Global Information Assurance Certification Paper

Certified Windows Security Administrator (GCNW)

Practical Assignment Version 3.1 (revised April 8, 2002)

Option 2 - Securing Windows 2000 with Security Templates

John Jenkinson July 2002

Table of Contents

Introduction 3

Description of System 5

Choice of Template / Checklist 10

Security Settings 11

Password Policy 11

Account Lockout Policy 12

Kerberos Policy 13

Audit Policy 13

User Rights Assignment 14

Security Options 16

Settings for Event Logs 20

Restricted Groups 21

System Services 23

Registry 28

File System 29

Apply The Template 32

Test the Template 35

Test the System's Functionality 40

Evaluate the Template 44

References 46

Appendix A Installation History 47

Appendix B gunhighsecdc.inf 49

Introduction

This paper describes using security templates to secure a Windows 2000 system in a small business environment. A computer network connected to the Internet is becoming a business necessity for competitive edge and compliance with regulations - all of which are eased by small business computer networks. Thus a computer network is almost essential for a small business. However, a small business does not have the computer staff to maintain that computer network, it must rely on a few systems to do many tasks, and the cost challenges are omnipresent. A small business will typically buy services that it needs with the intent of bringing those functions in house as the business grows and the computer network supporting that business grows as well.

The system is for an imaginary gun shop in a far northern state. The gun shop is new so the computer network will be modest to start, but built to allow growth. The owners know the importance of a computer network to the success of a business - they used to run a fortune cookie business that went broke attempting to compete after GIAC Enterprises started using computer networks to enhance their business. While a fortune cookie business has computer networks playing a more major role in the success of the business due to the inventory being on the computer network, the ability to sale the product using the computer network, etc. - a small gun shop can use a computer network to advantage as well. Tracking inventory, accounts payable & receivable, and the legal requirements imposed on gun shops for permits and background checks.

The shop has only three employees, Mr. and Mrs. Owner and the gunsmith, Mr. Smith. The gun smith brings his own laptop and plugs into the network at the gun store so we will need domain group policies to secure that system/machine so he can browse the Internet, send mail, read gun newsgroups, order parts, etc. His laptop runs Windows 2000 Professional so the two-node domain can run in native mode. During busy seasons temporary employees may be added. We proposed to add a small system to allow customers to browse the Internet only, but this was rejected due to the cost and legal liability issues. A point of sale terminal is planned as the first extension to the gun shop's network. The Windows 2000 Server system we will configure the security template for will be a domain controller. Why a domain controller? The benefits to the gun shop are several. Group policies in Active Directory are the prime one. Then system settings can be enforced and reapplied for both the main system and the gunsmith's laptop. Ability to have organizational units is another. Plans for growth include a firing range, catalogue sales to the bush, and the gunsmith wants to partner in the business. Also, it is better to grow into a system then grow out of a system.

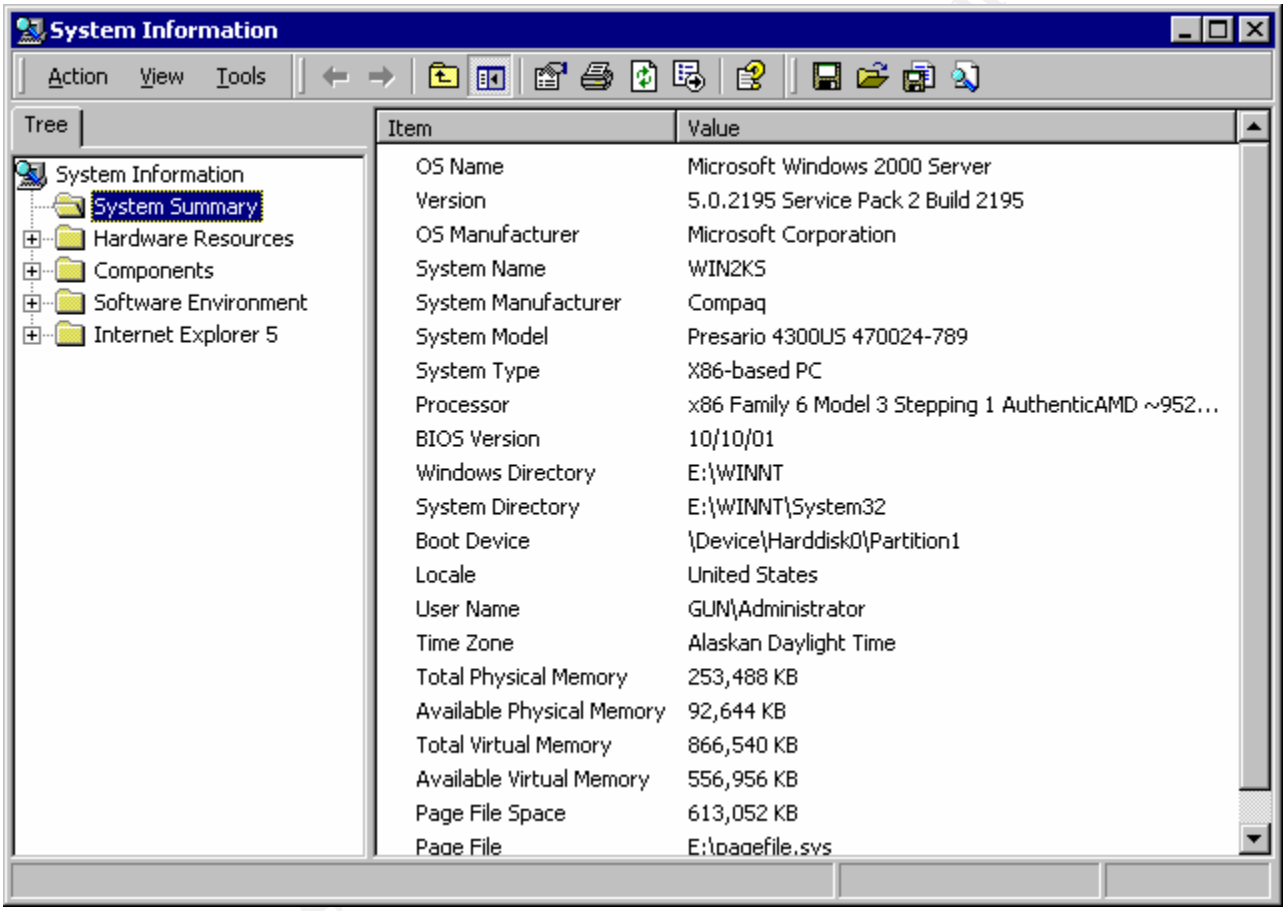
The security policy for the gun shop requires documentation of the security template and the security settings on the system in addition to the other security aspects so the lineage of the security template needs to be documented as well.

In summary, we have a system in a small business, a very small number of users, a system used for business purposes only, and good physical security. The checklist or template can thus be quite security stringent. In the manner of firewall deny all and allow by exception, we can pick the most strict security template and relax settings as necessary though the

template/checklist should be for a domain controller. By their nature domain controllers have features and many components added that need to be addressed by the template.

Description of System

The main system is a Compaq Presario 4300US with 256MB memory, 950MHz AMD CPU, 9GB hard drive, DVD/CD-R drive, 10/100Mbit Ethernet card, and floppy drive. This system was chosen due to the cost/performance ratio. A 950MHz CPU should keep up with the load but such a system can be purchased refurbished for less than $400. This allows more money to be spent on virus protection, a personal firewall, malware scanning package, etc.



The Internet connection will be via ADSL provided by the same telecommunications company that supplies the phone service. The ISP ADSL service chosen is on a PPPoE (Point to Point on Ethernet), which provides some security over the bridged connection type with a PPPoE username/password required for a connection. The ADSL modem will be connected to a Linksys EtherFast® Cable/DSL Router with a 4 port switch. This gives a router and switch combination with some firewall protection and allows up to 4 machines to connect to the Internet and the local network. The PPPoE username/password are configured on the LinkSys. The complex password to access the LinkSys for configuration is shared by the owners and the service provider. With the LinkSys the computers are given private Class C (192.168.0.0/16) IP addresses via DHCP with the LinkSys providing the Network Address Translation (NAT) service. We will use Cat5 wires, not wireless. A gun

shop's appliances like display cases do not move around a lot. The main machine and the LinkSys are in the gun shop's locked office.

No dialup is needed, so no modems are installed. No remote access is needed so telnet service, ftp, and remote control packages like PCAnywhere are not used nor configured.

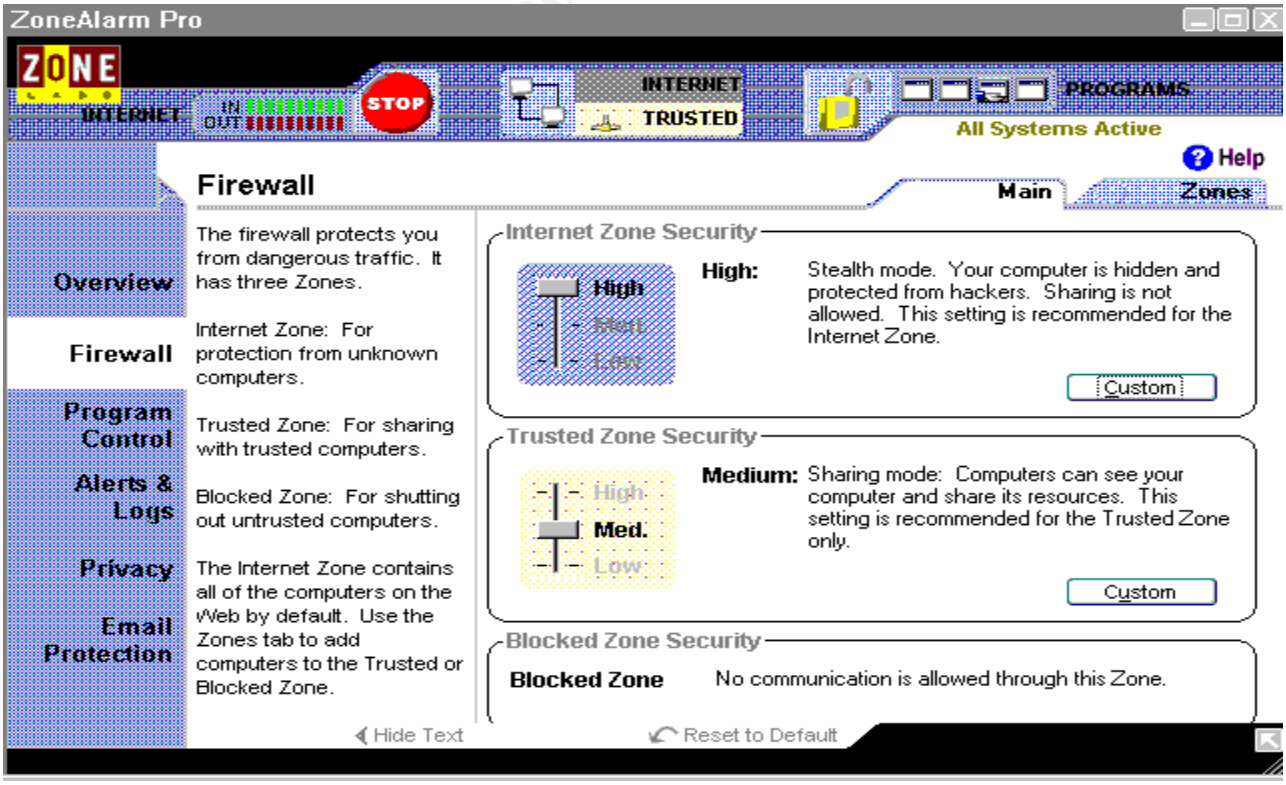
All the machines will run Zone Labs ZoneAlarm® PRO version 3.0.118, Norton AntiVirus version 7.60.926 and PestPatrol Version 3.0.

As mentioned the LinkSys provides a connection to the ADSL modem, functions as a 10/100Mb Ethernet switch, is a router from the Ethernet switch to the ADSL modem to the Internet, and has some firewall functions. It also holds the login configuration to the PPPoE server at the ISP to authenticate, negotiate, track status, and provide some logging of the connections.

ZoneAlarm PRO is the commercial version of the Zone Labs personal firewalls. They also offer an intermediate product, ZoneAlarm Plus, but we selected the Pro version. This is a personal firewall as well, but one of the few that notifies on attempts to connect out to the Internet.

PestPatrol might not find problems on a clean install, as we find and would hope, but should prove its worth as the system gains applications, downloaded files, and access time on the Internet.

The ZoneAlarm settings for the firewall portion

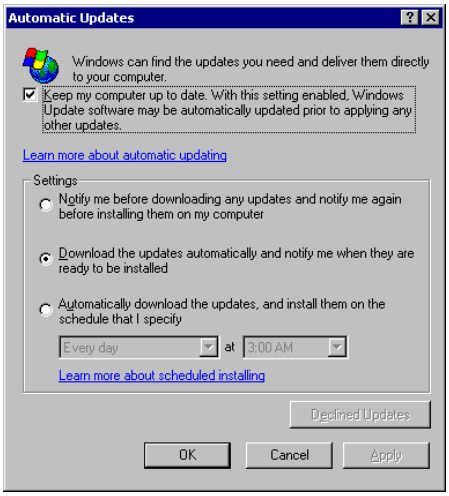


which gives high security for the Internet zone - this is what we want and need

The Norton AntiVirus is set up via Live Update to check for updates once a week and apply those updates automatically. It is set up to scan all drives and Exchange though the system does not use Exchange for email. It does not cost to scan and might prevent problems if Exchange or Outlook or similar are used.

PestPatrol scans are done at the service provider visits once a week.

Microsoft updates are set to download the updates and notify when ready to be installed. This is one of the three possible settings and is best suited for our circumstances. We choose to not have the updates installed automatically, we want the chance to review the changes AND control when these are applied. If a patch is available and critical we want that patch loaded and ready to apply.



The ISP will host the store's web site, but the system will run Microsoft Internet Information Services (IIS) web server to test the store's web pages before supplying them to the ISP for publishing. This service will be started as needed and stopped once the testing is completed. If possible the web pages will be viewed by Internet Explorer, Microsoft Word, or similar instead. Since the service has a possibility to be run, though that option is discouraged by the service provider and the stories in the media, the Microsoft supplied IIS hardening tool is to be run.

We will run Internet Explorer Version 5.5 with Service Pack 2 (SP2). Some of the shop's access to sites will not work with IE V6.0.

The applications to do inventory tracking, purchasing, accounts payable, etc. will be purchased (buy not build) and the data files will be split across New Technology File System (NTFS) for most data files and Encrypting File System (EFS) for private data. The gunsmith does most of the computer maintenance tasks and data that need protection from him and the firm(s) doing other computer system and network tasks will be on the EFS folder(s). The store's lawyer will maintain a backup of the EFS certificate.

Backup and disaster recovery will be done by a combination of copying all of the system drive to attached SCSI disk(s) and by a scheduled backup job of selected data files to output a file on the C: drive which is copied to a CD-R drive and taken to the bank with the days deposits on even days and to the owner's home safe on odd days. The disk copies are made at the end of the month after monthly closing and also taken to the bank safety deposit box on even numbered months and to the owner's home safe on odd numbered months. The disk-to-disk copies are done with an UNIX-like dd utility. This is accomplished by having a like disk to the system disk in manufacturer, geometry, and capacity – just SCSI instead. This allows the disk to be copied without regard to open files, partitioning, EFS, and less likelihood the dd can be root kited. CD-R media is less that 50 cents in bulk and the SCSI disks are inexpensive so the three needed for the disk-to-disk copy rotation were purchased to ensure some protection of the data, applications, and ease of recovery of the system.

The system shipped from Compaq with Windows XP Home installed on the C: drive. While XP has GPOs and security templates, it does not have the ability to run as a domain controller. The features of XP, being touted as more reliable, having payed for the XP license, and just for fun the owners wanted to retain the ability to run XP via dual boot. To secure the WIndows 2000 Server system, the ability to be booted to XP needs to be addressed. Since XP does configure with security templates and GPOs as well, the resulting template will be pared down to run on the XP system. The sensitive data will be in an EFS folder so that exposure is mitigated somewhat. XP Home does not support EFS, but XP Professional does. Some postings on the Internet indicate XP Home can be made XP Professional by registry modifications. We will require login to shutdown settings in both templates, the service provider reviews logs weekly so any shutdown and prolonged outages that might have occurred while the system was booted to XP can be found and reported. My experience with XP shows it to be more tolerant of errors in templates so the effort of removing domain controller settings should be less.

The system will be secured to the building with cables and key locks to prevent theft of the systems, though being in a well-secured gun shop lessens this possibility somewhat. The systems will be positioned such that both front and back of the system are visible to help detect installation of a keyboard sniffer device and to monitor the PCI slots for any unauthorized hardware additions. The system is placed on the desk for easy access to the CD-ROM drive for the daily backup and to lessen the chance of water damage if the shop's floor is flooded. It is shielded from the overhead sprinkler head by a shelf. The system has its serial number on file with the gun shop's lawyer.

A service provider will maintain the system. Weekly visits to check security, application, and event logs and other system functions like patches. ZoneAlarm logs, and hot fixes will be augmented by on call services. The administrator password will be shared between the service provider and the owners. While this lacks strict accountability that would be provided if each of the owners and the service provider each had a user account and a separate administrator account (that belonging to the Administrators group), having only two groups of people (the owners and the service provider) lessens the accountability problem some and sharing the built-in administrator account lessens the issues with keeping the added administrator accounts with the correct permissions, security settings, and ability to run the

recovery console. Another deciding factor in sharing the account was the three times the possibilities of cracking an administrator password if there were three administrator accounts.

The system will have the administrator user, a *mrowner* and *mrsowner* user for the owners, *gunsmith* for the gunsmith, and a *test* user such that the applications can be tested after installation by the administrator without needing the other users to test or have the administrator use one of their accounts. A check is made that the Guest account is still disabled and has a strong password. We do both in case the account is enabled in future. We could also apply restrictions on the account like login time restrictions, but choose not to at this time. Reason being risk management, the risk does not require the additional action.

The system is built with Microsoft Windows 2000 Server installed on a newly formatted NTFS partition. The disk was partitioned with two equal sized NTFS partitions. Service Pack 2 was then installed, the latest Microsoft Windows 2000 Security Rollup Package, recommended updates, and selected hot fixes applied. Then the system was connected to the Linksys and the Linksys network configured. Items done include changing the Administrator password on the Linksys, setting the ISP configurations for PPPoE, etc. For purposes of this paper the DNS name of gun.org (pronounced in the manner of gnu) is used. Then Norton VirusScan, ZoneAlarm, PestPatrol and the applications were loaded. After this was done the system, the Linksys, and cabling was taken to the gun shop. The connection to the Internet was tested, and then the system removed from the ISP Internet connection. Then the machine was promoted to a domain controller, the Microsoft Management Console (MMC) built, and a backup taken. At this point several tools were used to verify the function of the domain controller. These included running dcdiag and netdiag with the verbose switch and then stopping and restarting the Net Login service, then checking the logs for problems as suggested in the Microsoft Technet article.[2] Now that we have the machine as a domain controller, the Active Directory built and populated, the MMC and its associated snap-ins installed, we are ready to the security template work.

Thus we have a two node network at the LinkSys switch that connects to the Internet at the LinkSys router and ISP supplied ADSL modem. All the shop's employees use the system we will configure the template for as an application server, a file server and a general purpose system The system has additional duties as a domain controller, network monitor, administration machine for the network, and all the other functions to provide a computer network to support the shop's employees, to control and manage the shop, and to enhance the services provided to the shop's customers. To better understand the scope of the problem, look at the computer network infrastructure of a few of the GIAC practicals intended to service a fortune cookie company.

Choice of Template / Checklist

The choices for security templates are many. SANS, CIS, Microsoft, and NSA all have good templates to get started from. CIS only has level 1 and level 2 templates that provide minimal and prudent beyond minimal settings. We will use the high security domain controller template provided with the system in \%systemroot%\security\templates\hisecdc.inf. The NSA templates will be used to add items to a copy of this template then the system requirements will dictate more additions to the template before applying. Not only is the name and source of the security template, high security domain controller security template from Microsoft, a good starting point in practice – it does have a lot of benefit in name recognition to the customer. We have a high security domain controller template to apply to a high security domain controller. The NSA template for additions is W2KDC.INF

It is interesting to note the template from Microsoft for the domain controller is 162 lines while the template for the workstation is 318 lines. NSA's domain controller template is 240 lines while their workstation template is 235 lines. Both Microsoft and NSA have name recognition for the client and while the number of lines in the NSA templates indicate those are more comprehensive, the NSA templates are not as ordered as the Microsoft templates. An illustrating example is the [Profile Description] comment and string after registry keys and values. Security templates have sections delimited by the section name in square brackets. When building templates with text editing as we attempted to do at first, getting the entries in the correct section was one source of problems. To better maintain and document the templates we will use, the template will be in order given by the Security Configuration and Analysis report in MMC. The templates were edited taking care to organize and select the best settings from both templates into one to use. This is NOT the way to build a template in our experience. It is better to take one good starting point, bring that into the "Security Configuration and Analysis" GUI. Since templates are brought into a database and are incremental to the base template used as system install, apply templates in incremental fashion, and then review each setting. Once that is done the template can be exported and then documented. When reviewing the exported template it is noted the order from the imported template is not preserved, which explains the apparent lack of order in the NSA templates. Also the comments are stripped in the process of importing the template into the security database files (*.sdb) then exporting the template. A workaround could be to "cut and paste" the comments into the exported template to better document the template, but this has a disadvantage in that the template is modified from the export and actual settings could be modified in that process as well, thus loosing the assurance this is the unmodified export from the security database. It would be a nice feature improvement to preserve the order of the template and the comments. Be aware that incrementally adding templates to the template database and exporting a new template from that database will not include settings to the system from the "Security Configuration and Analysis" GUI. The non-template settings will be in the exported template after "Configure Computer Now...". Also be sure to review the log file produced to resolve any mismatches and be aware of the Not Configured items.

