Global Information Assurance Certification Paper

GIAC - Auditing NT

PRACTICAL ASSIGNMENT FOR SANS – New Orleans 2001

Prepared by

Satnam Bhogal

Introduction

This paper defined the requirements for GIAC Certificated in NT Security. This paper takes an individual through the necessary steps and guidance required to audit and tips on securing Windows NT Server including threats and vulnerabilities and how to address them. The format used in this paper has been based on questions and answers. I would strongly advice individuals to research on their own before using this paper.

1. Is Windows NT default installation secure?

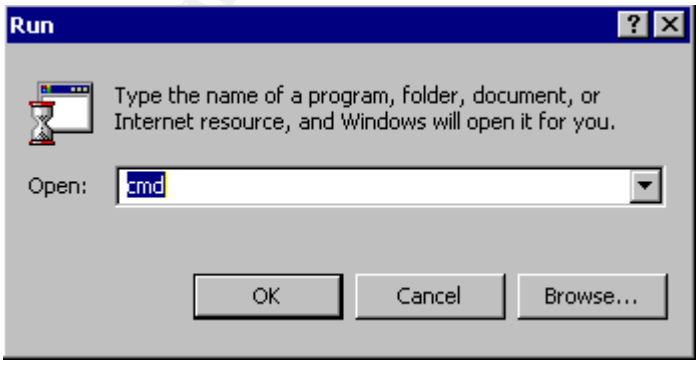
No. The installed version (out-of-the-box) of Windows NT is not configured securely. The initial installation of this operating system is wide open with full access for all users including the group "Everyone" and the guest account. I would strongly recommend the below steps to be taken to secure the operating system.

2. What format is better and secure to use with Windows NT Server, NTFS Format or FAT?

Windows NT by default formats the hard drive as FAT partition. FAT provides no security feature while NTFS does. As discussed in the Orange book, NTFS is the only file system on Windows NT that supports Discretionary Access Control (DAC) for file system objects and much more.

3. How can I convert FAT format to NTFS format?

- Click on the Start button
- Select Run and type "cmd"



- At the DOS Prompt type "convert C: /FS:NTFS /v"

The system will notify you that it cannot perform this conversion because the system is using this disk. You are prompted and asked if you want the conversion to take place at the next boot up.

- Answer "Y" for yes.
- Reboot the machine, for the changes to take place.

4. What are Service Pack(s) and Hotfixes?

Service Pack and Hotfxes is a collection of upgrades and patches for Windows NT and can be download from Microsoft site (www.microsoft.com\ntserver\).

Or

In simple terms, patch or program fix is called *service pack* (SP). There are a number of service packs out there, both for different versions of Windows NT and Windows 2000. Service packs are the means by which Windows NT product updates, patches, vulnerabilities are distributed

NOTE: Service packs are cumulative. This means that SP6 contains all of SP1 through 5 as well as the fixes introduced in older versions to Services Packs. Service packs often update a great amount of code by replacing major DLLs.

Hot fixes are intermediate fixes released between service packs and are not considered fully regression tested, and as such not recommended by Microsoft to be applied unless one really need the feature they provide. Lately, a bunch of security problems have been solved by means of releasing hot fixes.

NOTE: Service packs and hotfixes are the means by which Windows NT product updates, patches, vulnerabilities are distributed.

5. Can you take me through the steps of installing the Service Pack?

Follow the following:

- Create a folder and give it a name (any name).
- Download the service pack from any of the sites above.
- From the Start menu, open a command prompt from the RUN menu
- Move into the directory where the service pack executable is located.
- Executable the service pack exe file

The service pack will expand in a temp directory

There are six switches available with the service pack executable file which are self-explanatory and can be viewed with an " /?" command.

6. How can I be sure that the server pack was installed?

Once the service pack has been executed, you would be prompted to reboot your machine. Reboot your machine and follow the below:

- Click on the Start menu
- From the Run command,
- type Regedt32
  view the following registry value

  - HKEY_LOCAL_MACHINE
  - \Software\Microsoft\Windows NT\CurrentVersion
  - SourcePath
  - REG_SZ
  - Service Pack "the service pack version installed"

7. Where can I download the latest Service Packs and Hot Fixes?

Service Packs can be downloaded from the following links:

http://www.microsoft.com/downloads.
http://windowsupdate.microsoft.com
http://www.microsoft.com/NTServer/all/downloads.asp
http://www.microsoft.com/downloads

Description on the Hot Fixes and Services Packs can be found at the TechNet site:

http://www.microsoft.com/technet/support/sp.asp

My advice would be to test service pack and determine whether you require it or not before installing it. Microsoft can notify an individual of any patch or security vulnerability they release. You can subscribe at the Microsoft security link below:

http://www.microsoft.com/technet/security/notify.asp

NOTE: Always test any Windows NT, Service Packs on a staging server before applying them on your Production machines.

8. Why do Service Packs need to be reapplied after any change made to the operating system?

Service Packs need to be reapplied to maintain the security.

NOTE: When reapplying the patch, DO NOT overwrite any newer files.

9. Can Windows NT page file hold sensitive data?

Yes it can. Memory pages are swapped or paged to disk when an application needs physical memory. Even though the page file is not accessible while the system is running, it can be accessed by, for example, booting another OS.

- Follow the following command to view your Virtual Memory
- Click on the Start button
- Select Settings, then Control Panel
- Double click on the System icon
- Performance tab
- Virtual Memory

10. How can I protect it?

There is a registry key that can be created so that the memory manager clears the page file when the system goes down:

- HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\MemoryManagement\ClearPageFileAtShutdown: 1

Note: The system has to be rebooted or brought down to clear the page file.

11. Do I need to install Virus protection on my servers?

Always install virus software, as some types of viruses, such as those written in Java, MS Word scripting language, Excel macros, would play some tricks Windows NT machines.

According to DR Solomon, the MS Word based concept virus spread widely in part because several companies, have shipped CD-ROMs containing viruses.

Always avoid dual boot:

Other types of viruses can affect Windows NT machines if dual boot is chosen i.e. having some other types of operating system on the same hardware, e.g. OS/2, UNIX or other version of Windows. When using a dual boot, the bootable operating system, could have a virus in effect that destroy the boot sector or something like that, your NT partition will probably be destroyed as well

The following are some sites I have used to purchase/download Virus Software:

Sophos SWEEP for Windows NT (http://sophos.com/Marketing/ntgui.html)
WinGuard from DR Solomon (http://www.drsolomon.com)
Symantec's Norton Antivirus for NT http://www.symantec.com/nav/fs_nav20nt.html)
Datafellows F-PROT (http://www.datafellows.com)

12. I have heard a lot about the Microsoft Security Configuration Editor. How can it help me?

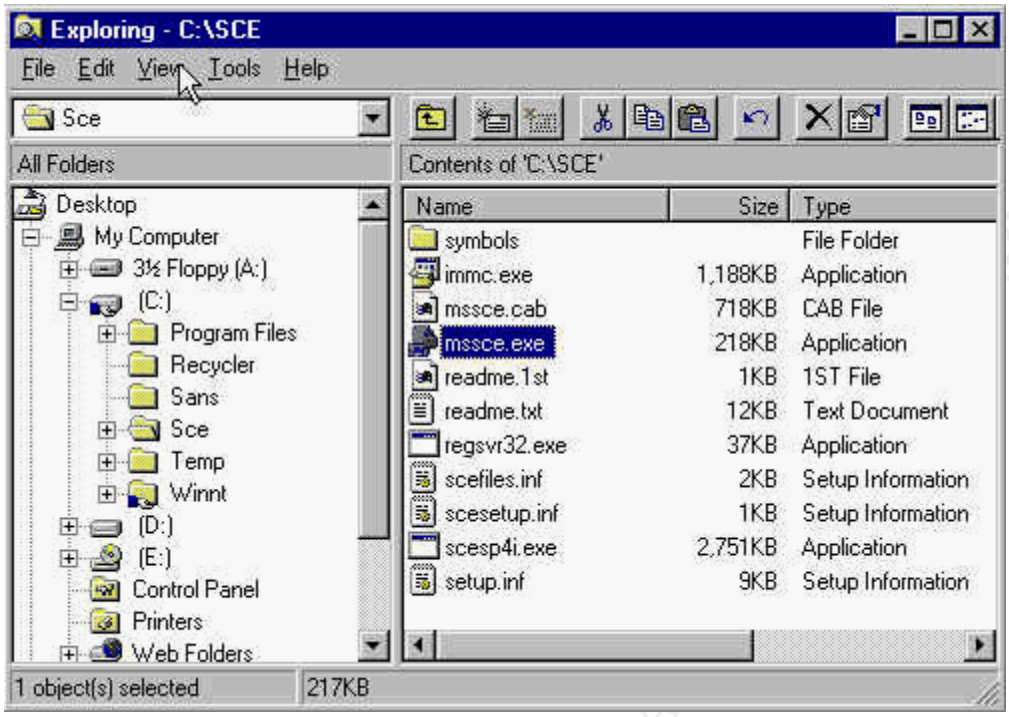
The Microsoft Security Configuration Editor is a tool that can be downloaded from Microsoft site, which that allows you to
:

- Define a template of security configuration settings
- Compare the local machine's settings against a template
- Configure the local machine's settings to match a template

The Microsoft Security Configuration Editor can be installed with Service Pack 4.0 or can be downloaded from:

http://www.microsoft.com/download.
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/tools/scm/

Download the file from the above site execute it.



