# Global Information Assurance Certification Paper

# Deploying Microsoft HiSecurity Template on a Windows 2000 Professional Workstation within a Windows NT 4.0 Domain



Joseph Matyaz

Securing Windows
GCNT Practical Assignment
Version 3.0 (revised August 13, 2001)
Option 2 – Securing Windows 2000 With Security Templates

# Introduction

The deployment of Windows 2000 has brought the availability of many new security features and enhancements to the hands of Network Administrators. Very few organizations can quickly and easily deploy the latest technology to all areas of their business. Political battles, IT Decentralization, cost (money), and other resource constraints can cause the adoption of new technology to be delayed. A mixture of Windows NT and Windows 2000 can be found in many organizations. A Windows 2000 Active Directory deployment requires significant planning and considerable coordination between all IT areas within an enterprise. This can be further complicated when different departments use competing software applications (for example: Microsoft Exchange and Lotus Notes, Microsoft SQL Server and Microsoft Access, IBM AIX and Sun Solaris) for essentially the same purpose. A single compromise could create considerable development and migration work for a department. Standardization via consensus agreements can be quite an undertaking.

In some cases the deployment of Windows 2000 to the Desktop has preceded the deployment of Windows 2000 to Servers. When this happens not all of the Windows 2000 security features and enhancements can be fully utilized. It is possible to secure a Windows 2000 Desktop while running a Windows NT Domain infrastructure.

I am securing a Windows 2000 Professional Workstation that is used by a mainframe application programmer (Cobol, CICS, DB2, JCL) for a health insurance company. The programming work is all done on a Mainframe using a 3270 Terminal emulator (Attachmate Extra). The programmers also use the Microsoft Office Suite for e-Mail, word processing, etc. The Windows 2000 workstation and the programmer's account are both members of the same Windows NT 4.0 Domain. Migration plans for changing to a Windows 2000 Active Directory Domain are in the works (conversion to take place in about 1 year) but the workstation needs to be secured prior to the establishment of the Windows 2000 Domain.

Workstation Hardware

The workstations are typical Intel boxes. Specifically, they are Dell OptiPlex GX 200s. They each have a single 933 Mhz Intel Pentium 4 Processor with 256 MB of RAM. Each has a 9 GB Hard drive (Western Digital WD100) formatted with a single 4 GB NTFS partition. The NIC (3Com EtherLink 10/100 3C905C-TX) and Video (NVIDIA TNT2 M128 4xAGP Ultra) controllers are both located on the motherboard. The CD-Rom (LITE-ON Corporation) is connected to a separate IDE controller from the disk drive. Each one also has a 3.5" NEC Floppy disk, a keyboard, and a Microsoft Wheel Mouse. A BIOS (Phoenix Technologies Ltd. A00) password has been set and must be entered when entering the BIOS Settings. The BIOS boot sequence is set to Hard Drive only. The remaining interrupts and I/O settings have been left at their default or AUTO setting.

Network Layout

Like the hardware, the network layout is also equally generic. Switched 100 BaseT Ethernet is run to every desktop via CAT5e cable. The wire closets are locked, only the Network

Administrators have keys. Fiber Optic cable connects the wire closets to a CISCO Catalyst 6500 Switch. All of the file servers are on a different network segment than the desktops. Each server has a 100 BaseT Ethernet connection to a port on the Catalyst 6500. Redundant routers and redundant links (point to point T1 lines) connect this facility with another building in the city and the corporate Data Center (in another city). The Data Center houses the Mainframe, the Midrange systems, and all external (Internet) access.

For the section of the company that I am responsible for; the majority of the computers (Servers, Workstations, and Laptops) are running Windows NT 4.0 Service Pack 6a. In addition there are few Windows 95 "Servers" as part of the Optika Imaging system and a few Windows 2000 Servers. All of the computers are part of a single Windows NT 4.0 Domain. A one-way trust exists between my Domain and a "Corporate" Windows NT 4.0 Resource Domain. A few managers map network drives to this domain for some file sharing of Human Resources and Accounting information. This division of the company has a separate dedicated LAN Support staff and is mostly autonomous.

Workstation Software

The workstation software includes a variety of applications that are used by the programming staff. Some are well-known office productivity packages and some are specific to our work environment. Each application is available to each programmer. Company IT Policy prohibits additional software from being installed by the programmers. The workstations are deployed using Norton's Ghost and Microsoft's Sysprep.

Workstation Software:

- Windows 2000 Professional (Service Pack 2)
- Adobe Acrobat Reader 5.0.1
- Attachmate Extra Personal Client 6.3
- Command Technology Corp SPF/SourceEdit Version 2.3
- IBM DB2 Client Connector for Windows NT 7.2
- IBM Online Manuals (IE Shortcut)
- LBMS Process Guide 7.0
- McSource 4.1
- Microsoft IE 5.50.4807 (Service Pack 2) (13-Dec-01 Critical Updates)
- Microsoft Office 2000 Suite 9.0
- Microsoft Office 2000 Suite SR-1
- Microsoft Project 98
- Microsoft SQL Server Client 6.50
- MicroTouch Systems IBID WhiteBoard Viewer 1.5
- Mobius Document Direct 2.2
- Norton AV Enterprise Corporate Edition 7.60.926
- Optika FilePower MultiView 4.5.0
- Quota Manager Inquiry Client 2.6.1a.70
- RightFAX 7.2
- Rocket Shuttle 6.1.1j
- Visio 2000 Professional SR1 6.0.2072

The individual programmers use the different applications to varying degrees. All use the Mainframe terminal emulator (Extra Personal Client) and Microsoft's Office Suite extensively.

Anti-Virus protection is provided by Norton Enterprise Anti-virus. An internal server automatically transfers new virus definitions to the programmer workstations. No third-party administrations tools are installed on the workstations for desktop management.

## Template Choice

No generic vendor supplied template or checklist can address all of the specific settings for an organization. They can serve as a guide or a starting point for additional customizations. Specialty applications, IT management policies, and organizational infrastructure can each contribute to the need for customizations.

Originally I had chosen to secure the workstation using the Microsoft supplied Secure Template (securews.inf). This is a well-known template from the manufacturer of the operating system, Microsoft Corporation. The published description for this template indicated that it had the appropriate network communication settings for my scenario. However, during the course of my evaluation I felt that the secure template did not provide as much benefit I was hoping to achieve. The settings aren't terribly strict and I felt there was considerable room for improvement.

The next "more secure" Microsoft supplied template is the HiSecurity Template (HiSecws.inf). This is actually the "most secure" of the Microsoft supplied security templates. I had originally chosen not to pursue this template because the network communication settings require the computer to be a member of a Windows 2000 Domain, which I do not have. What to do? I chose to adjust down the network communication settings just enough so that the requirement for Windows 2000 Domain Membership would not be necessary. It also seemed to make more sense to make a few adjustments to the HiSecurity Template (relaxed settings) than to add all of the registry and file system permission changes to the Secure Template. I will store the template I create along side the Microsoft supplied templates. Mine will be named ProgWS.inf.

Template Goals

Management has always placed Computer Security at the forefront of the IT Department's role. Protecting both the integrity and the privacy of company data are the cornerstones of this effort. All of the potential threats to company data are too numerous to mention. Each threat carries with it a certain amount of risk. These risks can be mitigated through good security practices. Windows 2000 Security templates are one tool that can be used to help secure the computer network.

Employee confidence is also at stake. Each programmer should feel certain that their computer is tool that they can depend upon in the performance of their job. It needs to be predictable and reliable. The programmers need a working PC so that they can fulfill their role of keeping the Mainframe applications running. No system is perfect so there will always be setbacks but the goal is to reduce their frequency and the degree to which they impact operations. Confidence in

the tool leads to greater productivity and less effort wasted on worrying if the tool is up to the latest challenge.

The Health Insurance Portability and Accountability Act (HIPAA) is Federal Legislation that governs the electronic transmission and storage of all healthcare information. The HIPAA law spells out minimum standards that must be met. It could be said that this is the Congress's way of trying to restore confidence in the privacy and confidentiality of the data contained within country's medical system. As the Information Age moves forward additional industries may come under more stringent controls. (Banking, Education, Communications, Transportation, etc.) This security template is also being used as a beginning step towards meeting the requirements set forth in the HIPAA legislation.

## Security Settings

Each section of the Modified HiSecurity Template (ProgWS.inf) is explained below. Where I have made alterations from the Microsoft HiSecurity Template those changes have been highlighted in RED.

Account Policy

The Account Policy section of the template sets up the rules that govern the accounts on the workstation. They apply to the local accounts on the workstation only. They do not apply to Domain Accounts that are used to log on to the workstation. Those settings would be applied to a Windows 2000 Domain Controller. Windows NT 4.0 Domain Controllers have some similar settings but they are outside the scope of this paper.

| Policy | HiSecws.inf | ProgWS.inf |
|---|---|---|
| Enforce password history | 24 passwords | 24 passwords |
| Maximum password age | 42 days | 30 days |
| Minimum password age | 2 days | 2 days |
| Minimum password length | 8 characters | 8 characters |
| Passwords must meet complexity requirements | Enabled | Enabled |
| Store passwords using reversible encryption | Disabled | Disabled |
| | | |
| Account lockout duration | 0 | 0 |
| Account lockout threshold | 5 invalid attempts | 3 invalid attempts |
| Reset account lockout counter after | 30 minutes | 60 minutes |
| | | |
| Enforce user logon restrictions | Not defined | Not defined |
| Maximum lifetime for service ticket | Not defined | Not defined |
| Maximum lifetime for user ticket | Not defined | Not defined |
| Maximum lifetime for user ticket renewal | Not defined | Not defined |
| Maximum tolerance for computer clock synch. | Not defined | Not defined |

Each account is required to have a password at least 8 characters long. The chosen password must be different from the last 24 passwords for the account (the maximum allowable value). The passwords will only be stored using non-reversible encryption, which prevents their disclosure even to Administrators.[1]

[1] MSDN: Windows 2000 Security Settings, Account Policies, Password Policy, Store passwords using reversible encryption for all users in the domain.

Each password must meet complexity requirements (contain no part of username, contains 3 of the 4 Microsoft character categories (uppercase letters, lowercase letters, numbers, allowable punctuation))[2]. This setting will significantly increase the strength of the passwords chosen by end users. It will probably require some end user education in order to be effectively understood (for example: explaining why "Hrd2Gu3ss" is much better than "January02").

While requiring passwords to be changed every 42 days is better than every 60 or 90 days I think this should be reduced even further, to 30 days. With the continuing increases of the computational power of today's computers the more frequently passwords are changed the less likely they are to be susceptible to brute force attacks or reverse cryptographic analysis.

Why set the minimum password age to 2 days? This setting is long enough to effectively prevent people from rapidly cycling through enough passwords to exceed the Password History setting to return to their "preferred" or "favorite" password. It is also not so long a timeframe that it restricts account owners from being able to change their password, on their own without intervention by an Administrator, if it is inadvertently compromised.

