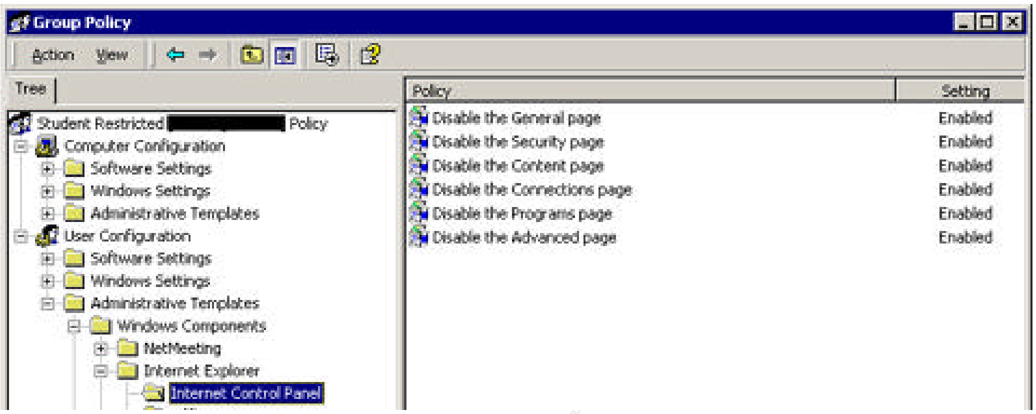


Policy	Setting
Internet Control Panel	
Offline Pages	
Browser menus	
Toolbars	
Persistence Behavior	
Administrator Approved Controls	
Search: Disable Search Customization	Not configured
Search: Disable Find Files via F3 within the browser	Not configured
Disable external branding of Internet Explorer	Not configured
Disable importing and exporting of favorites	Not configured
Disable changing Advanced page settings	Not configured
Disable changing home page settings	Not configured
Use Automatic Detection for dial-up connections	Not configured
Disable caching of Auto-Proxy scripts	Not configured
Display error message on proxy script download failure	Not configured
Disable changing Temporary Internet files settings	Not configured
Disable changing history settings	Not configured
Disable changing color settings	Not configured
Disable changing link color settings	Not configured
Disable changing font settings	Not configured
Disable changing language settings	Not configured
Disable changing accessibility settings	Not configured
Disable Internet Connection wizard	Enabled
Disable changing connection settings	Not configured
Disable changing proxy settings	Not configured
Disable changing Automatic Configuration settings	Not configured
Disable changing ratings settings	Not configured
Disable changing certificate settings	Not configured
Disable changing Profile Assistant settings	Not configured
Disable AutoComplete for forms	Not configured
Do not allow AutoComplete to save passwords	Enabled
Disable changing Messaging settings	Not configured
Disable changing Calendar and Contact settings	Not configured
Disable the Reset Web Settings feature	Not configured
Disable changing default browser check	Enabled
Identity Manager: Prevent users from using Identities	Not configured

4. Disable Internet Connection Wizard->Enabled
    a. A crafty student managed to get into Internet Connection Wizard and tried to set a proxy server for the Internet Explorer which prevented all the other users on that particular account from using the Internet that night. This setting prevents that from happening again.
5. Do not allow autocomplete to save passwords->Enabled.
    a. This policy is very important because multiple users share accounts on this machine. If this policy were not enabled, the user's accounts would be open for use by anyone using the account.
    b. While the use of multiple users with the same username is considered a security risk, it is a necessity. There are roughly 250 student employees that use these systems. This roster changes every semester not including new hires and firings. I experimented with delegation of user management to a few offices which proved

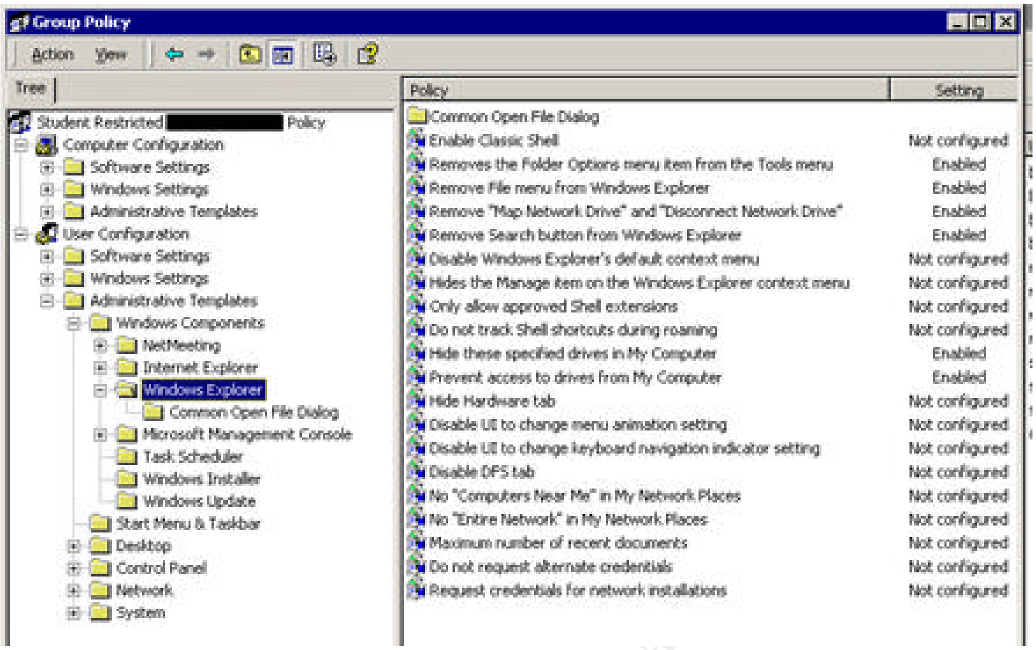
to cause more security risks than it mitigated. Because of the failure of such a policy, I went back to using multi-user accounts with passwords that change every semester and once in the summertime. This policy is also supplemented by the fact that extensive written logs are kept of students on duty in the buildings, as well as a student supervisor's log of what each student was working on for the evening. These logs can and have been used to review misuse when necessary.