After the files have been downloading, double-click on the "mssce.exe" file install the Microsoft Security Configuration Editor.

Start the MMC by clicking on the Start button, select run and type "mmc"

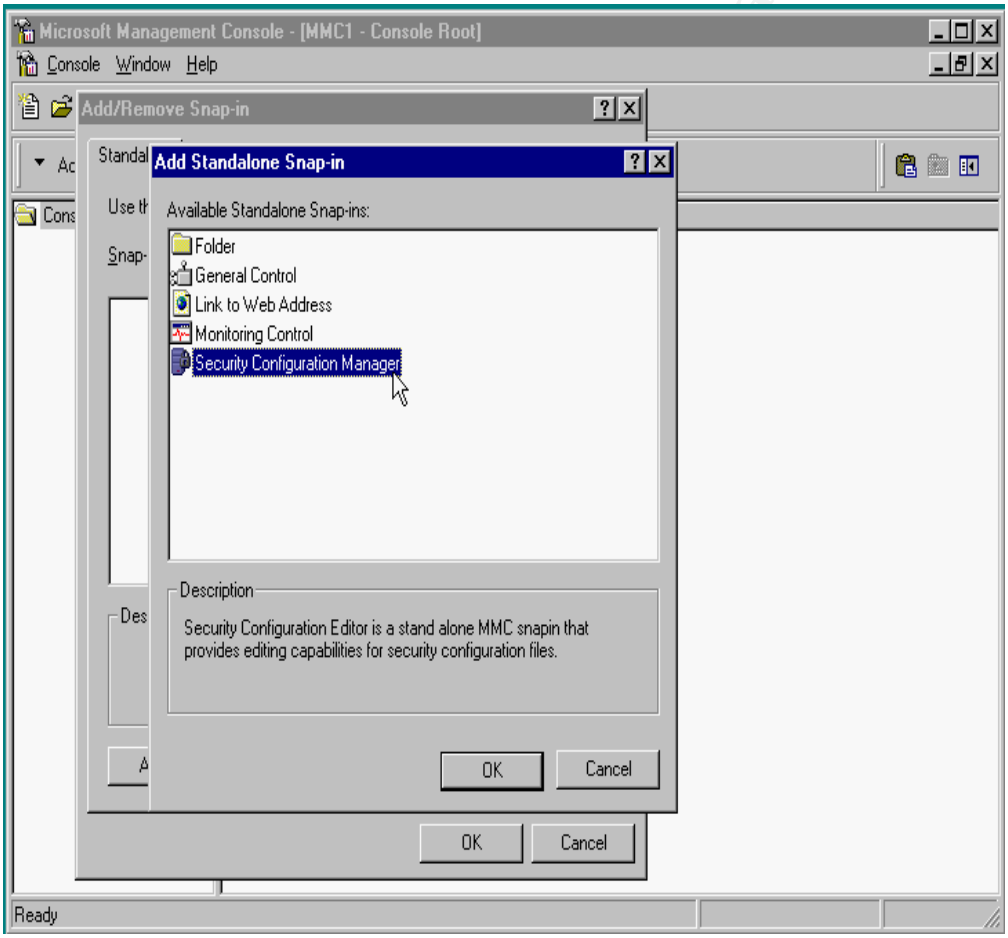
This will bring up the Microsoft Management Console.

Now we can add the Security Configuration Editor as a snap-in to the Microsoft Management Console.

From the command prompt launch the Microsoft Management Console (MMC).

- Click on the Start button
- From the menu select Microsoft Management Console (MMC).
  (This is take you into Microsoft Management Console.)

- From the Console Menu select Add/Remove Snap-In
- From the Add/Remove Snap-In click Add to open the Add Standalone Snap-in
- Select Security Configuration Manager then click OK
- Click OK again



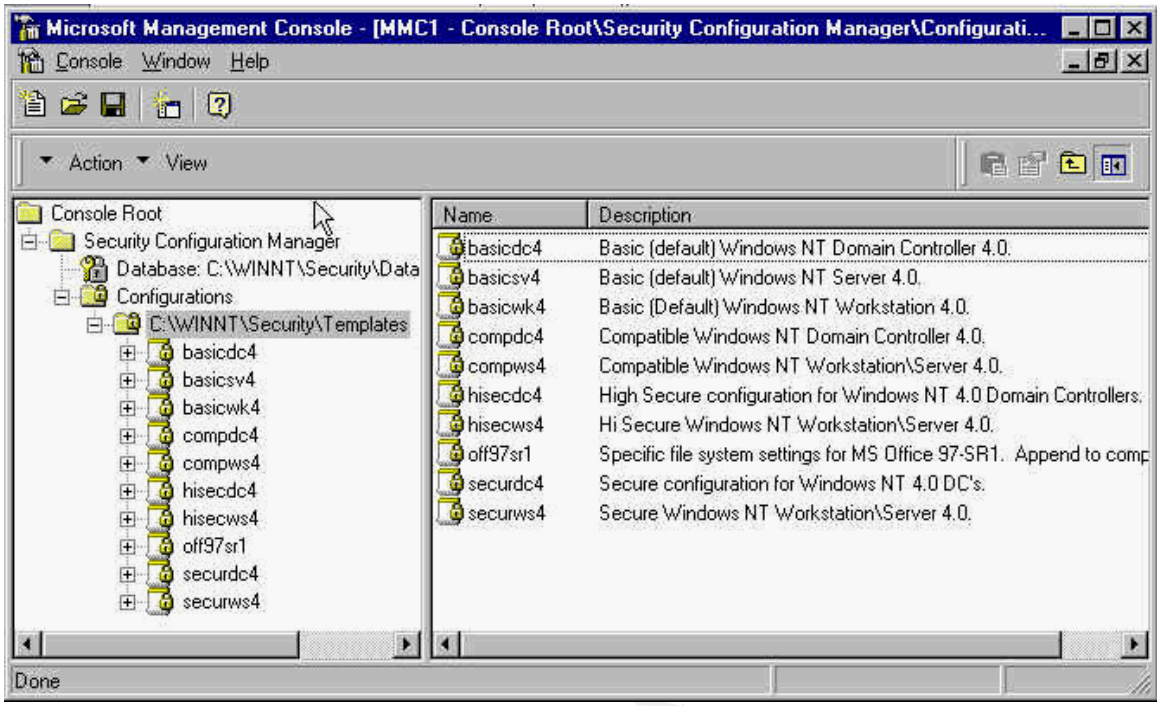
Once the Snap-In has been installed, the following polices, groups, service etc can be configured:

- **Account Policies** – You can use the tool to set access policy, including domain or local password policies, domain or local account lockout policy, and domain Kerberos policy.
- **Local Policies** – You can configure local audit policy, user rights assignment, and various security options such as control of floppy disk, CD-ROM, and so forth.
- **Restricted Groups** – You can assign group memberships for built-in groups such as Administrators, Server Operators, Backup Operators, Power Users, and so forth, as well as any other specific group that you would like to configure. This should not be used as a general membership management tool—only to control membership of specific groups that have sensitive capabilities assigned to them.
- **System Services** – You can configure security for the different services installed on a system, including network transport services such as TCP/IP, NetBIOS, CIFS File Sharing, Printing, and so forth. These can be configured both as start-up options (automatic, manual, or disabled) and you can also set access control on these services—grant or deny access to start, stop, pause, and issue control commands.
- **File/Folder Sharing** – This sub-area allows you to configure settings for Windows NT File Server (NTFS) and Redirector service. These include options to turn off anonymous access and to enable packet signatures and security when accessing various network file shares.
- Future releases will include other service specific sub-areas including services like Internet Information Server.
- **System Registry** – You can use the tool set to set the security on system registry keys.
- **System Store** – You can use the tool set to set the security for local system file volumes and directory trees.
- **Directory Security** – You can use the tool set to manage the security on objects residing in the Windows NT 5.0 Active Directory.

