Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

Daniel B. Schultz

GIAC Certified Windows Security Administrator (GCWN)
Practical Assignment
Version 3.1 (revised April 8, 2002),
Option 2 – Securing Windows 2000 With Security Templates

"Securing the Administrative Workstation with Security Templates"

Abstract

The workstations used by Systems Administrators (sysadmins) are a nexus of
sensitive information and software tools, which can compromise network security
or wreak havoc within the network, if misappropriated or misused. Further, these
workstations usually do not benefit from the same physical security as the
servers administered from them. Indeed, such workstations are often laptop PCs,
placing them at still greater risk of compromise. For these reasons and others,
administrative workstations merit special attention from security professionals, in
order to safeguard the machines and especially their contents. This document
presents options for securing these workstations' configurations, data and
communications, by way of security templates.

1. Description of System

The computer under consideration in this paper is a Windows 2000 Professional workstation, used by a systems administrator (sysadmin) of a corporate Windows 2000 Server and Active Directory infrastructure; all server and client systems have been installed as or upgraded to Windows 2000 or later. This workstation has a minimal configuration: 192MB of RAM, a 8GB hard disk, CD-ROM drive, floppy drive, and one network interface card. The simplicity of the system suits its role as a computer from which other computers are administered, as well as making it a less attractive target for theft. As is typical of such workstations, this one does not benefit from any special physical security other than that which protects the main entrance to the building where the sysadmin works.

Although beyond the reach of the security templates discussed in this document, two firmware changes were made to the administrative workstation to ameliorate the mediocre physical security: the workstation has been configured to require a power-on password, and has been configured to disallow booting from removable media.

The operating system has been upgraded to Windows 2000 Service Pack 3. Several hotfixes were applied, which were introduced after Service Pack 3, as shown below:
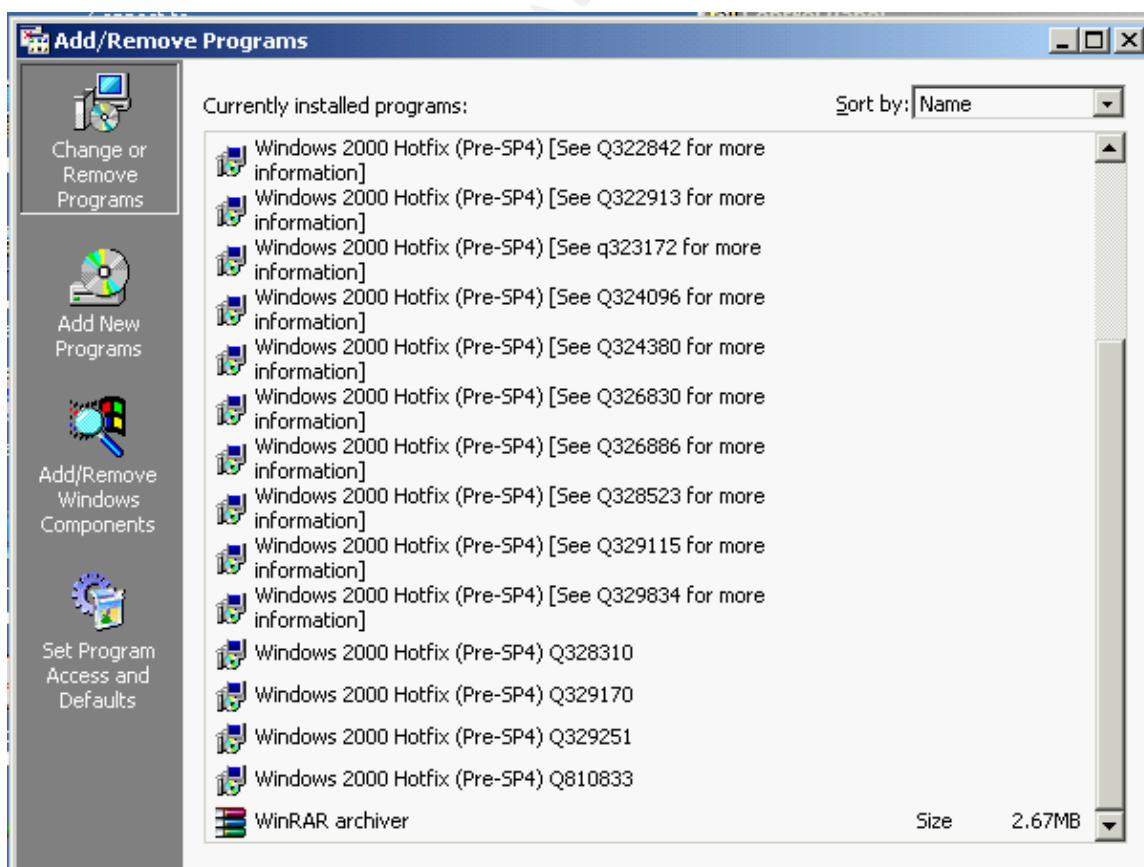
Other installed software includes the Windows 2000 Administration Tools Package (Adminpak.msi), which includes the updates for that package that were a part of the Windows 2000 Service Pack 1. The workstation also includes Adobe Acrobat version 4 and the Citrix ICA Client, version 6.31.1051.

The use of the Citrix application-serving solution is attractive for use on this administrative workstation for security reasons, as well as for the efficiency required of so minimal a system. Serving applications from a Citrix "farm" has made unnecessary the local installation of Microsoft Office. The vulnerabilities in Office, both those that are known and those that are yet to discovered (or introduced), are deemed too risky for a workstation which conducts many tasks with Domain Administrator privileges or greater rights.

Also installed is Solarwinds Engineer Edition, a suite of network analysis and reporting tools. Solarwinds is intended mostly for use in managing network hardware such as routers and switches, but also collects sensitive information about Windows servers and workstations, including hostnames, IP addresses and SNMP configurations.

Complementing the use of Citrix application serving and the use of the sysadmin's home directory in keeping potentially sensitive files off of local storage, the workstation will make use of folder redirection, enforced by way of Group Policy. There is a usage policy governing this system which prohibits the storage of sensitive documents. However, it is understood that adherence to this usage policy may be imperfect. The redirection of key folders assists the sysadmin by making it convenient to place data files in an approved location, and by redirecting files that applications might automatically place into those key folders. [1]

Other measures protect the filesystem, including the use of Windows 2000's Encrypting File System, and the use of Window Washer version 4.8 for the removal of temporary files and other historical data which are generated during the sysadmin's use of the workstation.

The remaining noteworthy aspect of the configuration is that both Domain Users and Domain Administrators have been removed from the local users and local administrators groups, respectively. The sysadmin uses a local account that belongs to the local users group for to login to the workstation. This same domain account belongs to Domain Administrators. This combination allows the sysadmin to perform privileged tasks in the domain, while remaining faithful to the principle of least privilege in his local rights. This arrangement is the norm, although the he must, on occasion, use the local Administrator account for some tasks. A somewhat less disconcerting option, using the "Run As" service to

---

[1] Security Operations Guide for Windows 2000 Server. Microsoft Corporation, 2002. 171

perform all administrative functions, does not work with the Administrative tools that are pertinent to Active Directory. [2]

2. Checklist or Template

Having reviewed the Common Criteria as presented in the *Microsoft Windows 2000 Security Configuration Guide* (both the baseline and high-security templates), the *Consensus Baseline Security Settings* from the Center for Internet Security, the *Guide to Securing Windows 2000 Group Policy* from the National Security Agency (NSA), and the templates provided by the National Institute for Standards and Testing (NIST), as well as *NIST's Special Publication 800-43, Systems Administration Guidance for Securing Microsoft Windows 2000 Professional System*, this author elected to use the "NISTWin2kProGold.inf" security template. [3, 4, 5, 6] This template was one of several offered by NIST and is referred to hereinafter as the "Gold template" or "Gold standard template."

There is much common heritage in the templates offered by the agencies and organizations mentioned above, but NIST provided the most thorough and most explanatory documentation, to accompany the Gold standard template. [7] Although the other potential sources provided documentation that might bolster the understanding of a particular security setting, NIST's documentation, as provided in Appendices B and G of the Gold standard documentation, was the most thorough and understandable.

The confidence inspired by such a thorough disclosure was the primary reason for choosing NIST's Gold template. It is something of a leap of faith to install a predefined security template; NIST's documentation minimized the number of items which had to be blindly trusted.

This template will be implemented via Group Policy for the Organizational Unit (OU) that contains this administrative workstation and other workstations that fulfill the same role. Overall, the intended purposes of applying the template are to ensure that every workstation in the OU is reasonably resistant to illegitimate

---

[2] The reader will notice that while e.g., the Services shortcut's p roperties can be modified to run as a different user, the Active Directory User and Computers' shortcut cannot be so modified.
[3] URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/issues/W2kCCSCG/W2kSCGc4.asp (20 Feb. 2003).
[4] URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/issues/w2kccscg/default.asp (20 Feb. 2003).
[5] Souppaya, M., Harris, A., McLarnon, M., and Selimis, N. Systems Administration Guidance for Securing Microsoft Windows 2000 Professional System, NIST Special Publication 800-43. National Institute for Standards and Testing, November, 2002.
[6] Haney, Julie M. Guide to Securing Windows 2000 Group Policy: Security Configuration Tool Set, Version 1.1.1. National Security Agency, July 22, 2002.
[7] FAQ #2 at URL: http://csrc.nist.gov/itsec/guidance_W2Kpro.html (20 Feb. 2003).

attempts to access it via local or network login, is hardened against software exploits, and is configured to retain a useful audit trail in the event of a security incident.

Further, the template provides a baseline against which the workstation can be periodically compared. Also, the governance of the OU by a Group Policy Object ensures that changes to the template can be implemented rapidly, as the role of the workstation or the risk it faces change.