6. Disable changing default browser check->Enabled.



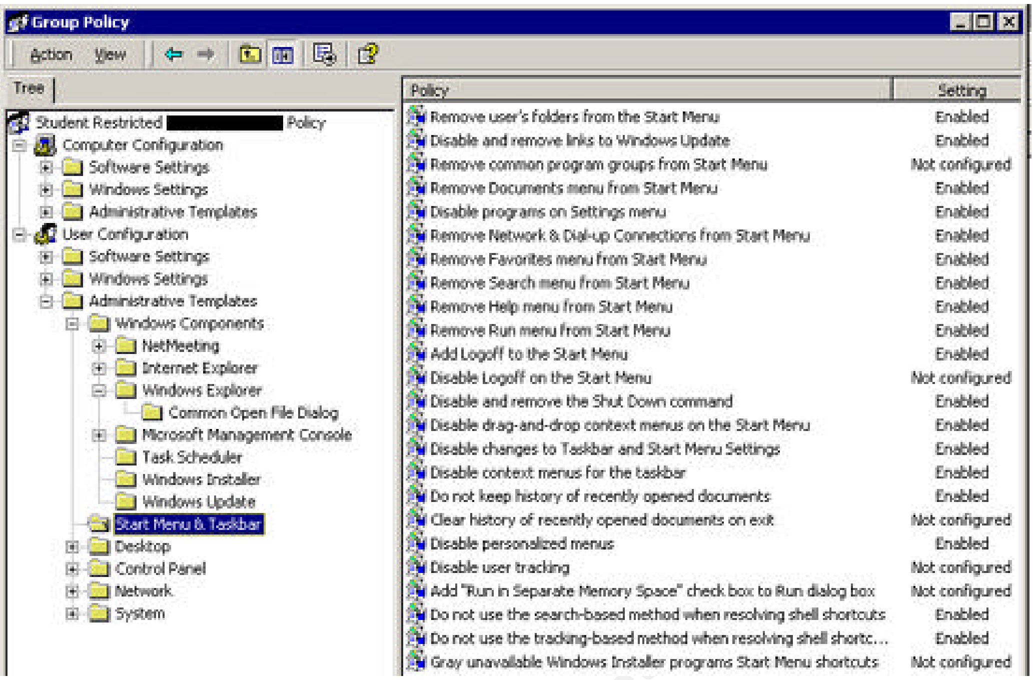
Policy	Setting
Disable the General page	Enabled
Disable the Security page	Enabled
Disable the Content page	Enabled
Disable the Connections page	Enabled
Disable the Programs page	Enabled
Disable the Advanced page	Enabled

7. Internet Control Panel->All Items Enabled.
    a. Initially some of the items were not configured. Every single item under each page that was left open for students to change did get changed at some point.
    b. In order to prevent these changes, I simply blocked access to the pages to change the settings for IE.



Policy	Setting
Common Open File Dialog	
Enable Classic Shell	Not configured
Removes the Folder Options menu item from the Tools menu	Enabled
Remove File menu from Windows Explorer	Enabled
Remove "Map Network Drive" and "Disconnect Network Drive"	Enabled
Remove Search button from Windows Explorer	Enabled
Disable Windows Explorer's default context menu	Not configured
Hides the Manage item on the Windows Explorer context menu	Not configured
Only allow approved Shell extensions	Not configured
Do not track Shell shortcuts during roaming	Not configured
Hide these specified drives in My Computer	Enabled
Prevent access to drives from My Computer	Enabled
Hide Hardware tab	Not configured
Disable UI to change menu animation setting	Not configured
Disable UI to change keyboard navigation indicator setting	Not configured
Disable DFS tab	Not configured
No "Computers Near Me" in My Network Places	Not configured
No "Entire Network" in My Network Places	Not configured
Maximum number of recent documents	Not configured
Do not request alternate credentials	Not configured
Request credentials for network installations	Not configured

8. Hide these specified drives in My Computer->Enabled
    a. Restrict All Drives.
9. Prevent Access to these drives in My Computer->Enabled.
    a. Restrict All Drives.
    b. What makes this particular policy the cornerstone of this setup is that with C: drive not available, programs will not install for the users because the folders used to install the software such as temp cannot be found or written to.



