Global Information Assurance Certification Paper

GIAC Certified Windows Security Administrator

Practical Assignment Version 5.0

Option Two: Topics in Windows Security

A Windows Security Baseline for Financial Institutions: Regulatory Recommendations, Baseline Creation, and Baseline Audit

Ty Purcell

February 10, 2005

Abstract

Financial institutions use technology in all areas of their business. Due to the sensitive information dealt with, security is an important element in the technology used at financial institutions. Laws and regulations such as the Gramm-Leach-Bliley Act (GLBA) enable governing agencies to provide guidance and regulate the security of financial institutions. Large financial institutions have the resources to interpret this guidance and implement effective security technologies. Smaller financial institutions may lack expertise and resources to interpret guidance and achieve an acceptable level of security.

This paper will interpret law, guidance, and regulations to define a baseline security standard for financial institutions running Windows Active Directory networks. Once established the procedure to properly configure the baseline will be presented in a modular step-by-step method. Finally, this paper will offer methods to audit each module of the baseline.

A Windows Security Baseline for Financial Institutions:
Regulatory Recommendations, Baseline Creation, and Baseline Audit

Due to the nature of their business, computer and network security at financial institutions has always been a top priority. Large financial institutions have many resources to address security needs. Smaller financial institutions however, may not have the expertise and funding to continuously stay ahead in the security arena. This is compounded by the recent introduction of the Gramm-Leach-Bliley Act (GLBA). GLBA mandates three things:

> (1) to insure the security and confidentiality of customer records and information;
> (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
> (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.[1]

The GLBA specifies that agencies will establish appropriate standards for the financial institutions subject to their jurisdictions relating to administrative, technical, and physical safeguards. Some of these agencies are the Office of the Comptroller of the Currency (OCC), Board of Governors of the Federal Reserve System, Board of Directors of the Federal Deposit Insurance Corporation (FDIC), Director of the Office of Thrift Supervision, Board of the National Credit Union Administration, and the Securities and Exchange Commission. These agencies govern National Banks, Credit Unions, State Banks, branches of Foreign Banks, bank holding companies, banks insured by the FDIC, brokers or dealers of securities, investment companies and advisors, and insurance providers. This creates a great range of financial institutions from a multi-billion dollar global entity to a small independent insurance provider. This large array coupled with the many governing agencies can create confusion for financial institutions. The governing agencies have provided guidance in the form of bulletins, alerts, Financial institution Letters, Federal Financial Institutions Examination Council (FFIEC) guidance, and guidance for conducting examinations of financial institutions.

While guidance has been provided it is often vague and is sometimes not up to date. This can leave financial institutions, specifically smaller independent financial institutions, wondering exactly what they are required to do to ensure security of their computers, networks, and customer data. A baseline security configuration is needed for financial institutions. This will allow financial institutions to increase their security levels while knowing that they are meeting the recommendations of the governing agencies. This will also aid the governing agencies in their examinations of the financial institutions. An examiner, as a part of their exam, will be able to test against the baseline and easily note compliance or lack thereof.

[1] Gramm-Leach-Bliley Act, 15 USC 6801

This baseline will establish a minimum operating system, utilize tools available in the operating system, open source tools, and tools that are relatively inexpensive. After meeting the baseline, it must be audited to ensure that the baseline continues to be met. Again, a modular step-by-step approach will be taken to audit each item in the baseline. The goal of the modular step-by-step approach is to enable a person with little experience to configure and audit the baseline. This would also enable financial institutions to hire a consultant to apply the baseline and then verify for themselves that the baseline has been met. This will give the financial institutions a simple means to run a secure network while also giving the examiners and auditors a means to technically audit a windows network. The end goal is to raise the bar of both security configuration and examination – resulting in a higher level of security across all financial institutions.

Section One

Establishing the Baseline

The baseline will focus on a Windows 2000 Active Directory network, excluding IIS, MSSQL, and Exchange. It must be noted that all Microsoft Windows operating systems prior to Windows 2000 are considered insecure for use in financial institutions. This is due to enhanced security tools in newer offerings, native insecurity in older operating systems, and lack of future support for older operating systems. For maximum security, systems must be patched with the most current service pack and all hotfixes. Systems must also use the NTFS file system on their disks. Group Policy will be used to automate and simplify security configuration.

Basic Network Configuration and Defense in Depth

A recent article in Bank Technology News suggested that financial institutions would like their regulating agencies to set levels of required security technology based on total deposit thresholds. "For example, if a bank holds at least $500 million in deposits, it requires an intrusion detection system (IDS) or something similar."[2] While that would be a clear-cut way for financial institutions to determine compliance, it does nothing to address the amount of technology already in use in an institution. A credit union with assets of $50 million might be connected to the Internet via a T1 and offering Internet banking, but based on the example; they would not be required to have an IDS. The other end of the spectrum could include a $600 million bank that utilizes dial-up modems only for Internet access. Would they need an IDS? A host-based IDS is called for, but certainly not a network-based IDS suitable for a broadband connection.

In order to protect the data of a financial institution and their customers, as specified by GLBA, if there is any access to the Internet there must be a firewall and intrusion detection/prevention systems (IDS/IPS). If a financial institution utilizes dial-up on a computer, then a host based firewall and IDS/IPS system must be deployed. Also, if an institution connects to the Internet via any type of "always on" connection (ISDN, DSL, etc.) then their network must also include a stand-alone firewall (either in appliance form or running on a dedicated server) and network based IDS/IPS. Also, effective virus, spyware, and trojan detection and removal software is necessary due to the risk of private data being leaked to external sources. This software should be deployed on all computers and detection patterns should be kept up to date. At this point we can create a diagram of a very basic secure network configuration (Figure 1).

[2] Kite, p.44.

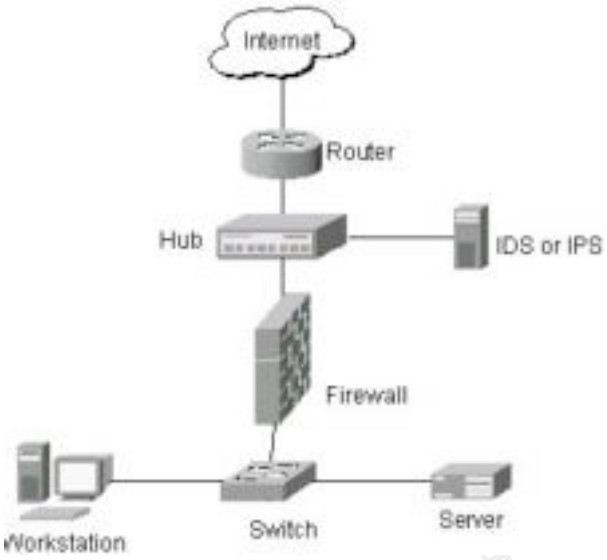


Figure 1 - Basic Secure Network Configuration

Defense in Depth is a term used in reference to having multiple layers of security guarding the desired item. Keeping with our financial focus, this could be best described in a scenario in which we wish to open a bank's vault. First, there probably is a security camera recording our approach to the vault. Once we arrive at the vault, we enter the code to disarm the alarm. If we don't know the code and attempt to proceed, an alarm will sound hopefully preventing access. Since we know the code, we proceed to open the combination lock and another person will use their key to open a keyed lock. Now that the vault door is open, there may be another camera inside recording activities in the vault (after all you would want to know if someone blew a hole in the wall to gain access!). There also may be another locked door behind which all the money is kept. As you can see there are many layers of security, some passive and some active that must be passed through to get inside of the vault. The same configuration should exist in order to protect your network, and in turn your important data.

Looking at the example of the vault, let's compare it to a network utilizing defense in depth (Figure 2). First, we have our security camera. This records our approach, even before we get to the vault door. In our network, this would be an IDS, since it detects and records our presence. Next, we have the alarm, which we must deactivate. This will be an IPS. An IPS detects malicious activity and prevents it by refusing access to the requested network resource (as would happen if we did not disarm the alarm). The vault door represents our primary firewall. The locks on the vault know to open when the correct key or combination is used. The firewall knows to permit traffic when the correct rule on the firewall is matched. If a rule does not exist that allows access to a requested resource, the request is denied. An attacker would then have to figure out how to defeat this layer of security. Past the vault door there is another security camera. So past the firewall, inside the network, we place another IDS. This helps to ensure that your internal users are using the network appropriately and that any unauthorized access from back-door methods such as modems or rogue wireless access points is detected. It is worth noting that in our network we can further extend

defense in depth by utilizing Host based firewalls and HIDS. This gives a total of five layers an attacker must defeat in order to compromise a computer (Figure 3).

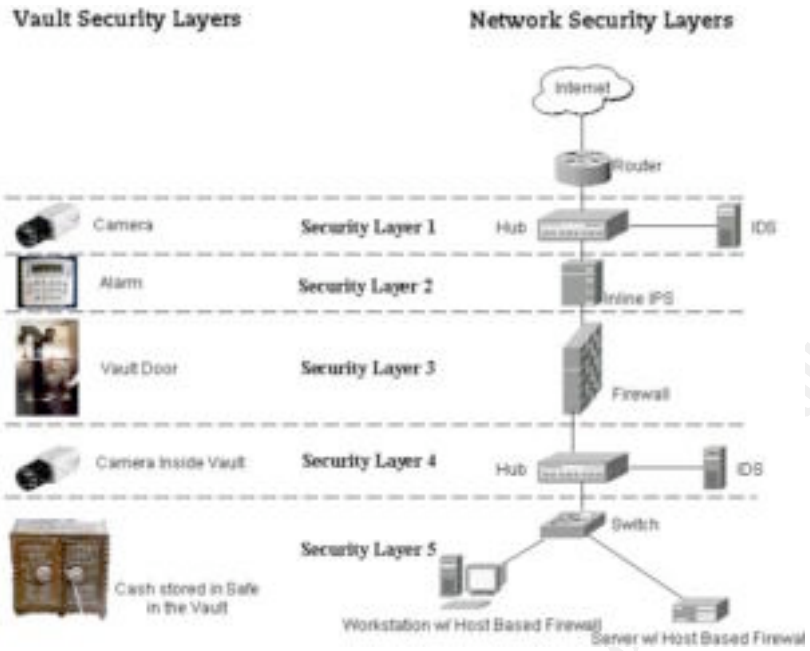


Figure 2 - Comparison of Vault and Network Security

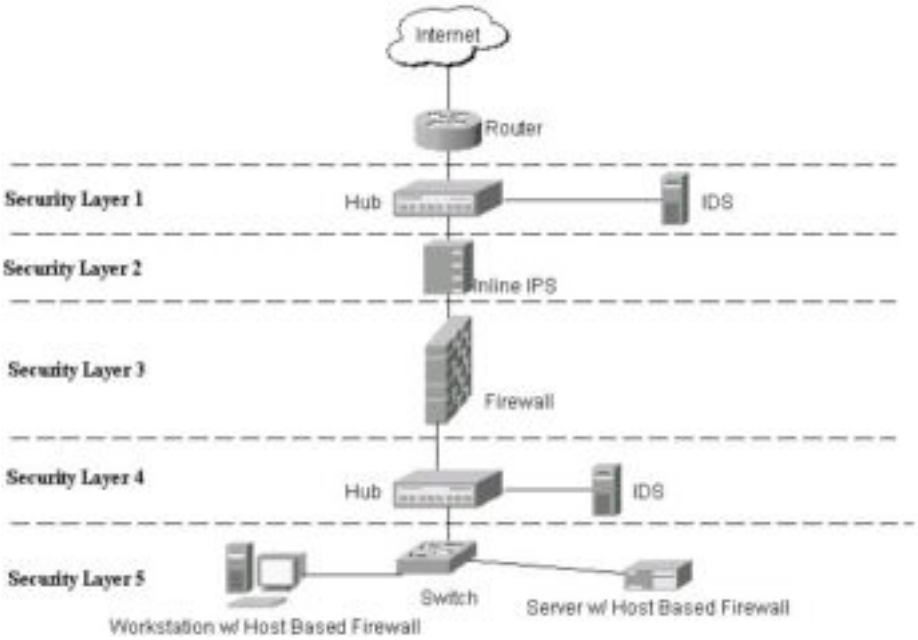


Figure 3 - Final Network Design Utilizing Defense in Depth

Protection against viruses and other malware, collectively referred to as malicious code, must also be configured with defense in depth in mind. Many IDS, IPS, and firewall vendors include detection for malicious code. This layered with scanning of all

email before it reaches the users, scanning of HTTP traffic, and detection on the computer level provide many opportunities to remove malicious code, and can prevent the spread if a computer does become infected.

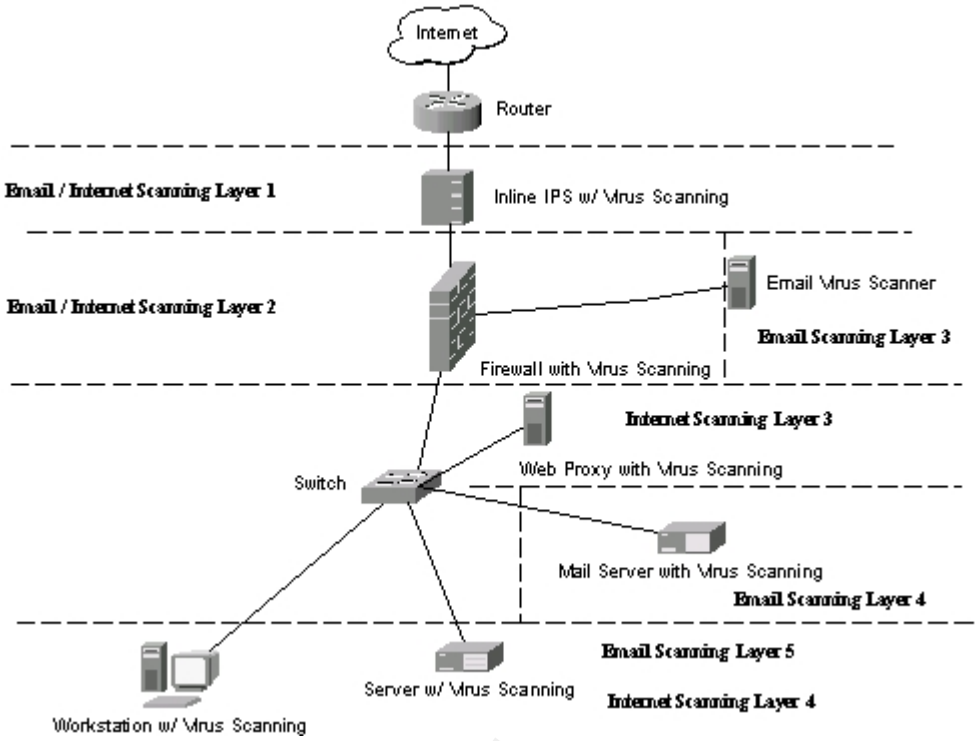


Figure 4 - Defense in Depth for Malicious Code

Baseline Modules

Password Requirements

Password requirements are often a difficult issue to discuss with users. They would like to use easy passwords, or often no passwords at all. However, this is the exact opposite of where institutions must be headed in order to secure their networks. To provide a secure environment to conduct business in, access to the network must be explicitly controlled. The FFIEC has released guidance that addresses this specific issue:

> "Password composition standards that require numbers or symbols in the sequence of a password, in conjunction with both upper and lower case alphabetic characters, provide a stronger defense against password cracking programs… ….While the use of passwords/PINs with 4 or more characters is currently a common industry practice for retail systems, the industry is moving toward use of passwords of 6 characters with a combination of letters and numbers, which is particularly appropriate for single-factor authentication methods, to provide stronger protection against compromise;" [3]

[3] FDIC, Authentication in an Electronic Banking Environment, p. 6, p. 7.

At first glance it appears that an appropriate standard can be easily achieved using the "Enable Password Complexity" option in Group Policy. However, this is not the case. The default password filter included in Windows 2000 will require that passwords be at least 6 characters long, not contain any part of the user's full name, and contain at least three out of the four following categories of characters: Uppercase letters, lowercase letters, numbers, and non-alphanumeric symbols. By only requiring 3 of the 4 categories, a problem is created. The character space that a password cracker must search is lessened. Also, while the guidance suggests a password of six characters, an eight-character password should be the minimum allowed. For example a six-character password with upper and lower case letters and numbers included would yield a possible 56.8 billion combinations (62^6). By increasing the password length to eight characters and including symbols in the required categories the possible combinations jumps to 722 trillion (72^8). This is a dramatic increase in the amount of combinations to try when a password cracker is run.