Note: the above list has been exacted from Microsoft site.

Using the MMC to compare your system configuration to a pre-defined security configuration.

A comprehensive security policy must be in place prior to implementing any of the SCE templates as configurations within these templates directly relate to security policies. Before creating a security configuration template, you have to take into consideration the type of environment your production servers are running. After creating your security configuration template, I would compare it with *hisecdc4* for financial institutions or a high profile customer, and the *basicdc4* template for a basic side.



Note: Always test your templates on a staging environment before deploying them it on a on your production environment.

The SECEDIT command line tool.

For deploying the tested template to your production environment, you can use the command line utility called **SECEDIT** and apply the policy. Microsoft recommends the use of this command utility when you have an Active Directory-based infrastructure and have several computers that need to be configured frequently. You can also create command batch files and then schedule them to run at off-hours using the task scheduler Alternatively; you may use Microsoft System Management Server (SMS) to distribute this task on several different computers.

For more information (White papers) visit

www.microsoft.com/ntserver/security/techdetails/prodarch/securconfig.asp

13. We all know that an Administration Account is the most powerful account build within Windows NT. What could be suggested for securing this account?

As a security measure, I would advice no one to use the built in Administrators account to work on the system. Each user with Administrative duties must have a uniquely identifiable account so that any administrative work may be tracked back to an individual.

The administrator account can never be locked out despite several-repeated failed log on attempts, even if the User Manager account policies have been set to "Lockout After Bad Logon Attempts". This is a very attractive account to hackers who try to break in by repeatedly guessing passwords.

Furthermore, do not allow shared accounts under any circumstances. With the built-in Administrator group, you cannot restrict the access or capabilities of those members. By default, this group as well as the built in Administrator account can perform any function on the system unrestricted. Although their actions will be audited, no "red" flags will appear in the event log since this group is unrestricted by the Operating System.

14. How can the Administrator account be secured?

I would used the following steps to secure the administration account:

- Rename the Administrator account:
  - From the User Manager.
  - Select administrator account,
  - From the pull down menu select User,
  - Select Rename to rename the administrator account.

Note: The benefit by renaming the account would be to strengthen the security, as it would leave the hackers guessing the account name as well as the password.

- Disable the Administrator account:

Disable the Administrator account (even if it has been renamed) using the PASSPROP utility, which is available with Service Pack 3 or the Windows NT Resource kit. Passprop has the following switches:

PASSPROP /?

/complex	Force passwords to be complex, requiring passwords to be a mix of upper and lowercase letters and numbers or symbols.
/simple	Does allow passwords to be simple.
/adminlockout	Does allow the Administrator account to be locked out. The administrator can still log on interactively on domain controllers.
/noadminlockout	Doesn't allow the administrator account to be locked out.

Note: The command line utility "passprop" is the only utility available to disable the Administrator account allows.

15. How can one enforce stronger passwords?

In order to automatically enforce the use of strong passwords NT service pack 2 and above includes a utility filter called Passfilt.dll.

With the Passfilt.dll utility installed, users can be forced to use stronger passwords i.e. minimum password length with User Manager utility and use complex passwords. In Service Pack 3, Microsoft shipped a DLL called PASSFILT.DLL. Passfilt.dll filters the passwords and forces the users to choose passwords must be a minimum of six characters and not contain any part of their userid.

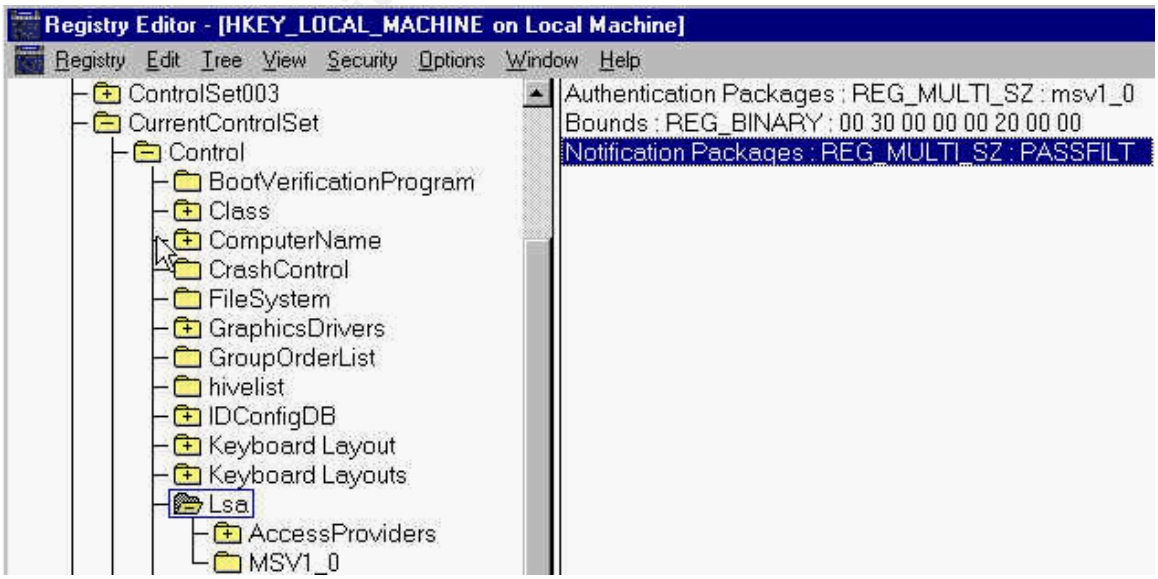
Once the Service Pack has been applied, add the following settings to the registry:

- Click on Start,
- Run,
- Type in regedt32.exe to bring up the Registry editor.
- Move to the following location.

HIVE: HKEY_LOCAL_MACHINE
Key: \System\CurrentControlSet\Control\Lsa

Select Edit, Add Value.

Value Name: NotificationPackages
Value Type: REG_MULTI_SZ
Value Data: PASSFILT



Note: The data must be entered exactly as shown and then press OK. **Passfilt.dll** can be found in the %systemroot%\system32 directory.

Another consideration is to use extended ASCII characters in the password, for example, holding the Alt key and typing 145 (on the numeric keyboard), then releasing the Alt key will generate a non-standard character not used by default in password cracking software. It should be noted that some applications such as web-based ones cannot handle the extended characters and thus this approach may prove problematic. In addition, Windows 9x and Windows for Workgroup clients seem to have trouble with the extended ASCII.

Note: For added security setup a three-part password and give one part each to three different people. This will require all three people to successfully logon as the Administrator account.

Create a separate group with administration privileges :

Create an individual user account for each person assigned administrative duties and make them a member of the "Super Admins" group. These users should also have a standard user account, without administration privileges, for performing routine functions. This should be a separate account from the their normal user account. The use of this account should be limited to emergency situations or investigative tasks. By creating a separate account for each System Administrator (SA), members of this group cannot be restricted using the User Rights settings.

To create a group with Systems Administrator (SA) privileges, follow the steps below:

- From the Start button,
- Select Programs, Administrative Tools, then User Manager.
- From the pull down menu User,
- Select "New Local Group…" and
- Create a group called "Super Admins" (Any name can be supplied).

Note: Only a small selected group should be given an account with membership to the built in Administrator group

16. Is the Guest Account safe to use?

No. You should, rename your guest account and disable it as much as possible

- Use the User Manager, to rename the account and disable it too.

17. How can auditing be switched on to alert me of any security breaches?

Enabling Windows NT auditing can inform you of actions that pose security risks and possibly detect security breaches. To activate security event logging, follow these steps:

- Log on as the administrator of the local workstation or server.
- Click the Start button,
- Select Programs, Administrative Tools,
- and then User Manager.
- From the Policies pull down menu, select Audit.
- Click the Audit These Events option.
- Enable the options you want to use.

The following audit choices are available:

Log on/Log off:	Logs both local and remote resource logins.
File and Object Access:	File, directory, and printer access.
Use of User Rights:	Any attempt to access a file or application not granted to a user will be detected in this audit.
User and Group Management:	Any user accounts or groups created, changed, or deleted. Any user accounts that are renamed, disabled, or enabled. Any passwords set or changed.
Security Policy Changes:	Any changes to user rights or audit policies.
Restart, Shutdown, and System:	Logs shutdowns and restarts for the local workstation.
Process Tracking:	Tracks program activation, handle duplication, indirect object access, and process exit.

Note: Files and folders must reside on an NTFS partition for security logging to be enabled. Once the auditing of file and object access has been enabled, use Windows NT Explorer to select auditing for individual files and folders.