There are a few key risks contemplated in the foregoing general statement of purpose, which must be mitigated, considering the circumstances and role of the administrative workstation.

For instance, the workstation is not physically secured against local login attempts; the "console" is exposed. Therefore, settings relevant to login attempts, account lockouts and passwords will be especially important, because of the open, office setting in which the workstation resides.

In implementing this security template, there is also an expectation that security will be standardized and hardened for those settings that govern which services are run at startup or are capable of being started, and for the settings that govern the context in which these services run. Stipulation of service accounts – the credentials under which a Windows 2000 service starts – is not a feature of the Gold template or Group Policy. However, Group Policy can be used to change the "Startup Type" of a service to Disabled, Manual or Automatic.

These services are potential entry points for malicious exploits. [8] Although the sysadmin will have only local user rights on his workstation (that is, the Domain Administrators group will be removed as a member of the local Administrators group), he will exercise Domain Administrator or greater rights within Active Directory, by virtue of his account's inclusion in the Domain Administrators group. Any exploit successfully launched against services running on the workstation might be able to leverage the sysadmin's Domain Administrator privileges, were he to logon with them as a matter of course. This is a key scenario that deployment of the templates seeks to prevent.

3. Security Settings

This section of the document highlights the nature and value of security settings which the Gold template establishes, and which are relevant to the goal of

---

[8] E.g., the notorious SNMP flaws and exploit, URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-006.asp (20 Feb. 2003).

securing the administrative workstation. Where appropriate, the settings are grouped for the sake of efficiency, brevity and coherence. [9]

3.1 Password Settings

As mentioned above, the workstation is not physically secured, making necessary the following settings regarding password and account policy.

- Enforce password history: 24 passwords remembered

- Maximum password age: 90 days

- Minimum password age: 1 day

- Minimum password length: 8 characters

- Passwords must meet complexity requirements: Enabled

The effect of these five settings is to mandate a password that is sufficiently novel, long and complex to frustrate brute force and dictionary attacks, especially against the local or domain Administrator accounts, which cannot be locked out by repeated login failures. Further, the settings for maximum and minimum password ages ensure, respectively, that old passwords are effectively retired from use (authorized and otherwise) and that new passwords cannot be generated in rapid succession until it is permissible to reuse a prior password.
Account Settings

- Account lockout duration: 15 minutes

- Account lockout threshold: 3 invalid attempts

- Reset lockout count in: 15 minutes

Together with strong passwords, these settings make it impractical to guess or brute-force a password, either manually or programmatically. This is an important setting for an unsecured machine.

3.2 Audit Policy

Successes and failures will be logged to the Event Viewer for the following events or activities.

- Account logon events

---

[9] The descriptions of the security settings are drawn largely from the comments accompanying the catalog of the Gold template settings in NIST Special Publication 800-43. B-2 - B-34.

- Account management

- Logon events

These settings will produce an informative audit trail of authentications to the workstation, as well as changes to any of its built-in groups or users. [10]

3.3 User Rights

- Access computer from network: Users, Administrators

- Deny access to computer from network: Guests

- Log on locally: Users, Administrators

- Shut down the system: Users, Administrators

The foregoing settings dictate that only two accounts can access this workstation, locally or remotely: the local Administrator account, and the domain account that is an Administrator in the domain but is only used as needed, via secondary logon. As mentioned in the section "Description of System" above, these are the only two user accounts configured on the workstation; other references to domain groups and users have been removed.

3.4 Security Options

- Additional restrictions for anonymous connections: No access without explicit anonymous permissions

The primary purpose of the restrictions on anonymous connections is the prevention of an exploit which allows an unauthenticated user to generate a list of the user accounts that are active on the workstation.

Two other parameters amongst the Security Options are pertinent here:

- Manage auditing and security log: Administrators

- Clear virtual memory pagefile when system shuts down: Enabled

The first ensures that the policy established at the OU level serves to protect the integrity of the audit trail; the second removes the potentially sensitive data

---

[10] URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsnetserver/proddocs/server/516.asp (20 Feb. 2003). This source provides a detailed explanation of this setting and the many event types it creates.

stored in the Windows pagefile whenever the system shuts down – another safeguard in the event the workstation or its hard disk is stolen.

All clients and servers with which the sysadmin might communicate via SMB are running Windows 2000 or later. This allows the following settings to be enabled.

- Digitally sign client communication (when possible): Enabled

- Digitally sign server communication (when possible): Enabled

- LAN Manager (LM) Authentication Level: Send NTLMv2 response only

The digital signature settings thus applied to SMB packets are intended to thwart "man-in-the-middle" attacks. [11] The LAN Manager setting prohibits use of LAN Manager's cryptographically weak password-hashing scheme. [12]

- Number of previous logons to cache: 1

This setting allows the sysadmin to login with cached credential one time, in the event that the workstation cannot locate a domain controller. The Gold template acknowledges the small security risk involved. [13]

- Prevent users from installing print drivers: Enabled

The sysadmin may make use of the local administrator account if a new print driver is needed. There is no need to expose this vulnerability during daily operations.

- Digitally encrypt secure channel data (when possible): Enabled

- Digitally sign secure channel data (when possible): Enabled

These settings will cause the workstation to sign and encrypt all traffic exchanged with domain controllers. In this case, the traffic contains a Domain Administrator's authentication data and should be protected from interception or eavesdropping.

3.5 Event Log Settings

---

[11] URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsnetserver/proddocs/server/568.asp (20 Feb. 2003).
[12] Smith, Randy Franklin. "Why NT Passwords are Weak." Windows & .Net Magazine. Winter 2000. URL: http://www.win2000mag.net/Articles/Index.cfm?ArticleID=15893 (20 Feb. 2003).
[13] NIST Special Publication 800-43. B-9.

The following settings ensure that event logs will contain enough historical information to be useful, and that only the sysadmin has access to them.

- Max application log size: 80MB

- Max security log size: 80MB

- Max system log size: 80MB

- Restrict guest access to application log: Enabled

- Restrict guest access to security log: Enabled

- Restrict guest access to system log: Enabled

3.6 System Services Settings

The Gold template recommends the following settings, in order to minimize the number of running but unneeded services on the workstation, which reduces the range of possible remote exploits. [14] Each relevant service is listed, followed by the suggested status and the author's comments, as needed.

- Computer Browser: Disabled

The sysadmin will be unable to locate servers or workstations via Network Neighborhood, and will have to rely on knowing the DNS names or IP addresses of those computers.

- FTP Publishing Service: Disabled

The availability of centralized, shared storage makes running an FTP server locally, unnecessary.

- Internet Connection Sharing: Disabled

This service is unnecessary and presents a potential for abuse, as it essentially creates a rogue proxy server on the network.

- NetMeeting RDS: Disabled

This service has been an avenue of exploit in the past. [15]

- Remote Registry Service: Disabled

---

[14] Security Operations Guide for Windows 2000 Server. 173.
[15] URL: http://support.microsoft.com/default.aspx?scid=kb%3ben-us%3b299796 (20 Feb. 2003).

This setting prevents remote manipulation of the local registry, which is desirable for the administrative workstation. (This setting will be disabled during the evaluation and testing section of this document, as it is reported to interfere with the Microsoft Baseline Security Analyzer.) [16]

- **SMTP service: Disabled**

This service is largely unneeded and has been subject to compromise at least twice. [17]

- **SNMP service: Disabled**

Multiple flaws in almost every vendor's implementation of SNMP were arguably the biggest security news of 2002. [18] However, disabling this service will break many of the Solarwinds modules installed on the sysadmin's workstation.

- **Telnet Server service: Disabled**

Vulnerabilities in Telnet services have been classified as high, because of the wide access this remote console provides to the targeted computer; telnet runs in the Local System context on Windows 2000. [19]

- **WWW Publishing Service: Disabled**

Web server service is not needed on this workstation, and a privilege-elevation exploit for this service was reported as recently as October 2002. [20]

3.7 File Permission Settings

The Gold template ensures consistent and secure NTFS permissions for many folders present in a default installation of Windows 2000 Professional. In some instances, members of the Users group are allotted read and execute permissions on system and application files but are prevented from changing, deleting or creating files. Other directories contain data sufficiently sensitive that

---

[16] NIST Special Publication 800-43. B-13.
[17] URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-011.asp and
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms01-037.asp (20 Feb. 2003).
[18] URL: http://www.cert.org/advisories/CA-2002-03.html (20 Feb. 2003).
[19] URL: http://www.cert.org/advisories/CA-2002-03.html and
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms02-004.asp (20 Feb. 2003).
[20] URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-062.asp (20 Feb. 2003).

the Gold template will allow access only to Administrators and the System account.

This section of the document describes key permissions settings within the Gold template, as they relate to securing an administrative workstation.

The %ProgramFiles% and %SystemRoot% directories, which by default are the "Program Files" and "WINNT" directories respectively, restrict Users to the following permissions:

- Read and Execute

- List Folder Contents

- Read

These permissions are propagated to files and subdirectories within the directories, although the Gold template will override that propagation on many subfolders and executables, in order to set more stringent permissions. The WINNT directory is the focus of many of the Gold template settings; relevant examples follow.

- \WINNT\dllcache: Only Administrators and System have rights, in order to protect the file cache used by Windows File Protection
- \WINNT\system32\GroupPolicy: Users have only List, Read and Execute rights, keeping Group Policy settings safe

- \WINNT\system32\regedit.exe *and* regedt32.exe: These two registry editors are unavailable to Users, although other copies in other locations could still be executed.

- \WINNT\$NtServicePackUninstall$: Each service pack or hotfix typically creates an uninstall folder. Users are not given rights to uninstall them.

- \WINNT\repair: This folder contains backup copies of the SAM files, which could be subjected to cryptanalytic attack. [21] Users have no rights at this folder.

- \WINNT\security: This folder contains security template files. Malicious changes to a template could compromise security if the template were later applied or reapplied. Therefore, the Users group is granted no rights here.