Other issues concerning passwords are the amount of time required before changing a password and how often a user can reuse a password. The amount of time required to crack a password of minimum length is the driving factor in the decision of how long to allow users to keep a password. In a financial institution's high-security environment, the maximum time that users should be allowed to keep eight character passwords utilizing a 72-character space is thirty days. Users have a tendency to reuse their old passwords. This reuse is not acceptable because it effectively undermines the use of a maximum age for passwords. If a user were allowed to reuse a password every 90 days, an attacker would have 120 days to crack their original password. Then they could logon with the new (old) password. In effect this could produce a very short list of passwords that users would reuse over and over. To combat this, the number of passwords Windows remembers must be set to it's maximum – twenty-four. Windows will then not allow users to reuse a password if it is one of the previous twenty-four. Also, with this set, users will likely assume that passwords are not permitted to be reused and will not attempt to reuse them. Another setting that will combat password reuse is setting a minimum password age. This setting will not allow users to change their password before it is a given number of days old. A user might attempt to change their password repeatedly until the system allows them to keep a password they have used before. Setting the minimum age to twenty days would prevent a user from reusing a password for 480 days. Again with the days to reuse of a password being so large, users will probably assume that passwords cannot be reused. Somewhat related to password requirements are account lockout policies. These policies set a threshold for the number of times a user can enter the wrong domain password until logon capabilities are disabled, the amount of time until account remains locked out, and how long until the lockout counter is reset. These settings must exist because there are programs that allow attackers to generate a username and then try different passwords until they successfully gain access. Users can quickly try a password several times and Windows will also try different means of authentication if one fails. So one failed logon attempt may be recorded by the Domain Controller as three logon attempts. An acceptable threshold for lockout is five logon attempts. Also, a member of the Account Operators or Administrators group should be required to unlock the account.

The final password standard recommendation is:

- A length of at least eight characters
- Uppercase characters
- Lowercase characters
- Numbers
- Non-Alpha Numeric Symbols
- Maximum Age of 30 days
- Minimum Age of 20 days
- Password History set to 24 passwords remembered
- Account Lockout Threshold of 5 attempts
- Administrator required to unlock a locked account

Physical Access

While placing computers in areas not accessible to the public is very important, one easy way that Windows helps to control unauthorized access is to utilize screen savers with passwords. The FFIEC's IT Examination Handbook advocates the use of password protected screensavers[4]. However, no guidance has been found concerning the length of time that must pass before the screensaver becomes active. In areas accessible to the public, an appropriate length of time before screen saver activation is five minutes. Users quickly become accustomed to this setting and if a user is actively using their computer they will use it at least once every five minutes. Also, any period of time longer that five minutes would lengthen the window in which an unauthorized person could gain access to the computer. In areas that are behind a locked door, screen saver activation could be set to a value of fifteen minutes or greater. Generally this would only be recommended in areas that have few users, all users with the same access privileges, and users utilizing more than one computer.

The final physical access recommendation is:

- Enforce password protected screen savers with an activation time of five minutes.

Disable Unneeded Services

An installation of Windows 2000 running SP 4 has approximately 55 native Microsoft services installed by default. A service is a method for starting a program when the system boots up. Many of the services are unnecessary for the average user and many services also have vulnerabilities. Leaving services running that are unused and possibly vulnerable could lead to system compromise. This goes against guidance provided by regulatory agencies and the GLBA because it could result in the loss of customer data. The Center for Internet Security has developed a Windows 2000 Level 2 Benchmark of baseline security settings. A benchmark also exists for 2000 Server, XP, and 2003 Server. These benchmark settings cover many areas, some of which we will discuss later. Contained in the benchmark is a list of services that CIS believes should be disabled to protect your computer.[5] It is recommended to disable all services that the Windows 2000 Level II benchmark recommends to be disabled by applying the

[4] FFIEC, IT Examination Handbook, p. 47.
[5] Shawgo, p. 38.

Win2kProGold template as described in the appendix and then disabling any other unused services that are identified in testing on your network.

The recommendation is:

- Apply the CIS Win2kProGold template to all workstations, then identify and disable any other unused services.

Secure Registry Settings

There are also other unnecessary features enabled by default in Windows 2000 that can lead to possible breaches in security. A few of these include:

- Dr. Watson Crash Dumps - Used to dump application errors to a file for future analysis, can include sensitive information such as usernames and passwords.
- Compact Disk Autorun – Allows CDs to automatically run programs when inserted. Can allow unauthorized or malicious programs to be installed or executed.
- Automatic Logon – Windows 2000 has a feature that logs the same user on each time the machine starts. This is achieved by storing the username and password in the registry in plaintext.
- Display the last logged on username – If you logoff of a Windows 2000 computer, it stores your username in the username box. When logging on you only have to enter your password. This can give anyone a valid username for the machine.

Since these and other features can cause the compromise of the machine, which would lead to possible loss of customer records and information, they must be securely configured. Thankfully, the Center for Internet Security has included in their Windows 2000 Level 2 benchmark a list of registry settings that will secure these unneeded features. Applying the Win2kProGold security template most easily configures these settings.

The recommendation is:

- Apply the CIS Win2kProGold template to secure registry settings.

Secure File System Settings

The main benefit of the NTFS file system is that it allows file level permissions to be set by user or group. This is a vast improvement over the FAT file system that allowed any user to access any file. While using NTFS alone is a security improvement over FAT, additional measures must be taken to prevent unnecessary user access to files and directories. These additional measures can prevent the elevation of privileges. Again, the Center for Internet Security provides a baseline for NTFS security in their Windows 2000 Level 2 benchmark. While these settings are too numerous to list in this document the list is available in the *Windows 2000 Professional Operating System Level 2 Benchmark – Consensus Baseline Security Settings*.[6]

The recommendation is to:

[6] Shawgo, p. 46.

- Apply the file system settings from the CIS Win2kProGold template.

Data Encryption

The FFIEC has a lot to say about encryption:

"Encryption is used to secure communications and data storage, particularly authentication credentials and the transmission of sensitive information. It can be used throughout a technological environment, including the operating systems, middleware, applications, file systems, and communications protocols. Encryption is used both as a prevention and detection control. As a prevention control, encryption acts to protect data from disclosure to unauthorized parties. As a detective control, encryption is used to allow discovery of unauthorized changes to data and to assign responsibility for data among authorized parties. When prevention and detection are joined, encryption is a key control in ensuring confidentiality, data integrity, and accountability."[7]

Encryption on Disk

A financial institution's main interest is in protecting the integrity and preventing unauthorized access to data. Data that must be protected can exist anywhere – from word processing documents to spreadsheets. The best way to achieve this high level of data protection is through the use of encryption. There are many ways to encrypt data, but Windows 2000 provides a built in method that transparently encrypts and decrypts data for authorized users.

The recommendation is to:

- Encrypt all sensitive data while stored on the file system.

Network Encryption

Again, in the FFIEC's IT Handbook, in the listed Tier II examination procedures, the following is stated, "Determine whether appropriate controls exists over the confidentiality and integrity of data transmitted over the network (e.g. encryption, parity checks, message authentication)."[8]

In a Windows network, as data is transmitted over the network, it exist in an unencrypted form. This makes it susceptible to compromise by sniffing or man-in-the-middle attacks. One of the methods suggested in guidance is to encrypt data. Windows 2000 has a built in feature for encrypting data that is transmitted over the network. This feature is an extension of the IP protocol, called IPSEC. IPSEC, available on many other operating systems, allows encryption of all or some network data. This encryption is achieved without the operating system or the program that originated the data knowing. For example, an application that uses FTP to send data to a Windows 2000 server sends the data unencrypted. If IPSEC is enabled and configured on both machines, that FTP traffic becomes encrypted – without the client or server program knowing that it is. Any information on the network can

[7] FFIEC, IT Examination Handbook, p. 48
[8] FFIEC, IT Examination Handbook, p. A-13

potentially be used by attackers to compromise the network. Since guidance recommends encryption and the functionality is built-in it is recommended to utilize IPSEC encryption.

The recommendation is:

- Encrypt all network traffic via IPSEC

Host Based Firewall

Often it is not one hole that results in system compromise, but a series of holes that allows attackers to conquer a system. To protect the integrity and confidentiality of computer systems and data every step possible must be taken to secure the network. Another step that can be taken is to deploy host based firewalls on every system. There are many virus scanning programs as well as stand-alone programs such as Zone Alarm that offer a host based firewall, but the capability also exists in versions of Windows beginning with Windows 2000. It is possible, using IPSEC filters, to implement a packet filter system. It is recommended to block all incoming traffic destined for ports not needed for normal network activity. An example would be to block access to ports 21 (FTP) and 23 (Telnet). The allowed incoming ports below will allow domain functionality in Windows 2000.

The recommended host based firewall rules are:

- Block all incoming traffic.
- Allow incoming traffic on ports:
  TCP: 46, 88, 135, 139, 445
  UDP: 46, 53, 137, 138, 445, 500
- Allow all outgoing traffic.

Authentication Methods

Part of a secure network is ensuring that a secure method of authentication is used. While regulation and guidance do not specifically address which means of authentication to use between a client and server, it is noted that proper authentication steps should include encrypting the transmission and storage of authenticators.[9] A financial institution must take steps to ensure that they are using the most secure methods of network authentication. Windows 2000, while using Kerberos as it's default authentication mechanism, has several other methods of authentication included for backwards compatibility. These include LM, NTLMv1, and NTLMv2. While all three methods do provide for encryption of authentication data while it is being transmitted, LM and NTLMv1 have weaknesses[10] that can result in easy compromise and sniffing of passwords using cracking programs such as L0pht Crack. To combat the weaknesses of prior authentication methods, NTLMv2 was released. NTLMv2 traffic cannot be sniffed by L0pht Crack. NTLMv2 also uses a challenge/response method to authenticate users. This means that the user's NTLM password hash is never sent over

[9] FFIEC, IT Examination Handbook, p. 18.
[10] Murphy

the network. It is possible to disable the use of the LM and NTLMv1 authentication methods.

The final recommendation is to:

- Disable use of LM and NTLMv1 authentication methods.
- Require use of the NTLMv2 and Kerberos authentication methods.

Remove Lan Manager Hash

As previously discussed, the Lan Manager (LM) hash is not a secure way for network authentication. Also, the stored LM hashes in the Active Directory or SAM databases can be cracked very easily. Password cracking utilities such as John the Ripper, and L0pht crack can crack non-complex password hashes in seconds. Complex passwords of length eight utilizing letters of upper and lower case, numbers, and symbols have been repeatedly cracked in less than twenty-four hours. However, the NTLM hash of the same complex password was not cracked. Since LM hashes are obviously not a secure method of storing authenticators[11] and we are not using LM authentication in our network the hashes must be removed from the Active Directory and SAM databases. Removing the LM hashes will prevent the use of LM authentication and will make it harder for passwords to be cracked should your Active Directory or SAM databases become compromised.

The final recommendation is to:

- Remove the LM hash from both the Active Directory and local SAM accounts databases.

Change and Secure Local System Credentials

In discussing passwords and user authentication, the FFIEC's IT Examination Handbook states:

> "Typically, hardware and software are installed with default users, with at least one default user having full access rights…….Default user accounts should be disabled, or the authentication to the accounts should be changed."[12]

> "Controls include training in and enforcement of password policies that make passwords difficult to guess. Such policies address the secrecy, length of the password15, character set, prohibition against using well-known user identifiers, and length of time before the password must be changed."[13]

This affects Windows workstation in an obvious place: the default users "Administrator", "Guest", and "ASPNET", if the .Net framework is installed. In the effort to secure the network user accounts, the local machine accounts can sometimes be forgotten. If these are left with the default usernames and settings, then attackers can gain control of a workstation through one of these local accounts and then move on to

[11] FFIEC, IT Examination Handbook, p. 18.
[12] FFIEC, IT Examination Handbook, p. 17.
[13] FFIEC, IT Examination Handbook, p. 20.

network access. To prevent compromise of the necessary accounts on the local computer, several changes must be made. The usernames must be changed, passwords set with strong, complex passwords, and passwords must be set to expire. Also, if possible the account must also be disabled.
The final recommendation for each account is:

Administrator
- Change account name
- Set a strong password
- Set the password to expire

Guest
- Change account name
- Set a strong password
- Set the password to expire
- Disable the account

Other Local Accounts (where possible)
- Set a strong password
- Set the password to expire
- Disable the account

Section Two

Meeting the Baseline – Step by Step

Password Complexity – PassFilt Pro

Since it has been established that the default Windows 2000 password filter is not acceptable for complex passwords, we must replace the default filter with a new filter. Password filters can be created with a little programming, or a programmer can be contracted to create a filter for you. However, there are several companies that provide ready-made password filters. One of these filters is PassFilt Pro from Altus Network Solutions. It is very flexible and provides many ways to enforce complex passwords while at the same time being inexpensive. The filter exists in two editions, one for single password policies and one that allows up to four policies that can be applied to global groups. This filter allows customization of the password policy in the following areas: (http://altusnet.com/download/Passfilt Pro SPE Documentation.pdf)

- Maximum Password Length (in characters):
- Reject passwords that don't contain at least (X) of the following character types: (Uppercase, Lower Case, Numeric, Special).
- Check for numeric characters in password.
- Minimum Numeric Characters Required:
- Maximum Numeric Characters Allowed:
- Check for upper case characters in password.
- Minimum Upper Case Characters Required:
- Maximum Upper Case Characters Allowed:
- Check for lower case characters in password.
- Minimum Lower Case Characters Required:
- Maximum Lower Case Characters Allowed:
- Check for alpha characters in password.
- Minimum Alpha Characters Required
- Maximum Alpha Characters Allowed
- Check for non-alphanumeric characters in password
- Minimum Non-Alphanumeric Characters Required
- Maximum Non-Alphanumeric Characters Allowed
- Reject password that contain vowels
- Reject passwords that contain 2 consecutive identical characters
- Reject passwords that begin with a number.
- Reject passwords that end with a number.
- Passwords must contain a numeric character in position (X)
- Passwords must contain a special character in position (X)
- Reject passwords that contain the username.
- Reject passwords that contain any part of the user's full name.
- Enable dictionary password checking.
- Enable dictionary substring search

A thirty-day demo of the single policy edition is available for download at from Altus. The install package consists of a MSI file and documentation. Installation and configuration of the filter is completed in four steps.

1. Open Active Directory Users and Computers, right click the Domain Controllers OU and select properties. Next click the "Group Policy" tab, select the Default Domain Controllers Policy and click the "Edit" button. A new window titled "Group Policy" will appear. Expand the tree on the following items Computer Configuration>Windows Settings>Account Settings. Under Account Settings select "Password Policy". In the right window you will see several policies listed. Double click the policy named "Passwords must meet complexity requirements". A Policy Setting box will popup, check the "Define this policy setting" checkbox, and then click the "Disabled" radio button. To finish click the "OK" button and close the GP window. The GP setting we just made – to disable password complexity, is made instantly – you don't have to save anything. The setting will now be replicated to all other domain controllers within the domain.

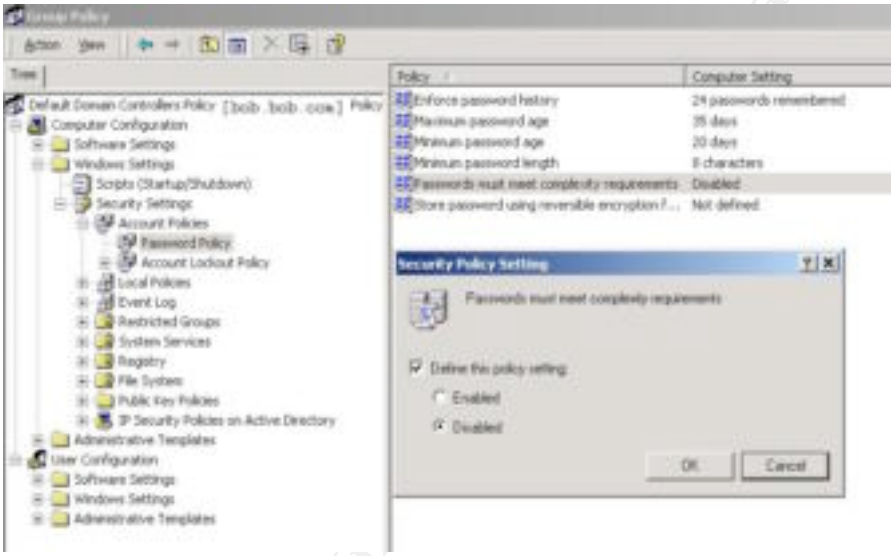


Figure 5 – Passwords must meet complexity requirements

2. While logged in to a Domain Controller, locate the PassfiltPro MSI file and double click to install. Click Next, Next, make note of the install location, and click Install. After installation is complete, click Finish. In order for the necessary files to load, you must reboot the Domain Controller. Repeat this step for each Domain Controller in your domain.
3. Next we must create a new Group Policy Object for PassfiltPro and load a template into it. Open the properties for the Domain Controllers container in ADUC. Select the Group Policy tab and click the "New" button. Give the new GPO a name that you will recognize such as "PassfiltPro". Now highlight the GPO you just created and click the edit button. Browse to Computer Configuration>Administrative Templates. Right click on Administrative Templates and select "Add/Remove Templates" from the menu. In the window

that opens browse to the folder where PassfiltPro was installed earlier and select the **passfiltpro.adm** template. Click Open and you will see the template you just selected listed in the list of currently installed templates. Click the Close button to return to the Group Policy editor. Now under Administrative Templates, a new template will exist with a name starting in "Passfilt Pro". Select this policy and in the right window double click "Registration". In the new window select the "Enable" radio button and then enter the registration or evaluation code you received from Altus. Select "OK" and we are finished with the installation.

