CompTIA Security+® Lab Series

Lab 18: Access Control/Audit

CompTIA Security+® Domain 5 - Access Control and Identity Management

Objective 2.3: Explain the fundamental concepts and best practices related to authentication, authorization and access control

Document Version: 2013-08-02

Organization: Moraine Valley Community College
Author: Jesse Varsalone

The original works of this document were funded by the National Science Foundation's (NSF) Advanced Technological Education (ATE) program Department of Undergraduate Education (DUE) Award No. 0702872 and 1002746; Center for Systems Security and Information Assurance (CSSIA) at Moraine Valley Community College (MVCC).

Contents

Introduction

This lab is part of a series of lab exercises designed through a grant initiative by the Center for Systems Security and Information Assurance (CSSIA) and the Network Development Group (NDG), funded by the National Science Foundation's (NSF) Advanced Technological Education (ATE) program Department of Undergraduate Education (DUE) Award No. 0702872 and 1002746. This work has been adapted by The Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48. This series of lab exercises is intended to support courseware for CompTIA Security+® certification.

By the end of this lab, students will be able to configure access control lists on a folder, set up auditing on a specific folder, and to view the Event Viewer for Security Incidents.

This lab includes the following tasks:

1 – Configuring ICMP on the Firewall
2 – Configuring Auditing for Object Access
3 – Viewing the Security Log to Determine Security Incidents

Objectives: Explain the security function and purpose of network devices and technologies

Companies need to protect their internal resources. This is often done by restricting access to files and folders using access control lists. An administrator has the ability to restrict access to files and configure auditing to log any attempted breaches.

NTFS – New Technology File System, or NTFS, is a Windows File System that allows users to configure security permissions on a file or folder to restrict object access.

ACL – An Access Control List, or ACL, restricts users from accessing files or folders.

Security Log – Within the Event Viewer, the Security Log has success and failure logs.

Auditing – A process by which items such as file and folder access are tracked.

Group Policy – The Group Policy editor can be utilized within the Microsoft Windows operating system to perform tasks such as turning on auditing for object access.

