SERVER SECURITY FOR A DOMINO SERVER

Disclaimer:

This document was prepared to complete the requirements for passing the GIAC certification exam for securing Windows NT system. The security policy implemented is for an administrative server in a college in an academic institution. The purpose is to sufficiently harden the system to prevent unauthorized users and students from possibly bypassing the system security. The author takes no responsibility to the correctness of the information presented here, the suitability of implementation for the stated purpose, or any other liabilities that arise from the use of this document.

Introduction

Our aim in this document is to prepare a server to be used in an academic institution (College administration) where it will be used as a domain controller for authenticating users, provide print and file sharing services, and to be a primary server for a Domino based system for workflow and document storage using domino.doc domino application. It will be used also as a web server for sharing administrative information and to provide directory services and scheduling for the college.

Considering the lack of sufficient number of skilled system administrators to follow up and maintain systems, it is necessary to design the system from the ground up to require very limited support, and to severely degrade the potential of a successful intrusion by unauthorized users or authenticated users.

Hardware selection:

1. Have enough system power and resources to support the number of users and the functionality desired.
2. For high reliability have a system featured with a RAID 5 controller with a minimum of 3 hard drives.
3. Select a fault tolerant system with predictive failure prediction capability.
4. Select a UPS system with sufficient power to support the system, and proper software. The combination should allow the system to gracefully shut down to prevent data corruption and have the ability to notify the system administrator of the power failure.
5. Proper backup system with a scheduling capability.
6. Select a server that can show the results of physical tampering. This is necessary in case someone forced his way to the motherboard to reset the BIOS settings.

Physically Securing the Server

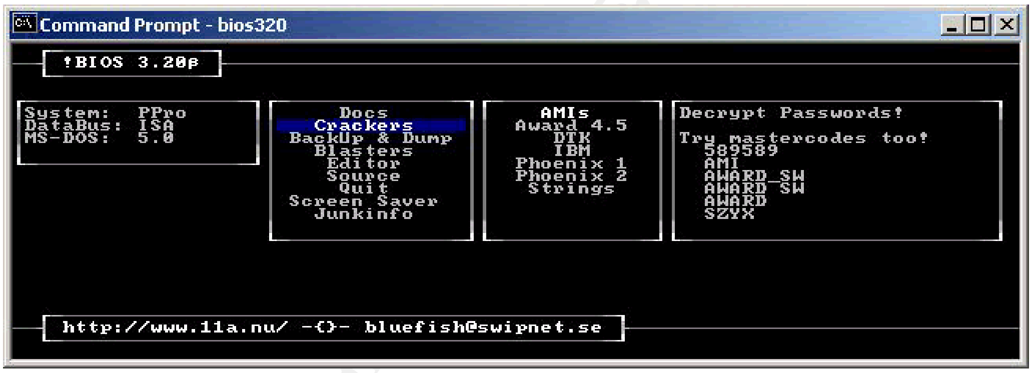
The server should be located at a physically secured location with monitored access. The server cabinet should be locked with access given only to system administrators.

Proper ventilation and temperature monitoring is important to consider in selecting the server location. Make sure that all connections are reliable and power requirements are met. Always connect the server to a switch and never use a hub, this is both for performance consideration and to prevent sniffing of the network traffic.

Hardware configuration of the server

Hardware configuration of the server is essentially the BIOS configuration of the system:

1. Disable the power-on password for the server. Power-on passwords if set can delay system recovery after a power outage since it requires a system administrator to physically walk to the server to enter the password. This is not convenient and can take along time.
2. Enable the Setup password for the BIOS. This is essential in case someone was able to enter the server room and restart the server. It is possible for that person then to steal the SAM database which compromises the whole system security.
3. Make sure in your setup that the system is not configured to boot from either the floppy disk, CD-ROM drive, or a zip drive. Having this capability can cause serious security breach of the system if the system is not physically secure. Further, there exists BIOS password crackers that can retrieve the password hashes from the bios after a floppy boot and can present the intruder with alternative passwords of the BIOS.



```
!BIOS 3.20β

System:   PPro       Docs            AMIs          Decrypt Passwords!
DataBus:  ISA      Crackers       Award 4.5
MS-DOS:   5.0    BackUp & Dump       DTK           Try mastercodes too!
                   Blasters          IBM             589589
                    Editor        Phoenix 1          AMI
                    Source        Phoenix 2          AWARD_SW
                     Quit          Strings           AWARD SW
                 Screen Saver                        AWARD
                   Junkinfo                          SZYX

http://www.11a.nu/ -{}- bluefish@swipnet.se
```

4. Disable all unused ports on the server. For example if the communications ports are not used in the server then disable them from the BIOS. Also consider disabling the USB controller to prevent plug and play devices from being attached to the server and weaken system security.

Network Positioning of the Server

The server is used primarily in the local LAN. However, later it might be decided to allow internet users to access certain type of information and announcements through the Domino web server. In this case it would be necessary to logically position the server in the Demilitarized Zone (DMZ) behind a firewall using a virtual LAN, and allow access from the internet only to port 80. Port 443 (SSL) can be enabled also in case College staff need to access the server remotely.

Windows NT Installation:

Perform a clean installation of the windows NT advanced server operating system. When installing the operating system, it is preferable to perform the installation with the system completely disconnected from the network. This will minimize the possibility of an intruder connecting to the system while in a vulnerable state. Only connect the system to the network after installing and securing the operating system and applying the latest service pack and any necessary patches and hot fixes.

Partitions:

Create multiple partitions on the storage devices. Designate one partition for the operating system files with enough space to host the system and the log files. Note that windows NT does not allow for log files location to be changed, and therefore add additional space on the partition comparable to the log files sizes configured for the system. Also note that service packs and patches can take additional space on this partition. Further, many of the applications installed on the system will add additional files to this partition. Also consider having additional space for a swap file that is equal to the physical RAM of the system. A sample installation of the system after applying the latest service pack and hot fixes resulted in a 300 MB of space consumed by the operating system directory without the space required for the log files. It is important to set the correct size of the system partition since the availability of disk space is essential for Windows NT operation and can cause the system to crash if it runs out of disk space. Configuring the log files with a larger size than the available disk space can crash the system and result in a DOS attack being successful against the server when the logs fill up.

[System Partition size = System + SP&patches + Logs + Swab-Crash-Dump + Additional-DLLs]

Create a dedicated partition for the virtual memory (swap file). Make this partition big enough to host the swap file, the anticipated temp directory files, and the spool files used to store print jobs.

Create a third Partition to host the applications and their data.

Format all partitions using NTFS file system, which is much faster than the FAT file system. NTFS can provide security to the data using access control lists (ACLs) and is better at recovering corrupted data.

Swap Files:

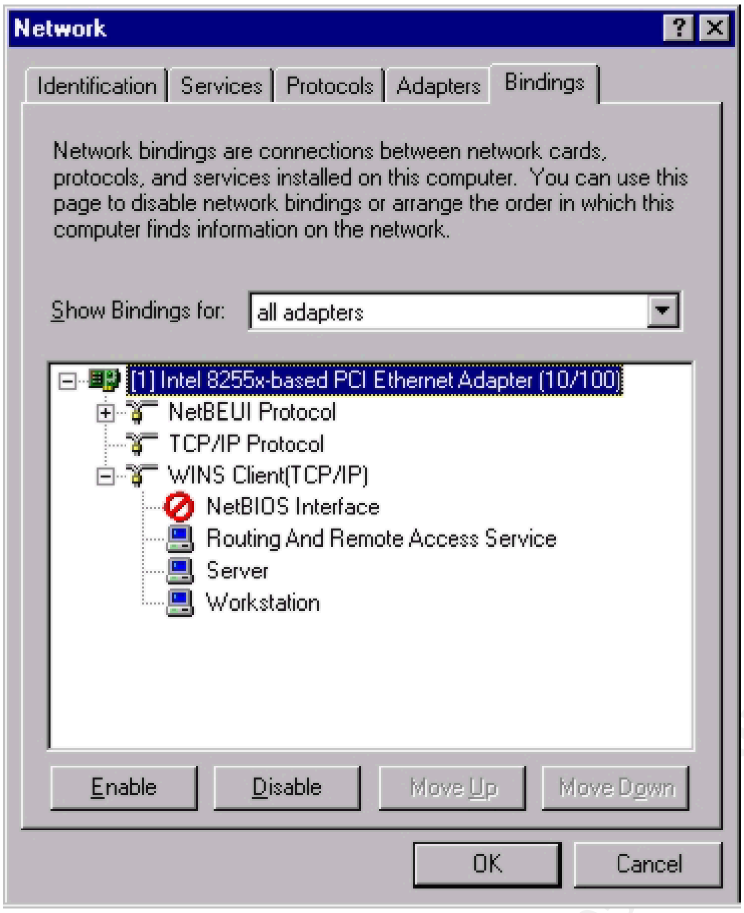
Set a swap file on the Windows NT system partition that is at least equal to the physical RAM available on the system in case the system fails. Also you need to enable crash dump option in the control panel/system/advanced/generate crash dump data file for possible analysis of the system state at the crash to determine the cause of the crash.

The second swap file should be created on its designated partition with at least double the amount of physical RAM of the system. This is necessary to allow the swap file to grow when larger applications are run without running out of swap space. Creating the swap file on a separate partition, other than the operating system's or data's partitions can enhance the performance of the.

Customize the Installation

In installing the system, it is necessary to customize the installation where only the necessary applications and services are installed. For example you should not allow the installation of the Internet Information Server (IIS), or allow the installation of outlook as part of the Internet Explorer setup. Be conscious as to what you allow to reside on the server since adding more programs means more points of vulnerability.

The network protocols and services allow access to the server from the network. Installing many services on the system can provide intruders with information about the system and introduce points of vulnerability when a vulnerability is discovered. Therefore, it is recommended to install the minimum protocols and services necessary for the proper operation of the server for its intended purpose. For this server install only TCP/IP and NetBEUI protocols. Do not install the NetBIOS service as it allows network connections to be shares over TCP/IP. Have TCP/IP bound to a separate network card if using two network cards to separate TCP/IP traffic from Microsoft Network traffic. This is will give the whole bandwidth to Domino and web traffic. This is also specially useful if the administration decides to make the web system available on the internet. Disable the NetBIOS interface on the WINS Client(TCP/IP) in the network bindings, note that this will not break the functionality of the NetBEUI protocol but will restrict the information available through TCP/IP.



Network bindings are connections between network cards, protocols, and services installed on this computer. You can use this page to disable network bindings or arrange the order in which this computer finds information on the network.

Show Bindings for: all adapters

- [1] Intel 8255x-based PCI Ethernet Adapter (10/100)
  - NetBEUI Protocol
  - TCP/IP Protocol
  - WINS Client(TCP/IP)
    - NetBIOS Interface
    - Routing And Remote Access Service
    - Server
    - Workstation

The network services installed on the system should include only:

1. RPC Configuration Service
2. NetBIOS Service
3. Routing and Remote Access Service
4. Workstation Service
5. Server Service

TCP/IP Configuration:

1. Use static IP addresses for your server. Do not use DHCP, otherwise the system might be susceptible to DOS attack by attacking the DHCP server and bringing it offline.
2. Install the RRAS (Routing and Remote Access Server) service to control the protocols you want the server to receive. It is necessary to upgrade to the RRAS instead of using the default TCP/IP filtering capabilities which are at best inadequate.
3. If for future expansion it was desired to publish the web pages of the domino server to the internet, it is necessary to add another Ethernet card and configure the domino server to allow only the http service to access the new card. This card should be part of a virtual LAN (VLAN) that is on the Demilitarized Zone (DMZ). It is crucial then to the IP Forwarding feature between the two hosted Ethernet cards in the system to prevent an attacker from passing from the internet to the local intranet in case the domino server is compromised.