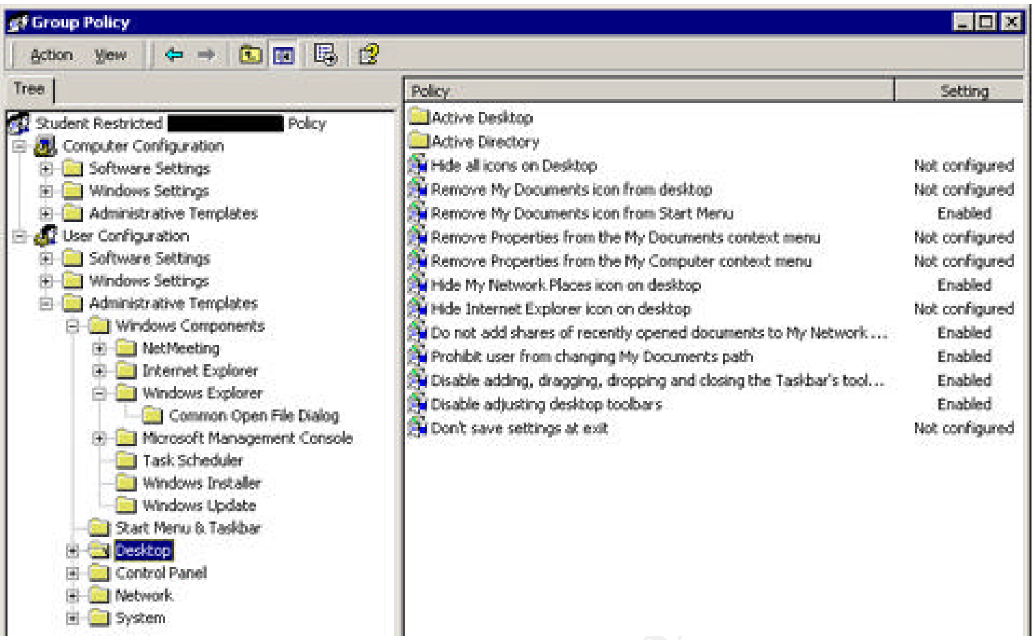
Policy	Setting
Remove user's folders from the Start Menu	Enabled
Disable and remove links to Windows Update	Enabled
Remove common program groups from Start Menu	Not configured
Remove Documents menu from Start Menu	Enabled
Disable programs on Settings menu	Enabled
Remove Network & Dial-up Connections from Start Menu	Enabled
Remove Favorites menu from Start Menu	Enabled
Remove Search menu from Start Menu	Enabled
Remove Help menu from Start Menu	Enabled
Remove Run menu from Start Menu	Enabled
Add Logoff to the Start Menu	Enabled
Disable Logoff on the Start Menu	Not configured
Disable and remove the Shut Down command	Enabled
Disable drag-and-drop context menus on the Start Menu	Enabled
Disable changes to Taskbar and Start Menu Settings	Enabled
Disable context menus for the taskbar	Enabled
Do not keep history of recently opened documents	Enabled
Clear history of recently opened documents on exit	Not configured
Disable personalized menus	Enabled
Disable user tracking	Not configured
Add "Run in Separate Memory Space" check box to Run dialog box	Not configured
Do not use the search-based method when resolving shell shortcuts	Enabled
Do not use the tracking-based method when resolving shell shortc...	Enabled
Gray unavailable Windows Installer programs Start Menu shortcuts	Not configured

10. Start Menu and Task Bar
    a. Remove the user's folder from the Start Menu
        i. Enabled
        ii. This policy hides the programs that are launchable from the top of the Start Menu.
        iii. This is only done as a precaution so that if software is installed that installs icons on the Start Menu, I don't have to go and uninstall this from each profile.
    b. Disable and remove links to Windows Update
        i. Enabled
        ii. This is an Administrator Only function, but it's better not to have it available on the Start Menu anyway.
    c. Remove Documents Menu from the Start Menu
        i. Enabled
        ii. This policy was enabled because when I was a student, administrators use to leave the Documents folder available. If I could find my way using Microsoft Word to an executable using the Open option in Word, I would open it in Word. The file would not execute, but it would put the shortcut to the executable in the Documents folder and then I could use this link to run the executable. Although this is not possible because of the drive restrictions, a crafty student might find some other way of using this.
    d. Disable Programs on Settings Menu
        i. Enabled

        ii. Prevents Control Panel, Printers, and Network and Dial-up Connections from running.
        iii. This is a very important setting in that it prevents a lot of user misuse.
    e. Remove Network and Dial-up Connections from the Start Menu.
        i. Enabled
        ii. Prevents users from running Network and Dial-up Connections.
        iii. While this is another Administrator only function in the important areas, there is some functionality that would cause problems if a student were to change settings.
    f. Remove Favorites Menu from Start Menu
        i. Enabled
        ii. This is just an addition menu on the Start Menu and is done as more of a personal preference.
    g. Remove Search Menu from Start Menu
        i. Enabled
        ii. Search can be misused very easily from getting names from Active Directory, finding system files, or mining for useful data in documents.
    h. Remove Help from Start Menu
        i. Enabled
        ii. While Help is more robust in Windows 2000, Help can be used to access menus and programs that I have chosen to lock out. If any lockout was missed, the program would be available through Help.
    i. Remove Run from the Start Menu
        i. Enabled
        ii. There is no need for this command on this system and could only be misused.
    j. Add Logoff to Start Menu
        i. Enabled
        ii. This command was put into place after our initial setup. Students would disconnect instead of logging out, which kept multiple sessions of the same user running on the server. This added to the memory load at around 16MB of memory per user. The next user would also pick up the disconnected session, rather than starting a new one.
        iii. Adding this feature and providing some documentation to students minimizes disconnections.
    k. Disable and remove Shut Down command
        i. Enabled
        ii. Regular users cannot shut down a server, but this was removed because it was unnecessary.
    l. Disable drag and drop context menus on the Start Menu
        i. Enabled

