Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

Windows 2000 Professional Security

In An Open Netware Environment:

Deploying The NSA Security Templates On Campus

John Ives
GCNT v.3.0

Table of Contents

Table of Figures

1 Introduction

There are a vast number of articles and books that outline how to secure a Windows NT/2000 Server; however the numbers quickly dwindle when you attempt to find source material on securing Windows Workstation or 2000 Professional, particularly when they are participating in heterogeneous environments. This lack of source material can be of great concern, because it can make securing office workstations difficult in large environments. Though local workstations don't, as a general rule, stand out as the target for most hacker attacks, they and their users frequently can be the weak link in an otherwise secure environment. In this paper, I am going to analyze the National Security Agency's (NSA) workstation security template for Windows 2000 Professional (`w2k_workstation.inf` is available via http://www.nsa.gov), and attempt to outline how useful it is in one of the most open environments possible, that of a public University. Of specific importance to this analysis will be the effects of this template on machines interacting with Novell Netware.

With many Universities having in excess of 30,000 nodes[1], comprised of almost every Operating System in use today, the potential for attacks both internal and external are abundant. The `w2k_workstation.inf` template, which implements the NSA's recommendations as found in "Guide to Securing Microsoft Windows 2000® Group Policy: Security Configuration Tool Set" (Haney, 18), seems to offer one of the strongest protection schemes available. Additionally, it is fairly well documented with descriptions of many of the settings implemented, making it easier to judge the settings against a given environment.

During this testing and analysis I expect all key files and registry settings to be secured at the hierarchically highest level possible (from both local and remote users) while still allowing enough flexibility for users to run most common office, communication and anti-virus applications. I also expect that with a couple of minor changes to the account policies as dictated by management in the form of password restrictions and guidelines, clients will continue to interact with our NDS tree and Netware servers. Additionally, I do expect that all new software will need to be installed by privileged users.

Because of the nature of the environment, this analysis won't deal with the use of Active Directory, but will deal with ways to maintain templates using Novell's ZENworks and its associated tools.

2 Environment, Equipment & Software

The network this equipment will be located on is an open network with every machine having an Internet accessible IP address and no firewall protection in place.[2] As a result every workstation needs to be configured with a high level of security to help safeguard it from the Internet at large. The system being tested is a user's Pentium II desktop workstation running Windows 2000 with service pack 2. In order to facilitate

---

[1] UC Berkeley, for example, has approximately 40,000 nodes.
[2] Currently blocks against specific hosts are placed on an ad hoc basis as a result of reported/discovered incidents. The University, like many others, is taking steps to implement a true firewall but has had problems dealing with the diversity and volume of traffic.

4

collaboration amongst users, these individual workstations are each connected to a Novell Netware 5.1 server, using the latest service pack and security fixes (currently it stands at service pack 3). Peer-to-peer networking is prohibited. Finally, workstation accounts are managed by Netware using a Dynamic Local User policy as part of Novell ZENworks Starter Pack. This particular policy package is used solely to manage the workstation account and as such doesn't control access to any of the normal user functionality like the control panel and the desktop environment.

For this analysis, the workstation has a common collection of office and communication applications. This software is used by the user in an office environment. Software version specifics are below, installation options (including relevant installation options on the server and workstation OS's) can be found in Appendix A:

Title	Manufacturer	Version	Rev.
Office XP Standard	Microsoft	10.2627.2625	
Internet Explorer	Microsoft	5.50.4807.2300	SP2
Netware Client w/ ZENworks Desktop Manager & Novell Application Launcher	Novell	4.8	SP3
Eudora	Qualcomm	5.1	R
Norton Anti-Virus Corporate Edition	Symantec	7.51.842	
MetaFrame	Citrix	4.20.741	
Acrobat Reader	Adobe	5.0.1	
Communicator	Netscape	4.78	
Winzip	WinZip	8.0	3105
HyperSnap	Hyperonics	3.42.00	
LaserJet 2200 Series PCL6 Print Driver	HP	4.3.2.96	1160
Acrobat	Adobe	5.0.0	

3 Settings

For each section that contains settings of relevance to this open Netware environment, this analysis will discuss the settings and what effect they should have. Because the Kerberos policy is significant for domain Group Policy Objects only and it is left undefined in this template (Haney 25), it will not be discussed.

3.1 Account Policies:

Password Policy

Though the password policy is a very strong one, and is well suited for use in an open environment, it is politically, too strict for this particular environment.   For the most part the administrative policies of a public university are practical, but they are just that policies and not rules. In an effort to balance the productivity of a large and diversely skilled group of users against the security of the systems the minimum password length has been established at 8 characters. As a result the template will be edited before application.

Beyond the issue of password length the password policy seems to be a good fit for an educational environment. Though the password policy settings actually allows

more time between required changes than Microsoft's `securews.inf` or `hisecws.inf` templates, setting the "Maximum password age" to 90 days as compared to 42, makes a lot of sense in dealing with users. Though one of the tenets of security seems to state that more frequent changes make it harder for attackers to guess, changing passwords too frequently will discourage users from picking strong, unique passwords (Norberg, 57) with them instead favoring only making minor modifications to existing ones, or writing the password down on a note at their desk. In an open environment where user accounts number in the thousands, requiring fewer password changes, but strong passwords is a justified tradeoff. This policy also substantially reduces the number of support calls from users who have forgotten their passwords.

The requirement that "Passwords must meet complexity requirements" provides a needed boost to Netware's native password settings which only provide "Minimum Password Length" and "Require Unique Passwords." The complexity requirement uses Microsoft's passfilt.dll (Haney, 23), which has been available since NT 4.0 Service Pack 2 (Microsoft Corporation [5]), requires that all passwords must use at least three of the following character types:

- Upper case characters (A-Z)
- Lower case characters (a-z)
- Numbers (0-9)
- Special Characters (e.g., punctuation marks)

Additionally, the passwords used with this option set can't contain any part of the username and must be a minimum of six characters. Though the 6 character password length is less than the 8 dictated by the policy as a whole, it does represent a fall back position that would prevent a blank password in a situation in which the 8 character length somehow becomes disabled.

At the workstation level, the setting to not store passwords using reversible encryption is also important because it means that the dynamically created and managed account won't store the Netware password it is created with in an easily decrypted form, providing further protection against tools like l0phtcrack. Reversible encryption means that the passwords are stored in such a way that the password could still be read and compared to an entered password as plain text through decryption (Microsoft Corporation [10]).

Account Lockout Policy

Because the accounts lockout policy is normally handled by the server, it isn't an essential policy under 'normal' conditions, however, placing it at the workstation augments the server's system and provides an important depth of defense. The NSA's guideline is that three failed login attempts within any 15 minute time span, will lock the account for 15 minutes. Since user accounts are dynamically created on the local workstation any accounts created there remain even if the system is taken off-line.[3] By enabling this option the attackers would be locked out of the workstation account in much the same way as they would be from the server. This setting is only incrementally

---

[3] Provided the "delete account on logoff" option isn't set as part of the ZENworks "Dynamic Local User" policy.

different than the four failed attempts in 20 minutes currently in use in our environment. In an effort to standardize policies I will be adjusting the settings on the w2k_workstation template to reflect our current policies before it is applied to the test equipment.

3.2 Local Policy Settings:

Audit Policy

The Audit Policy can be a particularly sensitive issue in our specific environment, because of the user to support staff ratio (compounded by the fact that not all of the support staff can correctly understand event logs), which makes it inordinately difficult to keep up with all of the audit logs.[4] By not logging successes for "Audit object access" and "Audit privilege use," this template attempts to keep the logs at a reasonable level, making it easier for administrators/security officers to analyze the events properly. Keeping reasonable log files is particularly important in an environment such as this where large numbers of computers are accessible to attackers and should be monitored. Because "Audit process tracking" tracks information for specific events like running and/or closing an application (Haney, 28) it is liable to generate a large amount of information on any Windows box. Likewise, auditing successes related to the "Audit object access" and "Audit privilege use" generate log events for a list of items a user was either explicit or implicitly given rights (Lundman 740). By not including these for auditing, the NSA template makes it easier to manage workstations which, in most environments including this one, outnumber servers by a significant margin.

User Rights Assignment

Of the User Rights Assignment there are several setting changes that are of particular importance in an open environment.

Removing Backup Operators, Power Users and Everyone from the "Access this computer from network" right is an incredibly important change in an open network with complete access to and from the Internet. Because the Everyone group includes null sessions and other non-authenticated users (Lundman 190) this setting substantially restricts the ability of outside intruders from logging on to the workstation. While the Backup Operators and Power Users rights are a less significant change because they have already been devalued by this template, with Power Users being a restricted group[5] and Backup Operators having all of their explicit rights revoked, this is still an important example of cleaning up permissions so the fewest possible people have access, particularly if an attacker somehow manages to create a user in one of these groups.

The w2k_workstation template revokes the Administrator's "Debug Programs" permissions. By doing this the Administrator's ability to attach a debugger to a process is revoked. This revocation prevents "…access to sensitive and critical operating system components" (Lundman 1521). As the NSA's guidelines correctly state, this permission should only be granted to Software Developers on an 'as necessary' basis

---

[4] Centralizing event logs is one of the many projects currently under consideration.
[5] See "Restricted Groups Setting"

(Haney 31). As Microsoft explained in Knowledge base article Q146965[6], with the Debug Programs right "…a user to attach to any process running on the system, including a process running in the system's security context…Once attached to such a process, a thread can be started in the security context of the process" (Microsoft Corporation [6]). Again, this change is an example of decreasing the vulnerability of a system by removing unnecessary user rights from individuals and groups.

A final set of rights that are significant in the way this template changes them are the rights associated with backing up and restoring a system. By restricting the "Restore files and directories" and "Back up files and directories" permissions to Administrator, and removing Backup Operators, this template lays the full responsibility of backup and restoration on the administrators. This is an important restriction because "this right supersedes file and directory permissions" (Haney 30), meaning that a user with these rights can copy and open files to which they wouldn't normally have permission. This right is not without its uses however and this change could be a problem in an environment with an extensive backup and restore capabilities for servers and workstations. This setting probably doesn't effect most educational environments, including this one, however as they frequently lack the resources to do this. In the end, removing this right from all but administrators helps mitigate this danger of these rights.