If more than 5 failed logons occur within 30 minutes (without any successful logons) the account will be "locked" until unlocked by an Administrator. Locking accounts prevents unlimited password guessing attempts by intruders. My organization's Policy requires that an account will be locked if more than 3 failed logons occur within 60 minutes. I agree with these slightly more strict settings. Giving a programmer 3 chances to successfully enter a password has been effective. In most cases 2 additional attempts would not help the programmer. Either they can remember their password and key it in carefully or they have forgotten their password, after returning from a vacation, for instance, and need to have it reset by an Administrator.

Since the workstation is not participating in a Windows 2000 Domain no Kerberos settings are required.

Audit Policy

The HiSecurity Template enables success and failure auditing for all events except Directory Service Access and Process tracking.

| Policy | HiSecws.inf | ProgWS.inf |
|---|---|---|
| Audit account logon events | Success, Failure | Success, Failure |
| Audit account management | Success, Failure | Success, Failure |
| Audit directory service access | Not defined | Not defined |
| Audit logon events | Success, Failure | Success, Failure |
| Audit object access | Success, Failure | Failure |
| Audit policy change | Success, Failure | Success, Failure |
| Audit privilege use | Success, Failure | Failure |
| Audit process tracking | No auditing | No auditing |
| Audit system events | Success, Failure | Success, Failure |

A Directory Service Access only occurs on an Active Directory Domain Controller so it does not need to be defined for Windows 2000 workstations. Process Tracking is generally more useful

[2] MSDN: Windows 2000 Security Settings, Account Policies, Password Policy, Passwords must meet complexity requirements of the installed password filter.

for troubleshooting and debugging than as a security-auditing feature. By setting this to Not Defined it can be enabled on individual workstations as needed without requiring a change to the Security Policy Template.

As a means to reduce the amount of events logged I suggest setting "Audit object access" and "Audit privilege use" to failure only. This may cause some useful information not to be collected but will significantly reduce the quantity of logged events that are recorded.

Security Options

The options available in this section of the HiSecurity Template define some overall security settings and address network communication. In order to enable the workstation to participate in a Windows NT 4.0 Domain some alterations are required. The analysis will be explained in sections to help clarify the alterations that I have made.

| Policy | HiSecws.inf | ProgWS.inf |
|---|---|---|
| Additional restrictions for anonymous connections | No access without explicit anonymous permissions | No access without explicit anonymous permissions |
| Allow server operators to schedule tasks (domain controllers only) | Not defined | Not defined |
| Allow system to be shut down without having to log on | Not defined | Enable |
| Allowed to eject removable NTFS media | Administrators | Administrators |
| Amount of idle time required before disconnecting session | 15 minutes | 15 minutes |
| Audit the access of global system objects | Disabled | Disabled |
| Audit use of Backup and Restore privilege | Disabled | Disabled |
| Automatically log off users when logon time expires | Not defined | Not defined |
| Automatically log off users when logon time expires (local) | Enabled | Enabled |
| Clear virtual memory pagefile when system shuts down | Enabled | Disabled |

The "Additional restrictions for anonymous connections" reduces the amount of information that can be access without first being authenticated. This should definitely be enabled to reduce the information that can potentially be gathered without authenticating.[3]

I suggest changing the shutdown option for computers that are available to non-Administrators. Enabling this setting permits a proper system shutdown without first having to log on to the computer. From the programmer's perspective this reduces the "hassle" of trying to turn off a computer system and therefore reduces the frequency with which workstations are powered off without being properly shutdown. In situations where only an Administrator is able to log on to a computer disabling this setting will prevent non-Administrators from being able to shutdown the computer since they won't be able to logon in order to get the shutdown option.

Enabling the logout of (local) users will enable a correlation between logon hours and when a computer can actually be used. If the goal of establishing logon hours is to force accounts to log out then this setting must be enabled. Without this setting any account that can log on at any point in time may remain logged on indefinitely.[4]

[3] MSDN: Windows 2000 Security Settings, Local Policies, Security Options, Additional restrictions for anonymous connections.
[4] MSDN: Windows 2000 Security Settings, Local Policies, Security Options, Automatically log off users when logon time expires (local).

Clearing the pagefile upon system shutdown can reduce the amount of sensitive information that may be available to the wrong account. I do not feel that the increase in shutdown time warrants this setting in my environment. Increased shutdown time would likely reduce the number of programmers that would shutdown their workstation every day. In my situation there is greater benefit derived from having the workstations restarted daily than the chance that anyone would exploit reading data from a non-cleared pagefile to gain access to sensitive information.

| Policy | HiSecws.inf | ProgWS.inf |
|---|---|---|
| Digitally sign client communication (always) | Enabled | Disabled |
| Digitally sign client communication (when possible) | Enabled | Enabled |
| Digitally sign server communication (always) | Enabled | Disabled |
| Digitally sign server communication (when possible) | Enabled | Enabled |

The lack of a Windows 2000 Active Directory requires that both of the signed communication (always) settings be disabled.[5] Since not all of the servers that the workstations will be communication with are running Windows 2000, forcing all communication to be signed is not feasible. Enabling it when possible is the next best option.[6]

| Policy | HiSecws.inf | ProgWS.inf |
|---|---|---|
| Disable CTRL+ALT+DEL requirement for logon | Disabled | Disabled |
| Do not display last user name in logon screen | Enabled | Disabled |
| LAN Manager Authentication Level | Send NTLMv2 only\ refuse LM & NTLM | Send NTLMv2 only\ refuse LM & NTLM |
| Message text for users attempting to log on | <BLANK> | <BLANK> |
| Message title for users attempting to log on | <BLANK> | <BLANK> |
| Number of previous logons to cache (in case domain controller is not available) | 10 logons | 0 logons |
| Prevent system maintenance of computer account password | Disabled | Disabled |
| Prevent users from installing printer drivers | Enabled | Disabled |
| Prompt user to change password before expiration | 14 days | 5 days |
| Recovery Console: Allow automatic administrative logon | Disabled | Disabled |
| Recovery Console: Allow floppy copy and access to all drives and all folders | Disabled | Enabled |
| Rename administrator account | Not defined | DesktopAdmin |
| Rename guest account | Not defined | DesktopGuest |
| Restrict CD-ROM access to locally logged-on user only | Disabled | Enabled |
| Restrict floppy access to locally logged-on user only | Disabled | Enabled |

Requiring the CTRL+ALT+DEL keystroke sequence for logon reduces the chance the account credentials will be compromised by a "fake" logon program.[7]

In my environment there is no attempt to keep Account Names private. The programming staff routinely uses their Account Name as an identifier for their work. Most of the programmers already know the Account Names of the other programmers by heart. Displaying the last logged on username actually increases security by enabling a programmer to recognize when someone else, whom they will probably recognize by username, has used their workstation. If they don't recognize the username they can contact an Administrator and request further investigation.

[5] MSDN: Windows 2000 Security Settings, Local Policies, Security Options, Digitally sign client communications (always) and Digitally sign server communications (always).
[6] MSDN: Windows 2000 Security Settings, Local Policies, Security Options, Digitally sign client communications (when possible) and Digitally sign Server communications (when possible).
[7] MSDN: Windows 2000 Security Settings, Local Policies, Security Options, Disable CTRL+ALT+DEL requirement for logon

Since all of the Servers that the programmer workstations need to communicate with are running either Windows 2000 or Windows NT 4.0 with Service Pack 6, NTLMv2 authentication should always be possible. Therefore, NTLM and LM authentication do not need to be supported.[8]

The absence or presence of a message that appears before logon does nothing to either enhance or reduce system security. I've read various claims that a message may grant some additional legal protection that may aide in criminal prosecution or civil court cases. By the time that a case is in court the cat is already out of the proverbial bag. My organization does use these disclaimers but I've removed them for this exercise.

I suggest setting cached logons to zero. If the workstation is unable to communicate with a Domain Controller for authentication then there are more significant problems that should be addressed. This also enhances security by requiring access to a Domain Controller in order to use a Domain Account. Stealing a programmer's computer and then attempting to log on using the programmers account name and password will not work. The computer must be able to communicate with a Domain Controller in order for the stolen computer and account to be used.

I suggest changing the expired password notification to 5 days. 14 straight days of notification can be an annoyance, which is magnified when the password lifetime is only 30 days, as suggested above. Without changing this setting almost half of the time a message will be displayed with the number of days left before the password will expire. This setting only applies to local accounts. The Windows NT 4.0 Domain Accounts will use the setting from the Windows NT Domain Controllers.

The Recovery Console should be set to require an administrative password for access. If not anyone can use it to compromise the computer. Additionally, I suggest enabling the full Recovery Console. Since it can only by used by a trusted administrator I see no reason to disable its functionality.[9]

The default Administrator and Guest accounts should be renamed. The new names can be specified via the Security Template. The chosen account names will certainly vary by organization. A company wide policy may even dictate what names should be used.

I also suggest altering the settings for remote access to the floppy drive and CD-ROM. I see no reason for permitting anyone but the local user to access the devices. For the programmers these devices are not shared so nobody should be accessing them.

| Policy | HiSecws.inf | ProgWS.inf |
|---|---|---|
| Secure channel: Digitally encrypt or sign secure channel data (always) | Enabled | Enabled |
| Secure channel: Digitally encrypt secure channel data (when possible) | Enabled | Enabled |
| Secure channel: Digitally sign secure channel data (when possible) | Enabled | Enabled |
| Secure channel: Require strong (Windows 2000 or later) session key | Enabled | Disabled |

[8] MSDN: Windows 2000 Security Settings, Local Policies, Security Options, LAN Manager Authentication Level.
[9] MSDN: Windows 2000 Security Settings, Local Policies, Security Options, Recovery Console: Allow floppy copy and access to all drives and folders.

Because of the lack of a Windows 2000 Domain for the Workstation to participate in, the requirement to use a strong session key must be disabled.[10] The software necessary to generate a strong session key is not present in Windows NT 4.0. All of the other Secure Channel settings can be enabled because all of the Servers that the Workstations will be communicating with are running either Windows 2000 or Windows NT 4.0 with Service Pack 6.[11]

| Policy | HiSecws.inf | ProgWS.inf |
|---|---|---|
| Secure system partition (for RISC platforms only) | Not defined | Not defined |
| Send unencrypted password to connect to third-party SMB servers | Disabled | Disabled |
| Shut down system immediately if unable to log security audits | Disabled | Enabled |
| Smart card removal behavior | Lock Workstation | Lock Workstation |
| Strengthen default permissions of global system objects (e.g. Symbolic Links) | Enabled | Enabled |
| Unsigned driver installation behavior | Do not allow Installation | Do not allow Installation |
| Unsigned non-driver installation behavior | silently succeed | silently succeed |

There are no RISC systems in place in my organization. There are also no third-party SMB servers in use in my organization. However, disabling the sending of unencrypted passwords via the security template is still a good idea. This will prevent the exposure of passwords in the event a rogue SMB server was installed and the workstations were connecting to it.[12]

I suggest changing the workstation to shutdown if it is unable to log security audit events. With the Event Log settings detailed above there is no reason that events should not able to be recorded.[13] If something has happened to prevent the recording of Security Audit Events the workstation should be shutdown.