4. Next double click the "Password Filter Configuration" policy. This will open a new window with all of the features shown in the list above. First select the "Enabled" radio button to enable the filter, and then configure the filter to match your policy. Four of the recommended password requirements can be set here, but there are also several other beneficial settings. The settings below will result in a strong PassfiltPro policy:

- Maximum Password Length (in characters): **127**
- Reject passwords that don't contain at least (**4**) of the following character types: (Uppercase, Lower Case, Numeric, Special).
- Check for numeric characters in password. **Enabled**
- Minimum Numeric Characters Required: **1**
- Maximum Numeric Characters Allowed: **127**
- Check for upper case characters in password. **Enabled**
- Minimum Upper Case Characters Required: **1**
- Maximum Upper Case Characters Allowed: **127**
- Check for lower case characters in password. **Enabled**
- Minimum Lower Case Characters Required: **1**
- Maximum Lower Case Characters Allowed: **127**
- Check for alpha characters in password. **Enabled**
- Minimum Alpha Characters Required: **1**
- Maximum Alpha Characters Allowed: **127**
- Check for non-alphanumeric characters in password: **Enabled**
- Minimum Non-Alphanumeric Characters Required: **1**
- Maximum Non-Alphanumeric Characters Allowed: **127**
- Reject passwords that begin with a number: **Enabled**
- Reject passwords that end with a number: **Enabled**
- Reject passwords that contain the username: **Enabled**
- Reject passwords that contain any part of the user's full name: **Enabled**
- Enable dictionary password checking: **Enabled**

Password Complexity – Other Group Policy Settings

While configuring PassFilt Pro, we noted that it would only enforce four of recommended settings. Minimum password length, password history, Minimum age, and Maximum age still must be configured. However these are all easily set in Group Policy.

1. First, open ADUC, and select Properties on the Domain Controllers OU. Next, click the Group Policy tab on the properties window. In the list of Group Policy

Object Links double click on the **Default Domain Controllers** policy. Once the Group Policy window is open browse down this path on the tree: Default Domain Controllers Policy > Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy. In the right hand window there are four policies that we will configure. Double click on each policy, check the define policy setting checkbox, set it to the setting below, and then click "OK".

- Enforce password history: **24 passwords remembered**
- Maximum password age: **30 days**
- Minimum password age: **20 days**
- Minimum password length: **8 characters**

2. Next, select the Account Lockout Policy, which is located under Security Settings in the Group Policy Window. In the right hand window there are three policies to be configured. Double click on each policy, check the define policy setting checkbox, set it to the setting below, and then click "OK".

   - Account lockout duration: **0**
   - Account lockout threshold: **5 invalid logon attempts**
   - Reset account lockout counter after: **99999 minutes**

These settings, combined with an enhanced password filter (Passfilt Pro), provide a strong password policy for your institution.

Physical Access

Forcing use of a logon screen saver is a good method to help control physical access via Group Policy. It is also very easy to do, and very flexible. If you have systems in a secure area such as a server room, it may be desirable to create a separate OU for those systems and enable a longer screensaver timeout. We will configure a default screen saver for all systems, and a screen saver with a longer time out for a specific OU.

1. Open ADUC, right click on the name of your domain, and select "Properties". Next click the Group Policy tab in the Properties window and select the "Default Domain Policy". Now, in the Group Policy window browse down the following path on the tree: Default Domain Policy > User Configuration > Administrative Templates > Display. In the right window select the "Enable" radio button and configure the four policies with the following settings:

   - Activate screen saver: **Enabled**
   - Screen saver executable name: **login.scr**
   - Password protect the screen saver: **Enabled**
   - Screen Saver timeout: **300 seconds**

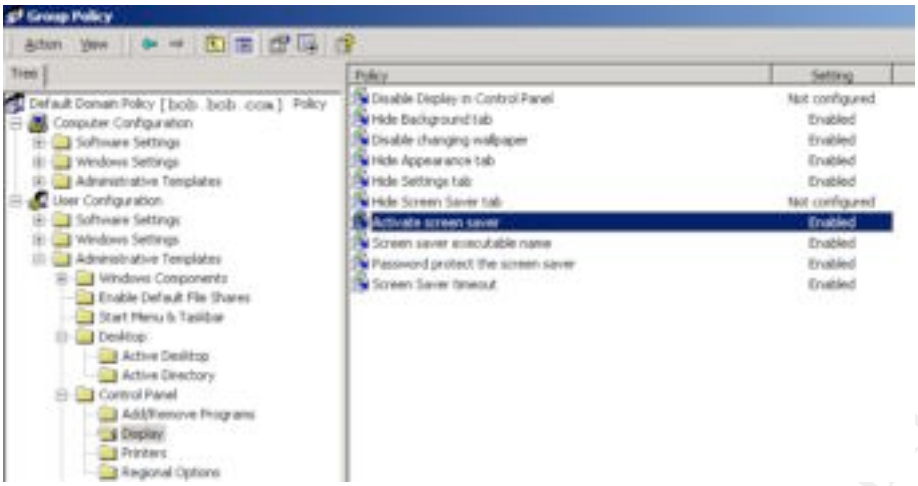


Figure 6

2. To configure a different screensaver timeout for a specific group of computers we must create a new OU and move a computer suitable for testing into it. This process is detailed in the *Active Directory and Group Policy* section. In this example we will create a "Test" OU and apply a longer screen saver timeout to the machines in it. Now, in ADUC right click on the Test OU and select Properties. Click the Group Policy Tab and in the Group Policy Objects Links you will see there are no linked Group Policy Objects. Click the "New" button and give the GPO a descriptive name –*Test Group Policy* is a good suggestion. After naming the policy, double click it to configure the screen saver settings for the policy. Just as above, in the Group Policy window browse down the following path on the tree: Default Test Policy > User Configuration > Administrative Templates > Display. In the right window select the "Enable" radio button and configure the four policies with the following settings:

    - Activate screen saver: **Enabled**
    - Screen saver executable name: **login.scr**
    - Password protect the screen saver: **Enabled**
    - Screen Saver timeout: **600 seconds**

    Now, browse down the following path on the tree: Default Test Policy > Computer Configuration > Administrative Templates > System > Group Policy. Enable the "User Group Policy loopback processing mode" policy and set the Mode to Merge. Merge will apply all normal Group Policy settings for the user and then apply the settings from the Test GPO. Any conflicts will result in the Test GPO user settings overwriting the normal GPO settings. In this case, a conflict will occur between the default domain policy's setting of a 300 second screen saver time out and the Test GPO's setting of 600 seconds. The 600-second time out will apply to computers in the Test GPO.

    Allow time for the settings to propagate to all of the computers in the domain. Rebooting the computer should help to reapply the machine and user group

policies since the machine policy is always refreshed on reboot and the user policy is refreshed on login. All computers in the domain should automatically launch the screensaver at five minutes of inactive time, and the computers in the Test OU should launch the screensaver at ten minutes. Users can change the screen saver using the display settings for the machine, however the next time GP refreshes, the setting will return to the specified time. To prevent users from changing display settings, Group Policy can be used to control the amount of access available. More information on this can be obtained from Microsoft.[14]

Disable Unneeded Services

The default Windows 2000 installation enables many services that are unnecessary for normal domain function. It is possible to visit each computer to disable services, but Group Policy makes it possible to disable services on all machines in your domain or just on one OU. CIS, in their Windows 2000 Professional Gold security template, disables the following services:

Service Name	Startup Value
Alerter	Disabled
ClipBook	Disabled
Computer Browser	Disabled
Fax Service	Disabled
IISADMIN	Disabled
Internet Connection Sharing	Disabled
Messenger	Disabled
MSFTPSVC	Disabled
NetMeeting Remote Desktop Sharing	Disabled
Remote Registry Service	Disabled
Routing and Remote Access	Disabled
SMTPSVC	Disabled
SNMP	Disabled
SNMPTRAP	Disabled
Telnet	Disabled
W3SVC	Disabled

To disable these services, apply the CIS security template using the process detailed in the *Applying the CIS Windows 2000 Gold Security Template* section of the appendix. While disabling the above services removes many vulnerabilities, there are still other services that can be disabled. These services will differ for every financial institution and it will be necessary to spend some time experimenting to see which services can be disabled with minimum consequences. Some possible services to consider disabling are:

Automatic Updates
Background Intelligent Transfer Service
COM+ Event System
DHCP Client
Indexing Service

[14] http://msdn.microsoft.com/library/default.asp?url=/library/en-us/gp/default.asp

Print Spooler
QoS RSVP
Remote Access Auto Connection Manager
Remote Access Connection Manager
Remote Procedure Call (RPC)
Remote Procedure Call (RPC) Locator
Removable Storage
Server
Smart Card
Smart Card Helper
Uninterruptible Power Supply
Wireless Configuration
Workstation

To disable a service using Group Policy, open ADUC and edit the test OU Group Policy object. Browse to Computer Configuration> Windows Settings> System Services. In the right window a list of services that are available on the local computer is show. If a service you wish to disable across the OU or domain is not available on the computer your are running ADUC from, you must run ADUC on the computer with the service running on it to disable it across the domain. To disable a service, locate it in the list on the right, double click it, and check the "Define this policy setting" checkbox.

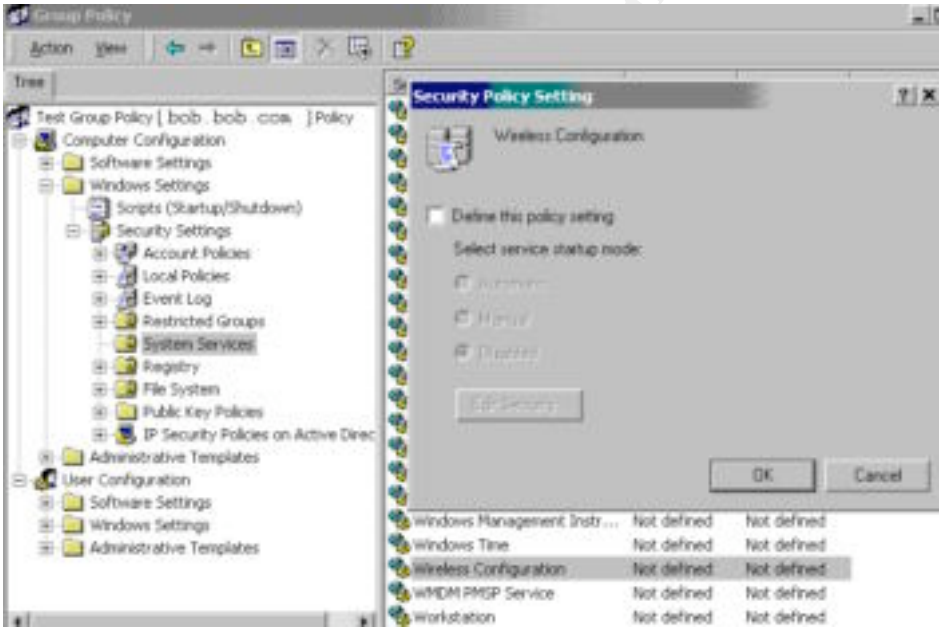


Figure 7

As soon as the box is checked a new window will open. Here you will define what users have full control, read, start – stop – pause, write, and delete permissions on the service. The "Everyone" group has full control permissions by default. Remove this group and click the add button. Select the "Domain Administrators" group and give them full control. This will prevent unauthorized users from starting the "Wireless

Configuration" service on workstations in the test OU. Click OK to return to the Security Policy Setting window, and make sure the radio button beside "Disabled" is selected. Click the "OK" button and the "Wireless Configuration" service will be disabled after propagation to machines in the test OU. Disable other services as testing shows that they are not needed in your Windows 2000 domain. Also document which services are to be disabled on each type of machine. This will aid you later in the audit process. Remember, the more services disabled on a machine leaves fewer places to attack. However, in your domain some programs may rely on services that are disabled in the Win2kProGold template. It is important to test all settings before implementing them across your domain.

Secure Registry Settings

Achieving an acceptable level of secure registry settings on a Windows 2000 workstation is fairly simple. Simply apply the Win2kProGold security template as shown in the appendix. In my opinion, the registry settings contained in the template are acceptable for a financial institution. However, some registry settings applied by the template may break some programs. For example, a piece of software might have previously had write access to a registry key, but after application of the template it might only have read access. This can be changed easily in Group Policy by editing the Group Policy Object. Browse to Computer Configuration> Windows Settings> Security Settings> Registry and find the key on which permissions need to be changed in the right hand window. Double click the key and then click the "Edit Security" button. If the group that needs access to the key is in the list give them the necessary permissions. If they are not, add them and then give them permission. Click "Apply" and then "OK" twice to return to Group Policy.

Secure File System Settings

Secure NTFS file system settings are another area that the Win2kProGold security template configures. An example of these NTFS settings are listed here:

System Root, Program Files, and System Drive:

Permissions:	Administrators (Local Computer):	Full Control
	Creator Owner:	Full Control
	System:	Full Control
	Users (Local Computer):	Read, Execute, List Folder Contents

While these settings are recommended for financial institutions, some programs require less restrictive file system permissions. Group Policy makes it easy to accommodate these programs by providing the ability to add folders and files to the template and set their access permissions. That way if a program requires write access to a file or a group of files in the C:\Winnt directory, we can use Group Policy to set the write permission on that file only. To add a file or directory to the File System settings in Group Policy, open ADUC and browse to Computer Configuration> Windows Settings> Security Settings> Event Log> File System. Right click "File System" and select "Add File" from the menu.

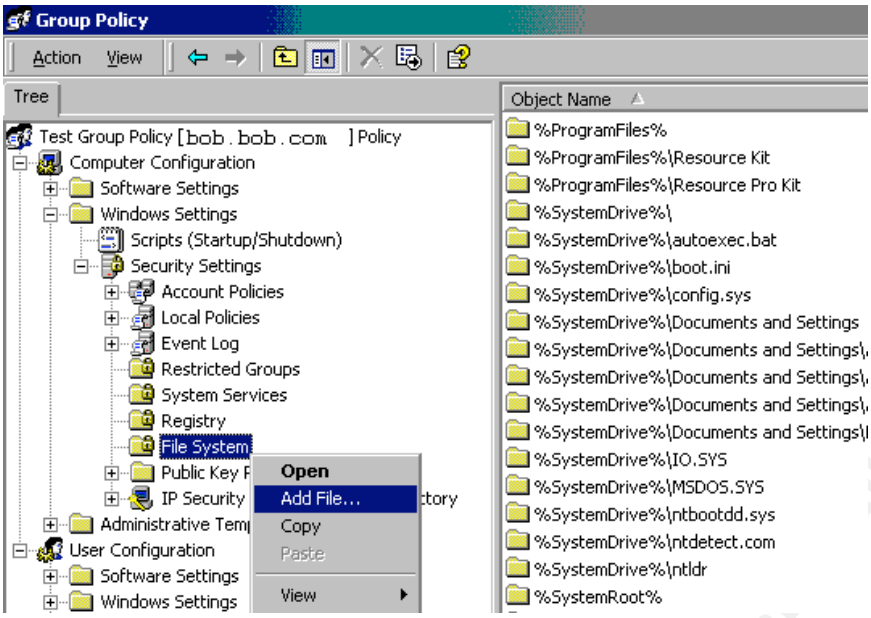


Figure 8

In the window that appears browse to the file or folder that you wish to add to the template. Select it and click "OK". In the next window, add all of the groups that need access to the file or folder and set their permissions. Remove any groups that do not need access. If the "Everyone" group is listed remove it and if the file or folder is inheriting overwriting permissions from it's parent uncheck the "Allow inheritable permissions…" checkbox. Click OK and the Template Security Policy Setting window will appear. In this window select the option that will give your application proper access. An example would be to select "Configure this file or folder then > Propagate inheritable permissions to all subfolders and files" if your application needs permissions on the whole folder. Click the "OK" button to complete the process.