Post Installation Issues

Emergency Repair Disk

The emergency repair disk (ERD) can be very helpful in restoring the system should a repair be required. It contains information about the system configuration and user. Creating the ERD during setup however will not capture any added users to the system, this can be remedied by running the RDISK command in passive mode and then in active mode
Create an Emergency Repair Disk initially by running the command passively:

```
RDISK /S-
```

Which will create current backup files of the SAM database and registry to the %systemroot%\system32\repair directory. Afterwards, run the command interactively to copy the files to the Emergency Repair Disk (floppy). Keep the floppy in a safe and secure place since it has the entire users and the hashes of their passwords. If this disk falls on the wrong hands it means that your system is horribly compromised.
A simple utility from l0pht group called samdump can read the SAM file and dump all the usernames and the hashes of their passwords.

Remove the OS/2 and POSIX Subsystems

Delete \%systemroot%\system32\os2

Delete all subkeys underneath \HKLM\Software\Microsoft\OS/2 Subsystem for NT

Delete value of OS2LibPAth in \HKLM\System\CurrentControlSet\Control\Session Manager\Environment

Clear contents of "Optional" in \HKLM\System\CurrentControlSet\Control\Session Manager\SubSystems, but leave the value "Optional" in place.

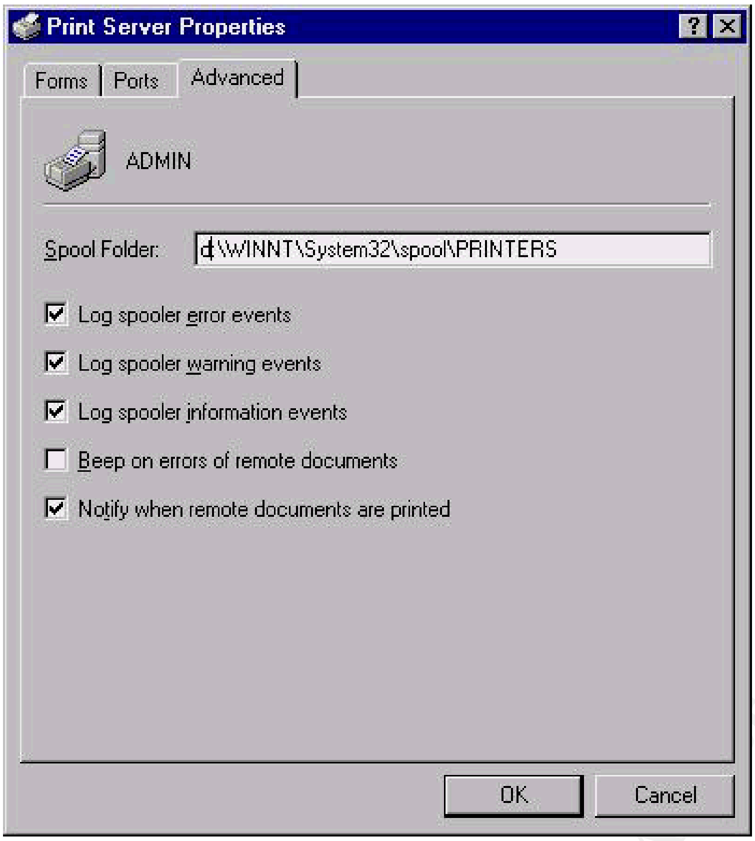
Delete the OS/2 and POSIX subkeys in \HKLM\System\CurrentControlSet\Control\Session Manager\SubSystems

Reboot

(Taken from Securing Windows NT Step by Step – SANS Institute)

Spooler file location configuration:

Change the location of the spooling directory to the partition set up for swap file. From the Start Menu/Settings/Printers, open the printers folder. Under File menu, select Server Properties. Click on the advanced tab and specify the spool folder locations. Note that the folder must be created first before it can be used for storing the spooled files.



Spool Folder: c:\WINNT\System32\spool\PRINTERS

☑ Log spooler error events

☑ Log spooler warning events

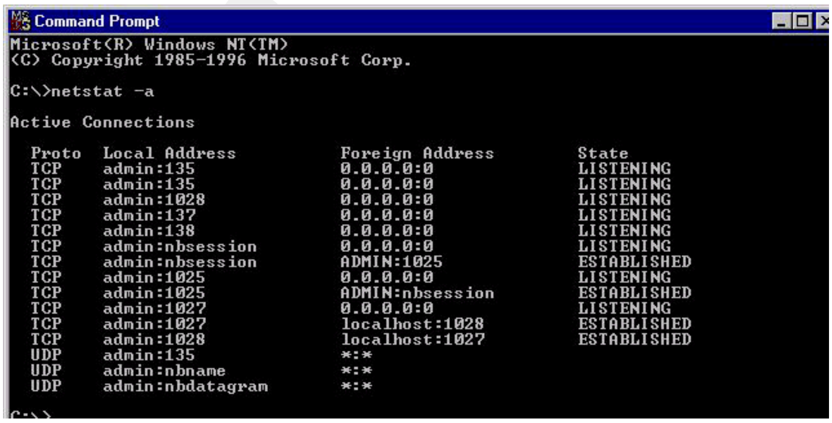
☑ Log spooler information events

□ Beep on errors of remote documents

☑ Notify when remote documents are printed

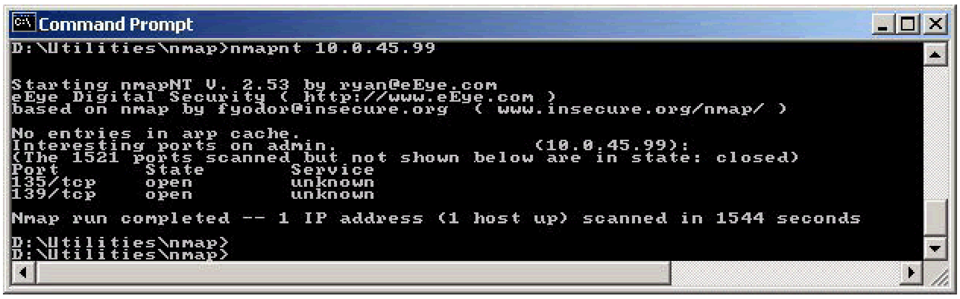
Confirm the Open Network

It is necessary to check the open network ports on the system both locally and from the network after the initial installation. Open network Ports on the system can be checked using the netstat command. Running a port scanner from a remote machine on the server can show the actual open ports on the server as it appears to users and intruders. You should check that only the ports configured show on by a remote scan.



```
Microsoft(R) Windows NT(TM)
(C) Copyright 1985-1996 Microsoft Corp.

C:\>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    admin:135              0.0.0.0:0              LISTENING
  TCP    admin:135              0.0.0.0:0              LISTENING
  TCP    admin:1028             0.0.0.0:0              LISTENING
  TCP    admin:137              0.0.0.0:0              LISTENING
  TCP    admin:138              0.0.0.0:0              LISTENING
  TCP    admin:nbsession        0.0.0.0:0              LISTENING
  TCP    admin:nbsession        ADMIN:1025             ESTABLISHED
  TCP    admin:1025             0.0.0.0:0              LISTENING
  TCP    admin:1025             ADMIN:nbsession        ESTABLISHED
  TCP    admin:1027             0.0.0.0:0              LISTENING
  TCP    admin:1027             localhost:1028         ESTABLISHED
  TCP    admin:1028             localhost:1027         ESTABLISHED
  UDP    admin:135              *:*
  UDP    admin:nbname           *:*
  UDP    admin:nbdatagram       *:*

C:\>
```

Network ports as they show from within the server

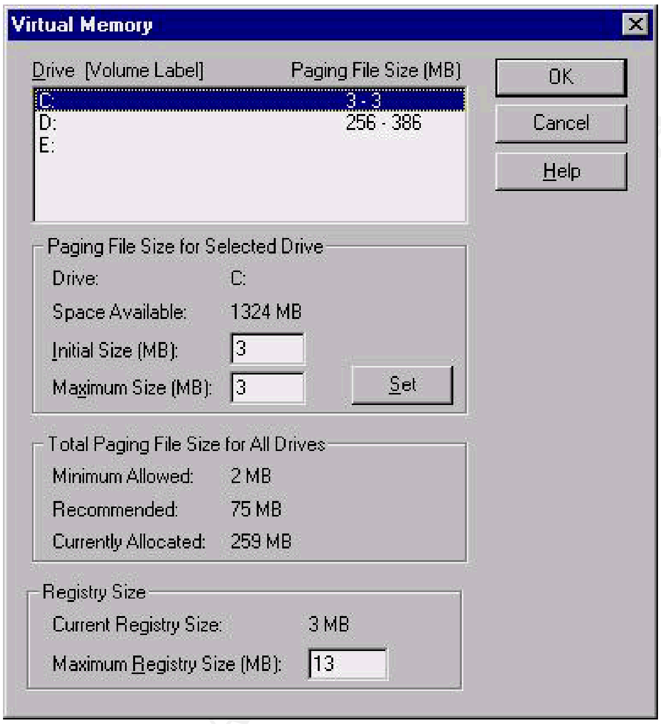


```
D:\Utilities\nmap>nmapnt 10.0.45.99

Starting nmapNT V. 2.53 by ryan@eEye.com
eEye Digital Security ( http://www.eEye.com )
based on nmap by fyodor@insecure.org  ( www.insecure.org/nmap/ )

No entries in arp cache.
Interesting ports on admin.                (10.0.45.99):
(The 1521 ports scanned but not shown below are in state: closed)
Port       State       Service
135/tcp    open        unknown
139/tcp    open        unknown

Nmap run completed -- 1 IP address (1 host up) scanned in 1544 seconds

D:\Utilities\nmap>
D:\Utilities\nmap>
```

Network ports as they appear from a remote scan to the server

Set the virtual memory:

As discussed earlier, the swap files should be located on another partition than the operating system's partition, and its size should be at least twice the size of the physical RAM.. For performance considerations, and if the generated crash dump file can not be analyzed due to the lack of technical skills, it is recommended to reduce the size of swap file on the system partition to a minimum.



Virtual Memory

Drive [Volume Label]	Paging File Size (MB)
C:	3 - 3
D:	256 - 386
E:	

Paging File Size for Selected Drive

Drive: C:

Space Available: 1324 MB

Initial Size (MB): 3

Maximum Size (MB): 3

Total Paging File Size for All Drives

Minimum Allowed: 2 MB

Recommended: 75 MB

Currently Allocated: 259 MB

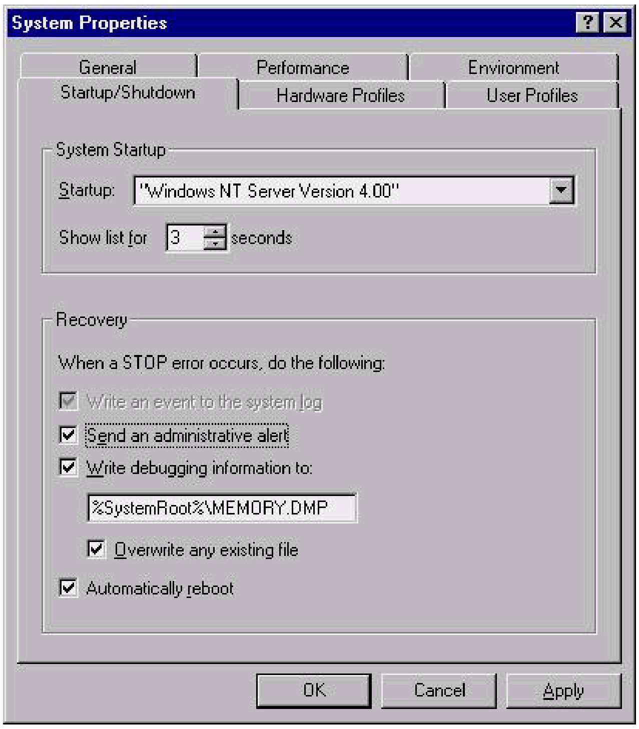
Registry Size

Current Registry Size: 3 MB

Maximum Registry Size (MB): 13

Recovery Options

Set the recovery options used when to the system crashes to send an administrative alert and reboot the system automatically. If crash dump information are needed, increase the swap file size on the system partition to be at least the size of the physical RAM and check the box to "Write debugging information to"