Security Options

As to be expected, many of the settings found under Security Options are crucial to increasing the overall system security. Among the key items which this template sets is the "Number of previous logons to cache" which is set to 0. By setting it to 0, this template prevents logon information from being stored to local memory where someone with the skills could potentially access the logon information. The offset of this for Windows NT/2000 domains is that it is impossible for users to login to their local machines if the network is down or if a server is not available (Microsoft Corporation [1]). This is not an issue in a Netware (ZENworks) environments, however, as the accounts are actually created locally.[7]

In addition to logon cache there are two new Security Options found as a result of installing the new sceregvl.inf found on NSA's website (better detail of this procedure will be found in the section applying on apply this template). The two new options, "Allow Automatic Administrator Logon" and "Disable Media Autoplay," both provide MMC access to registry keys which could, if mis-configured pose significant danger to a system. When enabled, "Allow Automatic Administrator Login Key" causes the computer to automatically log in the administrator account locally, thus anyone who has physical access to the computer or is able get an executable to run on that box (by placing it in the Administrator's startup folder for instance) can have complete control of the computer because anything done would be with the administrator's security clearance. "Disable Media Autoplay."

Though possibly self evident, it is important to note that enabling the "Do not display last user name in logon screen" is particularly important in a large educational

---

[6] The article deals with a bug in Windows NT 4 (Workstation, Server and Server Terminal Services Version) but it does a good job describing the danger of "Debug Programs."

[7] Not finding an actual reference for this I tested it by both disconnecting the computer from the network and logging in and logging in with the "Workstation Only" option selected.

8

environment. Because of the vast numbers of students, faculty and staff and the fact that they are frequently spread out over vast areas, making it difficult to know everyone who works in any one (logical) division, it would be very easy for individuals to walk through offices looking for usernames[8]. Admittedly, usernames are the easy half of the battle in terms of hacking into an account, but they are a necessary first step.

An additional restriction placed on as part of this installation, which can be important in this environment is the "Restrict CD-ROM access to locally logged on user." Though not common, there is an increasing demand for locating archived records onto removable storage like CD-ROMs. Because this restriction access to the interactive user, it serves to prevent the potential situation in which an attacker compromises the computer and, while one of the archives is in the drive, copies off sensitive information.

The Security Options section of the `w2k_workstation.inf` template comes with several fields that are considered site specific and should be changed for each environment and user base. The four fields considered site specific are the options to rename both the Administrator and Guest accounts, the "Message text for users attempting to log on " and the "Message title for users attempting to log on." For this analysis I will be populating all of these settings.

3.3 Event Log Settings:

The Event Log settings of this template, though seemingly excess at first glance, can greatly help Administrators understand the nature and sequence of any attack. Though it may seem shocking to look at, setting the log files maximum size to the maximum allowed (4194240Kb) makes sense in a large educational environment where logs may go a significant time without being adequately checked. When coupled with "Shut down the computer when the security log audit file is full" option, (which this template enables) it would be exceedingly difficult for an attacker to cover their tracks When combined with the application and system logs, the security log provides a long history of the state of the computer prior to, during and after any attacks, information that can be valuable to any forensic work.

At a more obvious level, restricting guest access to all of the logs is important in almost every environment and is enabled in this template. It is especially important in an environment where every computer is directly exposed to attackers, both via the Internet and from possible internal attackers.

3.4 Restricted Groups Settings:

In choosing to place the group "Power Users" in the "Restricted Groups" section the NSA guidelines/template removes any user assigned to that group. By default the Power Users group has the ability to, among other things, create local users and groups, Modify users and groups that they have created, and Perform per-computer installation of many applications (Microsoft Corporation [4]). As Microsoft acknowledges in the Default Access Control Settings in Windows 2000 white paper, however, these permissions also give Power Users the ability to "plant Trojan Horses" and "Make system-wide operating system and application changes that affect other users of the

---

[8] Unfortunately, there isn't a similar registry/Template setting to prevent users from post-it noting their passwords to their monitors.

9

system." While this is a secure decision on the part of the NSA guidelines and template, using "Restricted Groups" to remove accounts from the Power Users group can causes problems with some legacy or poorly written applications that require users to have Power Users rights (Microsoft Corporation [2]). To the best of my knowledge, none of the software we are using in this evaluation falls into this category.

3.5 System Services Settings:

By default the NSA guidelines don't restrict any services.   In an environment with little or no protection from the Internet, this is entirely too lax. By not restricting or disabling access to any services, the computer could, inadvertently, be left open to a number of potential compromises. To ensure the highest security possible all computers on a network, including workstations, should be installed and configured in as secure a fashion as possible, from that point security of all items (including services) should be loosened only as necessary to facilitate the computer's proper use. By not restricting any non-essential services by default, there is a potential that a Trojan horse or malicious user could use an as yet unknown exploit in a service that isn't otherwise used on the computer. For instance, Microsoft Security Bulletin MS01-007 outlines a vulnerability in the Network DDE service that would enable a user to run code in the local system context (Microsoft Corporation [8]). Since it is possible for a normal, interactive user to start the Network DDE service, it would be possible for someone to intentionally exploit this service to make modifications to the registry, manipulate more dangerous and or essential services (e.g. Indexing Service, Event Log, or Telnet), or possibly to elevate their own privileges. While there may be a legitimate need for a user to have access to some of the system services like Network DDE, which isn't essential, should be disabled or otherwise limited by any template used.

For the purposes of this analysis and because I know they are not necessary, appropriate and/or secure to run in our environment I will be removing several services. Specifically I will be modifying the template to disable and give only Administrators Full control of the following services: Fax Service, Infrared Monitor, Internet Connection Sharing, Smart Card, Smart Card Helper, Telnet and Uninterrupted Power Supply. With the exception of Telnet, all of these services require equipment or services not supported at the local desktop in our environment and for which there is no immediate or foreseeable move toward funding and supporting.

3.6 Registry Settings:

Perhaps the most important security change made in the template's registry settings is that it removes both Everyone and Power User from most if not all registry keys. The elimination of Everyone prevents all non-authenticated guests from accessing those registry keys. Since null sessions (a member of Everyone) can be used for information gathering, precisely because they don't require valid usernames and passwords, preventing them from getting access to anything in the registry is an important step in almost any environment, but particularly one that has few controls. An example of how important this is the registry key HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer which "contains information for the Windows Installer" (Haney 68) and to which the Everyone group had

Read access. By eliminating Everyone access in an open environment, attackers both internal and external to the campus will find information gathering more difficult.

The elimination of the Power Users group can be a mixed bag as has been previously described, but as a general rule the few users with access to the registry the better. This is particularly true since, some of the keys and values for which the power users group had access are in their own right dangerous, such as HKLM\Software\Microsoft\Windows\CurrentVersion\Run (to which the Power Users group has both the Set Value and Create Subkeys rights, among others).   The Run subkey lists programs that are run at startup, regardless of the user (Microsoft Corporation [9]). Since it is possible to run a malicious program (like a password sniffer) from this subkey, limiting access to it is essential.

3.7 File System:

The file system permissions modified by this template contains several key changes to the system which are important to system security, regardless of the environment in question. Foremost of the increased security settings is the assigning of selective permissions to the %SystemDrive% (the drive on which the operating system is installed – usually C:\). By default, Everyone (including guest and anonymous access users) has Full Control permissions to %SystemDrive%. This means that unauthorized users have the ability to create, edit, delete, etc., files and folders that they aren't explicitly blocked from through a lack of inheritance or explicit deny permissions. This also makes it possible for programs to be installed in the root of the %SystemDrive% by users whereas they can't be installed to the %SystemDrive%\Program Files directory.[9]

Of equal importance is the removal of the Everyone group from having Read & Execute permissions to the %SystemRoot% folder (usually Winnt). The ability of Everyone to read and execute files in the %SystemRoot% to which they weren't explicitly denied access could provide a wealth of reconnaissance information for anyone looking. As an example, hotfix uninstall files are kept in sub folders of %SystemRoot%. Because of the way these files are stored (in folders labeled $NtUninstall<knowledge base article>$) it is possible to tell if fixes have been applied, revealing potential vulnerabilities. Likewise, it would be possible to look for the presence of Resource Kit Tools by looking for the appropriate folders, and if they are not properly secured even run the tools.

4 Applying the Template

Though not particularly hard on the face of it, applying a template is not without its potential pitfalls, mostly in the form of using a template with incorrect settings for the computer's environment. As a result, it is important that any template should be well thought out and prepared for in advance.

---

[9] There are of course programs for which this still wouldn't be an issue with the lesser security, because they are hard coded to particular folders or need access to systems locations or registry settings even default permissions do not allow, such as %SystemRoot%\Fonts.

4.1 Pre-Application of w2k_workstation.inf

Prior to installing the `w2k_workstation.inf` file, the template should be saved to the template directory (`%SystemRoot%\Security\Templates`) and NSA's modified `sceregvl.inf` needs to be loaded in order to add new options as mentioned in the section on Security Options. To load the modified sceregvl.inf file:

1. While logged in as Administrator, rename the default `sceregvl.inf` file located in `%SystemRoot%\inf` to `sceregvl.old`
2. Copy the NSA's `sceregvl.inf` to `%SystemRoot%\inf`
3. Run `regsvr32 scecli.dll` from either a command prompt or the Run dialog box

Once the sceregvl.inf file has registered and the template has been edited a computer analysis should be performed to see what is changes will be made to the local computer as a result of applying the template.

4.2 Editing the Security Template

Once the new template file is in place and `scecli.dll` has been registered using the new `sceregvl.inf` file, it is now necessary to edit the template so as to modify the settings inappropriate to this environment.

1. While logged in with appropriate permissions, i.e. as an Administrator, run `MMC` from the Run dialog box
2. In the Management Console choose "Add/Remove Snap-in…" from the Console menu
3. Add the "Security Templates" snap-ins as seen here:

Figure 1 Adding Security Template Snap-in

4. From the "Security Templates" node in the console's left pane open the
   templates location %SystemRoot%\Security\Template and select the
   `w2k_workstation` template
5. Opening the `w2k_workstation` node go to each subsection e.g. Account
   Policies > Password Policy
6. Double click on any item needing to be changed and modify its setting
7. Repeat steps 5 and 6 as necessary for each subsection of w2k_workstation
   to complete the changes outlined in Section 3
8. When all changes have been completed right click on w2k_workstation and
   select "Save"

4.3 Template Application

Once the template has been edited it is possible to move on to applying a
template or, as a preliminary step, perform an analysis of a computer to see what will be
changed. Both the analysis and configuration of the computer can be preformed
through the use of either the MMC (Microsoft Management Console - a GUI tool) or
`secedit.exe` (a command line tool). In the specific case of this environment, it is also
possible to use ZENworks to apply the template to a system, however the fact that it is
necessary to 'pre-configure' a computer for use with the NSA template and that there is
a need for so much hands-on work (installation of the Novell Client with ZENworks,
placing of a script for ZENworks to use, etc.) prior to getting to the point where
ZENworks is useful, detracts from its usefulness as an install method.[10]

4.3.1 Analysis and Application via MMC

The steps to perform a system analysis and to apply a template to a system are
almost identical. In order to perform either task using the GUI interface of the MMC
program the following steps are performed:

1. While logged in with appropriate permissions, i.e. as an Administrator, run
   `MMC` from the Run dialog box
2. In the Management Console choose "Add/Remove Snap-in…" from the
   Console menu
3. Add the "Security Configuration and Analysis" and snap-in
4. Right click on "Security Configuration and Analysis" and choose "Open
   database"
5. Enter a name for the database and choose "Open"
6. Select the `w2k_workstation` template to import it into the database

---

[10] For those who might be interested in using ZENworks to install a template, the script used to maintain it
(as outlined in section 4.4.3) would need to be augmented with commands that first downloads the NSA's
`sceregvl.inf` into place and runs `regsvr32 scecli.dll /s` (the /s is for silent mode).