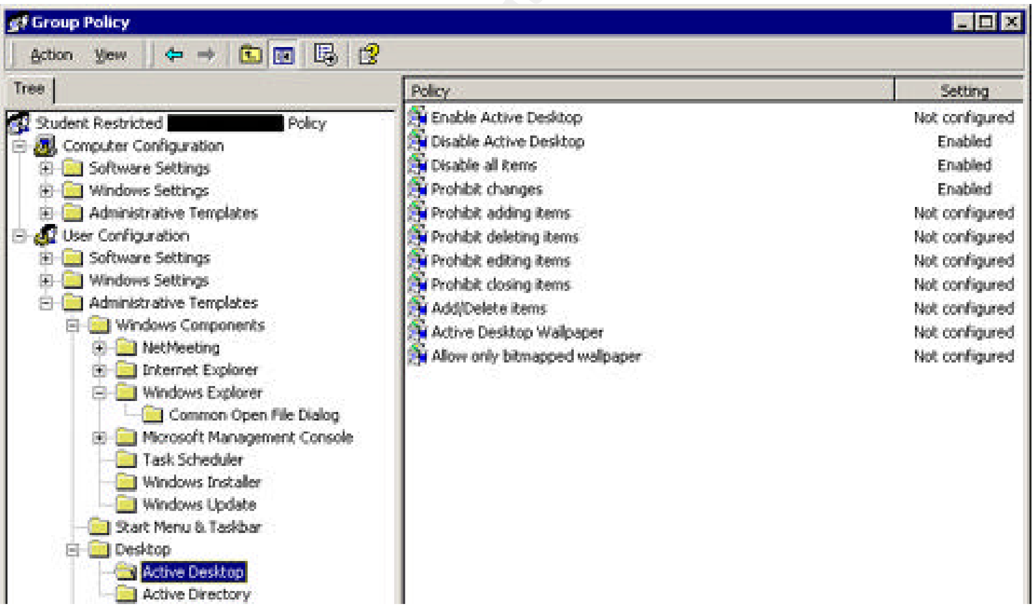
        ii. This prevents users from changing the Start Menu

m. Disable changes to the Task Bar and Start Menu Settings
    i. Enabled
    ii. Because the Terminal Server is being used with multiple users on individual accounts, allowing modifications such as this would only serve to annoy users.
n. Disable context menus for the Task Bar
    i. Enabled
    ii. This prevents use of any programs in the Task Bar such as Clock and NetShield. NetShield is the only program available and there's no reason why any user would need access to the program through this route.
o. Do not keep history of recently used documents
    i. Enabled
    ii. Redundancy to remove "Remove Documents Menu form Start Menu".
p. Disable personalized menus
    i. Enabled
    ii. Users complained that they could no longer find programs, and so this was removed to prevent rarely used programs form disappearing.
q. Do not use shell-based method when resolving shell shortcuts.
    i. Enabled
    ii. This would be a major security problem if the drives were not locked down. A user could create a .lnk file, import it to the system and then allow it to search the entire drive for a program to run. I used to use this trick as a student as well to run explorer (and other programs) when it was locked out of the available menus at the college I attended.
r. Do not use tracking-based method when resolving shell shortcuts.
    i. Enabled
    ii. See shell-based method above.



Policy	Setting
Active Desktop	
Active Directory	
Hide all icons on Desktop	Not configured
Remove My Documents icon from desktop	Not configured
Remove My Documents icon from Start Menu	Enabled
Remove Properties from the My Documents context menu	Not configured
Remove Properties from the My Computer context menu	Not configured
Hide My Network Places icon on desktop	Enabled
Hide Internet Explorer icon on desktop	Not configured
Do not add shares of recently opened documents to My Network ...	Enabled
Prohibit user from changing My Documents path	Enabled
Disable adding, dragging, dropping and closing the Taskbar's tool...	Enabled
Disable adjusting desktop toolbars	Enabled
Don't save settings at exit	Not configured

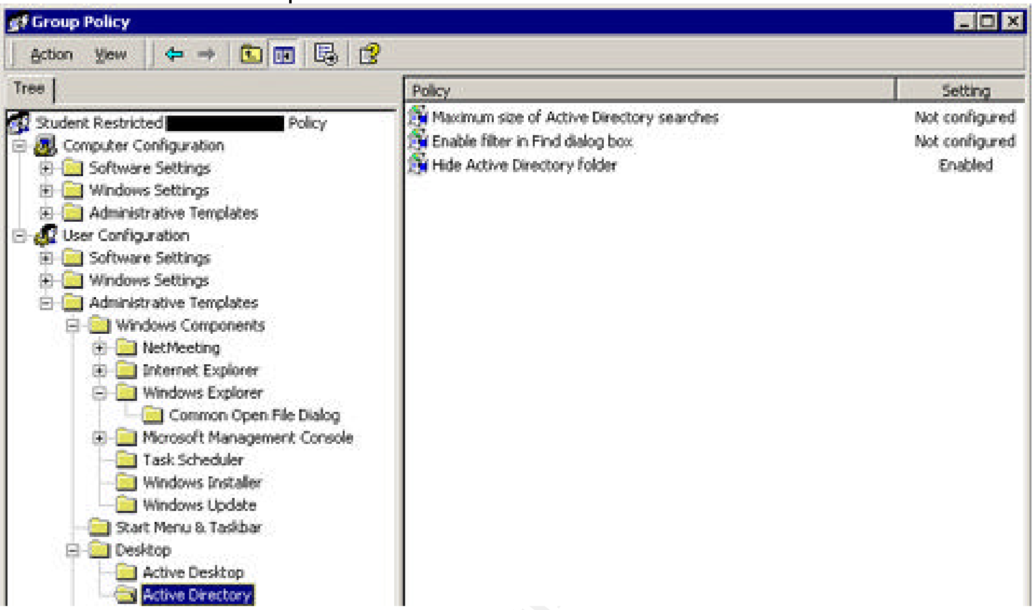
11. Desktop
    a. Hide My Network Places icon on desktop
        i. Enabled.
        ii. Students have a great tendency to snoop, this limits what can be seen.