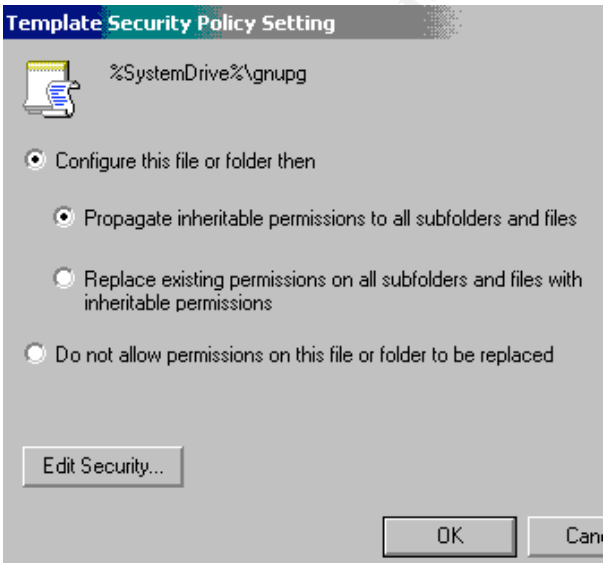


Figure 9

Data Encryption

Encryption on Disk

Windows 2000 includes a feature called the Encrypting File System (EFS). EFS is native to NTFS 3.x. It is possible to encrypt any file or folder on the system with the exclusion of files in the system root folder (C:/windows, C:/winnt), compressed items, and files that have the attributes Read Only, Hidden, or Archive. This makes it possible for financial institutions to protect customer data that is stored on disk. EFS can be used to encrypt databases, however it is advisable not to use EFS to encrypt databases due to possible performance issues. You are free to enable EFS on a test database to see the results. Encryption of customer data in database would be better handled at the field level. First we will see how easy it is to encrypt a folder and all of the files in it. Then we will look at a login script, deployable through Group Policy that will create an encrypted folder for users to place sensitive documents in. Since many files may be stored on a fileserver, we will start with encrypting a folder that is located on a network drive. First a setting must be made of the computer account of the fileserver. Open ADUC and find the computer account for your fileserver. Double click the account to edit and check the "Trust Computer for Delegation" checkbox, then click "OK".

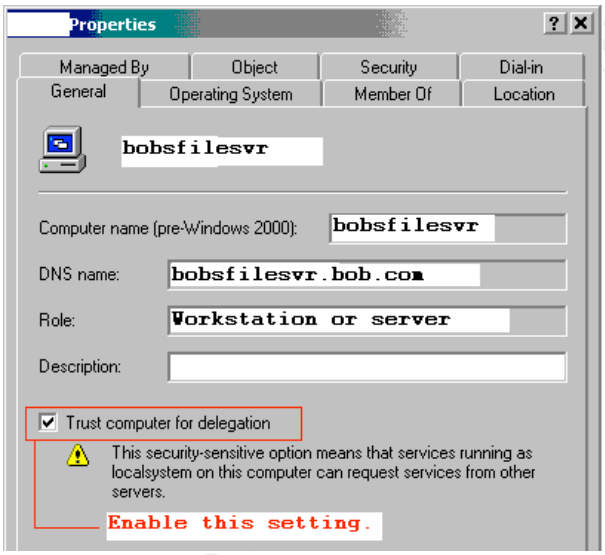


Figure 10

Now find a folder in your network drive, right click on it, and select properties. In the properties window that opens, on the general tab click the "Advanced" button. The Advanced Attributes window will display. Check the "Encrypt Contents to Secure Data" checkbox, click "OK", then click the "Apply" button on the properties page. A window will open asking you to confirm the changes you just made. Select the "Apply changes to this folder, subfolders, and files" radio button and click "OK".

That folder is now encrypted. Get an associate who normally has access to the folder to open a file that is in the folder. They will be able to see the files but will be prevented from opening them. It is important to note that if a user has NTFS delete permissions, then they can delete your encrypted files, but not read them. Also, currently in Windows 2000, encrypted files cannot be shared between users. That is – multiple users cannot share a folder of encrypted files. Windows Server 2003 and XP do have these capabilities. Here are a few more EFS caveats:

- The local computer admin account and the domain admin can recover encrypted files.
- Files on the way to or from an encrypted folder are transmitted in the clear. We will use IPSEC encryption of all network traffic to take care of this loophole later in this document.
- If you copy a file from an encrypted folder to a non-encrypted folder it becomes unencrypted.
- If you copy a file from an encrypted folder to another drive or partition that is not NTFS 3.x formatted, the file will be unencrypted.

Large Scale EFS Use

Now we will create a logon script to map a network drive, make a folder named "Encrypted", and then encrypt the folder. First, open notepad, enter the following text into a document. Next, save the file as **encrypted.bat** to the following path: \\mydomaincontroller\sysvol\bob.com\scripts

mydomaincontroller = the name of one of your domain controllers
bob.com = the name of your domain.
Scripts is a folder that was created for storing logon scripts. Items in the domain folder (bob.com) will get replicated to other domain controllers.

```
@echo off

net use z: \\bobsfilesvr\users\%username%

mkdir Z:\Encrypted

cipher /E /S:Z:\Encrypted /A /F Z:\Encrypted\
```

encrypted.bat script

The "net use" command maps a network drive to z: . In this example, there is a share called users on bobsfilesvr. In the users folder are folders corresponding with the usernames in the domain. So if Bob's username is bob, then he would have a folder named bob. The "%username%" is a variable that contains the username of the currently logged on user. This allows for some flexibility since many users will be sharing the same script. The next line in the script makes a folder named "Encrypted" in the Z drive. Finally, encryption is achieved with the cipher command. To see what each switch does, run "cipher /?" at a command prompt.

To make our login script active when users login we will assign it via Group Policy.

First, open ADUC and select an organizational unit or the domain. Again, for testing it would be best to select an OU with a small number of users. Next, right click on your choice, select properties, and then click the Group Policy tab. On the Group Policy tab edit the default policy. Open the following path on the Group Policy tree: User Configuration > Windows Settings > Scripts (Logon/Logoff). In the right hand window double click "Logon" to edit the logon scripts. In the Logon Properties window, click "Add", click "Browse" in the new window to find the encrypted.bat file we saved earlier. Your default location should be the current policy folder in the SYSVOL share. You may have to go up several levels to find the scripts folder. Once you have selected the encrypted.bat script, click "OK" in the "Add a Script" window. This should list your script in the "Logon Properties" window. Click "Apply" then "OK" to close the window.

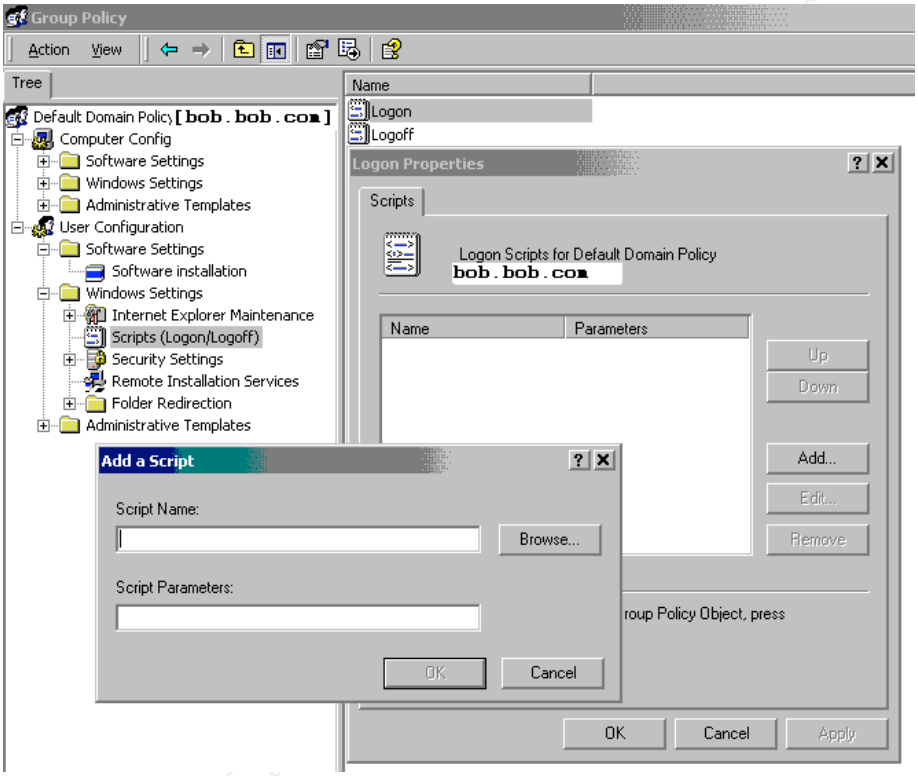


Figure 11

After propagation of the policy, have a user in the domain (or OU if you applied the script to and OU) reboot their computer and then logon. After logging on, have them open the my computer icon. The user should have a drive letter Z. Open this drive, and look for a folder called "Encrypted". After finding it, right click on it, select properties, and then click the "Advanced" button on the General tab. You should see a check in the "Encrypt Contents to Secure Data" checkbox. If you don't have a folder named "Encrypted", or if the folder is not encrypted first check to make sure the login script is executing. You should see it run before or during the loading of

the user's desktop. If the login script executes, try running the script from the command line. This will allow you to see any errors. Any files you put in the Encrypted folder will become encrypted themselves.

You now have the ability to effortlessly encrypt folders using 120-bit DESX [15] encryption. This will prevent other network users from viewing sensitive information concerning financial institution customers prevents viewing if the computer is booted into an alternative OS. Also, this method of encryption is transparent to your users. You could encrypt their entire My Documents folder and they would never know.

Network Encryption

The second piece of our encryption puzzle deals with encrypting data as it travels between computers in the domain. We will use a built-in feature of Windows 2000 and greater called *Internet Protocol Security* (IPSec). IPSec is "..a set of protocols developed by the IETF to support secure exchange of packets at the IP layer[16]." One exciting thing about IPSec is that it is implemented at the IP layer, or the Network layer of the DoD TCP/IP protocol model. What makes this exciting is that it enables us to encrypt all network traffic without the users ***or*** applications having to be IPSec aware! This means any application will work with IPSec. You may have even used IPSec before, since it is commonly used in VPNs. IPSec has two negotiation phases that occur in order to setup an IPSec session. We will make note later as we begin configuring each phase. An excellent three-part paper on IPSec is available at Security Focus.[17] It explains the basics of IPSec and then goes on to give good detail that is useful when configuring IPSec.

IPSec Policies are created using the IP Security Policy Management snap-in to the Microsoft Management Console (MMC). "Active Directory Users and Computers" is also a snap-in to MMC. Here we will build a custom MMC to keep tools within easy reach. Open MMC by clicking Start > Run and typing "mmc" in the open box. Click "OK" and the MMC will open. To add a snap in click Console > Add/Remove Snap-In. The "Add/Remove Snap-In" window will open. Click the "Add" button and the "Add Standalone Snap-In" window will appear. Select "IP Security Policy Management" from the list and click "Add". A window will open asking which computer the snap-in will manage. Select the radio button next to "Manage domain policy for this computer's domain" and click "Finish". Next, select "Active Directory Users and Computers" from the list and add it. Click the "Close" button and both of the snap-ins should be listed in the "Add/Remove Snap-In" window. Click "OK" and both snap-ins will appear under the console root in the MMC console.

[15] RSA Laboratories. What is DESX?
[16] Webopedia. IPSec
[17] Weber, Chris. Using IPSec in Windows 2000 and XP, Parts 1, 2, and 3

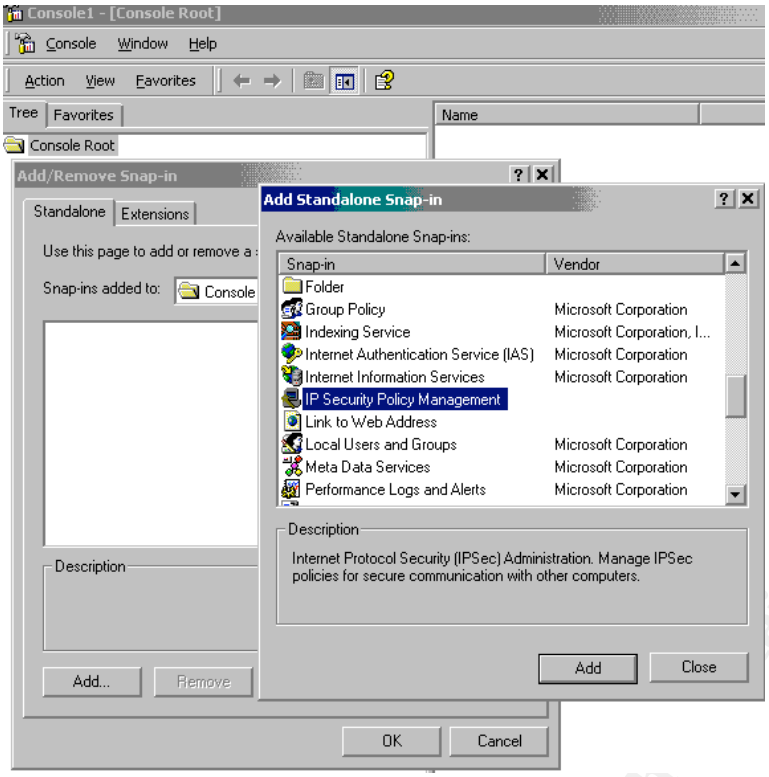


Figure 12

Now click Console > Save As to save the MMC console we have built. Give it a name such as *tools* and save it to the desktop or another folder. Expand the IPSec Policies snap-in and the right window will display a list of default IPSec policies for the domain. Right click each policy and select "Delete" from the menu. We will build our own custom policies. After deleting the policies we must stop a moment to plan our IPSec policies. These policies are similar to firewall rules in that we must define when to use IPSec and where we will use IPSec. For our example we will assume there is only one subnet, we have a firewall, and we have a Unix/Linux host that is not configured for IPSec. Firewalls can pass IPSec traffic but in our example we do not want traffic such as web or email going out through the firewall encrypted with IPSec. Also, Unix and Linux are IPSec capable, however that configuration is beyond the scope of this document. IPSec in Windows 2000 consists of policies. These policies are made up of rules, rules contain filter lists, which contain multiple IPSec filters. However, once a filter, rule, or policy has been created in Active Directory, it is accessible for use by other policies or rules. This way just a few rules can cover all IPSec policies in your domain.

First, we want to encrypt all traffic from our computer to all other computers in our subnet. Next, we do not want to send encrypted traffic to the firewall. Finally, we do not want to send encrypted traffic to the Unix machine. To achieve this mix of requirements, we will create one IPSec Policy and in that policy create three rules.

MyComputer	>	10.1.255.255		Encrypt all traffic
MyComputer	>	10.1.1.2	(Unix host)	Do Not Encrypt
MyComputer	>	10.1.1.254	(Firewall	Do Not Encrypt

Here, MyComputer represents *any* computer in the domain that will be sending IPSec traffic. In the IPSec Policy we will enable rule mirroring which in the first example, would make MyComputer accept IPSec traffic from any computer in the 10.1.255.255 subnet as well as send IPSec traffic to any computer in the subnet.

Now that we have defined on paper our IPSec destinations, we will define a policy. Open the "Tools" MMC we created earlier. Right click "IP Security Policies on Active Directory" and select "Create IP Security Policy" from the menu. Click next, then give the policy a descriptive name and detailed description.

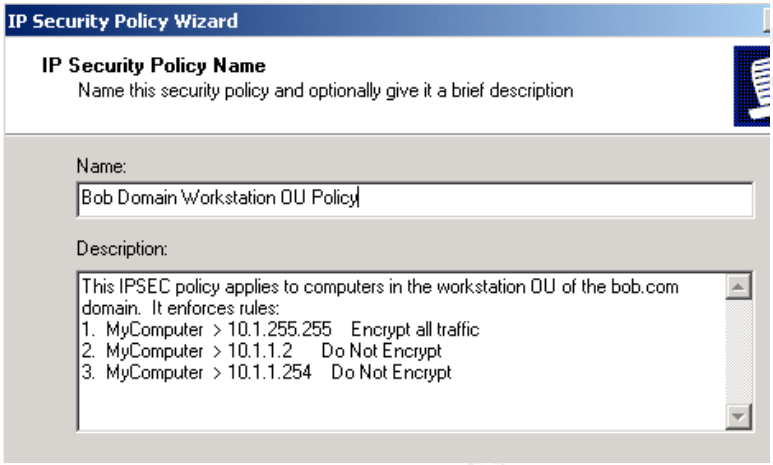


Figure 13

Click "Next" and make sure the checkbox for "Activate the default response rule" is checked. The default response rule is part of every policy, however you can choose to deactivate it. This rule exists only to respond to computers that request or require IPSec. It is a good idea to activate this because you might miss a machine in your rule configuration. On the next window, select the radio button beside "Windows 2000 default (Kerberos V5 protocol). This tells the rule to use Windows 2000 built-in Kerberos authentication. Moving to the next window, make sure the "Edit properties" checkbox is checked and then click "Finish". The "IP Security Policy Properties" window will open. This window has two tabs – Rules and General. The General tab contains the settings for Phase I of the IPSec negotiations and the filter action tab on the rules tab configures the Phase II settings. Phase I will be covered later, first we will address the rules tab.