---

[21] This is possible against an *unencrypted* SAM database, with products such as LC4, from @stake.

- \WINNT\tasks: This folder is restricted to Administrator access, because the Task Scheduler service runs with Local System privileges and draws its list of tasks from this folder. [22]

- \WINNT\system32\ftp.exe *and* irftp.exe *and* tftp.exe: Only Administrators and System have any rights to these executables, owing to their intended use of moving files to and from the workstation. The malicious utility of tftp.exe, for example, was a key in the spread of the Nimda virus. [23]

The Gold template also mandates a few key permissions changes to files on %SystemDrive% (typically C:\), intended to protect the integrity of the boot process:

- NTLDR: This file runs a check at boot to verify the integrity of NTOSKRNL.EXE.

- NTDETECT.COM: Gathers hardware information for NTLDR. [24]

- BOOT.INI: Can be tampered with to redirect the boot process to another OS installation.

3.8 Registry Settings

Most of the registry settings codified by the Gold template target the "CurrentControlSet" and the "ControlSet0x" keys. The template reserves Full Control permissions for Administrators and System, occasionally granting Full Control to Creator-Owner for the subkeys created for individual users. Read rights are granted to Users or Authenticated Users. CurrentControlSet keys impinge upon Group Policy, auditing, networking services and other key components. [25] For these reasons and others, protecting this key and its subkeys is a worthy aspiration.

Of interest is a registry key for which the Gold template removes all rights for all but Administrators and System: the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NetDDE key. This key regulates the NetDDE and NetDDE DSDM services. These services provide a hidden window and trusted shares, used within and between machines for

---

[22] A vulnerability in scheduled task handling was fixed in Windows NT 4.0, but this folder still must be protected. For background, see URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/fq99-051.asp (20 Feb. 2003).

[23] URL: http://vil.nai.com/vil/content/v_99209.htm (20 Feb. 2003).

[24] This file was one target of the Melissa virus. URL: http://www.symantec.com/avcenter/venc/data/w97m.melissa.u.html (20 Feb. 2003).

[25] A good example of the mischief accomplishable with free reign in CurrentControlSet can be found at URL: http://is-it-true.org/nt/atips/atips28.shtml (20 Feb. 2003).

interprocess communication. [26] Creation of new NetDDE shares could enable direct communication with another computer, so this key is guarded carefully by the Gold template. [27]

4. Application, Testing and Evaluation of the Template

4.1 Applying the Template

The author applied the template in the manner described by the Microsoft article #315416. [28] The template was deployed on a short series of empty test Organizational Units, and the Application Log was checked for an Event ID 1704 from the source "SceCli", indicating that the Group Policy objects were applied successfully.

The author then imported the Gold template to the single Group Policy object linked to the OU (admin-PCs) containing the administrative workstations (HOTH and VITRIOL). The new settings were verified by a quick check of the Password Policy in the Group Policy MMC, as well as the Application Log.

The deployment of security templates via Group Policy is intended to become the default, automated method for distributing security settings to computers as they are added to Active Directory domains, regardless of the role the computer fulfills. Group Policy will also be the method of choice for the automated distribution of changes to security templates.

The security settings propagated by this new Group Policy object will certainly change over time. Some of those changes may be in direct response to a security vulnerability, and time will be of the essence in deploying those new settings. As Group Policy is the method of choice (here) for ensuring uniformity in security settings, all computers will have to poll a domain controller for Group Policy changes on an interval that is deemed suitable for a response to a new threat.

For Windows 2000 Professional systems like the sysadmin's workstation, the default refresh interval for Group Policy is ninety minutes, with a randomization factor of up to 30 minutes. The randomization is intended to prevent too many computers from simultaneously polling a domain controller for Group Policy refresh. [29]

---

[26] For background, see URL: http://www.atstake.com/research/advisories/2001/a020501-1.txt (20 Feb. 2003).

[27] A working example of this can be read at URL: http://www.semaphorecorp.com/cgi/netdde.html (20 Feb. 2003).

[28] URL: http://support.microsoft.com/default.aspx?scid=kb%3ben-us%3b315416 (20 Feb. 2003).

[29] URL: http://support.microsoft.com/default.aspx?scid=kb%3ben-us%3b203607 (20 Feb. 2003).

One possible method of changing this interval is by editing the registry. This would have to be automated via a logon or logoff script to reach all of the targeted computers. A simpler method rests in the Group Policy configuration itself. Within the Group Policy MMC, under Computer Configuration \ Administrative Templates \ System \ Group Policy, is a setting "Group Policy refresh interval for computers". Once enabled, intervals can be set in minutes for both the refresh interval and the randomization factor, to a maximum of 45 days, and one day, respectively.

This method is more straightforward that a scripted editing of the registry. It can be applied at the domain level or at an OU. Also, there is a separate setting for adjusting these intervals on domain controllers, so that an Administrator can adjust the above setting without fear of harming his domain infrastructure.

4.2 Testing the Template's Security Settings

The Gold template sets the security option "Additional restrictions for anonymous connections" to have the value "No access without explicit anonymous permissions." This is enforced by setting the following registry value on the workstation:

\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\restrictanon-ymous = 2

A value of zero will allow anonymous connections, so-called "null sessions." With the value set by the Gold template, null session connections should be denied. This should hold true even though there are null session shares defined in:

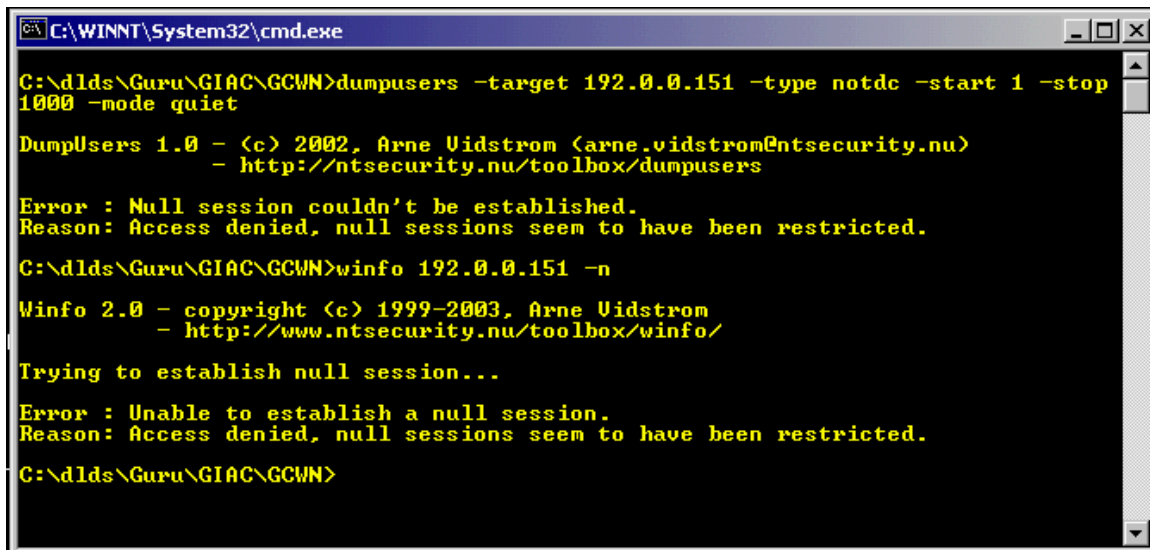HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\ Parameters\NullSessionShares

This parameter of the Gold template was tested with the use of two utilities, "WINFO" and "DumpUsers." [30] These are command-line utilities that take advantage of null sessions in order to capture a list of users (even if the names have been changed for the Guest and Administrator accounts) and the active shares on the workstation (hidden or openly advertised).

There are other utilities available that can exploit null-session connections, e.g., LDP.EXE, which ships with Windows 2000, and the LDAP mini-browser provided on the SANS Institute CD, which is provided to students for the SANS course "Securing Windows."

---

[30] URL: http://ntsecurity.nu/toolbox/winfo/ and http://www.ntsecurity.nu/toolbox/dumpusers/ (20 Feb. 2003).

The null-session capability has also been the target of a denial of service exploit on Windows NT 4.0, Windows 2000 and Windows XP. [31]

As shown in the figure below, these utilities were unable to create sessions with the workstation.


```
C:\WINNT\System32\cmd.exe                                              _|□|×|

C:\dlds\Guru\GIAC\GCWN>dumpusers -target 192.0.0.151 -type notdc -start 1 -stop
1000 -mode quiet

DumpUsers 1.0 - (c) 2002, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
           - http://ntsecurity.nu/toolbox/dumpusers

Error : Null session couldn't be established.
Reason: Access denied, null sessions seem to have been restricted.

C:\dlds\Guru\GIAC\GCWN>winfo 192.0.0.151 -n

Winfo 2.0 - copyright (c) 1999-2003, Arne Vidstrom
          - http://www.ntsecurity.nu/toolbox/winfo/

Trying to establish null session...

Error : Unable to establish a null session.
Reason: Access denied, null sessions seem to have been restricted.

C:\dlds\Guru\GIAC\GCWN>
```
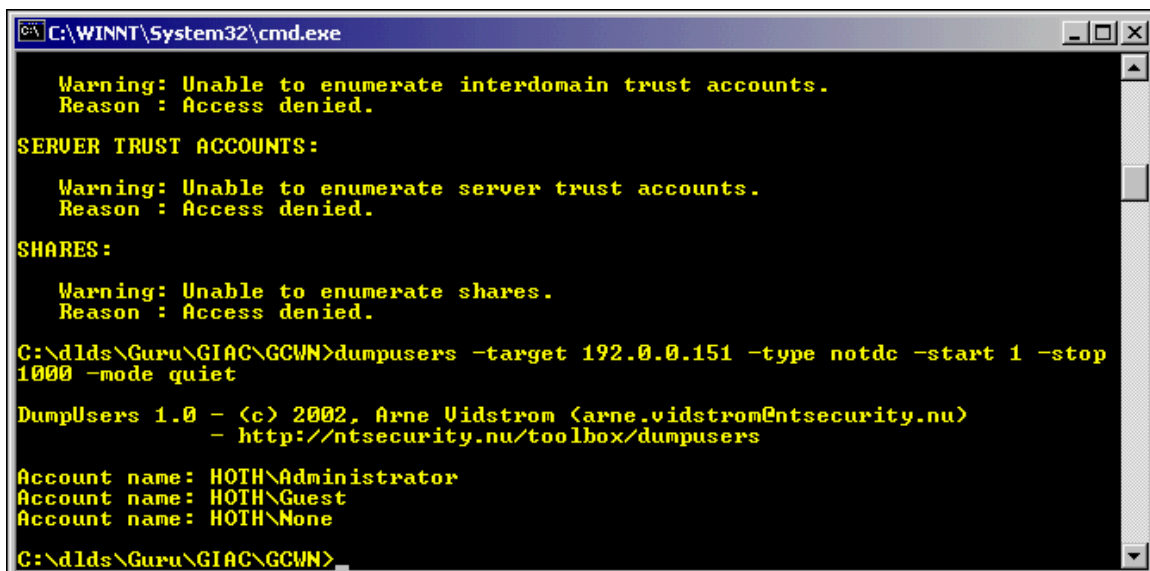
However, after changing the "Additional restrictions" setting back to "Rely on default permissions" and rebooting the workstation, DumpUsers was able to produce the following list.