13
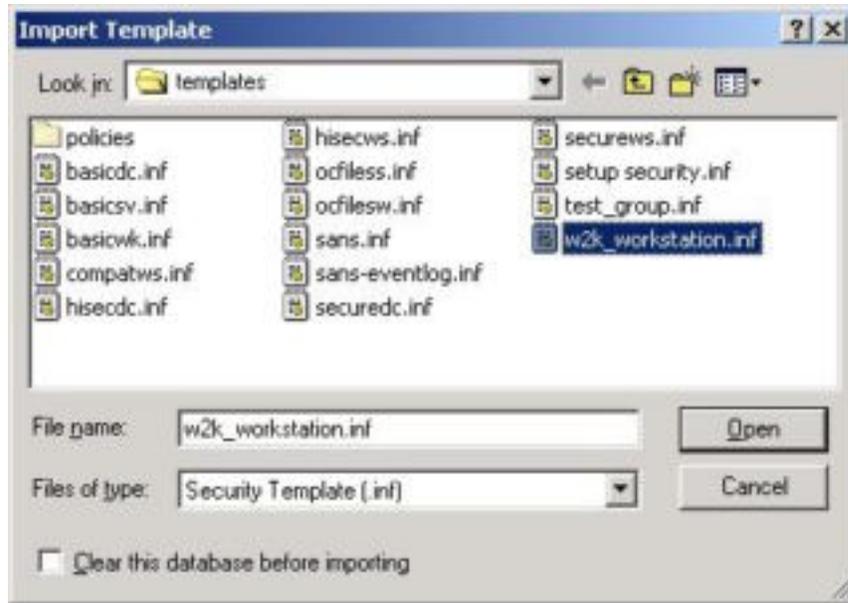
Figure 2 Import Template

7. Right click on "Security Configuration and Analysis" again and choose "Analyze Computer Now" to run a system analysis against the imported template or "Configure Computer Now" to apply

4.3.2 Analysis and Application via Secedit

To apply the security template via a command prompt the secedit.exe command is used. Secedit has the following syntax for applying a template:

secedit.exe /configure [/DB filename] [/CFG filename] [/overwrite] [/log logpath] [/areas area1 area2...] [/verbose] [/quiet]

The meanings of these options are:

Parameter	Description
/configure	Configures the computer according to the template using the remaining options
/db filename	The database file used or created for this command
/cfg filename	The security template file used to create the database file
/log LogPath	Where to store the log and what to name it
/verbose	Displays/logs detailed information
/quiet	Suppresses output to the screen and logs
/overwrite	Used to overwrite the database's configuration with a new one from the /cfg switch
/areas Areas	Used to configure on specific section of template, e.g., Registry

Besides applying a template using the /configure switch, secedit can also be used to analyze a system against a template by substituting /analyze for /configure. In addition to configuring and analyzing a computer, secedit can also export a template

14

from the security database (/export), refresh a system policy by reapplying the security settings (/refreshpolicy), and to validate a security templates syntax (/validate).

When secedit finishes analyzing or configuring the security settings the screen will return a message saying the "Task was completed" as shown below.
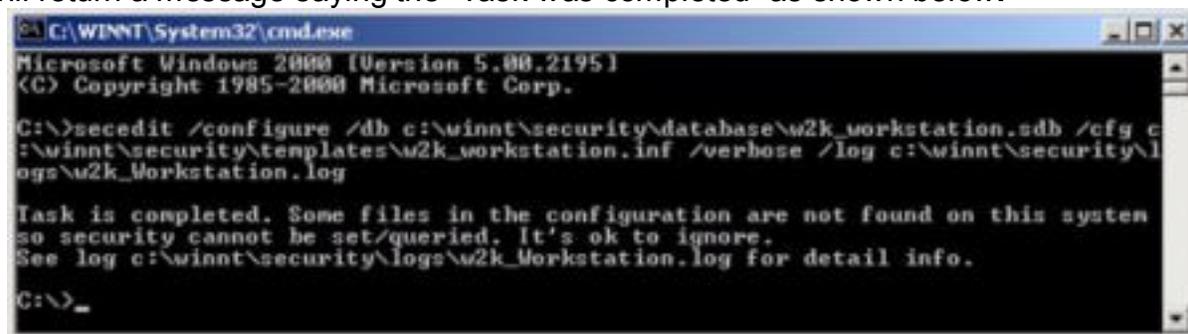
Figure 3 Secedit.exe /configure

4.4 Template Maintenance

Once the template has been applied and the system has been secured, it is still necessary to provide for the ongoing security of the system by maintaining and refreshing it overtime. This maintenance can take the form of an analysis or a re-application of the template as well as using local group policies and secedit's /refresh option. For this section I will be discussing how to perform refresh the account and machine policies as well as methods to perform regular system analysis and or configuration using a script. The tools that will be used are the MMC with group policy snap-in, the task scheduler and Novell ZENworks Starter Pack.

4.4.1 Using Local Group Policy Objects

Besides using a scheduler to reapply a template, some parts of the template can be included as part of a Local Group Policy Object. While Active Directory is able to distribute and refresh all of the settings found in the workstation template, local group policies are only able to refresh and maintain the account and local policies.

1. While logged in as an Administrator, run MMC from the Run dialog box
2. In the Management Console choose "Add/Remove Snap-in…" from the Console menu
3. Add the "Group Policy" snap-in
4. When prompted to "Select Group Policy Object" leave the object as *Local Computer* and click Finish
5. click Close and then click Ok
6. When you return to the console open Local Computer Policy > Computer Configuration > Windows Settings
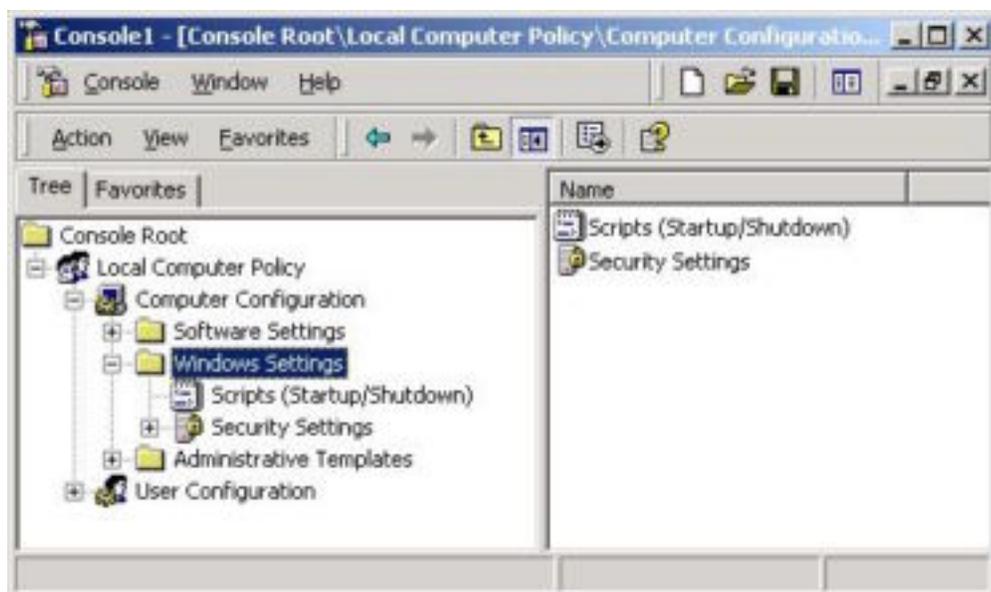
Figure 4 Local Group Policy Window

7. Right click on Security Settings in the left window and choose Import Template
8. When prompted for the template to import the policy from, navigate (if necessary) to the template used to secure the box, in this case `w2k_workstation.inf`

9. Close the MMC

As Microsoft Knowledge Base article Q203607 describes, it is possible to change the default Windows 2000 computer refresh interval of 30 minutes, however there is no need to do that in this environment (Microsoft Corporation [7]).

4.4.2 Maintaining security with Task Scheduler

Using Local Group Policy Objects are a good way of maintaining the account (password and lockout) and local (audit, user rights and security options) policies, however, there are times and situations which call for a more complete 'refreshing' of the template policies. Using a script and Task Scheduler it is possible to run secedit at scheduled times or at designated events such as computer startup. Because, of secedit's reliance on command line parameters and the need to do something with any log files generated, it is best to create the run secedit as a part of a script or batch file. For this example I am going to write a simple batch file that reapplies the restricted groups setting and logs the results to a file named for the area being processed. A similar script which uses the /analyze option and logs the results to a file named for the computer and the date can be found in Appendix B.

1. Open Notepad
2. In Notepad type (or paste) the following (its one line of text that wraps):

```
%systemroot%\system32\secedit.exe /configure /db
    %systemroot%\security\database\w2k_workstation.sdb /cfg
    %systemroot%\security\templates\w2k_workstation.inf /areas
    GROUP_MGMT /log %systemroot%\security\logs\group_mgmt.log
    /verbose
```

3. Save the file as `secedit-refresh.bat`[11] to a secure location like `c:\winnt\security`
4. From the Control Panel open "Scheduled Tasks"
5. From "Scheduled Tasks" double click "Add Scheduled Task"
6. Choose "Next"
7. When prompted for application to run click on "Browse"
8. Navigate to c:\winnt\security and select secedit-refresh.bat
9. For run frequency select Daily and click Next
10. Set the start time to 12:00AM and click Next
11. For the User name and password enter the Administrator's information and click Next
12. Click the "Open advanced properties for this task when I click Finish" check box and click Finish.
13. In the advanced properties click on the Schedule tab
14. Click on the Advanced button
15. Click the Repeat Task check box and change the frequency to 30 minutes and have it repeat until 11:59PM
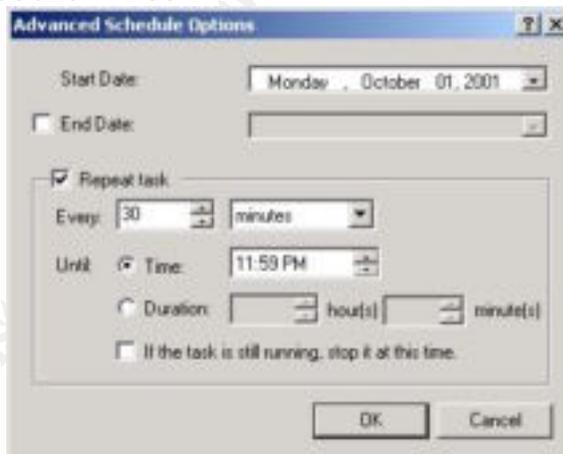
Figure 5 Advanced Scheduling Options

16. Click the OK button to exit the Advanced Schedule Options window and again to exit the scheduled jobs details.

A more thorough script could do a post processing of the file and log any anomalies (such as users found as members of the Power User group) to the security

---

[11] This batch file has an obvious disadvantage in that it requires the drive mapping to exist at the time it is run, however this is just a starting point, a more thorough script could use FTP or some other transport to get the log to a central location.

even log.[12] It would be just as easy to write a script that performs a system analysis or reapplies the template en mass on a scheduled basis.