Smart Cards are not in use in my organization. If they were available locking the workstation in the event one is removed would be the most appropriate setting.

I see no good reason not to strengthen the default permissions on global system objects. This essentially prevents non-Administrators from modifying system objects that they did not create.[14] Unsigned Drivers should not be allowed. All of the hardware drivers currently in use by my organization are signed. Reducing the opportunity for foreign code to be introduced via a device driver is something every Administrator should want to do. If only Administrators are installing device drivers this setting serves to help them check the authenticity of any driver that is installed.[15] Currently there is no method for signing non-drivers so any setting is acceptable.[16]

---

[10] MSDN: Windows 2000 Security Settings, Local Policies, Security Options, Secure channel: Require strong (Windows 2000 or later) session key.
[11] MSDN: Windows 2000 Security Settings, Local Policies, Security Options, Secure channel: Digitally encrypt or sign secure channel data (always) and Secure channel: Digitally encrypt secure channel data (when possible) and Secure channel: Digitally sign secure channel data (when possible).
[12] MSDN: Windows 2000 Security Settings, Local Policies, Security Options, Send unencrypted password to connect to third-party SMB servers.
[13] MSDN: Windows 2000 Security Settings, Local Policies, Security Options, Shut down system immediately if unable to log security audits.
[14] MSDN: Windows 2000 Security Settings, Local Policies, Security Options, Strengthen default permissions of global system objects (e.g. Symbolic links).
[15] MSDN: Windows 2000 Security Settings, Local Policies, Security Options, Unsigned driver installation behavior.
[16] Microsoft Windows 2000 Professional, C:\Winnt\Secuirty\Templates\hisecws.inf.

User Rights Assignments

The HiSecurity Template does not define any settings for User Rights. Instead it relies upon the default settings. I would suggest defining what those settings should be via the security template rather than relying upon the defaults not to be changed.

| Policy | ProgWS.inf |
|---|---|
| Access this computer from the network | Administrators, Backup Operators |
| Act as part of the operating system | |
| Add workstations to domain | Not Defined |
| Back up files and directories | Administrators, Backup Operators |
| Bypass traverse checking | Administrators, Backup Operators, Users |
| Change the system time | Administrators |
| Create a pagefile | Administrators |
| Create a token object | |
| Create permanent shared objects | |
| Debug programs | |
| Deny access to this computer from the network | Not defined |
| Deny logon as a batch job | Not defined |
| Deny logon as a service | Not defined |
| Deny logon locally | Not defined |
| Enable computer and user accounts to be trusted for delegation | Not defined |
| Force shutdown from a remote system | Administrators |
| Generate security audits | |
| Increase quotas | Administrators |
| Increase scheduling priority | Administrators |
| Load and unload device drivers | Administrators |
| Lock pages in memory | |
| Log on as a batch job | |
| Log on as a service | |
| Log on locally | Administrators, Backup Operators, Users |
| Manage auditing and security log | Administrators |
| Modify firmware environment values | Administrators |
| Profile single process | Administrators |
| Profile system performance | Administrators |
| Remove computer from docking station | Administrators, Backup Operators, Users |
| Replace a process level token | |
| Restore files and directories | Administrators, Backup Operators |
| Shut down the system | Administrators, Backup Operators, Users |
| Synchronize directory service data | Not defined |
| Take ownership of files or other objects | Administrators |

The above settings are essentially the default settings for a Windows 2000 Professional installation. Rather than relying upon the defaults I think that it is better to specify them. I've removed the Power User group from the above settings. The Power Users group will be defined to have no members, so the group doesn't need to be assigned any user rights. A number of the user rights have no setting. This actually forces that right to be removed from any group or user that might have it assigned. A Not Defined setting in the security template neither adds nor removes the use right; instead the workstation's default setting is used. This permits changes on a workstation by workstation basis without the need to modify the security template.

Event Log (GPO Only)

The HiSecurity Template sets a maximum size for the Security log of 10 MB and sets events to be overwritten as needed. Guest access to the System, Security, and Application logs is disabled (enable restrict access).

| Policy | HiSecws.inf | ProgWS.inf |
|---|---|---|
| Maximum application log size | Not defined | 5120 kilobytes |
| Maximum security log size | 10240 kilobytes | 10240 kilobytes |
| Maximum system log size | Not defined | 5120 kilobytes |
| Restrict guest access to application log | Enabled | Enabled |
| Restrict guest access to security log | Enabled | Enabled |
| Restrict guest access to system log | Enabled | Enabled |
| Retain application log | Not defined | Not defined |
| Retain security log | Not defined | Not defined |
| Retain system log | Not defined | Not defined |
| Retention method for application log | Not defined | As needed |
| Retention method for security log | As needed | As needed |
| Retention method for system log | Not defined | As needed |
| Shut down the computer when the security audit log is full | Not defined | Disabled |

From a security standpoint these settings are pretty good. They create a security log large enough to contain a large number of events and remove the ability of Guests to access the log files. Events recorded in the Security log will only be overwritten when the log file has reached its maximum size of 10Mb. I prefer the "Overwrite events as needed" setting because the "Do not overwrite events" setting causes more recent events to be discarded if the security event log becomes full. The "Overwrite events after X days" could also cause more recent events to be discarded too.

I would suggest only changing one of the event log settings as a security improvement. I suggest changing "Shut down the computer when the security audit log is full" to Disabled instead of Not defined. This setting can generate some controversy. First, it only reinforces the way Windows 2000 is configured out of the box, essentially re-enforcing the default. Disabling the automatic shutdown of the workstation reduces the ability to launch a Denial of Service Attack by simply filling up the Security Event Log. Microsoft recommends a different policy setting "Shut down system immediately if unable to log security audits" which is located in the Security Options section of the Local Security Policy if this feature is desired.[17]

While not strictly security settings, I also suggest defining a maximum log size of 5 MB (5120 Kb) for the System and Application logs. Both the System and Application logs should also be set to Overwrite events as needed. With today's larger Hard Drive sizes a 10 MB Security log and 5 MB System and Application logs there is typically plenty of space available for other files.

Restricted Groups (GPO Only)

The HiSecurity Template does not define any Restricted Groups. I would suggest defining some via the security template.

| Group | Members |
|---|---|
| Administrators | Local Administrator Account, Domain Administrators Group |
| Backup Operators | Local Administrator Account, Domain Backup Operators Group |
| Guests | Local Guest Account |
| Power Users | <Empty> |
| Replicator | <Empty> |
| Users | Local Administrator Account, Domain Users Group |

[17] MSDN: Windows 2000 Security Settings, Event Log, Settings for Event Logs, Shut down the computer when the security audit log is full.

The above built-in groups should each have their membership specified via the security template. Any custom organization groups can also have their membership spelled out, as in the custom Domain Backup Operators group above.

System Services (GPO Only)

The list of system services will depend upon which services are installed on the workstation. The HiSecurity Template does not define any settings for any system services. I would suggest defining some via the security template.

| Policy | ProgWS.inf | Security |
|---|---|---|
| Alerter | Not Defined | |
| Application Management | Not Defined | |
| ClipBook | Not Defined | |
| COM+ Event System | Not Defined | |
| Computer Browser | Automatic | Administrators - Full Control |
| DefWatch | Not Defined | |
| DHCP Client | Automatic | Administrators - Full Control |
| Distributed Link Tracking Client | Automatic | Administrators - Full Control |
| Distributed Transaction Coordinator | Not Defined | |
| DNS Client | Automatic | Administrators - Full Control |
| Event Log | Automatic | Administrators - Full Control |
| Fax Service | Not Defined | |
| Indexing Service | Disabled | Administrators - Full Control |
| Internet Connection Sharing | Disabled | Administrators - Full Control |
| IPSEC Policy Agent | Automatic | Administrators - Full Control |
| Logical Disk Manager | Automatic | Administrators - Full Control |
| Logical Disk Manager Administrative Service | Not Defined | |
| Messenger | Not Defined | |
| Net Logon | Automatic | Administrators - Full Control |
| NetMeeting Remote Desktop Sharing | Disabled | Administrators - Full Control |
| Network Connections | Not Defined | |
| Network DDE | Not Defined | |
| Network DDE DSDM | Not Defined | |
| Norton AntiVirus Client | Automatic | Administrators - Full Control |
| NT LM Security Support Provider | Not Defined | |
| Performance Logs and Alerts | Automatic | Administrators - Full Control |
| Plug and Play | Not Defined | |
| Print Spooler | Not Defined | |
| Protected Storage | Automatic | Administrators - Full Control |
| QoS RSVP | Not Defined | |
| Remote Access Auto Connection Manager | Disabled | Administrators - Full Control |
| Remote Access Connection Manager | Disabled | Administrators - Full Control |
| Remote Procedure Call (RPC) | Automatic | Administrators - Full Control |
| Remote Procedure Call (RPC) Locator | Not Defined | |
| Remote Registry Service | Automatic | Administrators - Full Control |
| Removable Storage | Automatic | Administrators - Full Control |
| Routing and Remote Access | Disabled | Administrators - Full Control |
| RunAs Service | Automatic | Administrators - Full Control |
| Security Accounts Manager | Automatic | Administrators - Full Control |
| Server | Automatic | Administrators - Full Control |
| Smart Card | Disabled | Administrators - Full Control |
| Smart Card Helper | Disabled | Administrators - Full Control |
| System Event Notification | Automatic | Administrators - Full Control |
| Task Scheduler | Automatic | Administrators - Full Control |
| TCP/IP NetBIOS Helper Service | Automatic | Administrators - Full Control |
| Telephony | Disabled | Administrators - Full Control |
| Telnet | Disabled | Administrators - Full Control |
| Uninterruptible Power Supply | Disabled | Administrators - Full Control |
| Utility Manager | Not Defined | |
| Windows Installer | Not Defined | |
| Windows Management Instrumentation | Automatic | Administrators - Full Control |
| Windows Management Instrumentation Driver Ext | Not Defined | |
| Windows Time | Not Defined | |
| Workstation | Automatic | Administrators - Full Control |

None of the disabled services are needed in my environment. Using the security template to force them to be disabled prevents them from being exploited for nefarious purposes. Likewise, I've used the security template to guarantee some of the services will be running and that they can only by managed by Administrators.

Registry (GPO Only)

The security template's registry settings are essentially concentrated on the HKLM\Software\Microsoft\WindowsNT\CurrentVersion keys and the HKLM\System\CurrentControlSet keys. Many of the settings grant Read and Execute rights to the Users and Power Users groups and Full Control Rights to the Administrators Group, SYSTEM, and CREATOR OWNER. Some of the permissions are changed to grant Everyone Read and Execute rights, with no one having Full Control. There are also a few registry keys that have been set up to prevent inheritable permissions from layers above propagating down. The security template does not enable Auditing on any registry keys or values.