---

[31] This exploit was also capable of using an authenticated user connection, and was promptly patched by Microsoft. URL: http://online.securityfocus.com/advisories/4416 (20 Feb. 2003).

```
C:\WINNT\System32\cmd.exe                                          _ □ ×

    Warning: Unable to enumerate interdomain trust accounts.
    Reason : Access denied.
SERVER TRUST ACCOUNTS:

    Warning: Unable to enumerate server trust accounts.
    Reason : Access denied.

SHARES:

    Warning: Unable to enumerate shares.
    Reason : Access denied.

C:\dlds\Guru\GIAC\GCWN>dumpusers -target 192.0.0.151 -type notdc -start 1 -stop
1000 -mode quiet

DumpUsers 1.0 - (c) 2002, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
               - http://ntsecurity.nu/toolbox/dumpusers

Account name: HOTH\Administrator
Account name: HOTH\Guest
Account name: HOTH\None

C:\dlds\Guru\GIAC\GCWN>_
```

This series of test verifies that this aspect of the Gold template is functioning as expected.

A second test verified that the Gold template's setting for cached logons was in force. The work performed on the administrative workstation is almost entirely composed of domain administration tasks, or of administrative tasks for applications which rely on the functionality of the domain. Examples would be the administration of Exchange or Systems Management Server.
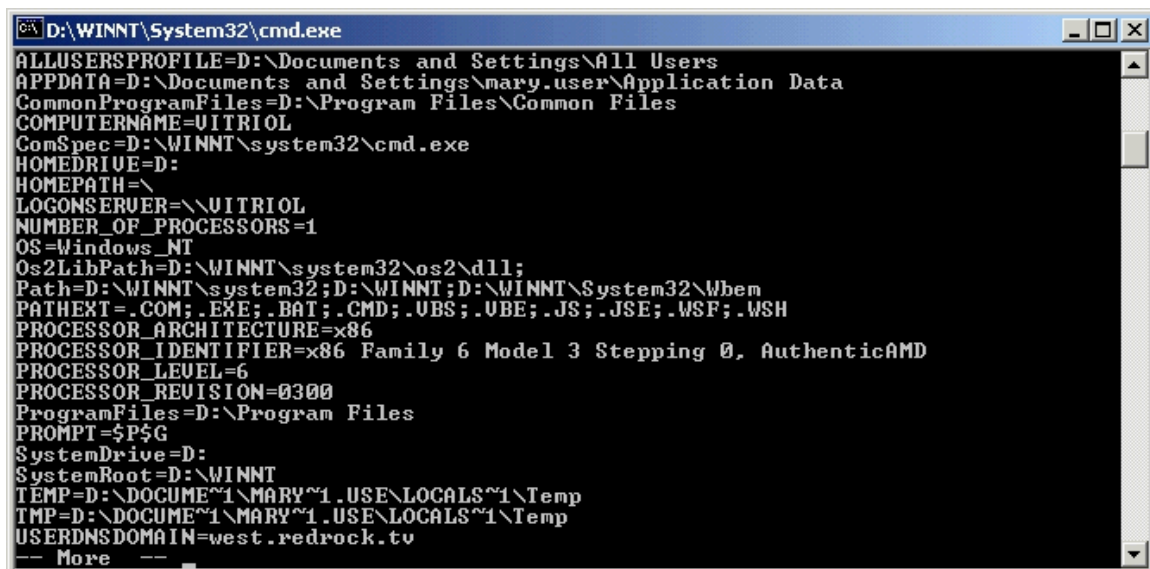
If no domain controller is available to authenticate the sysadmin's logon, there will likely be few administrative tasks which he can accomplish. However, the Gold template comprehends the usefulness of at least one cached login, given the "slight risk" involved. [32]

The method for this test is very simple. A logon attempt will be made at the administrative workstation. Pending the successful logon, the sysadmin will then logoff and the domain controller will be disabled by powering it down. The sysadmin will try once more to logon and again will logoff. That will have been the single, allowed cached logon. The sysadmin will attempt a second cached logon attempt; if the Gold template's setting for this option is in force, the second logon attempt will fail.

The Domain Administrator (but local user) "mary.user" logged in at the sysadmin's workstation, under normal network conditions, without incident. As planned, the single domain controller was shut down. "Mary.user" again logged in. A quick check of the "LOGONSERVER" value provided by the SET command

---

[32] NIST Special Publication 800-43. B-9.

verified that the name of the server that processed the login was \\VITRIOL. This is the local computer's name; had the logon been processed by the domain controller, its name, \\CAMINO, would have appeared for this value. Subsequent logon attempts produced the message that the user could not logon because the domain WEST was not available. This indicated that the Group Policy setting prevailed and that the sysadmin's workstation could no longer rely on the cached set of credentials.


```
D:\WINNT\System32\cmd.exe                                                _ □ ×
ALLUSERSPROFILE=D:\Documents and Settings\All Users
APPDATA=D:\Documents and Settings\mary.user\Application Data
CommonProgramFiles=D:\Program Files\Common Files
COMPUTERNAME=VITRIOL
ComSpec=D:\WINNT\system32\cmd.exe
HOMEDRIVE=D:
HOMEPATH=\
LOGONSERVER=\\VITRIOL
NUMBER_OF_PROCESSORS=1
OS=Windows_NT
Os2LibPath=D:\WINNT\system32\os2\dll;
Path=D:\WINNT\system32;D:\WINNT;D:\WINNT\System32\Wbem
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 6 Model 3 Stepping 0, AuthenticAMD
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=0300
ProgramFiles=D:\Program Files
PROMPT=$P$G
SystemDrive=D:
SystemRoot=D:\WINNT
TEMP=D:\DOCUME~1\MARY~1.USE\LOCALS~1\Temp
TMP=D:\DOCUME~1\MARY~1.USE\LOCALS~1\Temp
USERDNSDOMAIN=west.redrock.tv
-- More --
```

Third in the series of tests is an attempt to defeat the following security option, propagated by Group Policy:

- Remote Registry Service: Disabled

From the domain controller, a Domain Administrator (*the* Administrator, in fact) launches REGEDIT and selects "Connect Network Registry". \\HOTH (the other sysadmin workstation built for testing purposes) is named as the target computer.

As expected, the security option's restriction prevailed, and REGEDIT raised the following alert after failing to connect to \\HOTH:


```
Error Connecting Network Registry                                          ×
 ⊗   Unable to connect to \\Hoth.  Make sure that this computer is on the network, has remote administration enabled,
     and that both computers are running the remote registry service.

                                    OK
```