4.4.3 Maintenance via Novell ZENworks 2 Starter Pack

Because the environment in question is a Netware 5.1 environment, we do have and use the ZENworks 2 Starter Pack that comes with this version of Netware. Historically we have used ZENworks primarily for the local account management feature that allows users to gain access to the local workstation with their NDS identity. In running this analysis I've also decided to use ZENworks to maintain the system.[13] In practice, using ZENworks is not much different than using the task scheduler, however, ZENworks has more flexibility in terms of scheduling. ZENworks, for instance, makes it possible to schedule the script for any number of different times including: login, logout, when the screen saver is active, when the desktop is active, daily (or on certain days of the week, and repeating as frequently as desired on those days), weekly (again on as many days of the week as desired), monthly and yearly. Additionally, events scheduled as part of ZENworks can be run as the System, the Interactive User or as an Unsecure System.[14]

In order to use ZENworks to configure a workstation the workstation must have the Novell Netware Client **(Novell, Inc. [1])** and be imported into NDS.[15] Because of restrictions on the length of parameters it is possible to pass directly to an executable via ZENworks it is best to have a script on the box that actually calls secedit and does any pre/post processing. Once these requirements are met, the following steps outline how to use ZENworks to create a new policy that can regularly analyze and/or configure workstation using NWAdmin:

1. Right click on the container (organization or organizational unit) that will contain the policy and select "Create"
2. From the New Object window choose "Policy Package" and click OK
3. From the Policy Package Wizard choose WinNT-Win2000 User Package[16] and click Next

---

[12] The script to do this would be better suited to a more complete scripting language like VB Script or Perl.
[13] Using this same procedure it is possible to do the initial template application as well, however, the need to do preparatory work as described in section 4.1, lends itself to 'at console' methods like secedit and MMC.
[14] As the warning message indicates, Unsecure System is to be avoided wherever possible because it permits "Address Mappings between the user and system space…"
[15] A discussion of importing workstations is outside of the scope of this paper and is generally a set-up issue, however, http://www.novell.com/documentation/lg/zen2/wrks_enu/data/hc8lvjx8.html discusses how and why to import workstations. Additional information can be found in Gerald Foster's Desktop Management with Novell ZENworks.
[16] It is also possible to create a "WinNT-Win2000 Package" (for the workstation) with the same objective and steps. I prefer to create a user package so that it can be set not to run while support staff are working at the computer.

Figure 6 ZENworks User Package

4. Change the package name and location if necessary and click Next
5. Leave all of the built-in policies unselected and click Next
6. At the "Associations" box click "Add"
7. Browse to the object (user, group, ou, etc.) this policy is to be associated with and click "OK"[17]
8. Click Next when you are finished adding associations
9. Review the Policy Package Wizard's summarizing information for accuracy and click "Finish"
10. When you return to the main NWAdmin screen double click the newly created policy.
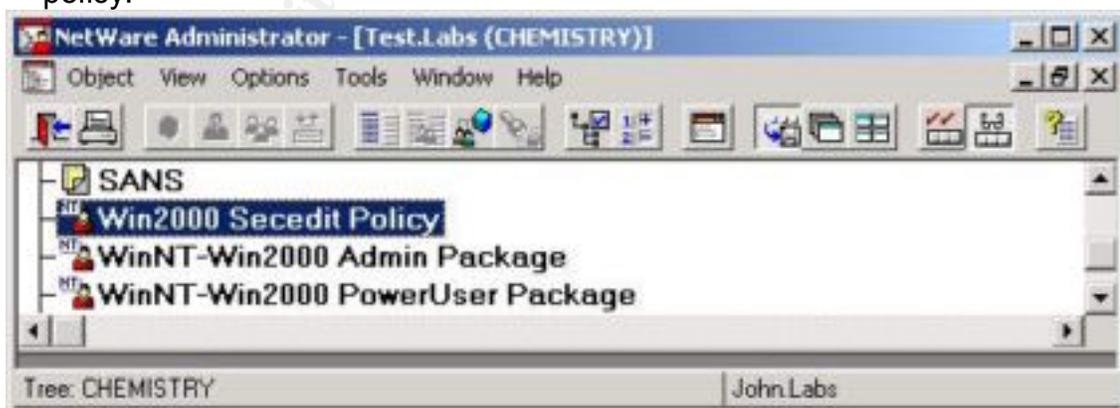
Figure 7 New ZENworks Policy

11. Click "Add Action"

---
[17] It is only possible to have one policy of any given type associated with a container, so in some cases it may be necessary to create a group that users can be a member of to be associated with a package.

12. Enter "Secedit – Analysis" for the action name and click "Create"
13. With the Secedit – Analysis action selected click on "Details"
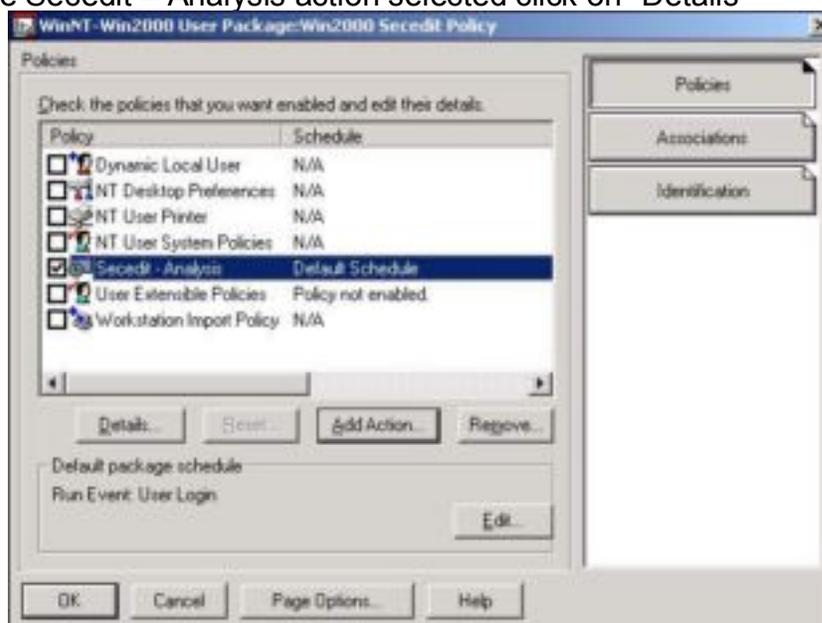
Figure 8 ZENworks Secedit Policy

14. For the Policy Schedule select an appropriate Schedule
15. Click on the "Advanced Settings" button
16. Under the "Impersonation" tab select "System" and click "OK"
17. Click on the "Actions" tab
18. In the Actions window click on "Add"
19. Enter the path to a script stored on the workstation (an example of which can be found in Appendix B) and click "OK"
20. Click "OK" again to return to the package details
21. Click "OK" again to return to NWAdmin

Using this same package, and creating different actions with different schedules, it is possible to configure analysis on certain days of the week and automatically reapply the template on other days.

4.5 Verifying logs

Once the template has been applied or the system has been analyzed against a template, the log should be examined for errors or omissions.[18] While examining the log, it should be noted that many errors occur because the files or registry keys do not exist, or the file can't be modified because it is open as seen in the following examples:

Configuration Errors:
```
----Configure File Security...
    Configure c:\.
```

---

[18] While the maintenance script I used as an example didn't include any functionality to centralize the logs, a more thorough one would copy the logs to a central archive or at the very least use a script to generate event logs entry of any problems.

```
Warning 32: The process cannot access the file because it is being used by
another process.
      Error building security descriptor for c:\pagefile.sys.
      Configure c:\autoexec.bat.
      Configure c:\boot.ini.
  […]
      Configure c:\ntbootdd.sys.
Warning 2: The system cannot find the file specified.
      Error setting security on c:\ntbootdd.sys.

Analysis Errors:
Mismatch      - c:\winnt\system32\regedt32.exe.
[…]
----Analyze Registry Keys...
Not Configured - machine.
```

In the configuration errors log examples, secedit was trying to secure access to, among other things `pagefile.sys` and `ntbootdd.sys`. Because the `pagefile.sys` is being used as memory swap space by the operating system, secedit couldn't change any settings related to it. Similarly, `ntbootdd.sys` couldn't be secured because it doesn't exist on IDE based systems.[19] The analysis errors, which could be scanned automatically, show that regedt32.exe doesn't have the permissions that were expected by the template and that the HKEY_LOCAL_MACHINE hive was not configured in the template.

5 Testing the Template

Using templates, especially ones that are very restrictive, can cause problems with a number of applications that don't function correctly with certain restrictions to the file or registry system. As a result it is necessary to test that the template was applied correctly and to test that any software being used on the local machines aren't hindered from normal operation by users.

5.1 Checking that the template is applied properly

Now that the template has been edited and applied it is necessary to test and verify that it was applied correctly. Though looking at the log file created by secedit or the MMC is an important way to see what was supposedly changed by the template, there is no real substitute for looking directly at the changes in action. In order to spot check that the template was applied correctly to the local machine, I have elected to check the following information: Group Membership; File System Settings on %SystemRoot%; User Rights Assignment and the Security Event Log. To perform these checks I used the MMC with the Event Viewer snap-in, DumpSec 2.8.1 (http://www.systemtools.com/somarsoft/) to get DACLs on %SystemRoot% and group memberships, and Hyena 3.0k (http://www.systemtools.com/hyena/) to view the user rights assignments.