File System (GPO Only)

The security template's file permission settings are primarily concentrated on the %systemdirectory% (typically \winnt\system32) and %systemroot% (typically \winnt). Many of the setting grant Read and Execute rights to the Users and Power Users groups and Full Control Rights to the Administrators Group, SYSTEM, and CREATOR OWNER. Some of the permissions are changed to grant Everyone Read and Execute rights, with no one having Full Control (ie: %systemroot%\explorer.exe). This setting will prevent any modifications to the explorer.exe file unless the permissions a first changed. This detailed permission setting is also the exception rather then the rule (explorer.exe was the only executable file singled out). There are also a few folders which have their settings changed to prevent inheritable permissions propagating down to them. A few key boot files (boot.ini, ntdetect.com, ntldr., etc.) have had their permissions changed to prevent their alteration by non-administrators.

The security template does not enable Auditing on any files of folders.

| Folder | Permissions |
|---|---|
| %SystemDrive%\Program Files\E!PC\Sessions | Administrators: Full Control, Users: Modify |
| %SystemDrive%\Program Files\McSource\bin\Temp | Administrators: Full Control, Users: Modify |
| %SystemDrive%\Program Files\McSource\HTML | Administrators: Full Control, Users: Modify |

The "Program Folders" folder is also set to Read and Execute for Users and Full Control for Administrators. This may cause issues with some programs. I've added adjustments for the applications in my environment that require them. The Program Files folder has long been a read-only area for users. Any permission changes that need to be made are documented in the installation instructions for each application. I've included those that are necessary in the ProgWS.inf security template.

## Applying the Template

Without the availability of a Windows 2000 Domain it is not possible to use the "traditional" Group Policy Objects (GPO) to apply and automatically refresh the security template.

As part of the workstation's initial configuration it is quite easy to apply the template through the use of the MMC Snap-In "Local Computer Policy" (Start MMC, Add Snap-In, Local Computer Policy, Windows Settings, Security Settings, Right Click, Import Policy). This does not provide much of an automated approach nor is it "refreshable" over time. As listed above, the "Local Computer Policy" MMC Snap-In also only updates the Account Policies and Local Policies. It ignores the Event Log, Restricted Groups, System Services, Registry, and File System sections of the security template (these section are listed as Only applicable through GPOs). According to Microsoft, "The Restricted Groups folder is available only in Group Policy objects associated with domains, OUs, and sites. The Restricted Groups folder does not appear in the Local Computer Policy object."[18] Similar text accompanies the other sections.[19] [20] [21]

By using the command line tool SECEDIT it is possible to convert the Security template into a Security database. Automating the deployment and potentially a periodic refresh can then be accomplished through the use of scripts. A full description of the command syntax for secedit can be found by entering the secedit command with no arguments. The full command I used to convert the security template into a Security Database is:

```
C:\Winnt\System32\SECEDIT.exe /configure /DB C:\Winnt\Security\Database\ProgWS.sdb /CFG
C:\Winnt\Security\Templates\ProgWS.inf /overwrite /log C:\Winnt\Security\Logs /verbose
```

(the above command has been wrapped for readability but is entered only on 1 line)

All of the files are in the "default" locations. Their paths have been spelled out for clarity. This command creates a security database named ProgWS.sdb that contains only the settings in the ProgWS.inf security template. A detailed log of each change is written in the logs folder. As the security database is created these settings are also applied to the workstation. These settings supercede the original, or default, security settings that were created as part of the installation of Windows 2000 professional.

This policy can be re-applied at any time with the command:

```
C:\Winnt\System32\SECEDIT.exe /configure /DB C:\Winnt\Security\Database\ProgWS.sdb /quiet
```

These two commands have a huge advantage over applying the policy using the "Local Computer Policy" MMC Snap-In. Secedit will apply all of the policies in the security template not just those visible in the "Local Computer Policy" MMC Snap-In. The downside to applying all of the settings is that the registry and file system permission changes take a while to complete.

To further automate this process a script file can be used to push the security policy template out to each workstation. I created script to copy the updated ProgWS.inf file to the programmer

[18] MSDN: Windows 2000 Security Settings, Restricted Groups.
[19] MSDN: Windows 2000 Security Settings, System Services.
[20] MSDN: Windows 2000 Security Settings, Registry.
[21] MSDN: Windows 2000 Security Settings, File System.

workstations.[22] [23] [24] [25] [26] [27] [28] [29] By default the ProgWS.inf file resides in the templates directory of the workstation the script is being run from and the workstation names are in column two of an Excel Inventory file. General comments on what is happening in the script are included at the end of each line. This script is highly specific to my environment but could be modified for other organizations.

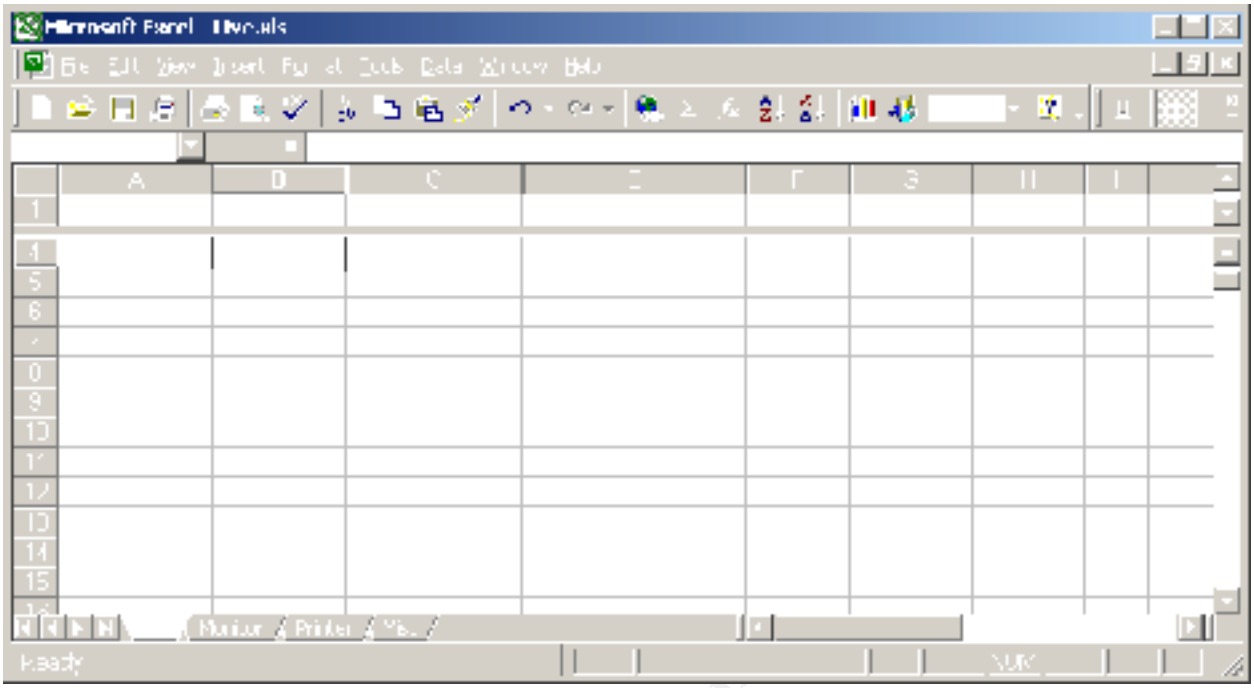
**Sample Deploy Policy Script**

```
'*********************************************************************************
' Script Name: Update_ProgWS_Excel.vbs
'     Version: 1.0
'      Author: Joe Matyaz
'Last Updated: 22-Jan-02
'     Purpose: Copy the updated security template to each workstation in the Inventory
'              spreadsheet
'       Usage: Script takes two arguments: Security Template   Spreadsheet location
'*********************************************************************************
On Error Resume Next

If WScript.Arguments.Count <> 2 Then
    sMaster = "C:\Winnt\Security\Tempaltes\ProgWS.inf"       'My customized Security Template
    sExeclList = "Y:\TechSupp\LanAdmin\Inventory\Live.xls"   'Inventory Spreadsheet
Else
    sIPaddress = WScript.Arguments.Item(0)
    sLogName = WScript.Arguments.Item(1)
End If
set oFileSystem = Wscript.createObject("Scripting.FileSystemObject")  'Get security template file
set oMaster = oFileSystem.GetFile(sMaster)
Set xlFile = Wscript.CreateObject("Excel.Application")       'Start Excel
call xlFile.Workbooks.Open(sExeclList,0)                     'Open Spreadsheet
xlFile.WorkSheets("CPU").Activate                            'Make CPU sheet the current one
RowCounter = 2                                               'Workstation names start in row 2
Set oNetwork = WScript.CreateObject("WScript.Network")
Do until xlFile.Range("B"& RowCounter) = ""                  'Repeat until no more workstations
   sWorkstation = xlFile.Range("B"& RowCounter)              'Get workstation name
   oNetwork.MapNetworkDrive "Z:", "\\"+ sWorkstation +"\C$"  'Map network drive
   If Err.number = 0  Then                                   'Check for a connection problem -
                                                             'Workstation could be turned off
      oMaster.Copy "Z:\Winnt\Security\Templates\ProgWS.inf",True  'Copy template to workstation
      oNetwork.RemoveNetworkDrive "Z:", True                 'Disconnect from workstation
   end if
      RowCounter = RowCounter + 1                            'Increment workstation
Loop
xlFile.Quit                                                  'Close Excel
```

The Excel Spreadsheet contains additional information about each computer. Only the workstation names in column "B" are used by the script.

[22] Boswell, Fossen, Page 135.
[23] MSDN: Windows Script Technologies, Script Runtime, FileSystemObject Object, FileSystemObject Basics, Programming the FileSystemObject.
[24] Shannon.
[25] MSDN: Working with Microsoft Excel Objects, Understanding the Range Object, The Range Property.
[26] MSDN: Windows Script Technologies, Windows Script Host, Reference, Methods, MapNetworkDrive Method.
[27] MSDN: Windows Script Technologies, Windows Script Host, Reference, Methods, RemoveNetworkDrive Method.
[28] MSDN: Welcome, Office Solutions Development, Microsoft Office, Microsoft Office XP, VBA Language Reference, Microsoft Excel Visual Basic Reference, Methods, A, Activate Method.
[29] Boswell, Fossen, Page 82-83.



This script is pretty simple. It incorporates no real error checking. There is also no mechanism to track which workstation were able to be updated and which ones failed. Once the security template has been copied to all of the workstations it is possible to configure the workstations to refresh themselves at system startup, via a startup script, without any Administrator or programmer involvement. This is the method that I would suggest using to implement the security template.

By adding a script that runs every time the computer starts the security template can be made self-refreshing. Two files are necessary on each workstation (their deployment can be scripted in the same way as the security template deployment).

**Apply Policy ProgWS.bat**

```
C:\Winnt\System32\SECEDIT.exe /configure /DB C:\Winnt\Security\Database\ProgWS.sdb /CFG
C:\Winnt\Security\Templates\ProgWS.inf /overwrite /log C:\Winnt\Security\Logs\scesrv.log <
C:\Winnt\Security\yes.txt
```

(the above command has been wrapped for readability but is only one line in the file)

**Yes.txt**

```
Y
```

The first file rebuilds the security database and applies the setting to the computer. The second file is necessary to supply a "Y" key press as a confirmation.