Policy	Setting
Enable Active Desktop	Not configured
Disable Active Desktop	Enabled
Disable all items	Enabled
Prohibit changes	Enabled
Prohibit adding items	Not configured
Prohibit deleting items	Not configured
Prohibit editing items	Not configured
Prohibit closing items	Not configured
Add/Delete items	Not configured
Active Desktop Wallpaper	Not configured
Allow only bitmapped wallpaper	Not configured

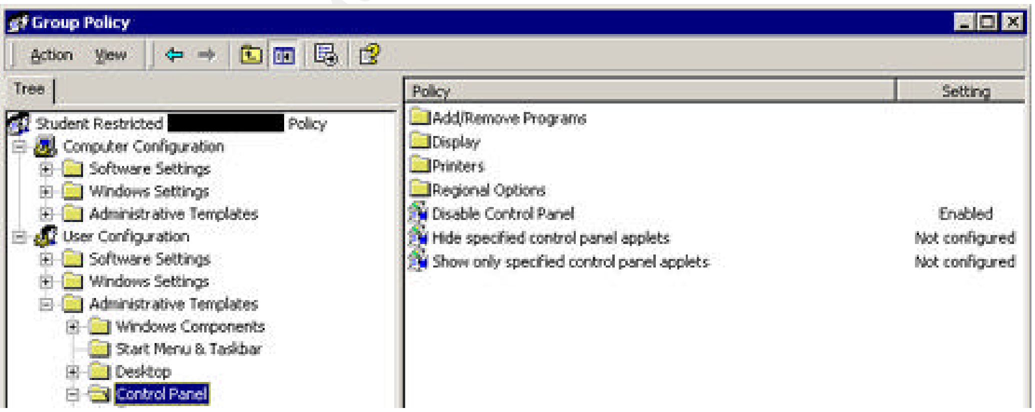
    b. Active Desktop

        i. The three items listed effectively block use of the Active Desktop. This feature is also blocked in Terminal Services configuration Server Settings. Active Desktop allows for a rich desktop environment with wallpaper, HTML, and scripts. All three items are not necessary and have the potential for exploitation.



Policy	Setting
Maximum size of Active Directory searches	Not configured
Enable filter in Find dialog box	Not configured
Hide Active Directory folder	Enabled

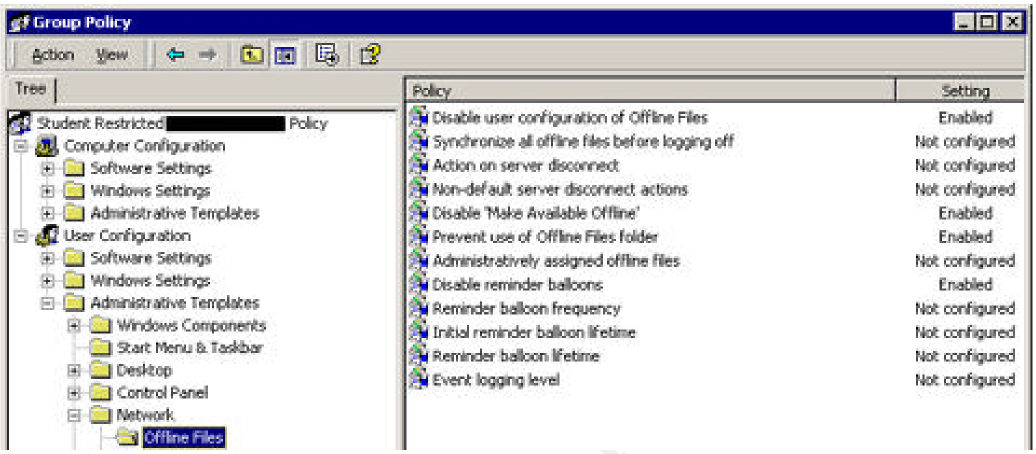
12. Active Directory
    a. Hide Active Directory folder
    b. This was hidden to prevent user snooping and also to prevent students from adding printers using Active Directory lookup. Being able to add printers in this fashion is helpful to staff in the domain, but students usually add the printers and cause confusion for staff who don't know where the printing is coming from.



Policy	Setting
Add/Remove Programs	
Display	
Printers	
Regional Options	
Disable Control Panel	Enabled
Hide specified control panel applets	Not configured
Show only specified control panel applets	Not configured

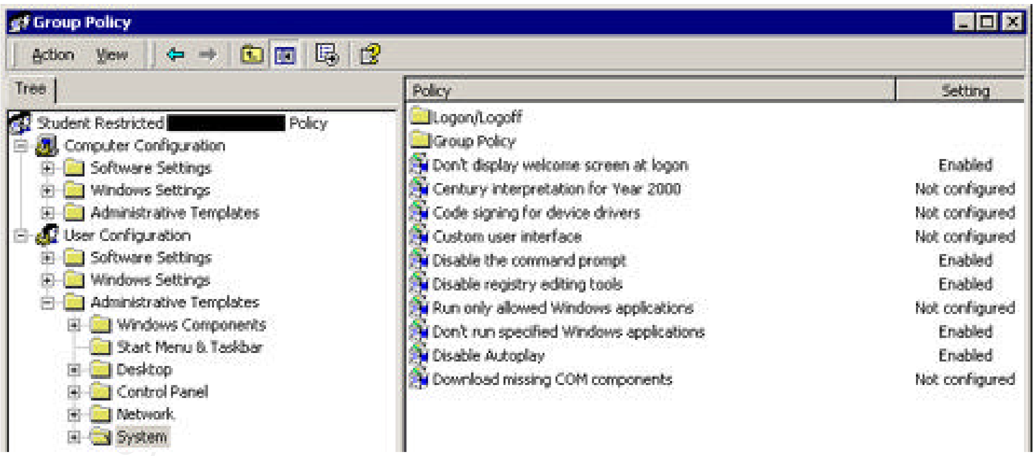
13. Disable Control Panel
    a. The Control Panel is disabled.

b. The Control Panel is an excellent environment to cause problems and change settings. This area of Windows shouldn't be left open to most users if it can be avoided.
c. Although the options within Control Panel can be blocked for extra granularity, blocking Control Panel and Help prevents the use of these items.