---

[19] As explained by the Windows 2000 Professional Resource Kit, "Ntbootdd.sys is a copy of the SCSI device driver…used when using the SCSI or Signature syntax in the file Boot.ini" (Ackerman 250)

5.1.1 Group Membership – Power User

Prior to applying the template, a user was created by Administrator using the Computer Management tool. The new user, named poweruser, was made a member of the Power User group explicitly for the purpose of testing the template. After applying the template, poweruser was no longer apart of any groups. Further testing showed that ZENworks Dynamic Local User policy could create another user as power user (newpoweruser) if configured that way. However, that user would of course be removed from the power users group if the template was reapplied. For this testing I used ZENworks, though anything that reapplied the template (or at least secedit's /area GROUP_MGMT option) should generate the same results. The following Dump Sec report shows both accounts without any group memberships:

```
10/13/2001 7:24 PM - Somarsoft DumpSec (formerly DumpAcl) - \\IGATE2 (local)
UserName              Groups

CollegeAdministrator  Administrators
CollegeGuest          Guests
newpoweruser
poweruser
test1                 Users
user                  Users
```

5.1.2 DACLs

The %SystemRoot% variable relates to the drive and directory where Windows 2000 have been stored (frequently C:\winnt) and, because of the critical nature of the files found here, its Access Control List (ACLs) settings are of the utmost importance to the systems security. Because of the number of files and permissions found in the WinNT directory and its sub directories, it is not feasible to look at all of the permissions and check that the template permissions were applied correctly, but we can examine the permissions on a few key files and directories and compare them to the permissions found in the template file.

For this comparison, I have used DumpSec by SomarSoft (http://www.somarsoft.com/) to print out the ACLs of the %SystemRoot% folder and am comparing the permissions on C:\WINNT\security\, C:\WINNT\system32\secedit.exe, and C:\WINNT\system32\GroupPolicy against permissions found in `w2k_workstation.inf`. The following permissions are taken from DumpSec[20]:

```
10/16/2001 11:18 AM - Somarsoft DumpSec (formerly DumpAcl) - \\IGATE2 (local)
Path (exception dirs and files)          Account              Own  Dir  File
[…]
C:\WINNT\security\                       IGATE2\Administrators  o    all  All
C:\WINNT\security\                       CREATOR OWNER                    All
C:\WINNT\security\                       SYSTEM                      all  All
[…]
C:\WINNT\system32\regedt32.exe           IGATE2\Administrators  o         All
C:\WINNT\system32\regedt32.exe           SYSTEM                           All
[…]
```

---

[20] Because of formatting difficulties it was necessary to add the results to a table so that they would be legible.

```
C:\WINNT\system32\GroupPolicy\          IGATE2\Administrators   O    all  all
C:\WINNT\system32\GroupPolicy\          Authenticated Users         R X  R X
C:\WINNT\system32\GroupPolicy\          SYSTEM                      all  All
```

Comparing these permissions to those expected from the template revealed no
discrepancies between what was reported and what was expected. The Creator Owner
permissions to the files in C:\WINNT\SECURITY reflects that the permissions were to
be applied onto "Subfolders and files only" of this folder and not onto the directory itself.
Similarly, the Authenticated Users Read and Execute permissions assigned to
C:\WINNT\system32\GroupPolicy\ are also found in the template.

5.1.3 Security Event Log

One of the essential settings in the template is the event log, because it is the
event log that allows administrators to profile the events that lead up to and continue
through any attack. To check that its settings are correct, it is possible to use the MMC
with the Event Viewer snap-in. By right clicking on the Security log and checking its
properties', as seen in Figure 9, it is apparent that the "Maximum log size" had in fact
been set to 4194240 KB and that events were not to be overwritten as intended by the
template.
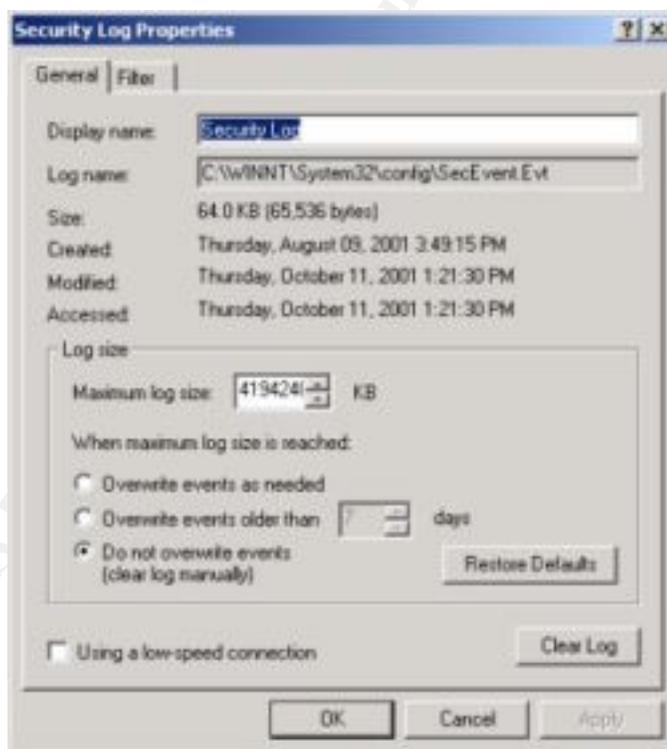
Figure 9 Security Log Properties

5.1.4 User Rights Assignment

User rights simultaneously represent some of the greatest dangers to a system
and, if applied correctly, its greatest security features. By being able to fine tune the
rights individuals and groups receive, it is possible to give users the fewest rights
possible and create the fewest vulnerabilities. Because of the length of the report copied

out of Hyena,[21] the user rights report can be located in Appendix C, however, it's important to note that a comparison of its actual and the w2k_workstation.inf template's intended permissions revealed no discrepancies.

5.2   Checking User Interaction

Since this computer is a user's workstation, its foremost responsibilities include allowing the user to login, use standard office software, communicate via email, and print. To that end I will be testing each of these functions as a normal user[22], and, where necessary and possible, providing screen captures and network traffic to demonstrate relevant information.

5.2.1   User Login

Perhaps the most troubled group of settings related to the application of the NSA came as a result of the Password Policy settings. Because the problems occurred at the client, during the logon process it was impossible to get screen captures of the problems, however, I will describe them in this section and outline what was done to deal with each of them.

If a new account attempts to login and that account doesn't have a password or has a password that doesn't meet the complexity requirement a second login dialog box occurs prompting for a local username and password. A similar thing happens in a NT/2000 network if you attempt to create a user with a password that isn't complex enough, the difference, however, is that when the account is being created on a Windows Server, it can't be created without a complex password while in a Netware environment it can. The obvious solution to the immediate problem is that all new users must be created with passwords that meet the Windows 2000 complexity requirements. Additionally, as part of our ongoing goal of increasing our password security, we will be looking into using Connectotel Password Policy Manager (http://www.connectotel.com/ppm/), a client and administrator snap-in that can be used to enforce strong passwords.

Beyond the above situation in which the initial password doesn't meet the complexity requirement, there is an additional problem with initial passwords. The first time a user logs in they are prompted to change their password, however changing it at that login causes a Password Synchronization Error stating "A minimum password age restriction has been set on your account. You cannot change your NT/2000 password at this time." Obviously the problem has to do with the one day minimum password age set by the template.

Though Windows has a minimum password age to prevent a user from changing their password repeatedly until they get back to their original password, this is not necessary in Netware. As Novell describes in TID 10021212, the number of passwords kept is based upon the time it would take to go through the entire cycle of passwords. If a user only changes their password when it is required the server only tracks eight passwords, however if the user changes it more frequently than required the server will

---

[21] Because of Hyena's expectation that the computer was part of a domain, I was not able to save a report however I was able to copy it to a notepad document which I was able to clean up for easier use here..

[22] All of the installed software as outlined in Section 2 was tested, however, the applications discussed here are considered the most vital. There weren't any problems found with any of the software not discussed here.

24

track passwords for eight times the number of days between required changes, in this case 720 days (8*90 days). Theoretically, if someone had an automated script they could take up a bit of memory by continuously changing passwords for 720 days, however, the danger is probably insignificant, compared to the benefit of requiring almost two years before the user could reuse a password.

5.2.2 Office XP Standard

There were no problems working with any documents in Word, Excel or PowerPoint. Using FileMon and RegMon (both programs are by Sysinternals – www.sysinternal.com) to look for any failed file or registry access attempts revealed a number of attempts to access common files like shell32.dll, however, these attempts were followed immediately by successes as seen in the following exert:

```
2032  9:58:41 AM  WINWORD.EXE:924   IRP_MJ_CREATE
      C:\WINNT\System32\shell32.dll ACCESS DENIED     Attributes: N Options:
Open
2033  9:58:41 AM  WINWORD.EXE:924   IRP_MJ_CREATE
      C:\WINNT\System32\shell32.dll SUCCESS      Attributes: N Options: Open
2034  9:58:41 AM  WINWORD.EXE:924   IRP_MJ_QUERY_INFORMATION
      C:\WINNT\System32\shell32.dll SUCCESS      FileInternalInformation
```

Additionally, these access issues didn't seem to have a negative impact on the user interaction and were also found on an identical system that hadn't had the w2k_workstation template applied. Because of the problems users of Word 97 on Windows 2000 had while attempting to use spelling and grammar tools (Microsoft Corporation [11]), particular attention was paid to these tools and they too generated no errors.