In summary, the CIS and similar baseline templates are intended to get a system to a baseline security level so we can all be more secure. The system matches the high security

domain controller template of which we have two major choices – Microsoft and NSA. We first merged the two via text edits but then used the incremental properties of these two to incrementally apply both to the system baseline template, apply other settings needed by the configuration, then exported to obtain our resulting template.

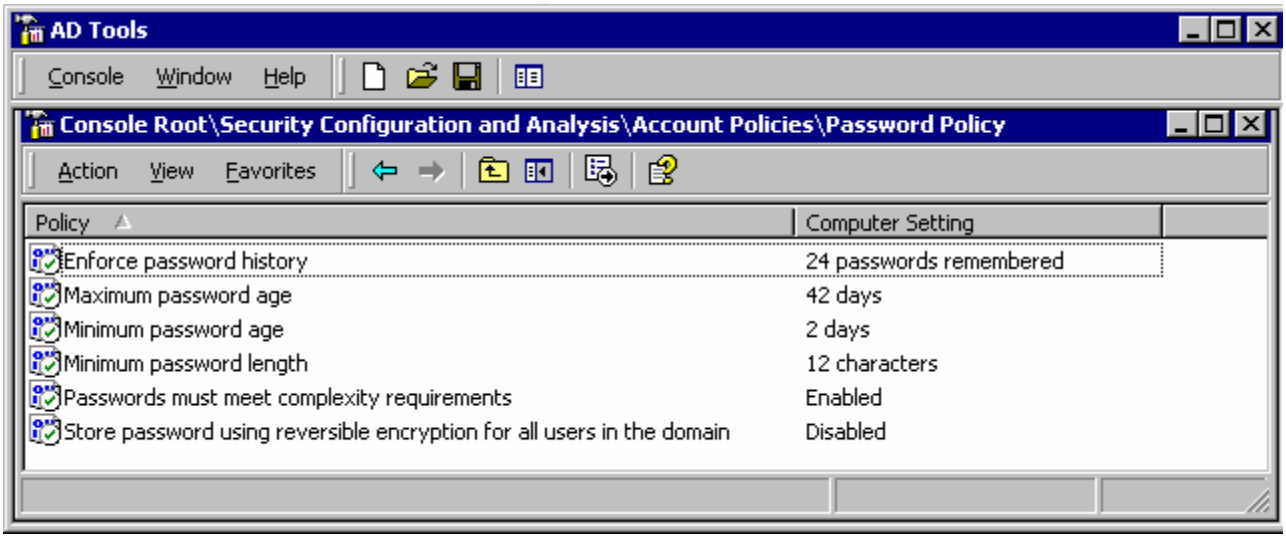
The template after the merge, edit, and export, is in Appendix B.

Security Settings

The security settings, those controlled by security templates, should conform to the security policy, enhance security, not hamper business function, and fit within the limits of the hardware. When conflicts occur in business requirements and security/service recommendations the service provider will give advice with pros and cons and encourage the owners to seek second opinions via web searches and newsgroup postings.

Password policies are subjective in scope and settings. Strong settings can cause users to employ non-secure methods to comply with enforced policy while keeping some semblance to their desired methods. Writing down the password, incrementing a number for password history, etc. The owners are aware of strong passwords helping strengthen security and have agreed to the password and account policy settings in the security templates. These enforce their practice in choosing and maintaining passwords, but also provide enforcement for the gunsmith and any temporary help that might be used.

Password Policy



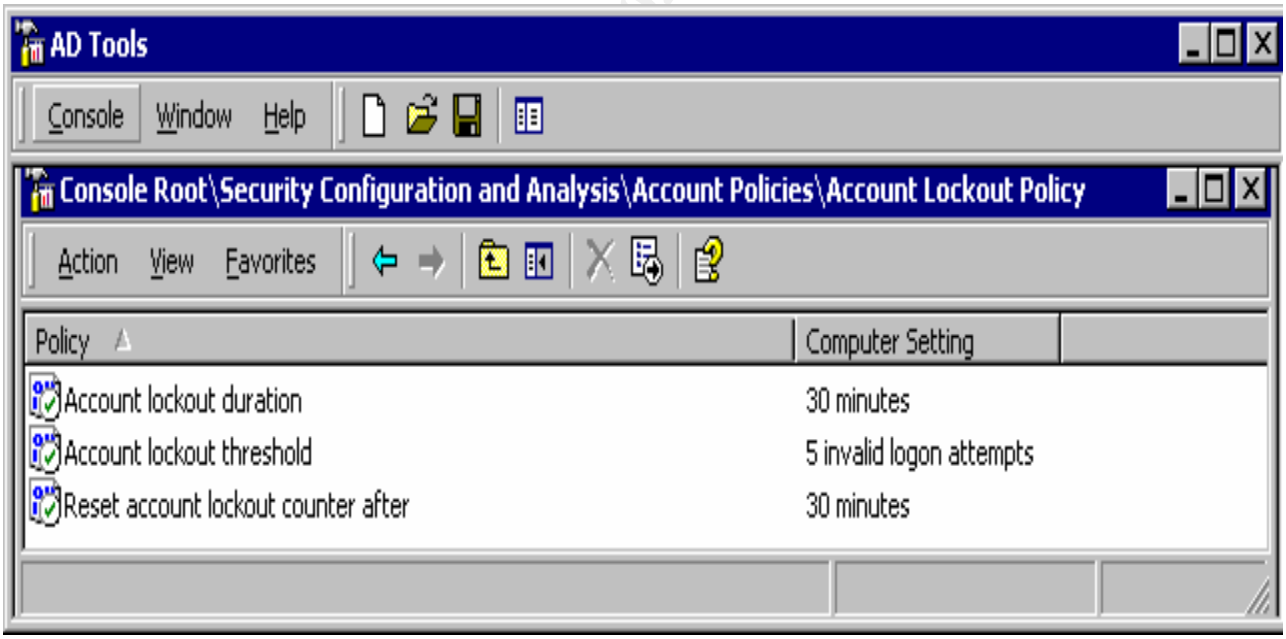
So we have passwords that last about a month and a half. Password expiration is usually based on the amount of time it takes to crack a password or the time the data the password protects is viable. We suggested and the owners agreed on the 42 day default value. About two years of password history with password changes at expiration. This might seem extreme, how many good 12 character passwords can the users come up with? It is anticipated this value will be adjusted down in the future. Two days minimal password age so it is hoped the user will become used to the new password in that amount of time, these

settings are usually on generated passwords where the user is given a list of generated passwords and must choose from that list. In this case the users make the passwords so this will not be as much an issue. Passwords complexity is enforced and passwords are a minimum of 12 characters. Password complexity means the password must contain characters from three of the four classes of:

- English upper case characters A,B,C,D,...Z
- English lower case characters a,b,c,d,...z
- Westernized Arabic numerals 0,1,2,3,...9
- Nonalphabetic characters such as punctuation symbols

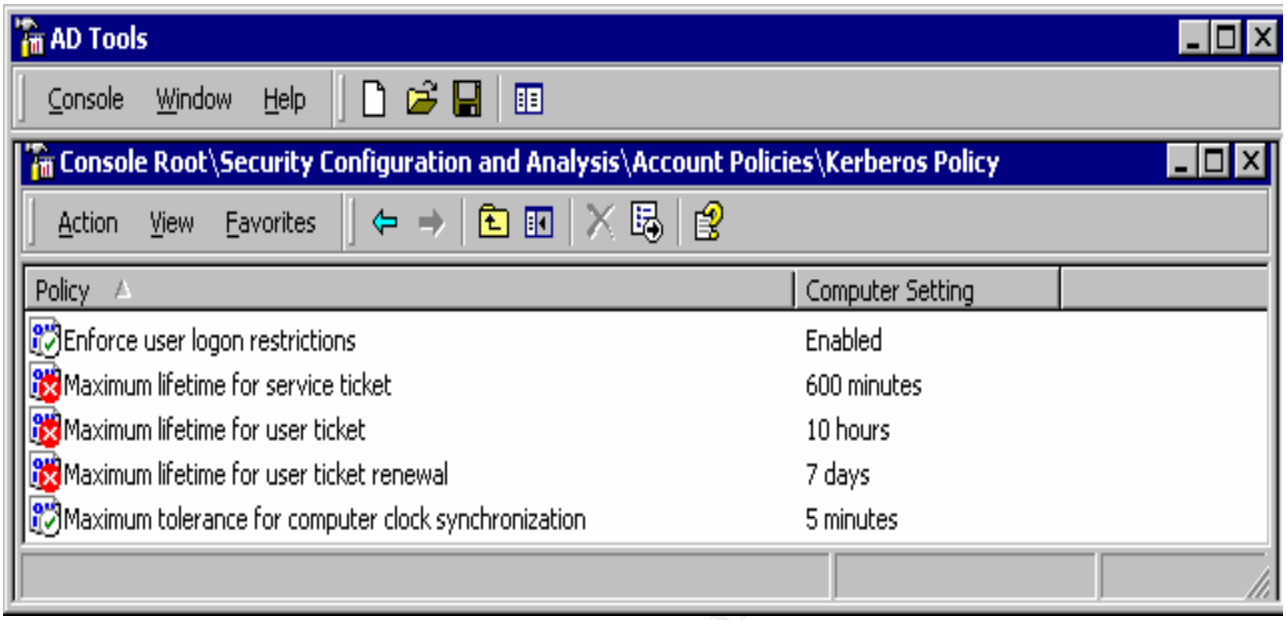
The owners were briefed on methods of choosing complex passwords of this length like using shorthand notation for a phrase. Twelve characters seem to be a good choice to enforce the intent of using key characters from phrases instead of permutations of dictionary words. This also allows the users to choose passwords of more than 12 characters as well. Reversible encryption is not required by any application, so it is disabled.

Account Lockout Policy



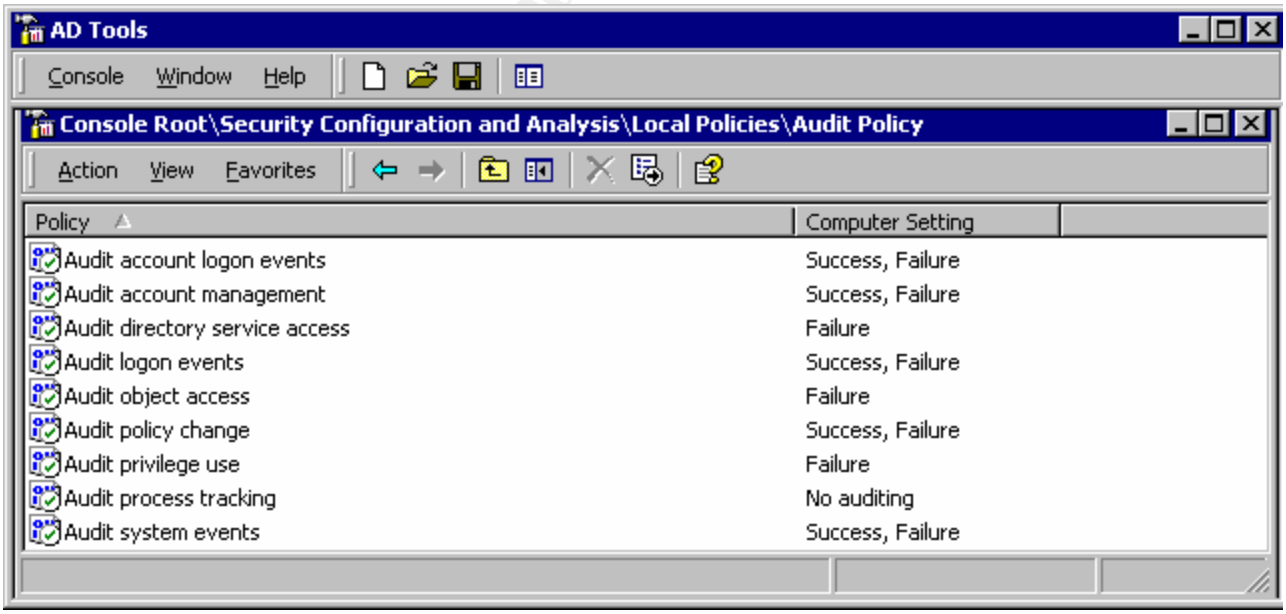
Five invalid password failures is a balance in convenience and security as are the 30 minutes of account lock on five failed login attempts and the lockout counter reset. These settings will be re-evaluated when the Point of Sale terminal is installed since the shop will then not be able to function without the computer system for 30 minutes at that time. The value of 5 for lockout seems to be how long it might take for the user to realize the CAPS lock is on or one of the common causes of mis-typed passwords is in effect.

Kerberos Policy



Use the Kerberos Key Distribution Center to check for user restrictions before granting a ticket. Only let tickets last a typical store day. Only accept 5 minutes of tolerance in time variance between the domain controller and the laptop or Point of Sale terminal

Audit Policy

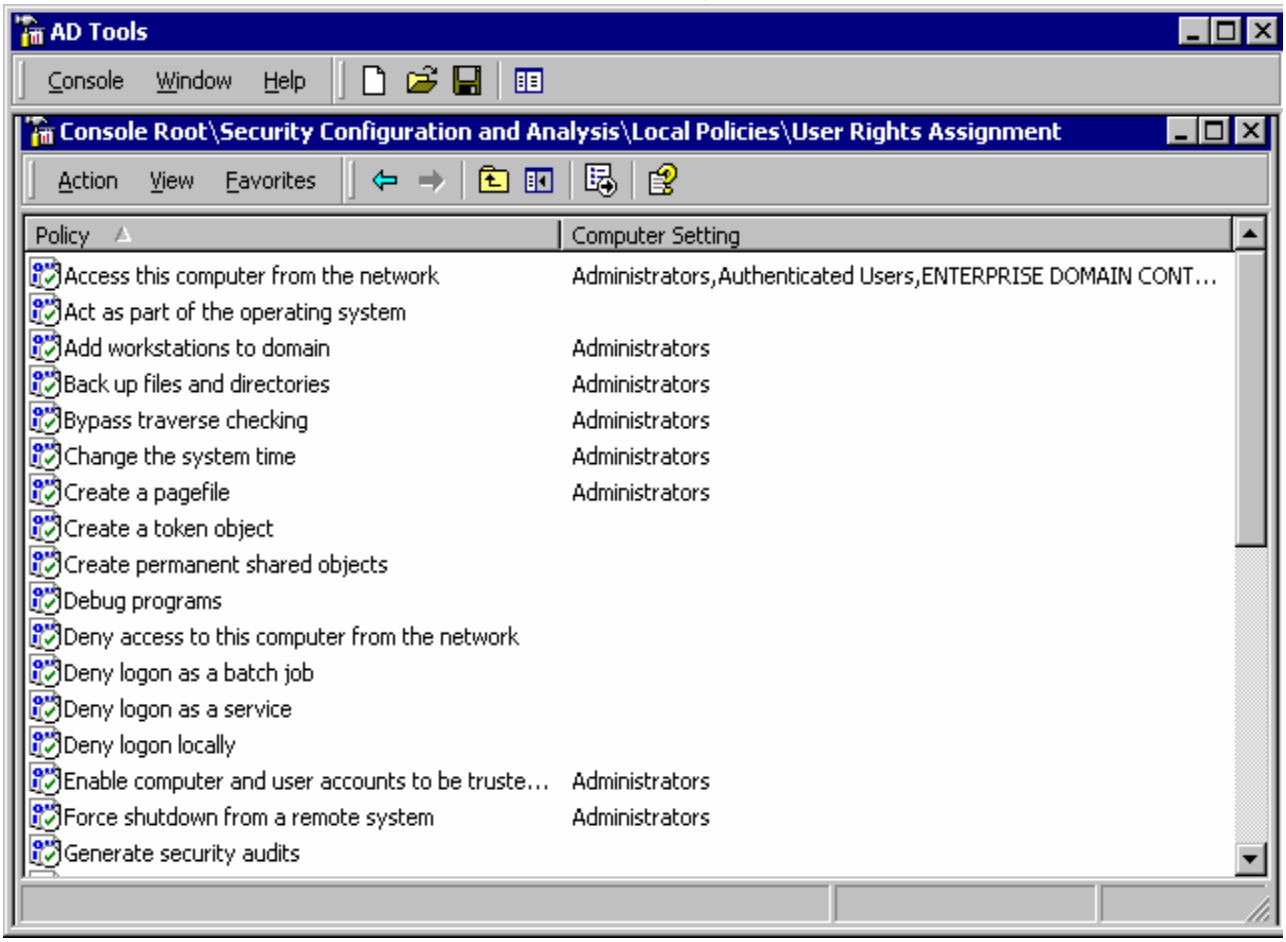


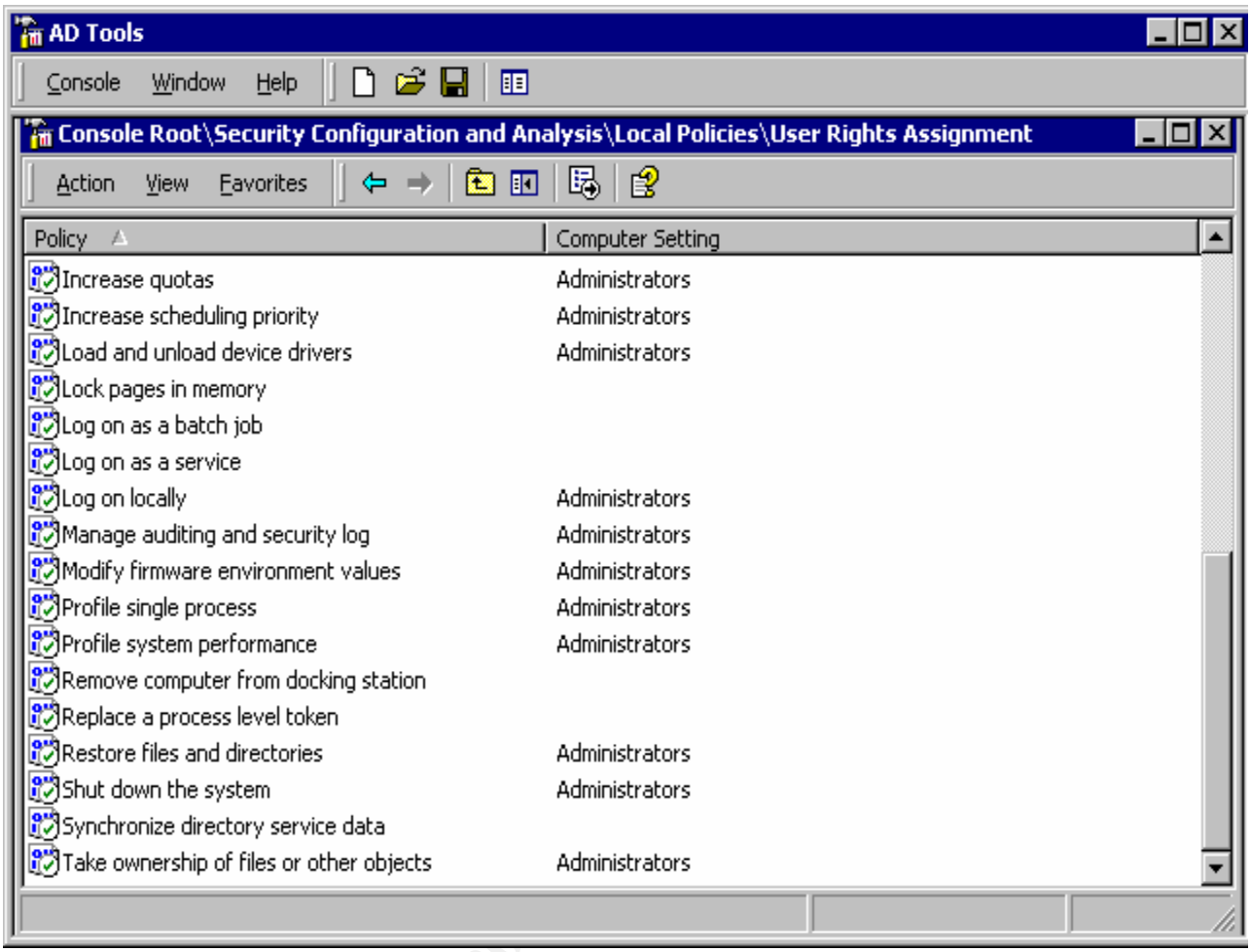
The normal running of the gun shop's computer network should not produce a large amount of audit records. A follow on project the service provider proposed is a scan of the audit logs for unusual activity. This would include the ZoneAlarm, PestPatrol, and LinkSys logs as well. As currently configured the audit policy is out-of-the-box (i.e. green checks in white circles).

The previous day's audit logs are written to a CD and taken to the bank each day as mentioned above. Audit logs can provide some warning if the gunsmith starts to accumulate data for his own future use or if one of the owners is thinking of a marital split and manipulating the computer in an irregular manner. This means the template and its associated settings must take care of both outside and inside threats. Inside threats might not be considered on a network with a man and wife owners and a gunsmith wanting to partner in the shop, but should be.

The files and folders to have auditing enabled are not set in the template, but done ad hoc. The reason is all but the gunsmith is a quasi-administrator, and he will be if he becomes a partner. So having such settings in GPOs and templates allows almost every user the ability to know at system turnover what files and folders are audited or to be easily determined by examining the GPOs or templates. By setting these explicitly when needed it is hoped the intended action to be audited is more unaware, the task to determine the items audited now a scan of the file system instead of just the template or GPOs.

User Rights Assignment





We will restrict *Access to this computer from the network* to administrators, authorized users, and enterprise domain controllers. This setting prevents remote access so users must be on the machine for access. This setting will need to be reviewed for the Point of Sale terminal.