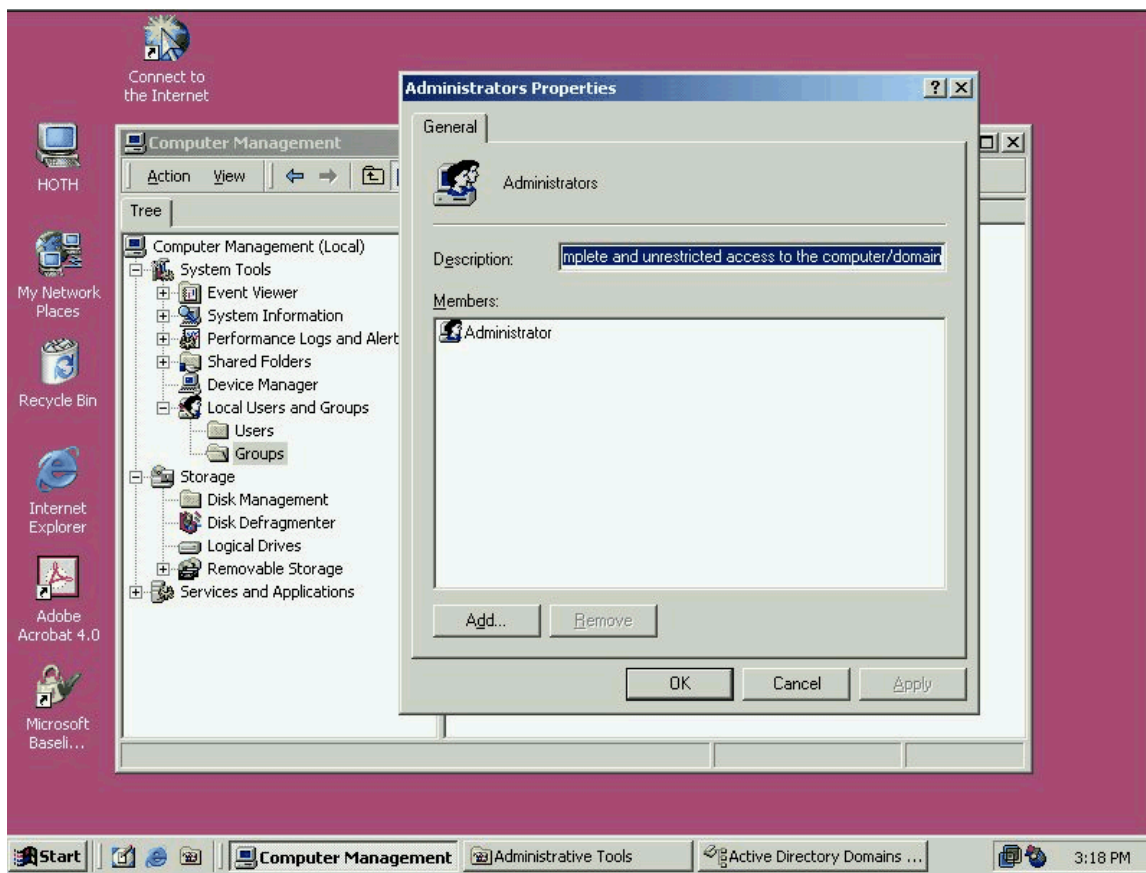4.3 Testing the System's Functionality

Having completed a reasonable verification of the domain's enforcement of the imported Gold template, this document will now provide the results of functionality tests – tests that are representative of normal activities for the sysadmin workstation. The reader will recall that the sysadmin who utilizes the workstation holds Domain Administrator rights in Active Directory. However, he sports rights no greater than User on the workstation itself. The workstation of course has a local Administrator account, but the use of that account is meant to be occasional and restricted for tasks that absolutely require those rights – the installation of new software, for example.

This arrangement is intended to reduce the risk inherent in logging in with administrator rights in order to perform privileged tasks, while also unnecessarily running non-privileged applications in that same administrative context. This exposes the workstation to many risks; the classic examples of vulnerable applications are Web browsers and e-mail applications. [33]
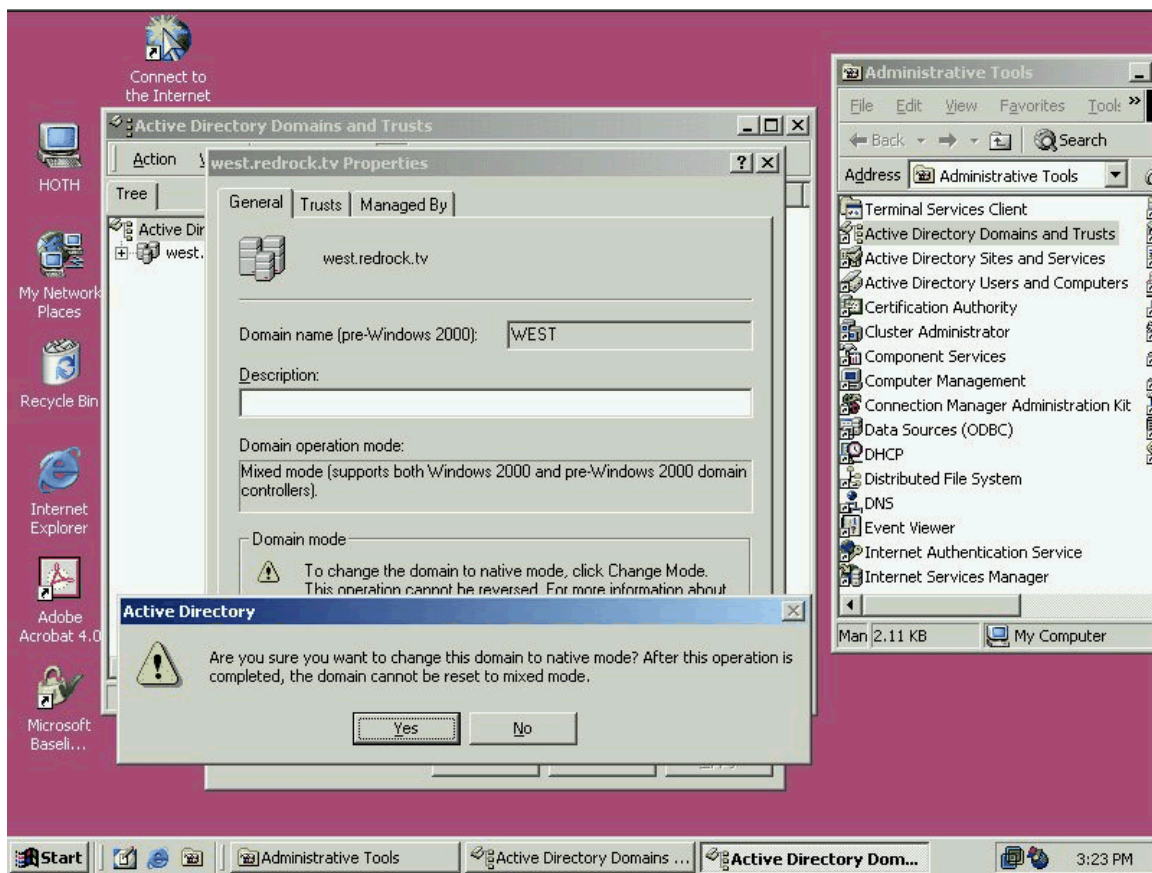
In keeping with the intended purpose of the sysadmin workstation, three basic administrative tasks will be attempted from the workstation. Before undertaking those tasks, the author submits the following figures, verifying that the sysadmin user, "Mary.user", is not a local administrator on the workstation. This is a requirement of the assignment.
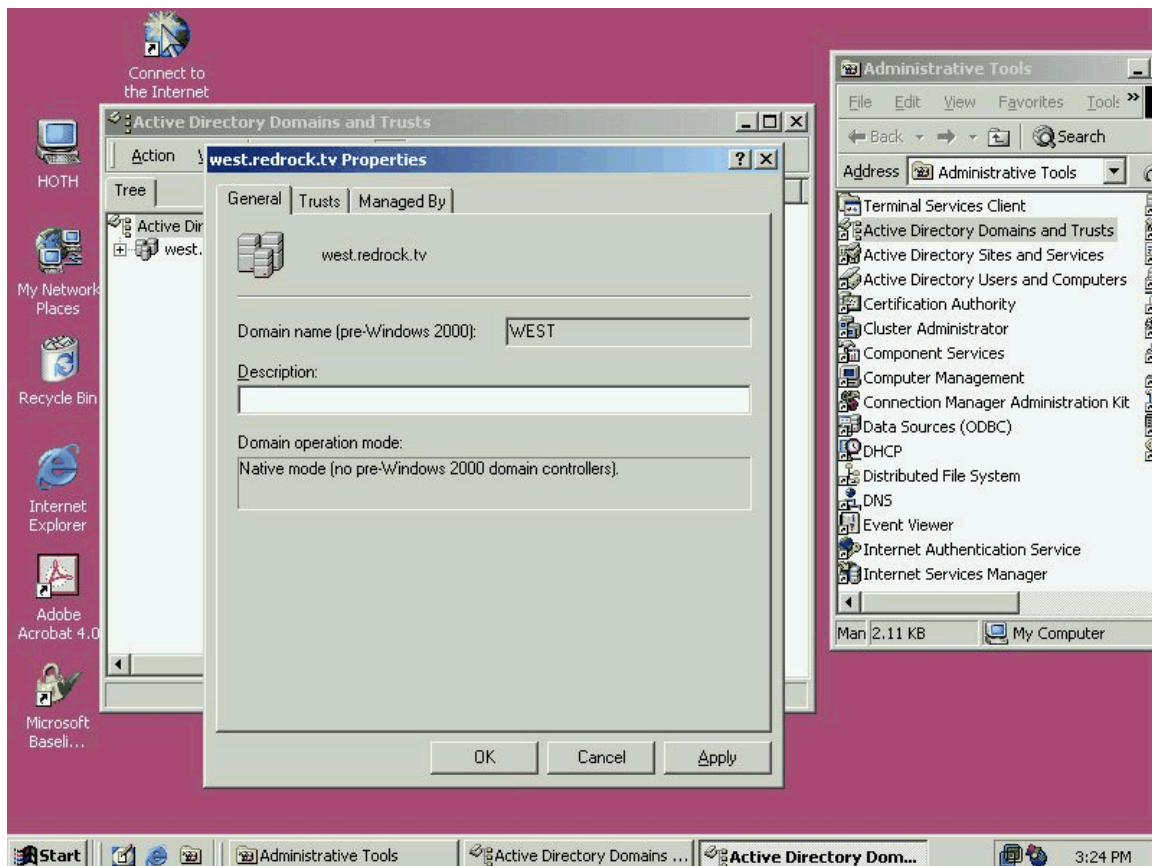
---