In setting the Audit Policy, the following minimum settings are recommended:

Audit These Events		
	Success	**Failure**
Logon and Logoff		
File and Object Access		
Use of User Rights		
User and Group Management		
Security Policy Changes		
Restart, Shutdown, and System		
Process Tracking		

Click the Success check box to enable event logging for successful operations, and the Failure check box to enable event logging for unsuccessful operations.

Note: Auditing is a "detection" capability rather than "prevention" capability. It will help you discover security breaches after they occur and therefore should always be considered in addition to various preventive measures.

18. By turning the Auditing turned on, would it not fill up the log files? Can the logs file be increase in size?

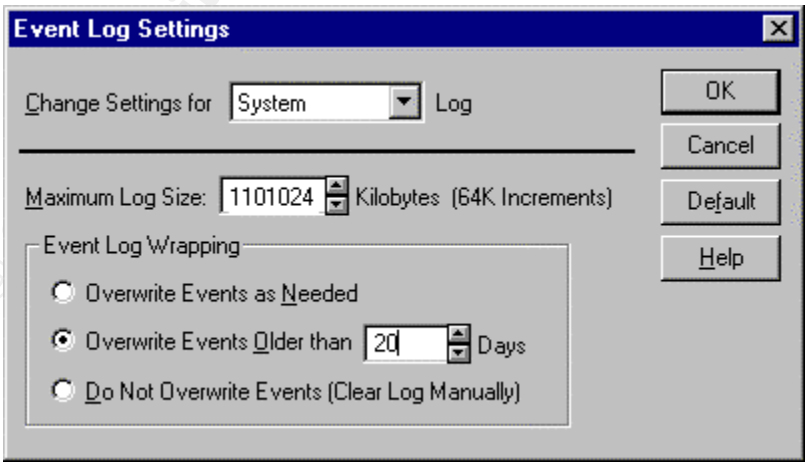
Yes. In the Event Viewer there are three different logs; which are System, Security and Application. The three logs visible in the Event Viewer are stored as individual files in the

\%SystemRoot%/System32\Config folder.

To increase the above three log files, follow the steps below:

- From the Start button
- Select Programs,
- Administrative Tools,
- then Event Viewer.
- Select the Log pull down menu,
- then select Log Settings.:

System: Raise Max log size to 10048K and change setting to: Do Not Overwrite Events.
Security: Raise Max log size to 10048K. and change setting to: Do Not Overwrite Events.
Application: Raise Max log size to 10048K and change setting to: Do Not Overwrite Events.



To further protect the log files, we shall restrict the Guest Access to the event log Registries. Use the Registry Editor to create the following registry keys:

- Hive: HKEY_LOCAL_MACHINE\
- Key: System\CurrentControlSet\Services\EventLog\Application\
- Name: RestrictGuestAccess
- Type: REG_SZ
- Value: 1

- Hive: HKEY_LOCAL_MACHINE\
- Key: System\CurrentControlSet\Services\EventLog\Security\
- Name: RestrictGuestAccess
- Type: REG_SZ
- Value: 1

- Hive: HKEY_LOCAL_MACHINE\
- Key: System\CurrentControlSet\Services\EventLog\System\
- Name: RestrictGuestAccess
- Type: REG_SZ
- Value: 1

19. How can Account Policies be set with User Manager?

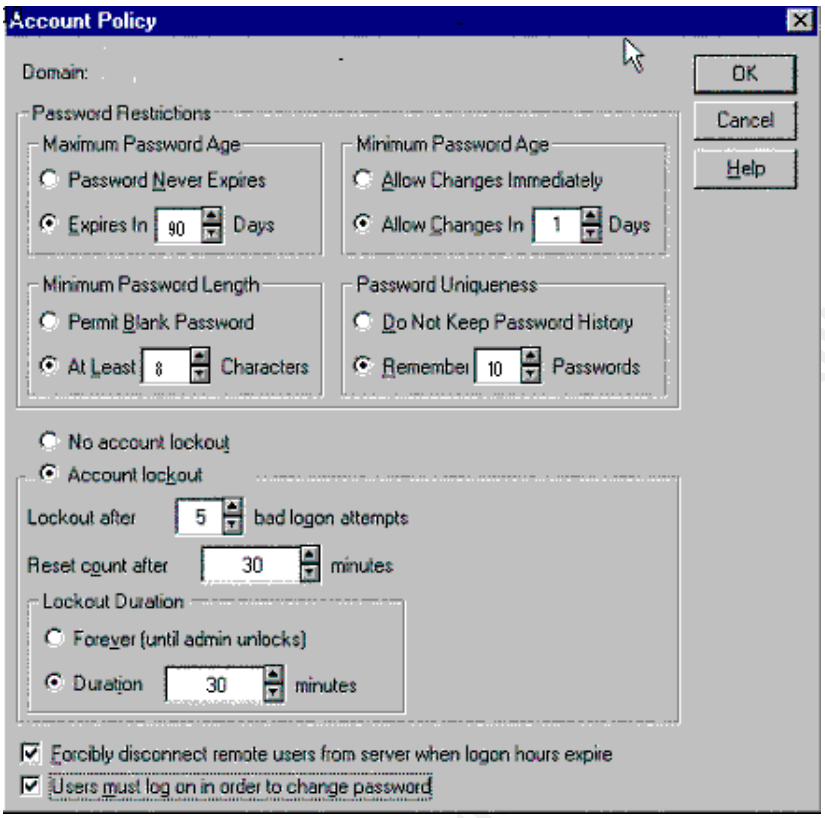
This section, we will set password properties using the User Manager.

You must be logged on locally as an administrator to configure these settings.

- Go to the Start button,
- Select Programs, Administrative Tools,
- Select User Manager.
- From the Policies pull down menu select Account.

Set the Policy as follows:

Maximum Length	90 days
Minimum Change	1 day
Minimum Length	8 characters
Remember	10 passwords
Lockout After	5 attempts
Reset Count After	30 Minutes
Lockout	Forever until Administrator unlocks. If the item is checked, users must log on in order to change password.



Note: The lockout box should not be checked if you have Windows 95 computers attached to your network. It will prevent these users from being allowed to change their password.

20. How can one prevent Halt on Audit Failure?

To prevent the "Halt on Audit Failure" from occurring you can create the following Registry value:

Hive: HKEY_LOCAL_MACHINE\
Key: System\CurrentControlSet\Control\Lsa
Name: CrashOnAuditFail
Type: REG_SZ
Value: 0

Discussion: This is also the key you will need to repair if you have set the Halt on Audit Failure setting. This key will change to a value of 2 and modify the type to a REG_DWORD. Reset the type to REG_SZ and change the value to 1 if you are using these feature.

21. How can I use the Password Database Encryption?

Windows NT 4.0 Service Pack 3 (SP3) introduced a new feature utility that allows you to chose more advanced encryption on the SAM database to provide stronger password protection called the System Key (SYSKEY). This adds a second layer of encryption for the Lan Manager and MD4 hashes of the SAM

Note: The default protection is a hashing routine that has been published on Hacker Web sights.

Running the Syskey utility:

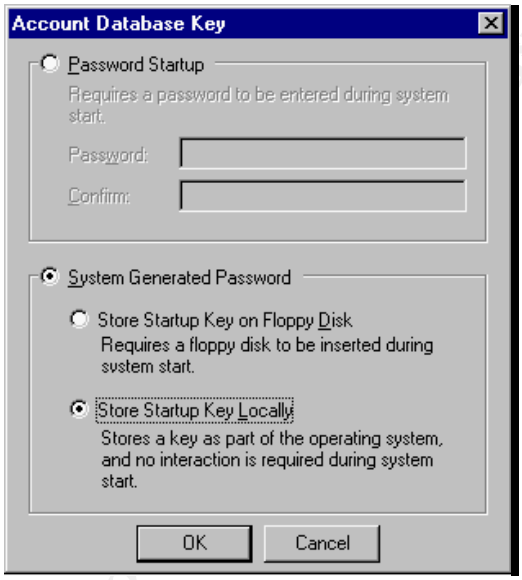
- Go to the Start button,
- Select Run,
- Then type in SYSKEY.EXE.
- The following screen will appear.

- Select "Encryption Enabled"
- click on OK.

- Click on OK

- Click on OK

  The Account Database screen will appear.



- Click on System Generated Password Box
- Click on Store Key Locally (you can choose any from 1 - 3 options for backing up the System Key)
- Click on OK
  Restart the computer.

There are three ways to use the Syskey utility to encrypt (backup), the SAM database how the system would startup to decrypt the SAM database, and are used in one of three ways:

- The system generates a secure key, which is hidden on the computer itself with a "complex obscuring function" to conceal it for unattended system startup, but the system key is stored locally and may be compromised in the future. (If Store Startup Key Locally was selected)
- The system generates a secure key, which is stored on a floppy disk and must be available during system startup or reboots and it is not stored locally. (If Store Startup Key on floppy was selected).