Pod Topology

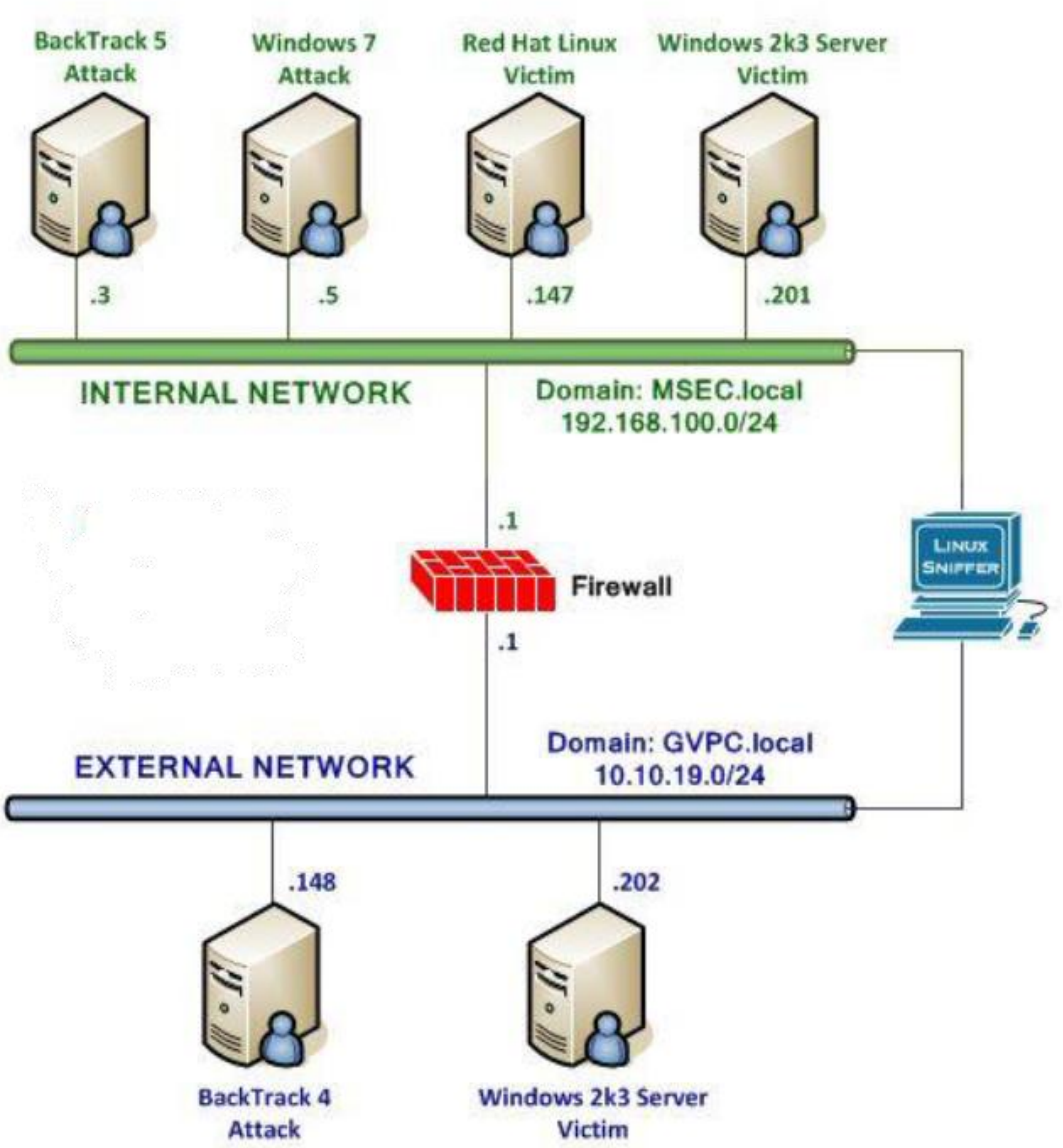


Figure 1: Topology

Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

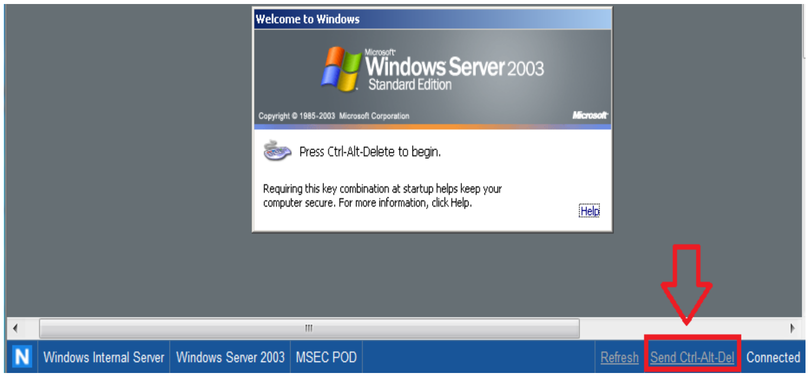
Required Virtual Machines and Applications

Log in to the following virtual machine before starting the tasks in this lab:

Windows 2k3 Server Internal Victim Machine	192.168.100.201
Windows 2k3 Server administrator password	password

Windows 2003 Server Login:

1. Click on the **Windows2k3 Server Internal Victim** icon on the topology
2. Use the PC menu in the NETLAB+ Remote PC Viewer to send a **Ctrl-Alt-Del** (version 2 viewer), or click the **Send Ctrl-Alt-Del** link in the bottom right corner of the viewer window (version 1 viewer).



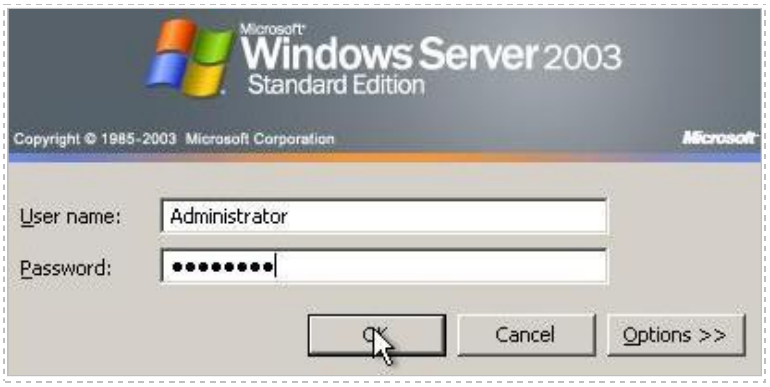
Welcome to Windows

Press Ctrl-Alt-Delete to begin.