Getting the programmer workstation to automatically run the startup script can be accomplished in one of two ways, manually or via scripts.

A startup script can be manually added as the workstations are initially deployed using the "Local Computer Policy" MMC Snap-In (Computer Configuration, Windows Settings, Scripts (Startup/Shutdown), Startup). Add the name and the path to the startup script and any necessary

parameters for the script. The default location for the startup scripts is: C:\Winnt\System32\GroupPolicy\Machine\Scripts\Statup but they can be placed anywhere on the local machine. I store mine in the C:\Winnt\Security folder to prevent potential future conflicts with Group Policies applied from an Active Directory domain.

Shutdown and user logon and logoff scripts can be managed using similar methods.

Convincing a workstation to run a script every time it is started can also be scripted. To accomplish this I've added the "Apply Policy ProgWS.bat" and Yes.txt files to the C:\Winnt\Security directory on each programmer workstation (scripted in the same way as the security template deployment). I then manually configured one workstation to run this script (.BAT file) every time the computer starts. This created a scripts.ini file in the C:\Winnt\System32\GroupPolicy\Machine\Scripts folder. This file holds the key to getting the script to run.

**Scripts.ini**

```
[Startup]
0CmdLine=C:\WINNT\security\Apply Policy ProgWS.bat
0Parameters=
```

By deploying this same file to every programmer workstation (deployment can be scripted in the same way as the security template deployment) the Apply Policy ProgWS.bat will run every time the workstation is started. In my testing I found this to increase the workstation boot process by about 1 minute and 50 seconds. While the security database is being applied the message "Running startup scripts…" is displayed in the Windows 2000 Professional Startup Dialog Box.

When deploying these files via scripts care must be taken not to foul up other existing scripts that may already be in place. More sophisticated scripting could probably alleviate some of the issues. The preferred method would be to deploy Active Directory and let the full featured Group Policy Objects manage the distribution of security templates and their scripts.

Instead of only refreshing the policy at system startup the Apply Policy ProgWS.bat script could also be run at every logon, logoff, and shutdown. If sporadic refreshing were an issue, it could also be scheduled to run periodically using the Task manager (deploying this can also be scripted).

Scripts that at set to run at logon and logoff run in the context of the user instead of in the system context.[30] As most of the objects modified by the security template cannot be modified without Administrative authority there is little point to running the script within a user's context. If the script is set to run at startup, there is also little point to running it at the time of shutdown.

In my opinion the length of time it takes to apply the template is too long. The many permission changes on the registry and file system are the culprit. It is possible to speed up the startup of the computer by only processing part of the security database using the secedit /areas command. Different sections of the security database could be applied at different intervals using the Task manager, the secedit /areas command, and some additional scripts.

[30] Fossen, Page 134.

The command line tool SECEDIT is very powerful. Not only does the tool permit the application of security templates to be automated it can also be used to apply all of the sections within a security template, removing the restrictions imposed by the "Local Computer Policy" MMC Snap-In.

## Testing the Template

I suppose that logging on and being able to work productively in the midst of unending attacks would be the ultimate test. My testing will be some somewhat less dramatic.

Automatic Refresh Testing

I logged on to a programmer workstation using my Domain account (Administrative rights). I started the MMC console and added the "Local Security Policy" MMC Snap-In (MMC, Console, Add/Remove Snap in…, Add, Group Policy, Group Policy: Local Computer, Finish, Close, OK). I changed a single setting in Account Polices section. I set the Enforce password history setting to zero (Local Computer Policy, Computer Configuration, Windows Settings, Security Settings, Account Policies, Password Policy, Enter: Zero - Do not keep a password history). I then reloaded the security settings (Highlight Security settings, Action, Reload). I checked the settings and saw that the effective setting was now 0 passwords remembered.

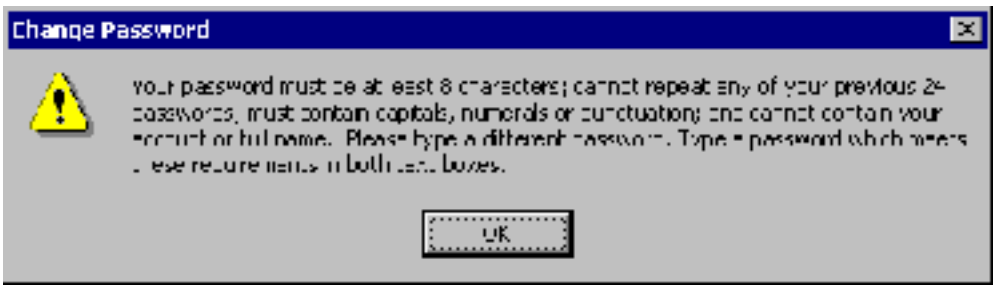
I then restarted the programmer workstation.

Again I logged on to the programmer workstation using my Domain account (Administrative rights). I started the MMC console and added the Local Security Policy snap-in (MMC, Console, Add/Remove Snap in…, Add, Group Policy, Group Policy: Local Computer, Finish, Close, OK). I again reloaded the security settings (Highlight Security settings, Action, Reload). I checked the settings and saw that the effective setting had returned to 24 passwords remembered.

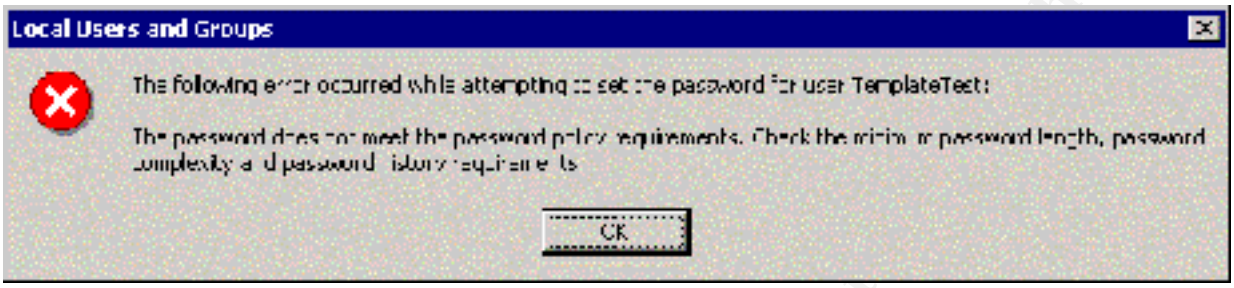
Password Complexity Settings

As an Administrator I created a local account named: TemplateTest.

I logged on as user TemplateTest. I attempted to change the password to "password". In response I received a very descriptive error message that explained most of the "complex" password requirements.

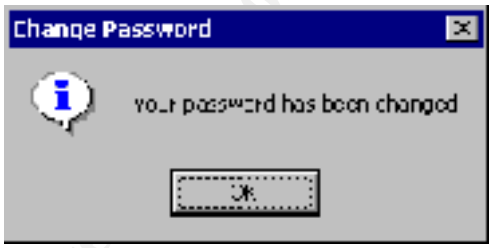


I logged off and then back on as an Administrator. I started used the Computer Management MMC Snap-In. I located the TemplateTest account and again attempted to change the password to "password" using my Administrative rights. . Upon clicking OK the following dialog box appeared.




It was good to see than even an Administrator is not able to bypass the account policies. All accounts on the workstation must comply with the account policy settings.

Finally, I logged off and then back on using a test Domain Account. Once again I attempted to change the password to "password". As anticipated the "Require complex password" account policy setting did not apply and I was able to successfully change the password.