The rules tab will contain IPSec rules after we create them. To create an IPSec rule, click the add button. The "Rule Properties" window will now open. Click the "IP Filter List" tab and click the "Add" button. In the next window we will configure IP Filters to add to the IP filter list. In the IP Filter List window, clicking the add button will open the filter properties window. The first tab, Addressing, defines the source

and destination address as well as mirroring for this filter. With mirroring enabled if we define the source as our IP address and the destination as another ip, we will also be able to receive IPSec traffic from the origination from the destination IP. Enabling mirroring helps simplify IP filter lists. Set the source address as “My IP Address” and the destination address as “A specific IP Subnet”. Fields for the IP address and subnet mask will appear. Fill these in according to the rules we established on paper earlier.

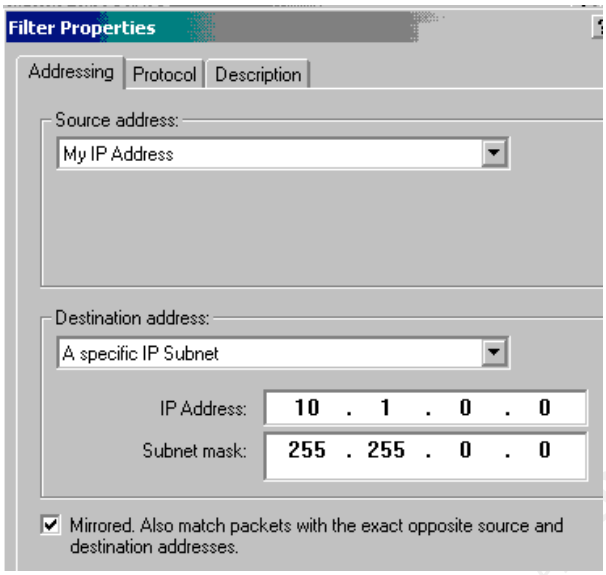


Figure 14

Next, select the protocol tab. Make sure the protocol type is set to “Any”. It is possible to define which specific protocol to apply IPSec filters to, however typically it is best to keep the filters as simple as possible. In the Description field on the Description tab, in detail describe what this filter does. For example, “Filters traffic on all protocols from My IP Address to the 10.1.0.0 subnet. This filter is mirrored.” In the months down the road when you go back to make a change or troubleshoot a problem with IPSec, you will quickly be able to familiarize yourself with your setup if you take the time now to make detailed descriptions. Clicking the “Apply” button will return you to the IP Filter List window. Here you can add more IP Filters. This would be needed if we had other subnets or hosts that we wanted to allow access to. In our example we have one subnet that we are using IPSec on, so we will name this filter and then move to the next step of our setup. Give the IP Filter List a descriptive name such as “My IP to 10.1.0.0 subnet”, enter a detailed description for what filters are contained in the list, and click the “Close” button.

Now that an IP Filter list and IP Filter have been defined, our final step is to tell the rule what action to perform when traffic matches the selected filter. This is where the IPSEC Phase II settings are configured. On the IP Filter List tab select the radio button next to the IP Filter you just setup. Next, click the Filter Action Tab, make sure the “Use Add Wizard” checkbox is not checked, then click the “Add”

button. There are three settings for filter actions – Permit, Block, or Negotiate Security. Permit simply allows unsecured communication with the hosts defined by the filter. Block will block all traffic for the hosts defined by the filter and Negotiate Security allows for secure communication. For our filter we just setup we want to require IPSec on all traffic between My IP address and the 10.1.0.0 subnet so we will select the radio button beside "Negotiate Security". Directly below the three radio buttons is the Security Method list. Click the "Add" button to add a security method for our secure communications. Select the radio button beside the "Custom" security method and then click the settings button below that. A window will open that allows you to define custom security method settings for this filter action. Check the second check box and select SHA1 as the integrity algorithm followed by 3DES for the encryption algorithm. In the "Session Key Settings" session, check both "Generate a new key" checkboxes. In the first one delete the value and enter "500000", in the second box enter "600". These settings define how often new encryption keys get generated. In high security environments such as financial institutions, it is very important to generate new keys often. However, generating new keys too often can cause effects on network performance. Finish defining the custom settings by clicking the "OK" button.

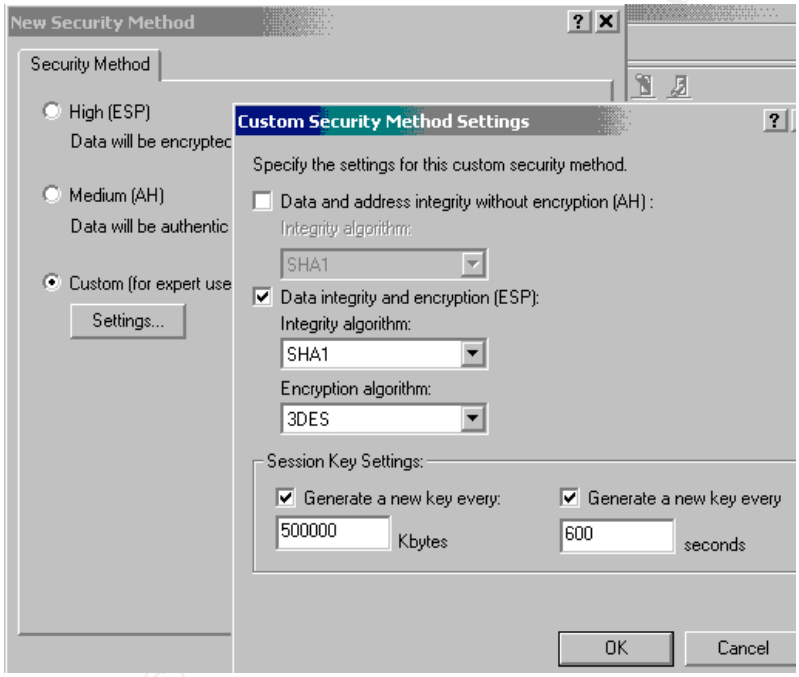


Figure 15

Return to the filter action properties window by clicking the "OK" button in the security method window. The security method just created will be displayed in list form in the Security Method preference order window. More that one security method can exist, enabling machines trying to establish secure communication to negotiate a security method that they both can use. In smaller networks managed by one or a few people, it may be best to have just one security method. The benefits of this are that it is easy to ensure that the most secure security method is

being used and it will be easy to tell if any machines are trying to communicate unsecurely – since they won't be able to communicate at all. In other settings, such as where different OU's are managed by different groups and where many machines are communicating securely it may be necessary to have several security methods to allow machines to successfully negotiate secure communication settings.

Below the Security Method list are three check boxes. Enabling the first checkbox allows your computer to accept communication from computers that are not communicating securely, but your computer responds using IPSec. Basically this will let the other computer know to communicate using IPSec if it can. This is good to enable on your LAN, however on any publicly accessible computer it is best to leave it disabled. So for our example, enable it.

The next checkbox enables unsecured communication with computers who are not IPSec aware. Primarily, this should only be enabled when doing initial testing with IPSec. In section three a tool, called IPSecmon, that shows IPSec details for a machine is covered. After making sure all hosts are communicating securely, then this setting should be disabled because leaving it enable defeats the whole purpose of using IPSec. Make sure this box is not checked.

The final checkbox enables a feature called "Session key Perfect Forward Secrecy" (SKPFS). When this feature is not enabled, when new session encryption keys are needed, they are generated from the original keys. So if an attacker compromised the original keys, the new keys can be generated. With SKPFS enabled, new keys that are not linked to the old keys are generated. This prevents an attacker from being able to generate valid new keys if one key is compromised. Enabling SKPFS may result in performance penalties since generating a new key each time is slower that generating a key based on the old key. However, it is more secure, so we will enable it by clicking the checkbox.

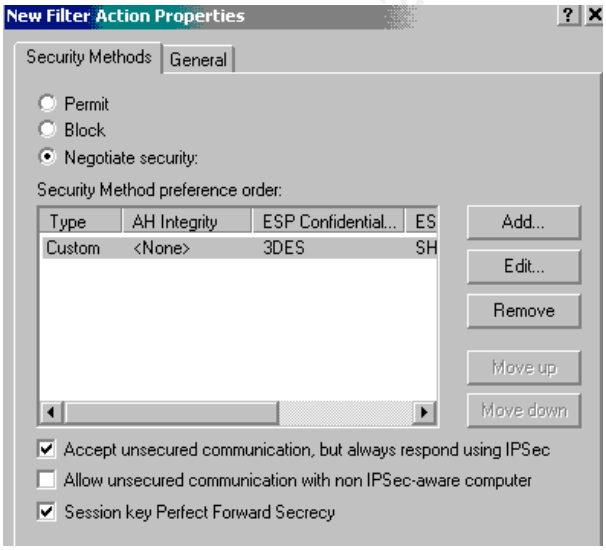


Figure 16

On the General tab, enter a descriptive name for the filter action such as "IPSec Enabled Default" since this will be the default filter action for IPSec. In the

description field, enter a detailed description of what the filter action does such as "Negotiate – ESP Confidential: 3DES, ESP Integrity: SHA1, Key Lifetimes: 500000/600, Accept unsecured, SKPFS". Click the "Apply" button then "OK" to return to the Rule Properties – Filter Action tab. The filter action just created will be displayed. Select the radio button beside it and click the "Connection Type" tab.

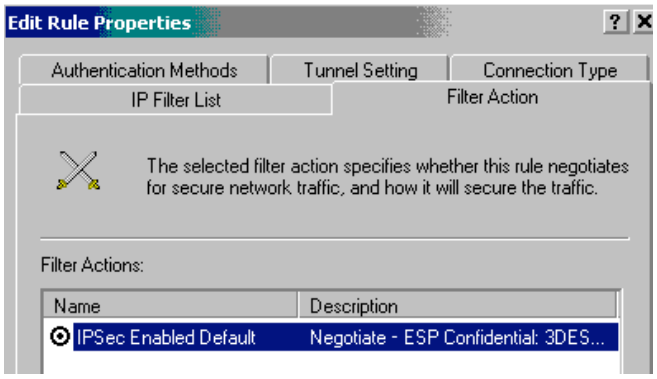


Figure 17

The connection type tab has three radio buttons: All network connections, LAN, and Remote access. This specifies what connections the rule will apply to. In our case, it is best to click the "All Network Connections" radio button. This ensures that any machines connecting remotely will communicate securely. On the Tunnel Setting tab, make sure the radio button beside "This rule does not specify an IPSec tunnel" is selected. Finally, click the "Authentication Methods" tab and make sure kerberos is the only Authentication Method available. If there are other methods, select them and click the remove button. If kerberos is not listed, click "Add", then select the radio button beside "Windows 2000 default (Kerberos V5 protocol)", and click the OK button. In the "Edit Rule Properties" window click the "Apply" button, then click "OK". The Policy Properties window will now display with our newly added rule listed in the list of security rules.

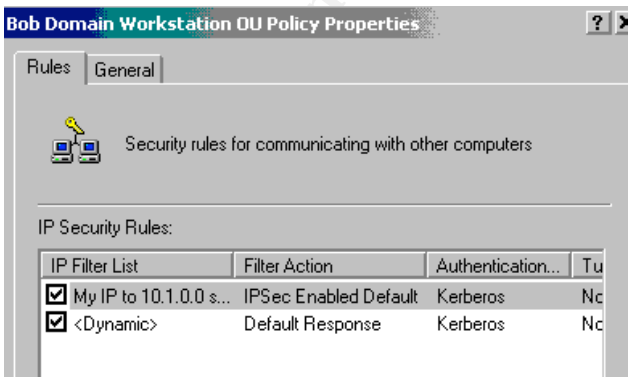


Figure 18

Now that one rule has been created, there are still two rules to create. These rules will each require the creation of IP filter lists, IP filters, and IP filter actions. At

this time, create the next two rules that were defined earlier with the following settings:

MyComputer > 10.1.1.2 (Unix host) Do Not Encrypt

Rule Settings:
Filter List Tab: Add a new filter.

Filter Settings:
Source Address: My IP Address
Destination Address: A Specific IP Address
IP Address: 10.1.1.2
Mirrored: Yes
Protocol: Any
Name: My IP Address to 10.1.1.2

Filter Action Tab: Add a new filter action.

Filter Action Settings:
Security Method: Permit (traffic is unchanged and unsecured).
Name: Permit Unsecured Traffic

Connection Tab:
Connection Type: All Network Connections

Tunnel Setting Tab:
Tunnel Setting: This rule does not apply to an IPSec Tunnel

Authentication Methods Tab:
Authentication Method: Kerberos

MyComputer > 10.1.1.254 Firewall Do Not Encrypt

Rule Settings:
Filter List Tab: Add a new filter.

Filter Settings:
Source Address: My IP Address
Destination Address: A Specific IP Address
IP Address: 10.1.1.254

Mirrored:	Yes
Protocol:	Any
Name:	My IP Address to 10.1.1.254

Filter Action Tab: **Select "Permit Unsecured Traffic" filter action.**

Connection Tab:

Connection Type: All Network Connections

Tunnel Setting Tab:

Tunnel Setting: This rule does not apply to an IPSec Tunnel

Authentication Methods Tab:

Authentication Method: Kerberos

The only differences in these two rules are the IP addresses and not having to define a new IP filter action for the second rule. IP filter lists, IP filter actions, and Policy rules, exist independently of each and can be assigned to other policies, rules, etc. An example is the ability to assign an IP filter list to more than one policy.

So now that the three rules that make up our IPSec policy have been defined, it is time to assign that policy to an OU. First, it is necessary to create another IPSec policy that contains only the default response rule. This will allow a computer to respond using IPSec if another computer requests it. By setting this policy first and allowing sufficient time for it to propagate to all domain members, it will ensure a smooth transition to secure communication. So create a new IP Security policy, name it "Default Response", and enter "Default Response rule only, applied at the domain level" in the description field. Activate the default response rule and select Kerberos authentication. Edit the properties of the new rule and select the "General" tab. Click the "Advanced" button to open the IKE Phase I settings. Enable Master key Perfect Forward Secrecy and then click the "Methods" button. Remove any settings that use DES for encryption or use Diffie-Hellman Low (1) group.

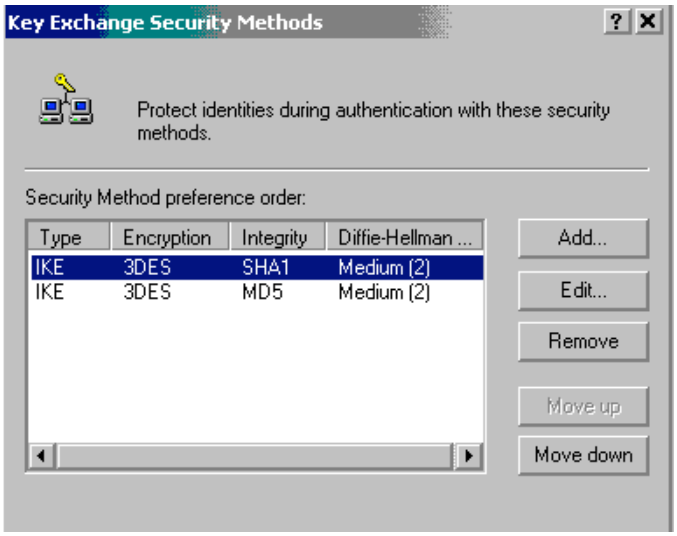


Figure 19

Click OK on the Key Exchange Security Methods window, the Key Exchange Settings window, and the policy properties window.

Now open ADUC and right click on the domain, select properties, then click the group policy tab. Double click the "Default Domain Policy" and browse down the following path on the group policy tree: Computer Configuration> Windows Settings> Security Settings> IP Security Policies on Active Directory. When you click IP Security Policies on Active Directory you will see the policies we have created listed in the right window. To assign the Default Response policy, right click the policy and select assign from the menu. Now close Group Policy and you are finished with the Default Response policy.