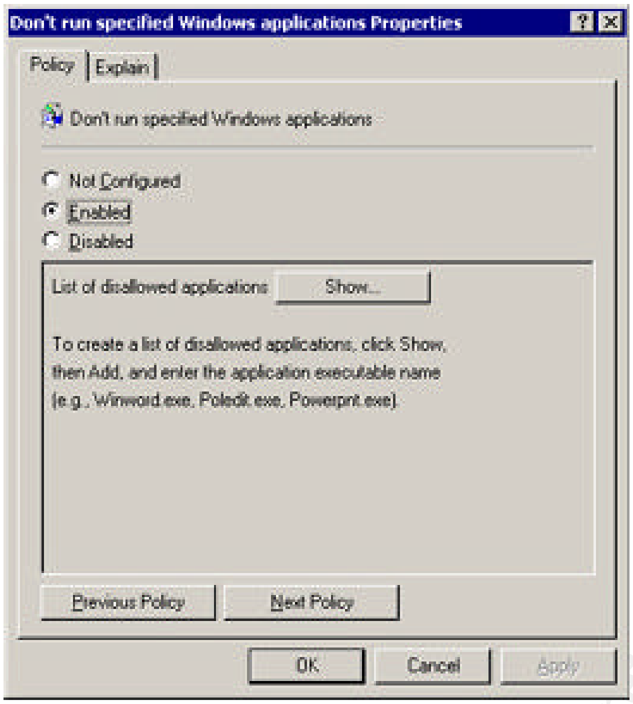
Policy	Setting
Disable user configuration of Offline Files	Enabled
Synchronize all offline files before logging off	Not configured
Action on server disconnect	Not configured
Non-default server disconnect actions	Not configured
Disable 'Make Available Offline'	Enabled
Prevent use of Offline Files folder	Enabled
Administratively assigned offline files	Not configured
Disable reminder balloons	Enabled
Reminder balloon frequency	Not configured
Initial reminder balloon lifetime	Not configured
Reminder balloon lifetime	Not configured
Event logging level	Not configured

14. Offline files have been disabled. There are one or two students who kept finding ways to try to enable Offline Files and Folders. Although there was no reason to do this, it may have been out of boredom. I finally disabled this in Group Policy after finding this setting enabled, even though the shares would not allow offline use.



Policy	Setting
Logon/Logoff	
Group Policy	
Don't display welcome screen at logon	Enabled
Century interpretation for Year 2000	Not configured
Code signing for device drivers	Not configured
Custom user interface	Not configured
Disable the command prompt	Enabled
Disable registry editing tools	Enabled
Run only allowed Windows applications	Not configured
Don't run specified Windows applications	Enabled
Disable Autoplay	Enabled
Download missing COM components	Not configured

15. Disabling the command prompt and registry editing tools prevent many forms of misuse.



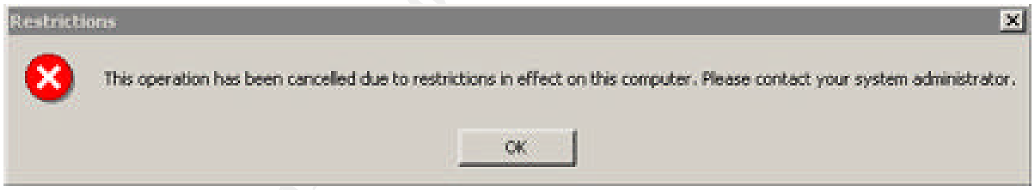
Don't run specified Windows applications

○ Not Configured
● Enabled
○ Disabled

List of disallowed applications

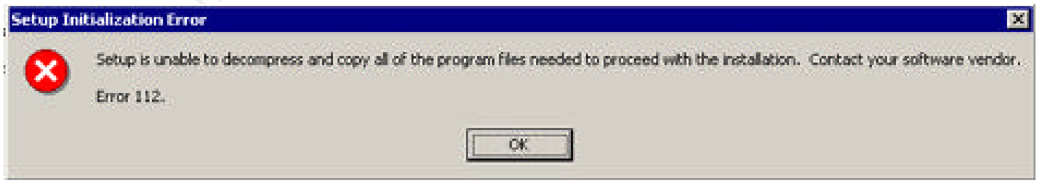
To create a list of disallowed applications, click Show, then Add, and enter the application executable name (e.g., Winword.exe, Poledit.exe, Powerpnt.exe)

16. Don't run specified Windows applications would be more of a psychological operation than one of function. Before AOL responded to frustrated administrator's complaints that AOL Instant Messenger could be installed without Administrative privileges, I created a top 25 list of annoying programs users tried to install including all IM software, Napster, Adobe Acrobat Reader, RealPlayer, etc. and placed the names in the list of disallowed applications.



This operation has been cancelled due to restrictions in effect on this computer. Please contact your system administrator.

   a. When the program was run, the user would receive this message screen. Students would get the picture that they were not allowed and most usually gave up.