Requiring this key combination at startup helps keep your computer secure. For more information, click Help.

Figure 2: CTRL-ALT-DEL

3. Enter the User name, **Administrator** (verify the username with your instructor).
4. Type in the password, **password**, and click the **OK** button (verify the password with your instructor).



User name: Administrator

Password: ••••••••

Microsoft Windows Server 2003
Standard Edition
Copyright © 1985-2003 Microsoft Corporation
Microsoft
OK
Cancel
Options >>

Figure 3: Windows 2k3 login

1 Configuring ICMP on the Firewall

There are many firewall solutions that companies can use. PfSense is an open source, FreeBSD based operating system, which requires minimal disk space.

1.1 Setting up Access Control Lists on Folders

1. On the **Windows2k3 Server Internal Victim Machine,** double-click the shortcut to the command prompt icon on the desktop.

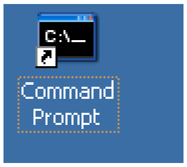
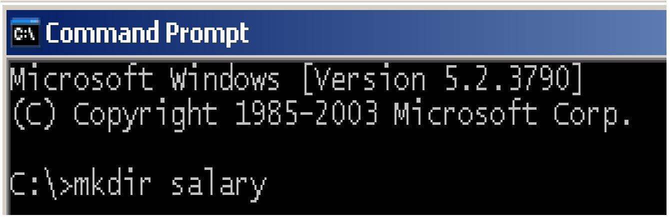


Figure 4: Opening the Command Prompt

2. Type the following command to create a folder named salary on C:
   C:\>**mkdir salary**

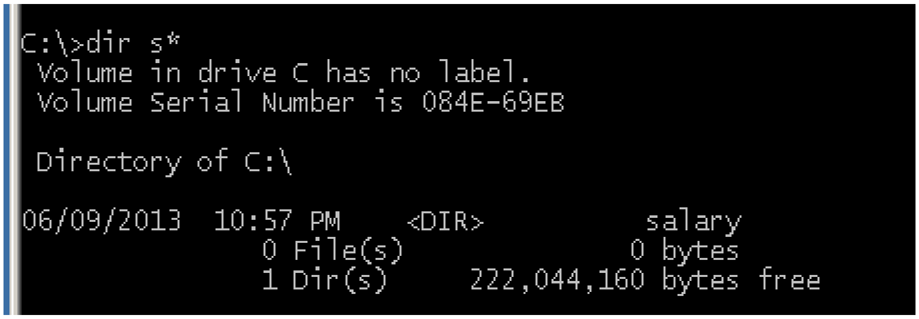


```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\>mkdir salary
```

Figure 5: Making a Salary Directory

We can view all files and folders beginning with the letter "s", using the "*" wildcard.

3. View the newly created Salary folder by typing the following command
   C:\>**dir s***

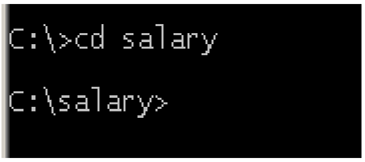


```
C:\>dir s*
 Volume in drive C has no label.
 Volume Serial Number is 084E-69EB

 Directory of C:\

06/09/2013  10:57 PM    <DIR>          salary
               0 File(s)              0 bytes
               1 Dir(s)     222,044,160 bytes free
```

Figure 6: Viewing the Newly Created Directory

We will now go into the Salary folder using the change directory command.

4. Go into the Salary folder by typing the following command:
   C:\>**cd salary**

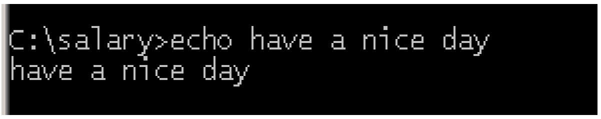


```
C:\>cd salary

C:\salary>
```

Figure 7: Entering the Salary Directory

In the next step, we will create a text file using the *echo* command. In both Microsoft Windows and Linux, the echo command can be utilized to create and append files. The echo command was designed simply to repeat phrases typed by the user.