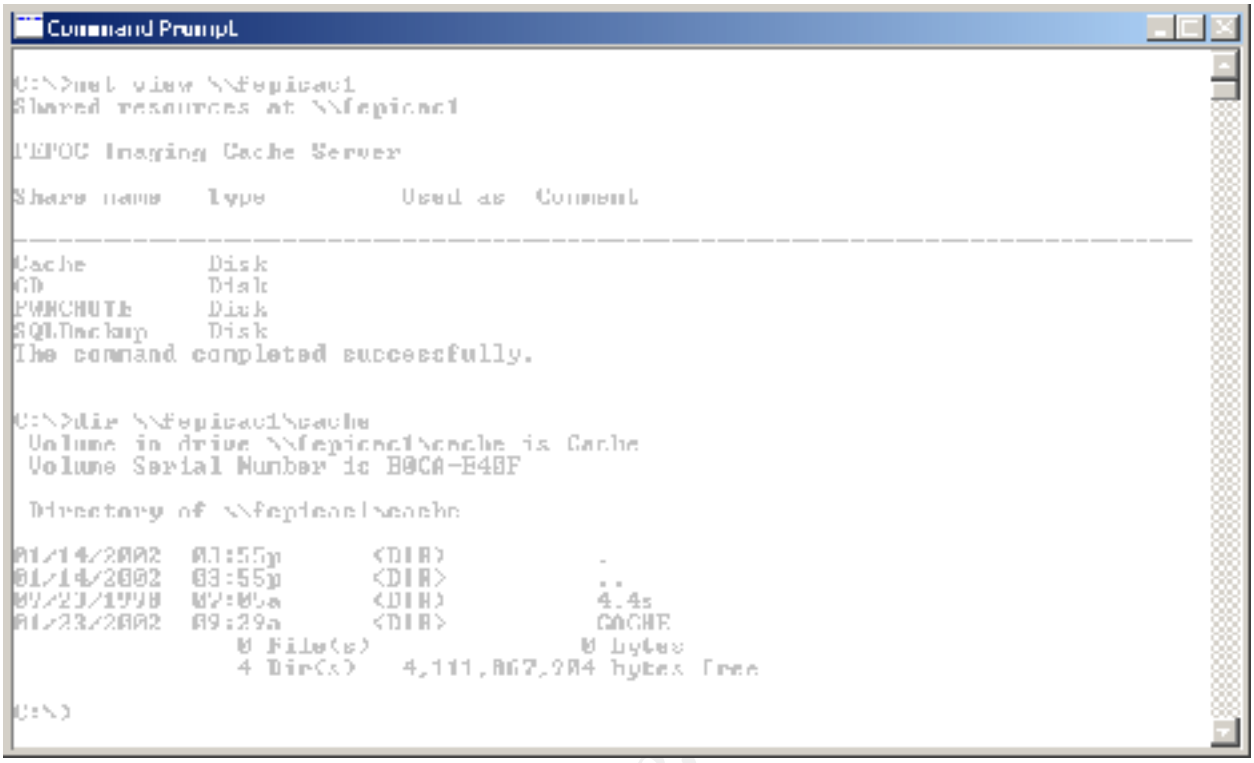



Communication with Windows 95

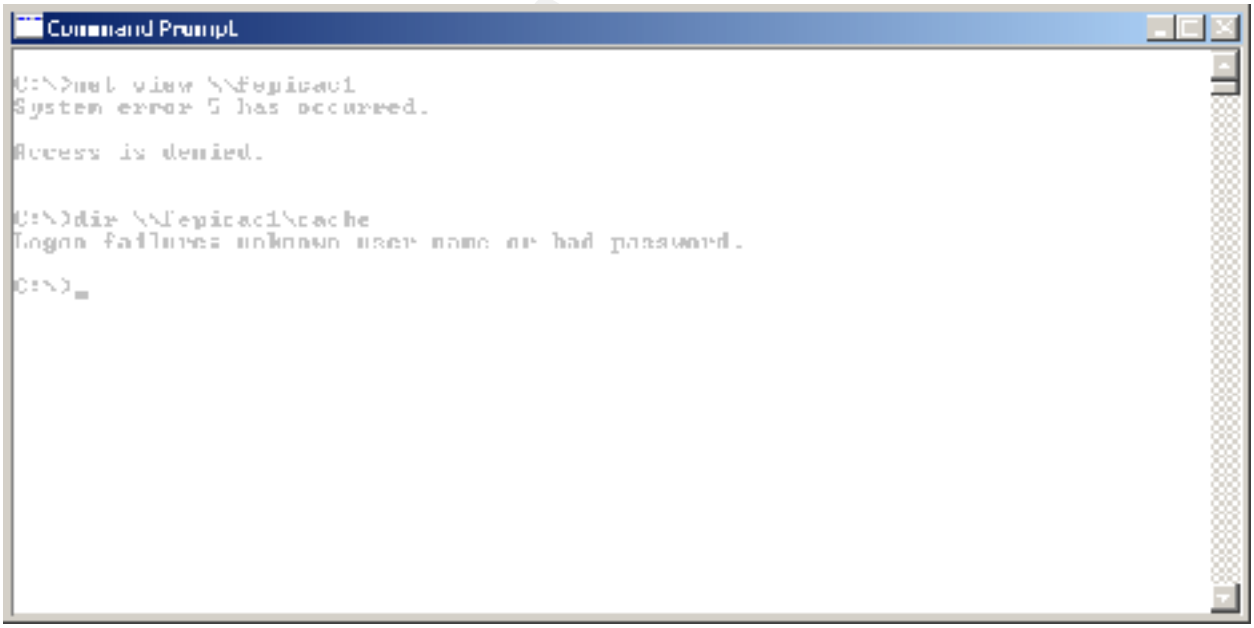
This is a reverse example of the previous ones. This example demonstrates how the application of the ProgWS.inf security template can prevent unwanted communication from taking place.

The application of the ProgWS.inf Security Template should not permit communication between a Windows 95 PC and the secured programmer workstation. The Optika Imaging System in my organization has a few Windows 95 computers that make up the 10-server system. Interaction with the Windows 95 computers is supposed to take place through the Optika Imaging software running in conjunction with a SQL Server database. I'll not go into all of the details but just say that direct interaction between the workstation and the Cache Server (running Windows 95) is not desirable. With the application of the security template that direct communication should no longer be possible.

I tried to view resources on the Windows 95 workstation and get a list of the available files.




On a programmer workstation after the application of the security template the command no longer returns a list of the available shares. An attempt to list the files on one of the existing shares is also met with failure.




Since the other Optika Imaging Servers are still running Windows NT 4.0 they don't have any problems communicating with the Windows 95 OCR Server.

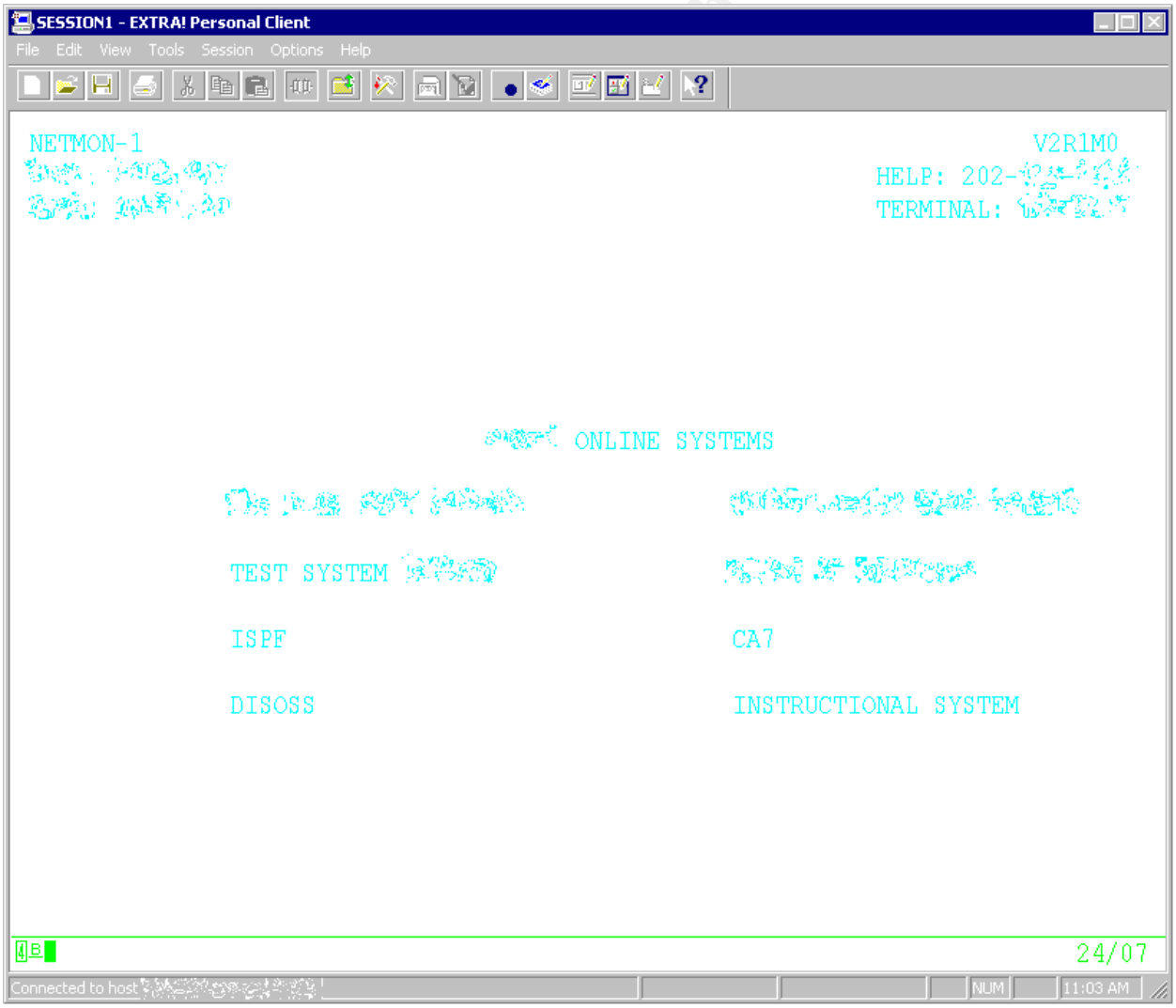
Connect to Workstation CD or Floppy

I logged on to a programmer workstation using my Domain account (Administrative rights). I attempted to map a network drive to a secured programmer workstation's CD-ROM Administrative share (D$). The command failed with a "The network name cannot be found" message. A little further investigation using the "Computer Management" MMS Snap-in revealed that the Administrative shares for the drives were no longer being created.

While these were simple tests of the security template in action, the proof was in the pudding.

Use Extra Personal Client

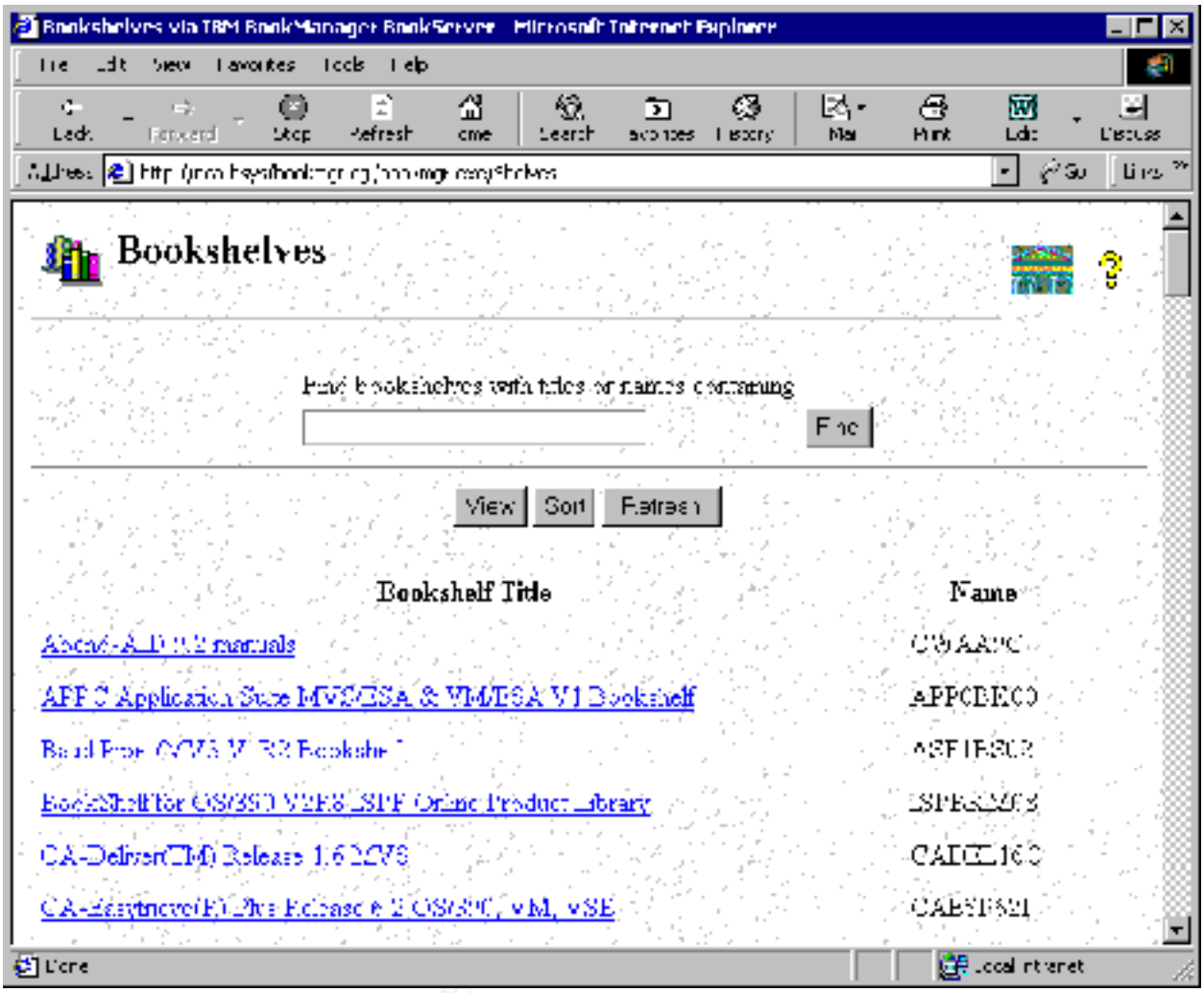
I logged on the programmer workstation using a test Domain account, TestUserJ, to simulate the access that a programmer would have. Starting the mainframe terminal emulation session did not produce any problems. Some of the file system settings needed to be adjusted because of the way the software updates its session files. The folders and files that needed permission adjustments were already well known within my organization.