System Startup

Startup: "Windows NT Server Version 4.00"

Show list for 3 seconds

Recovery

When a STOP error occurs, do the following:

☑ Write an event to the system log

☑ Send an administrative alert

☑ Write debugging information to:

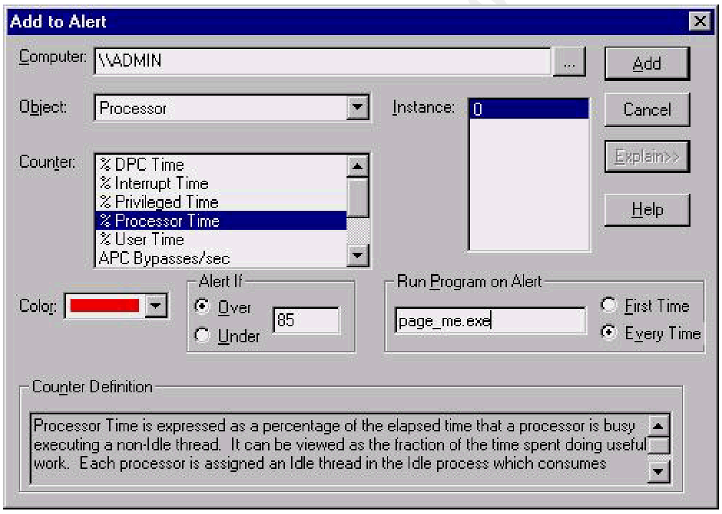
%SystemRoot%\MEMORY.DMP

☑ Overwrite any existing file

☑ Automatically reboot

Monitor the System for DOS Attack

Denial of Service attacks can result in a variety of effects on the server including crashing the system to the BSOD or increasing the CPU usage to 100%. When the system is under normal operation it seldom exceeds a CPU threshold usage 80% for a long period of time. We can set an administrative alert using the performance monitor to page the system administrator whenever this threshold is exceeded to signify the possibility of a DOS attack. This can be set using the Performance Monitor Alerts in the Administrative Tools:



Computer: \\ADMIN

Object: Processor

Instance: 0

Counter:
% DPC Time
% Interrupt Time
% Privileged Time
% Processor Time
% User Time
APC Bypasses/sec

Color: 🟥

Alert If
● Over 85
○ Under

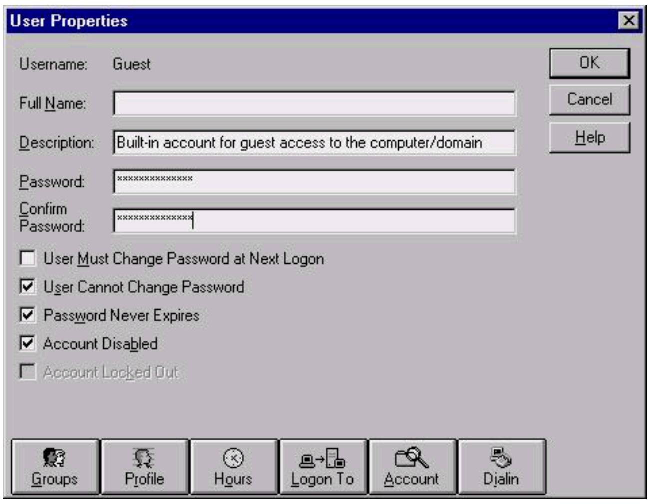
Run Program on Alert
page_me.exe
○ First Time
● Every Time

Counter Definition

Processor Time is expressed as a percentage of the elapsed time that a processor is busy executing a non-Idle thread. It can be viewed as the fraction of the time spent doing useful work. Each processor is assigned an Idle thread in the Idle process which consumes

Disable the Guest Account

Disable the guest account to prevent unauthorized users from connecting to the server. If a user is connecting to the server with invalid username, the system tries to log him in using as a guest if the guest account is enabled. If we set a password on the Guest account, then the system will require the invalid user to enter the same password set for the Guest account. It is therefore important to set a Guest password that is very hard to guess. Further, for our purpose, we will disable the account completely.



User Properties

Username: Guest

Full Name:

Description: Built-in account for guest access to the computer/domain

Password: xxxxxxxxxxxxxx

Confirm Password: xxxxxxxxxxxxxx

□ User Must Change Password at Next Logon

☑ User Cannot Change Password

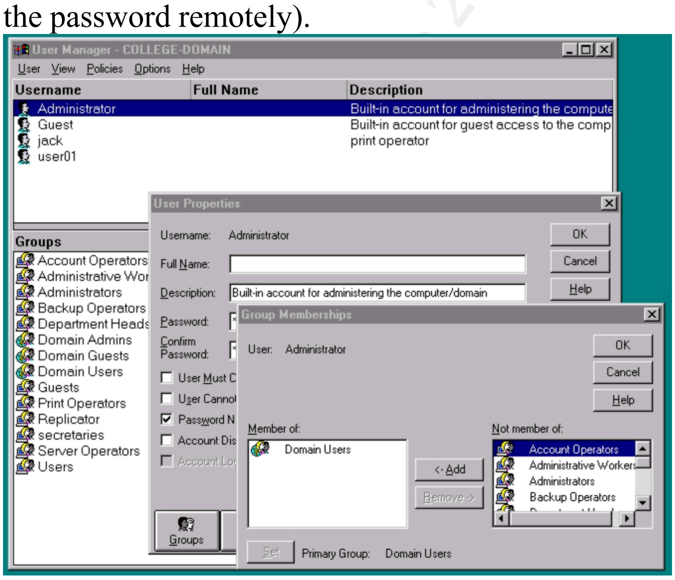
☑ Password Never Expires

☑ Account Disabled

□ Account Locked Out

Protect the Administrator Account

The administrator account has a great power and therefore it should be protected. Since the Administrator account name is well known, it is helpful to create a decoy Administrator account with no privileges. This is accomplished by copying the administrator account to a new account to preserve the account description, and rename the actual administrator account to a different name with a different description (such as jack account, with ‘print operator’ description). Rename the copy of the administrator account back to Administrator and make sure to remove this account from the Administrators and Domain Administrators groups. Set a hard password for this account (include extended ASCII code keys to make it hard to crack the password remotely).



User Manager - COLLEGE-DOMAIN

Username	Full Name	Description
Administrator		Built-in account for administering the compute
Guest		Built-in account for guest access to the comp
jack		print operator
user01		

Groups

Account Operators
Administrative Wor
Administrators
Backup Operators
Department Heads
Domain Admins
Domain Guests
Domain Users
Guests
Print Operators
Replicator
secretaries
Server Operators
Users

User Properties

Username: Administrator

Full Name:

Description: Built-in account for administering the computer/domain

Password:

Confirm Password:

□ User Must C

□ User Cannot

☑ Password N

□ Account Dis

□ Account Loc

Group Memberships

User: Administrator

Member of:

Domain Users

Not member of:

Account Operators
Administrative Workers
Administrators
Backup Operators

Primary Group: Domain Users

Since the administrator account by default cannot be locked with multiple bad login attempts, it is susceptible to dictionary and brute force attack remotely. It is necessary to enable the locking feature on the administrator account when accessed through the network. This is achieved by using the windows NT resource kit program

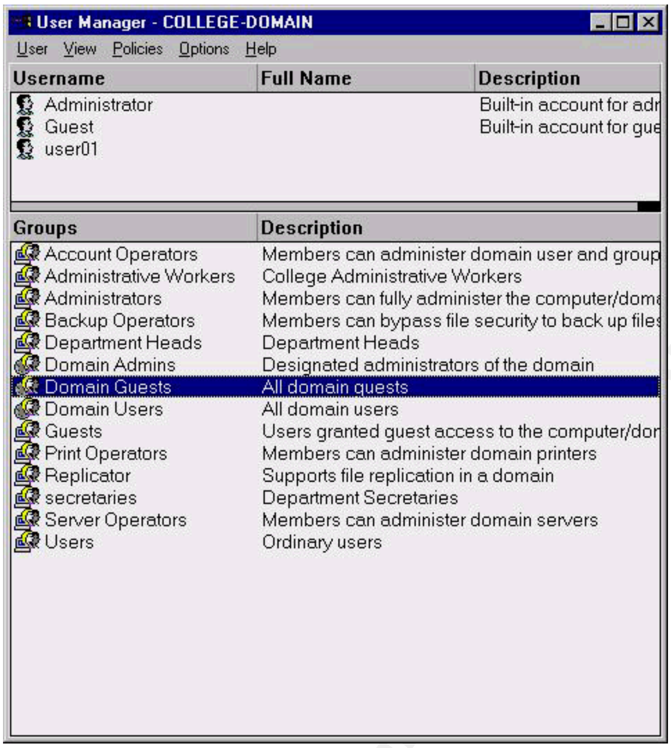
PASSPROP.EXE using the command line:

```
Passprop /adminlockout
```

Note that this will force the system administrator to login locally on the server to enable the account again.

Define Users Roles

To manage users effectively and provide each user with enough access rights to perform his work, it is necessary to group the users into different access levels and to create a Local group on the server for each type of users. These local groups in conjunction with Global groups can provide effective access control over users, and will simplify the work needed in assigning permissions for users.



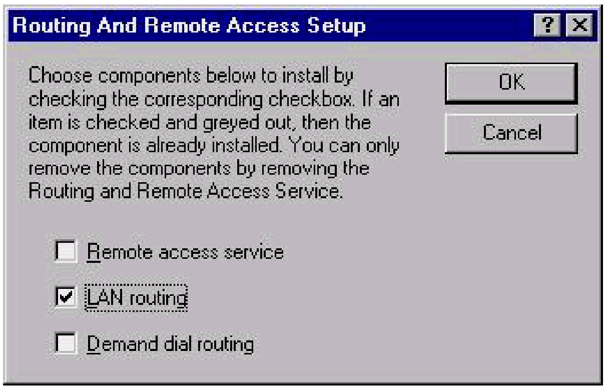
Username	Full Name	Description
Administrator		Built-in account for adr
Guest		Built-in account for gue
user01		

Groups	Description
Account Operators	Members can administer domain user and group
Administrative Workers	College Administrative Workers
Administrators	Members can fully administer the computer/doma
Backup Operators	Members can bypass file security to back up files
Department Heads	Department Heads
Domain Admins	Designated administrators of the domain
Domain Guests	All domain guests
Domain Users	All domain users
Guests	Users granted guest access to the computer/dor
Print Operators	Members can administer domain printers
Replicator	Supports file replication in a domain
secretaries	Department Secretaries
Server Operators	Members can administer domain servers
Users	Ordinary users

Control Network Access to Server

To allow the system administrator some control over the access to the server from the network, Microsoft has replaced the security configuration of the network ports accessed through the advanced button in the TCP/IP protocol properties of the control panel with a more robust and effective packet filtering service that can give control over inbound and outbound network traffic. This new service is called the Routing and Remote Access Service (RRAS) and is freely downloadable from Microsoft site at http://www.microsoft.com/NTServer/nts/downloads/winfeatures/rras/rrasdown.asp

RRAS can provide effective packet-filtering functionality to limit connections to and from the server by port number and IP address of clients.
Download and install the RRAS Service. Since no dialup connection is configured in the server, select only LAN Routing


Routing And Remote Access Setup

Choose components below to install by checking the corresponding checkbox. If an item is checked and greyed out, then the component is already installed. You can only remove the components by removing the Routing and Remote Access Service.