[33] URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/howto/seclogon.asp (20 Feb. 2003).
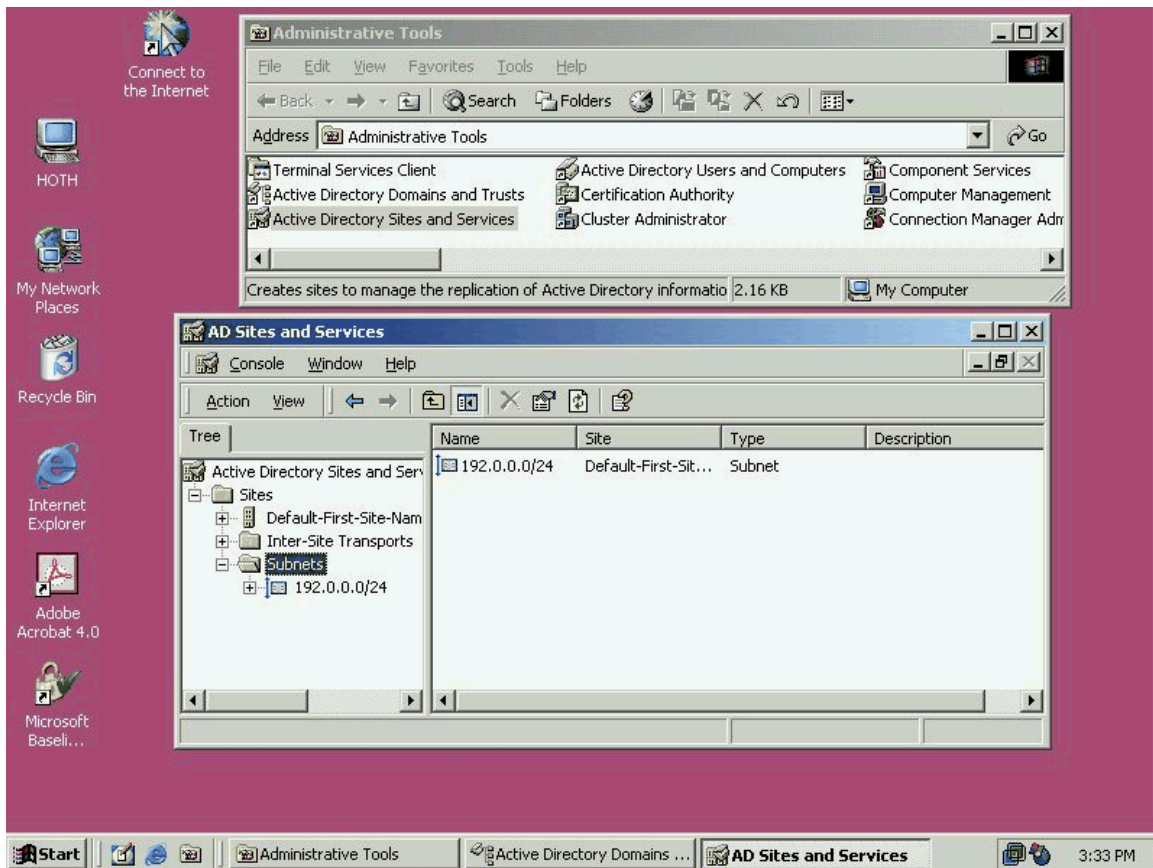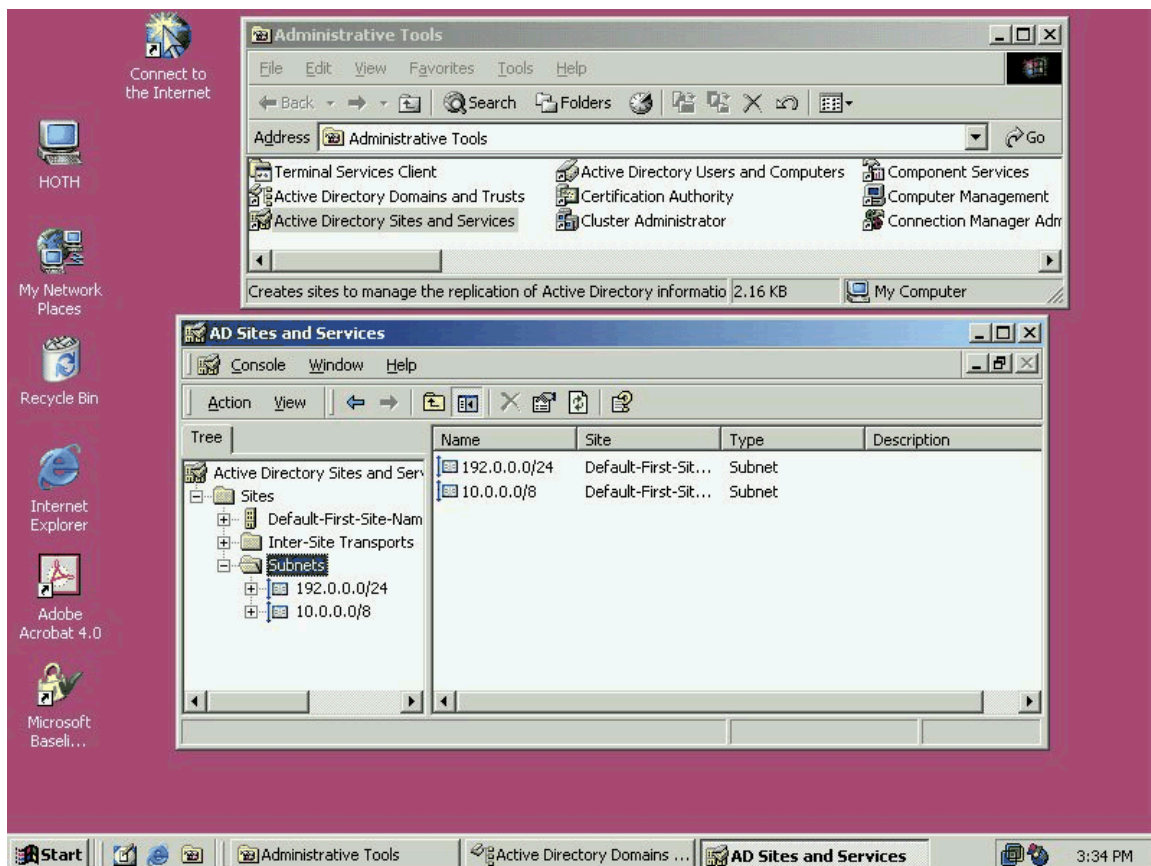
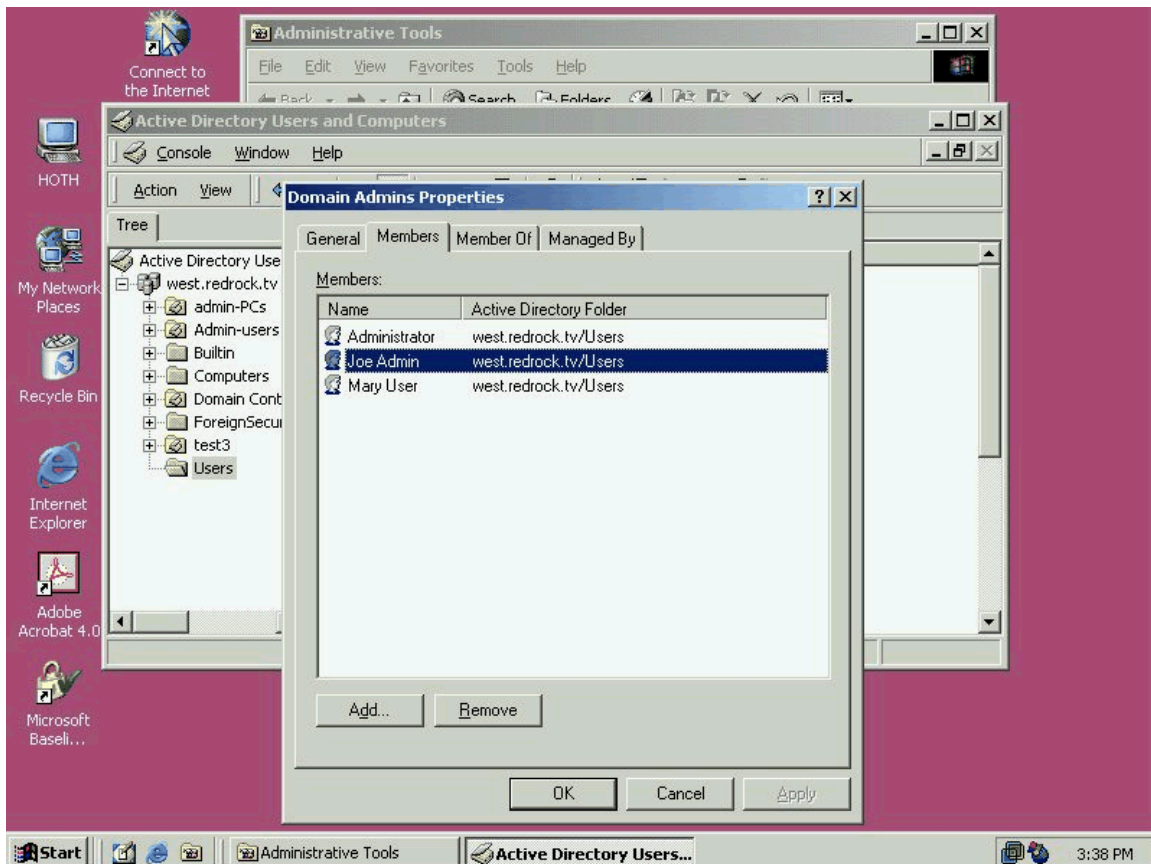The first task will be to change the mode of the domain to Native mode.