- The system key can be generated (MD5) from a password using up to 128 characters long, which must be entered on system startup, which is used to encrypt the SAM database too. This key is generated every time the system reboots, thus no need for backup.

For more information on the SYSKEY, click the link below:
http://support.microsoft.com/support/kb/articles/q143/4/75.asp

Note: Encrypting the SAM DB is irreversible.

22. What is NTLM v2 Authentication?

NTLMv2 was shipped in SP4 with enhancement to NTLM security protocols, which significantly improves both the authentication and session security mechanisms of NTLM

NTLMv2 also uses a challenge/response method of confirming the user's password. A summary of the features of NTLMv2 are:

- The LM hash of the user's password plays no role whatsoever.
- Client input into the challenge (a salt) to prevent chosen plain text attacks. This prevents the use of pre-computed databases of hashes/keys to speed the cracking.
- The client's response is different with each session even if the user's password stays the same.
- Use of HMAC-MD5 for the 128-bit password hashes.
- Use of a timestamp to verify that response is timely.
- Mutual authentication (client to server and server to client) based on client challenge to the server.
- The most efficient cracking method is a dictionary/brute force search of all possible passwords. Hence, NTLMv2 is just as strong (or only as strong) as the password itself.
- Man-in-the-middle (MITM) attacks infeasible because of mutual authentication.
- Replay attacks infeasible because server's challenge is different each time. In order to enable NTLM v2 go the following registry hive
- Downgrade attacks can be made infeasible by registry values that will require NTLMv2 from either the server's or client's side.
- L0phtCrack 2.52 cannot extract password hashes from NTLMv2 Authentication sessions. Nor is any future version expected to be able to do so with any useful efficiency.

Note: The above have been extracted from Jason Fossen Book

Hive:	HKEY_LOCAL_MACHINE
Key:	\System\CurrentControl Set\Control\Lsa
Value Name:	Lmcompatibilitylevel
Value Type:	REG_DWORD
Value Data:	0 to 5 (Level 0-3 for Clients) (Level 4-5 for DC's)

Level 0	This is the default behavior. NTLM v2 is not enabled.
Level 1	The user's computer will attempt to negotiate NTLM v2 with the domain controller. If the attempt is unsuccessful the negotiation will revert to Level 0 Authentication.
Level 2	The user's computer will only NT authentication (MD4). All DC's must be upgraded to SP4.
Level 3	The user's computer will only authenticate with NTLM v2. Server running Win9x, Win for Workgroups, and WinNT SP3 can still be accessed as long as DC's are running SP4 or higher.
Level 4	Set this on a DC when you only want to use MD4 and NTLM v2 clients. I.E. the clients must be Windows NT.
Level 5	Set this on a DC when you only want to use NTLM v2. All clients must be WinNT with SP4 or later installed.

23. Is there any way to prevent a Null Sessions from Listing Usernames or Restricting Anonymous Logon?

NULL session connection, also known as Anonymous Logon, is a way of letting a not logged on user to retrieve information such as user names and shares over the network. It is used by applications such as explorer.exe to enumerate shares on remote servers. The worst part is that it lets non-authorized users to do more than that. Particularly interesting is remote registry access, where the NULL session user has the same permissions as built-in group Everyone.
A hacker can use null sessions that can be used to get a list of user accounts from the registry. Since Windows NT uses null sessions in place of username and passwords when accessing resources, etc. they are a source of security holes.

With SP3 for NT4.0 a system administrator can restrict the NULL session access, make the following registry edit.

Hive:	HKEY_LOCAL_MACHINE
Key:	\System\CurrentControl Set\Control\Lsa
Value Name:	RestrictAnonymous
Value Type:	REG_DWORD
Value Data:	1

Note: Since restricting null sessions has the possibility of breaking certain network services, it is important to test this registry edit on a on a staging server.

For more information:

http://support.microsoft.com/support/kb/articles/Q143/4/74.asp

24. What is a Emergency Repair Disk?

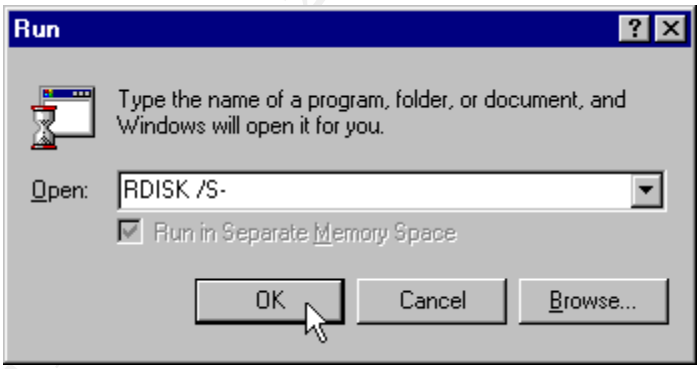
An Emergency Repair Disk (ERD) contains critical Windows NT operating system data and can be used to:

- Repair the SAM
- Security Policy

By default, the RDISK utility in Windows NT Server and Workstation does not back up all of the Registry. To backup entire the Registry, including the DEFAULT, SAM and SECURITY files using RDISK, you must use the /s switch, i.e. running "rdisk /s".

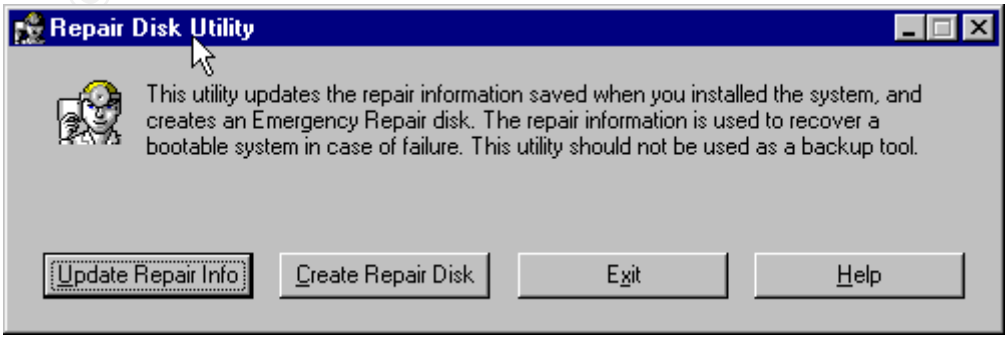
Creating emergency Repair Disk (ERD)

- Click on Start
- Select Run menu



- Type rdisk/s

The following dialog box appears:



From the above dialogue box you can create a new Emergency Repair Disk or update an existing one.

Note: The ERD should be locked up and/or protected. Combined with the Administrator password at the time it was made, an emergency repair disk gives full access to the system.

25. Can you suggest any other good Security practices that can be followed?

The following are some good security practices I would recommend.

Logging Off or Locking the Workstation

Unattended Computers:

Users should either log off or lock the workstation if they will be away from the computer for any length of time. Logging off allows other users to logon (if they know the password to an authorized account); locking the workstation does not. The workstation can be set to lock automatically if it is not used for a set period of time by using any screen saver with the Password Protected option.

Setting the screen saver password:

- Place the mouse in an open area of the desktop and press the right mouse key.
- Select Properties from the menu that appears.
- Select the Screen Saver tab at the top of the Display control panel,
- then assign a screen saver and place a check in the "Password protected" box.
- Set the "Wait" time to no more than 15 minutes.

Backups protect your data:

Regular backups protect your data from hardware failures and honest mistakes, as well as from viruses and other malicious mischief. Obviously, files must be read to be backed up, and they must be written to be restored. Backup privileges should be limited to backup operators—people to whom you are comfortable giving read and write access on all files. By virtue of being a member of this group, Backup Operators can bypass all file and directory access restrictions on the system. Therefore, those

Note: Those persons assigned the backup duties should be assigned a separate account for performing them as well as a common user account for daily activities.

Backup utility(Remote access)

The Backup utility included with Windows NT allows you to back up the registry as well as files and directories. To restrict network access to the registry, use the Registry Editor to create the following registry key:

Hive:	HKEY_LOCAL_MACHINE
Key:	\System\CurrentcontrolSet\Control\SecurePipeServers\winreg
Name:	RestrictAnonymousAccess
Type	REG_DWORD
Value:	1

Set the security permissions set on the key below, which would define which users or groups could connect to the system for remote registry access. The default Windows NT Workstation installation does not define this key and does not restrict remote access to the registry.
Set the following security permissions the key below to:

Registry Table :	HKEY_LOCAL_MACHINE	
Key Path	SYSTEM\CurrentControlSet\Control\Secure\PipeServers\Winreg	
Users/Groups &	Administrator	Set to Full Control
Permissions:	System Admin	Set to Full Control

FTP Service.

