Extreme Hardening of Windows 2000 Professional: A Case Study

John H Scanlan IV

GIAC Security Essentials Certification (GSEC)
Practical V1.4b option 2
November 2003

Abstract

I am an Instructor / teacher in the military. My primary job is to teach everything involved with the setup and configuration a Windows NT domain in a tactical environment. In one of our many classrooms, I have 10 servers running Windows NT 4.0 Server and 20 workstations with Windows 2000 Professional in 3 classrooms. Since I am an instructor in the military, I have the privilege and luxury to make everything uniform and implement as many restrictions as I see fit while still allowing the student use the computer to learn. Focusing on the 20 Windows 2000 workstations, I decided to come up with a solution to reduce the administrative burden of restoring 20 computers back to their original condition after every cycle of students. At the same time, the computers needed to be locked down so wayward students would not loose focus or be tempted to try to see what they could get away with.

Since every computer is the same make and model and each computer had the exact same components, I decided that an image or clone was the best choice. I tasked myself to develop and create a Windows 2000 clone. This new clone disk was derived from numerous resources, my own knowledge, and modeled after the Defense in Depth strategy. [1] By creating this clone, I have saved and will potentially save hundreds of hours a year otherwise spent restoring these computers back to their original condition every ten weeks.

In the beginning…

Imagine three classrooms with 20 computers each. All three classrooms have identical computers with the exact same Windows 2000 Professional load on each of them. The classroom is sectioned into 10 intranets to simulate the student setting up a small domain referred to as their “site”. Each intranet is essentially a Local Area Network. Each Local Area Network connects to their respective neighbors to simulate setting up a Wide Area Network. Within each Local Area Network, the students have two Windows 2000 Professional workstations and one Windows NT 4.0 Server. None of the Windows 2000 workstations or Windows NT Servers have a “live” connection to the Internet.

I am going to be focusing on the 60 workstations with Windows 2000 Professional hereafter know as “Student PC’s”. Every student can logon to his or her Student PC as the Administrator and everyone will use the same administrator password since this is a training environment. The student is given a simple IP scheme of 192.168.X.0 where “X” is their “site” number and they all will be told what subnet mask to use, usually /27 or 255.255.255.224. Once the student sets up their individual Local Area Network, each StudentPC should be able to communicate with every other StudentPC in the classroom. To test this, the students will ping the IP address of everyone in the room.

Initially, it was considered that setting up our classrooms like this was a good idea due to simplicity and ease of setup. We soon found out that this was a huge problem. To state the obvious, each student is given access to the administrator account with the password being the same for every PC. This sets the stage for user intervention throughout the class. One student will discover the “NET SEND” command and then every body in class is shooting messages as fast as they can type. Once they figure out they are armed with access to every computer, they start trying anything they can just to see what they get away with. All it takes is one student to figure out something, like connecting to and editing a remote registry. [2] The student tells his buddy, and then the whole class is trying to see what they can do. Sometimes this can be amusing but at the same time it can be very harmful. Since most of these students are young and inexperienced, they have a tendency to make simple mistakes in the registry of either their own registry or someone else’s registry and then it crashes. One of many lessons learned through experience. Accidental mistakes like this ultimately affects the learning as a whole because I have to take time away from teaching to fix a student’s computer.

Based upon my experience, every student has the desire be an individual. With this in mind, every student will set a different background, every screen saver will be different, and students tend to change either their administrator password or set a screen saver password. Troubleshooting a student’s computer becomes a nightmare when you have to try to figure out a different password for every student or wait for that student to enter his unique password.

I initially developed a clone disk with very simple restrictions to stop users from changing simple settings like their background and screen saver. This seemed to work for about a week or so. I soon found students circumventing these simple restrictions with ease. I then created another clone disk with updated restrictions to only have them bypassed again. This was discouraging and at the same time intriguing.

During development….

I have to give credit to SANS for giving me the incredible resource of Volume Two, SANS Security Essentials with CISSP CBK. [3] Section V was an outstanding reference during my trials and tribulations. Another very good reference is “Windows 2000 Professional Baseline Security Checklist”. [4] This reference helped me in the thinking process for developing this Clone CD.