We will not have an account with *Act as part of the operating system*, no application needs this setting.

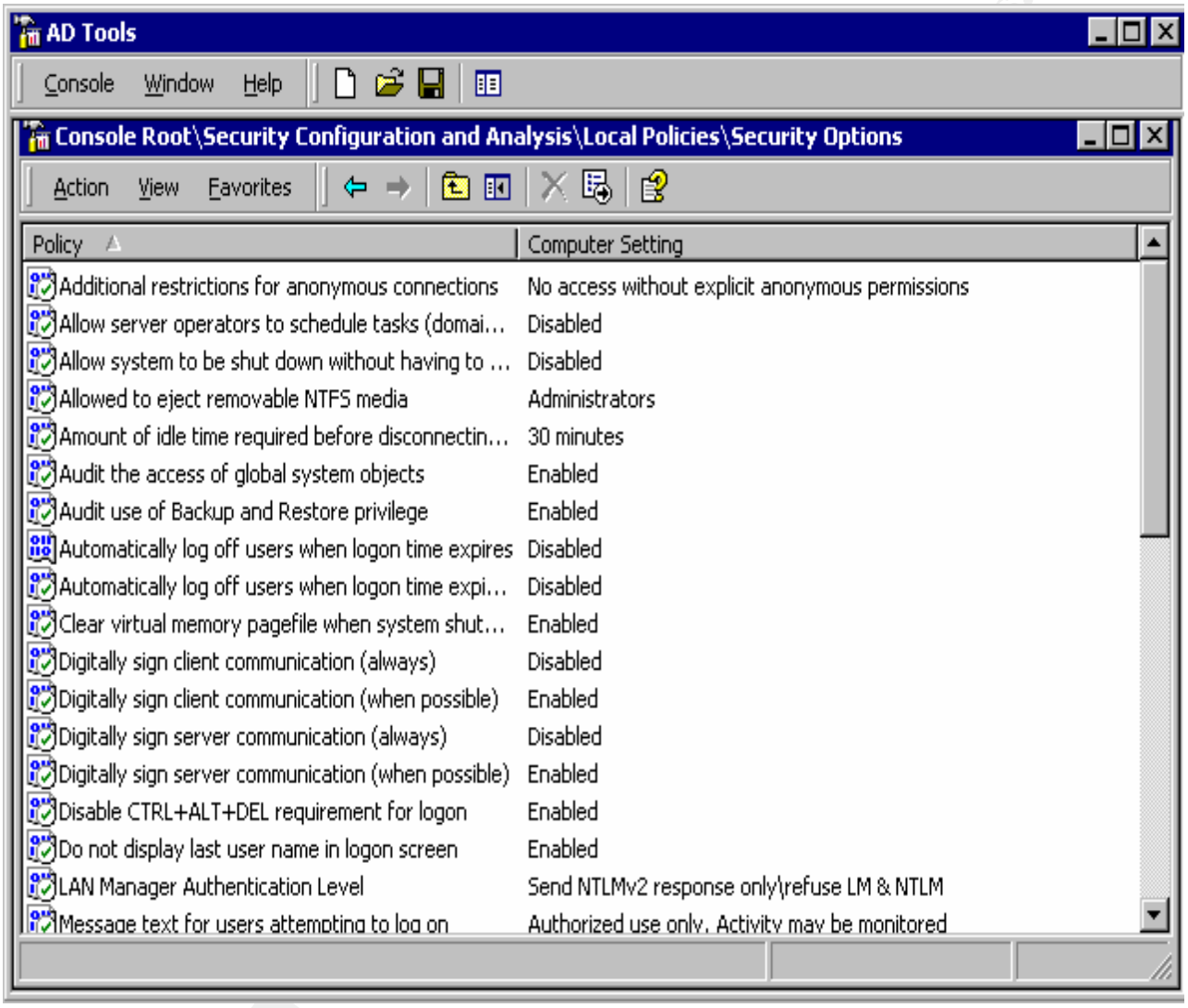
Only administrators get *Add workstations to domain* and *Backup files and directories.* If these functions need to be performed then the service provider or the owners will need to use the administrator account.

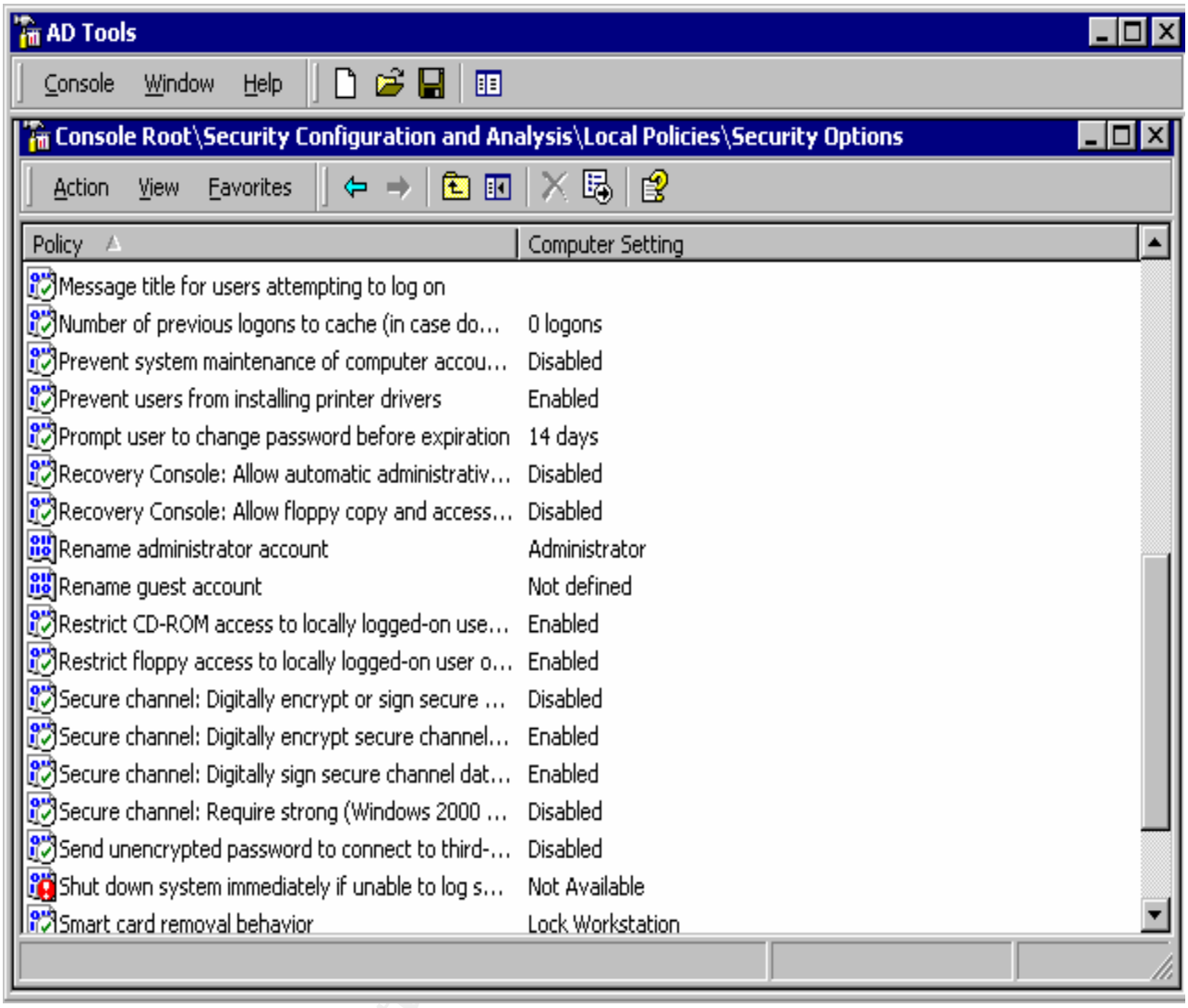
No users may *Bypass traverse checking*, only administrators. The system is small enough to configure the file system to not need this ability for non-administrators.

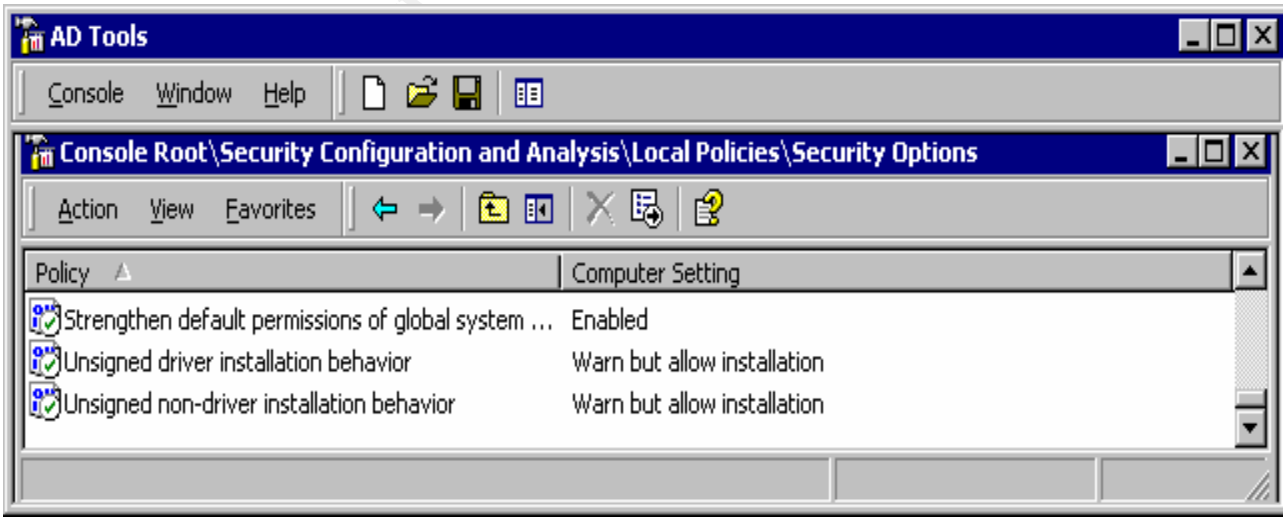
In general terms the system is to be run like a Unix machine. The owners have the ability to become administrators by using the shared password on the administrator account upon advice from the service provider or have the service provider do the tasks on their visits to the machine. There will be no Power Users, no Backup Operators, etc. Items not explicitly set to allow the administrator using the MMC tool can, of course, add access. If a quick fix is

needed that requires administrator rights, the *runas* command can be used much like su in UNIX, though limited to command line quick fixes.

Security Options







There are three possible settings for *Additional restrictions for anonymous connections*. We choose the most restrictive *No access without explicit anonymous permissions.* This option removes "Everyone" and "Network" from the anonymous user's token preventing null sessions and requires the anonymous user be explicitly granted access to resources. As mentioned in the previous section, we will run this machine much like a UNIX machine, an older UNIX machine, with administrator and everyone else privilege distinctions – thus no server operators so no server operators to schedule tasks.

We don't want to have the shutdown option on the login screen, we do want the user shutting down the machine to login first so the username is in the audit logs and provides accountability for machine shutdowns. This will also help ensure the system has not been booted into the XP Home system.

Administrator only can eject removable NTFS media since we have no requirements otherwise.

Thirty minutes as default for idle SMB sessions to be disconnected suits our requirements.

We wish to audit the access of global system objects and the use of Backup and Restore privilege.

We disable automatic log off on accounts since there will be many occasions when all the employees may need access to the computer network at all hours of the day, all days of the week. While this might allow someone to access the machine with a snooped username and password at off hours, the decision here is to determine this potential activity with session logs and allow the employees continued access with no restrictions based on time of day. It was considered to enable this setting for use on the accounts of temporary employees. It was possible that those accounts might need access restrictions by time of day or day of week. In fact it was realized that temporary employees work more hours than the regular employees. This is especially true when the temporary are filling in for the regular employees during vacation, sick days, etc. They are not as familiar with the system and take longer to accomplish the same tasks.

We clear virtual memory, the page file, when the system shuts down to remove any sensitive data like account names, filenames, etc. stored there.

Digitally signing is left as *when possible*. It would be possible to add a machine to the LinkSys Ethernet switch and see the traffic. As both the lap top and system are Windows 2000 *when possible* should imply all the time. What is unclear is how the point of sale terminal will integrate. Leaving this as when possible allows us to work with the terminal addition without modifying the template. Risk here is small since it is thought another cable to the switch will be noticed since it is in the office with the system. This setting will be reviewed when that addition is made to the network.

We disable the *Disable CRTL+ALT+DEL* to add that bit of security to avoid keystroke capture of passwords.

We also enable the *Do not display last username in login screen*. Though only a few users are on the machine, the last user is most probably the current user, and it would help in avoiding typos in username entry – the setting does raise the security consciousness of the user attempting the login.

We accept only NTLMv2 *Authentication level* as we have no machine type other than Windows 2000.

We have added a simple login banner with the recommended *Authorized use* and a notice of monitoring.

No login caching, we are the domain controller and the data that would be cached is on this machine anyway.

Ability to install printer drivers is left to the default of enabled since the administrator via the service provider will do such tasks.

We have set password lifetime to 42 days, so 14 days notice of password expiration seems a good value.

The two recovery console settings stay as default (disabled) for good security.

A fair amount of debate on renaming the administrator and guest accounts resulted in the decision to leave them as they are. The strong password, physical security, and other factors contributed to that decision. While the owners were willing to make other concessions to security, they thought this one not worth the effort since the real administrator account has a known Security ID (SID).

Restrict CD-ROM access to locally logged-on user is enabled since the drive is used to make backups of logs and select data files. Similarly the floppy, though for no particular reason. If a requirement comes up in future this can be changed. Another option is to remove the floppy for security reasons like autorun and to boot from floppy. The amount of files distributed on floppy media now makes this a more viable option.

The secure channel settings are set as the digital signature settings.

Send unencrypted password …, enough said to leave this disabled.

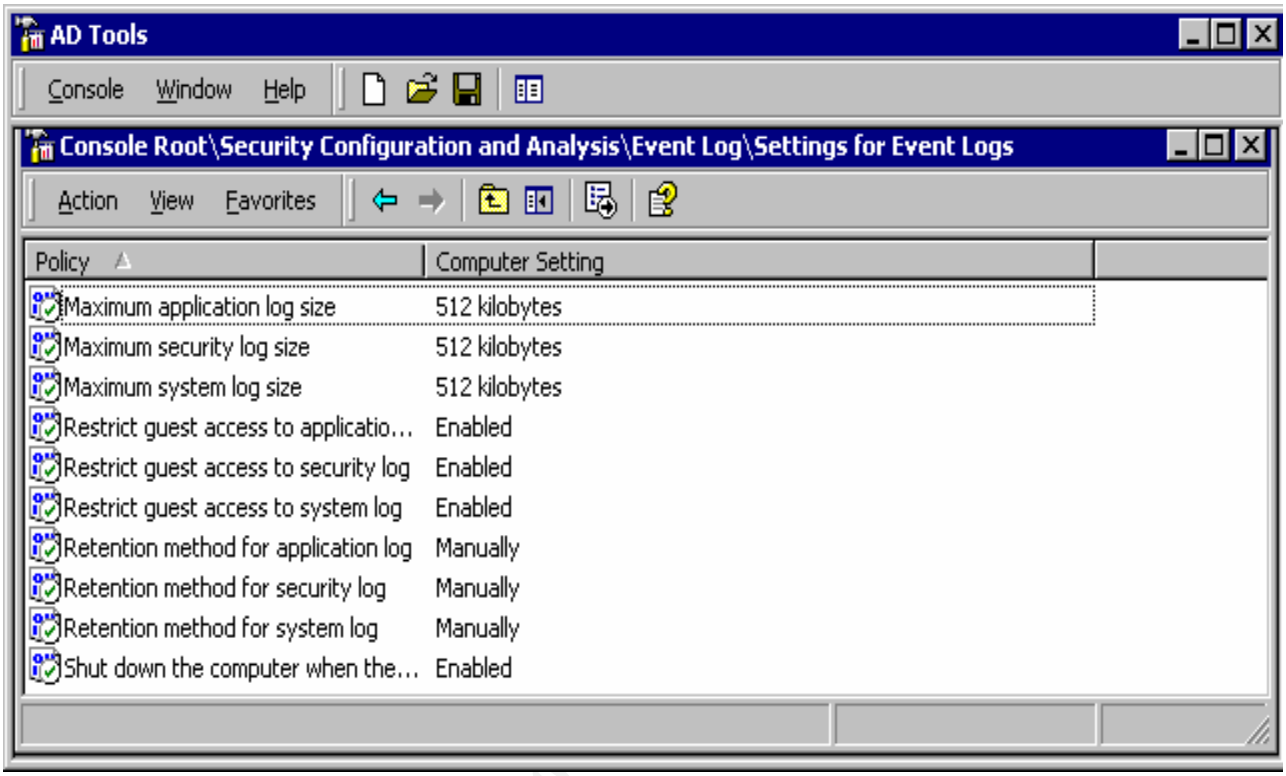
Shutdown system immediately if unable to log security audits left enabled. If this situation does occur the methods of resolving the space exhaustion without loosing the audits that might show a problem are known the owners. A buffer file was created such that its removal can get the system going again.

We cannot afford smart cards yet so those settings stay as default.

Strengthen default permissions of global system objects as default (enabled) since no reason to allow users access to such objects they did not create.

Unsigned installation behavior left as *Warn but allow* as a good compromise.

Settings for Event Logs



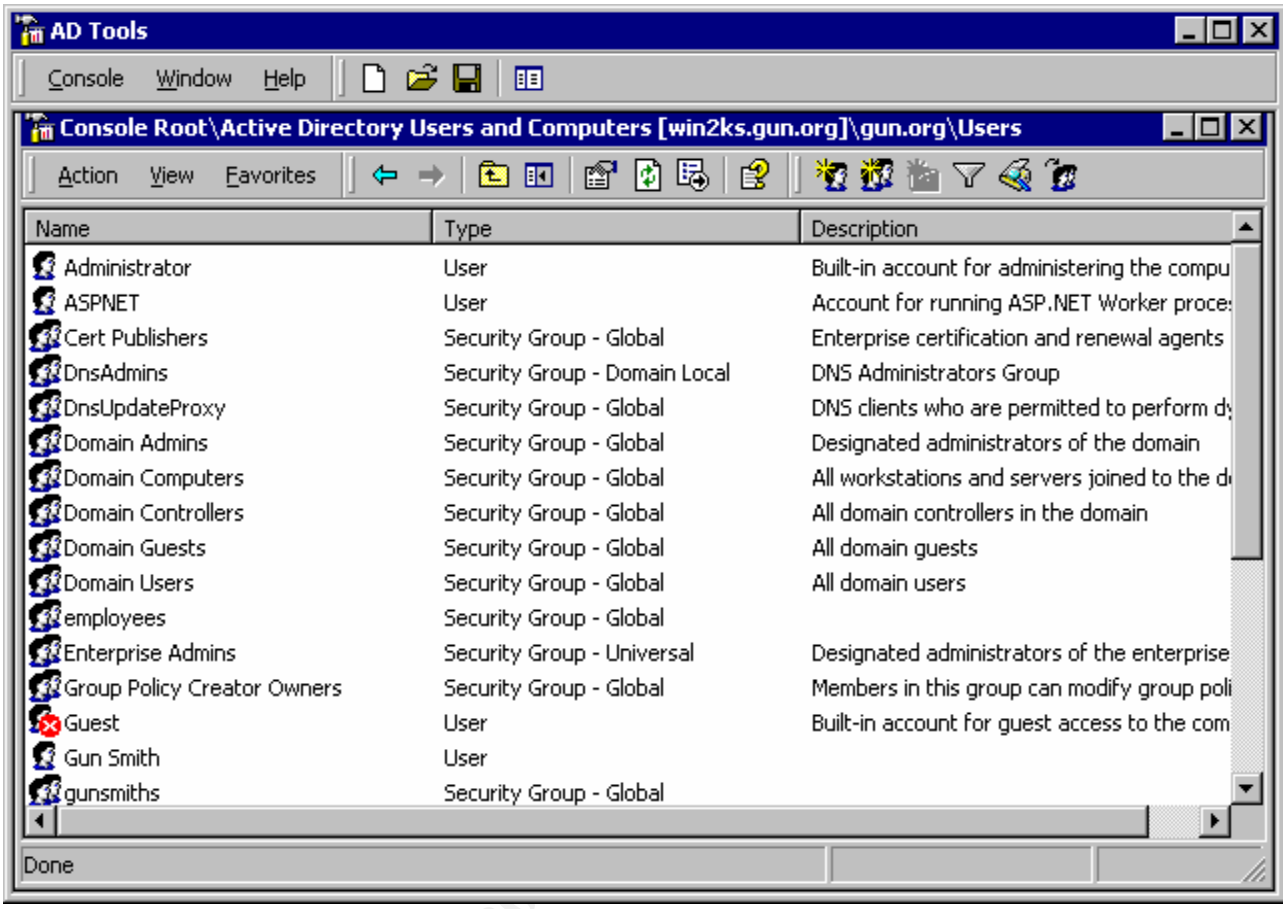
With only a 9GB disk, and that split into two partitions, the maximum size of the application, security, and system logs was set to the value of 512KB. This seems very small, and this value used to be the minimum maximum setting. From monitoring the system the value is sufficient and optimum since the shop's applications require a lot of disk space for temporary files for sorting and producing reports. While security and the logs are important, the applications are more so. Since the security logs are important and we have limited their size to a very small value, we will set the system to shutdown if the security log is full. We have included a buffer file that can be removed to get the system running again to examine the logs to determine the problem. If there is ever an occasion when this becomes an issue we can take the appropriate action at that time like getting another disk for application data.