Screen shot has been altered to obfuscate potentially sensitive information.

Browse IBM Online Manuals

The programmers use the IBM online Manuals as reference material for their daily work. The manuals are accessed via a Web Browser (http://nca-bsys/bookmgr-cgi/bookmgr.exe/Shevles). After supplying a valid username and password (not Windows NT Username and password) for internal server NCA-BSYS, access is granted to the list of available resources.




Microsoft Office Suite

I didn't really expect any problems with Microsoft's own personal productivity products. I tested the launching a usage of each of the Microsoft Office Suite applications using both my Domain account (Administrative rights) and a test programmer account (TestUserJ). Each of the applications started without any problems. I was able to manipulate several documents on mapped network drives using Word and Excel. I viewed a Power Point presentation and both sent and received messages using Outlook.

## Final Evaluation

The Microsoft supplied HiSecurity Template (HiSecws.inf) can certainly increase the security of a Windows 2000 Professional workstation. I was able to use that template as a guide and create my own ProgWS.inf Security Template that could incorporate almost all of the same security policies but still permit membership in a Windows NT 4.0 Domain. This modified template provides essentially the same benefits as the "most secure" template from Microsoft. With some scripting, and programmer patience, an Administrator can roll out any necessary alterations to

the security template to the workstations. If configured, the workstations could also periodically re-apply a set of pre-defined security settings on a scheduled basis.

A single security template is not the end; it is only a single step along the path to secure computing.

Computer viruses are not something that is terribly new. However, with the rise of the Internet many have spread much more rapidly. As viruses become more sophisticated users must sometimes be protected from themselves. “I Love You”, “Anna Kournikova”, “Melissa”, “SirCam”, and “Goner” were all spread directly though user interaction. Others, for example Nimda, Code Red, exploit inherent weaknesses in software and can spread themselves without any human interaction. Steps can be taken on each computer that reduce or eliminate the ability of viruses to spread and the damage that they can inflict. Due to the nature of business, valuable company data is available to many of the employees. Many need access to this data in order to complete their every day work. Each employee could potentially compromise the integrity of the data they have access to. It is up to Administrators to work to prevent this. While each Security Template setting may not appear to offer some protection against a known vulnerability good security practices also help prevent against future or unknown vulnerabilities.

Future investigations should include “Application Settings” (.ADM files). Application settings files (or Policy files) are essentially registry changes. Many of these registry changes have some security implications. The appropriate settings can increase the security of the system. Application settings are beyond the scope of this paper but they most certainly can affect the application of Group Policy Objects (GPOs).

More robust scripts would also be highly desirable. Error checking, a more sophisticated interface, and logging are all sorely needed. These types of features can be developed, tested, and added without the need to visit each workstation. My support responsibilities are limited to equipment located in a single building so any workstation visit is relatively uncomplicated. With ever expanding networks this is not something that I will be able to rely upon in the future. In the future Scripting may be to only way to go.

Integration with Active Directory will also be key for my company. Today Windows 2000 Professional and Windows NT 4.0 Server are the norm. The future will be quite different. Fortunately, Security Templates integrate quite well with Group Policy Objects. The greater sophistication that the multiple layers in which GPOs are applied and the automatic refresh capabilities will make Security Templates even more valuable. As new exploits are devised more rapid deployment of fixes will also be possible. In the future, less scripting may be required, but so will the Administrator involvement.

Compliance with the HIPAA Legislation is going to occupy a considerable amount time for all health providers in this country. The laws are settings all kinds of new minimum standards. Only time will tell if we are better off.

Attacks to the computer systems can come in a variety of forms. There is no “Silver Bullet” security tool that will save the day. The most secure computer systems will be built around

multiple lines of defense. The defenses will be continuously evolving. “Computer Security” is a never-ending battle. As new vulnerabilities are discovered new exploits will be produced.

Physical Access Controls, Anti-Virus Software, Intrusion Detection Systems, Firewalls, Egress Filtering, Activity Audit Logs, Education programs, oh yes, and Security Templates are all tools available to administrators. Each must be appropriately applied in order to have a secure computer network. Windows 2000 Security Templates are just one tool available to Administrators who are trying to keep would be intruders at bay.