FTP Service through Windows NT Network.

Windows NT also comes with another standard Internet service called file transfer protocol (FTP). A common use of FTP is to allow public file access via anonymous log on. When configuring FTP server, the System Admin assigns the server a user account for anonymous logons and a default home directory. The default anonymous user account for FTP is GUEST.

I would recommend to secure the FTP session to follow the below:

- That the default user account be changed to a different user account and should have a password.
- This account should not be member of any privileged groups so that the only default group that shows up in the security token during log on is Everyone.
- The account should not be allowed "Logon on Locally" user right to restrict "insider attacks".
- The home directory parameter should be configured carefully. FTP server exports entire disk partitions. The System Admin can only configure which partitions are accessible via FTP but not which directories on that partition. Therefore, a user connecting via FTP can move to directories "above" the home directory. Therefore, in general it is recommended that if FTP service needs to run on a system, it is best to assign a complete disk partition as the FTP store, and to make only that partition accessible via FTP.

CD-ROM Restrictions.

Since this Auto-Play feature on CD_ROM can launche as a service, the User Rights settings will not prevent malicious code or Trojan horse applications from starting as soon as a CD-ROM is installed in the drive

To prevent the Auto-Play feature from launching when a disk is inserted into the CD-Rom set the following Registry Key.

Hive: HKEY_LOCAL_MACHINE
Key: \System\CurrentControlSet\Services\CDRom
Name: Autorun
Type REG_DWORD
Value: 0

Securing Base System Objects.

The registry setting below informs the Windows NT Session Manager that security on the base system objects should be at C2 security level. This value enables stronger protection on base objects.

To enable stronger protection on base objects, verify and add if needed, the following value to the registry key.

Hive: HKEY_LOCAL_MACHINE
Key: \System\CurrentControlSet\Control\SessionManager:
Name: ProtectionMode
Type: REG_DWORD
Value: 1 This is the default value

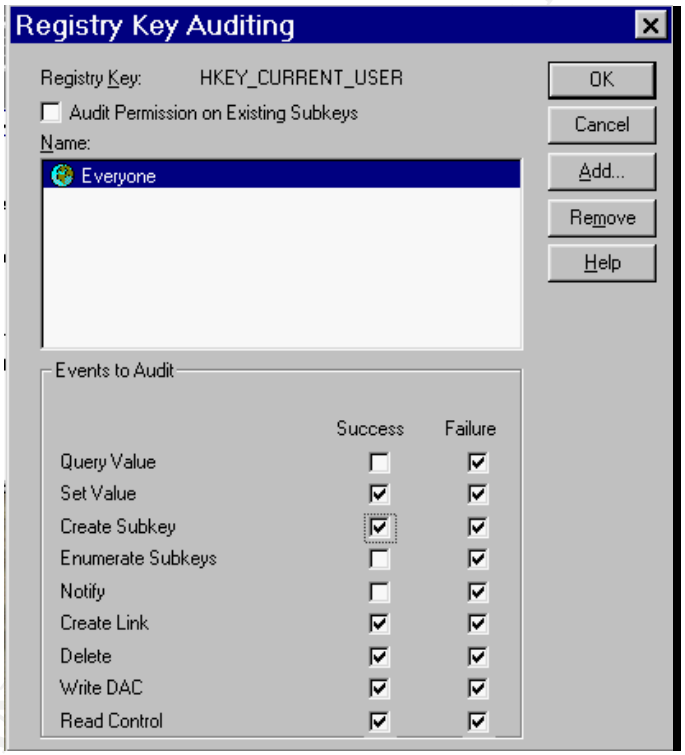
Auditing Base Objects

To enable auditing on base system objects, add the following key value to the registry key. This registry key setting tells Local Security Authority that base objects should be created with a default system audit control list.

Hive: HKEY_LOCAL_MACHINE
Key: \System\CurrentControlSet\Control\Lsa:
Name: AuditBaseObjects
Type: REG_DWORD
Value: 0001

Enable Auditing on the registry keys:

- From the Start Button select Programs,
- Windows NT Explorer.
- Go to the (NT Root Directory)\SYSTEM32 and
- Double click on REGEDT32.EXE. (Alternatively, you can Start - Run - REGEDT32 Return) This will launch the Registry editor.
- Select each of the
- Registry Trees (HKEY_CURRENT_USER; HKEY_CLASSES_ROOT; HKEY_USERS; and HKEY_LOCAL_MACHINE)
- Then select "Security", and Auditing from the Pull down menu.
- Select the Add button, then select the group "Everyone". This will allow you to mark the blocks.



Physical Security Considerations:

All equipment should be located in a controlled environment. As a minimum, server equipment should be kept in a restricted access area under tighter control than the normal workstation would normally be given.

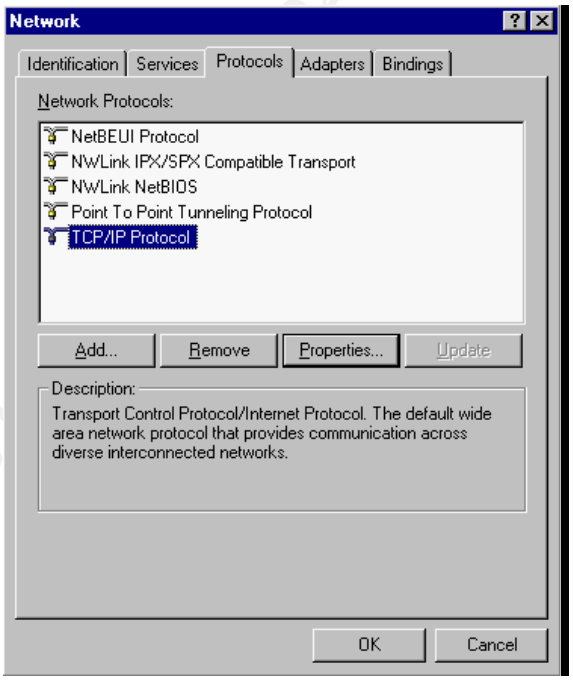
Network Services, Protocols and Bindings

Ports should be set to only allow connection of required port numbers. The default Primary Domain Controller installation will include the following services:

- Computer Browser,
- NetBIOS interface,
- RPC configuration,
- Server and Workstation
- Protocol is TCP/IP.

The network bindings include NetBIOS Interface, Server and Workstation.

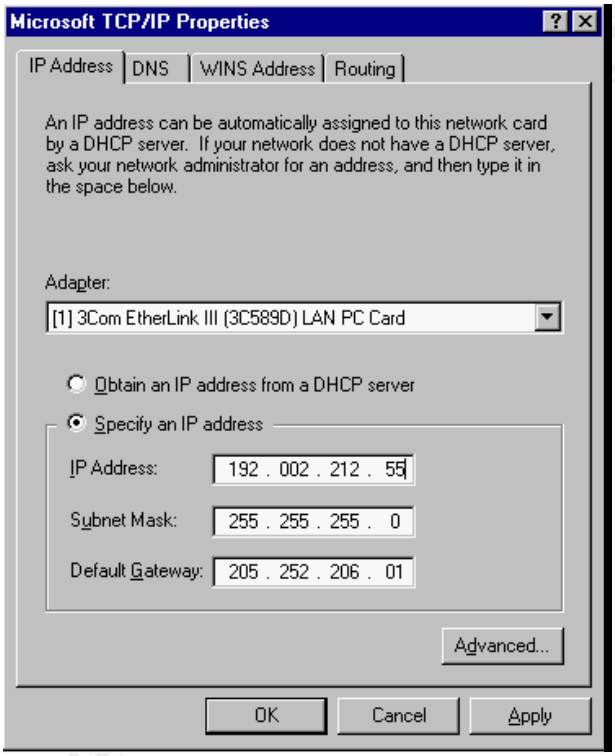
- From the Start button,
- Select Settings,
- Control Panels.
- Double click on "Network",
- Select the "Protocols" tab from the top,
- Highlight "TCP-IP Protocol", and
- Select properties.