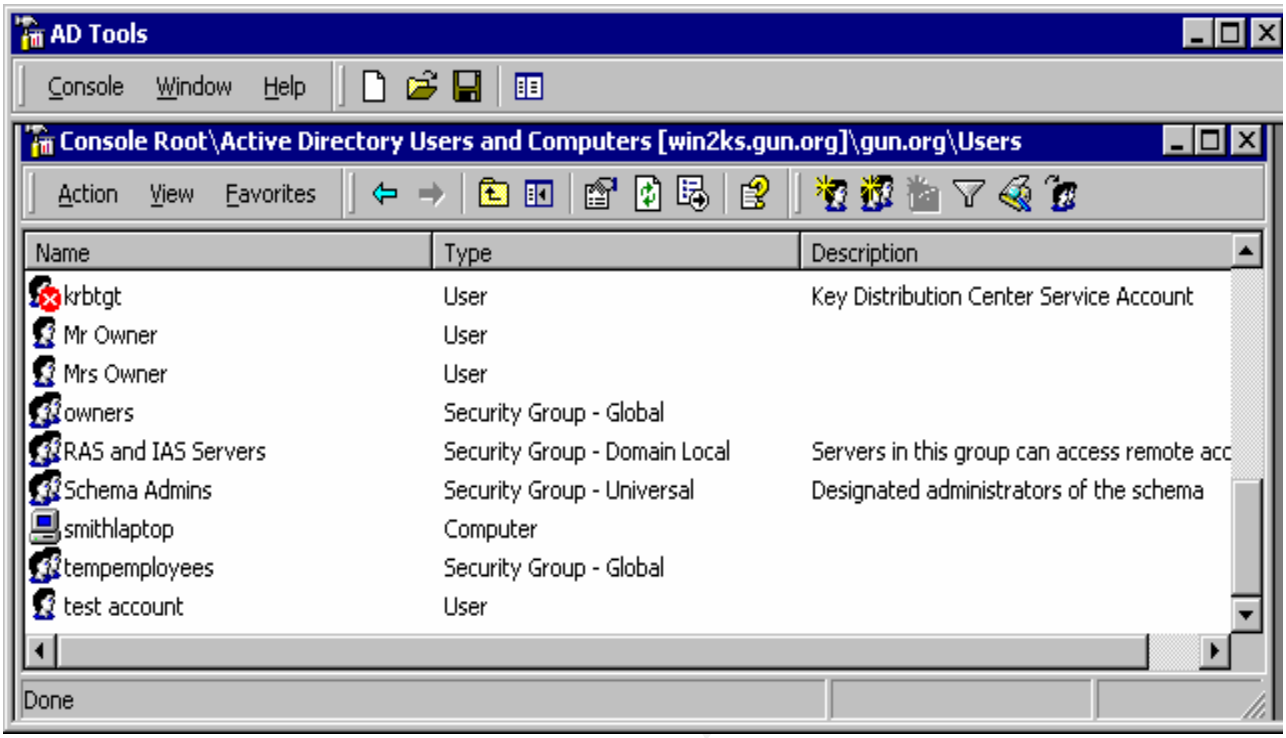
Guest has no need to access any of the logs as Guest has no login.

As the service provider reviews logs on a weekly basis and the logs are copied to CD-R daily the retention method is changed to days. The logs are copied to the CD-R scheduled daily backup since they still fit on the media with the application data. Thus no additional cost for media and a small amount of time to provide the capability of having those logs. When the application data grows to fill the CD-R, this process will be reviewed.

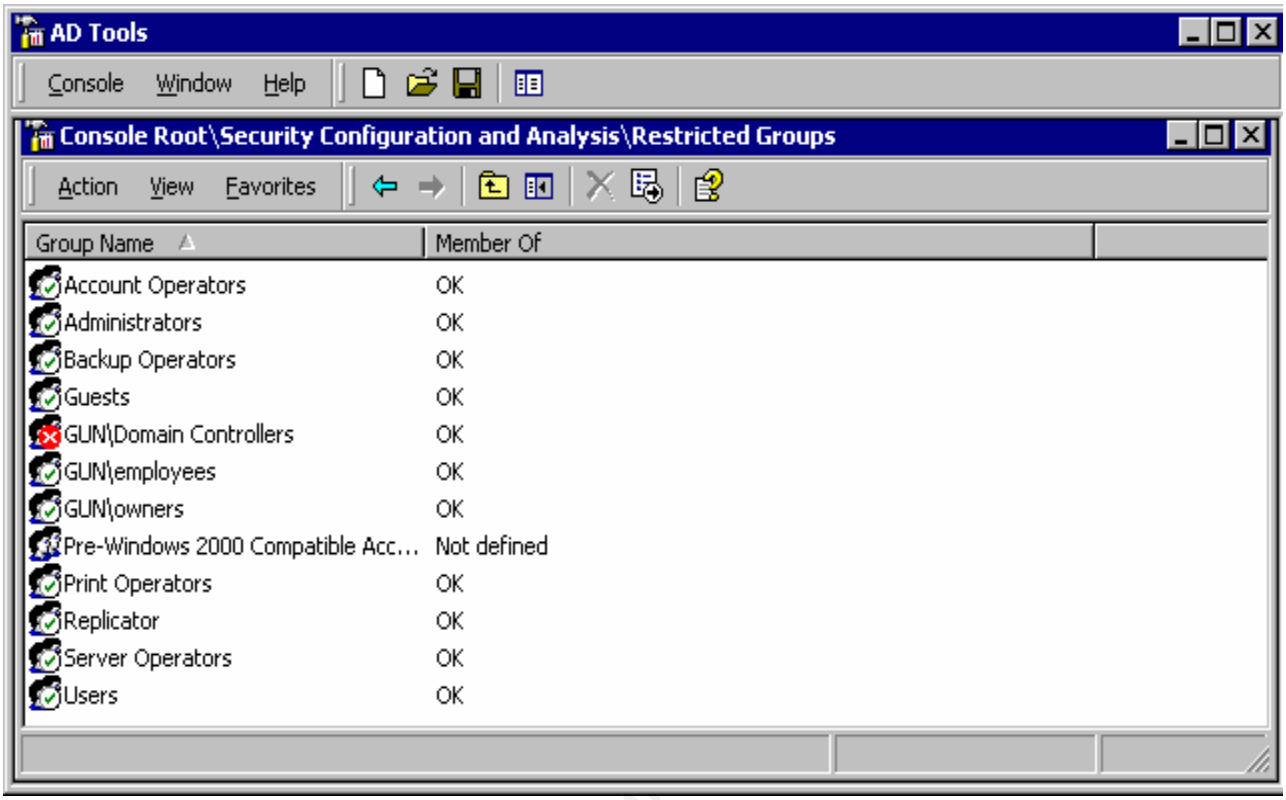
To be consistent with the setting in *Security options*, we enable *Shutdown computer when the security audit log is full*

Restricted Groups





All applications tested run with domain user group access, none required the Power user group (which is not added to a domain controller anyway). By using restricted groups in the security template and thus in the group policy, group membership is enforced. So if someone were able to create a new account or add another account to a restricted group, that setting would be removed at the next group policy update. Most of the groups will be added, but not *tempemployees* as we wish to be able to add and remove users from this group without having them removed or added by GPOs for obvious reasons. In particular we want to add *GUN\Domain Controllers* to prevent another domain controller being added to the domain and network, *GUN\employees* and *GUN\owners* to keep those groups from changing membership.



System Services

One of the key elements of securing a computer network is to not run network services that are not needed. Much like the restricted group enforcement just above, security templates allow us to not only disallow unneeded services, but to enforce that restriction by group policy. Problem is, of the 90 or so services, which are critical, which are needed, which are safe to disable? Most are clear in their names what they do, a few are not. A few checklists do exist for listing system services like one for IIS servers, but our case is somewhat different. We are running a domain controller, application server, fileserver, etc. all on one machine AND we need to be flexible on what might be added as the computer network grows AND be as secure as possible. There are quite a few articles on TechNet dealing with problems after re-adding services so we will disable the services known to be not needed only – we will not remove the service. The tables below are taken from a Microsoft TechNet article on Securing Servers Based on Role.[2]

The first table is for member servers

Service	Startup Type	Reason for inclusion in Member Server Baseline
COM+ Event Services	Manual	Allows management of Component Services
DHCP Client	Automatic	Required to update records in Dynamic DNS
Distributed Link Tracking Client	Automatic	Used to maintain links on NTFS volumes
DNS Client	Automatic	Allows resolution of DNS names
Event Log	Automatic	Allows event log messages to be viewed in Event log
Logical Disk Manager	Automatic	Required to ensure dynamic disk information is up to date
Logical Disk Manager Administrative Service		Manual Required to perform disk administration
Netlogon	Automatic	Required for domain participation
Network Connections	Manual	Required for network communication

Performance Logs and Alerts	Manual	Collects performance data for the computer, writes it to log or triggers alerts
Plug and Play	Automatic	Required for Windows 2000 to identify and use system hardware
Protected Storage	Automatic	Required to protect sensitive data such as private keys
Remote Procedure Call (RPC)	Automatic	Required for internal processes in Windows 2000
Remote Registry Service	Automatic	Required for hfnetchk utility (see Note)
Security Accounts Manager	Automatic	Stores account information for local security accounts
Server	Automatic	Required for hfnetchk utility (see Note)
System Event Notification	Automatic	Required to record entries in the event logs
TCP/IP NetBIOS Helper Service	Automatic	Required for software distribution in Group Policy (may be used to distribute patches)
Windows Management Instrumentation Driver		Manual Required to implement performance alerts, using Performance Logs and Alerts
Windows Time	Automatic	Required for Kerberos authentication to consistently function
Workstation	Automatic	Required to participate in a domain

Then a table for domain controller services in addition to member servers.

Service	**Startup Type**	**Reason for inclusion in Domain Controller Baseline**
Distributed File System	Automatic	Required for Active Directory Sysvol share
DNS Server	Automatic	Required for Active Directory integrated DNS
File Replication	Automatic	Needed for file replication between domain controllers
Kerberos Key Distribution Center	Automatic	Allows users to log onto the network using Kerberos v5
NT LM Security Support Provider	Automatic	Allows clients to log on using NTLM authentication
RPC Locator	Automatic	Allows the domain controller to provide RPC name service

Which gives our System Services settings:

We choose to leave *Alerter* and *Messenger* system services. Though most papers and security checklists choose to disable these, we think the value provided by these two services running together overcomes the risks.

We put *Plug and Play* to manual due the recent problems with this service and our anticipated use of this service in adding new hardware.

We disable *WINS*, it is going away and not needed in a native Windows 2000 domain.

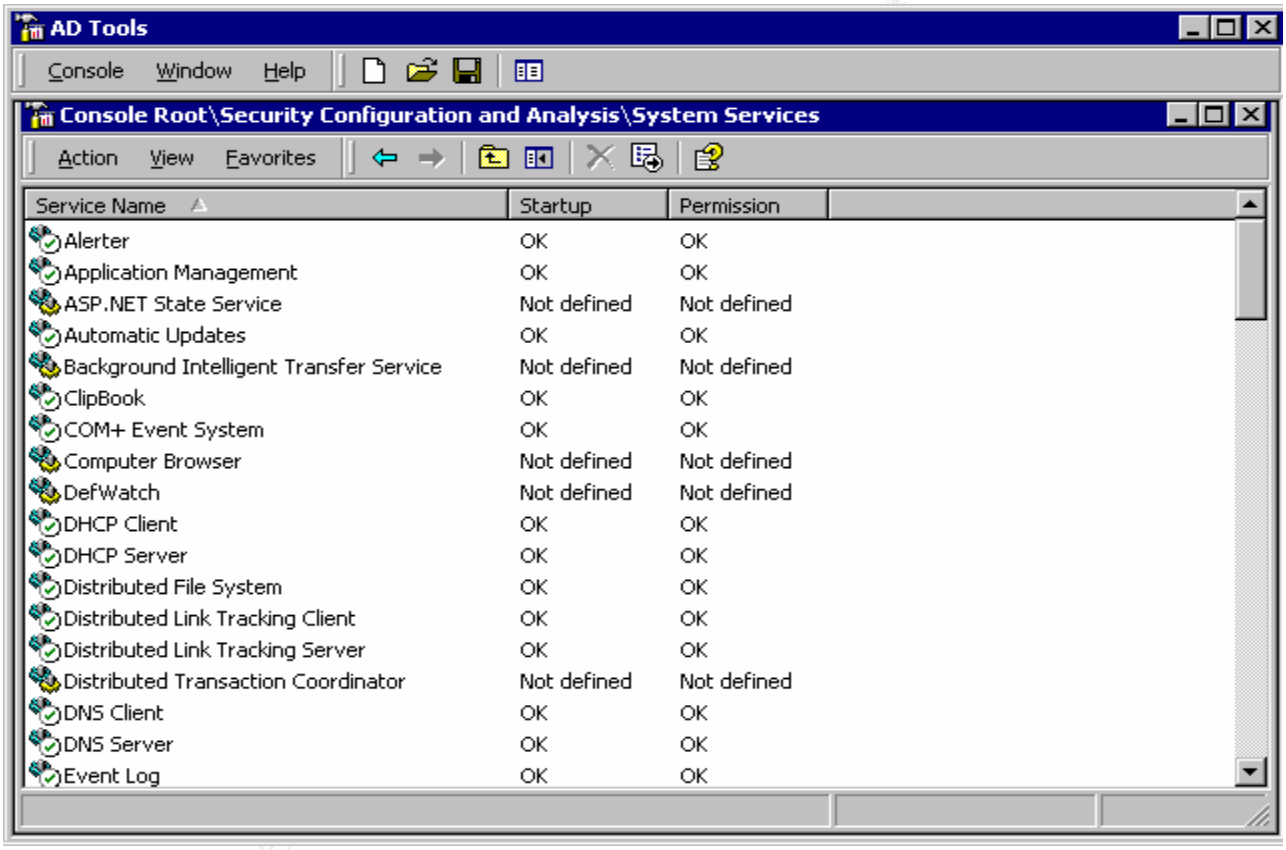
The setting for *Computer Browser* system service illustrates the problem of analysing system services settings in the security template. My search engines, search on Microsoft's web pages, etc. yielded little information. Sounds important and useful. Sounds exploitable or at least an information leak as well. As this system service was also in Windows NT Version 4, is it really needed in a Windows 2000 native domain? Will not Active Directory provide such a service? Some detail on the service function is available in the Services Control Panel. Then there are services we might need later as the computer network grows like the Macintosh service. Throw in the system services provided as part of packages line Norton AntiVirus, PestPatrol, etc. and the task becomes even more difficult. Luckily there are the services like Telnet and Fax services we know we do not need – yet anyway.

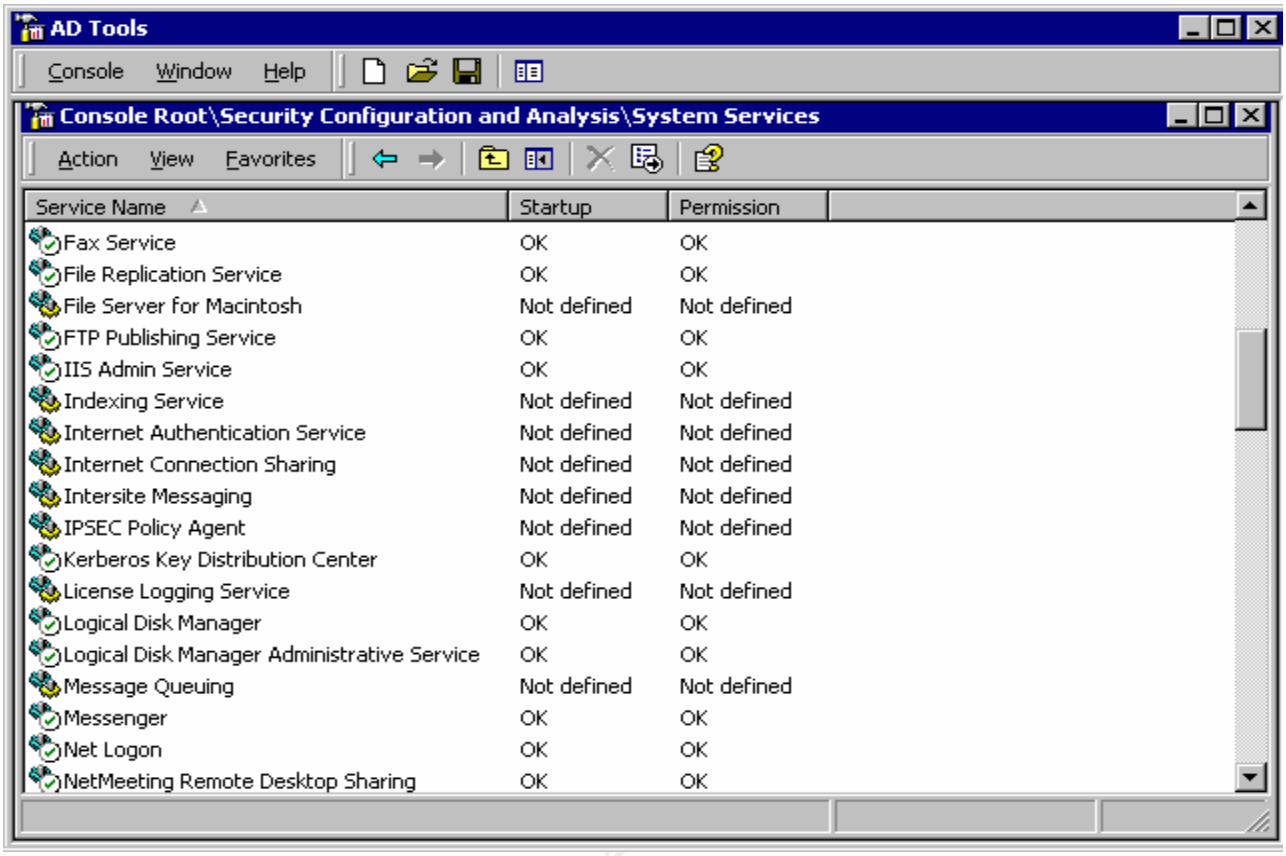
We do disable DHCP server as the LinkSys performs this function and we do not want two competing services.

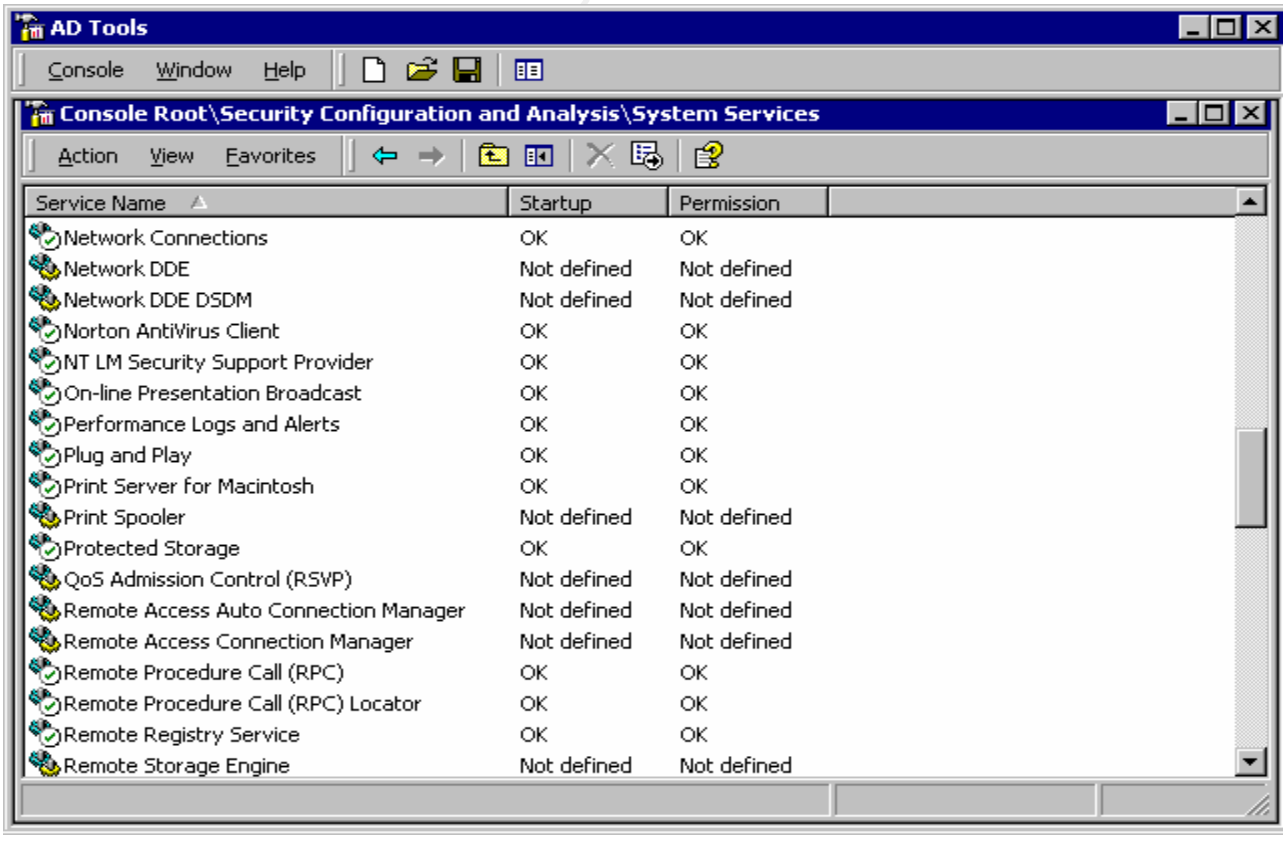
WMDM PMSP Service appears to be part of media player. Media player is a nice utility, but has been the subject of a few patches lately and the source of a bit of controversy due to the wording of the license agreement you acknowledge before getting the patch[3].