# Appendix A

**ProgWS.inf**

```
[Unicode]
Unicode=yes
[System Access]
MinimumPasswordAge = 2
MaximumPasswordAge = 30
MinimumPasswordLength = 8
PasswordComplexity = 1
PasswordHistorySize = 24
LockoutBadCount = 3
ResetLockoutCount = 60
LockoutDuration = -1
RequireLogonToChangePassword = 0
NewAdministratorName = "DesktopAdmin"
NewGuestName = "DesktopGuest"
ClearTextPassword = 0
[System Log]
MaximumLogSize = 5120
AuditLogRetentionPeriod = 0
RestrictGuestAccess = 1
[Security Log]
MaximumLogSize = 10240
AuditLogRetentionPeriod = 0
RestrictGuestAccess = 1
[Application Log]
MaximumLogSize = 5120
AuditLogRetentionPeriod = 0
RestrictGuestAccess = 1
[Event Audit]
AuditSystemEvents = 3
AuditLogonEvents = 3
AuditObjectAccess = 2
AuditPrivilegeUse = 2
AuditPolicyChange = 3
AuditAccountManage = 3
AuditProcessTracking = 0
AuditAccountLogon = 3
CrashOnAuditFull = 0
[Registry Keys]
"USERS\.DEFAULT\SOFTWARE\Microsoft\Protected Storage System Provider",1,"D:AR"
"USERS\.DEFAULT\Software\Microsoft\NetDDE",2,"D:P(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"USERS\.DEFAULT",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles",1,"D:AR"
"MACHINE\SYSTEM\CurrentControlSet\Enum",1,"D:AR"
"MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip",2,"D:(A;CI;GR;;;WD)"
"MACHINE\SYSTEM\CurrentControlSet\Services\EventLog",2,"D:(A;CI;GR;;;WD)"
"MACHINE\SYSTEM\CurrentControlSet\Control\Print\Printers",2,"D:(A;CI;GR;;;WD)"
"MACHINE\SYSTEM\CurrentControlSet\Control\ProductOptions",2,"D:(A;CI;GR;;;WD)"
"MACHINE\SYSTEM\CurrentControlSet\Control\ContentIndex",2,"D:(A;CI;GR;;;WD)"
"MACHINE\SYSTEM\CurrentControlSet\Control\Computername",2,"D:(A;CI;GR;;;WD)"
"MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Security",2,"D:P(A;CI;GR;;;BA)(A;CI;GA;;;SY)(A;CI;G
A;;;CO)"
"MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg",2,"D:P(A;CI;GA;;;BA)(A;;GR;;;
BO)"
"MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layouts",2,"D:(A;CI;GR;;;WD)"
"MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layout",2,"D:(A;CI;GR;;;WD)"
"MACHINE\SYSTEM\ControlSet010",1,"D:AR"
"MACHINE\SYSTEM\ControlSet009",1,"D:AR"
"MACHINE\SYSTEM\ControlSet008",1,"D:AR"
"MACHINE\SYSTEM\ControlSet007",1,"D:AR"
"MACHINE\SYSTEM\ControlSet006",1,"D:AR"
"MACHINE\SYSTEM\ControlSet005",1,"D:AR"
"MACHINE\SYSTEM\ControlSet004",1,"D:AR"
"MACHINE\SYSTEM\ControlSet003",1,"D:AR"
"MACHINE\SYSTEM\ControlSet002",1,"D:AR"
"MACHINE\SYSTEM\ControlSet001",1,"D:AR"
"MACHINE\SYSTEM\Clone",1,"D:AR"
```

```
"MACHINE\System",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;G
A;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Windows",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA
;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time
Zones",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Svchost",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA
;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Setup\RecoveryConsole",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA
;;;SY)(A;CI;GA;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\SecEdit",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA
;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\ProfileList",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;C
I;GA;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\009",1,"D:AR"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Perflib",2,"D:P(A;CI;GR;;;IU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\IniFileMapping",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(
A;CI;GA;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\FontMapper",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI
;GA;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Font
Drivers",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\EFS",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;C
O)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Drivers32",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;
GA;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Classes",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA
;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AsrCommands",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;C
I;GA;;;CO)(A;CI;SDGWGR;;;BO)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AEDebug",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA
;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Accessibility",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A
;CI;GA;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion",2,"D:(A;CI;GR;;;WD)"
"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies",1,"D:AR"
"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer",1,"D:AR"
"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy",1,"D:AR"
"MACHINE\SOFTWARE\Microsoft\SystemCertificates",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(
A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Secure",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY
)(A;CI;GA;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Protected Storage System Provider",1,"D:AR"
"MACHINE\SOFTWARE\Microsoft\NetDDE",2,"D:P(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"MACHINE\Software\Classes",2,"D:(A;CI;GR;;;WD)"
"MACHINE\Software",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
[Version]
signature="$CHICAGO$"
Revision=1
[Service General Setting]
Browser,2,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
cisvc,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
Dhcp,2,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
```

```
dmserver,2,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
Dnscache,2,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
EventLog,2,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
Fax,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
LanmanServer,2,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
LanmanWorkstation,2,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
LmHosts,2,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
mnmsrvc,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
Netlogon,2,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
Norton AntiVirus Server,2,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
NtmsSvc,2,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
PolicyAgent,2,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
ProtectedStorage,2,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
RasAuto,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
RasMan,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
RemoteAccess,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
RemoteRegistry,2,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
RpcSs,2,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
SamSs,2,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
SCardDrv,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
SCardSvr,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
Schedule,2,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
seclogon,2,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
SENS,2,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
SharedAccess,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
SysmonLog,2,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
TapiSrv,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
TlntSvr,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
TrkWks,2,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
UPS,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
WinMgmt,2,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)"
[Privilege Rights]
SeNetworkLogonRight = *S-1-5-32-544,*S-1-5-32-551
SeBackupPrivilege = *S-1-5-32-544,*S-1-5-32-551
SeChangeNotifyPrivilege = *S-1-5-32-544,*S-1-5-32-551,*S-1-5-32-545
SeSystemtimePrivilege = *S-1-5-32-544
SeCreatePagefilePrivilege = *S-1-5-32-544
SeDebugPrivilege =
SeRemoteShutdownPrivilege = *S-1-5-32-544
SeIncreaseQuotaPrivilege = *S-1-5-32-544
SeIncreaseBasePriorityPrivilege = *S-1-5-32-544
SeLoadDriverPrivilege = *S-1-5-32-544
SeSecurityPrivilege = *S-1-5-32-544
SeSystemEnvironmentPrivilege = *S-1-5-32-544
SeProfileSingleProcessPrivilege = *S-1-5-32-544
SeSystemProfilePrivilege = *S-1-5-32-544
SeTakeOwnershipPrivilege = *S-1-5-32-544
SeShutdownPrivilege = *S-1-5-32-544,*S-1-5-32-551,*S-1-5-32-545
SeInteractiveLogonRight = *S-1-5-32-544,*S-1-5-32-551,*S-1-5-32-545
SeUndockPrivilege = *S-1-5-32-544,*S-1-5-32-551,*S-1-5-32-545
SeRestorePrivilege = *S-1-5-32-544,*S-1-5-32-551
SeCreateTokenPrivilege =
SeCreatePermanentPrivilege =
SeAuditPrivilege =
SeLockMemoryPrivilege =
SeBatchLogonRight =
SeServiceLogonRight =
SeAssignPrimaryTokenPrivilege =
SeTcbPrivilege =
[Profile Description]
Description=Programmer Workstation Security Template
[Group Membership]
*S-1-5-32-544__Memberof =
*S-1-5-32-544__Members = *S-1-5-21-492386247-1492126603-992442622-500,*S-1-5-21-2027572783-
380191574-1256410061-512
*S-1-5-32-551__Memberof =
*S-1-5-32-551__Members = *S-1-5-21-492386247-1492126603-992442622-500,*S-1-5-21-2027572783-
380191574-1256410061-1749
*S-1-5-32-546__Memberof =
*S-1-5-32-546__Members = *S-1-5-21-492386247-1492126603-992442622-501,*S-1-5-21-2027572783-
380191574-1256410061-514
```

```
*S-1-5-32-547__Memberof =
*S-1-5-32-547__Members =
*S-1-5-32-552__Memberof =
*S-1-5-32-552__Members =
*S-1-5-32-545__Memberof =
*S-1-5-32-545__Members = *S-1-5-21-2027572783-380191574-1256410061-513,*S-1-5-21-492386247-
1492126603-992442622-500
[File Security]
"c:\boot.ini",2,"D:PAR(A;;FA;;;BA)(A;;0x1200a9;;;PU)(A;;FA;;;SY)"
"c:\ntdetect.com",2,"D:P(A;;GXGR;;;PU)(A;;GA;;;BA)(A;;GA;;;SY)"
"c:\ntldr",2,"D:P(A;;GXGR;;;PU)(A;;GA;;;BA)(A;;GA;;;SY)"
"c:\ntbootdd.sys",2,"D:P(A;;GXGR;;;PU)(A;;GA;;;BA)(A;;GA;;;SY)"
"c:\autoexec.bat",2,"D:P(A;;GXGR;;;BU)(A;;GXGR;;;PU)(A;;GA;;;BA)(A;;GA;;;SY)"
"c:\config.sys",2,"D:P(A;;GXGR;;;BU)(A;;GXGR;;;PU)(A;;GA;;;BA)(A;;GA;;;SY)"
"%ProgramFiles%",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OIC
I;GA;;;CO)"
"%SystemRoot%",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;
GA;;;CO)(A;;GXGR;;;WD)"
"%SystemRoot%\explorer.exe",2,"D:(A;;GXGR;;;WD)"
"%SystemRoot%\CSC",1,"D:AR"
"%SystemRoot%\debug",1,"D:AR"
"%SystemRoot%\Offline Pages",1,"D:AR"
"%SystemRoot%\Profiles",1,"D:AR"
"%SystemRoot%\Registration",1,"D:AR"
"%SystemRoot%\repair",2,"D:P(A;CI;GXGR;;;BU)(A;CI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OI
CI;GA;;;CO)"
"%SystemRoot%\Tasks",1,"D:AR"
"%SystemRoot%\Temp",2,"D:P(A;CI;0x100026;;;BU)(A;CI;0x100026;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY
)(A;OICI;GA;;;CO)"
"%SystemRoot%\addins",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(
A;OICI;GA;;;CO)"
"%SystemRoot%\Connection
Wizard",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO
)"
"%SystemRoot%\Driver
Cache",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)
"
"%SystemRoot%\java",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;
OICI;GA;;;CO)"
"%SystemRoot%\msagent",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)
(A;OICI;GA;;;CO)"
"%SystemRoot%\security",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY
)(A;OICI;GA;;;CO)"
"%SystemRoot%\speech",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(
A;OICI;GA;;;CO)"
"%SystemRoot%\twain_32",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY
)(A;OICI;GA;;;CO)"
"%SystemRoot%\Web",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;O
ICI;GA;;;CO)"
"%SystemDirectory%",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;
OICI;GA;;;CO)(A;OICI;GXGR;;;WD)"
"%SystemDirectory%\appmgmt",1,"D:AR"
"%SystemDirectory%\DTCLog",1,"D:AR"
"%SystemDirectory%\GroupPolicy",1,"D:AR"
"%SystemDirectory%\NTMSData",1,"D:AR"
"%SystemDirectory%\Setup",1,"D:AR"
"%SystemDirectory%\ReinstallBackups",1,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A
;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemDirectory%\repl",1,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;S
Y)(A;OICI;GA;;;CO)"
"%SystemDirectory%\repl\import",1,"D:(A;OICI;SDGXGWGR;;;RE)"
"%SystemDirectory%\repl\export",1,"D:(A;OICI;SDGXGWGR;;;RE)"
"%SystemDirectory%\spool\printers",1,"D:P(A;CI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OIC
I;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemDirectory%\config",2,"D:P(A;CI;GXGR;;;BU)(A;CI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)
(A;OICI;GA;;;CO)"
"%SystemDirectory%\dhcp",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;S
Y)(A;OICI;GA;;;CO)"
"%SystemDirectory%\dllcache",2,"D:P(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemDirectory%\drivers",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;
;;SY)(A;OICI;GA;;;CO)"
```

```
"%SystemDirectory%\CatRoot",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;
;;SY)(A;OICI;GA;;;CO)"
"%SystemDirectory%\ias",2,"D:P(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemDirectory%\mui",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY
)(A;OICI;GA;;;CO)"
"%SystemDirectory%\ShellExt",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA
;;;SY)(A;OICI;GA;;;CO)"
"%SystemDirectory%\wbem",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;S
Y)(A;OICI;GA;;;CO)"
"%SystemDirectory%\wbem\mof",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA
;;;SY)(A;OICI;GA;;;CO)"
"%SystemDrive%\Program Files\E!PC\Sessions",2,"D:AR(A;OICI;FA;;;BA)(A;OICI;0x1301bf;;;BU)"
"%SystemDrive%\Program Files\McSource\bin\Temp",2,"D:AR(A;OICI;FA;;;BA)(A;OICI;0x1301bf;;;BU)"
"%SystemDrive%\Program Files\McSource\HTML",2,"D:AR(A;OICI;FA;;;BA)(A;OICI;0x1301bf;;;BU)"
[Registry Values]
MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print
Services\Servers\AddPrinterDrivers=4,0
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ShutdownWithoutLogon=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\AuditBaseObjects=4,0
MACHINE\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing=3,0
MACHINE\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel=4,5
MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous=4,2
MACHINE\System\CurrentControlSet\Control\Session Manager\Memory
Management\ClearPageFileAtShutdown=4,0
MACHINE\System\CurrentControlSet\Control\Session Manager\ProtectionMode=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignature=4,0
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableForcedLogOff=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\AutoDisconnect=4,15
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySignature=4,
1
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\RequireSecuritySignature=4
,0
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnablePlainTextPassword=4,
0
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\DisablePasswordChange=4,0
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SignSecureChannel=4,1
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SealSecureChannel=4,1
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSignOrSeal=4,1
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireStrongKey=4,0
MACHINE\Software\Microsoft\Driver Signing\Policy=3,2
MACHINE\Software\Microsoft\Non-Driver Signing\Policy=3,0
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableCAD=4,0
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLastUserName=4,0
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption=1,
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText=1,
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SecurityLevel=4,0
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SetCommand=4,1
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRoms=1,1
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateDASD=1,0
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateFloppies=1,1
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount=1,0
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\PasswordExpiryWarning=4,5
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ScRemoveOption=1,1
```

## References


Boswell, Bill, Fossen, Jason. 5.5 Windows 2000: Scripting and Security. SANS Institute, 2001.

Boswell, William. Inside Windows 2000 Server. New Riders Publishing, 2000.

Fossen, Jason. 5.1 Windows 2000: Active Directory and Group Policy. SANS Institute, 2001.

Microsoft Corporation. "MSDN: Welcome to the MSDN Library", URL: http://msdn.microsoft.com/library/default.asp (10-Jan-2002).

Microsoft Corporation. "MSDN: Microsoft Windows Script Technologies" URL: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/script56/html/vtoriMicrosoftWindowsScriptTechnologies.asp (20-Jan-2002).

Microsoft Corporation. "MSDN: Windows 2000 Security Settings" URL: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/gp/615.asp (10-Jan-2002).

Microsoft Corporation. "MSDN: Working with Microsoft Excel Objects" URL: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/modcore/html/deovrworkingwithmicrosoftexcelobjects.asp (20-Jan-2002).

Microsoft Corporation. "Windows 2000 Professional CD" (17-Dec-1999).

Shannon, Mathew. "Convert Excel Files to CSV… (Vbscript)" URL: http://cwashington.netreach.net/depo/view.asp?Index=229&ScriptType=vbscript (20-Jan-2002).

Last Updated: May 28th, 2018

# Upcoming Training


| | | | |
|---|---|---|---|
| **SANS Crystal City 2018** | **Arlington, VA** | **Jun 18, 2018 - Jun 23, 2018** | **Live Event** |
| **University of Pennsylvania - SEC505: Securing Windows and PowerShell Automation** | **Philadelphia, PA** | **Jun 25, 2018 - Jun 30, 2018** | **vLive** |
| **SANSFIRE 2018** | **Washington, DC** | **Jul 14, 2018 - Jul 21, 2018** | **Live Event** |
| **SANSFIRE 2018 - SEC505: Securing Windows and PowerShell Automation** | **Washington, DC** | **Jul 16, 2018 - Jul 21, 2018** | **vLive** |
| **SANS Boston Summer 2018** | **Boston, MA** | **Aug 06, 2018 - Aug 11, 2018** | **Live Event** |
| **SANS Amsterdam September 2018** | **Amsterdam, Netherlands** | **Sep 03, 2018 - Sep 08, 2018** | **Live Event** |
| **SANS Network Security 2018** | **Las Vegas, NV** | **Sep 23, 2018 - Sep 30, 2018** | **Live Event** |
| **SANS vLive - SEC505: Securing Windows and PowerShell Automation** | **SEC505 - 201810,** | **Oct 01, 2018 - Nov 07, 2018** | **vLive** |
| **Mentor Session - SEC505** | **Baltimore, MD** | **Oct 04, 2018 - Nov 15, 2018** | **Mentor** |
| **SANS San Diego Fall 2018** | **San Diego, CA** | **Nov 12, 2018 - Nov 17, 2018** | **Live Event** |
| **SANS OnDemand** | **Online** | **Anytime** | **Self Paced** |
| **SANS SelfStudy** | **Books & MP3s Only** | **Anytime** | **Self Paced** |