□ Remote access service

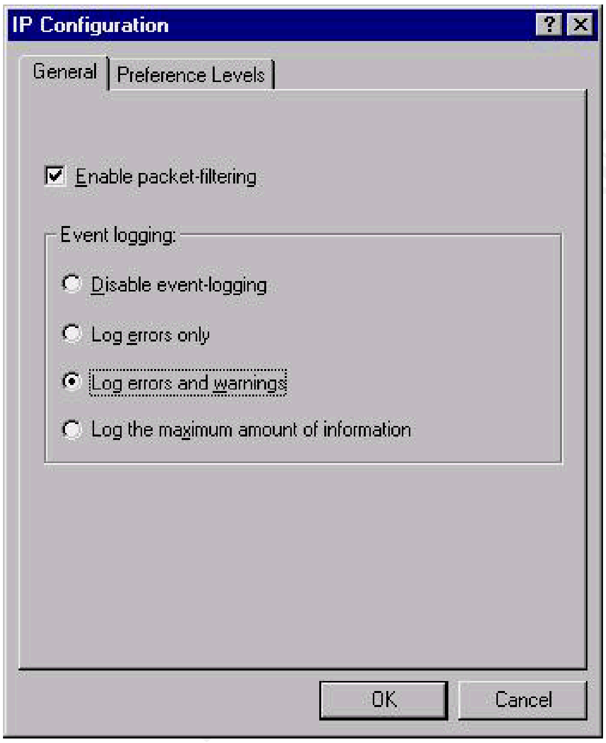
☑ LAN routing

□ Demand dial routing

The RRAS can be managed remotely using the GUI installed with the service at

%SystemRoot%\System32\MPRADMIN.EXE. A command line tool is also available that can be used remotely with scripting support called ROUTEMON.EXE.

Before you can use the packet filtering feature of RRAS it is necessary to turn the packet filtering feature on by selecting the “Enable Packet Filtering” checkbox in the “IP Configuration” window of the interface card:


IP Configuration

General | Preference Levels

☑ Enable packet-filtering

Event logging:

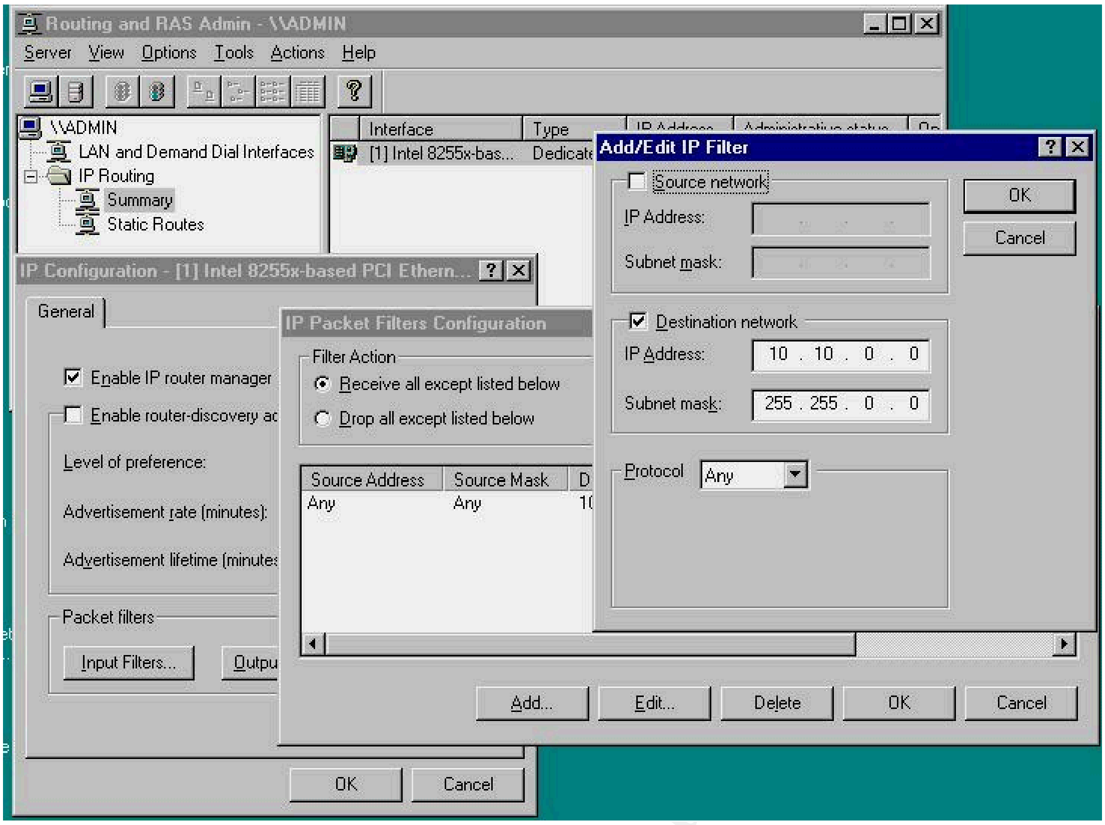
○ Disable event-logging

○ Log errors only

● Log errors and warnings

○ Log the maximum amount of information

It is then necessary to select “Configure Interface” to add new filters for inbound and outbound connections per machine and per protocol.


Routing and RAS Admin - \\ADMIN
Server View Options Tools Actions Help
\\ADMIN
LAN and Demand Dial Interfaces
IP Routing
Summary
Static Routes
Interface
Type
[1] Intel 8255x-bas...
Dedicate
IP Configuration - [1] Intel 8255x-based PCI Ethern...
General
IP Packet Filters Configuration
Add/Edit IP Filter
Packet filters
Input Filters...
Outpu
Add...
Edit...
Delete
OK
Cancel

☑ Enable IP router manager
□ Enable router-discovery ac
Level of preference:
Advertisement rate (minutes):
Advertisement lifetime (minutes

Filter Action
● Receive all except listed below
○ Drop all except listed below

Source Address	Source Mask	D
Any	Any	1(

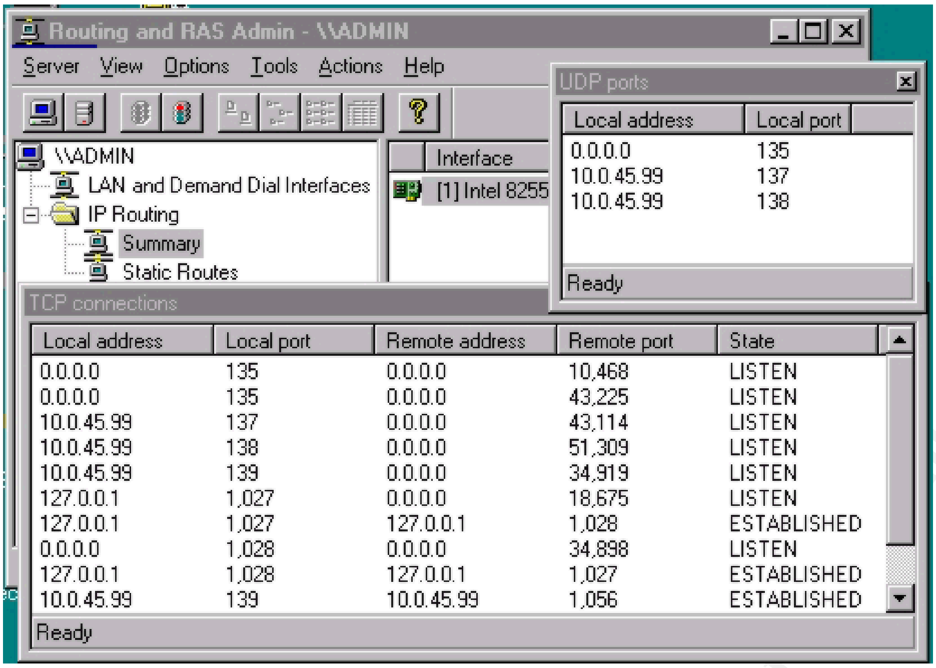
□ Source network
IP Address:
Subnet mask:

☑ Destination network
IP Address: 10 . 10 . 0 . 0
Subnet mask: 255 . 255 . 0 . 0

Protocol: Any

This tool allows the administrator very specific control on who is allowed to connect to the server and through which protocol and which port. It can be used to specifically allow only certain machines to connect to the server and denies everybody else in a high security environment.

The RRAS can show which network ports are open on the server, this includes both tcp and udp ports. It can also list all the network connections of the server with the remote machines. The list of ports are dynamically updates. This information can also be obtained across the network.


Routing and RAS Admin - \\ADMIN
Server View Options Tools Actions Help
\\ADMIN
LAN and Demand Dial Interfaces
IP Routing
Summary
Static Routes
Interface
[1] Intel 8255
UDP ports
TCP connections

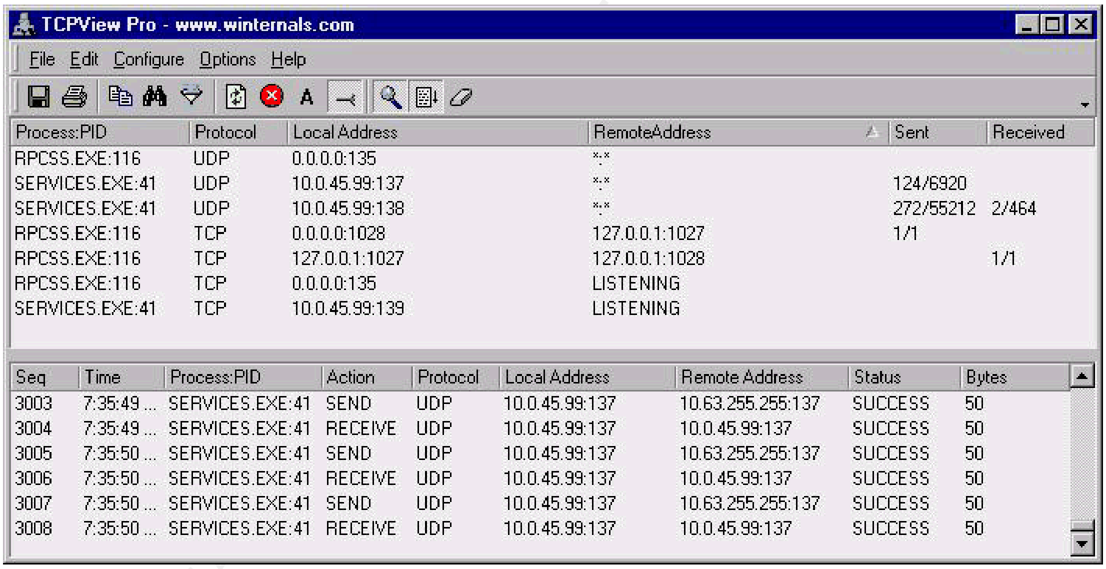
Local address	Local port
0.0.0.0	135
10.0.45.99	137
10.0.45.99	138

Ready

Local address	Local port	Remote address	Remote port	State
0.0.0.0	135	0.0.0.0	10,468	LISTEN
0.0.0.0	135	0.0.0.0	43,225	LISTEN
10.0.45.99	137	0.0.0.0	43,114	LISTEN
10.0.45.99	138	0.0.0.0	51,309	LISTEN
10.0.45.99	139	0.0.0.0	34,919	LISTEN
127.0.0.1	1,027	0.0.0.0	18,675	LISTEN
127.0.0.1	1,027	127.0.0.1	1,028	ESTABLISHED
0.0.0.0	1,028	0.0.0.0	34,898	LISTEN
127.0.0.1	1,028	127.0.0.1	1,027	ESTABLISHED
10.0.45.99	139	10.0.45.99	1,056	ESTABLISHED

Ready

The only drawback for this service is the lack of association between the opened network ports and the applications and services using tem. This problem is resolved by a program called TCPView from www.winternals.com which can list both the open network ports and the services/programs using them. A screenshot is shown here.