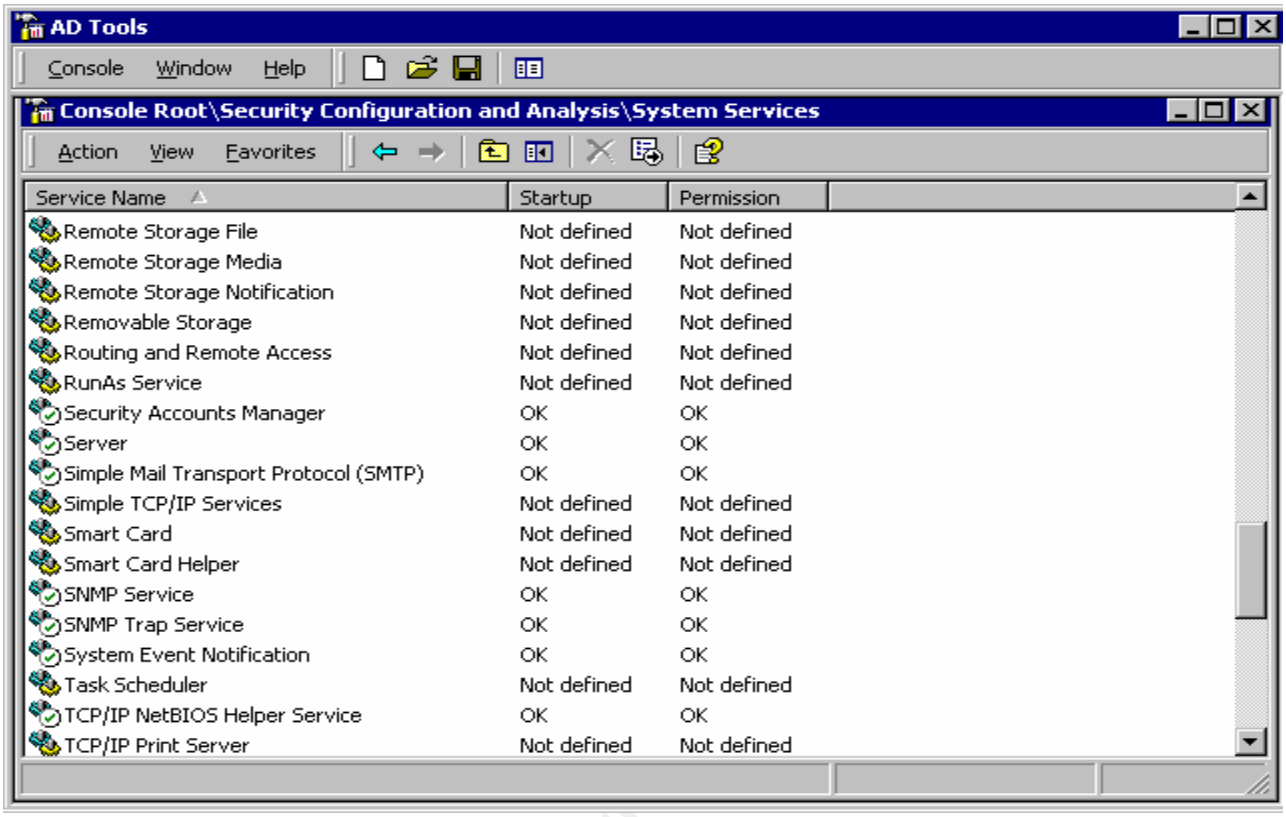
In summary we disable the bad, enable the good, leave the unknown as undefined. The bad are *ClipBook, Fax service, FTP Publishing, IIS Admin, NetMeeting, On-Line Presentation Broadcast, Print Server for Macintosh, SMTP, SNMP* and *telnet.*

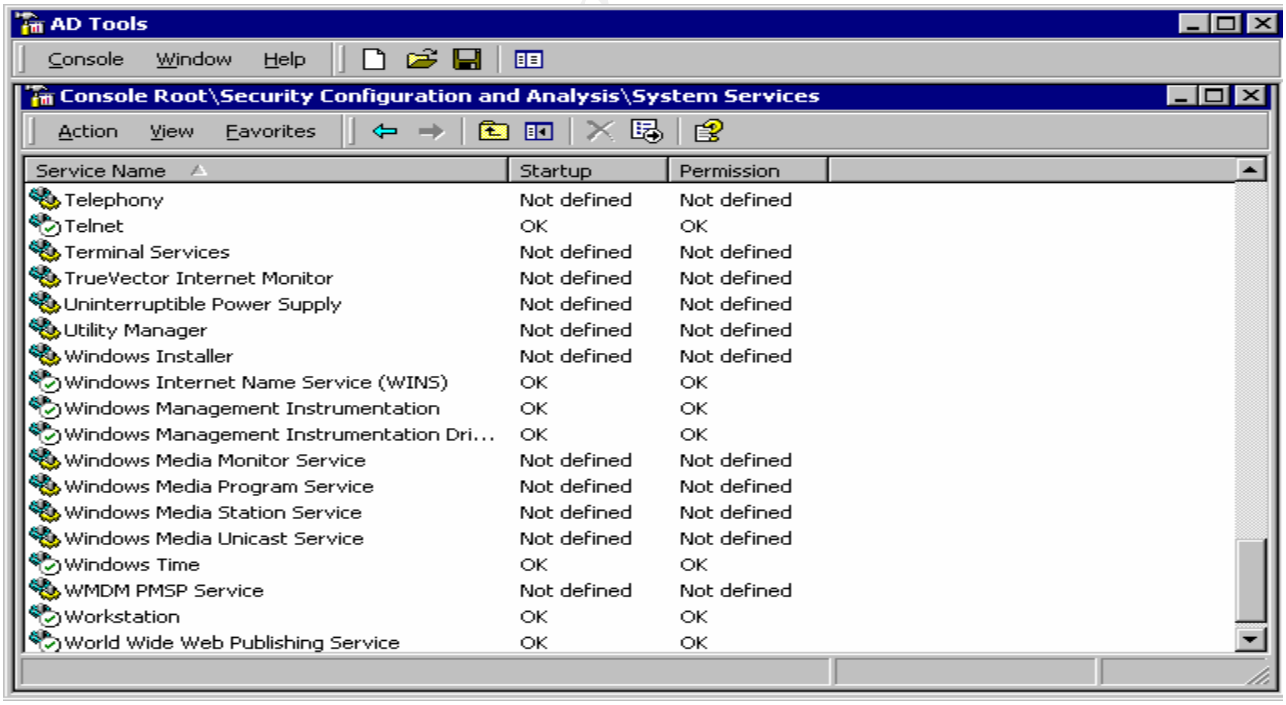
Other issues with the addition of the Point of Sale terminal would be an Uninterruptible Power System (UPS), which would cause a re-evaluation of the UPS system service, and the system in general. Normal power outages in the area do occur and no real need for the computer network to function during power outages currently exist. After the Point of Sale terminal is added, then there will be a need to have the computer network functional during power outages, especially for power outages that would cause a run on a local gun shop.











Registry

Permissions on registry entries are usually augmented with permissions on the registry editors or restrictions on their use by GPOs to prevent their invokation by users. This might be fine for the Microsoft supplied registry editors, but there are more editors available on the Internet so registry permissions are viewed as a single line of defence.

For registry items themselves, the incremental nature of the two templates applied (Microsoft supplied highsecdc.inf and the NSA W2KDC.inf) do add most of the common settings for enhancing security like disable of autorun for all devices. Autorun is the feature that starts a setup program when a new CD-ROM is inserted, plays a music CD-ROM, etc. It is not good to run the setup.exe on any CD-ROM or floppy that happens to be inserted into the machine.

machine\software\microsoft\windows\currentversion\policies\explorer\nodrivetypeautorun=4,255

We do add a few registry additions and changes like:

machine\system\currentcontrolset\control\filesystem\ntfsdisable8dot3namecreation=4,1

which disables the creation of the old eight.three filenames. This was added for backward compatibility with Windows and not needed by any of the gun shop's applications.

For some TCP/IP stack protection we add:

machine\system\currentcontrolset\services\tcpip\parameters\DisableIPSourceRouting=4,2

Source routing provides the ability to specify explicitly the route taken to a node. This is not normally needed and can be used maliciously. The value of 2 discards all incoming source routed packets.

machine\system\currentcontrolset\services\tcpip\parameters\EnableICMPRedirect=4,0

ICMP redirects are messages sent typically by routers to have nodes notified they should modify their router tables. The 0 value disregards such messages

machine\system\currentcontrolset\services\tcpip\parameters\EnableSecurityFilters=4,1

The value of 1 for this registry setting enables security filters that can be configured from the control panel for the network interface card.

machine\system\currentcontrolset\services\tcpip\parameters\SynAttackProtect=4,2

SYN flooding is a denial of service technique where many SYN packets (the first packet of the three-way handshake for TCP connections) cause the node to exhaust resources keeping these half open sessions. The value of 2 lessens this possibility.

machine\system\currentcontrolset\services\tcpip\parameters\EnableDeadGWDetect=4,0

The value 1 disables the feature such that allows the detection and use of backup gateways. We do not want this feature, we will explicitly set the single gateway.

machine\system\currentcontrolset\services\tcpip\parameters\EnablePMTUDiscovery=4,0

A value of false (0) for this setting prevents detection and setting of the Maximum Transmission Unit (MTU) for paths not on the local network, setting the MTU to 576 bytes. This sometimes speeds up WAN connections in addition to the security aspects. But it could also hurt performance so this setting will be reviewed after a few weeks.

machine\system\currentcontrolset\services\tcpip\parameters\KeepAliveTime=4,300,000

This setting increases the timer for sessions where the stack has not seen a packet to prevent the unnecessary reestablishment of the session.

machine\system\currentcontrolset\services\tcpip\parameters\TcpMaxConnectResponseRetransmissions=4,2

The setting of 2 is default and causes SYN attack protection. Having the setting in the template ensures we have this protection

machine\system\currentcontrolset\services\tcpip\parameters\TcpMaxDataRetransmissions=4,3

We throttle back from 5 to 3 the number of data retransmissions.

machine\system\currentcontrolset\services\tcpip\parameters\NoNameReleaseOnDemand=4,1

Protects against name release attacks on the NetBIOS name

machine\system\currentcontrolset\services\tcpip\parameters\PerformRouterDiscovery=4,0

Microsoft default is 2, but recommends 0 to disable router discovery via RFC 1256

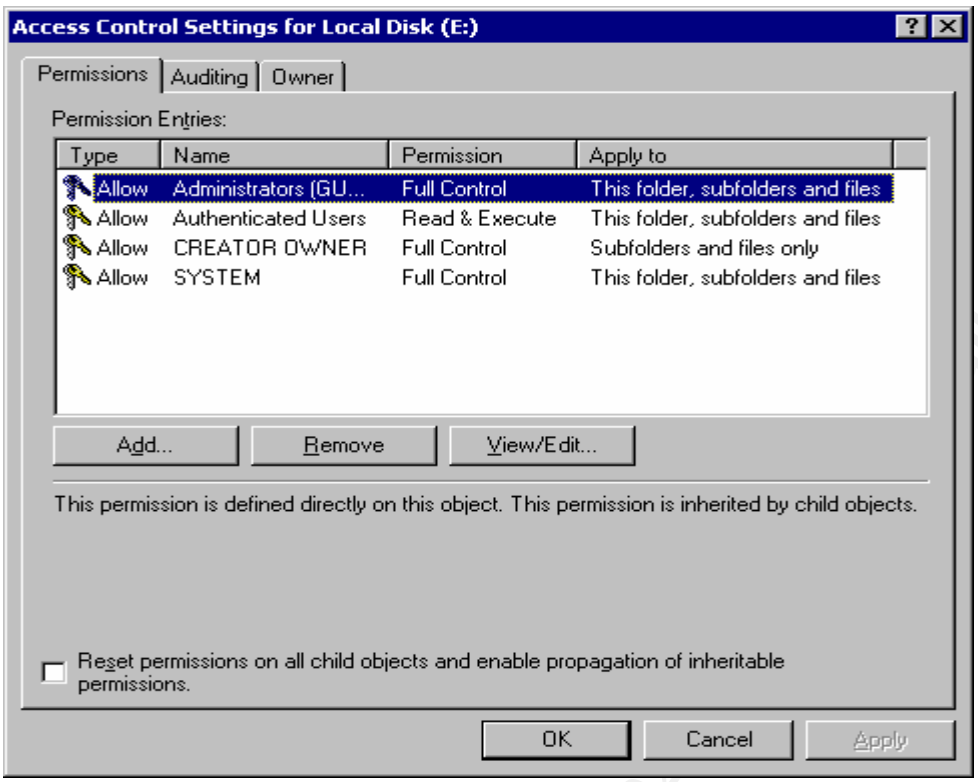
machine\system\currentcontrolset\services\tcpip\parameters\TcpMaxPortsExausted=4,5

More SYN attack protection, this when SYN attack protection kicks in, after 5 connections

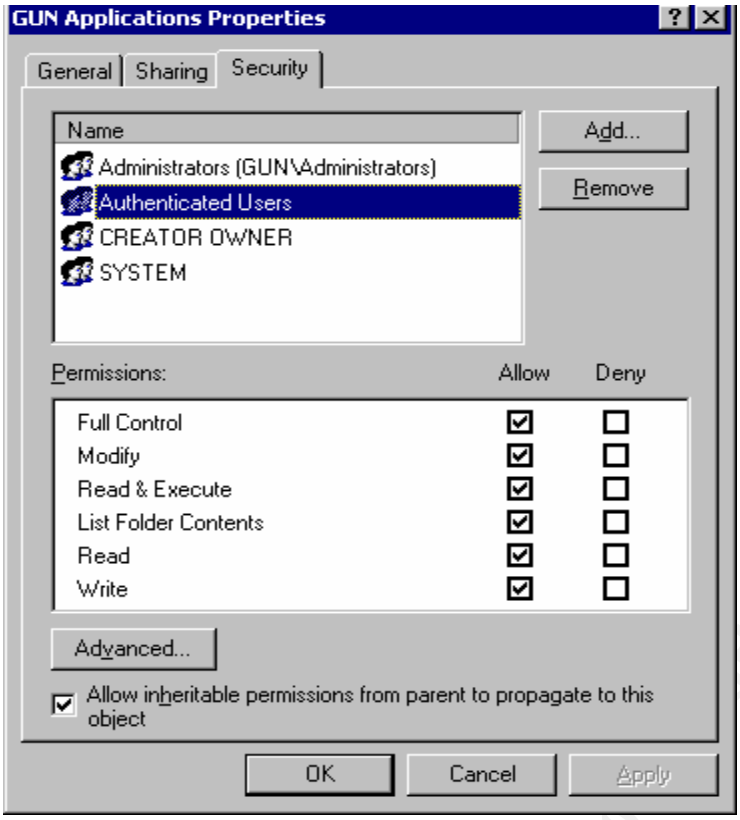
These taken from the Microsoft TechNet article on Securing Servers Based on Role cited above.[2]

File System

The additive affect of the two supplied security templates has configured the permissions on the file system of the E:\ drive. Any subsequent changes will not be done via the template and then reapplying that template to the system. A check was made to ensure the Everyone group had its access removed. For the E:\ drive Administrators, CREATOR OWNER, and SYSTEM have Full Control and Authenticated Users Read and Execute.



Similarly for E:\Program Files, E:\Documents and Settings, E:\WINNT, etc. The shop's applications are placed in E:\GUN Applications which gives full control to Authenticated Users as well.



The way to apply these permissions is by the properties of the folder. The way to apply these permissions to be set and enforced by the security template is with the *File System* setting in the Security Configuration and Analysis MMC snap-in. Once the template is exported and imported into the GPO these permissions can be enforced. Be very careful when applying these permissions in security templates, mistakes can be brutal. You may get exactly what you ask for

As mentioned above the template built thus far has most of the settings we require. What is not clear is what the lines in the security template in the [File System] section really mean. An example line:

```
5="e:\documents and settings", 0, "D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICI;FA;;;SY)"
```

The number just increases and seems loosely based on the file system hierarchy. Numbers are in Hex, an equal sign, a quoted parameter that appears to represent the drive and folder or path, comma, number, comma, then another quoted parameter of some type of string. We can take these entries in the template on faith, they are added in and the GUI interprets the settings for permissions we desire, or find the Microsoft document that describes these entries. Once the format of these strings are determined (note the [Service General Setting] and [Registry Keys] have similar formats) we could have more flexibility in maintaining our template. It took me some time with search engines to find the MSDN library document thought several newsgroup postings asked the same question and had no reply. The strings are Security Descriptor String Format strings that are part of the Security Descriptor Definition Language (SDDL). To summarize that document the string has up to 4

components: O: for owner SID, G: for group SID, D: or Discretionary Access Control List (DACL), and S: for the System Access Control List (SACL). The component parts of the ACLs, the Access Control entries (ACE) and the SIDs are also available on a similar MSDN library documents also in he same MSDN article. Using the above example and the MSDN articles

5="e:\documents and settings", 0, "D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICI;FA;;;SY)"

The folder E:\Documents and Settings has a DACL with control flags of DACL_PROTECTED and AUTO_INHERIT_REQ set. There are three ACEs. Taking each in turn:
(A;OICI;FA;;;BA) Allow; Object Inherit and Container Inherit ACE; File All Access for the Built-in Administrator group
(A;OICI;0x1200a9;;;AU) Allow; Object Inherit and Container Inherit ACE; a hex representation of the access rights; for Authenticated Users. This MSDN article gives the hex representation of access rights. Determining the rights is left as an exercise for the reader

(A;OICI;FA;;;SY) Allow; Object Inherit and Container Inherit ACE; File All Access or System

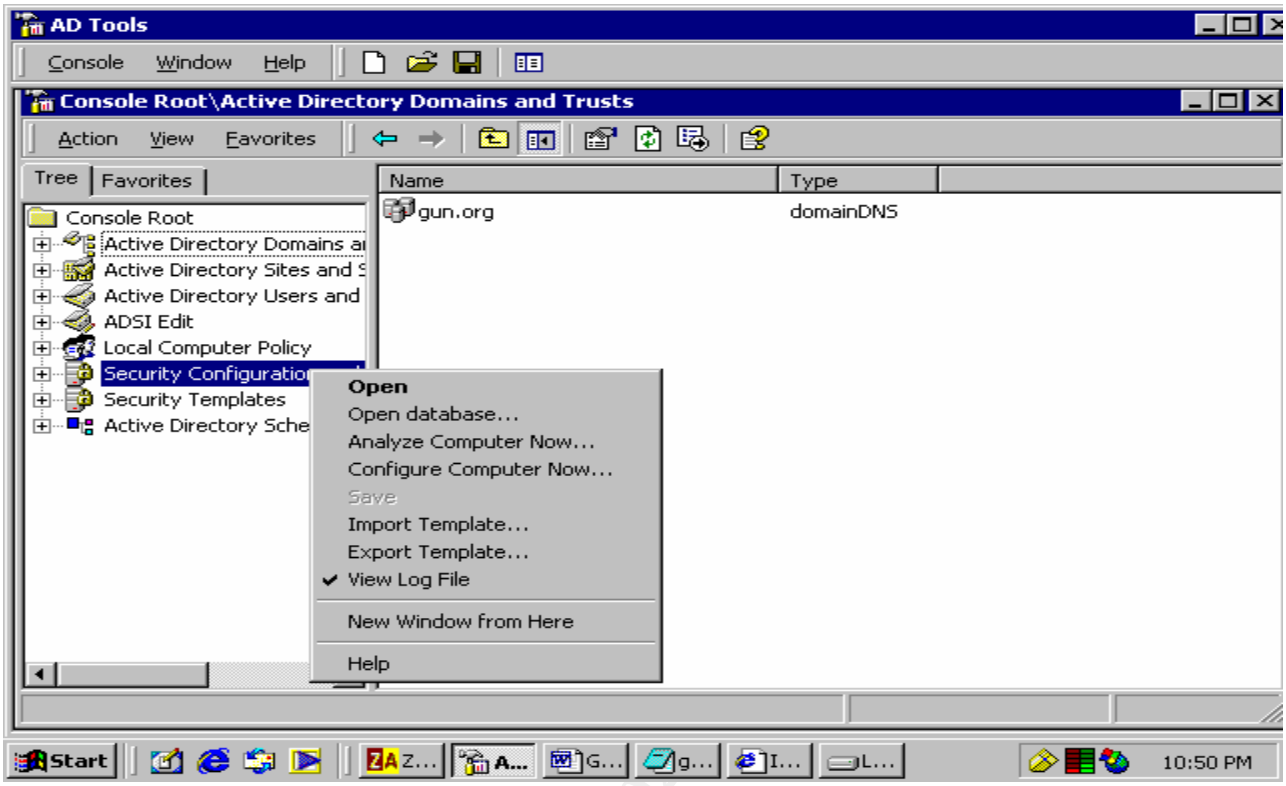
Apply The Template

The hard part is done, now an easy part. There are two ways to apply the template. The GUI Security Configuration and Analysis MMC snap-in we have been using and the secedit command line tool. The command line tool has more options and flexibility. The GUI is more intuitive and forgiving. We can use the best of both worlds by using the power of the command line tool for tasks like checking the syntax of the security template, then the GUI for tasks like the analysis.