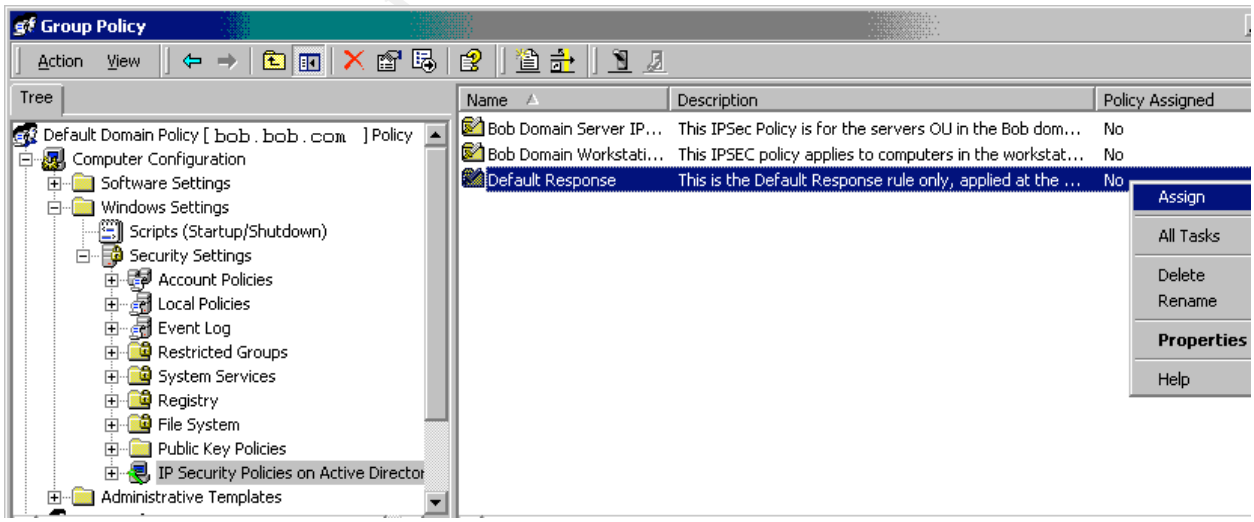


Figure 20

After waiting for the Default Response policy to propagate, it is time to enable our IP Sec policy on an OU. It is important to spend time planning your IPSec implementation. For example, if you have two OU's that have members that must communicate and you enable an IPSec policy only on one of the OU's there will be communication problems on your domain. In our example we will have an OU for servers, and an OU for workstations. A separate IPSec policy has been created for the server OU. This policy is identical to the workstation IPSec Policy. The same policy could have been used for both OU's but two policies were used to minimize impact if changes are necessary to one of the IPSec policies down the road. Now, following the process we used to enable the Default Response policy on the domain, enable the workstation IPSec policy on the workstation OU, followed by the server IPSec policy on the server OU. If possible test your IPSec policy on a test OU before implementing it domain wide. This will enable you to fine tune and trouble-shoot your IPSec policy on a few machines. The tool ipsecmon, discussed in section three, can be run during testing to tell what IPSec sessions are occurring on a machine, and what methods of secure communication are being used. Once finished with fine tuning and testing, the Windows 2000 network will be communicating securely and be compliant with regulatory recommendations.

Host Based Firewall

Utilizing IPSec that is built in to Windows 2000 we will now configure a packet filtering firewall. Again, spend time planning the filters necessary for your network. Envision every type of communication that goes on and then find out what incoming ports that communication requires. In our example we will apply our firewall rules to our domain that is already running IPSec, so we will just have a few filters. First, we will block all traffic to the machine, then allow incoming traffic on TCP Port 50 (ESP Traffic), and incoming traffic on TCP Port 51 (AH Traffic). In this example we have not included any hosts that are not communicating with IPSec.

IP Filters for a Packet Filtering Firewall:

Rule 1:

Filter:	Any IP Address > My IP Address	Block

Rule 2:

Filter:	Any IP Address > My IP Address: TCP 50	Allow
Filter:	Any IP Address > My IP Address: TCP 51	Allow

NOTE: *The IPSec filter action "Block" in Windows 2000 does not mean to reject the packet. It silently drops the packet and DOES NOT send an ICMP unreachable back to the sender. Also, UDP port 500 is needed for IKE negotiation traffic. However, it along with Kerberos traffic (UDP/TCP port 88) are two of the default filter exemptions included in Windows 2000 IPSec filters.*[18]

[18] Microsoft, Traffic That Can--and Cannot--Be Secured by IPSec – Knowledge Base 253169.

These rules will both be created in the IPSec policy that was created earlier, so launch “IP Security Policies on Active Directory”, open the policy properties, and add the following rules:

Any IP Address > My IP Address Block All

Rule Settings:
Filter List Tab: Add a new filter.

Filter Settings:
Source Address: Any IP Address
Destination Address: My IP address
Mirrored: Yes
Protocol: Any
Name: Any IP Address to My IP Address, Mirrored

Filter Action Tab: Add a new filter action.

Filter Action Settings:
Security Method: Block (traffic is dropped).
Name: Block All Traffic

Connection Tab:
Connection Type: All Network Connections

Tunnel Setting Tab:
Tunnel Setting: This rule does not apply to an IPSec Tunnel

Authentication Methods Tab:
Authentication Method: Kerberos

Any IP Address > My IP Address:50,51/TCP Permit

Rule Settings:
Filter List Tab: Add a new filter.

#1 Filter Settings:
Source Address: Any IP Address
Destination Address: My IP Address
Mirrored: Yes
Protocol: TCP
Set the IP protocol port: To this port: 50
Name: Any IP Address to My IP Address TCP port 50

#2 Filter Settings:
Source Address: Any IP Address

Destination Address:	My IP Address
Mirrored:	Yes
Protocol:	TCP
Set the IP protocol port:	To this port: 51
Name:	Any IP Address to My IP Address TCP port 51

Filter Action Tab: Select "Permit Unsecured Traffic" Filter Action.

Connection Tab:
Connection Type: All Network Connections

Tunnel Setting Tab:
Tunnel Setting: This rule does not apply to an IPSec Tunnel

Authentication Methods Tab:
Authentication Method: Kerberos

Figure 21 - Protocol Selection for IPSec Filters

Note: *For initial testing and fine-tuning of the IPSec packet filtering firewall, it is advisable to create a new IPSec policy, add the rules and filter actions that were configured in the* ***Network Encryption*** *section, and then add the rules for packet filtering. Then assign the new IPSec policy to a test OU.*

Authentication Methods

Our recommendation states that we should require use of NTLMv2 and Kerberos authentication methods while disabling use of other less-secure methods. This setting can be configured across your entire domain using Group Policy. To do this, open ADUC, right click the domain name, and click properties. Select the Group Policy tab and double click the Default Domain policy. Next, in the Group Policy window, navigate the following path: Computer Configuration > Windows Settings > Security Settings >

Local Policies > Security Options. In the right windowpane, double click the "Lan Manager Authentication Level" policy. Check the "Define this policy setting" checkbox, and select the setting "Send NTLMv2 response only / refuse LM & NTLM". Click OK and you are done with part of the configuration. Wait to allow propagation of this policy to all domain systems before setting this on the Domain Controllers OU. If we set the Domain Controllers GPO to use only NTLMv2 and to refuse LM & NTLM, then we could end up with a situation in which some systems cannot communicate with the Domain Controllers, and therefore couldn't update their Group Policy. So after allowing sufficient propagation time, the same step must be performed on the Domain Controllers OU.

Note: *This is one setting that should be tested on a test group of computers first. Set the GPO on the Domain Controllers to "Send LM & NTLM – use NTLMv2 session security if negotiated". This will allow you to see if any authentication problems develop between the computers in the test group and the Domain Controllers. Potential problems could also develop between computers in the test OU and application servers not using NTLMv2. It would be possible to create a Servers OU, move all server machine accounts to it, and then set it's GPO Lan Manager Authentication Level setting to "Send LM & NTLM – use NTLMv2 session security if negotiated". Then when you have all issues ironed out change the Lan Manager Authentication Level on groups of machines in an organized manner, allowing time for settings to propagate before changing the next group.* ***This is definitely a policy setting that you do NOT want to configure on the Friday afternoon before you leave for vacation!***

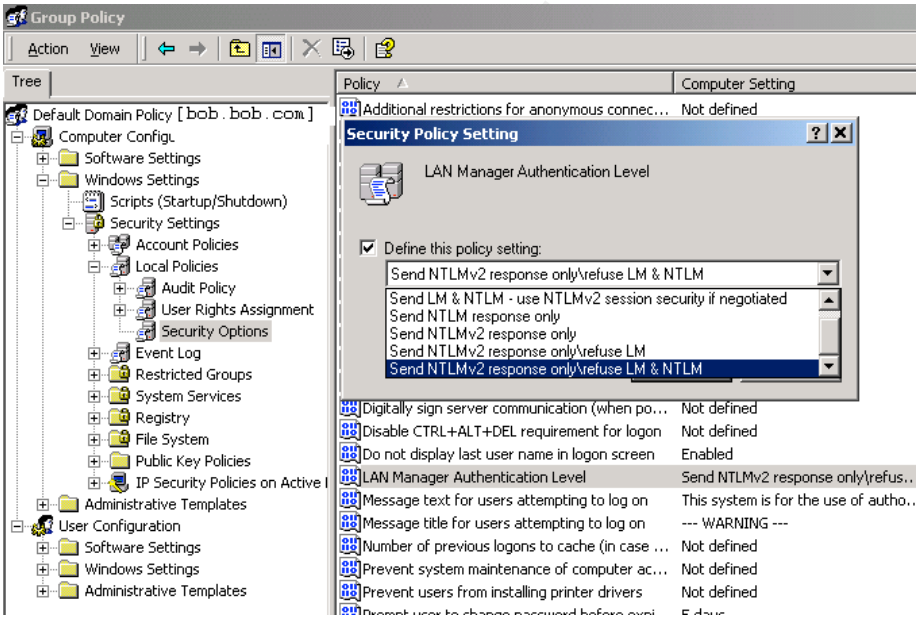


Figure 22

Remove Lan Manager Hash

The next module deals with how passwords are stored on Domain Controllers. In this section we will add a key and a value to the registry on each Domain Controller. First, it is important to note that some older applications may require the LM hash. You probably will have identified any problems when you set the LM Authentication Level in the previous section. It would be wise to call your application vendors to ask what kind of Windows authentication their application uses. To remove the LM hash, complete the following steps on each domain controller:

1. Click the Start button, go to run, and type "regedit" in the open box. Click the "OK" button. The registry editor will open. Expand the tree on the following path: HKEY_Local_Machine > System > CurrentControlSet > Control > Lsa. Left click to highlight "Lsa", then right click and select New > Key from the menu (1). Name the key "NoLMHash". Next click on right click on Lsa again and select New > DWORD Value from the menu.

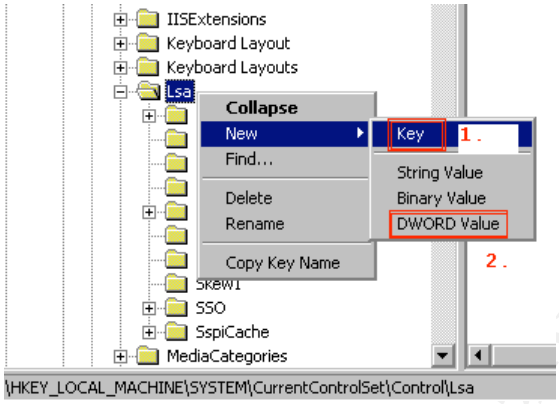


Figure 23

Name the value NoLMHash, and then double click the NoLMHash DWORD value and set the value to 1.

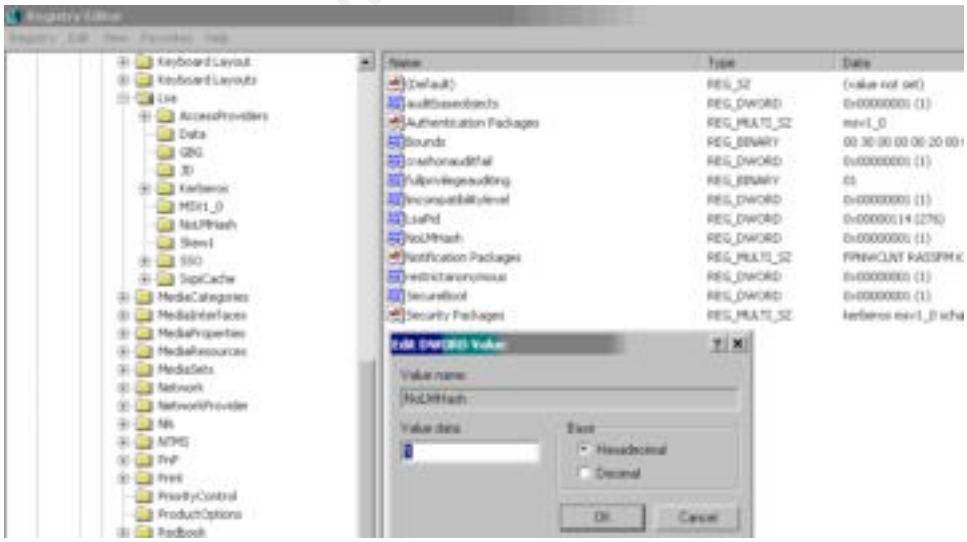


Figure 24

You should now have added two values to the Lsa key: A subkey NoLMHash and a DWORD value of NoLMHash. Make sure that the NoLMHash DWORD did not get created in the NoLMHash key. Select the NoLMHash key (a yellow folder under Lsa) and you should see a single value named "Default" in the right window.

The LM hash is not automatically removed from Active Directory and the local SAM database. It is removed only when the user resets their password. So from the time you make the registry settings on each domain controller, it could be thirty days until all LM hashes are gone. We will look further into this in the audit section using a tool called ***L0phtCrack***.

Change and Secure Local System Credentials

Earlier the need to secure the local system accounts was discussed. Luckily, some of these changes can be made to all computers through group policy. However, some settings will require a visit to each machine. We will look at the GP settings first.

With Group Policy we can change the username on the administrator and guest accounts on the local pc. You can unique account names for each OU, or have the same unique name for the whole domain. We will focus on renaming the accounts at the Default Domain Policy level.

1. Open ADUC, and right click the domain name. Select properties from the menu, and select the Group Policy tab. Double click the Default Domain Policy to edit the GP. Browse down the GP tree following this path: Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options. In the list of policies in the right window pane, double click the name of the policies below, check the "Define this policy setting checkbox" and enter the name that you would like to rename the account to. Make it something easy to remember, but hard to guess for an attacker. The policies to edit are:

    - Rename administrator account
    - Rename guest account

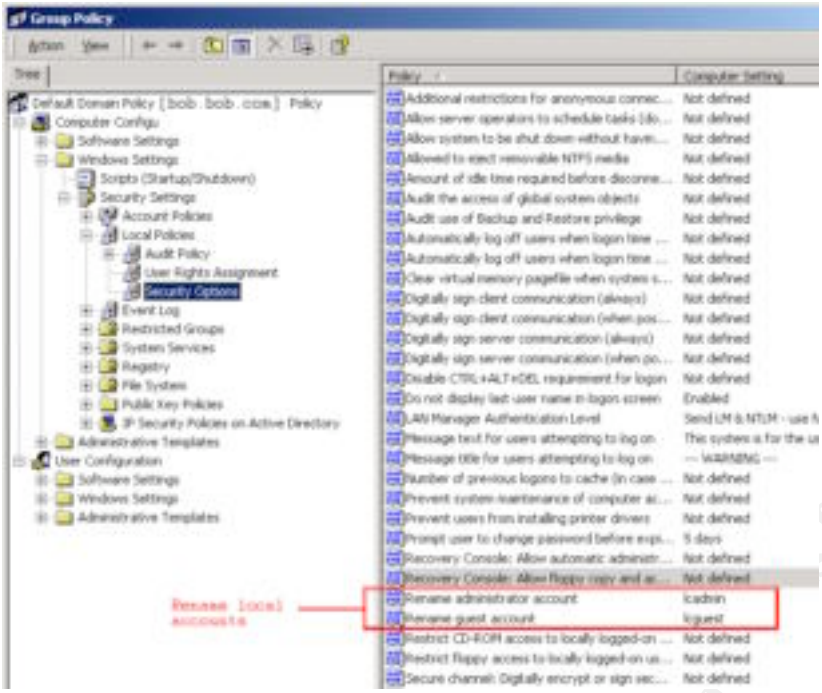


Figure 25

The last step in securing local system credentials is setting a strong password, setting that password to expire, and disabling the accounts if possible. This can be done as part of a monthly patching visit. To do this, logon to each system as an user with administrative rights to the local system. Right click on the My Computer icon and select “Manage” from the menu that appears. This opens the Computer Management console. From here you can control many aspects of the local computer. Browse down the following path on the tree: Computer Management (Local) > System Tools > Local Users and Groups > Users. In the right window you will see the local accounts listed. In the figure below, Group policy has already renamed them. Double click on each account to bring up its properties window. In the properties window uncheck the “Password never expires” checkbox and check the “Account is disabled” checkbox. Iron out any problems by disabling accounts on one computer before making the changes on all machines.