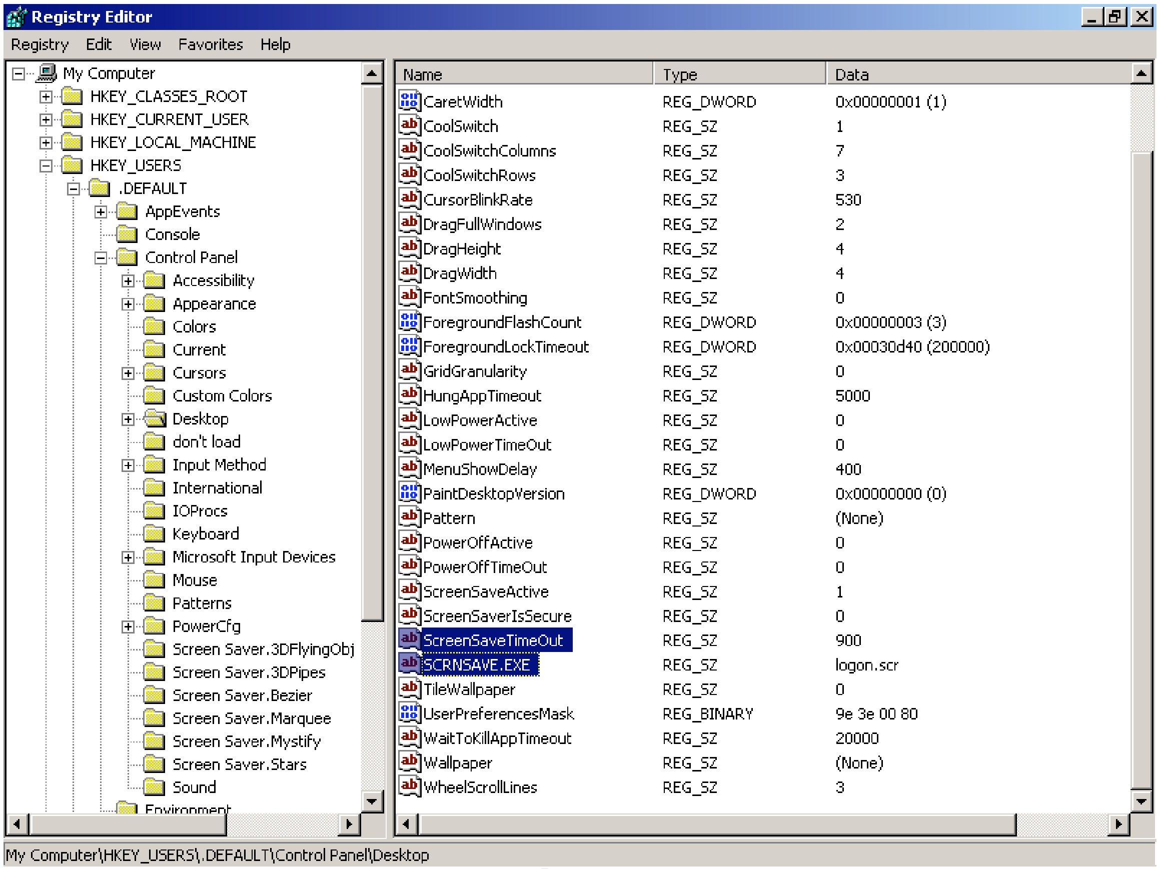
During the development of the Clone CD, I enlisted the help from many of my former students. Each time I would make a change to the clone, they would be there to find another way to bypass what I have done or find another vulnerability.

I started implementing security restrictions using the Local Computer Policy. The Local Computer Policy is an outstanding tool once you understand what you would like to restrict. I didn’t use any resources when using the Local Computer Policy; it was more or less trial and error. I used the Microsoft Management Console (MMC) to get to the Local Computer Policy. Every restriction starts under; Local Computer Policy, User Configuration, Administrative Templates…