TCPView Pro - www.winternals.com
File Edit Configure Options Help

Process:PID	Protocol	Local Address	RemoteAddress	Sent	Received
RPCSS.EXE:116	UDP	0.0.0.0:135	*:*		
SERVICES.EXE:41	UDP	10.0.45.99:137	*:*	124/6920	
SERVICES.EXE:41	UDP	10.0.45.99:138	*:*	272/55212	2/464
RPCSS.EXE:116	TCP	0.0.0.0:1028	127.0.0.1:1027	1/1	
RPCSS.EXE:116	TCP	127.0.0.1:1027	127.0.0.1:1028		1/1
RPCSS.EXE:116	TCP	0.0.0.0:135	LISTENING		
SERVICES.EXE:41	TCP	10.0.45.99:139	LISTENING		

Seq	Time	Process:PID	Action	Protocol	Local Address	Remote Address	Status	Bytes
3003	7:35:49 ...	SERVICES.EXE:41	SEND	UDP	10.0.45.99:137	10.63.255.255:137	SUCCESS	50
3004	7:35:49 ...	SERVICES.EXE:41	RECEIVE	UDP	10.0.45.99:137	10.0.45.99:137	SUCCESS	50
3005	7:35:50 ...	SERVICES.EXE:41	SEND	UDP	10.0.45.99:137	10.63.255.255:137	SUCCESS	50
3006	7:35:50 ...	SERVICES.EXE:41	RECEIVE	UDP	10.0.45.99:137	10.0.45.99:137	SUCCESS	50
3007	7:35:50 ...	SERVICES.EXE:41	SEND	UDP	10.0.45.99:137	10.63.255.255:137	SUCCESS	50
3008	7:35:50 ...	SERVICES.EXE:41	RECEIVE	UDP	10.0.45.99:137	10.0.45.99:137	SUCCESS	50

A list of the windows used ports is available at: http://www.microsoft.com/WINDOWS2000/library/resources/reskit/samplechapters/cnfc/cnfc_por_zqyu.asp

System Updates:

Installing the system and configuring it properly is not sufficient to keep the system secure. Over time new problems with the operating system are found which can be exploited by hackers. Also new functionalities might be added by Microsoft. Therefore, it is necessary to stay up to date with the new developments. Such information as new vulnerabilities, availability of new patches, hot fixes, and service packs can be obtained from multiple sources, some of theses sources are:

1. Microsoft Security Bulletins and Advisories, (http://www.microsoft.com/security).
2. NTBugtraq Security Mailing List (http://www.securityfocus.com)
3. SANS NewsBites (www.sans.org)

Microsoft develops a patch for new vulnerabilities and announce their existence. However, these patches sometimes are not sufficiently tested and might not work appropriately. Therefore it is necessary to test these patches on a non-production system to make sure it functions with the installed software before deploying them to the production system. Other updates to the system are released in the form of Hot Fixes. Patches and Hot fixes are then incorporated in a service pack. Installing the latest service pack and any pertinent hot fixes and patches to the system will bring the system up to date, and is a necessary procedure to follow before putting the system in a production environment.

Service Pack

The current service pack is SP6a, which is a re-release of SP6 fixing a problem with lotus notes "winsock connection refused" error which is detailed in Q246009 (http://support.microsoft.com/support/kb/articles/Q246/0/09.ASP). The list of problems fixed in SP6a are available in two parts :

Q241211 (http://support.microsoft.com/support/kb/articles/Q241/2/11.ASP)

Q244690 (http://support.microsoft.com/support/kb/articles/Q244/6/90.ASP)

Service Pak 6a is available for download from:
http://www.microsoft.com/ntserver/nts/downloads/recommended/SP6/allSP6.asp

If you are not sure which service pack you installed in your system check either

If HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Hotfix\Q246009\Installed = 1, it's SP6a.

or run winver program from the command line, if it shows the following, then you have SP6a installed:

```
Microsoft(R) Windows NT (R)
Version 4.0 (Build 1381: Service Pack 6)
Copyright (C) 1981-1996 Microsoft Corp
Revised Service Pack 6a
```

Service packs should always be reapplied after any changes in the operating system.

Patches and Hot Fixes:

Patches and hot fixes post service pack 6a are located at
http://www.microsoft.com/technet/security/current.asp?productID=51
It is very important to keep up with Microsoft advisories since for the last two years (1999, 2000) Microsoft has released more than 50 advisories for each year. Some of these advisories were very serious in the problems they fix that if the system is left

without applying the patch it will leave the system open to remote attack that results in a total compromise of the system.

Status of Patches and Hot Fixes

Although SP6a is the latest service pack to the Windows NT Server 4.0 operating system, many new patches were released after it. Also, a survey of the post service pack patches showed that some of the problems that were fixed with a patch after the release of service pack 5 were not incorporated in Service Pack 6a, and therefore will have to be applied manually if the system configuration requires it.

The following table shows the advisories with patches available since the release of Service Pack 5. Assuming that you have applied SP6a, the status column indicates the status of the vulnerability in your system. Note that some of the problems reported before SP6a was released are still not fixed in SP6a and the patches released post-SP5 cannot be installed on the system if SP6a is installed. This list covers announcements after SP5 to end of August, 2000.

Make sure to reapply the service pack whenever new hardware or software is installed.

Date	Description	Status	Recommendation
July 28, 2000	**MS00-052: Patch Available for "Relative Shell Path" Vulnerability**	Not Fixed	Apply Manually
July 27, 2000	**MS00-047: Patch Available for "NetBIOS Name Server Protocol Spoofing" Vulnerability**	Not Fixed	Apply Manually
June 08, 2000	**MS00-040: Patch Available for "Remote Registry Access Authentication " Vulnerability**	Not Fixed	Apply Manually
May 25, 2000	**MS00-036: Patch Available for "ResetBrowser Frame" and "HostAnnouncement Flooding" Vulnerabilities**	Not Fixed	Apply Manually
May 19, 2000	**MS00-029: Patch Available for "IP Fragment Reassembly" Vulnerability**	Not Fixed	Apply Manually
April 20, 2000	**MS00-027: Patch Available for "Malformed Environment Variable" Vulnerability**	Not Fixed	Apply Manually
April 12, 2000	**MS00-024: Tool Available for "OffloadModExpo Registry Permissions" Vulnerability**	Not Fixed	Apply Manually
March 30, 2000	**MS00-021: Patch Available for "Malformed TCP/IP Print Request" Vulnerability**	Not Fixed	Apply Manually
March 9, 2000	**MS00-008: Patch Available for "Registry Permissions" Vulnerability**	Not Fixed	Apply Manually
February 1, 2000	**MS00-007: Patch Available for "Recycle Bin Creation" Vulnerability**	Not Fixed	Apply Manually
January 21, 2000	**MS00-004: Patch Available for "RDISK Registry Enumeration File" Vulnerability**	Not Fixed	Apply Manually
January 17, 2000	**MS00-005: Patch Available for "Malformed RTF Control Word" Vulnerability**	Not Fixed	Apply Manually
December 16, 1999	**MS99-057: Patch Available for "Malformed Security Identifier Request" Vulnerability**	Not Fixed	Apply Manually
December 16, 1999	**MS99-056: Patch Available for "Syskey Keystream Reuse" Vulnerability**	Not Fixed	Apply Manually
December 9, 1999	**MS99-055: Patch Available for "Malformed Resource Enumeration Argument" Vulnerability**	Not Fixed	Apply Manually
November 4, 1999	**MS99-047: Patch Available for "Malformed Spooler Request" Vulnerability**	Not Fixed	Apply Manually
October 22, 1999	**MS99-046: Patch Available to Improve TCP Initial Sequence Number Randomness**	Not Fixed	Apply Manually
September 30, 1999	**MS99-041: Patch Available for "RASMAN Security Descriptor" Vulnerability**	Not Fixed	Apply Manually
September 20, 1999	**MS99-038: Patch Available for "Spoofed Route Pointer" Vulnerability**	Not Fixed	Fix will not install on SP6a

September 10, 1999	**MS99-036: Windows NT 4.0 Does Not Delete Unattended Installation File**	Not Fixed	Perform Manually if needed
September 3, 1999	**MS99-034: Patch Available for "Fragmented IGMP Packet" Vulnerability**	Not Fixed	Fix will not install on SP6a.
July 29, 1999	**MS99-026: Patch Available for "Malformed Dialer Entry" Vulnerability**	Fixed	No Action Necessary
July 6, 1999	**MS99-024: Patch Available for "Unprotected IOCTLs" Vulnerability**	Fixed	No Action Necessary
June 30, 1999	**MS99-023: Patch Available for "Malformed Image Header" Vulnerability**	Not Fixed	Fixed in SP 5
June 23, 1999	**MS99-021: Patch Available for "CSRSS Worker Thread Exhaustion" Vulnerability**	Fixed	No Action Necessary
June 23, 1999	**MS99-020: Patch Available for "Malformed LSA Request" Vulnerability**	Fixed	No Action Necessary
May 28, 1999	**MS99-017: Patch Available for "RAS and RRAS Password" Vulnerability**	Fixed	No Action Necessary
May 20, 1999	**MS99-016: Patch Available for "Malformed Phonebook Entry" Vulnerability**	Fixed	No Action Necessary
May 17, 1999	**MS99-015: Patch Available for "Malformed Help File" Vulnerability**	Fixed	No Action Necessary

Clients Used

- Since the security of the server and the network is a prime concern, only Windows NT workstations are allowed as clients to the server. This is requested since the security of the server can be jeopardized by an intruder obtaining a normal user account from a vulnerable client. The clients should have service pack 6a installed on them, and should be allowed to authenticate with the server only using NTLMv2 by setting the registry key (HKLM\System\CurrentControlSet\Control\Lsa\LMCompatibilityLevel) value to 3.
- Also Disable administrative shares on all clients (C$, D$, …, Admin$) which are created by default. Use the following to disable auto sharing
  It is possible to disable the automatic sharing by adding the value
  Value name: AutoShareWks
  Value Type : REG_DWORD
  Value Data : 0
  Key: HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters
- Disable remote browsing of registry by securing the registry key:

  HKLM\CurrentControlSet\Control\SecurePipeServers\Winreg
- Note that these settings can be pushed to the clients when designing a login script for users.
- Require a screen password with password locking ability
- Install anti-virus programs on all clients, and constantly update them.

Hardening the System

Further measures are necessary to protect the system before being accessible by clients.

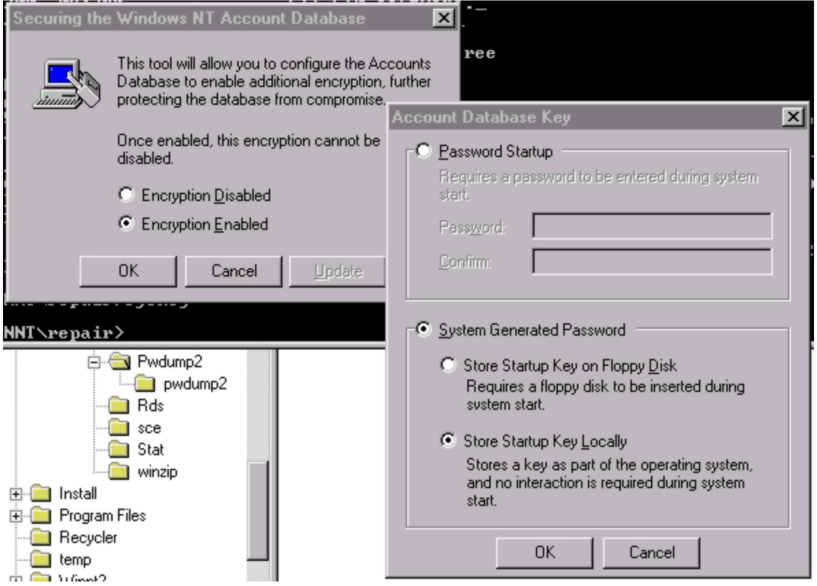
DOS Attack

Fine Tune the System to minimize the effects of a SYN flood that can cause a DOS: A SYN flood tries to tie up the resources of the NT Server, to minimize the impact of the attack it is necessary to fine-tune the default parameters windows uses in dealing with initiated but uncompleted SYN requests. After applying SP6a, check the following registry value: \HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect and set its value to 2 (if not available, create the REG_DWORD value called SynAttackProtect in \HKLM\System\CurrentControlSet\Services\Tcpip\Parameters, and set its value to 2). This will reduce the retransmission of the SYN-ACK retries to free the system for legitimate connections. For additional information to further tune the system up to minimize the DOS attacks effects refer to knowledge base article Q142641 on http://www.microsoft.com/TechNet/security/dosrv.asp.