Recall that in the steps taken thus far we have taken a newly installed system with its baseline security template, added two incremental templates (highsecdc from Microsoft and w2kdc from NSA), then adjusted settings based on the system requirements, exported those database settings to our gunhighsecdc.inf template, made a few edits to add some TCP/IP stack settings and other additions. Security templates are slightly sensitive to syntax and need to be validated before applying. The command line tool is best for this task. The GUI validates as part of applying and errors are more difficult to find.

```
E:\WINNT\security\templates>secedit /validate gunhighsecdc.inf

Template E:\WINNT\security\templates\gunhighsecdc.inf is validated
```

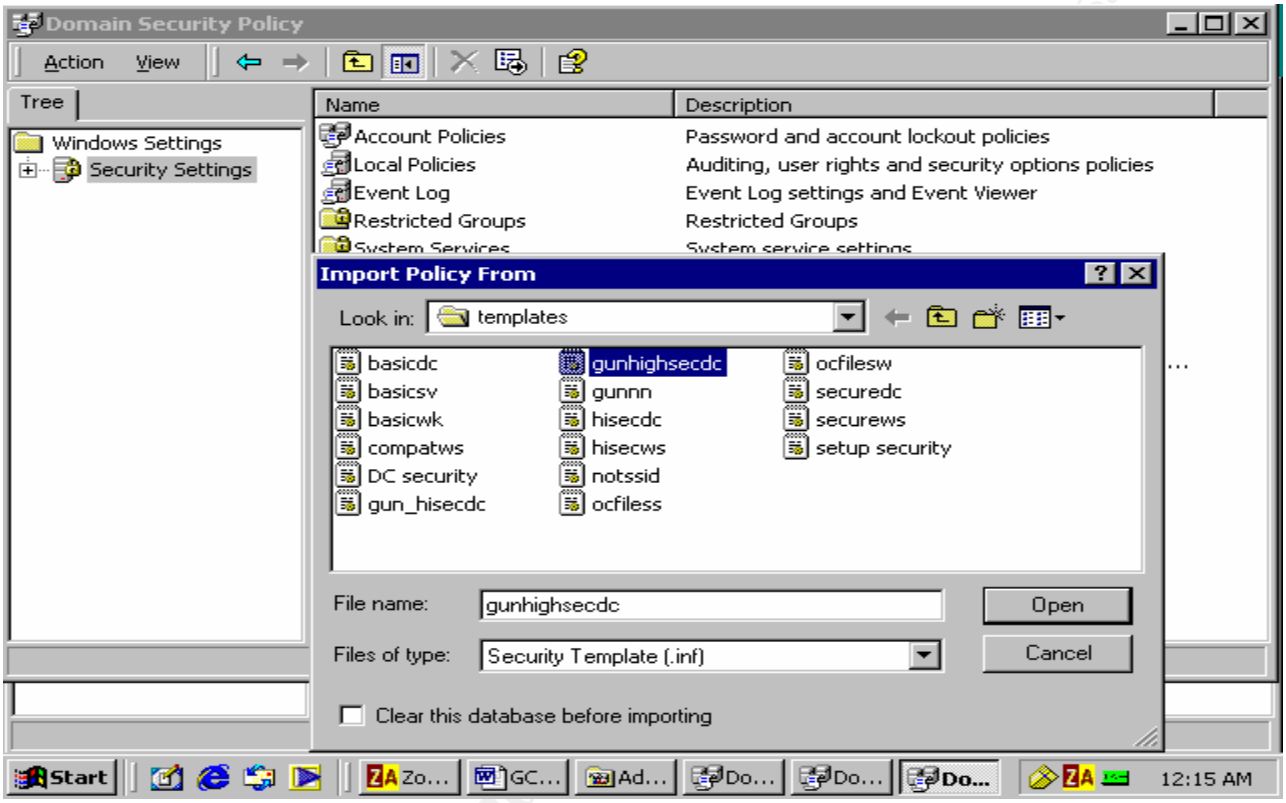
Much better than when we tried to produce the template by editing the text files. To do the next steps we will use the Security Configuration and Analysis MMC snap-in. If this snap-in is not in your MMC console it can be easily added in the manner of the other snap-ins like the name implies.



After the snap-in is added, left click on the Security Configuration and Analysis which brings up the popup menu shown. Select *Open Database* which brings up a window showing the previous databases used (if any). I use the name of the security template, but any name will do. Once the database name is selected a popup of the available security templates from %systemroot%\security\templates is presented. From our steps above the gunhighsecdc.inf file is selected. Next step is to *Analyze the Computer now…*to determine the system settings of the currently running system and the settings to be set by the application of the template. This is where the GUI is handy as the settings are logically grouped and presented. The next step is to *Configure Computer now…* (having a good backup available of course). Both the *Analyse* and the *Configure* steps produce a log file, be sure to check both before proceeding to the next step. Once the Configure is done (a popup window shows the steps and progress) another check of the settings with the GUI to make sure all is well. Now export the template as a copy to something similar to the imported template (e.g. gunhighsecdc_export.inf). We had intended to add comments to this export to document the settings, but have decided to use a document similar to this paper for that purpose. Then the exported template is unmodified from the export operation. The GUI allows you to view the two log files, or you can use WordPad or similar to search for problems.

Shop security policy requires the security template settings to be checked and maintained. Group Policy Objects (GPO) can do this for us. To get the just configured template into a GPO, Import the just exported template into the Local Computer GPO. Why the local computer GPO? A few of the settings are too restrictive for the laptop so these settings will not all be applied to the domain, site or OU levels. Another reason is the most of the settings are machine specific, i.e. system services, TCP/IP settings, items specific for a domain controller, etc. When the network grows and the other GPOs are modified they should be on

items like group and account restrictions and not in conflict with the settings we have added to the supplied template. In the process of doing those GPO modifications the settings on the domain controller will be checked to ensure the local computer's GPO settings for the machine specific items are not overwritten by the GPOs applied after the local GPO.



At the weekly site visits and log review, the gun shop employees have the opportunity to request changes to the GPO, the security template settings, or other aspects of the system. These change requests can come from the users, from analysis of the logs and systems, or from industry news. Version numbers do not exist in Windows, but we can put a version in the filename of the security templates. An example would be gunhighsecdc_mmddyy.inf for the input text, gunhighsecdc_export_mmddyy.inf for the template after export from the secedit.exe or the GUI front-end. A copy of the current template is still kept in a file names gunhighsecdc.inf. Since these are text files and we do not place comments in the templates, then the normal text tools can determine the differences in the templates. The filenames give the dates the templates were placed into production, and the properties of the templates give the create, modified, and accessed dates and times. The templates are part of the backup scheme.

Part of the service provider's offerings is the testing of additions, changes, and deletions to the security template in a non-production mode. This is easily done with templates and the disk-to-disk copies of the system. The service provider just need a comparable machine at their location, boot from the disk copy of the system, apply the to be tested template, and do

the testing. EFS is a real benefit here as the service provider can not see those files unless they change the password on the account owning the EFS folders. Another potential problem with this type of testing is if any of the applications are tied to the shop's machine by a licensing mechanism.

Test the Template

The big test, shutdown the computer and reboot. The first thing you should note is the text in the "Starting Windows 2000" box. The *Applying Security Settings* is one to watch for. Monitor disk activity lights and note the progression through the boot up process. If the system does not reboot, do not panic. It may on subsequent reboots, try again. If the system still does not boot, then recover to the last backup and try the process again.

Some change in settings will be noticed immediately after reboot, like no username in the login dialog box, the presence of the warning banner, etc. Once you login, be sure the check the system, event, and application logs to determine if any errors or events were caused by the new settings in the security template. Next with the checklist used to build the template or a copy of the template itself, check the portions of the system that should be affected and if the settings have had the desired affect.

The account passwords will not have the new requirements for complexity after the reboot until new passwords are set. Changing the accounts passwords shows those policy settings enforced. Attempts to add new accounts with passwords not meeting the template's settings produce a popup window with text:

The password does not meet the password policy requirements. Check the minimum length, password complexity, and password history requirements.

Existing users attempting to set a password that does not the policy set by the template get a more informative popup window with text:

Your password must be at least 12 characters; cannot repeat any of your previous 24 passwords; must contain capitals, numerals, or punctuation; and cannot contain your account or full name.

The administrator should know the policy when creating new accounts and is not given the details of the policy, while the users are given the details. Note the details do match the template settings. This might be too much information, an information leak, if a session is left unattended and someone else attempts to change the currently logged in user's password. We have the screen saver password protected with a timeout of 10 minutes so this is that much less of a problem and it does give the details of the policy which should balance that risk.

Next check the password expiration since password history size is given above. For this use the command line *net user <username> /domain*. The relevant text:

Password last set	8/9/2002 1:06 PM
Password expires	9/21/2002 11:53 AM

shows the password lifetime and expiration set as per the template.

Testing the expiration notification is a more difficult problem. We can wait 42 – 14 = 28 days or set the date on the machine forward or backward 28 days. Setting the date forward or backward has a bad affect in that the modification dates on files will be set to the artificial date. Temporarily setting the notification to 42 days will of course be overwritten by the GPO reapplying the policy – which for a domain controller is 5 minutes as default. For these reasons password expiration notification is not immediately tested.

Passwords are of course the first line of defense – thus the checking of most password related settings.

Checking account lockout policy is done by attempting to logon with the test and administrator account and supply more that 5 invalid passwords. The test account should be locked out for 30 minutes, the administrator account should not.

In doing these lockout attempts follow up and check the security log in the event viewer. When at the Failure Audit line double click to see if this was indeed the test account. You should see the other events like account lockout and enable in the event viewer as well.

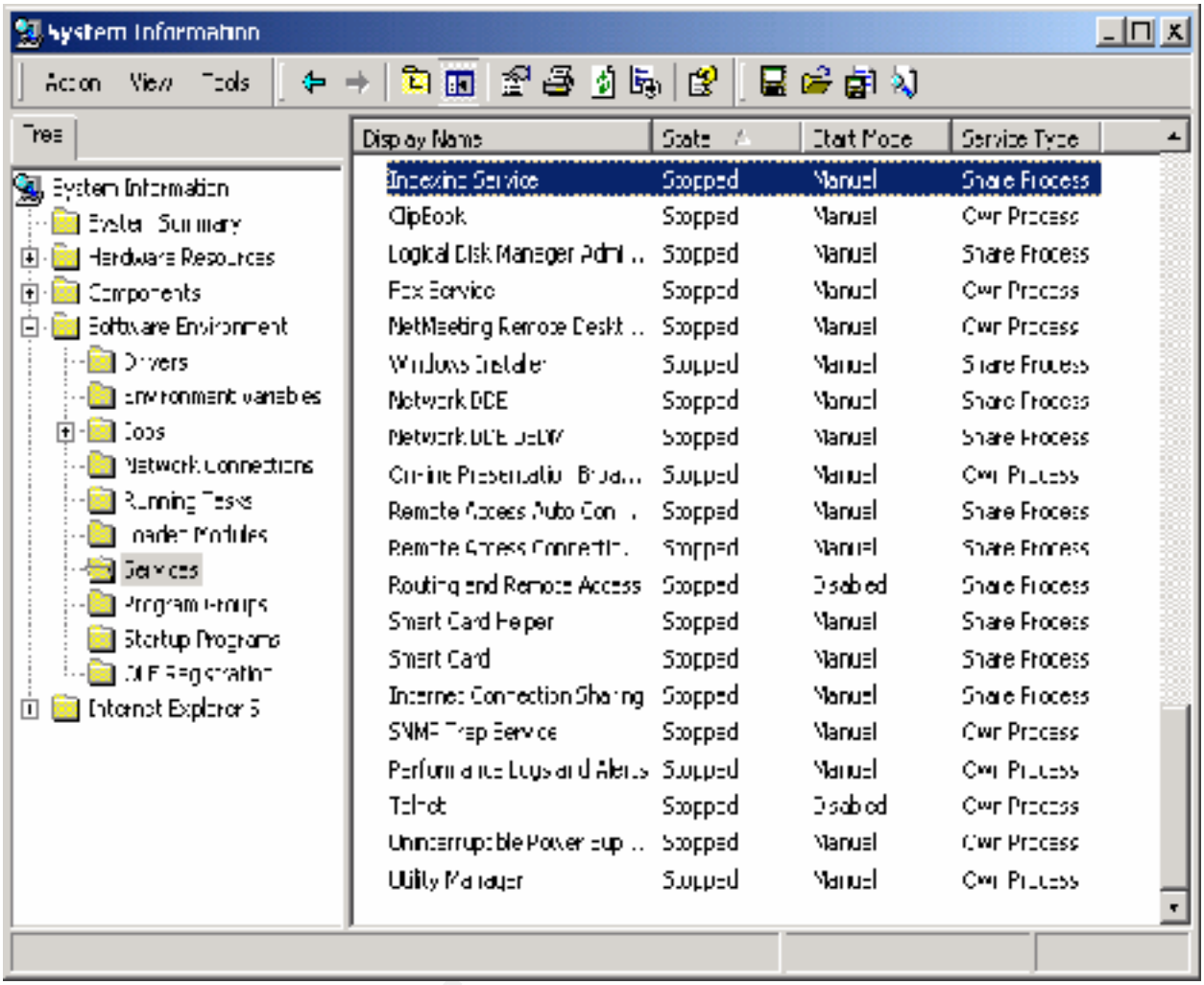
It is important to see if we can access the machine via null session. From the gunsmith's laptop command line

```
net use \\targetserver\ipc$ "" /user:""
```

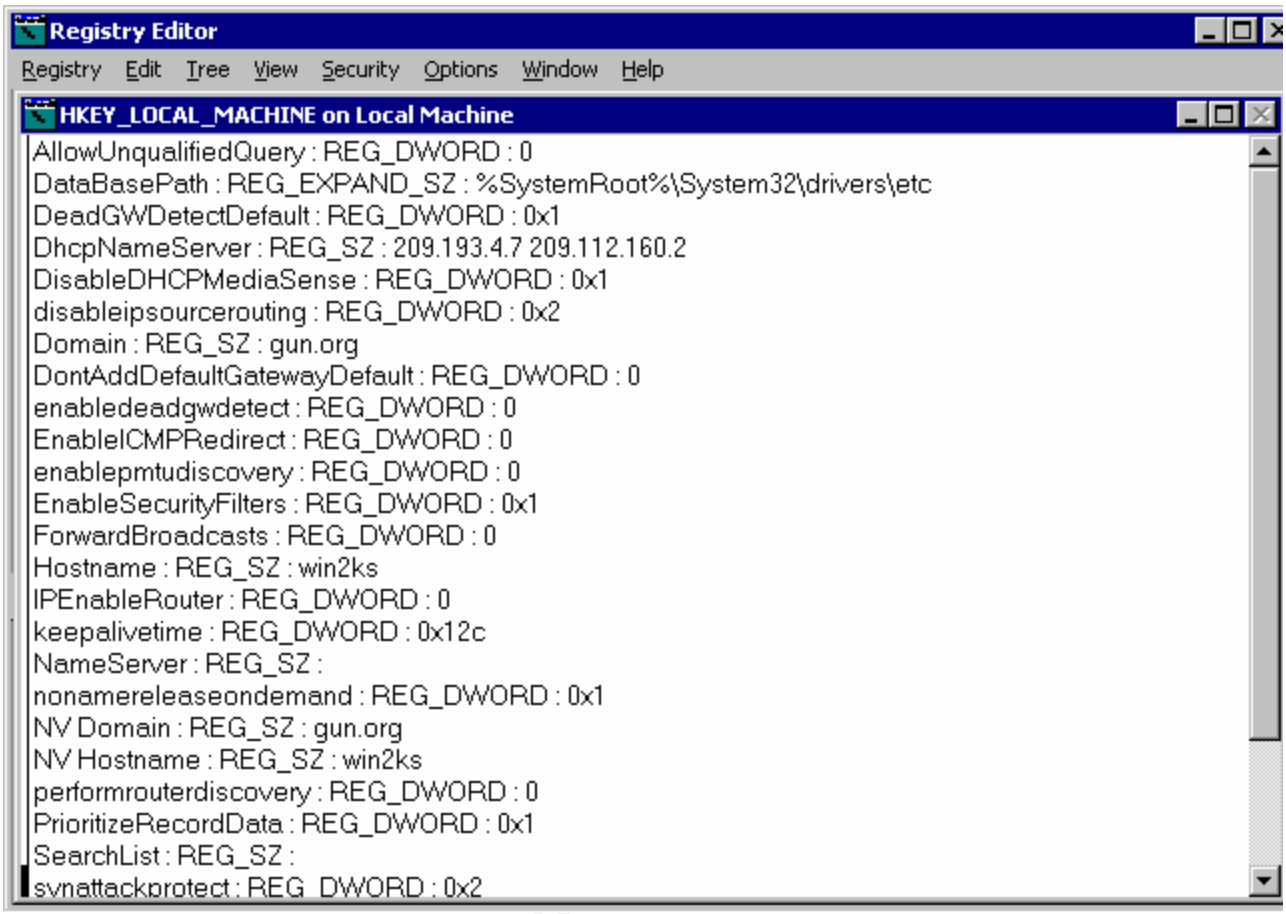
Access denied is what we want to see.

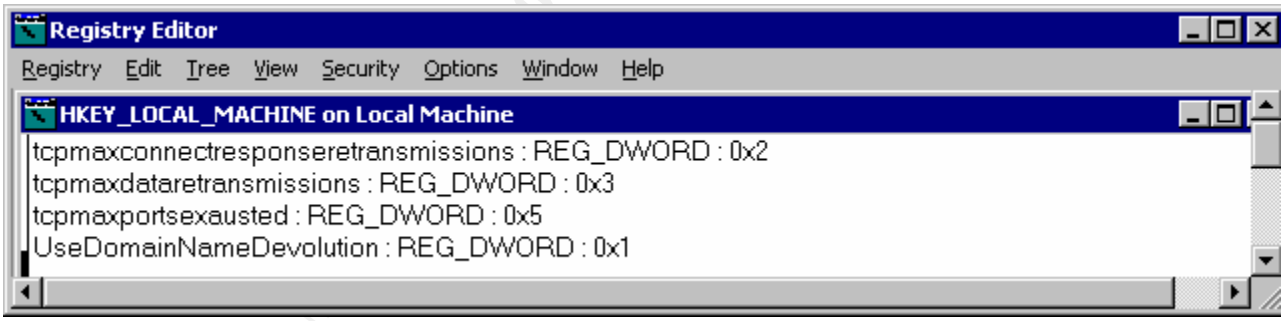
We added the test user to the DomainAdmins group and verified the setting was accepted. Then waited for a GPO refresh, and checked the group's members again. The test account was still a member. Then a wait of 90 minutes, still no joy. The test account was removed and the event viewer run to see if there was an entry showing the problem. As this is not working as expected the service provider will research and test again at a future weekly visit.

To check services running the command line utility *winmsd* was run. While this utility was used to check for services running (System Information -> Software Environment -> Services), it is a good time to check each of the components for consistency. We are interested in determining if the problem services we turned off in the template are in the stopped state. Indeed they were.



One of the items we will check is the tcpip parameter changes we added by editing the template which is more prone to error than the incremental adding of supplied templates most of the settings come from. Running the registry editor after the reboot shows the parameters have been set as desired:

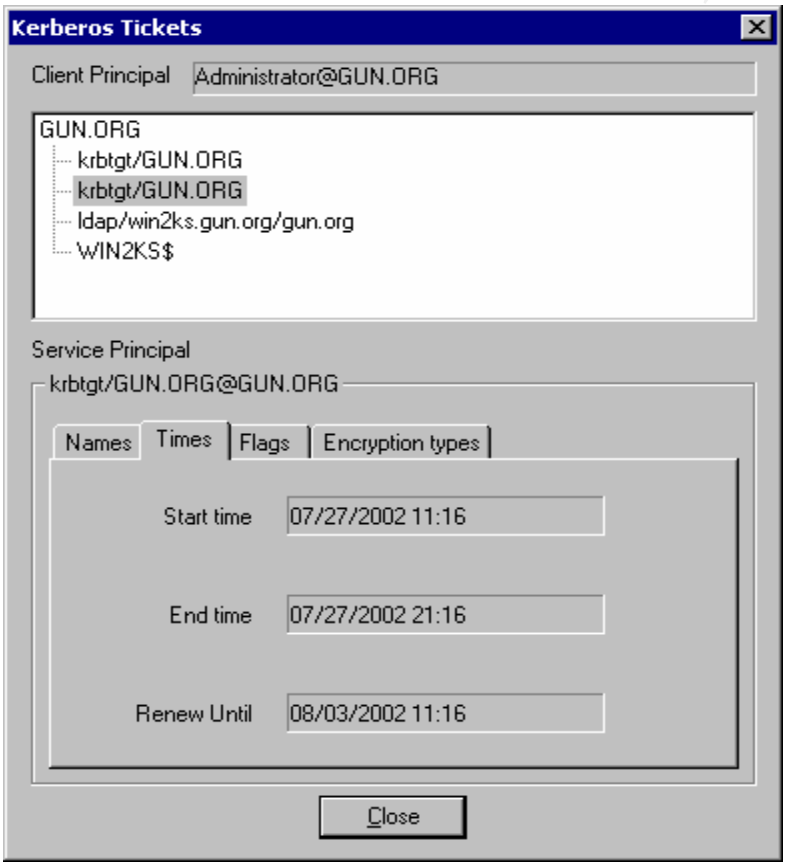




Of the settings we changed, the easiest one to test would be the source routing deny. To test the laptop runs tracert with the –j <host list> host option. We run this both ways with the LinkSys router as the specified route. Recall the laptop has not had this specific template applied so does not have the registry entry for disablesourcerouting set to 2. In the case of the main system using source routing to the laptop, the tracert succeeds. In the case of running from the laptop to the domain controller, the normal tracert succeeds while the source-routed tracert fails with a timeout, which is consistent with the dropping of the ICMP packets. A search of the security, system, and application logs did not show the event of this packet drop nor did any of the files in the debug folder.

```
E:\>tracert -j 192.168.1.xxx 192.168.1.yyy

Tracing route to win2ks.gun.org [192.168.1.yyy]
over a maximum of 30 hops:

  1    *        *        *     Request timed out.
  2    *        *        *     Request timed out.
  3    *        *        *     Request timed out.
  4    *     ^C
E:\>tracert 192.168.1.yyy

Tracing route to win2ks.gun.org [192.168.1.yyy]
over a maximum of 30 hops:

  1   <10 ms   <10 ms   <10 ms  win2ks.gun.org [192.168.1.yyy]

Trace complete.
```

Another item to check is the Kerberos settings, specifically the ticket granting ticket and maximum lifetime for a ticket. Recall we asked for 10 hours and 7 days as the values to be changed to by the template

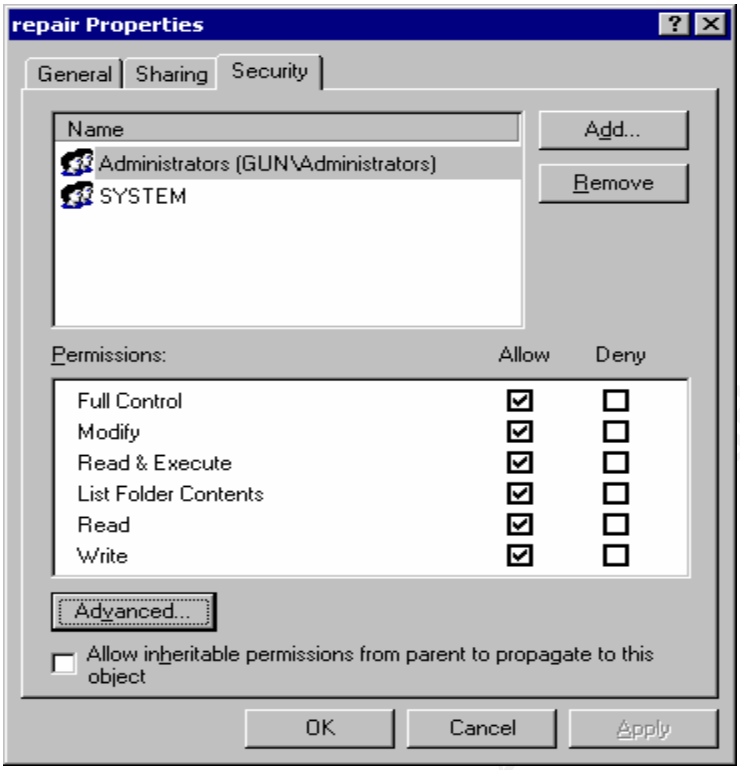


and so they are.