Do to the length of the restrictions that I have set; I have created Appendix A with all of the restrictions. There is one thing to keep in mind when making or setting these restrictions. Every restriction you set here affects every user, including the Administrator. After some research, I soon find out a way to create a backdoor, if you will. I created an account called “Instructor” before I made the restrictions in the Local Computer Policy. I still want students to be able to use the Administrator account so they may join the computer to a domain. Here are the steps for the backdoor. 1.) Make all necessary changes in the Local Computer Policy. 2.) Reboot the computer. 3.) Login to all accounts. 4.) Login as Instructor. 5.) Navigate to C:/winnt/system32/grouppolicy/user. 6.) Create a new folder, to make it easier, “Backup”. 7.) Cut Registry.pol. 8.) Paste inside of “Backup”. 9.) Reboot the computer. 10.) When the computer boots up, login as the Instructor. 11.) Open the Command Prompt. 12.) Type in the following: at \\(computer name) (time) /interactive “gpedit.msc” (Computer name) is whatever the computer name / NetBIOS name is. (Time) works on one-minute intervals. Type in the time + one minute. Example… if the current time is 2:16 PM, type in 14:17. *Note… you must use the 24-hour time. 13.) The next thing you must do is reverse EVERY change that you have made in the Local Computer Policy. Although it was a daunting task, I made a list of every change so I could reference every change that I made. 14.) Navigate to C:/winnt/system32/grouppolicy/user/backup. 15.) Copy Registry.pol to C:/winnt/system32/grouppolicy/user. 16.) Reboot the computer. 17.) Logon to all accounts the check to see if the settings have taken effect. If you follow these 17 steps, you will have a "backdoor" to the computer that will bypass all of security settings have put in place. These 17 steps differ slightly from Microsoft's "HOW TO: Apply Local Policies to all Users Except Administrators on Windows 2000 in a Workgroup Setting". [5] Once you make these changes, that's it. If you make a change in the Local Computer Policy because you forgot something or need to add a restriction, you have start all over. If you make a change, you have essentially closed the "loop hole" you have created for yourself and now every setting applies to you. One of the main restrictions set now is disabling access to the registry. If you have access to the registry, you can change every restriction you have enforced.

With this in mind, there is one major registry setting I have made. There is a huge security "hole" using the default Windows screen saver. Whenever Windows 2000 Professional is first booted up and you leave it sit there, 15 minutes or 900 seconds later you get the default screen saver. I'm referring to logon.scr. With appropriate access, a user can change the default screen saver to open a command prompt. Changing this will give you a command prompt instead of the default screen saver. Why is this important to bring up? If the default screen saver is changed to a command prompt, a user can now navigate through the operating system before the security policy is implemented.
If you haven't tried this or forgot about this trick, please take the time to try this. I'm going to tell you briefly how to employ this trick, then I will tell you how to stop or prevent it.

First, navigate to C:/winnt/system32. This is where most of your system files are. Make a copy of CMD.exe. Rename it to logon2.scr. Rename logon.scr to logon1.scr. Go back to logon2.scr and remove the "2" so you now have a copy of CMD.exe named logon.scr. Open the registry and click on "edit" then "find". Type in logon.scr and press find, this will take you directly to where you need to go in the registry. Take a look at "ScreenSaveTimeOut". If you notice, the default value is 900. This value is 900 seconds or 15 minutes. Change this value to 30 seconds. Reboot the computer and wait 30 seconds. Viola, you now have access to the command prompt. From there, you can now access the registry and anything you want. To prevent this "hole", open the registry, click on edit, find and type in logon.scr. This will take you to the exact registry key. Change the "ScreenSaveTimeOut" key to 0. With the field set to 0 seconds, you will never get the default Windows screen saver thus preventing a user from getting the chance to bypass your security settings.



Name	Type	Data
CaretWidth	REG_DWORD	0x00000001 (1)
CoolSwitch	REG_SZ	1
CoolSwitchColumns	REG_SZ	7
CoolSwitchRows	REG_SZ	3
CursorBlinkRate	REG_SZ	530
DragFullWindows	REG_SZ	2
DragHeight	REG_SZ	4
DragWidth	REG_SZ	4
FontSmoothing	REG_SZ	0
ForegroundFlashCount	REG_DWORD	0x00000003 (3)
ForegroundLockTimeout	REG_DWORD	0x00030d40 (200000)
GridGranularity	REG_SZ	0
HungAppTimeout	REG_SZ	5000
LowPowerActive	REG_SZ	0
LowPowerTimeOut	REG_SZ	0
MenuShowDelay	REG_SZ	400
PaintDesktopVersion	REG_DWORD	0x00000000 (0)
Pattern	REG_SZ	(None)
PowerOffActive	REG_SZ	0
PowerOffTimeOut	REG_SZ	0
ScreenSaveActive	REG_SZ	1
ScreenSaverIsSecure	REG_SZ	0
ScreenSaveTimeOut	REG_SZ	900
SCRNSAVE.EXE	REG_SZ	logon.scr
TileWallpaper	REG_SZ	0
UserPreferencesMask	REG_BINARY	9e 3e 00 80
WaitToKillAppTimeout	REG_SZ	20000
Wallpaper	REG_SZ	(None)
WheelScrollLines	REG_SZ	3