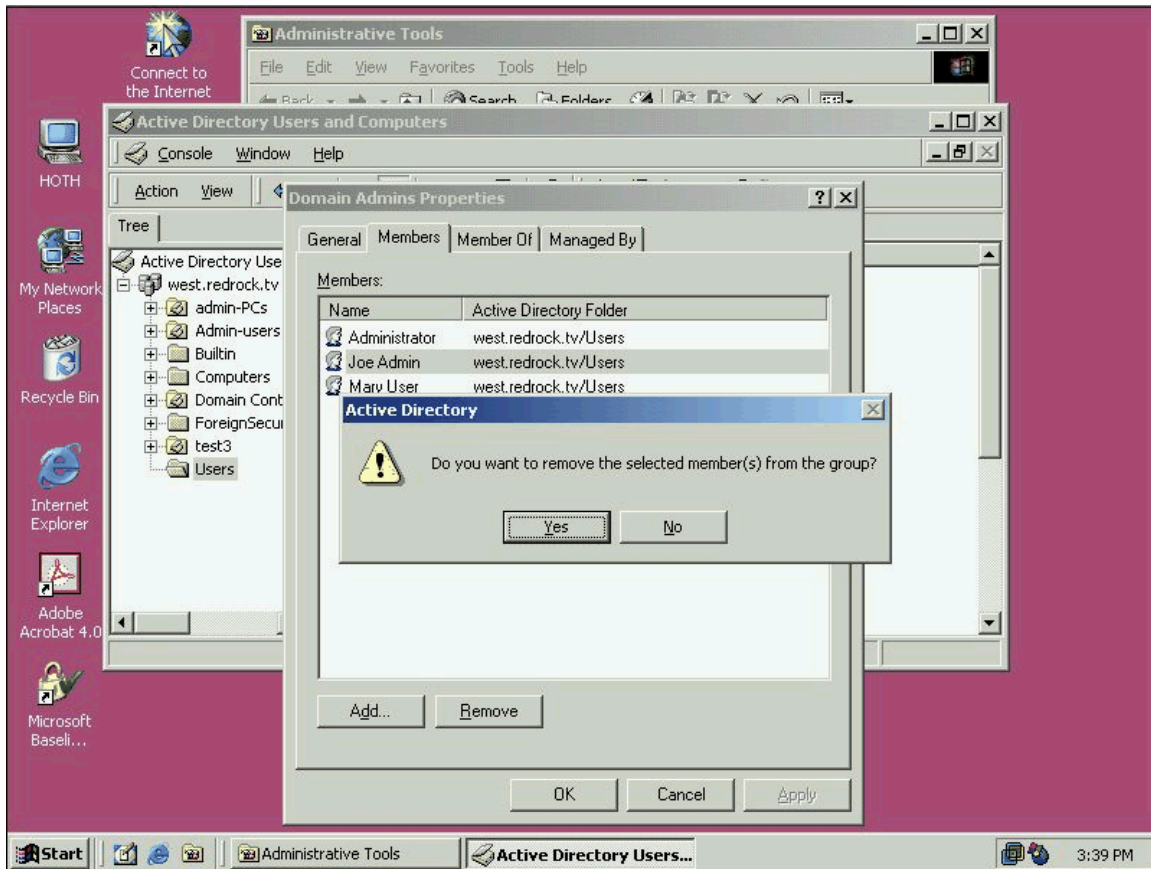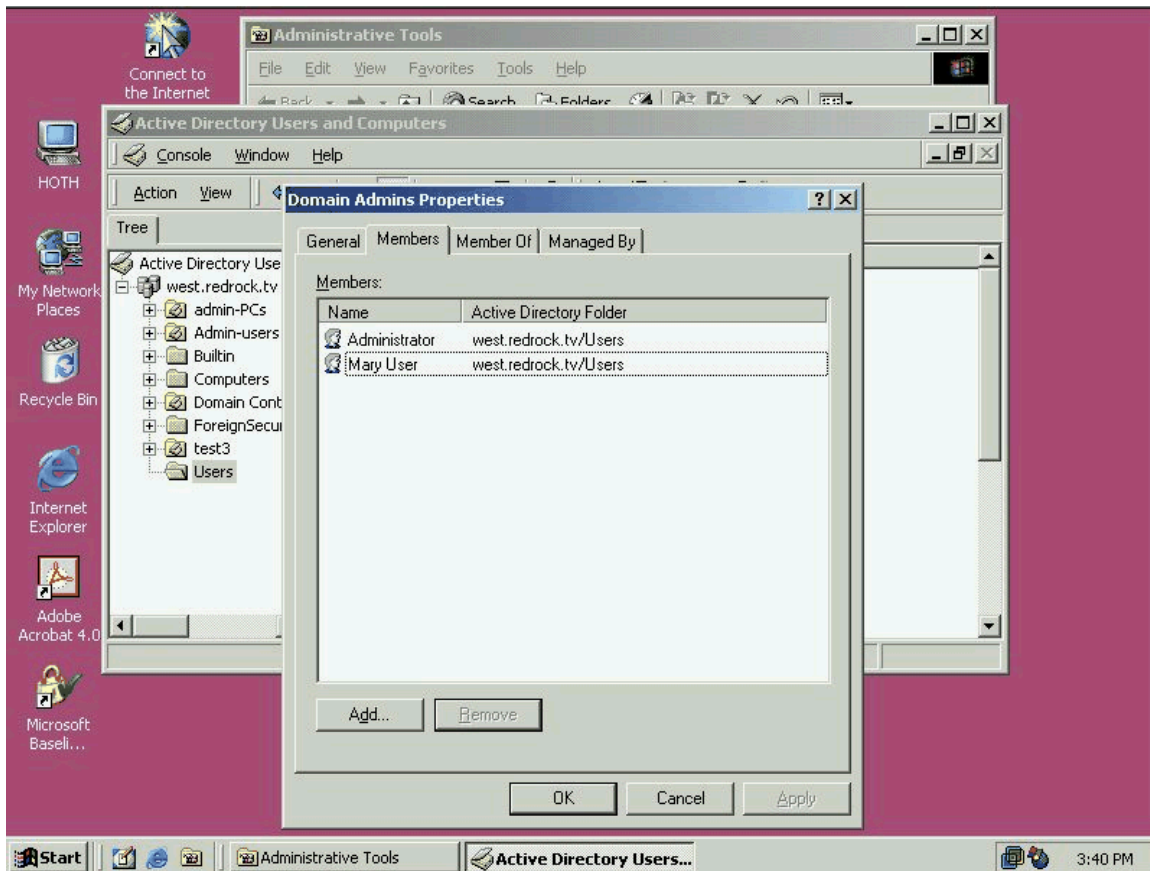The second task will be to add a subnet via the Active Directory Sites and Service utility.

The final task will be to remove an account object from the membership list of Domain Administrators.

5. Evaluation of the Gold template

The heritage of the Gold template is evident in the thoroughness of the security options and permissions that it enforces. Being a derivative work and an expansion of several prior templates created by other organizations, it is arguably the most complete as well. As noted above, it is also very thoroughly documented, more so than the other templates considered as candidates for this assignment.

The goal in creating the template may well have been to provide a starting point for securing Windows 2000 computers and domains; indeed, the accompanying documentation refers to the intent to "provide guidance and recommended practices" rather than making an announcement that the organizations involved have created the cure-all for Windows 2000 security vulnerabilities, even if only at the moment of the document's publication. [34]

This realization or perspective is valuable to Systems Administrators who are certainly in need of security solutions but are often pressed for time. Following the prescribed method for deploying the Gold template through Group Policy may

---

[34] NIST Special Publication 800-43. 1-2.

constitute due diligence on the part of Systems Administrators but it should not be carried out blindly. Nor should the application of this template, or any other, be the end of the Systems Administrator's efforts, even in the very limited sense of maintaining security through Group Policy.

On the other hand, the Gold template may be too restrictive for some environments. For Systems Administrators in such environments, applying a security template without thorough research beforehand might earn the wrath of users who have come to expect a more free hand with regard to the use and modification of their computers.

This document has concerned itself with securing computers that are used in carrying out the extremely sensitive tasks of Windows 2000 domain administration. Integrity of authority and communications are indispensable in this situation, where a compromise could result in tremendous expense and lost man-hours. [35]

Such an environment demands a skeptical assessment of the suitableness and effectiveness of the chosen Gold template. This author has identified several items within the Gold template which should be strengthened for use on the sysadmin's workstation which is the focus of this document.

5.1 Password Policy

Regarding password strength, the Gold template is too lax, but only in one aspect: password length. It enforces an eight-character minimum, along with enabling complexity requirements and endorsing the NSA password filter DLL. [36] The complexity requirement can produce a false sense of security in a short password, however. As demonstrated at softheap.com, crackers are keenly aware of human tendencies in the placement of a required special character. It generally shows up at the end of the password, making brute-force attacks easier. [37] Microsoft itself recommends a stronger password for administrative accounts, and cautions against password reuse, while providing a gentle reminder that the Windows 2000's limit on password length is 127 characters. [38] This author has historically used only strong passwords (by the standards of the NSA DLL) of no fewer than twenty characters.

5.2 User Rights

---

[35] For an innovative, online calculator for the cost of computer downtime, see URL: http://www.dallastone.com/downtime.html (20 Feb. 2003).

[36] NIST Special Publication 800-43. B-2.

[37] URL: http://www.softheap.com/security/security-of-my-passwords.html (20 Feb. 2003).

[38] URL: http://www.microsoft.com/technet/security/tools/chklist/w2ksvrcl.asp?frame=true#c (20 Feb. 2003). This author would also caution against password reuse across server product lines. E.g., Domain or Local Administrator passwords should not be reused for a SQL Server "sa" account or an Exchange service account.

For the role that the sysadmin workstation plays, the Gold template's settings for User Rights assignments will also require modification. Some of the settings are too restrictive while others hand out rights in a manner that is inconsistent with this particular role. Those User Rights, the suggested changes and supporting rationales follow.

- Access this computer from the network: the Users group should be excluded; the sysadmin should not enable file or printer sharing, which would be the only reason to allow Users this right.

- Back up files and directories: local Users will need this right, as the sysadmin will be logging in primarily with those rights. No other users will be able to connect from the network or logon locally, so this does not present a new risk. [39]

- Restore files and directories: same rationale as "Back up files and directories."

- Deny access to this computer from the network: the Domain Users and local Users groups should be added, to block users who might be granted individual privileges for network logon.

- Manage auditing and security log: the sysadmin's domain user account should be granted this right, to foster the habit of checking the workstation's logs every day. [40]

- Allowed to eject removable NTFS media: the sole group with this right, Administrators, should be stripped of this right. Local storage of potentially sensitive data is discouraged in this environment, and NTFS media are subject to compromise by non-Windows 2000 computers that can read NTFS. [41] This setting does not prevent the use of removable media, but is a reminder that removable media should be considered insecure.