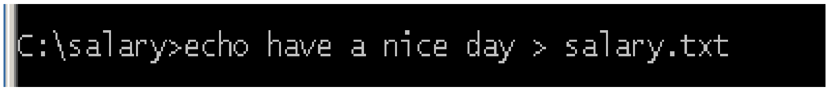
5. Type the following command to echo the phrase "have a nice day":
   C:\salary> **echo have a nice day**



```
C:\salary>echo have a nice day
have a nice day
```

Figure 8: The echo command

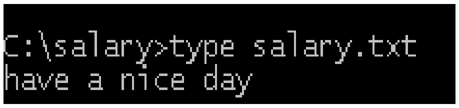
6. Use the echo command to write the phrase "**have a nice day**" to a text file named **salary.txt** by typing:
   C:\salary> **echo have a nice day > salary.txt**



```
C:\salary>echo have a nice day > salary.txt
```

Figure 9: Redirecting the output of echo into a file

7. To view the contents of the salary.txt file, type the following command:
   C:\salary> **type salary.txt**

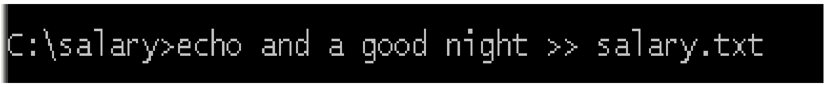


```
C:\salary>type salary.txt
have a nice day
```

Figure 10: Reading the contents of a file

A single redirect will create a new file, erasing any prior contents in the file. A double redirect will append the file and add the new echo statement to the bottom of the file.

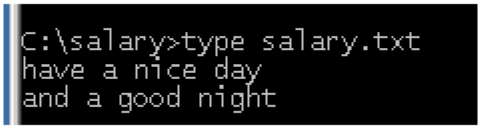
8. Type the following command to add an additional line to salary.txt:
   C:\salary>**echo and a good night >> salary.txt**



```
C:\salary>echo and a good night >> salary.txt
```

Figure 11: Appending information to a file

9. To view both lines of the salary.txt file, type the following command:
   C:\salary> **type salary.txt**

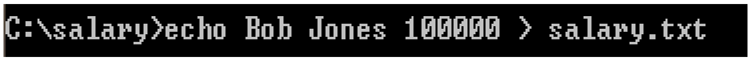


```
C:\salary>type salary.txt
have a nice day
and a good night
```

Figure 12: Reading the contents of a file

When a single redirect is used, all of the previous information in the file is removed.

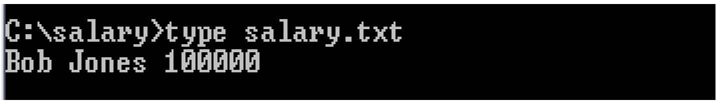
10. Type the following command to erase the previous information in salary.txt
    C:\salary> **echo Bob Jones 100000 > salary.txt**



```
C:\salary>echo Bob Jones 100000 > salary.txt
```

Figure 13: A Single Redirect will erase the file

11. To view the contents of the salary.txt file, type the following command:
    C:\salary> **type salary.txt**

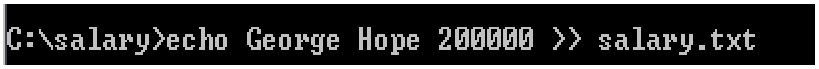


```
C:\salary>type salary.txt
Bob Jones 100000
```

Figure 14: Reading the contents of a file

Whenever a double redirect is used, the new echo statement will be appended.

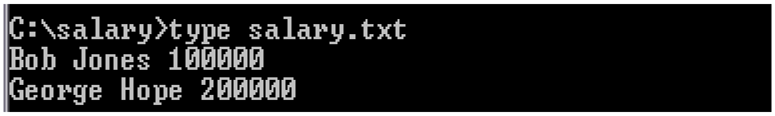
12. Type the following command to append information to the salary.txt file:
    C:\salary>**echo George Hope 200000 >> salary.txt**



```
C:\salary>echo George Hope 200000 >> salary.txt
```

Figure 15: Appending Information to the File

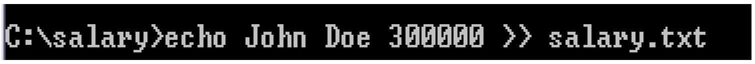
13. To display the contents of the salary.txt file with the additional text line, type:
    C:\salary> **type salary.txt**



```
C:\salary>type salary.txt
Bob Jones 100000
George Hope 200000
```