Note: *The local administrative account cannot be disabled.*

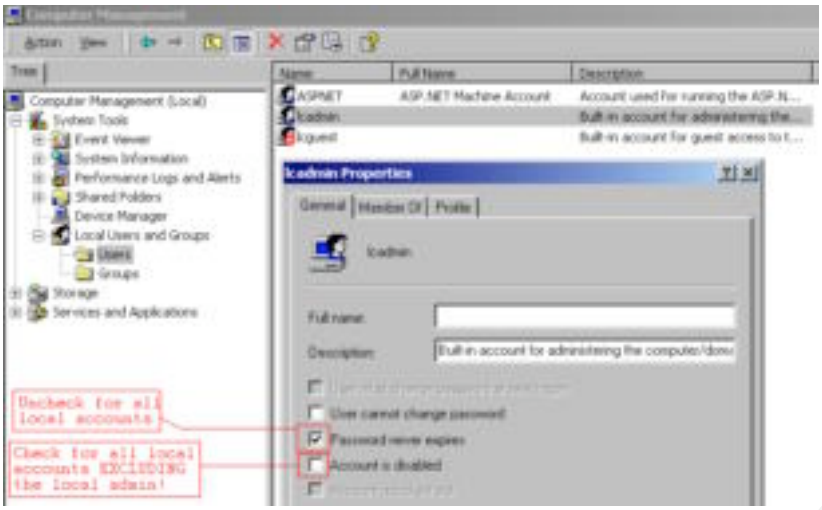


Figure 26

Now we will finish with setting a secure password. This password should be a strong password that matches your password policy. Also, since these passwords may change only once a year and are rarely used, make them at least twelve characters long. Do not make the local account passwords the same as the password on your domain admin account. If you do, compromise of a local account on one system could result in a root level compromise of the whole domain! To set the password, right click on the local account name and select “Set Password” from the menu. Enter the new password, enter it again to confirm, then click the “OK” button.

After testing the local account changes and implementing them on all systems in your domain, you have a local account configuration that is more secure than the default, and you have added one more layer to your defenses.

Section Three

Ensuring Baseline Compliance – Now and in the Future

This section details how to perform a basic audit of the modules of the established baseline. The goal is to verify that the settings are in effect in the easiest way. This approach is designed to be quick and easy to perform. In areas that more advanced audit tools would also prove beneficial the tools will be briefly discussed.

Password Complexity

The simplest way to check password complexity settings is to check the Account Policies settings in the Domain Controllers Group Policy Object. Check these settings by retracing the steps used to configure the password complexity settings in section two. Consult section one and make sure that the section one settings match the settings that are configured in section two. Also check the Passfilt Pro policy in the Domain Controllers Group Policy Object for matches to the password policy in section one.

Another more in-depth way to audit password complexity is to run a program that attempts to "crack" passwords by brute-force guessing or other means. A very popular and powerful program is L0phtCrack (LC5). L0phtCrack is a product of @*stake*, which was recently purchased by *Symantec*. A trial version was previously available but now it appears that you must purchase L0phtCrack to test it. It is a very good tool to have to use in auditing passwords and is relatively inexpensive. More information on L0pthCrack can be obtained from http://www.L0pht.com .

Physical Access

To check the physical access settings defined in section one simply check the timeout setting on several randomly picked workstations in the financial institution. To do this right click on the desktop, select properties from the menu, then click the "Screen Saver" tab. The wait time should be set at five minutes and you should not be able to change the screen saver settings. The wait time can be adjusted, but if you save, close, and reopen the display properties you will see that the time has reverted to five minutes.

Disable Unneeded Services

Auditing the services running on a sampling of random workstations is achieved by comparing the list of services that are disabled for that particular system to the local services that are disabled in the Services snap-in. This snap-in is available in the Administrative Tools folder in the Control Panel. The CIS Windows Security Scoring Tool, discussed in the next paragraph, also compiles a list of non-default services on the local machine and their running state.

Secure Registry Settings and Secure File System Settings

The most efficient way to audit registry settings and file system settings as well as overall security of a system is to run the CIS Windows Security Scoring Tool that was included the W2kProGold security template that was applied via Group Policy. The tool

compares security settings on the local computer to the settings in the specified template. Launch the tool, select the W2kProGold template, and click "Score". After a few minutes the following report will display, and you will receive a score between one and ten, with ten being perfect.

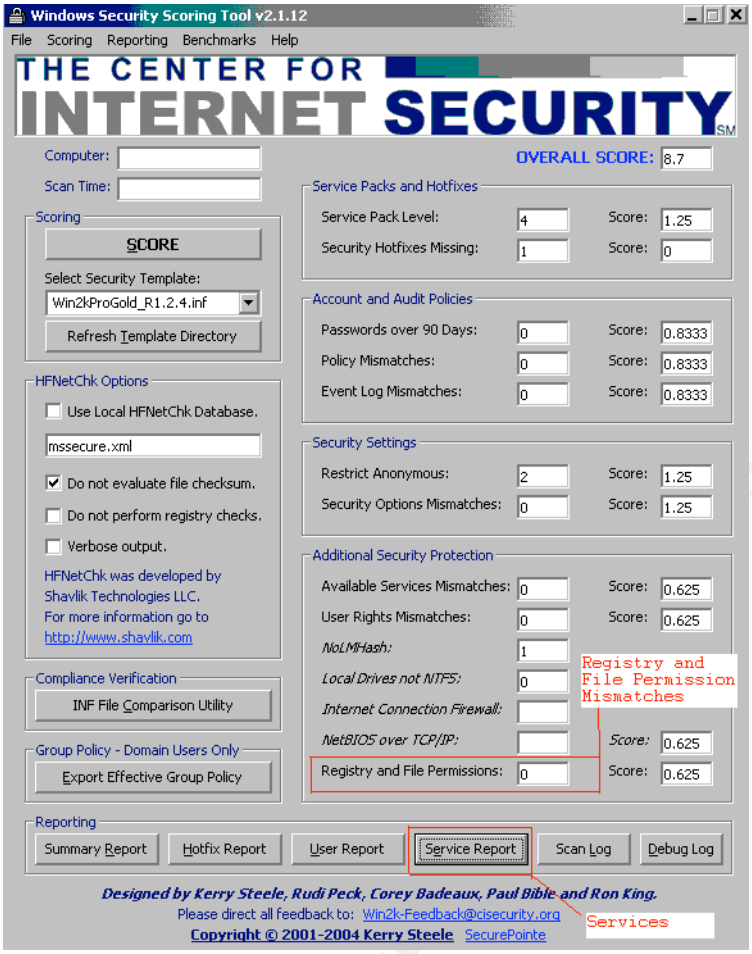


Figure 27

If you have customized any services, registry permissions, or file permissions, then it will be difficult to score well. It is possible for you to export a custom security template from Group Policy that matches your domain settings and then test against the custom template. See **"***Creating a Custom Security Template Using the MMC Snap-in"*[19] for information on creating a custom security template.

Data Encryption

Encryption on Disk

The are two quick and easy ways to ensure that sensitive data is being encrypted using the EFS feature of Windows 2000. As a standard network user that has NTFS read permission to the file but does not own the encrypted file, right click the file or

[19] MSDN, Creating a Custom Security Template Using the MMC Snap-in.

folder, select properties from the menu, and then click the “Advanced” button in the properties window for the file or folder. A window showing Advanced Attributes will open. If the file or folder is encrypted the “Encrypt contents to secure data” checkbox will be checked.

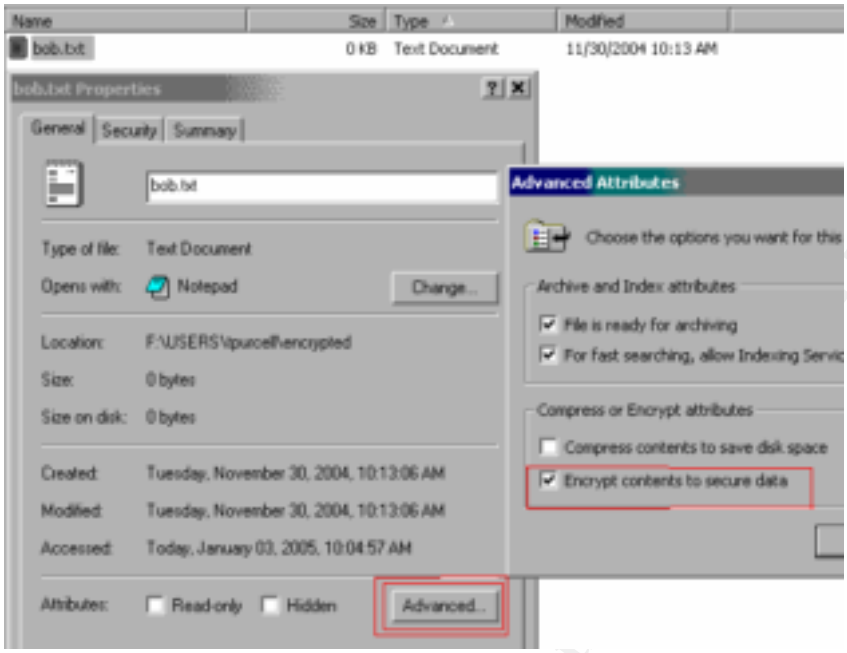


Figure 28

Another way to check encryption is to try to open the same file using a text editor. In the following example, I try to open an encrypted Excel spreadsheet that I have NTFS read permissions on, but belongs to spiffy.

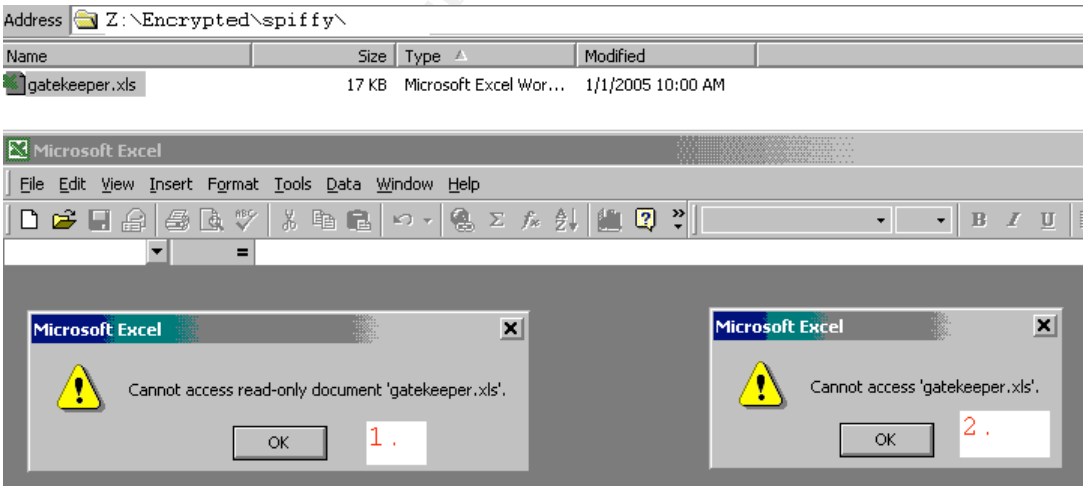


Figure 29

Excel returns a couple of misleading errors, first reporting that it cannot access a read-only document, then just saying it can't access the document. It never says that the file is encrypted, but we didn't get access.

Network Encryption

Windows 2000 provides a tool for monitoring IPSec communication statistics called IPSecmon. This tool, discussed in more detail in section three, provides a list of all active associations, their security method, name of the filter, and the source and destination address of the association. It also provides statistics that are useful for troubleshooting IPSec. In our case it is a quick and easy way to ensure that machines are communication securely. Simply run it locally on several random machines. It is also beneficial to run on a domain controller, since every domain member must communicate through the domain controller.

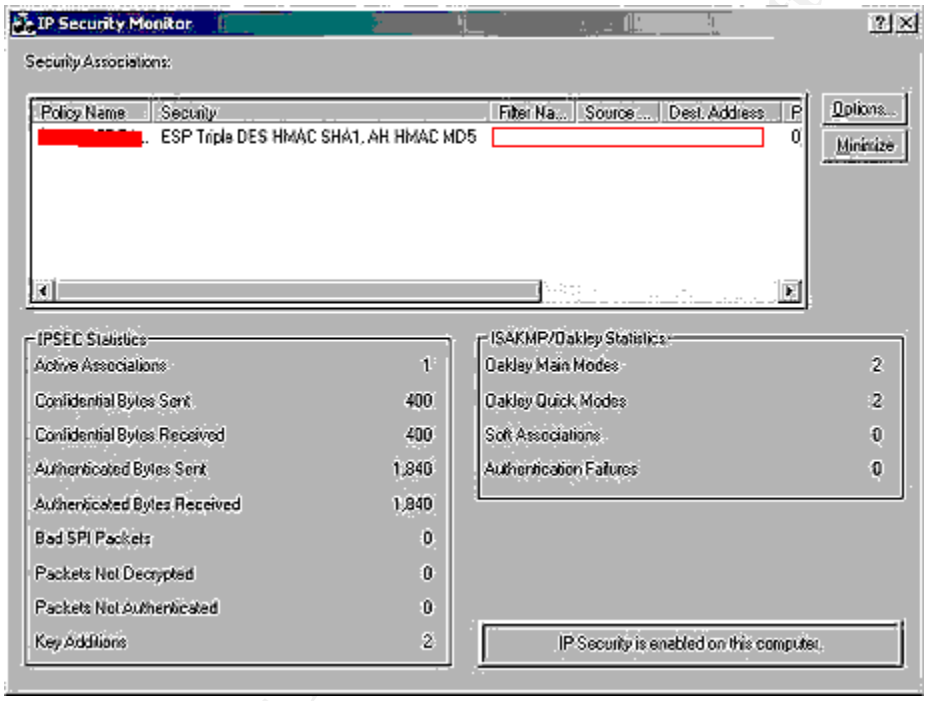


Figure 30

Change and Secure Local System Credentials

In section two when the local system credentials were changed using active directory, the credentials were also secured by disabling all local accounts possible, setting strong passwords, and setting passwords to expire. Auditing these settings is performed by taking a random sample of workstations and comparing the local account settings to the settings recommended for local accounts in the baseline. These settings could be audited remotely by using the "Computer Management" MMC. This is accessible by right clicking on the My Computer icon, selecting "manage" from the menu, and then browsing to System Tools> Local Users and Groups> Users. To access a remote computer, right click "Computer Management (Local)", select "Connect to another Computer", enter the name, and click the "OK" button.

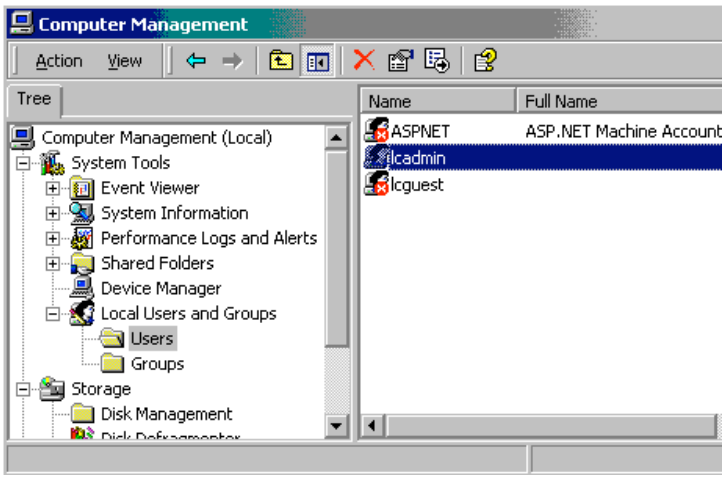


Figure 31

Host Based Firewall

Auditing host based firewall settings is slightly more involved than auditing other baseline modules. Here we must scan a computer with a port scanner to see which ports respond as being available. A tool called Nmap (Network Mapper) is the tool of choice for this task. Nmap is available for free at http://www.insecure.org/nmap/ . Nmap was developed on Linux, however a Windows port has been made to enable users to run it from Windows computers. If you are unfamiliar with Linux, either download and install the Windows version according to the instructions on the nmap website, or download Knoppix. Knoppix is a Linux distribution that fits on a cd. You download the ISO image, burn it to a CD, and then boot from the CD. Everything runs from CD, and it does not touch your harddrive. This will enable you to run Linux on any PC and give you access to tools such as Nmap. Knoppix download and install instructions are available at http://www.knoppix.org/ .