5.3 Security Options

- Digitally sign server / client communication (when possible / always): set to "always" because this environment is entirely Windows 2000, the sysadmin can be sure that all of the systems he communicates with can sign their SMB packets. Leaving these settings to "when possible" leaves

---

[39] The reader should keep in mind the local Users group has as its only member the sysadmin's domain account (apart from the NT AUTHORITY entries), and that the local Administrators group has only one: the local Administrator.

[40] NIST Special Publication 800-43. G-2.

[41] URL: http://www.sysinternals.com/ntw2k/freeware/ntfsdospro.shtml (20 Feb. 2003).

open the possibility that an non-signing SMB server could be interposed, the "man-in-the-middle" attack. [42]

5.4 Event Log Policy

- Maximum log sizes: because the sysadmin workstation is of a minimal hardware configuration, the maximum log sizes will be pared to 40MB, from 80MB. Heeding NIST's warnings about the auditing items that will create a flood of log entries, the reduced log size should be adequate.

5.5 Restricted Groups

- Restricted Groups: the sysadmin's domain accounts (the primary being in local Users and the other in local Administrators) will be reflected here. Only NT AUTHORITY\INTERACTIVE and NT AUTHORITY\ Authenticated Users will join the single domain account in local Users.

5.6 System Services Settings

- QoS RSVP Provider: Disabled, as no QoS-Aware programs are installed on the sysadmin's workstation.

- SNMP Service and SNMP Trap Service: Manual rather than the recommended setting of Disabled, in support of SNMP-based management tools installed on the workstation. SNMP access should be restricted by IP address and community names should be long and complex. [43]

5.7 File Permissions Settings

With four exceptions, this author finds that the Gold template's file permissions are adequate. The following should be altered:

- TFTP.EXE

- FTP.EXE

- IRFTP.EXE

---

[42] URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/proddocs/568.asp (20 Feb. 2003).

[43] van Oorschot, Jan, Wortelboer, Jeroen, Wisse, Dirk. "Windows 2000, SNMP and Security." SecurityFocus Online, April 2001. URL: http://www.securityfocus.com/infocus/1301 (20 Feb. 2003).

Administrator should be left as the Owner of these files, but all permissions should be removed from them. This is a reasonable measure in eliminating avenues by which files might be remotely copied, without disrupting normal file operations at the workstation. Finally, ROUTE.EXE should have identical permissions to the three files above, due to the dangers concomitant to the introduction of spurious TCP/IP routes. If a hacker can make his computer a waypoint in the sysadmin's communications, he will be able to sift through all unencrypted data and to subject captured, encrypted packets to cryptanalytic attack. On Windows 2000, access to ROUTE.EXE also would provide an attacker with an easy method for viewing the workstation's routing table.

5.8 Registry Values

Table B-13 of NIST's Gold template documentation enumerates the registry values that are defined in the template. [44] This author recommends the following changes and additions, all of which relate to the configuration of the System File Checker application.

- MACHINE\ SOFTWARE\ Microsoft\ Windows NT\ CurrentVersion\ Winlogon\ SFCScan: value should be set to "1", which will cause SFC to check for the validity of the system files at each boot.

- MACHINE\ SOFTWARE\ Microsoft\ Windows NT\ CurrentVersion\ Winlogon\ SFCShowProgress: value should be set to "0", hiding the SFC progress meter.

- MACHINE\ SOFTWARE\ Microsoft\ Windows NT\ CurrentVersion\ Winlogon\ SFCDisable: value should be set to "4", which disables any popups concerning SFC's intent to restore copies of original files. [45]

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Setup\SourcePath: value should be the local file path to (but not including) the i386 directory, wherein the system files are stored.

SYSTEM would be the only account requiring permissions on the i386 folder, because the Windows File Protection "uses Winlogon as the protection service that is running in the context of the system account. WFP does not interact with normal users," according to Microsoft Support. [46] The purpose of these changes is to provide an unobtrusive framework for the regular operation of the SFC. The missing component would of course be a local copy of the system files (space permitting) from which the SFC could draw.

---

[44] NIST Special Publication 800-43. B-33 - B-34.
[45] URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;222473 (20 Feb. 2003).
[46] URL: http://support.microsoft.com/?kbid=258911 (20 Feb. 2003).

5.9 Living with Security Templates and Tools in an Enterprise

The entirety of the process surrounding the induction of templates and the application of them through Group Policy has been long in the telling, but the implementation itself was very straightforward and understandable. However, after an implementation, the graphical tools that made the process so intuitive become cumbersome when trying to manage more than one workstation.

Lending itself to a scripted implementation, the SECEDIT tool is a more practical choice for the keeping abreast of multiple, networked computers' configurations. The Active Directory structure discussed in this document contains an OU strictly for the sysadmin workstations, with a linked Group Policy object. That same object will allow SECEDIT to be run from a script which applies only to that OU. Placing the command string for SECEDIT into the logon script *after* a network drive has been mapped will allow SECEDIT to compare the workstation to a SECEDIT database stored on that drive. The tool can then return its log file to that path, so that the logs can be checked for discrepancies that should be corrected. [47] SECEDIT, along with the judicious management of security settings via Group Policy, will benefit Systems Administrators greatly, and allow them more time to attend to the many security threats that are beyond the reach and scope of these powerful tools.

The author also tested a third-party application, NetIQ's Group Policy Administrator, in the search for a product that would provide more useful reporting features than Microsoft Baseline Security Analyzer, and a more intuitive user interface that the Security Analysis and Configuration snap-in. If this application also would provide the ability to forecast the impact upon effective security settings of changes to Active Directory, without actually making any changes to Group Policy, templates, or Active Directory itself, this would at the very least save some time spent on testing. This forecasting ability and better reporting might also save the author from causing downtime or unintentionally opening a security hole.

The Group Policy Administrator's main MMC screen provides a "Filters" function under each Group Policy object that it locates in a domain. This is a much quicker way to audit permissions on each Group Policy object than right-clicking at each OU and navigating to the Security pane of each Group Policy object.

Group Policy Administrator also provides a very readable report of the settings particular to each Group Policy object. The report includes hyperlinks at the top which jump to corresponding sections within the rather lengthy report. The only flaw uncovered was that the tool is able to report status on a Group Policy's Security Options, but cannot seem to extract the labels for those options. This would have to be corrected by NetIQ to provide the promised data.

---

[47] Syntax for SECEDIT can be viewed by typing "SECEDIT /?" at a Windows 2000 command prompt.

By far the most useful tool is the Group Policy Planning & Analysis MMC. This tool provides a concise report of what will change, from a user's perspective, if for instance he is removed from a Active Directory group or is moved to another OU. NetIQ provides a "Resultant Policy" item in the snap-in, showing the user's effective security profile under all applicable Group Policy objects after a hypothetical change is made.

For this test, the author created a hypothetical resultant policy, as it would exist for "Mary.user" if she were removed from the Domain Administrators group. A screen print of this report is provided.

The author will not belabor the reader with additional screen prints or further endorsements. The Group Policy Administrator Suite is available as a free, trial download at NetIQ's web site, http://www.netiq.com.

Bibliography and References

Haney, Julie M. Guide to Securing Windows 2000 Group Policy: Security Configuration Tool Set, Version 1.1.1. National Security Agency, July 22, 2002.

Security Operations Guide for Windows 2000 Server. Microsoft Corporation, 2002.

Smith, Randy Franklin. "Why NT Passwords are Weak." Windows & .Net Magazine. Winter 2000. URL: http://www.win2000mag.net/Articles/Index.cfm?ArticleID=15893.

Souppaya, M., Harris, A., McLarnon, M., and Selimis, N. Systems Administration Guidance for Securing Microsoft Windows 2000 Professional System, NIST Special Publication 800-43. National Institute for Standards and Testing, November, 2002.

van Oorschot, Jan, Wortelboer, Jeroen, Wisse, Dirk. "Windows 2000, SNMP and Security." SecurityFocus Online, April 2001. URL: http://www.securityfocus.com/infocus/1301

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/issues/W2kCCSCG/W2kSCGc4.asp

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/issues/w2kccscg/default.asp

http://csrc.nist.gov/itsec/guidance_W2Kpro.html.

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-006.asp

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsnetserver/proddocs/server/516.asp

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsnetserver/proddocs/server/568.asp.

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-011.asp

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms01-037.asp

http://www.cert.org/advisories/CA-2002-03.html

http://www.cert.org/advisories/CA-2002-03.html

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms02-004.asp

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-062.asp

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/fq99-051.asp

http://vil.nai.com/vil/content/v_99209.htm

http://www.symantec.com/avcenter/venc/data/w97m.melissa.u.html

http://is-it-true.org/nt/atips/atips28.shtml

http://www.atstake.com/research/advisories/2001/a020501-1.txt

http://www.semaphorecorp.com/cgi/netdde.html

http://support.microsoft.com/default.aspx?scid=kb%3ben-us%3b315416

http://support.microsoft.com/default.aspx?scid=kb%3ben-us%3b203607

http://ntsecurity.nu/toolbox/winfo/

http://www.ntsecurity.nu/toolbox/dumpusers/

http://online.securityfocus.com/advisories/4416

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/howto/seclogon.asp

http://www.dallastone.com/downtime.html

http://www.softheap.com/security/security-of-my-passwords.html

http://www.microsoft.com/technet/security/tools/chklist/w2ksvrcl.asp?frame=true#c

http://www.sysinternals.com/ntw2k/freeware/ntfsdospro.shtml

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/proddocs/568.asp

http://support.microsoft.com/default.aspx?scid=kb;EN-US;222473

http://support.microsoft.com/?kbid=258911