Figure 16: Applying the New Configuration

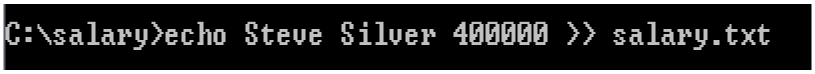
14. Type the following command to append information to the salary.txt file:
    C:\salary> **echo John Doe 300000 >> salary.txt**



```
C:\salary>echo John Doe 300000 >> salary.txt
```

Figure 17: Appending Information to the File

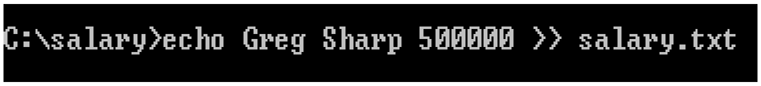
15. Type the following command to append information to the salary.txt file:
    C:\salary>**echo Steve Silver 400000 >> salary.txt**



```
C:\salary>echo Steve Silver 400000 >> salary.txt
```

Figure 18: Appending Information to the File

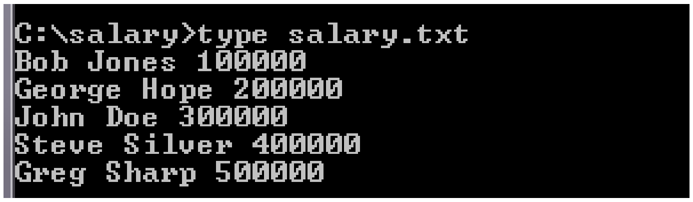
16. Type the following command to append information to the salary.txt file:
    C:\salary>**echo Greg Sharp 500000 >> salary.txt**



```
C:\salary>echo Greg Sharp 500000 >> salary.txt
```

Figure 19: Appending Information to the File

17. To view all 5 names and the corresponding salary information, type:
    C:\salary> **type salary.txt**

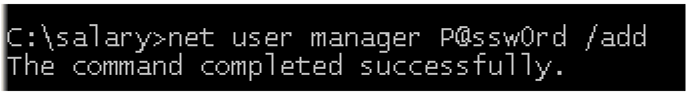


```
C:\salary>type salary.txt
Bob Jones 100000
George Hope 200000
John Doe 300000
Steve Silver 400000
Greg Sharp 500000
```

Figure 20: Adding a New Rule

We will create two user accounts that will be part of the ACL placed on the Salary folder.

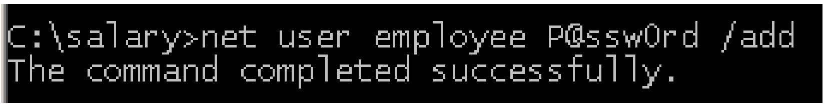
18. Create a user called **manager** with the password of **P@ssword** by typing:
    C:\salary>**net user manager P@ssw0rd /add**



```
C:\salary>net user manager P@ssw0rd /add
The command completed successfully.
```

Figure 21: Adding a User Account

19. Create a user called **employee** with the password of **P@ssword** by typing:
    C:\salary>**net user employee P@ssw0rd /add**



```
C:\salary>net user employee P@ssw0rd /add
The command completed successfully.
```