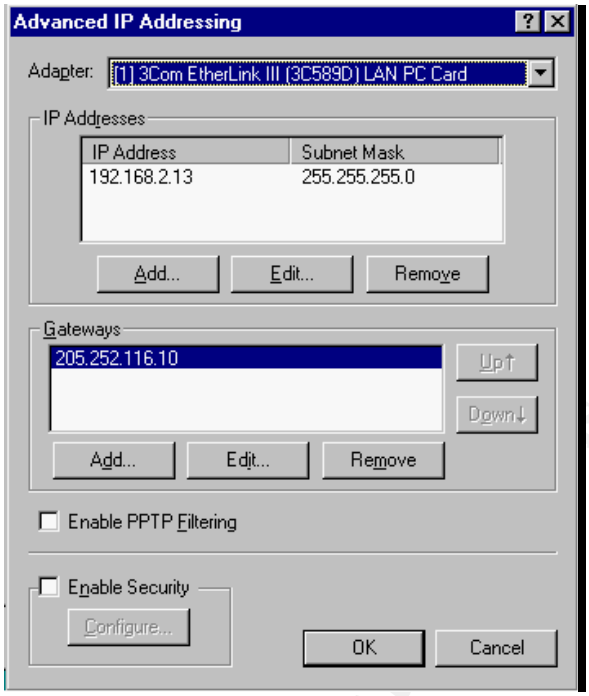
You should see the TCP/IP Properties window.

Note: The following is a list of the ports used by NBT.

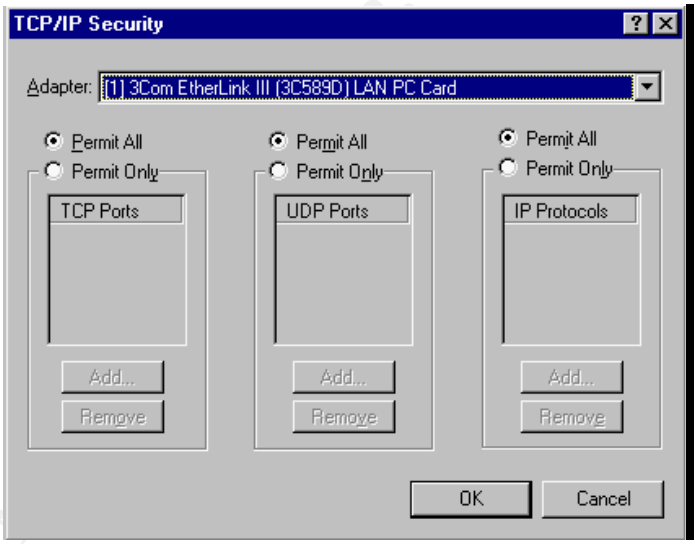
- netbios-ns 137/tcp NETBIOS Name Service
- netbios-ns 137/udp NETBIOS Name Service
- netbios-dgm 138/tcp NETBIOS Datagram Service
- netbios-dgm 138/udp NETBIOS Datagram Service
- netbios-ssn 139/tcp NETBIOS Session Service
- netbios-ssn 139/udp NETBIOS Session Service



➢ Select the "Advanced" button from the lower right corner of the window to bring up the Advanced IP Addressing window.



Place a check in the "Enable Security box in the lower left corner, then select configure.



- Select "Permit Only" on each of the three (TCP Ports, UDP Ports, and IP Protocols).
- Add the following port numbers to both TCP and UDP.

Port Number	Port Name
20	FTP data
21	FTP
22	SSH (SSH Remote Login Protocol)
23	Telnet
25	SMTP
53	DNS
80	HTTP
88	Kerberos
90	WINS
110	POP3
161	SNMP
162	SNMPTRAP
443	SSL
8080	SHTTP
6	TCP
17	UDP

Note: The above table is just guidance and would vary from one's environment. All ports should be added only after further investigation of one's environment

Passwords

Anyone who knows a user name and the associated password can log on as that user. Users should take care to keep their passwords secret.

Here are a few tips:

- Change passwords frequently, and avoid reusing passwords.
- Avoid using easily guessed words and words that appear in the dictionary. phrase or a combination of letters and numbers works well.
- Don't write a password down—choose one that is easy for you to remember.

Controlling Access to the Computer

No computer will ever be completely secure if people other the than authorized user can physically access it. For maximum security on a computer that is not physically secure (locked safely away), follow all or some of the following security measures:

- Disable the floppy based boot if the computer hardware provides the option. If the computer doesn't require a floppy disk drive, remove it.

  Note: In the Windows NT Resource Kit, there is a utility named FloppyLock. FloppyLock runs as a service and prevents access to floppy drives by all users except Administrators and power Users.

- The CPU should have a case that cannot be opened without a key. The key should be stored safely away from the computer.
- The entire hard disk should be NTFS.
- If the computer doesn't require network access, remove the network card.

Hiding the Last User Name

By default, Windows NT places the user name of the last user to log on the computer in the User name text box of the Logon dialog box. This makes it more convenient for the most frequent user to log on. To help keep user names secret, you can prevent Windows NT from displaying the user name from the last log on. This is especially important if a computer that is generally accessible is being used for the (renamed) built-in Administrator account.

To prevent display of a user name in the Logon dialog box, use the Registry Editor to create or assign the following registry key value:

- Hive: HKEY_LOCAL_MACHINE\SOFTWARE
- Key: \Microsoft\Windows NT\Current Version\Winlogon
- Name: DontDisplayLastUserName
- Type: REG_SZ
- Value: 1

Network Services, Protocols and Bindings

The default Primary Domain Controller installation in my opium should include the Computer Browser, NetBIOS interface, RPC configuration, Server and Workstation "services". Only TCP/IP protocol that should be running on the PDC connected to the Internet.

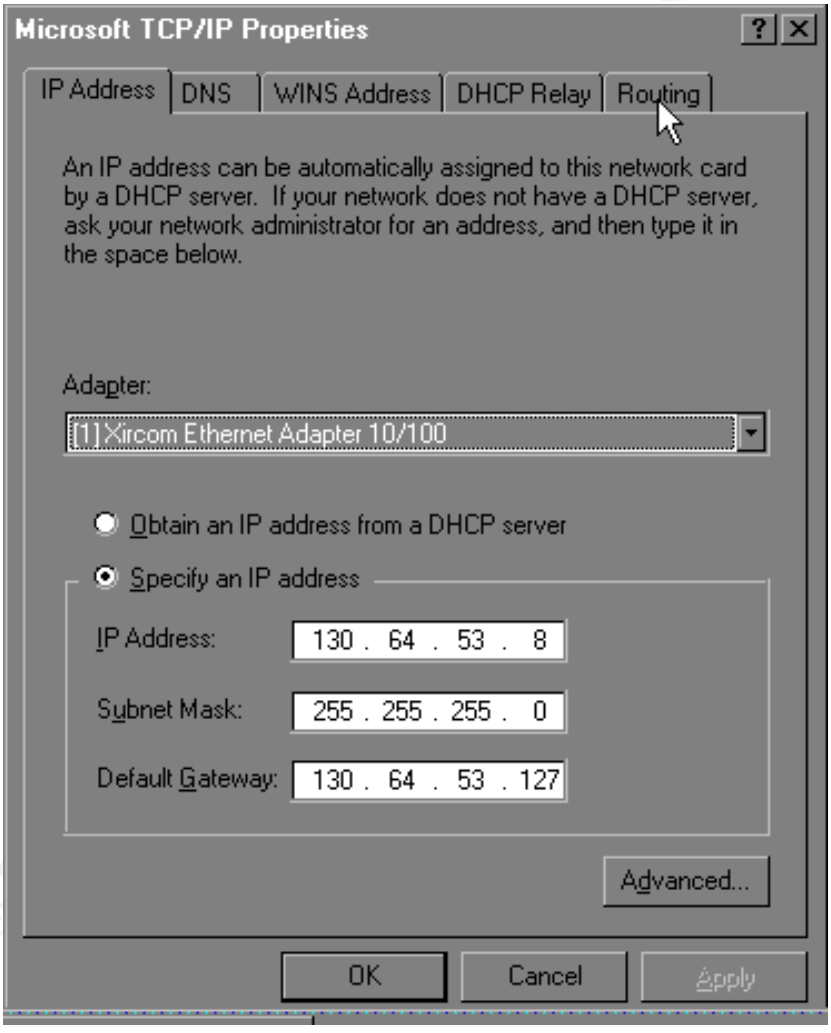
If the server is directly connected to an outside network,

- Disable the TCPIP <-> NETBIOS binding on the outbound NIC, unless it is required for your environment. (Demonstrated in the next step)