Run Nmap from the command prompt with the following command:

```
[bob@bob bob]# nmap -sS -p 1-65535 10.1.1.33
```

In the above example, -sS tells nmap to use a “half-open” scan. This scan does not complete a full TCP connection on each port. “ –p 1-65535” tells nmap to scan ports 1 through 65535 and 10.1.1.33 tells nmap the IP address of the host to scan. It must be noted that some nmap functions require root access to run. Use Sudo if this is the case. Don’t execute as root!

Once Nmap is done running, you should see results similar to this:

```
[bob@bob bob]# nmap -sS -p 1-65535 10.1.1.33

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Note: Host seems down. If it is really up, but blocking our ping probes, try
-P0
Nmap run completed -- 1 IP address (0 hosts up) scanned in 30 seconds
```

Run nmap using the –P0 option instead of –sS . It will take a long time if the machine is properly firewalled, but it should report the ports that are actually open.

Authentication Methods

To ensure proper authentication methods are being used on machines in the domain, check the registry setting that was initially configured in section two. It should reflect the setting of "Send NTLMv2 response only / refuse LM & NTLM". To check this setting click Start> Run, enter "regedit" the open field, and click OK. Once regedit has launched, browse down the following path: HKEY_Local_Machine> System> CurrentControlSet> Control> LSA. The dword value "lmcompatibilitylevel" in the right windowpane should be set to "5" for highest authentication security. Keep in mind that program restrictions on your domain may have forced you to use a less secure method of authentication. If that is the case make sure the reason for use of this method is documented. Check this setting on several random computers in your domain to ensure that this Group Policy setting is in effect everywhere.

Remove Lan Manager Hash

The final audit module has two ways to check for removal of the Lan Manager Hash. First, the previously mentioned L0phtCrack tool, as part of it's cracking process displays the LM hash as well as the NTLM hash. If the LM Hash is not being stored on the domain controller, a L0phtCrack audit of the passwords will show the values in the LM Hash column to all be the same. This has is basically a "null" hash, and L0phtCrack interprets the account as having no password. However, the NTLM hash column will have a different password hash for each account. The following screenshot is from L0phtCrack 4.

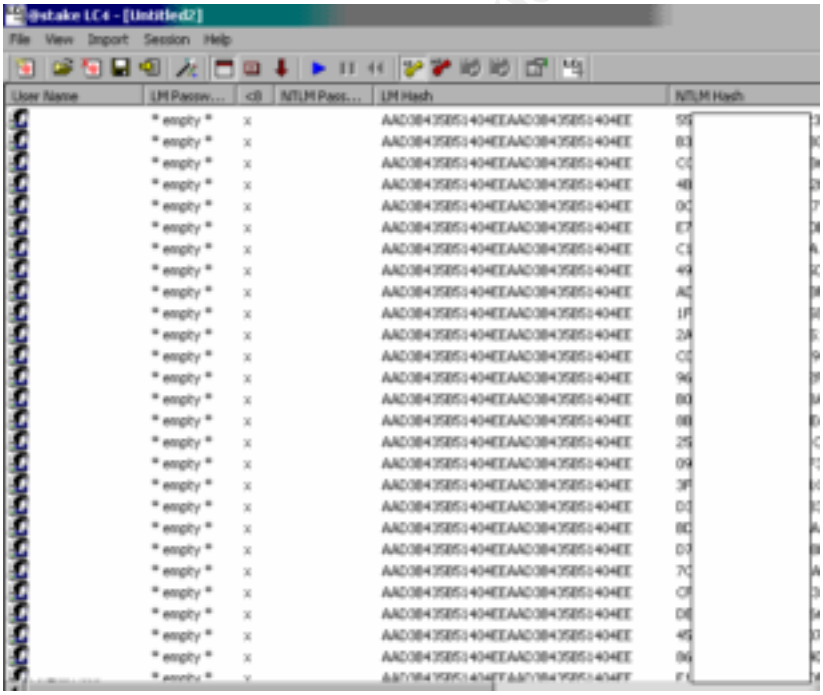


Figure 32

The final way to audit the removal of the LMHash is to see if the registry settings added in section two exist. Under the LSA key in the registry, a subkey of NoLMHash should exist. Also under the LSA key a DWORD value of NoLMHash should exist. The value of the NoLMHash DWORD should be 1. Check these registry settings on all domain controllers.

Conclusion

In the financial institutions of today technology is being used more and more. With the growth of technology comes increased risk since valuable customer information is potentially accessible to malicious persons all around the world. Groups such as the FFIEC, OCC, and the Federal Reserve have made regulatory recommendations. However, a firm baseline security standard was still needed to help financial institutions interpret these recommendations, ensure that their networks are secure, and to perform basic technical audits of these networks. This document has interpreted regulatory recommendations to create a modular baseline, detailed the steps necessary to configure each module of the baseline, and then provided basic audit steps to ensure baseline compliance.

While it may not be possible for every financial institution to implement each module of the baseline, as many as possible should be implemented and perhaps required. A higher level of security at each financial institution coupled with a more technical audit of financial institutions will continuously raise the level of security, which is necessary due to the increasing risks of using technology. Raising the levels of security in our financial institutions has one goal: to protect the information of our customers. Protecting a customer's information is our responsibility – after all they are our customer.

Appendix

Active Directory and Group Policy

With the introduction of Windows 2000 Server, Microsoft drastically changed the way that domain information is handled. This change was Active Directory. Active Directory is a database that contains information on items such as user accounts, passwords, groups, Group Policy, computer accounts and properties, Exchange Server 2000 information, printers, and many others. In addition to user groups, and mail groups AD allows for further grouping through Organizational Units (OU). OUs are the last logical structure element of Active Directory that stacks up like this:

Forests ⇒ Trees ⇒ Domains ⇒ Organizational Units.

Our focus will be on single domain implementation with multiple OUs. OUs are useful for separating users and computers into more focused groups. A couple of examples would be an OU for each FI location, OUs for computers located in high security areas, and a test OU. Creating OUs is a straightforward process. First, install the Windows 2000 Administration Tools found on your Windows 2000 server cd. They are in a MSI file named ADMINPAK.MSI, locate in the i386 directory. These tools can be installed on any computer in the domain, however you would not want to install them on every computer in the domain. Once the admin tools are installed open the Settings ⇒ Control Panels ⇒ Administrative Tools folder. Next, click on the *Active Directory Users and Computers* (ADUC) shortcut. This will open and display the Active Directory Users and Computers console. On the left side of the window, you should see your domain with a container tree below it. Some of these folders are Computers, Domain Controllers, and Users. If these containers are hidden click the "+" sign next to the domain name to expand the tree. The Computers, Domain Controllers, and Users containers are all OUs. To create a new OU, simply right click on the domain and select "New Organizational Unit". Give it a descriptive name and the OU is created. To move users or computers to the new OU, browse to the objects current OU, right click the object and select move. A window will open allowing you to select the destination OU, select it and click "FINISH". Now in the left window, click the OU that was just created and you should see the item that was just moved in the right window.

We will be dealing primarily with one feature of AD that is known as Group Policy (GP).[20] Imagine a company where employees conform to policy continuously. This company also has an all-seeing boss that reminds employees of policy periodically and enforces policies if necessary. Now, replace the company with a Windows 2000 domain and the boss becomes Group Policy. Group Policy is a set of settings (or policies) that can be applied to Local Computers, Sites, Domains, or OUs. Order of enforcement is each policy overrides all previous policies. So a setting in a GP on an OU will override Domain, Site, and Local Computer settings for the same item. (Setting

[20] Microsoft has a technical overview document titled "Windows 2000 Group Policy" that is a good guide to understanding Group Policy.

the No Override option on a domain GPO will keep an OU's GPO from overwriting the domain GPO settings.) Multiple Group Policy Objects (GPO) can exist in each domain, and more than one can apply to each domain or OU. Each GPO consists of two configuration groups – Computer Configuration and User Configuration.
Now that you have a vague idea of what Group Policy is, it is time to look at the internals of a GPO. Open ADUC and right click on the name of your domain. Click properties and then select the Group Policy tab. Select the Default Domain Policy and click the edit button. This will open the Group Policy window. In the left windowpane you will see the Computer Configuration and User Configuration sections. Click the + to expand each tree. Each section has multiple sections below it. Drill down through the folders on the Computer Configuration tree following this path: Windows Settings> Security Settings> Local Policies> Audit Policy. The Audit policy settings will be displayed in the right windowpane. Double click on the "Audit account logon events" policy setting and a window will pop up with the specific options for that item. Click "Cancel" to close without making changes. Take the time to explore and become familiar with what is available in Group Policy. Based on the author's experience, it is also important to note that using Group Policy requires patience. It takes time for changes to GP to replicate throughout the domain. Plan on making a GP change and then waiting for the changes to occur.

Applying the CIS Windows 2000 Gold Security Template

1. Download the Windows 2000 Workstation template and security-scoring tool from http://www.cisecurity.com/sub_form.html .
2. Execute the CIS_Win.exe file to install the Windows 2000 Security Scoring Tool. The default installation path is in C:\Program Files\CIS
3. Once the install is finished browse to the C:\Program Files\CIS\templates directory and copy the file "Win2kProGold_R1.2.4.inf" to C:\WINNT\security\templates. (The template you download may be more recent, just be sure to the Win2kProGold template).
4. As an administrator, apply the template on a non-production Windows 2000 workstation using the following command on the command line: (The command is entered all on one line).

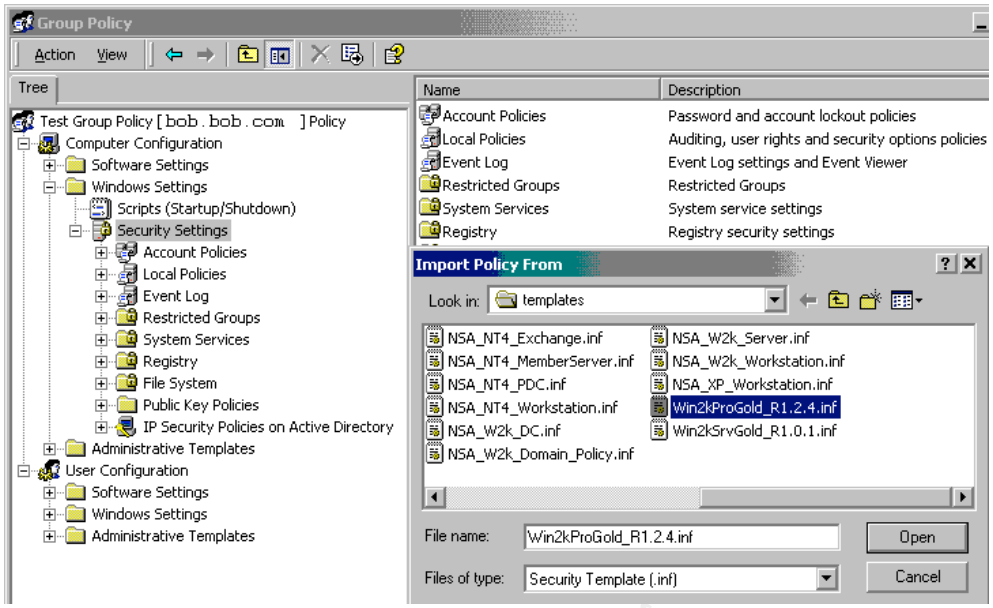
```
C:\>secedit /configure /verbose /db
c:\winnt\security\db\Win2kProGold1.2.4.sdb /log
c:\winnt\security\logs\Win2kProGold1.2.4.log /cfg
c:\winnt\security\templates\Win2kProGold_R1.2.4.inf
```

5. Reboot the computer.

The previous steps configure a single system according to the template. Now we will see how to configure many systems using Group Policy.

1. Launch ADUC and open Group Policy on a test OU. Browse down and right click on Security Settings. A menu will appear, select "Import Policy". A window will

display allowing you to select a policy to import. Locate the Win2kPro_R1.2.4.inf file, select it, and click open.



The settings contained in the Win2kProGold template will now be imported into Group Policy on the test OU. If there were any conflicts with previously configured GP settings then the template will overwrite them. After importing the template into the test OU Group Policy, browse through the Security Settings to fine-tune the policy for your institution.

After exiting group policy, the new settings will propagate to the members of the test OU and the machines will have been hardened with the Win2kGold security template.

References

Seaman, Joseph. "Gramm-Leach-Bliley Act Title V Complexities and Compliancy for the Community Banking Sector." November 22, 2002. http://www.sans.org/rr/papers/14/911.pdf . (4 Oct. 2004)

"Gramm-Leach-Bliley Act, 15 USC 6801 and 6805(b)." November 1999 http://www.ffiec.gov/ffiecinfobase/resources/info_sec/con-15usc_6801_6805-gramm_leach_bliley_act.pdf . (4 Oct. 2004).

Federal Deposit Insurance Corporation. "Financial Institution Letters: Authentication in an Electronic Banking Environment." August 8, 2001. http://www.ffiec.gov/ffiecinfobase/resources/info_sec/fdi-fil-69-2001-authentication_in_electronic_bank_environ.pdf . (4 Oct. 2004).

Federal Deposit Insurance Corporation. "Financial Institution Letters: Security Monitoring of Computer Networks." October 3, 2000. http://www.ffiec.gov/ffiecinfobase/resources/info_sec/fdi-fil-67-2000-security_monitoring_computer_nets.pdf . (4 Oct. 2004).

Office of the Comptroller of the Currency. "OCC Bulletin: Guidelines Establishing Standards for Safeguarding Customer Information." February 15, 2001. http://www.ffiec.gov/ffiecinfobase/resources/info_sec/occ-bul_2001_08_guideline_stand_safegud_cust_info.pdf . (4 Oct. 2004).

Office of the Comptroller of the Currency. "OCC Alert: Network Security Vulnerabilities." April 24, 2001, (Alert 2001-4) http://www.ffiec.gov/ffiecinfobase/resources/info_sec/occ_alert-2001_04_network_security_vulnerabilities.pdf . (4 Oct. 2004).

Kite, Shane. "Shifting Gears: Tackling IT Security When a Bank Grows." Bank Technology News, Vol. 17 No. 08 (August 2004): 44.

Federal Financial Institutions Examination Council (FFIEC). "IT Examination Handbook." December 2002, http://www.ffiec.gov/ffiecinfobase/booklets/information_security/information_security.pdf . (4 Oct. 2004).

Shawgo, Jeff. "Windows 2000 Professional Operating System Level 2 Benchmark Consensus Baseline Security Settings." The Center for Internet Security, September 02, 2003. http://www.cisecurity.com/bench_win2000.html . (4 Oct. 2004).

Murphy, Michael. "Authentication in Windows NT and Windows 2000." May, 2001.

http://www.giac.org/practical/Michael_Murphy_GCNT.doc . (4 Oct. 2004).
Fossen, Jason. "Windows 2000/XP/2003 Active Directory"–SANS Institute, 2004

Fossen, Jason. "Windows 2000/XP/2003 Group Policy and DNS"–SANS Institute, 2004

Fossen, Jason. "Windows 2000/XP/2003 IPSEC and VPNs"–SANS Institute, 2004

Fossen, Jason. "Windows 2000/XP/2003 PKI, Smart Cards and EFS"–SANS Institute, 2004

Microsoft Developers Network. "Creating a Custom Security Template Using the MMC Snap-in." September 2004, http://msdn.microsoft.com/library/default.asp?url=/library/en-us/xpehelp/html/xetbscreatingcustomsecuritytemplateusingmmcsnap-in.asp (3 Jan. 2005).

Microsoft. "Traffic That Can--and Cannot--Be Secured by IPSec – Knowledge Base 253169." September 2003, http://support.microsoft.com/default.aspx?scid=kb;en-us;253169 (3 Jan. 2005)

Weber, Chris. "Using IPSec in Windows 2000 and XP, Part 1" December 2001, http://www.securityfocus.com/infocus/1519 (3 Jan. 2005).

Weber, Chris. "Using IPSec in Windows 2000 and XP, Part 2" December 2001, http://www.securityfocus.com/infocus/1526 (3 Jan. 2005).

Weber, Chris. "Using IPSec in Windows 2000 and XP, Part 3" January 2002, http://www.securityfocus.com/infocus/1528 (3 Jan. 2005).

RSA Laboratories. "What is DESX?" http://www.rsasecurity.com/rsalabs/node.asp?id=2232 (3 Jan. 2005).

Webopedia. "IPSec" May 2004, http://www.webopedia.com/TERM/I/IPsec.html (3 Jan 2005).

Microsoft. "Windows 2000 Group Policy" July 2000, http://www.microsoft.com/windows2000/techinfo/howitworks/management/grouppolwp.asp (3 Jan 2005).