My Computer\HKEY_USERS\.DEFAULT\Control Panel\Desktop

There are several things you can do if you have access to the registry, especially this portion of the registry. As you can see, SCRSAVE.EXE equals logon.scr. What if you change this to regedit.exe? It's a good thing I have set the restrictions so the users can't access the registry. This trick is also useful if you have forgot you password, lets say, the Administrator password on a system where you can logon as a regular user. [6] Using this way to bypass Windows security is more popular than you may think, be wary of users, they ARE smarter than you think or smarter than they lead on to be. The students that I see in my school, at such a young age of 18-23, know this just as well as us older folks know the ends and outs of Windows 3.11 or Windows 95.

Even though we have restricted access to the registry, and we have secured a "hole", there is still another vulnerability to be dealt with. I'm referring to files that have the ability to make changes to the registry. Specifically .REG, .VBS, .VBE, .JSF, .JSE, and .WSF files. A user who has knowledge of these files can be very dangerous. There is a way to combat these types of files from doing harm to your system. Referencing www.is-it-true.org, [7] I have used a registry file written by a friend of mine, who wishes to remain anonymous, and modified it a little. When you double click on this file, all six types of files open in Notepad. This is what it looks like:

REGEDIT4

--[Space]--

```
[HKEY_CLASSES_ROOT\JSFile\Shell]
@="Edit"
    --[Space]--
[HKEY_CLASSES_ROOT\JSEFile\Shell]
@="Edit"
    --[Space]--
[HKEY_CLASSES_ROOT\VBSFile\Shell]
@="Edit"
    --[Space]--
[HKEY_CLASSES_ROOT\VBEFile\Shell]
@="Edit"
    --[Space]--
[HKEY_CLASSES_ROOT\WSFFile\Shell]
@="Edit"
    --[Space]--
[HKEY_CLASSES_ROOT\REGFile\Shell]
@="Edit"
```

By setting these settings in the registry, you have now prevented a user from executing these file types from windows. These files will, however, still work if incorporated into an install program or under certain circumstances with DOS.
If you decide to write this registry file, there must be a space between each entry. You may cut and paste this directly into Notepad and delete the *--[Space]--*. Rename the .txt file to .reg and you are done. If you are not satisfied with the results of this registry file, you can change everything back by replacing "Edit" with "Open". The only bad thing is now you have to open the registry to reverse the changes because the last line prevents registry files from being executed. You will have to find each string and make your changes there.
Please read more about the registry before making any changes to the registry. Use this file at your own risk.

There is one more file type that I did not mention. The install files or .ini files. I actually watched one of my 18-year-old prodigy students write this .ini file right in front of me. He created a .ini file called "Test.ini".
Here is the text of what he wrote.

```
[version]
signature="$CHICAGO$"
LayoutFile=layout.inf
SetupClass=BASE
    --[Space]--
[DefaultInstall]
AddReg=Test.AddReg
    --[Space]--
[Test.AddReg]
```

```
HKCU,"Software\Microsoft\Windows\CurrentVersion\Policies\System","DisableRegistryTools",65537,0
```

“WOW” was the only thing I could say once he showed me this neat trick. This student enabled access to the registry by using an install file and setting “DisableRegistryTools” value to 0. A value of 0 means either off or disabled. All he had to do is search for any .ini file and open it so he can view it. He then copied some of the information from the file and pasted it to the file he just created. He then used “regsvc.exe” and “regwiz.exe” to find out the exact location of the correct registry key. He placed all of the information in the correct order, and that was it. He right clicked on the file and clicked install. Subsequently he proceeded to open “regedit.exe”. Needless to say, I was amazed. After witnessing this, I tried to combat this only to run into several problems. As soon as I started to set restrictions on the .ini files, some programs would not work correctly and I could not install programs correctly.

The fact that I witnessed the student using certain files, prompted me to investigate these certain files. I started a lengthy investigation on every executable file in the \system32 directory and other directories. To my amazement, there are many executable files throughout the whole Windows 2000 structure that can be used to circumvent many restrictions set on a computer. I am not going to go into great detail about every file and what it’s purpose is, however, I will let you know which files need special attention.