Securing the SAM Database

The SAM database is used by the operating system to store the hashes of the passwords of the system users. It is possible for an intruder to retrieve the hashes of the passwords from the SAM database to gain access to the system. Since the SAM database is usually backed up in the \%systemroot%\repair folder when the Rdisk /S-command is issued or an emergency repair disk is created, the entire copy of the SAM database can be copied from this directory if someone has access to the server (unlike the active SAM file). Therefore it is important to keep the machine physically secure and restrict the shares area. This also means storing the Emergence Repair Disks in a very secure place. Permissions for this directory should not allow regular users to read/write files in this directory. NTFS permissions should be set to limit their access. Microsoft has released a program called SYSKEY that can encrypt the SAM database file. Use SYSKEY to encrypt the SAM database to prevent intruders from accessing the password hashes should they have access to the SAM database file.

Note that encrypting the SAM database does not prevent l0pht crack program from retrieving the password hashes from the registry should the intruder have access to the registry either locally or over the network.



This tool will allow you to configure the Accounts Database to enable additional encryption, further protecting the database from compromise.

Once enabled, this encryption cannot be disabled.

○ Encryption Disabled
● Encryption Enabled

○ Password Startup
Requires a password to be entered during system start.
Password:
Confirm:

● System Generated Password

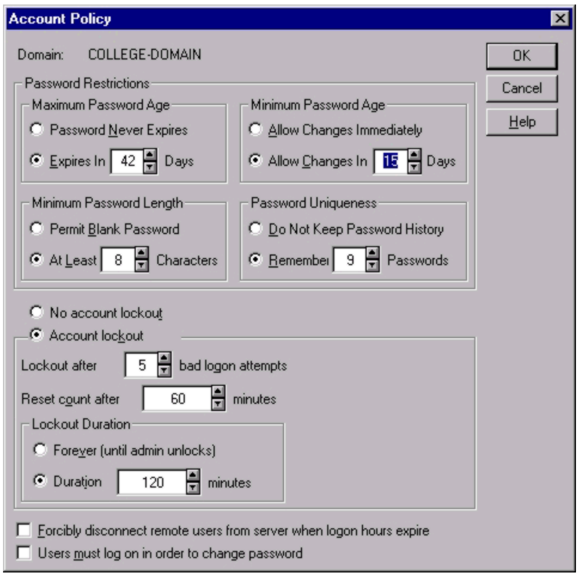
○ Store Startup Key on Floppy Disk
Requires a floppy disk to be inserted during system start.

● Store Startup Key Locally
Stores a key as part of the operating system, and no interaction is required during system start.

Password Issues

Enforcing a strong password policy is an important issue for the security of the server.

1. From the user manager, change the default system password/account policy as follows



Account Policy

Domain: COLLEGE-DOMAIN

Password Restrictions

Maximum Password Age
○ Password Never Expires
● Expires In 42 Days

Minimum Password Age
○ Allow Changes Immediately
● Allow Changes In 15 Days

Minimum Password Length
○ Permit Blank Password
● At Least 8 Characters

Password Uniqueness
○ Do Not Keep Password History
● Remember 9 Passwords

○ No account lockout
● Account lockout

Lockout after 5 bad logon attempts
Reset count after 60 minutes

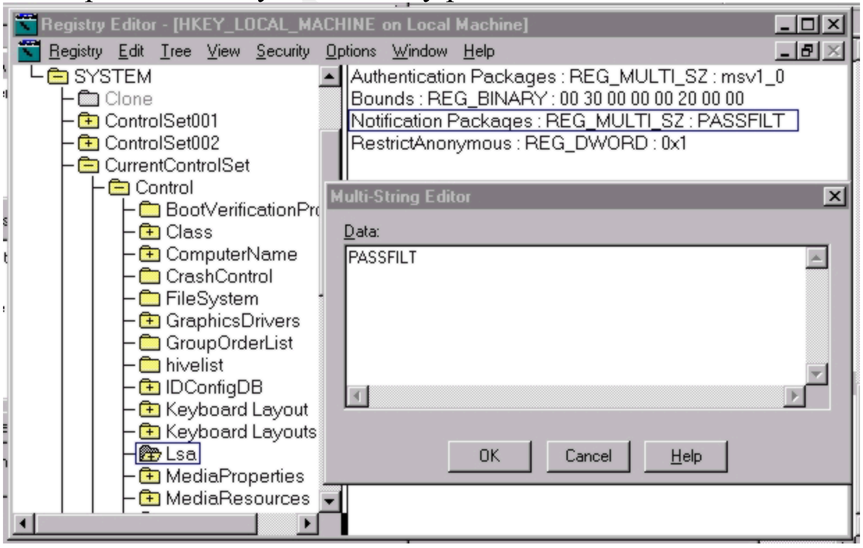
Lockout Duration
○ Forever (until admin unlocks)
● Duration 120 minutes

□ Forcibly disconnect remote users from server when logon hours expire
□ Users must log on in order to change password

   Note that the minimum password age is set to 15 days. This is done to prevent users from cycling through the remembered passwords to activate the old (favorite) password again.

2. Implement the password filters and make sure that the password sub-authentication subsystem is active. Modify the registry key *HKLM/system/CurrentControlSet/Control/Lsa/Notification* Packages to PASSFILT

   Setting the PASSFILT option will require any password to include at least three of the following: upper case letters, lower case letters, numbers, and non-alphanumeric symbols in any password.



Registry Editor - [HKEY_LOCAL_MACHINE on Local Machine]

```
SYSTEM
  Clone
  ControlSet001
  ControlSet002
  CurrentControlSet
    Control
      BootVerificationPr
      Class
      ComputerName
      CrashControl
      FileSystem
      GraphicsDrivers
      GroupOrderList
      hivelist
      IDConfigDB
      Keyboard Layout
      Keyboard Layouts
      Lsa
      MediaProperties
      MediaResources
```

```
Authentication Packages : REG_MULTI_SZ : msv1_0
Bounds : REG_BINARY : 00 30 00 00 00 20 00 00
Notification Packages : REG_MULTI_SZ : PASSFILT
RestrictAnonymous : REG_DWORD : 0x1
```

Multi-String Editor

Data: PASSFILT

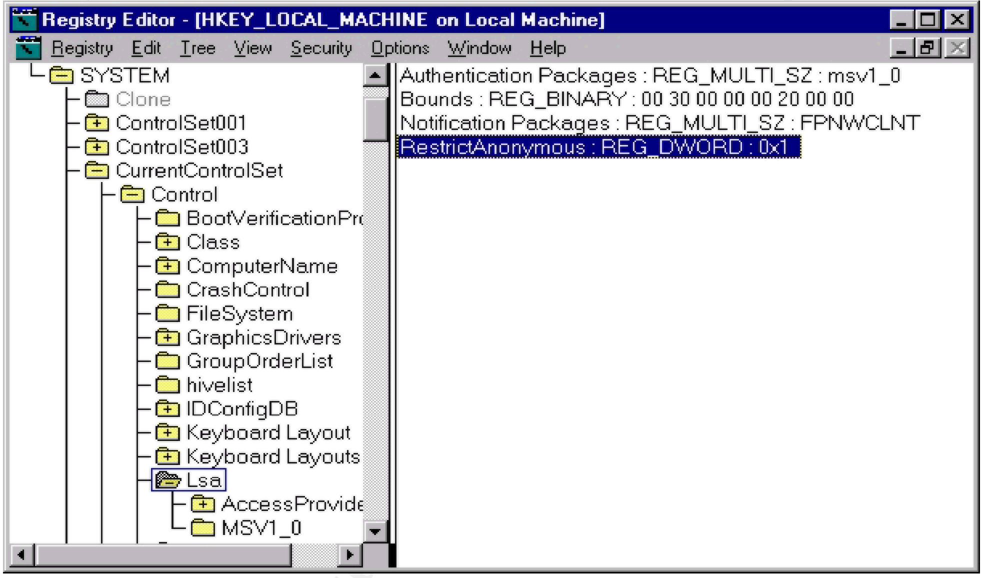
3. Use the resource kit program PASSPROP.EXE to activate complex passwords:

   PASSPROP /complex

Limit non-users Access to Server and Resources

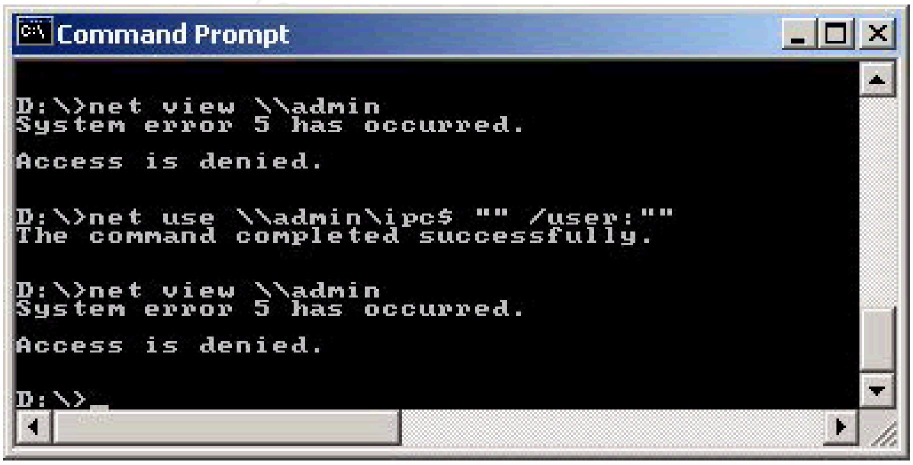
Controlling the "Null Session" Access

A null session is created between the client and the server when a process/user access the server with a null username and null password. This user is considered part of the everyone group. This is a universal access method of windows NT servers which is used primarily for Inter-Process Communication (IPC) between servers and clients. It is an essential service for proper operation of the server and some applications. However, this connection does not require any kind of authentication and could allow a malicious user to obtain certain information about the server and users. This includes the ability to list users names, groups, shares, security policy, …etc. To properly secure the system, it is necessary to control the information available through null sessions without breaking the system or the running applications.
RestrictAnonymous registry key can be used to prevent anonymous connections to the \\servername\ipc$ named pipe. Setting this value to 1 will disable null users connections but will not affect the operation of the Domino server, the file and print sharing, or authentication of users to the server.



```
Authentication Packages : REG_MULTI_SZ : msv1_0
Bounds : REG_BINARY : 00 30 00 00 00 20 00 00
Notification Packages : REG_MULTI_SZ : FPNWCLNT
RestrictAnonymous : REG_DWORD : 0x1
```

When RestrictAnonymous is implemented, a remote user without account can not view resources on the server even when trying the IPC$ null user session.



```
D:\>net view \\admin
System error 5 has occurred.

Access is denied.

D:\>net use \\admin\ipc$ "" /user:""
The command completed successfully.

D:\>net view \\admin
System error 5 has occurred.

Access is denied.

D:\>_
```

Prevent "null session" users from using shared resources

Implementing RestrictAnonymous registry value can limit the information available to non-users of the system but does not disable the "null session" connection. Looking at the previous Command Prompt screenshot, we notice that null session command was completed successfully. This means that the session was actually established. Knowing that that "null session" user is a member of the everyone group, having any share on the server with permissions for the everyone group will allow the remote "null session" user to access the share. Creating the following REG_DWORD value called RestrictNullSessAccess to 1 in the following registry key

HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters

will disallow null users from accessing shares even if they are set accessible by the Everyone group. Exception to this restriction are set by the value name NullSessionShares of type REG_MULTI_SZ under the same registry key. This exception will still allow null sessions to access the listed resources, primarily, to prevent the system from failing.

Prevent users from listing scheduled jobs
Using the security menu option in the regedt32.exe registry editor, remove all user's permissions to access the following registry key except for Administrators and SYSTEM account.:

HKLM\System\CurrentControlSet\Services\Schedule

Even after installing service pack 6a the permissions allow authenticated users to list the scheduled jobs on the server.