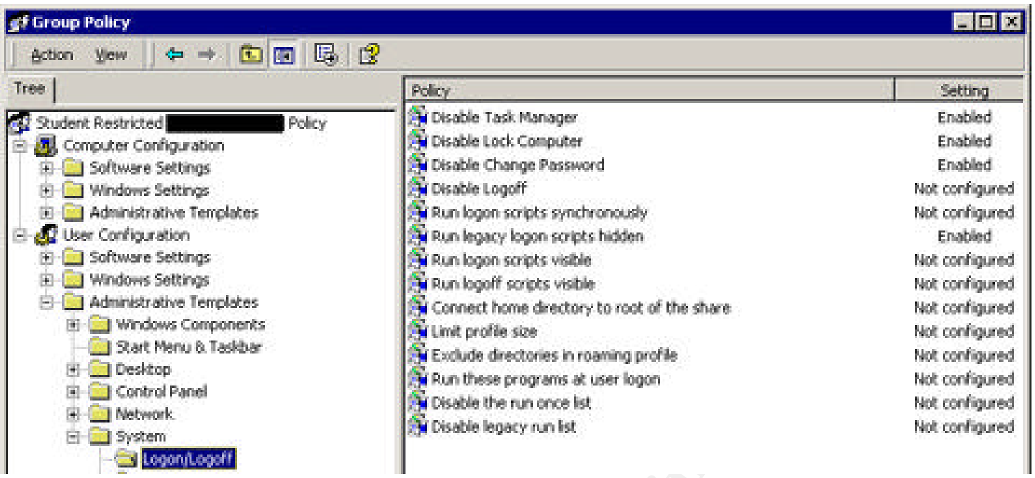


Setup is unable to decompress and copy all of the program files needed to proceed with the installation. Contact your software vendor.

Error 112.

   b. Because the C: drive was disabled for users in Group Policy, even if the name of the software wasn't on the list, the students would receive above message due to a failed temporary folder installation.

The first example is more preferable because it sends a clear message; the second message would lead students to continue to try.



- Student Restricted [redacted] Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates
  - User Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates
      - Windows Components
      - Start Menu & Taskbar
      - Desktop
      - Control Panel
      - Network
      - System
        - Logon/Logoff

Policy	Setting
Disable Task Manager	Enabled
Disable Lock Computer	Enabled
Disable Change Password	Enabled
Disable Logoff	Not configured
Run logon scripts synchronously	Not configured
Run legacy logon scripts hidden	Enabled
Run logon scripts visible	Not configured
Run logoff scripts visible	Not configured
Connect home directory to root of the share	Not configured
Limit profile size	Not configured
Exclude directories in roaming profile	Not configured
Run these programs at user logon	Not configured
Disable the run once list	Not configured
Disable legacy run list	Not configured

17. Logon/Logoff
    a. Disabling Task Manager, and Change password are important to prevent some annoying forms of misuse including students changing multi-user passwords or trying to see or kill current processes running on the their view of the task manager. Terminal Server also prevents user from killing critical processes. In Terminal Server, users are only allowed to view their own processes, only an administrator can view all processes running for a system.
    b. Running legacy logon scripts hidden given students less of an idea where their logon scripts (and therefore Domain Controllers) reside.

After Snapshot

The largest security threat was faced from the inside rather than from a network or hacker-based attack. There was no evidence that any of the systems had ever been damaged by a virus or by network intrusion although it is possible that this had happened and we weren’t aware of it. The use of a firewall, intrusion detection system, virus scanning software, port blocking on thin clients, configuration guides and log analysis drastically reduced the threat from outside attack even further than had already been done to the original systems. The inside threat, while usually not malicious, was one that presented (and continues to present) an exceptional challenge and was one of the largest factors in making the decision to begin this undertaking. All of the system damage and compromise that was detected was due to internal users. Most of the settings and policies that were put into place were the direct result of an issue that manifested from the old systems. Following a Defense in Depth strategy helped mitigate many of the risks faced by the thin clients and the Terminal Server.

With past issues in mind, I set up test workstations and asked a few of the Helpdesk students from our office with a penchant for finding ways around policies to try and break the system. The students reacted happily to the challenge presented and began trying to break the system I had built. The initial and ongoing reaction to the thin client workstation was that is was very tightly secured and not worth the trouble. The Terminal Server did have a few vulnerabilities initially. Internet Explorer was initially not as locked down through Group Policy as it should have been. One of the students succeeded in rendering it unusable by changing the proxy settings. Some folder's permissions were not set correctly and students were able to delete files and folders they should not have been able to get into. The settings were adjusted to prevent this. It was important to iron out the feel of the system before rolling it out to its true target audience so that buy-in would be as successful as possible. The most important aspect of creating the locked down system was that the students would accept the system as restrictive as it was without growing to dislike it; that dislike led to the original security issues and damage that took place on the older systems. The Helpdesk students' suggestions were very important for designing a feel to the system which would foster an atmosphere of acceptance.

Only a small amount of documentation and training turned out to be necessary for the student employees. We created a sheet that included hyperlinks to the University's Student Code of Conduct, Computing Use Policies, and our additional rules for conduct on the systems. We kept the information to a minimum, but with links, it gave us the ammunition we needed for accountability that was sorely lacking.

The staff were given shared drives to the Terminal Server shares appropriate to their office called a T: drive. T: drives pointed to the overall share for their offices which exposed the subdirectories that served as the student's My Documents folders. The staff were pleased that they would be able to interact with the students' work at this level and it also allowed the staff to monitor files that were added to the folders taking the appearance of supervision away from the IT staff.

The students were pleased with the new units. It was slightly awkward explaining that the processing was taking place on the server and not on the workstations. However, the students received it well because their thin clients were extremely fast. In fact, regular staff complained that the new student system was much faster than their own desktop computers. Computers that went down as frequently as a few times a month in some cases have not required any work since their creation. Current complaints about the system are related to a lack of floppy drives, no speakers for listening to music, and a lack of desktop publishing software on the Terminal Server. It has proven difficult to explain that the system was never designed to be a desktop publishing platform because it only transmits 256 colors to the thin client.