I have already shown you how to use AT.EXE so schedule a program to run. Here are a few more in no particular order:

FILES

Regedit.exe Updreg.exe Append.exe Attrib.exe Cacls.exe Cipher.exe
Cscript.exe Doskey.exe Dosx.exe Finger.exe Forcedos.exe Help.exe
IEshwiz.exe MMC.exe Mstask.exe Net.exe Net1.exe Netsh.exe Recover.exe
Regsvc.exe Regsvr32.exe Regwiz.exe Replace.exe Rexec.exe RSH.exe
Secedit.exe Sethc.exe Setreg.exe Share.exe Shrpubw.exe Sol.exe
Sysedit.exe Themes.exe User.exe Winmine.exe Wscript.exe Xcopy.exe
Appwiz.cpl Desk.cpl Main.cpl Compmgmt.msc Fsmgmt.msc gpedit.msc
Lusermgr.msc Secpol.msc Edit.com Qbasic.exe

FOLDERS

All folders that begin with… $NtUninstall dllcache GroupPolicy CSC HELP
Installer ServicePackFiles Backup Dell Dellutil I386 DOS

During my “trial and error” period of creating Image CD’s, I eventually set the attributes of every file and folder above to “hidden”. A co-worker mentioned “Security through Obscurity”. I remembered reading about it and hearing about it in the SANS Track 1 course but I didn’t remember exactly what it was about. After researching more on the Internet, I completely understood the perception behind “Security through Obscurity”. [8] There are many different views about “Security through Obscurity”, but it works well with what I am doing. After setting the attributes to hidden, I created another image for my smart students to play with. It did not take them long to figure out that the files were just hidden but still accessible. Some of the students found it aggravating that they could not click on “Tools, then Folder Options…”. When setting the restrictions in the Local Computer Policy, this option was disabled. This prevents users from being able to view the hidden files.

Before I start discussing user rights and permissions, I want to make it clear that I am using NTFS on the hard drive. If you use FAT or FAT32, you are just asking for trouble. The only type of file system that has any security is NTFS. Unlike FAT or FAT32, NTFS has a security tab that allows you to assign user rights and permissions. Also, with NTFS, you have an advanced tab that allows you to configure user right and permissions.

After the smart students “hacked” there way passed the security settings, I shifted my focus to “User Rights and File Permissions”. I started to mess around with file permissions early in my venture. Remember the Net Send issue mentioned earlier? I put a stop to Net Send messages by placing specific user rights on the Net.exe and Net1.exe command. After observing a student use the ATTRIB command, I started to invest a lot of time in user rights and permissions and what effect they would have on the overall outcome of my project. The ATTRIB command, if you are not familiar with it, will let you view and manage the attributes of any file.

As stated previously, I created a user account called “Instructor”. I have left the Administrator account alone. The “Instructor” account has “Full Control” on every file and folder listed above. The Administrator account and the Instructor account belong to the administrators group. This makes assigning permissions an overwhelming task. I actually right clicked on every file and folder to assign the appropriate permissions. I assigned the permissions as follows:
Administrator -- No Access
Instructor -- Full Access
I feel trial and error is a good way to learn in a controlled environment. There were three things I forgot to do. The first thing was the System account. The system account needs access to certain files for the operating system to function correctly. The second thing was the Users Group. Without setting user rights on the Users Group, a new user account could be created with access to every file or folder I wanted restricted. The third thing was the ability to Take Ownership of

Files and Objects. The student could login as the Administrator then take ownership of the files and then continue to wreak havoc. This meant that I had to make a change to the Local Group Policy. You guessed it, I had to start all over and reset the restrictions and then go back and make the “loophole“ for the administrators account. Here is what the file permissions look like after fixing the previous three problems.

Administrator -- No Access
Instructor -- Full Access
System -- Read & Execute
Users – No Access

Please take the time to research File Permissions before making any changes to the operating system. This will save you plenty of wasted hours trying to recover from a simple mistake.

Looking back on everything I have set, there is still another vulnerability that needs to be addressed: The help files. Although very helpful in most cases, the help files can be harmful if a user knows how to exploit them correctly. I am not talking about a crafty way to edit the help files; I’m talking about using them as they were intended. I have set restrictions to prevent the Administrator account to create new users. To get around this using the help files, all you have to is strike the “F1” key while looking at the desktop. You now see the helpful Windows 2000 help file. Click on search and type in “Add a new user to the computer”. Click on display. This is what you see.