The incremental NSA template changed the file security on the repair directory

1f="e:\winnt\repair", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"

to permit full file access by administrator and system only. This due to the sensitivity of the files stored there by the recovery utility. Checking those permissions:



shows the settings are as desired.

Test the System's Functionality

Using the test account all the system functions appear to work. The account can open Word documents, create and save spreadsheets, and browse folders consistent with the account and group memberships. Some testing in the shop's application portfolio also caused no problems. This testing shows basic system functionality sufficient to have the shop's employees able to test without encountering a basic configuration error.

Now the respective owner accounts need to create and save word documents and excel spreadsheets. Each of the accounts needs to verify they can read documents and data created by the other accounts consistent with file permissions, ACLs, and security settings. Though not a strict requirement of the system or template, the ability to restrict access to files from other accounts needs to be tested as well. This is best accomplished with a checklist such that each of the employees is given a set of tasks to accomplish in two categories:

Something to check. e.g., can each read a file or folder where they have been granted implicit permissions like group *owner* read access or is their access denied to a file where another account has set deny on an ACL.

Something to do. e.g. creating a new document for attempted access by the other accounts or setting permissions on a file to prevent access.

This checklist and series of tasks prevents the drudgery of the users having to login, perform a task, logout and have another user check that task then repeating again and again for each test.

Once the basics of the system are tested the application, system, and security logs are checked for any problem. Then the debug folder files are checked.

As this all went well with no problems, the application suite was tested. This testing followed a similar script or checklist. Now instead of creating a document, saving, and attempting access from another account, a data item was created or changed and the other accounts verified they could see that change or addition. Data items on the EFS folder had their function of denying the gun smith tested with the test account to prevent hurt feelings of the gunsmith. For one of the applications this testing caused some problems. The local test account caused a consistent application shutdown when attempting to gain access to data items in the EFS folder. The logs indicate this is an application problem and not a system problem caused by the template.

Another problem that was found in system testing involved the C: drive and the XP Home system it contained as shipped from the hardware vendor. It would no longer boot. The error message:

WINDOWS 2000 could not start because the following file is missing or corrupt:

\WINDOWS\SYSTEM32\CONFIG\SYSTEM

In general the practice is to install the older version of Windows first, Windows 2000 Server in this case. No specific reason is given since each combination will probably be different. In the specific case of Windows 2000 Server and Windows XP the problem is usually solved by a reload of NTLDR.EXE in the XP boot file. In this case it appears to be the XP systems registry hive. The owners indicate this has happened to them before when attempting to add Windows 2000 to the existing XP system. Their attempts to repair caused the Windows 2000 system to not boot as well.

While the intent was to leave the XP capability via dual boot, the owners were not anxious to have the XP capability returned. They did want to leave the C: drive as is for now. This to preserve the files containing the XP licensing information and the potential to repair the ability to boot XP. Windows XP lost some of its desirability when it was decided to run the system as a domain controller as XP Server is not yet available. As noted before the system might be low on available space soon and the decision to reclaim the space on the C: drive holding the XP system files will be made at that time.

Acceptance testing is very subjective. The provider is anxious to get their check and get on to other work, the system is bound to function – it's the 100th one they have done just like this one. The customer is anxious to write the check, get the provider away from the machine so they can start using and gaining experience with their new machine. Other systems like VAX/VMS have built in system exercisers. Tell the exerciser how many users it is supposed to simulate, the duration of the tests, and it would go and provide a "normal" user load on the machine for the requested number of users. Afterwards the logs of the system exerciser would show any problems. A search was made for similar functionality for Windows 2000 with no success. The resource kit also did not have a similar function that could be found. The reason for this lack of a tool is probably due to the nature of computing as changed from VAX/VMS and current systems like Windows 2000. The tool for VMS and similar is a long list of operating system commands on a command line. While Windows has command line equivalents for most of its administration commands, not so the user commands. It is called Windows for a reason. A tool can be made to emulate a user at the machine with Windows, Icon, Menu, Pointing device (WIMP), just not easily made. Almost all "System Exercisers" are hardware or hardware component exercisers.

We will rerun the tools that verified the system after domain controller and Active Directory population (dcdiag and netdiag) and a bit of system testing has been done with the testing of the template. The test user was used to open and save word documents, excel spreadsheets, WordPad, IE access to web pages in favorites. Then the owners tested the applications the shop will use for normal running of the business and few problems found. BUT as anyone who has been in the computer game for awhile knows, no amount of testing will find all problems.

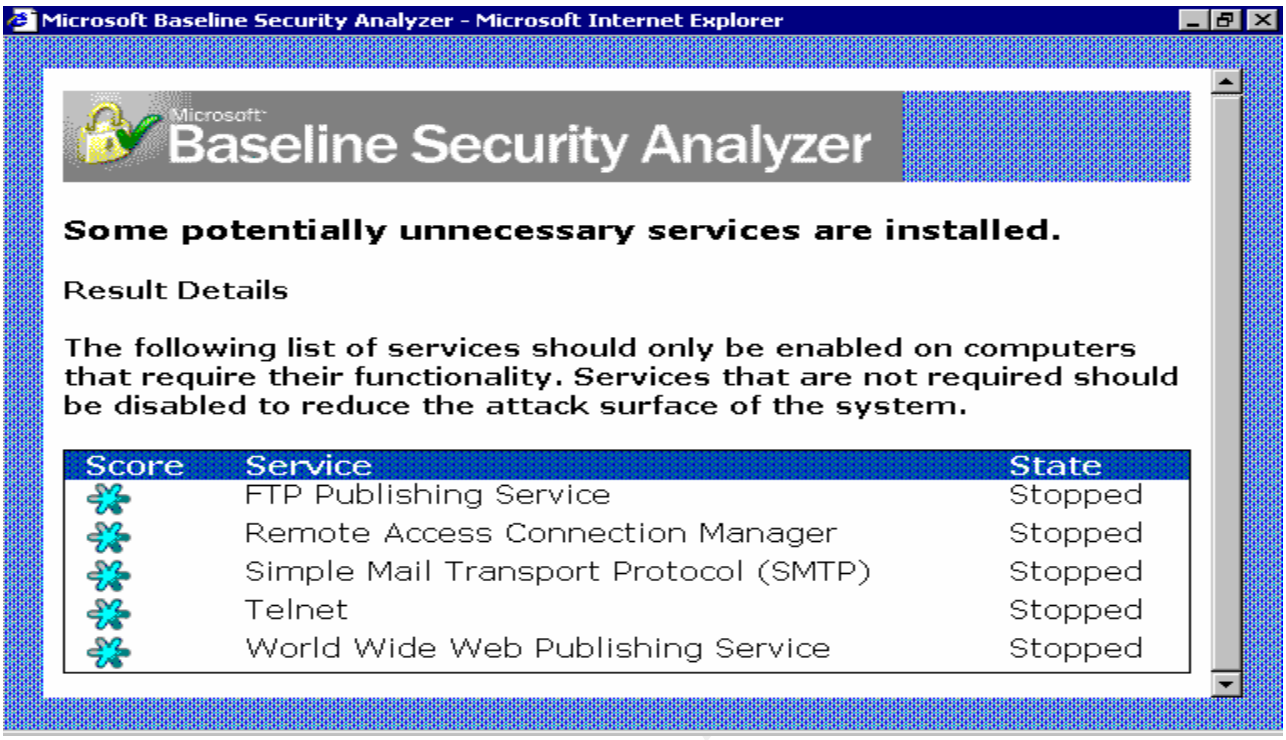
Attempts to run the ISS scanner from the resource kit all failed. Even if it was successfully run the implications would be suspect due to the old version on the resource kit.

So, what more can be done to test the system?

A run of Microsoft's hfnefchk showed some items to investigate

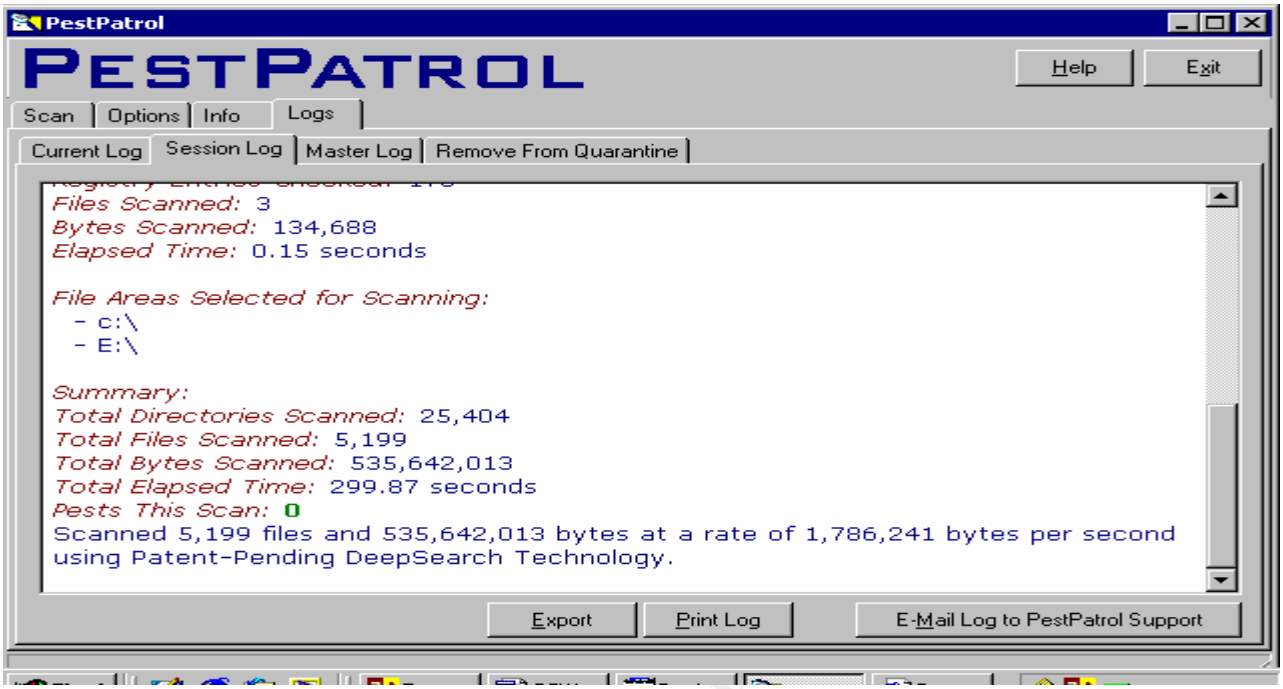
```
* WINDOWS 2000 SERVER SP2

Note          MS01-022      Q296441

Warning       MS02-001      Q311401

Patch NOT Found MS02-016    Q318593

* INTERNET EXPLORER 5.5 SP2

Note          MS02-027      Q323889
```

The follow on to hfnetchk is Microsoft Baseline Security Analyser. That was run as well and it did show some items to note. The scan showed the disabled services as stopped.



The Baseline Security Analyser found some hotfixes to investigate; users *administrator, guest* and *apsnet* with non-expiring passwords; autologin not enabled; all drives with NTFS; restrict anonymous set; no more than two administrators; auditing enabled; SQL Server not found; and the IIS lockdown tool not yet run. The Analyser also found the C: drive shared. As seen in the document thus far the system is on the E: drive. Recall the C: drive is used to store files that are burned to CD-ROM as part of backup and disaster recovery. There is no need for this share so it was removed.

PestPatrol scan showed no problems.



Evaluate the Template

The security templates, Security Configuration and Analysis GUI, Group Policy Objects, domains, Active Directory, and the other aspects of Windows 2000 make it a lot easier to configure, maintain, and document security. If we were to add a major component to the system in future like IIS, there are incremental IIS security templates. The process would be to take the current settings as a result of gunhighsecdc template, apply an IIS security template as an incremental template, analyse the settings that would be changed by the IIS template, apply those changes to the computer, test, and document. Be sure to read the comments in the templates. A note in the highsecdc template we used has a comment about assuming the system was a clean install on NTFS.

Our job in configuring the system for the customer was easy once we got out of our previous mindset of editing the templates for optimal settings instead of letting the system do that work for us. We feel, and the customer agrees, that our choices of settings controlled by security templates have been good and have configured a more secure system and domain.

A feature of templates we could not find was how to remove a registry entry and have GPO enforce that removal. As example we would like to remove and have the GPO keep removed features like OS/2 and POSIX support. None of the systems applications need these features. To remove the features involves removing the registry setting and the supporting files and folders. The ability to set registry settings is demonstrated, but not the

ability to remove those entries and have GPOs keep them removed. An alternative method is to define the keys to run an executable that would send an alert to the security log.

Note that neither the Microsoft nor NSA templates had any settings for the System Services. All that section came from our settings. I can understand the lack of such settings in the Microsoft template, but not the NSA. I would hope to see at least ClipBook disabled.

Security templates do not now configure items like Public Key Infrastructure (PKI) or IP Security (IPSec).

We also need to check more than the application, system, and security logs for problems and issues with the security templates. As mentioned before the review of the logs produced by the *Configure Computer Now…* and *Analyse Computer Now…* need to be checked. These logs are available in the GUI but also in %systemroot%\security\logs. Another source of logging to check after configuring the system via security templates is the %systemroot%\Debug folder and the logs therein.

Securing the system also implies securing the applications. Setting security zones in IE, disabling macro expansions in Word, ZoneAlarm settings, … almost every setting is a registry entry. As seen registry entries not in supplied templates can be set via templates and GPOs. In theory such items could be set via templates. Would that not be better than setting those settings via the applications which then set the registry? Probably not for several reasons. The application can be replaced by a patched, new version, or replacement application. Two separate groups or at least two mindsets usually tend to the security template and the applications, so the association of an application problem and a security template setting of a registry value might not be apparent. If the settings were imposed by a GPO it would be difficult to associate the change that got the application functioning properly a few seconds ago has reverted to the old behaviour due to GPO refresh. As seen the security templates do help in securing systems, but securing applications is probably best done with the application itself or via system utilities as directed by the application documentation.

As seen above a scan of the system after the configuration with templates showed the C: drive to be shared. It was unshared after this discovery, but that setting will be considered as an addition to the security template built for this system. This will be the life of the template from now on. New vulnerabilities, new system requirements, overlooked settings, etc. will mean the template is a living document.

From the resulting template listed in Appendix B, it can be seen a lot has been added and changed from the starting Microsoft highsecdc and the incrementally added NSA W2KDC template. This is the power of security templates in Windows 2000, choose the best template to start the process, but do not let the process end there. Add incremental templates to suit additions to the system like IIS, and add settings to best suit the changing requirements of the system, site, OU, and domain.

References

1. Institute for Security Technology Studies, Dartmouth College, "Comprehensive Review of Windows 2000 Security Policy Templates and Security Configuration Tool", David B. Koconis, March, 2001 http://www.ists.dartmouth.edu/IRIA/knowledge_base/sectemplates/sectemplates_full.htm

2. Microsoft TechNet, "Security Operations Guide for Windows 2000 Server" http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/windows/windows2000/staysecure/Default.asp

3. New Scientist News Service, "Microsoft's anti-piracy plans spark controversy" http://www.newscientist.com/news/news.jsp?id=ns99992483

4. LabMice.net, " Windows 2000 Security Checklist" http://www.labmice.net/articles/securingwin2000.htm

5. SANS Institute, "Security Configuration Tool and Template Settings. Usefulness and Shortcomings of the Preconfigured Security Policy Templates that are Included with Windows 2000", Robert Hule, December, 2000 http://rr.sans.org/win/settings.php

6. Minasi, Mark, Mastering Windows 2000 Server, Sybex, 2000

7. Microsoft MSDN Library, "Security Descriptor String Format"

http://msdn.microsoft.com/library/default.asp?url=/library/enus/security/Security/security_descriptor_string_format.asp

8. Microsoft MSDN Library, "Windows 2000/Windows NT Access Mask Format"

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/security/security/windows_2000_windows_nt_access_mask_format.asp

Appendix A Installation History

Successful Monday, July 29, 2002 **Root Certificates Update**
Read more... Web site
Successful Monday, July 29, 2002 **Security Update, February 13, 2002 (MSXML 3.0)**
Read more... Web site
Successful Monday, July 29, 2002 **Q320920: Security Update (Windows Media Player 7.1)**
Read more... Web site
Successful Friday, July 26, 2002 **Q320920: Security Update (Windows Media Player 7.1)**
Read more... Automatic update
Successful Saturday, July 13, 2002 **Q318138: Security Update**
Read more... Automatic update
Successful Sunday, July 07, 2002 **Microsoft .NET Framework Service Pack 1 (English)**
Read more... Automatic update
Successful Saturday, July 06, 2002 **Microsoft .NET Framework**
Read more... Web site
Successful Saturday, July 06, 2002 **DirectX 8.1**
Read more... Web site
Successful Saturday, July 06, 2002 **Q320920: Security Update (Windows Media Player 7.1)**
Read more... Automatic update
Successful Saturday, June 29, 2002 **Windows Media Player 7.1**
Read more... Web site
Successful Saturday, June 29, 2002 **Windows 2000 Compatibility Updates**
Read more... Web site
Successful Saturday, June 29, 2002 **Root Certificates Update**
Read more... Web site
Successful Saturday, June 29, 2002 **COM+ Rollup Package 18.1**
Read more... Web site
Successful Saturday, June 29, 2002 **Euro Conversion Tool**
Read more... Web site
Successful Saturday, June 29, 2002 **Q282010: Microsoft Jet 4.0 Service Pack 6 (Windows 2000)**
Read more... Web site
Successful Saturday, June 29, 2002 **Security Update, February 12, 2002**
Read more... Web site
Successful Saturday, June 29, 2002 **Security Update, February 14, 2002 (Internet Explorer 5.5)**
Read more... Web site
Successful Saturday, June 29, 2002 **Security Update, February 22, 2002**
Read more... Web site

Successful Saturday, June 29, 2002 **Security Update, March 4, 2002**
Read more... Web site
Successful Saturday, June 29, 2002 **Security Update, March 7, 2002**
Read more... Web site
Successful Saturday, June 29, 2002 **Security Update, November 20, 2001**
Read more... Web site
Successful Saturday, June 29, 2002 **Q311967: Security Update**
Read more... Web site
Successful Saturday, June 29, 2002 **Q319733: Internet Information Services Security Roll-up Package**
Read more... Web site
Successful Saturday, June 29, 2002 **Q320206: Security Update**
Read more... Web site
Successful Saturday, June 29, 2002 **Windows Automatic Updating, June 2002**
Read more... Web site
Successful Saturday, June 29, 2002 **Q321599: Security Update**
Read more... Web site
Successful Saturday, June 29, 2002 **Q320920: Security Update (Windows Media Player 6.4)**
Read more... Web site
Successful Saturday, June 29, 2002 **Q321232: Security Update (Internet Explorer 5.5 Service Pack 2)**
Read more... Web site
Successful Saturday, June 29, 2002 **Internet Explorer 5.5 Service Pack 2 and Internet Tools**
Read more... Web site