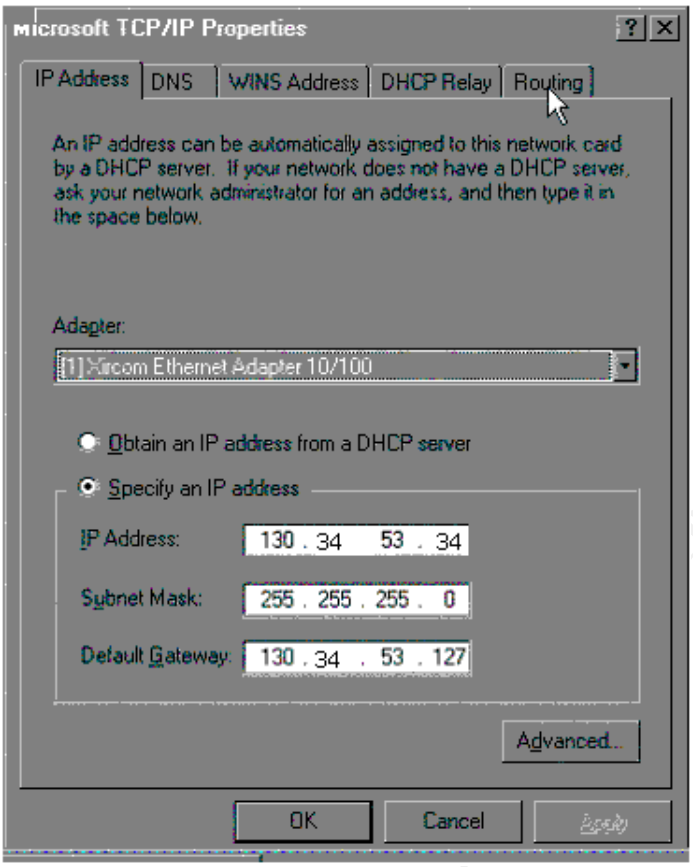
- Verify that the Enable IP Forwarding option on the Routing panel (shown below Fig 1.0) is not checked. Although IP forwarding is necessary on specific gateways, it is generally not recommended for the Primary Domain Controller. The Primary Domain Controller shouldn't be used to forward IP packets that might expose the network to certain types of attacks.

  Assuming that you have a connection to the Internet from your Windows NT Server machine, an increasingly common configuration, this may expose you to the comings and going of the Internet.

For example let's assume that you've correctly installed Microsoft Proxy Server on your Windows NT Server machine and you have two network adapters to create a physical separation zone. Your firewall protection via Microsoft Proxy Server is largely a function of keeping a squeaky clean Local Address Table (LAT) that prevents intruders from penetrating your LAN. However, it is a common configuration error that I've observed at some sites running Microsoft Proxy Server to have the Enable IP Forwarding check box selected. That defeats the whole purpose of the LAT-based firewall in Proxy Server. The firewall now has a large hole in it with IP forwarding enabled. What goes out can come back in.



Note: Be very cautious with the Enable IP Forwarding check box.



Switch off TCP/IP forwarding

- Click on the Start button,
- Select Setting, then
- Select Control Panel, and
- Select the Network icon
- From the Dialog screen,
- Select Protocol tab and
- Select Properties.

The Microsoft TCP/IP Properties screen appears select Routing seen below.

- In the Routing tab screen, make sure that the Enable IP Forwarding box is not checked.

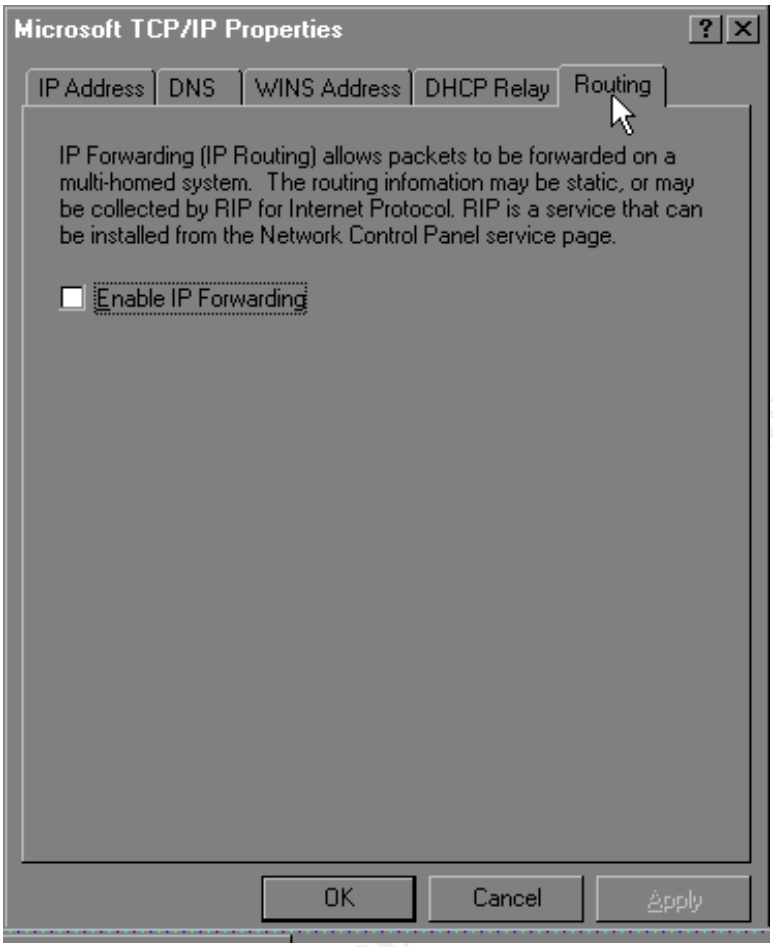
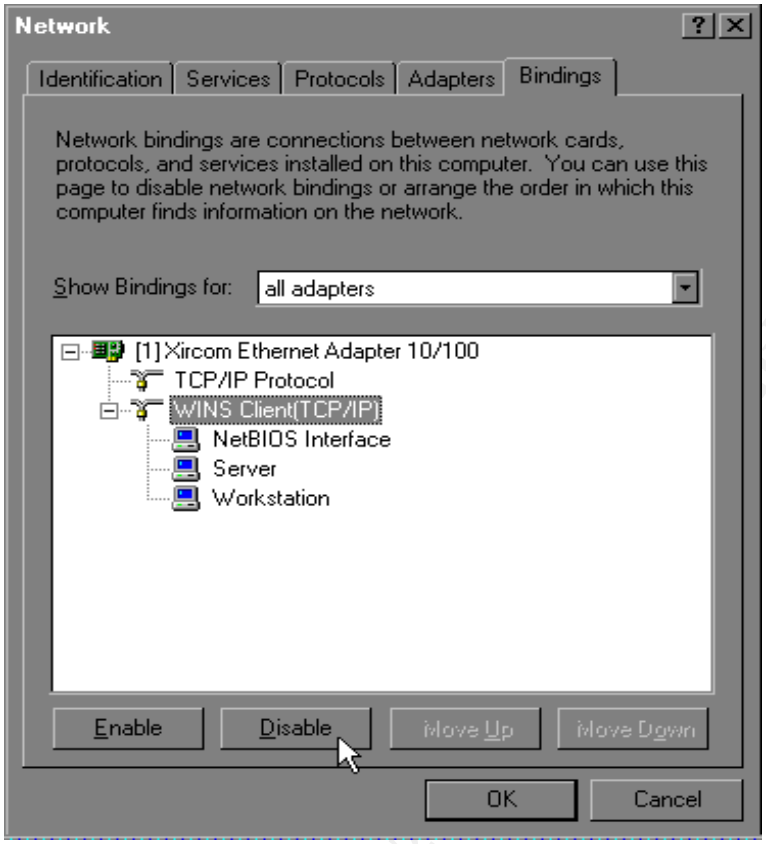


Fig 1.0

Removing Bindings

To protect Windows NT networking data and SMB/NetBIOS services, I would recommend unbinding the NetBIOS on a Primary Domain Controller with two internal NIC cards,

- Click on the Start button
- Select Settings
- Select Control Panel
- Double-click on the Network icon and
- Select the Bindings tab
- Click on NetBIOS Interface and
- Click on the Disable button



Display a Legal Notice Before Log On:

The logon message is required to legally enforce any claims of illegal penetration into a system. The warning banner is placed in the Message Text window. Windows NT can display a message box with the caption and text of your choice before a user is given a logon screen. (It is recommended that the exact language of the warning be coordinated with the legal advisors of the organization).

Add a logon notice by adjusting or creating the following two Registry keys.

Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\WindowsNT\Current Version\Winlogon
Name: LegalNoticeCaption
Type: REG_SZ
Value: the text of the title for the dialog box showing the notice

Example Logon Banner:

"This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel. "

Resources

1. Fossen, Jason Windows NT Security: Step-by-Step. SANS GIAC Track 5

2. NT Security News. Available: http://www.ntsecurity.net/.

3. Microsoft Security Bulletins. Available: http://www.microsoft.com/technet/security/.