To add a new user to the computer

1. Open Users and Passwords in Control Panel.
2. Click Add
3. Follow the instructions on the screen…

Click on the URL type link Users and Passwords and it will take you directly to the Users and Password screen where you can add users at will. You can now add a new user account and give this user administrative privileges that can access everything restricted. To prevent users from utilizing the help files, I have methodically located most of the most frequently used help files. These help files have the extension of .chm (compiled help files). I assigned user rights just like I assigned them for the other files and folders above. Now the student cannot use the help files to help bypass the security measures put in place. I understand that this is a very drastic step in locking down Windows 2000. If you are trying to lock down Windows 2000 and you do not want to go through the whole process of finding every help file as I have, pay special attention to “Windows.chm”. This is the main Windows help file and is usually located at: C:/WINNT /help.

Finding these vulnerabilities and preventing my students from exploiting them have eventually lead to the completion of the clone CD I have created.

The outcome…

After setting all of these restrictions, I have completed the Clone CD I originally tasked myself to complete. There are still some vulnerabilities that need to be addressed.

One of these vulnerabilities is the BIOS. When the computer boots up, anyone can access the BIOS. Since everyone has access to the BIOS, then anyone can set a BIOS password. The only way to overcome this is to set the BIOS password on every computer. I have decided not to use a universal password for the BIOS.

Another vulnerability is the floppy drive. A student can use a floppy disk and copy any file he/she needs to the hard drive and bypass the security that way. There is a nice little program that you can get from Microsoft called Floplock. “When the Floplock service is installed and set to start automatically, only users in the appropriate groups have access to the computer's floppy disk drives.” [9] Floplock comes with the Windows NT Resource Kit and the ZAK (Zero Administration Kit). Floplock works well with Windows 2000. I decided not to use Floplock because I still wanted my students to use the Administrator account, which is in the Administrators Group. Floplock will not work on an account if it’s in the Administrators Group.

Another vulnerability is adding these computers to a Domain. As stated in the beginning, I teach every aspect of setting up a Windows NT 4.0 domain in a tactical environment. I teach my students how to add these computers to the Windows NT domain once they create it. Once the student adds the computer to the domain, this opens up a whole new can of worms. Even though the computer now belongs to a domain, the users account used to login to the domain belongs to the Users Group on the computer. The user still has the restrictions applied. If the user is smart enough, he/she can copy the files needed to bypass Windows security directly from the domain controller of which the computer now belongs.

The last vulnerability that I’ll talk about is the password for the instructor account. The password for the Instructor account time bomb waiting to go off. Since every computer will have the same password for the instructor account, it’s only a matter of time when a student will stumble across the password. While creating this clone CD, I have put a lot of though into the password for the Instructor account. I have setup a local written policy that states that the password must be changed every 30 days on every computer a student has access to. I will

generate a password using the “pass phrase” structure incorporating uppercase characters, lowercase characters, special characters, and numbers. By now everyone should be used to setting a strong password and seeing this example. Take the word “password”. You can make a stronger password by changing “password” into “P@$$w0rd”. I wanted to make things a little harder to crack by using a brute force password cracker. Take the phrase “ Never Underestimate The Power Of Stupid People In Large Groups”. You can now form a password to resemble, “ Nueth3Pow3ro$pinLgroups”. The password may seem hard to follow, however, I used this password many years ago as a telnet password on a router. By creating this out of a phrase, you now have a hard to break brute force password. Don’t get me wrong, brute force will win every time, but it will take longer to crack. I have also edited the registry to use NTLMv2 only.
For more information, please read “The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus”, section W3.5.5 through W3.5.7 on the SANS Top 20 vulnerabilities website. [10]

I feel that I have created a very good platform to build upon. If I stumble over different ways to bypass Windows security, I will treat it like an upgrade or service pack. I will wait until I have several vulnerabilities before I go through the whole process of creating a new Clone CD. I do have an advantage though… I have documented every step needed in creating this Clone CD. Though these restrictions were drastic, to say the least, you may find it helpful to employ some of these restrictions throughout your workspace provided you are allowed to.
I was granted full reign on these computers to do whatever I wanted. Hopefully you now understand why this is called Extreme Hardening of Windows 2000 Professional.