5.2.3 Eudora

Using Eudora to check and send email generated no problems. All messages were sent and received as desired and a Windump (the Windows port of tcpdump - http://netgroup-serv.polito.it/windump/) revealed an appropriate number of syn/syn+ack/fin connections. Figure 10 shows the email that was sent and received from this box as a test of the email capabilities.
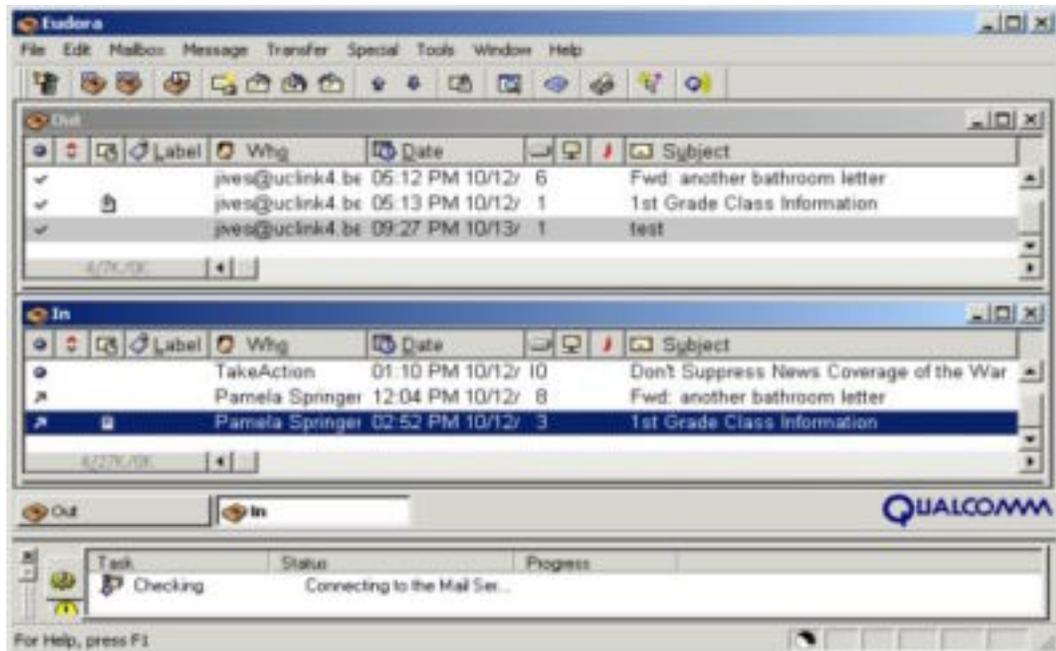
Figure 10 Eudora in Action

5.2.4 Printing – Acrobat

Printing, though becoming less crucial with the use of electronic communications, still plays an important role in the archiving and distribution of information. Today's printing is no longer just applying ink to paper but also includes printing into relatively stable digital forms, like PDF. In the traditional form of printing, attempts to print to an HP2200DN printer via TCP/IP generated no errors or problems, unfortunately the same can not be said for the printing to PDF.

To test Acrobat (distiller not the reader) I elected to try printing to PDF from multiple applications, including Internet Explorer, Word 2002 and, later, while trying to isolate the problems, notepad. In all of these instances I found that when I attempted to save the file to the desktop it never appeared there and no error messages were ever returned. Examining the port information in the print screen I noticed that the default port location was "C:\Document and Settings\All Users\Desktop*.pdf", but attempts to change the 'port' location didn't help. The Adobe knowledgebase document 324728 discussed a similar problem in Windows NT 4.0 in which saves to the desktop were being sent to the Default User's Desktop, however, it's suggested fixes alone did not work. In order to understand what was happening I ran Regmon and Filemon while attempting to print from word and notepad only to find the following errors:

From Word
```
15114 32.74702343 WINWORD.EXE:768    SetValue    HKLM\Software\Adobe\Acrobat
Distiller\5.0\PrinterJobControl\\4  ACCDENIED
16829 33.79307985 SPOOLSV.EXE:416    DeleteValueKey
     HKLM\Software\Adobe\Acrobat Distiller\5.0\PrinterJobControl\4
     ACCDENIED
```

From Notepad

```
21948 39.45220384 notepad.exe:764    SetValue    HKLM\Software\Adobe\Acrobat
Distiller\5.0\PrinterJobControl\\3  ACCDENIED
22086 39.50544944 SPOOLSV.EXE:416    DeleteValueKey
      HKLM\Software\Adobe\Acrobat Distiller\5.0\PrinterJobControl\3
      ACCDENIED
```

In both of these cases the program was attempting to write a value to the HKLM\Software\Acrobat\Acrobat Distiller\5.0\PrinterJobControl registry key, followed by SPOOLSV.EXE trying to delete it, but both programs were denied access to `SetValue`. In order to allow the printing of PDF files to the desktop it was necessary to change the permissions for the Users group to this registry key. The permissions to this key under the `w2k_workstation.inf` template had given the Users group read access to "this key and subkeys" and creator owner full control to only the subkeys. With these permissions, however, it wasn't possible for users to create print jobs correctly. By granting and removing individual rights to the Users group it was possible to determine that it was necessary to assign them the `Set Value` permission. Once this was done it was possible to 'print' jobs to the desktop without problem. Because this permissions only allow users the ability to create a new value and assign it data, it shouldn't represent a significant change in a systems overall security, especially since the values appear to be deleted once they job has been completed. Additionally, this fix works for all members of the User's group and can be altered in the template and reapplied as necessary.

5.3 System Protections

In terms of system stability and security, what a user is able to do is just as important as what they are not able to do, to this end I have elected to test this template against intentional misuse by the user. Users attempting to install personal software have always been a problem in managed environments, but the proliferation of free, recreational software available on the internet, has compounded the issue. User installed software can create conflicts with supported software and potential opening holes for worms and other attacks. Additionally, as some of this software is less truly recreational in nature, user installed software can also represent a significant amount of lost work viewed in the context of a large environment.

One of the more successful types of software of late, and one that seems to be blurring the lines between personal and professional life, is instant messaging. It was surprising to discover that, when a user level account attempted to install the Yahoo Instant Messenger (version 2001.9.4.1) they received a message saying that the installer couldn't reach the Yahoo Messenger Server. A subsequent Windump showed an identical pattern of syn/syn+ack/fin connections between the attempt to install as admin and the attempt to install as user (see Appendix C for Windump output). However, as the following logs from Filemon and Regmon revealed, `yahoo!_messenger_install.exe` created a file (GLB3A.TMP) which then made several failed attempts to create new keys in three different registry locations (specifically: HKLM\Software\Microsoft\Tracing, HKLM\Software\Novell\Library, and HKLM\Software\Novell\Winsock 2\ClassInfo) and was denied access.

27

Filemon
```
243   12:02:52 PM yahoo!_messenge:748    IRP_MJ_CREATE
      C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\GLB3A.tmp    SUCCESS        Attributes:
N Options: Create
244   12:02:52 PM yahoo!_messenge:748    IRP_MJ_CLEANUP
      C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\GLB3A.tmp    SUCCESS
245   12:02:52 PM yahoo!_messenge:748    IRP_MJ_CLOSE
      C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\GLB3A.tmp    SUCCESS
```

Regmon
```
85    10.94133556 GLB3A.tmp:524     CreateKey
      HKLM\Software\Microsoft\Tracing    ACCDENIED
86    10.96103806 GLB3A.tmp:524     CreateKey
      HKLM\Software\Microsoft\Tracing    ACCDENIED
[…]
93    11.15272947 GLB3A.tmp:524     CreateKey    HKLM\SOFTWARE\NOVELL\LIBRARY
      ACCDENIED
94    11.15305884 GLB3A.tmp:524     CreateKey    HKLM\SOFTWARE\NOVELL\LIBRARY
      ACCDENIED
96    12.15324322 GLB3A.tmp:524     CreateKey    HKLM\Software\Novell\Winsock
2\ClassInfo ACCDENIED
97    12.15397180 GLB3A.tmp:524     CreateKey    HKLM\Software\Novell\Winsock
2\ClassInfo ACCDENIED
```

It was apparently this inability to CreateKeys that caused the Yahoo! Instant Messenger Installer to fail and generate a false report of a server connection problem.

Another type of application that has become really popular on campuses and elsewhere over the last couple of years has been is personal files sharing utilities like Napster and Gnutella. Because of the questionable legality of these programs and because they provide an access point for someone to pull files off of the local workstation, tests were also run to see if a program like Gnotella v.1.0.5 (a Gnutella client found at http://www.gnotella.com) could be installed and run. Like Yahoo Instant Messaging, Gnotella also failed to install properly and could not be run. Unlike Yahoo! Instant Messaging, however, Gnotella did get much farther into the install process actually placing files in the user's profile in C:\Documents and Settings\. Though the install program was able to install part of the software, it was unable to install several key files into \Winnt\System32. This failure resulted in the application failing to run when launched.

5.4   Template Evaluation

Overall, the NSA w2k_workstation.inf template is very strong and represents a good starting point for use in an open environment, however, it is not without its problems and weaknesses. Like many security templates and guidelines, the NSA assumes a strong system of firewalls and stringently managed desktops, unfortunately many Universities lack this sort of across the board support and security. In this sort of environment, even those computers that are tightly managed are vulnerable to attacks from both on and off of campus.

5.4.1 General Recommendations

In general there are several areas I would have liked to have seen better secured by the template, foremost on that list is System Services. It is unfortunate, in my evaluation, that this template doesn't take the approach of locking down all non-essential or frequently used functions and allowing the administrator to only open the system as necessary. Had the template taken this approach services such as the Fax Service, which are only rarely used in networked environments, would be locked down. Admittedly, there aren't any known vulnerabilities in the Fax Service at this time, but, as a general rule it is essential that only necessary functions should be running on a computer. Along these same lines, the NSA template should have been particularly interested in disabling the Telnet service. Since Telnet has historically been a notoriously dangerous system with passwords being sent as clear text across the network, I feel it is irresponsible of Microsoft to have installed it and every available step should be taken to ensure that it isn't misused[23] (Norris).

A discussion of the weaknesses in this template's Restricted Group settings would not be complete without a discussion of the TelnetClients and Backup Operators groups. Though not possible to do exclusively with a template, the documentation for this template should have also discussed the merits of creating a TelnetClients group (Microsoft Corporation [3]) and assigning it the Restricted Groups portion of the template as a form of defense-in-depth, preventing telnet access should the service be turned on negligently or via Trojan horse. This is particularly important in open environments where telnet port probes are frequent[24]. Additionally, under the w2k_workstation template the Backup Operator's rights to backup and restore files have been eliminated along with all other explicitly assigned rights. As a result, it makes sense to also include Backup Operators as a restricted group, for the same reasons that it made sense to place the Power Users group into the restricted groups list, to keep user distinctions clear and group assignments as simple and clean as possible.

The final area that I see as being left with insufficient protection is %SystemDrive%\i386. Some software manufacturers place the i386 folder from the Windows installation CD on the %SystemDrive% (usually C:\). This is done so that users can easily install (or reinstall) operating components and software. Though many sites remove this folder either by erasing it, rebuilding the computer from scratch or by using a hard disk imaging program like Norton Ghost (http://enterprisesecurity.symantec.com/products/products.cfm?productID=3), sites that don't should secure it so that only Administrators will have access. The danger in the i386 folder comes from two related issues. The first problem is that i386 contains files that, in their proper place are out of the reach of the user, such as regedit.exe which can be found at i386\regedit.exe. Similarly, i386 also contains system files that may have been replaced in subsequent hotfixes and service packs because of insecurities found in their applications.

---

[23] It is possible to provide some password security to to a Windows 2000 computer using IPSec, however, this requires an understanding of IPSec and some extra configuration.

[24] Looking at personal firewall logs on my workstation reveals an average of 2-3 telnet port probes a week.