The overall security of the domain has been greatly enhanced on multiple levels due to this project:

1. The domain is now 100% Windows 2000, allowing symmetrical, automatic, late-evening patching using Microsoft Systems Management Server 2.0[18] throughout the domain.
2. Windows NT 4.0 clients are locked down in a manner that it is unlikely (although never impossible) that they will be compromised. This does not lessen the need for random checks of equipment to make sure nothing has become an issue, although I am comfortable with the amount of monitoring these systems get.
3. The Terminal Server resides behind a firewall with intrusion detection on both the inside and outside of the firewall.
4. The thin clients reside on VLANs that are monitored by intrusion detection software.
5. The VLANs that the systems reside on are scanned using vulnerability scanning software during business hours on a quarterly basis.
6. The Terminal Server is locked down enough that no new software can be installed and issues on the Terminal Server are extremely rare. Printing has become the largest annoyance in that on rare occasions, a document fails to print and the print spool needs to be manually emptied and restarted.
7. We have accommodated all 35 workstations without a large quantity of lag time on the Terminal Server.
8. The Terminal Server is protected by virus scanning software that is updated hourly with heuristics scanning also enabled to detect unknown viruses. Because of the high use of the Terminal Server, viruses are blocked on the average of one a day.
9. The system is backed up each evening using a remote backup agent with weekly offsite storage of tapes.
10. The workstations are easily clonable and can be replaced due to hardware failures with an hour of the initial call.
11. IT staff are familiar with the Windows 2000 environment which gives them better ability to answer calls into the Help Desk than the original WinNT systems. The IT staff also spend less time dealing with problems related ot these systems which given them more time to focus on more important issues.

Conclusion

The system satisfies the original goals that it was established for (listed above). Our biggest problem currently is laying the boundaries within which the system can and cannot perform. It has become a challenge to provide computing resources to match the complex demands of the staff and students while meeting the IT department's goals of security, reliability, and ease of use. This project was successful not only because it incorporated many of the resources,

---

[18] "Microsoft Systems Management Server." URL: http://www.microsoft.com/smserver/default.asp. (28 Feb. 2003).

concepts, and strategies outlined in the GSEC course and many other security resources that have sprouted up in the past few years that were not available at the time in the same depth when the original NT 4.0 systems were installed; but also because it was designed with a clear set of criteria and goals.

References

1. "nt-netbios-nullsession (170)." URL: http://www.iss.net/security_center/static/170.php. (20 Feb. 2003).
2. "Restricting Information Available to Anonymous Logon Users." 1434748. 1 Aug. 2001. URL: http://support.microsoft.com/default.aspx?scid=KB;en-us;q143474. (20 Feb. 2003).
3. Nordahl-Hagen, Petter. "Offline NT Password & Registry Editor, Bootdisk." 26 Jan. 2003. URL: http://home.eunet.no/~pnordahl/ntpasswd/. (20 Feb. 2003).
4. Reilly, Michael D. "Setting NT System Policies." Getting Started with NT. 5621. July 1999. URL: http://www.winnetmag.com/Articles/Index.cfm?ArticleID=5621. (20 Feb. 2003).
5. "Appendix F - Windows 2000 Server and Professional Systems Requirements." Windows 2000 Server Deployment Planning Guide. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/reskit/deploy/part7/sdgappf.asp. (21 Feb. 2003).
6. "Terminal Services Client Cannot Connect to a Server Running 128-bit Encryption." 257894. 11 Oct. 2002. URL: http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B257894. (22 Feb. 2003).
7. "How to Lock Down Windows NT and Internet Explorer 4.01 Desktop." 198771. 1 Oct. 2002. URL: http://support.microsoft.com/default.aspx?scid=kb%3ben-us%3b198771. (23 Feb. 2003).
8. "NT 4 Lockdown" 27 Jan. 2003. URL: http://www.snakegully.nu/tech/nt4lockdown.html. (23 Feb. 2003).
9. "Microsoft Baseline Security Analyzer." Tools and Checklists. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/Security/tools/tools/MBSAHome.ASP. (25 Feb. 2003).
10. "Nessus." URL: http://www.nessus.org/. (28 Feb. 2003).
11. Caswell, Brian and Roesch, Marty. "Snort - The Open Source Network Intrusion Detection System." 24 Feb. 2003. URL: http://www.snort.org/. (25 Feb. 2003).
12. Mackey, David. "Securing Windows 2000 Terminal Services." Windows 2000 Terminal Services. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/win2kts/maintain/optimize/secw2kts.asp. (25 Feb. 2003).

13. "National Security Agency Security Recommendation Windows 2000 Guides Download Page." 23 Feb. 2003. URL: http://nsa2.www.conxion.com/win2k/download.htm. (25 Feb. 2003).
14. "How to Change Terminal Server's Listening Port." 187623. 14 Oct. 2002. URL: http://support.microsoft.com/?kbid=187623. (26 Feb. 2003).
15. "PRB: Policy to Not Display Last Username on RDP Client." 193353. 14 Oct. 2002. URL: http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B193353. (26 Feb. 2003).
16. "OFF2000: How to Install Office 2000 on Windows 2000 Terminal Server." 224313. 6 Aug. 2002. URL: http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B224313. (28 Feb. 2003).
17. "Predefined security templates." Windows Server 2003 Product Documentation. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/sag_SCEdefaultpols.asp. (28 Feb. 2002).
18. "Microsoft Systems Management Server." URL: http://www.microsoft.com/smserver/default.asp. (28 Feb. 2003).