References…

1. National Security Agency (NSA) “Defense in Depth - A practical strategy for achieving Information Assurance in today’s highly networked environments.” 2 September 2003 http://nsa2.www.conxion.com/support/guides/sd-1.pdf

2. Rana, Shrishail “Editing a Remote Computer's Registry” 3 October 2003 http://www.systweak.com/winreg/wr15.htm

3. Cole, Eric Fossen, Jason Northcut, Stephen Pomeranz, Hal, SANS Security Essentials with CISSP CBK Version 2.1, Volume Two United States of America, April 2003

4. Microsoft Corporation. Microsoft TechNet. “Windows 2000 Professional Baseline Security Checklist”. 28 May 2003

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/w2kprocl.asp

5. Microsoft Corporation. Microsoft Knowledge Base Article – 293655. “HOW TO: Apply Local Policies to all Users Except Administrators on Windows 2000 in a Workgroup Setting”. 28 June 2003
http://support.microsoft.com/default.aspx?scid=kb;en-us;293655

6. Waskowich, Terry. “WANT TO SET YOUR WINDOWS NT ADMINISTRATOR PASSWORD? - Second Edition” 6 July 2003.
http://www.compusmart.ab.ca/theclub/terrywas/winnt/winntpwd2.htm

7. Wayne’s Windows Administrator Support site for Windows NT / Windows 2000 / Windows XP / Penetration Testing / Firewalls. “User Tip #79: Set Explorer to open unknown files with Notepad” 30 September 2003
http://is-it-true.org/nt/utips/utips79.shtml

8. Beale, Jay. "Security Through Obscurity" Ain't What They Think It Is” 30 September 2003
http://www.bastille-linux.org/jay/obscurity-revisited.html

9. Microsoft Corporation. Microsoft Knowledge Base Article – 185704 30 September 2003
http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/q185/7/04.asp&NoWebContent=1&NoWebContent=1

10. SANS Institute. “The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus”. Version 4.0 October 8, 2003 Copyright (C) 2001-2003, SANS Institute. 3 October 2003
http://www.sans.org/top20/#w3

Appendix A

Local Computer Policy Settings

Windows Components	
-Internet Explorer	
search: Disable Find Files via F3 within the browser	Enable
disable changing advanced page settings	Enable
disable changing connection settings	Enable
do not allow auto complete to save passwords	Enable
disable the reset web settings feature	Enable
-Internet Control Panel	
disable security page	Enable
disable content page	Enable
disable connections page	Enable
disable programs page	Enable

disable advanced page	Enable
-Browser menus	
file menu: disable save as … menu option	Enable
view menu : disable source menu option	Enable
disable context menu	Enable
disable save this program to disk option	Enable
-Tool Bars	
disable customizing browser tool bars	Enable
Windows Explorer	
Removes the Folder Options menu from the Tools menu	Enable
MMC	
- Restricted/ permitted snap-ins	
active directory users and computers	Disable
active directory domains and trusts	Disable
active directory sights and services	Disable
computer management	Disable
local users and groups	Disable
security configuration and analysis	Disable
security templates	Disable
shared folders	Disable
-Group policy	
group policy snap in	Disable
group policy tab for active directory tools	Disable
administrative templates (computers)	Disable
administrative templates (users)	Disable
remote installation services	Disable
security settings	Disable
software installation (computers)	Disable
software installation (users)	Disable
- Task scheduler	
prevent task run or end	Enable
prohibit browse	Enable
-Start Menu & Taskbar	
disable and remove links to windows update	Enable
remove run menu from start menu	Enable
disable changes to taskbar and start menu settings	Enable
clear history of recently open documents on exit	Enable
Desktop	
-Active desktop	Enable
enable active desktop	Disable
prohibit changes	Enable
active desktop wallpaper	Disable
Control Panel	
-Add/remove programs	
hide add new programs page	Enable

hide add/remove windows components page	Enable
hide the “add a program from CD Rom or floppy disk” Option	Enable
Go directly to components wizard	Enable
Display	
hide background tab	Enable
disable changing wallpaper	Enable
hide appearance tab	Enable
hide screen saver tab	Enable
Network	
-Network and dial up connections	
prohibit renaming LAN connections or RAS	Enable
System	
disable registry editing tools	Enable
disable auto play	Enable