Securing Named Pipes

Secure the NetLogon Channel
To prevent man in the middle attack during login, it is necessary to secure the NetLogon channel by digitally signing the packets to ensure their integrity, and by encrypting the traffic. Make using signing or encryption required for the connection to succeed. This is implemented by using the following registry values

SignSecureChannel	set to 1
SealSecureChannel	set to 1
RequireSignOrSeal	set to 1

Which should be added under the registry key:

HKLM\CurrentControlSet\Services\NetLogon\Parameters

Using these settings prevent l0pht crack from intercepting the password hashes when in packet capture mode.

Limit Authentication Traffic to NTLMv2 - Prevent NTLM and LM authentication

Windows NT server can support authentication using LanManager (LM), Windows NT (NTLM), and NTLMv2. LM and NTLM hashes incorporate weak encryption by today's standards and can be broken with today's desktop machine's power, Further, the hashes can be captured from the network using simple programs like L0PHT crack sniffer or many other programs. NTLMv2 uses a challenge response where the server uses the user's password as an encryption key to create a challenge to the client, and therefore the password hash is not transmitted on the network. The algorithm also uses a timestamp to verify that the response is timely.

Limit the server's authentication to NTLMv2 and prevent LM and NTLM authentication by setting LMClientLevel value to 5 in the following registry key:

Set HKLM\System\CurrentControlSet\Control\Lsa\LMCompatibilityLevel to 5

Make sure that all clients have this value set to 3 to force clients to use NTLMv2 only for authentication.

Make sure that both the clients and server have the same level of encryption by installing the latest update to Internet Explorer and installing the 128-bit encryption. It becomes necessary here also to have use the high encryption service pack 6a afterwards to update the system.

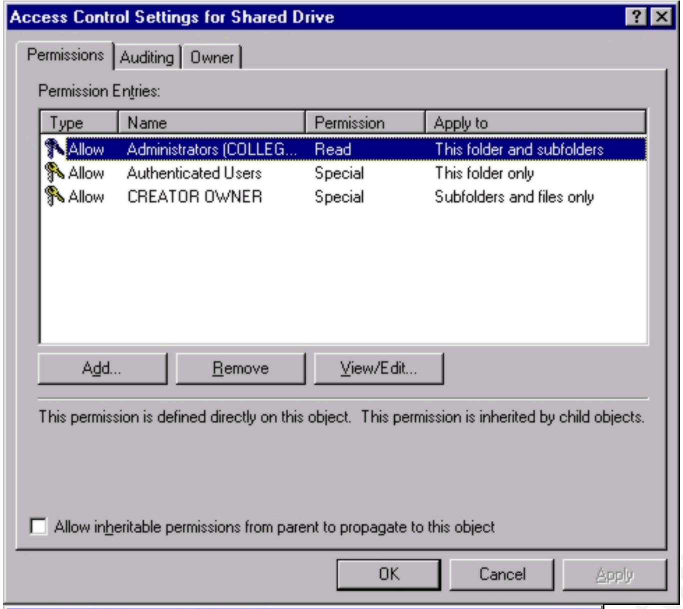
Server Shares

- Do not create any shares that expose the system files to users.
- Administrative shares (C$, D$, Admin$) are created by default on the server. It is possible to disable the automatic sharing by adding the value AutoShareServer of type REG_DWORD and setting its value to 0 under the registry key:
  HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters
- When creating shares be very specific of what you are sharing. Make sure to combine the NTFS and share permissions to fine-tune the access privileges of the share.
- Create a public share on the NTFS data partition for users. This share should allow for privacy between the users without involving the administrator. The settings proposed here will have each directory created by a user protected from other users while preserving the users full control over the directory:

  Automatic Permission Adjustment on Public Share

  Since this server will be used to authenticate users and for file sharing and print services. It is necessary to create a public shared drive (directory) that allows all authenticated users to create directories and store their files and to automatically protect each created directory from being accessed by other users while giving the owner of the directory full access to it. The following set of permissions allows every authenticated user that right, allows the administrator to list the contents of the created directories without having access to the data or programs stored. It also prevent any other user from accessing or listing directories of other users. The only problem with this configuration is that it does not allow the user to change the name of the created directory on the share (the directory name will be "New Folder (1), …", and therefore it is suggested that each user create a directory on his local drive with the name he desires, then copy that directory to the shared drive. The user will have full control inside his created directory, even deleting his directory.

To create this configuration, create a share with full access to Authenticated Users group from the share menu. Then using the NTFS permissions define the following:



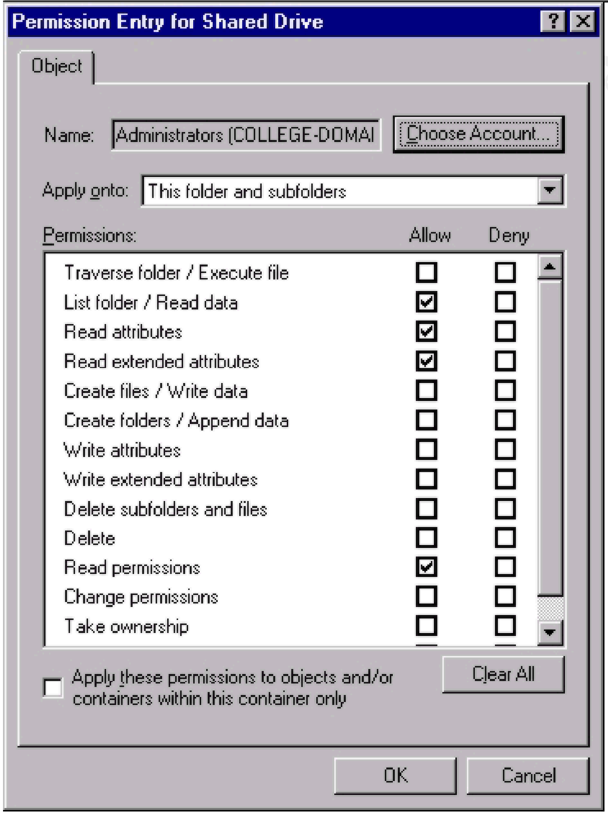
Access Control Settings for Shared Drive

Permission Entries:

Type	Name	Permission	Apply to
Allow	Administrators (COLLEG...	Read	This folder and subfolders
Allow	Authenticated Users	Special	This folder only
Allow	CREATOR OWNER	Special	Subfolders and files only

This permission is defined directly on this object. This permission is inherited by child objects.

☐ Allow inheritable permissions from parent to propagate to this object



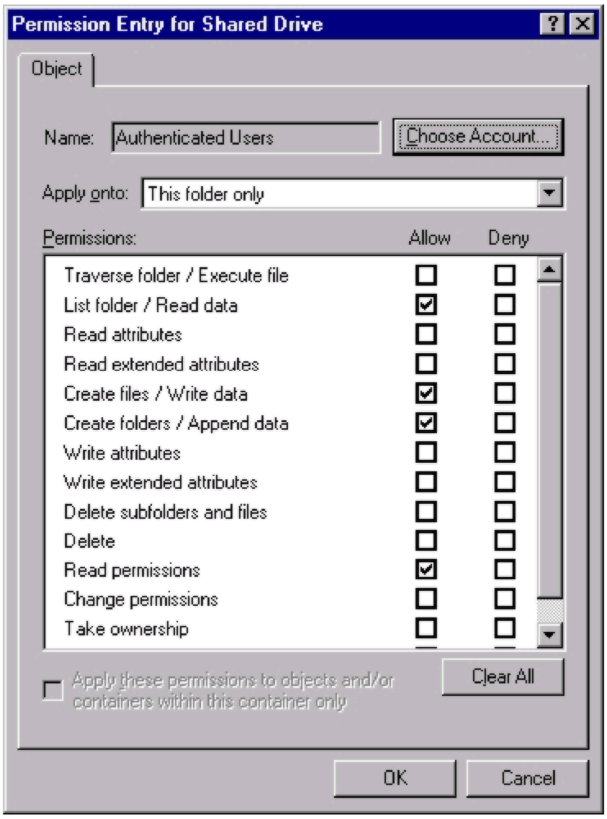
Permission Entry for Shared Drive

Name: Administrators (COLLEGE-DOMAI

Apply onto: This folder and subfolders

Permissions:	Allow	Deny
Traverse folder / Execute file	☐	☐
List folder / Read data	☑	☐
Read attributes	☑	☐
Read extended attributes	☑	☐
Create files / Write data	☐	☐
Create folders / Append data	☐	☐
Write attributes	☐	☐
Write extended attributes	☐	☐
Delete subfolders and files	☐	☐
Delete	☐	☐
Read permissions	☑	☐
Change permissions	☐	☐
Take ownership	☐	☐

☐ Apply these permissions to objects and/or containers within this container only



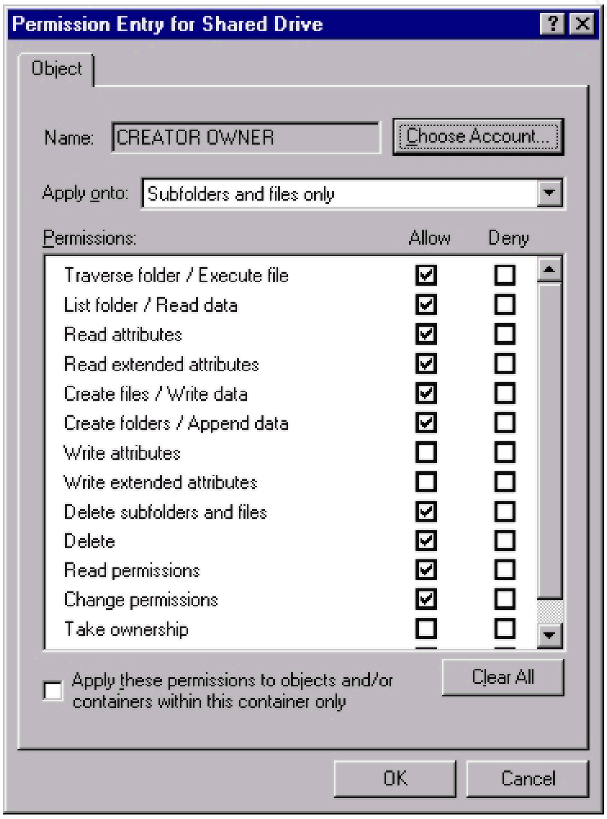
Permission Entry for Shared Drive

Name: Authenticated Users

Apply onto: This folder only

Permissions:	Allow	Deny
Traverse folder / Execute file	□	□
List folder / Read data	☑	□
Read attributes	□	□
Read extended attributes	□	□
Create files / Write data	☑	□
Create folders / Append data	☑	□
Write attributes	□	□
Write extended attributes	□	□
Delete subfolders and files	□	□
Delete	□	□
Read permissions	☑	□
Change permissions	□	□
Take ownership	□	□

□ Apply these permissions to objects and/or containers within this container only



Permission Entry for Shared Drive

Name: CREATOR OWNER

Apply onto: Subfolders and files only

Permissions:	Allow	Deny
Traverse folder / Execute file	☑	□
List folder / Read data	☑	□
Read attributes	☑	□
Read extended attributes	☑	□
Create files / Write data	☑	□
Create folders / Append data	☑	□
Write attributes	□	□
Write extended attributes	□	□
Delete subfolders and files	☑	□
Delete	☑	□
Read permissions	☑	□
Change permissions	☑	□
Take ownership	□	□

□ Apply these permissions to objects and/or containers within this container only

System Path

A misconfigured path can allow an authenticated user to store programs on the server in an unprotected area of the file system and then have the system invoke that program. One example is the Sub-Authentication package configured by default into windows NT, where the system will look for the Sub-Authentication packages listed under the registry key : HKLM\System\CurrentControlSet\Lsa\MSV1_0 and hand it the user name and password for further action before the user is logged in. Windows NT by default will look for "FPNWCLNT" which is a sub-authentication package, if not installed, the Trojaned program on the path will be invoked under the SYSTEM authority. Since NetWare is not used on this server, it is recommended to delete ths value "FPNWCLNT" from the registry key MSV1_0, and checking the system path, and making sure that each directory on the path is restricted by NTFS permissions.