5.4.2 Environmentally Specific Recommendations

In addition to the above issues which deal with general weaknesses in the template, there are a number of changes that need to be performed to the template to facilitate its use in our environment. As discussed earlier, there are a couple of password related settings (password length being the most significant) that could not be used in this particular environment and were changed prior to application. However, beyond that, testing showed that in a Netware and ZENworks environment password management, is best left to the server. This is not to suggest that the settings on the workstation should be left undefined, only that the settings should be, at most equivalent (in terms of password management) to that of the server, and more likely a little looser with regard to password change frequency and password age so as to not cause any conflicts.

Additionally, in environments such as this, where Acrobat Distiller is commonly deployed, the template should be modified to give Users the `Set Value` permission to the Hkey_Local_Machine\Software\Acrobat\Acrobat Distiller\5.0\PrinterJobControl registry subkey. Going forward it is my intention to work with our support staff to build a catalog of these sorts of issues so that individual 'compatibility' templates can be generated and maintained for all of the software we use.

5.5 Conclusions and Topics for Further Research

In a rapidly changing environment, any security change has the potential of creating repercussions for the entire environment, however, the changes in w2k_workstation.inf, occurred with what ultimately were only minor conflicts in this Netware environment. Perhaps the most impressive thing about implementing this template wasn't the level of security it achieved, but the way in which the errors it caused were, overall, fairly easily diagnosed and solved. It had been my anticipation that a template that caused this many changes could have been very dangerous when applied directly to a workstation without any special configurations in place. What this seems to demonstrate, more than anything else, is the degree to which the Netware and Windows security are independent of each other, and while this independence comes with the overhead of needing to understand both, it also has the benefit of not relying exclusively on one security paradigm.

While this testing and analysis occurred with only minor difficulties there are always a number of variables that can be tested and researched further. Over the coming year we are planning on rolling out Netware 6 and deploying the full version of ZENworks. As part of the Netware 6 rollout it will be necessary to test our security templates and procedures against the new 'thin' client methods (iFolder and Netdrive) used to access files on the server. Of particular concern in this testing will be the security of the iFolder software which facilitates the synchronization of files between the local computer and the server and which the data for transit (Novell[3]). Also of great concern, though from more of a server security standpoint (as compared to the workstation), will be the security of NetStorage which allows individuals to connect to a Netware server using HTTP, HTTPS, HTML, XML, and WebDAV (Novell [2]). Similarly, it is important to do test and analyze the implications of our ZENworks 3.2 (currently the latest released version) deployment. With version 3.2 we will have the ability to do remote management of the desktop to a much higher degree. In addition to being able

to install applications and apply templates remotely (and to a greater degree than currently feasible), support staff will have the ability to remotely control the computer. The security of this, as well as the templates effects on this ability should be researched and tested thoroughly.

Appendix A – Test System Configuration

Workstation Operating System:
OS Version – Windows 2000 with Service Pack 2 Build 2195
File System – NTFSv5
Installation options – Default
Network Options – Custom without `Client for Microsoft Networks` and `File and Printer Sharing for Microsoft Networks`
Networking Protocols – TCP/IP only

Server Operating System:
OS Version – Netware 5.1 with Service Pack 3
File Name Support – Standard and Long
Networking Protocols – TCP/IP and IPX/SPX
ZENworks Starter Pack

Software:
Internet Explorer 5.5 with SP2 – Upgraded to 5.5 SP2 with default options from IE 5.0
Netscape 4.78 base install with High Encryption – Installed to default location leaving IE as default browser, also installed without resetting home or search pages.
Eudora – Installed to default location with all default settings
Adobe Acrobat Reader – Installed to default location with default settings
Office XP – Custom install without Outlook, but with typical settings for all other options
Netware Client 4.8sp3 – Installed with only ZENworks Desktop Manager and Novell Application Launcher options, Connects using the IP only to NDS
Norton Antivirus Corporate Edition – Installed to default location as an unmanaged client
Winzip – Installed to default location in classic mode
HyperSnap – Installed to default location with default options
MetaFrame – Installed to default location with default options

Printing:
HP 2200DN – connected via Windows 2000 IP printing
Adobe Acrobat Distiller 5.0 – Installed with default settings

Appendix B – seceditAnalysis.bat

The following script can be used to periodically analyze the system against a template and to record the results to a file named after the computer and the date in %systemroot%\security\logs\.

```
@echo off
REM *************************************************************
REM
REM  seceditAnalysis.bat - performs a secedit.exe /analyze routine
REM  and stores results to a file named <computername>--<date>.log
REM  located in %systemroot%\security\logs\
REM
REM *************************************************************

set secPath=%systemroot%\security

REM Pull the current system date and parse it into year, month and day
@for /f "tokens=1,2,3,4 delims=/ " %%a in ( 'date/t' ) do @set year=%%d
@for /f "tokens=1,2,3,4 delims=/ " %%a in ( 'date/t' ) do @set month=%%b
@for /f "tokens=1,2,3,4 delims=/ " %%a in ( 'date/t' ) do @set day=%%c
set logName=%computername%--%month%-%day%-%year%.log

REM the following should all appear on one line in the batch file
%systemroot%\system32\secedit.exe /analyze /db
     %secPath%\database\w2k_workstation.sdb /cfg
     %secPath%\templates\w2k_workstation.inf /log %secPath%\logs\%logName%
     /verbose
```

33

Appendix C – User Rights

The following user rights were taken by Hyena v3.0 (http://www.systemtools.com/hyena/) and are used to verify the user rights were applied correctly from the w2k_workstation.in template.

Object Name	Member	Access	Path	Size
SeAssignPrimaryTokenPrivilege	(None)	Replace a process level token	\\IGATE2	n/a
SeAuditPrivilege	(None)	Generate security audits	\\IGATE2	n/a
SeBackupPrivilege	Administrators	Back up files and directories	\\IGATE2	n/a
SeBatchLogonRight	(None)	SeBatchLogonRight	\\IGATE2	n/a
SeChangeNotifyPrivilege	Users	Bypass traverse checking	\\IGATE2	n/a
SeCreatePagefilePrivilege	Administrators	Create a pagefile	\\IGATE2	n/a
SeCreatePermanentPrivilege	(None)	Create permanent shared objects	\\IGATE2	n/a
SeCreateTokenPrivilege	(None)	Create a token object	\\IGATE2	n/a
SeDebugPrivilege	(None)	Debug programs	\\IGATE2	n/a
SeDenyBatchLogonRight	(None)	SeDenyBatchLogonRight	\\IGATE2	n/a
SeDenyInteractiveLogonRight	(None)	SeDenyInteractiveLogonRight	\\IGATE2	n/a
SeDenyNetworkLogonRight	(None)	SeDenyNetworkLogonRight	\\IGATE2	n/a
SeDenyServiceLogonRight	(None)	SeDenyServiceLogonRight	\\IGATE2	n/a
SeEnableDelegationPrivilege	(None)	Enable computer and user accounts to be trusted for delegation	\\IGATE2	n/a
SeIncreaseBasePriorityPrivilege	Administrators	Increase scheduling priority	\\IGATE2	n/a
SeIncreaseQuotaPrivilege	Administrators	Increase quotas	\\IGATE2	n/a
SeInteractiveLogonRight	Administrators	SeInteractiveLogonRight	\\IGATE2	n/a
SeInteractiveLogonRight	Users	SeInteractiveLogonRight	\\IGATE2	n/a
SeLoadDriverPrivilege	Administrators	Load and unload device drivers	\\IGATE2	n/a
SeLockMemoryPrivilege	(None)	Lock pages in memory	\\IGATE2	n/a
SeMachineAccountPrivilege	(None)	Add workstations to domain	\\IGATE2	n/a
SeNetworkLogonRight	Administrators	SeNetworkLogonRight	\\IGATE2	n/a
SeNetworkLogonRight	Users	SeNetworkLogonRight	\\IGATE2	n/a
SeProfileSingleProcessPrivilege	Administrators	Profile single process	\\IGATE2	n/a
SeRemoteShutdownPrivilege	Administrators	Force shutdown from a remote system	\\IGATE2	n/a
SeRestorePrivilege	Administrators	Restore files and directories	\\IGATE2	n/a
SeSecurityPrivilege	Administrators	Manage auditing and security log	\\IGATE2	n/a
SeServiceLogonRight	(None)	SeServiceLogonRight	\\IGATE2	n/a
SeShutdownPrivilege	Administrators	Shut down the system	\\IGATE2	n/a
SeShutdownPrivilege	Users	Shut down the system	\\IGATE2	n/a
SeSyncAgentPrivilege	(None)	Synchronize directory service data	\\IGATE2	n/a
SeSystemEnvironmentPrivilege	Administrators	Modify firmware environment values	\\IGATE2	n/a
SeSystemProfilePrivilege	Administrators	Profile system performance	\\IGATE2	n/a
SeSystemtimePrivilege	Administrators	Change the system time	\\IGATE2	n/a
SeTakeOwnershipPrivilege	Administrators	Take ownership of files or other objects	\\IGATE2	n/a
SeTcbPrivilege	(None)	Act as part of the operating system	\\IGATE2	n/a
SeUndockPrivilege	Administrators	Remove computer from docking station	\\IGATE2	n/a
SeUndockPrivilege	Users	Remove computer from docking station	\\IGATE2	n/a

34

Appendix D – Yahoo Instant Messenger WinDump Logs

The following Windumps (a Windows port of the UNIX program TCPDump) shows that there were virtually no differences between a user attempting to install Yahoo nstant Messenger as themselves and the same user attempting to install it using the Windows 2000 "Run as" option.