Appendix B gunhighsecdc.inf

gunhighsecdc security template

```
[Unicode]
Unicode=yes
[Version]
signature="$CHICAGO$"
Revision=1
[System Access]
MinimumPasswordAge = 2
MaximumPasswordAge = 42
MinimumPasswordLength = 12
PasswordComplexity = 1
PasswordHistorySize = 24
LockoutBadCount = 5
ResetLockoutCount = 30
LockoutDuration = 30
RequireLogonToChangePassword = 0
ClearTextPassword = 0
[System Log]
MaximumLogSize = 4194240
AuditLogRetentionPeriod = 2
RetentionDays = 7
RestrictGuestAccess = 1
[Security Log]
MaximumLogSize = 4194240
AuditLogRetentionPeriod = 2
RetentionDays = 7
RestrictGuestAccess = 1
[Application Log]
MaximumLogSize = 4194240
AuditLogRetentionPeriod = 2
RetentionDays = 7
RestrictGuestAccess = 1
[Event Audit]
AuditSystemEvents = 3
AuditLogonEvents = 3
AuditObjectAccess = 2
AuditPrivilegeUse = 2
AuditPolicyChange = 3
AuditAccountManage = 3
AuditProcessTracking = 0
AuditDSAccess = 2
AuditAccountLogon = 3
CrashOnAuditFull = 1
[Kerberos Policy]
MaxTicketAge = 7
MaxRenewAge = 10
MaxServiceAge = 60
MaxClockSkew = 5
TicketValidateClient = 1
[Profile Description]
Description=Assumes clean-install NTFS file\reg ACLs. Includes SecureDC settings with Windows 2000-only enhancements.
Empties Power Users group. NSA Enhanced Security for Windows 2000 Domain Controllers
[Registry Values]
machine\system\currentcontrolset\services\netlogon\parameters\signsecurechannel=4,1
machine\system\currentcontrolset\services\netlogon\parameters\sealsecurechannel=4,1
machine\system\currentcontrolset\services\netlogon\parameters\requirestrongkey=4,0
machine\system\currentcontrolset\services\netlogon\parameters\requiresignorseal=4,0
machine\system\currentcontrolset\services\netlogon\parameters\disablepasswordchange=4,0
machine\system\currentcontrolset\services\lanmanworkstation\parameters\requiresecuritysignature=4,0
machine\system\currentcontrolset\services\lanmanworkstation\parameters\enablesecuritysignature=4,1
machine\system\currentcontrolset\services\lanmanworkstation\parameters\enableplaintextpassword=4,0
machine\system\currentcontrolset\services\lanmanserver\parameters\requiresecuritysignature=4,0
machine\system\currentcontrolset\services\lanmanserver\parameters\enablesecuritysignature=4,1
machine\system\currentcontrolset\services\lanmanserver\parameters\enableforcedlogoff=4,0
```

machine\system\currentcontrolset\services\lanmanserver\parameters\autodisconnect=4,30
machine\system\currentcontrolset\services\tcpip\parameters\DisableIPSourceRouting=4,2
machine\system\currentcontrolset\services\tcpip\parameters\EnableICMPRedirect=4,0
machine\system\currentcontrolset\services\tcpip\parameters\EnableSecurityFilters=4,1
machine\system\currentcontrolset\services\tcpip\parameters\SynAttackProtect=4,2
machine\system\currentcontrolset\services\tcpip\parameters\EnableDeadGWDetect=4,0
machine\system\currentcontrolset\services\tcpip\parameters\EnablePMTUDiscovery=4,0
machine\system\currentcontrolset\services\tcpip\parameters\KeepAliveTime=4,300,000
machine\system\currentcontrolset\services\tcpip\parameters\TcpMaxConnectResponseRetransmissions=4,2
machine\system\currentcontrolset\services\tcpip\parameters\TcpMaxDataRetransmissions=4,3
machine\system\currentcontrolset\services\tcpip\parameters\NoNameReleaseOnDemand=4,1
machine\system\currentcontrolset\services\tcpip\parameters\PerformRouterDiscovery=4,0
machine\system\currentcontrolset\services\tcpip\parameters\TcpMaxPortsExausted=4,5
machine\system\currentcontrolset\control\session manager\protectionmode=4,1
machine\system\currentcontrolset\control\session manager\memory management\clearpagefileatshutdown=4,1
machine\system\currentcontrolset\control\print\providers\lanman print services\servers\addprinterdrivers=4,1
machine\system\currentcontrolset\control\filesystem\ntfsdisable8dot3namecreation=4,1
machine\system\currentcontrolset\control\lsa\submitcontrol=4,0
machine\system\currentcontrolset\control\lsa\restrictanonymous=4,2
machine\system\currentcontrolset\control\lsa\lmcompatibilitylevel=4,5
machine\system\currentcontrolset\control\lsa\fullprivilegeauditing=3,1
machine\system\currentcontrolset\control\lsa\crashonauditfail=4,1
machine\system\currentcontrolset\control\lsa\auditbaseobjects=4,1
machine\software\microsoft\windows\currentversion\policies\system\shutdownwithoutlogon=4,0
machine\software\microsoft\windows\currentversion\policies\system\legalnoticetext=1,Authorized use only. Activity may be monitored
machine\software\microsoft\windows\currentversion\policies\system\legalnoticecaption=1,
machine\software\microsoft\windows\currentversion\policies\system\dontdisplaylastusername=4,1
machine\software\microsoft\windows\currentversion\policies\system\disablecad=4,1
machine\software\microsoft\windows\currentversion\policies\explorer\nodrivetypeautorun=4,255
machine\software\microsoft\windows nt\currentversion\winlogon\scremoveoption=1,1
machine\software\microsoft\windows nt\currentversion\winlogon\passwordexpirywarning=4,14
machine\software\microsoft\windows nt\currentversion\winlogon\cachedlogonscount=1,0
machine\software\microsoft\windows nt\currentversion\winlogon\autoadminlogon=4,0
machine\software\microsoft\windows nt\currentversion\winlogon\allocatefloppies=1,1
machine\software\microsoft\windows nt\currentversion\winlogon\allocatedasd=1,0
machine\software\microsoft\windows nt\currentversion\winlogon\allocatecdroms=1,1
machine\software\microsoft\windows nt\currentversion\setup\recoveryconsole\setcommand=4,0
machine\software\microsoft\windows nt\currentversion\setup\recoveryconsole\securitylevel=4,0
machine\software\microsoft\non-driver signing\policy=3,1
machine\software\microsoft\driver signing\policy=3,1
[Group Membership]
*S-1-5-21-1343024091-1563985344-1060284298-1123__Memberof =
*S-1-5-21-1343024091-1563985344-1060284298-1123__Members = *S-1-5-21-1343024091-1563985344-1060284298-1120,*S-1-5-21-1343024091-1563985344-1060284298-1119
*S-1-5-21-1343024091-1563985344-1060284298-1124__Memberof =
*S-1-5-21-1343024091-1563985344-1060284298-1124__Members = *S-1-5-21-1343024091-1563985344-1060284298-1120,*S-1-5-21-1343024091-1563985344-1060284298-1119,*S-1-5-21-1343024091-1563985344-1060284298-1128,*S-1-5-21-1343024091-1563985344-1060284298-1121
*S-1-5-21-1343024091-1563985344-1060284298-516__Memberof =
*S-1-5-21-1343024091-1563985344-1060284298-516__Members =
*S-1-5-32-544__Memberof =
*S-1-5-32-544__Members =
*S-1-5-32-545__Memberof =
*S-1-5-32-545__Members =
*S-1-5-32-546__Memberof =
*S-1-5-32-546__Members =
*S-1-5-32-548__Memberof =
*S-1-5-32-548__Members =
*S-1-5-32-549__Memberof =
*S-1-5-32-549__Members =
*S-1-5-32-550__Memberof =
*S-1-5-32-550__Members =
*S-1-5-32-551__Memberof =
*S-1-5-32-551__Members =
*S-1-5-32-552__Memberof =
*S-1-5-32-552__Members =
[Privilege Rights]
seassignprimarytokenprivilege =
seauditprivilege =

```
sebackupprivilege = *S-1-5-32-544
sebatchlogonright =
sechangenotifyprivilege = *S-1-5-32-544
secreatepagefileprivilege = *S-1-5-32-544
secreatepermanentprivilege =
secreatetokenprivilege =
sedebugprivilege =
sedenybatchlogonright =
sedenyinteractivelogonright =
sedenynetworklogonright =
sedenyservicelogonright =
seenabledelegationprivilege = *S-1-5-32-544
seincreasebasepriorityprivilege = *S-1-5-32-544
seincreasequotaprivilege = *S-1-5-32-544
seinteractivelogonright = *S-1-5-32-544
seloaddriverprivilege = *S-1-5-32-544
selockmemoryprivilege =
semachineaccountprivilege = *S-1-5-32-544
senetworklogonright = *S-1-5-9,*S-1-5-11,*S-1-5-32-544
seprofilesingleprocessprivilege = *S-1-5-32-544
seremoteshutdownprivilege = *S-1-5-32-544
serestoreprivilege = *S-1-5-32-544
sesecurityprivilege = *S-1-5-32-544
seservicelogonright =
seshutdownprivilege = *S-1-5-32-544
sesyncagentprivilege =
sesystemenvironmentprivilege = *S-1-5-32-544
sesystemprofileprivilege = *S-1-5-32-544
sesystemtimeprivilege = *S-1-5-32-544
setakeownershipprivilege = *S-1-5-32-544
setcbprivilege =
seundockprivilege =
[Registry Keys]
1="classes_root", 2, "D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
2="machine\software", 2, "D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
3="machine\software\microsoft\netdde", 2, "D:PAR(A;CI;KA;;;BA)(A;CI;KA;;;SY)"
4="machine\software\microsoft\os/2 subsystem for nt", 2, "D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
5="machine\software\microsoft\protected storage system provider", 1, "D:AR"
6="machine\software\microsoft\windows nt\currentversion\asrcommands", 2,
"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CI;CCDCLCSWRPSDRC;;;BO)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
7="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)"
8="machine\software\microsoft\windows\currentversion\group policy", 0, "D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CI;KA;;;SY)"
9="machine\software\microsoft\windows\currentversion\installer", 0, "D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CI;KA;;;SY)"
a="machine\software\microsoft\windows\currentversion\policies", 0, "D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CI;KA;;;SY)"
b="machine\system", 2, "D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
c="machine\system\clone", 1, "D:AR"
d="machine\system\controlset001", 0, "D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
e="machine\system\controlset002", 0, "D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
f="machine\system\controlset003", 0, "D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
10="machine\system\controlset004", 0, "D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
11="machine\system\controlset005", 0, "D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
12="machine\system\controlset006", 0, "D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
13="machine\system\controlset007", 0, "D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
14="machine\system\controlset008", 0, "D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
15="machine\system\controlset009", 0, "D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
16="machine\system\controlset010", 0, "D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
17="machine\system\currentcontrolset\control\securepipeservers\winreg", 2, "D:PAR(A;CI;KA;;;BA)(A;;KR;;;BO)(A;CI;KA;;;SY)"
18="machine\system\currentcontrolset\control\wmi\security", 2, "D:P(A;CI;GR;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
19="machine\system\currentcontrolset\enum", 1, "D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CI;KA;;;SY)"
1a="machine\system\currentcontrolset\hardware profiles", 0, "D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
1b="machine\system\currentcontrolset\services\snmp\parameters\permittedmanagers", 2,
"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
1c="machine\system\currentcontrolset\services\snmp\parameters\validcommunities", 2,
"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
1d="users\.default", 2, "D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
1e="users\.default\software\microsoft\netdde", 2, "D:PAR(A;CI;KA;;;BA)(A;CI;KA;;;SY)"
1f="users\.default\software\microsoft\protected storage system provider", 1, "D:AR"
[File Security]
1="e:\", 0, "D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
```

2="e:\autoexec.bat", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
3="e:\boot.ini", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
4="e:\config.sys", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
5="e:\documents and settings", 0, "D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICI;FA;;;SY)"
6="e:\documents and settings\administrator", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
7="e:\documents and settings\all users", 0, "D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICI;FA;;;SY)"
8="e:\documents and settings\all users\documents\drwatson", 2,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICIIO;DCLCWP;;;AU)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
9="e:\documents and settings\all users\documents\drwatson\drwtsn32.log", 2,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1301bf;;;AU)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
a="e:\documents and settings\default user", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICI;FA;;;SY)"
b="e:\inetpub", 1, "D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
c="e:\io.sys", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICI;FA;;;SY)"
d="e:\msdos.sys", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICI;FA;;;SY)"
e="e:\my download files", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1201bf;;;AU)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
f="e:\ntbootdd.sys", 2, "D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
10="e:\ntdetect.com", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
11="e:\ntldr", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
12="e:\program files", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
13="e:\program files\resource kit", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
14="e:\system volume information", 1, "D:PAR"
15="e:\temp", 2, "D:PAR(A;OICI;FA;;;BA)(A;CI;DCLCWP;;;AU)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
16="e:\winnt", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
17="e:\winnt\$ntservicepackuninstall$", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
18="e:\winnt\csc", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
19="e:\winnt\debug", 0, "D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
1a="e:\winnt\debug\usermode", 0, "D:PAR(A;OICI;FA;;;BA)(A;;CCDCWP;;;AU)(A;OIIO;DCLC;;;AU)(A;OICI;FA;;;SY)"
1b="e:\winnt\ntds", 0, "D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
1c="e:\winnt\offline web pages", 1, "D:AR(A;OICI;FA;;;WD)"
1d="e:\winnt\regedit.exe", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
1e="e:\winnt\registration", 0, "D:PAR(A;OICI;FA;;;BA)(A;OICI;FR;;;AU)(A;OICI;FA;;;SY)"
1f="e:\winnt\repair", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
20="e:\winnt\security", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
21="e:\winnt\system32", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
22="e:\winnt\system32\appmgmt", 0, "D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICI;FA;;;SY)"
23=":\winnt\system32\config", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
24="e:\winnt\system32\dllcache", 2, "D:P(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
25="e:\winnt\system32\dtclog", 0, "D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
26="e:\winnt\system32\grouppolicy", 0, "D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICI;FA;;;SY)"
27="e:\winnt\system32\ias", 2, "D:P(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
28="e:\winnt\system32\ntbackup.exe", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
29="e:\winnt\system32\ntmsdata", 0, "D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
2a="e:\winnt\system32\rcp.exe", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
2b="e:\winnt\system32\regedt32.exe", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
2c="e:\winnt\system32\reinstallbackups", 1,
"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
2d="e:\winnt\system32\repl", 0, "D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICI;FA;;;SY)"
2e="e:\winnt\system32\repl\export", 0, "D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICI;0x1200a9;;;RE)(A;OICI;FA;;;SY)"
2f="e:\winnt\system32\repl\import", 0, "D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICI;0x1301bf;;;RE)(A;OICI;FA;;;SY)"
30="e:\winnt\system32\rexec.exe", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
31="e:\winnt\system32\rsh.exe", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
32="e:\winnt\system32\secedit.exe", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
33="e:\winnt\system32\setup", 0, "D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICI;FA;;;SY)"
34="e:\winnt\system32\spool\printers", 2, "D:PAR(A;OICI;FA;;;BA)(A;CI;DCLCSWWPLO;;;AU)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
35="e:\winnt\sysvol", 0, "D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
36="e:\winnt\sysvol\domain\policies", 0,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICIIO;FA;;;CO)(A;OICI;0x1301bf;;;PA)(A;OICI;FA;;;SY)"
37="e:\winnt\tasks", 1, "D:AR"
38="e:\winnt\temp", 2, "D:PAR(A;OICI;FA;;;BA)(A;CI;DCLCWP;;;AU)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
[Service General Setting]
1="alerter", 2,
"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCS
WRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;
WD)"
2="appmgmt", 3,
"D:(A;OICI;CCLCSWLORC;;;WD)(A;OICI;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;OICI;CCLCSWLORC;;;PU)(A;OICI;CC
LCSWRPLO;;;IU)(A;OICI;CCLCSWRPLO;;;BU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
3="clipsrv", 4,
"D:(A;OICI;CCLCSWLORC;;;WD)(A;OICI;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;OICI;CCLCSWLORC;;;PU)(A;OICI;CC
LCSWRPLO;;;IU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

4="dfs", 2,
"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCS
WRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;
WD)"
5="dhcp", 2,
"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCS
WRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;
WD)"
6="dhcpserver", 4,
"D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLC
SWRPWPDTLOCRRC;;;PU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
7="dmadmin", 3,
"D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCD
CLCSWRPWPDTLOCRSDRCWDWO;;;SO)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
8="dmserver", 2,
"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCS
WRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;
WD)"
9="dns", 2,
"D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLC
SWRPWPDTLOCRRC;;;PU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
a="dnscache", 2,
"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCS
WRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;
WD)"
b="eventlog", 2,
"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCS
WRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;
WD)"
c="eventsystem", 3,
"D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLC
SWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPLOCRRC;;;WD)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
d="fax", 4,
"D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLC
SWRPWPDTLOCRRC;;;PU)(A;;LCRP;;;WD)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
e="iisadmin", 4,
"D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLC
SWRPWPDTLOCRRC;;;PU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
f="kdc", 2,
"D:(A;OICI;CCLCSWLORC;;;WD)(A;OICI;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;OICI;CCDCLCSWLORC;;;PU)(A;OICI;
CCLCSWRPLO;;;IU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
10="lanmanserver", 2,
"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCS
WRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;
WD)"
11="lanmanworkstation", 2,
"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCS
WRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;
WD)"
12="lmhosts", 2,
"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCS
WRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;
WD)"
13="macprint", 4,
"D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLC
SWRPWPDTLOCRRC;;;PU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
14="messenger", 2,
"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCS
WRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;
WD)"
15="mnmsrvc", 4,
"D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLC
SWRPWPDTLOCRRC;;;PU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
16="msftpsvc", 4,
"D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLC
SWRPWPDTLOCRRC;;;PU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
17="netlogon", 2,
"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCS
WRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;
WD)"

18="netman", 3,
"D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCD
CLCSWRPWPDTLOCRSDRCWDWO;;;SO)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
19="norton antivirus server", 2,
"D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCD
CLCSWRPWPDTLOCRSDRCWDWO;;;SO)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
1a="nslservice", 4,
"D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLC
SWRPWPDTLOCRRC;;;PU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
1b="ntfrs", 2,
"D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCD
CLCSWRPWPDTLOCRSDRCWDWO;;;SO)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
1c="ntlmssp", 3,
"D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLC
SWRPWPDTLOCRRC;;;PU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
1d="plugplay", 3,
"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCS
WRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;
WD)"
1e="protectedstorage", 2,
"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCS
WRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;
WD)"
1f="remoteregistry", 2,
"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCS
WRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;
WD)"
20="rpclocator", 2,
"D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLC
SWRPWPDTLOCRRC;;;PU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
21="rpcss", 2,
"D:(A;OICI;CCLCSWLORC;;;WD)(A;OICI;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;OICI;CCLCSWLORC;;;PU)(A;OICI;CC
LCSWRPLO;;;IU)(A;OICI;CCLCSWRPLO;;;BU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
22="samss", 2,
"D:(A;OICI;CCLCSWLORC;;;WD)(A;OICI;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;OICI;CCLCSWLORC;;;PU)(A;OICI;CC
LCSWRPLO;;;IU)(A;OICI;CCLCSWRPLO;;;BU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
23="sens", 2,
"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCS
WRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;
WD)"
24="smtpsvc", 4,
"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCS
WRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;
WD)"
25="snmp", 4,
"D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLC
SWRPWPDTLOCRRC;;;PU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
26="snmptrap", 4,
"D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLC
SWRPWPDTLOCRRC;;;PU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
27="sysmonlog", 3,
"D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCD
CLCSWRPWPDTLOCRSDRCWDWO;;;SO)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
28="tlntsvr", 4,
"D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCD
CLCSWRPWPDTLOCRSDRCWDWO;;;SO)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
29="trksvr", 2,
"D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCD
CLCSWRPWPDTLOCRSDRCWDWO;;;SO)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
2a="trkwks", 2,
"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCS
WRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;
WD)"
2b="w32time", 2,
"D:(A;OICI;CCLCSWLORC;;;WD)(A;OICI;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;OICI;CCLCSWLORC;;;PU)(A;OICI;CC
LCSWRPLO;;;IU)(A;OICI;CCLCSWRPLO;;;BU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
2c="w3svc", 2,
"D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLC
SWRPWPDTLOCRRC;;;PU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

2d="winmgmt", 2,
"D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
2e="wins", 4,
"D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
2f="wmi", 3,
"D:(A;OICI;CCLCSWLORC;;;WD)(A;OICI;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;OICI;CCDCLCSWLORC;;;PU)(A;OICI;CCLCSWRPLO;;;IU)(A;OICI;CCLCSWRPLO;;;BU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
30="wuauserv", 2,
"D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

Last Updated: January 22nd, 2019

Upcoming Training

SANS Anaheim 2019	**Anaheim, CA**	**Feb 11, 2019 - Feb 16, 2019**	**Live Event**
SANS Dallas 2019	**Dallas, TX**	**Feb 18, 2019 - Feb 23, 2019**	**Live Event**
SANS 2019 - SEC505: Securing Windows and PowerShell Automation	**Orlando, FL**	**Apr 01, 2019 - Apr 06, 2019**	**vLive**
SANS 2019	**Orlando, FL**	**Apr 01, 2019 - Apr 08, 2019**	**Live Event**
Mentor Session - SEC505	**New York, NY**	**May 08, 2019 - Jun 26, 2019**	**Mentor**
SANS Security West 2019	**San Diego, CA**	**May 09, 2019 - May 16, 2019**	**Live Event**
SANSFIRE 2019	**Washington, DC**	**Jun 15, 2019 - Jun 22, 2019**	**Live Event**
SANSFIRE 2019 - SEC505: Securing Windows and PowerShell Automation	**Washington, DC**	**Jun 17, 2019 - Jun 22, 2019**	**vLive**
SANS Boston Summer 2019	**Boston, MA**	**Jul 29, 2019 - Aug 03, 2019**	**Live Event**
SANS Prague August 2019	**Prague, Czech Republic**	**Aug 12, 2019 - Aug 17, 2019**	**Live Event**
SANS Network Security 2019	**Las Vegas, NV**	**Sep 09, 2019 - Sep 16, 2019**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**