Control Network Access to the Registry

Enable auditing on the registry access

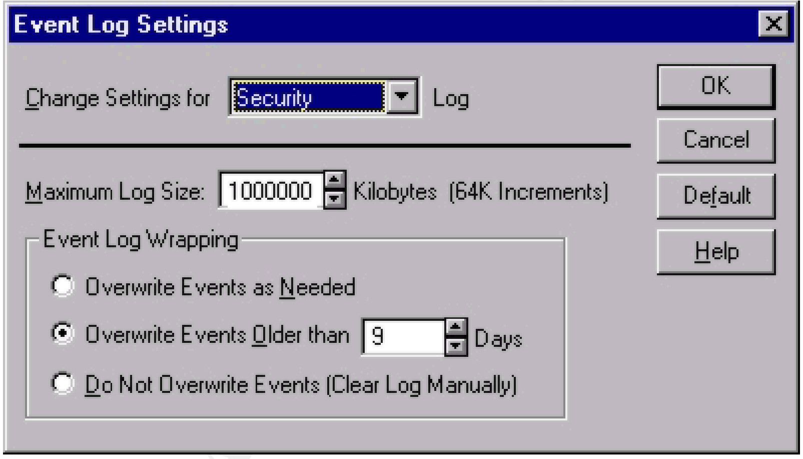
Disable remote browsing or registry by securing the registry key:

HKLM\CurrentControlSet\Control\SecurePipeServers\Winreg

Using the registry editor regedt32.exe, select security – permissions and allow only Administrators Full Control. Remove all others from the list.

Event Logs Management

Increase the logs size as much as possible. Of special consideration is the security log which will host the audit logs and can indicate signs of intrusion.



Event Log Settings

Change Settings for Security Log

Maximum Log Size: 1000000 Kilobytes (64K Increments)

Event Log Wrapping

○ Overwrite Events as Needed
● Overwrite Events Older than 9 Days
○ Do Not Overwrite Events (Clear Log Manually)

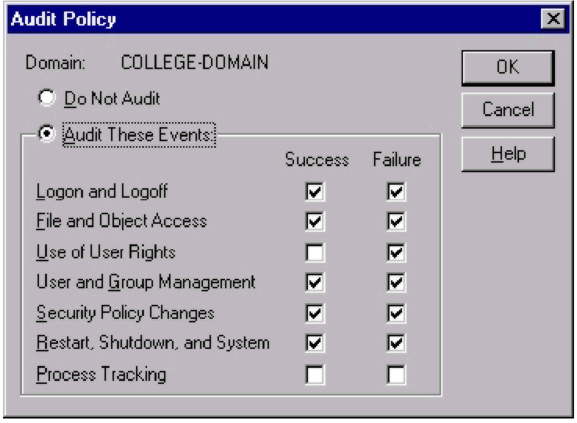
Configure the event logger to overwrite events older than 9 days. In order to keep track of the server logs even after they are overwritten it is necessary to download the event logs to the administrator's machine for analysis and archiving on CD-ROMs.

SomarSoft have released DUMPEVT, a command line tool that can read the event log of the server remotely and store it in a specific directory. It can also track the point of the last dump so that no duplicate data is stored. On the administrator workstation, schedule DUMPEVT to download the event logs from the server to the local machine. Create a directory "college-domain" with three subdirectories for the three event logs (app, sec, sys) and schedule the following commands:

```
dumpevt /computer=admin /logfile=sec /outfile=d:\college-domain\security\security.txt
dumpevt /computer=admin /logfile=sys /outfile=d:\college-domain\system\system.txt
dumpevt /computer=admin /logfile=app /outfile=d:\college-domain\applications\applications.txt
```

Enable Auditing on the system

Logging system events can help in the analysis of intrusion attempts and how far in the system the intrusion has been successful. Of special importance is the logging of failed events. Although it might be normal daily event that a user mistypes his password and retries for two times, logging of this activity on the system can show intrusion attempts when multiple users accounts show the same behavior. Security audit log can show even who attempted to access the registry remotely. Periodic download and analysis of the security log is vital for the well being of the system.



Domain: COLLEGE-DOMAIN

○ Do Not Audit

● 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	□	□

User Rights Changes

Many of the changes that were necessary with earlier service packs have been fixed. Only minor changes need to be done here:

- Bypass traverse checking: no one
- Force Shutdown from a remote server : Administrators only
- Logon locally: Administrators, backup operators, server operators
- Disallow “bypass traverse checking” for everyone

Screen Saver

Using a screen password protected screen saver with a very short time before the system is locked down can help in locking the system in case the administrator becomes distracted and leaves the console logged in. It is better to select a blank screensaver to eliminate the possibility of a crash of the screen saver that might leave the system unprotected.

Install virus scanners

Install virus scanners on the server and the client machines. Virus scanners can protect the server resources and clients, and prevent infected files from residing on the server. This will minimize the possibility of viruses spreading to the different clients or the server and its applications. A special virus scanner should be installed that functions with the Domino server to scan all e-mail and file attachments. It is essential to update the virus information files routinely and when a new virus breakout is announced in the security lists.

Security Policies Tools

Two tools are freely available from Microsoft to help in enforcing system policies, these are system policy editor, and the Security Configuration Editor.

system policy editor

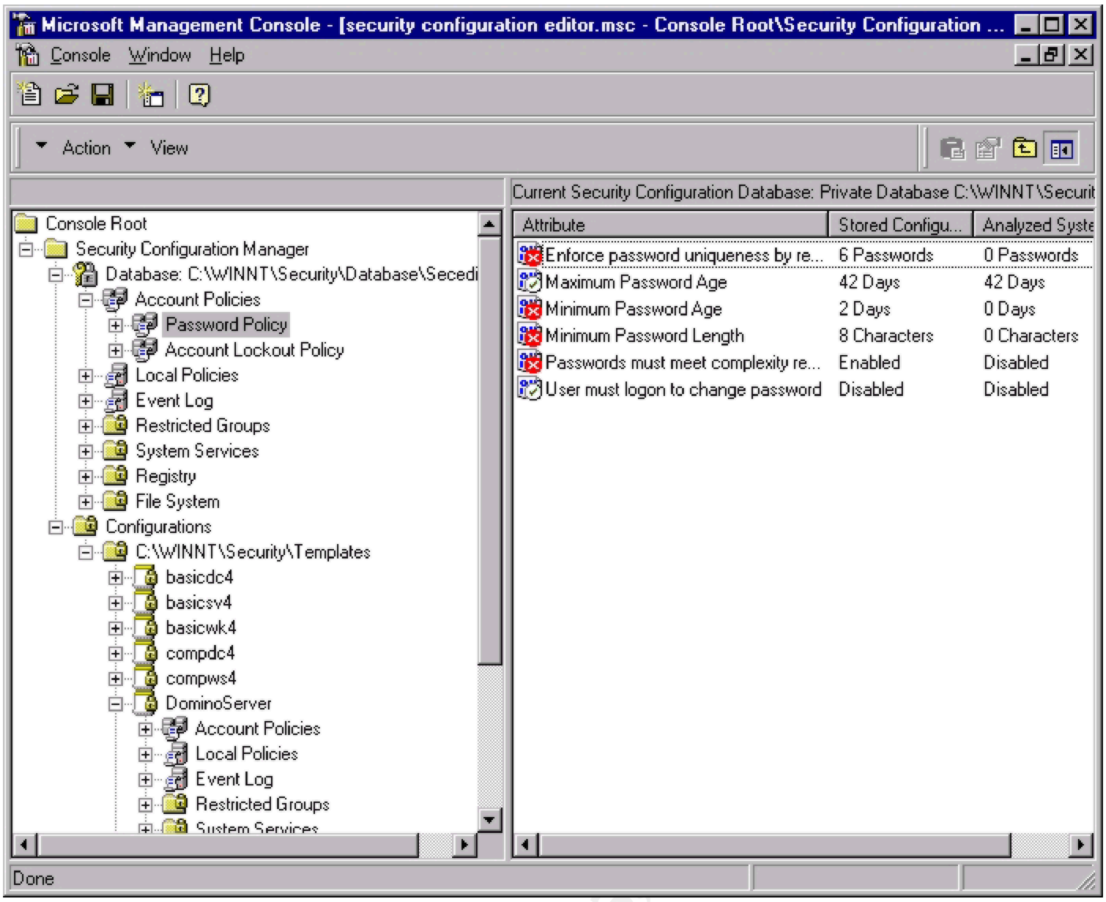
Is used to create individual policies for users and machines when they login to the server. It is possible to apply many restrictions to the machines and users. However, this tool is aimed primarily at protecting the client machine from misuse of the logged-in user.

Security Policy Editor (SCE)

The Microsoft Security Configuration (MS-SCE) Editor is used to design and implement a security policy for the system. It can be used to design a security policy for the server or for the client machines, however, they must be implemented locally in each machine not across the network.

MS-SCE can implement security policies for accounts, local machine, event log, restricted groups, system services, registry values, security on registry keys, and NTFS permissions.

Microsoft has released along with the MS-SCE tool many templates for both clients and server machines. One of these templates is for high security domain controller. Copy this template and save it as DominoServer template. Since this template has the largest configurable parameters, it is suggested that you review all parameters in the template and check its applicability for your server. After updating the template, it is necessary to analyze the live system against the sittings defined in the template, this will result in a view like the one shown here which compares the template configuration to the active configuration. After reviewing this analysis, you can configure your system according to the template.



Attribute	Stored Configu...	Analyzed Syste
Enforce password uniqueness by re...	6 Passwords	0 Passwords
Maximum Password Age	42 Days	42 Days
Minimum Password Age	2 Days	0 Days
Minimum Password Length	8 Characters	0 Characters
Passwords must meet complexity re...	Enabled	Disabled
User must logon to change password	Disabled	Disabled

DOMINO Issues

This document is not about installing, securing, or operating a Domino server. It is about preparing a secure server for Domino to run on. Therefore, security issues for the Domino server are not discussed. Only some points are mentioned here Domino has some security issues

- Allow only tcpip ports, disable netbios and ipx ports
- Do not install the Domino Directory NT Sync Services
- Select Install Domino as a service option during the installation
- During installation, allow domino setup to add Anonymous account to all databases with no access, then allow anonymous access on a database by database case.
- Configure domino not to allow browsing of databases for web users.
- Obtain and install a certificate for the server, if not interested, use the Server Certificate Administration database (certsrv.nsf) to create self certified certificate to activate SSL on the server.
- Secure the services registry key to prevent unauthorized change:
  HKLM\System\CurrentControlSet\Services\Lotus Domino Server (LotusDominoData)
  so that only the SYSTEM and Administrator accounts can have change capability
- Encrypt Databases that are sensitive.
- Encrypt network traffic if sniffing is a problem.
- Allow anonymous web browsing of the Domino-http web server area. Create a web page as a default entry point that lists all the public databases with links to the Domino Data Directory.
- Secure the certifier id
- When accessing sensitive databases over the web, Check the option to activate web access through SSL in the database properties windows to encrypt all network traffic.
- When designing databases of a secure nature, make sure that not only you secure the desired views, it is vital to secure the sensitive fields of the data.
- Install a Domino-specific virus scanner to actively monitor all e-mail and attached files for viruses and stop infected files from being transmitted to clients before they are cleaned. Constantly update the virus definition files.

After installing the Domino server many new network ports are opened.

1352	notes client
25	SMTP incoming and outgoing connections
80	Web server
443	SSL for web server connections
389	LDAP Connections
636	LDAP SSL connections
63148	IIOP connection port
63149	SSL IIOP connections
2039 – 2043	For Desktop Enabled applications
2129 – 2142	For Desktop Enabled applications

It is necessary to configure these ports in the RRAS to allow incoming connections to the server.