Windump for user

```
17:46:31.625844 igate2.CChem.Berkeley.EDU.1140 > dl1.yahoo.com.80: S
   678278556:678278556(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)
17:46:31.631238 dl1.yahoo.com.80 > igate2.CChem.Berkeley.EDU.1140: S
   1851924055:1851924055(0) ack 678278557 win 1 <mss 1460> (DF)
17:46:31.631379 igate2.CChem.Berkeley.EDU.1140 > dl1.yahoo.com.80: . ack 1
   win 17520 (DF)
17:46:31.631806 igate2.CChem.Berkeley.EDU.1140 > dl1.yahoo.com.80: . 1:2(1)
   ack 1 win 17520 (DF)
17:46:31.735500 dl1.yahoo.com.80 > igate2.CChem.Berkeley.EDU.1140: . ack 2
   win 32767 (DF)
17:46:31.735655 igate2.CChem.Berkeley.EDU.1140 > dl1.yahoo.com.80: P 2:56(54)
   ack 1 win 17520 (DF)
17:46:31.835363 dl1.yahoo.com.80 > igate2.CChem.Berkeley.EDU.1140: . ack 56
   win 32767 (DF)
17:46:32.335259 dl1.yahoo.com.80 > igate2.CChem.Berkeley.EDU.1140: P
   1:1329(1328) ack 56 win 32767 (DF)
17:46:32.335348 dl1.yahoo.com.80 > igate2.CChem.Berkeley.EDU.1140: F
   1329:1329(0) ack 56 win 65535 (DF)
17:46:32.336512 igate2.CChem.Berkeley.EDU.1140 > dl1.yahoo.com.80: . ack 1330
   win 16192 (DF)
17:46:32.336699 igate2.CChem.Berkeley.EDU.1140 > dl1.yahoo.com.80: F 56:56(0)
   ack 1330 win 16192 (DF)
17:46:32.342197 dl1.yahoo.com.80 > igate2.CChem.Berkeley.EDU.1140: . ack 57
   win 32767 (DF)
17:46:32.348503 igate2.CChem.Berkeley.EDU.1141 > dl1.yahoo.com.80: S
   678498398:678498398(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)
17:46:32.353423 dl1.yahoo.com.80 > igate2.CChem.Berkeley.EDU.1141: S
   1696890575:1696890575(0) ack 678498399 win 1 <mss 1460> (DF)
17:46:32.353532 igate2.CChem.Berkeley.EDU.1141 > dl1.yahoo.com.80: . ack 1
   win 17520 (DF)
17:46:32.353853 igate2.CChem.Berkeley.EDU.1141 > dl1.yahoo.com.80: . 1:2(1)
   ack 1 win 17520 (DF)
17:46:32.454604 dl1.yahoo.com.80 > igate2.CChem.Berkeley.EDU.1141: . ack 2
   win 32767 (DF)
17:46:32.454765 igate2.CChem.Berkeley.EDU.1141 > dl1.yahoo.com.80: P 2:56(54)
   ack 1 win 17520 (DF)
17:46:32.490448 dl1.yahoo.com.80 > igate2.CChem.Berkeley.EDU.1141: P
   1:224(223) ack 56 win 32767 (DF)
17:46:32.490526 dl1.yahoo.com.80 > igate2.CChem.Berkeley.EDU.1141: F
   224:224(0) ack 56 win 65535 (DF)
17:46:32.491364 igate2.CChem.Berkeley.EDU.1141 > dl1.yahoo.com.80: . ack 225
   win 17297 (DF)
17:46:32.491562 igate2.CChem.Berkeley.EDU.1141 > dl1.yahoo.com.80: F 56:56(0)
   ack 225 win 17297 (DF)
17:46:32.495962 dl1.yahoo.com.80 > igate2.CChem.Berkeley.EDU.1141: . ack 57
   win 32767 (DF)
```

35

Windump for User posing as Admin (using "Run as")

```
17:47:24.004637 igate2.CChem.Berkeley.EDU.1142 > dl1.yahoo.com.80: S
    691460660:691460660(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)
17:47:24.009218 dl1.yahoo.com.80 > igate2.CChem.Berkeley.EDU.1142: S
    4047375333:4047375333(0) ack 691460661 win 1 <mss 1460> (DF)
17:47:24.009722 igate2.CChem.Berkeley.EDU.1142 > dl1.yahoo.com.80: . ack 1
    win 17520 (DF)
17:47:24.009790 igate2.CChem.Berkeley.EDU.1142 > dl1.yahoo.com.80: . 1:2(1)
    ack 1 win 17520 (DF)
17:47:24.110691 dl1.yahoo.com.80 > igate2.CChem.Berkeley.EDU.1142: . ack 2
    win 32767 (DF)
17:47:24.110907 igate2.CChem.Berkeley.EDU.1142 > dl1.yahoo.com.80: P
    2:124(122) ack 1 win 17520 (DF)
17:47:24.210025 dl1.yahoo.com.80 > igate2.CChem.Berkeley.EDU.1142: . ack 124
    win 32767 (DF)
17:47:24.684895 dl1.yahoo.com.80 > igate2.CChem.Berkeley.EDU.1142: P
    1:1329(1328) ack 124 win 32767 (DF)
17:47:24.684954 dl1.yahoo.com.80 > igate2.CChem.Berkeley.EDU.1142: F
    1329:1329(0) ack 124 win 65535 (DF)
17:47:24.685109 igate2.CChem.Berkeley.EDU.1142 > dl1.yahoo.com.80: . ack 1330
    win 16192 (DF)
17:47:24.685700 igate2.CChem.Berkeley.EDU.1142 > dl1.yahoo.com.80: F
    124:124(0) ack 1330 win 16192 (DF)
17:47:24.690874 dl1.yahoo.com.80 > igate2.CChem.Berkeley.EDU.1142: . ack 125
    win 32767 (DF)
17:47:24.698003 igate2.CChem.Berkeley.EDU.1143 > dl1.yahoo.com.80: S
    691701125:691701125(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)
17:47:24.702455 dl1.yahoo.com.80 > igate2.CChem.Berkeley.EDU.1143: S
    3430764558:3430764558(0) ack 691701126 win 1 <mss 1460> (DF)
17:47:24.702584 igate2.CChem.Berkeley.EDU.1143 > dl1.yahoo.com.80: . ack 1
    win 17520 (DF)
17:47:24.702837 igate2.CChem.Berkeley.EDU.1143 > dl1.yahoo.com.80: . 1:2(1)
    ack 1 win 17520 (DF)
17:47:24.800056 dl1.yahoo.com.80 > igate2.CChem.Berkeley.EDU.1143: . ack 2
    win 32767 (DF)
17:47:24.800274 igate2.CChem.Berkeley.EDU.1143 > dl1.yahoo.com.80: P
    2:124(122) ack 1 win 17520 (DF)
17:47:24.862140 dl1.yahoo.com.80 > igate2.CChem.Berkeley.EDU.1143: P
    1:1329(1328) ack 124 win 32767 (DF)
17:47:24.862203 dl1.yahoo.com.80 > igate2.CChem.Berkeley.EDU.1143: F
    1329:1329(0) ack 124 win 65535 (DF)
17:47:24.863363 igate2.CChem.Berkeley.EDU.1143 > dl1.yahoo.com.80: . ack 1330
    win 16192 (DF)
17:47:24.863491 igate2.CChem.Berkeley.EDU.1143 > dl1.yahoo.com.80: F
    124:124(0) ack 1330 win 16192 (DF)
17:47:24.867837 dl1.yahoo.com.80 > igate2.CChem.Berkeley.EDU.1143: . ack 125
    win 32767 (DF)
```

36

Bibliography

Ackerman, Pilar, et. al., <u>Windows 2000 Professional Resource Kit</u>. Redmond, Washington: Microsoft Press Inc, 2000.

Foster, Gerald. <u>Desktop Management with Novell ZENworks.</u> Sebastopol: O'Reilly & Associates, Inc, 2000.

Haney, Julie M. "Guide to Securing Microsoft Windows 2000® Group Policy: Security Configuration Tool Set" Version 1.0. 17 May, 2001. URL: http://nsa2.www.conxion.com/win2k/r1/guide_to_securing_microsoft_windows_2000_sct.pdf (16 Sept. 2001).

Lundman, Don , et. al., <u>Windows 2000 Server Resource Kit Distributed Systems Guide</u>. Redmond: Microsoft Press Inc, 2000.

Microsoft Corporation. "Cached Logon Information" 15Aug. 2001. URL: http://support.microsoft.com/support/kb/articles/Q172/9/31.ASP (7 Oct. 2001).

Microsoft Corporation. "Cannot Install or Run Some Programs with Standard User Account" 10 Oct. 2001. URL: http://support.microsoft.com/support/kb/articles/Q248/0/03.ASP (12 Oct. 2001).

Microsoft Corporation. "Creating a Local Group Can Restrict Other Users From Gaining Access to a Windows 2000-Based Computer through Telnet" 31 July 2001. URL: http://support.microsoft.com/support/kb/articles/Q250/9/08.asp (12 Oct. 2001).

Microsoft Corporation. "Default Access Control Settings in Windows 2000" April 1999. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/maintain/featusability/secdefs.asp (7 Oct. 2001).

Microsoft Corporation. "Enabling Strong Password Functionality in Windows 2000 – Q225230" 1 Jan. 2000. URL: http://support.microsoft.com/directory/article.asp?ID=KB;EN-US;Q225230 (21 Sept. 2001).

Microsoft Corporation. "GetAdmin Utility Grants Users Administrative Rights(Q146965)" 8 Aug. 2001. URL: http://support.microsoft.com/support/kb/articles/Q146/9/65.asp (3 Oct. 2001).

Microsoft Corporation. "How to Modify the Default Group Policy Refresh Interval(Q203607)" 1 Jan. 2000. URL: http://support.microsoft.com/support/kb/articles/Q203/6/07.asp (14 Oct. 2001).

Microsoft Corporation. "Microsoft Security Bulletin MS01-007" 9 Feb. 2001. URL:
http://www.microsoft.com/technet/security/bulletin/MS01-007.asp
(15 Oct. 2001).

Microsoft Corporation. "Run" 2001 URL:
http://www.microsoft.com/windows2000/techinfo/reskit/en-us/regentry/9331.asp (1 Oct.
2001)

Microsoft Corporation. "Store password using reversible encryption for all users in the
domain" URL: http://msdn.microsoft.com/library/default.asp?url=/library/en-
us/gp/505.asp (30 Sept. 2001).

Microsoft Corporation. "WD97: Spelling, Grammar Not Avaiable in Word Running on
Windows 2000" 9 Feb. 2001URL:
http://support.microsoft.com/support/kb/articles/Q257/6/43.ASP (7 Oct. 2001).

Norberg, Stefan. Securing Windows NT/2000 Servers for the Internet. Sebastopol:
O'Reilly & Associates, Inc, 2001.

Norris, Ed. "Analysis of a Telnet Session Hijack via Spoofed MAC Addresses and
Session Resynchronization" 20 Mar. 2001. URL:
http://www.sans.org/infosecFAQ/threats/hijack.htm (15 Oct. 2001).

Novell, Inc. "Client32 and MS Client for NW Comparison" 24 May 1999. URL:
http://support.novell.com/cgi-bin/search/searchtid.cgi?/2951164.htm (Oct. 12 2001).

Novell, Inc. "NetStorage Overview and Installation" URL:
http://www.novell.com/documentation/lg/nw6p/pdfdoc/netstorgs.pdf (15 Oct. 2001).

Novell, Inc. "What is Novell iFolder?" URL:
http://www.novell.com/documentation/lg/ifolder/ifolder/data/ab3op88.html (15 Oct.
2001).

Novell, Inc. "What is the meaning of Require Unique Passwords?" 6 Nov. 1999. URL:
http://support.novell.com/cgi-bin/search/searchtid.cgi?/10021212.htm (29 June 2001).