Figure 22: Adding a User Account

20. On the **Windows 2k3 Server Internal Victim Machine,** click on **Start** button and select **My Computer.**

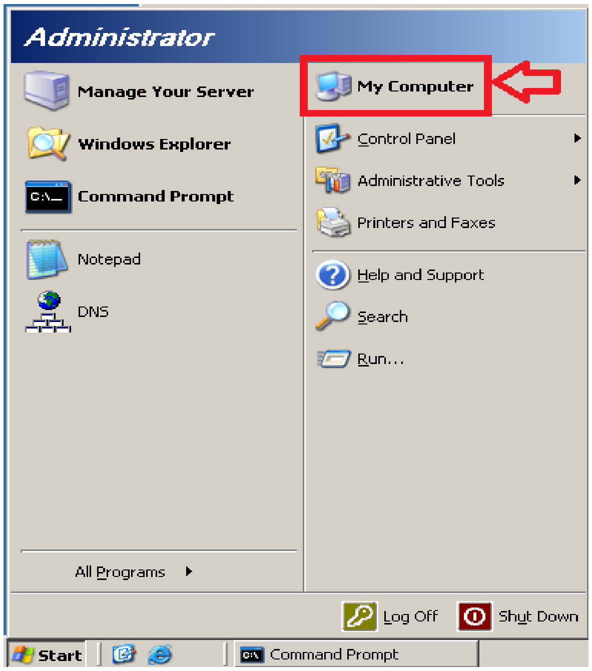
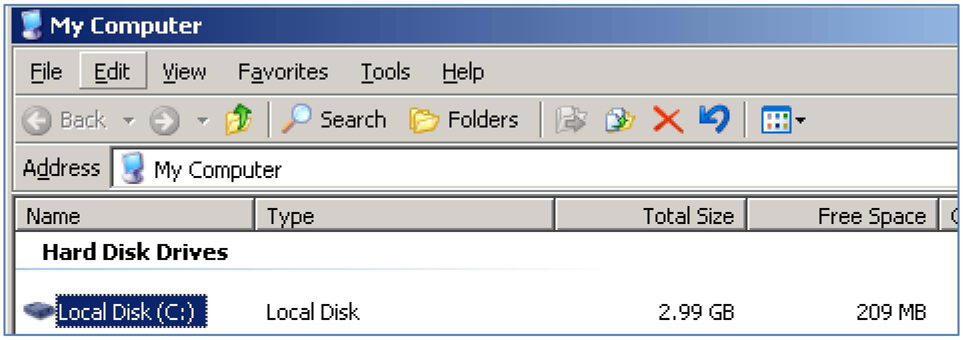


Figure 23: Selecting My Computer

21. Double-click on **Local Disk (C:)** to view the contents of the C: Drive.



Name	Type	Total Size	Free Space
Hard Disk Drives			
Local Disk (C:)	Local Disk	2.99 GB	209 MB

Figure 24: Selecting the C: Drive

22. Right-click on the **salary** folder and select **properties** from the submenu.

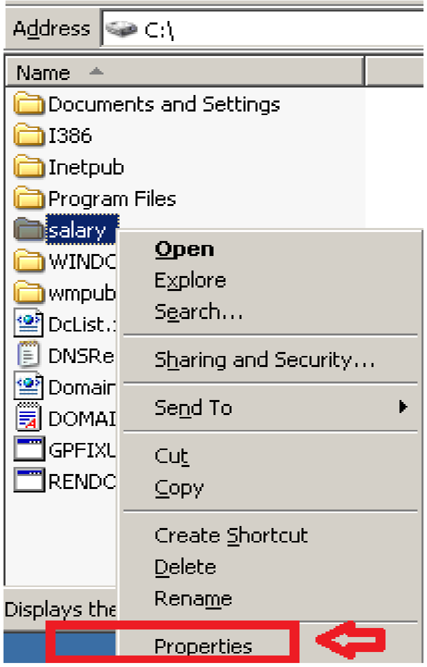


Figure 25: The Properties if the Salary Folder

23. In the properties of the Salary folder, click on the **Security** tab.

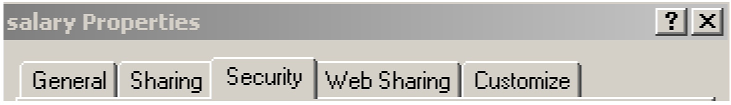
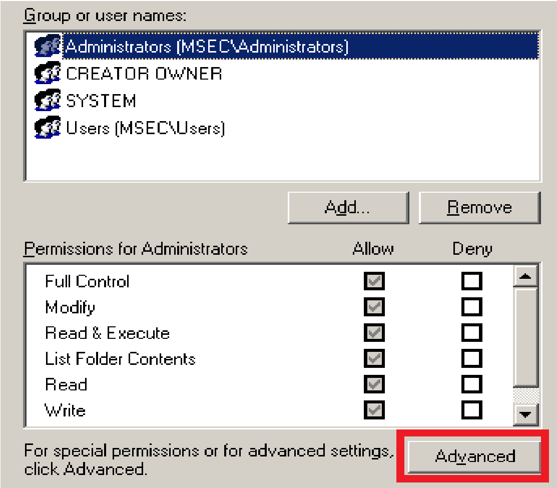


Figure 26: The Security Tab

24. Click the **Advanced** button to access advanced settings for the Salary folder.


Group or user names:

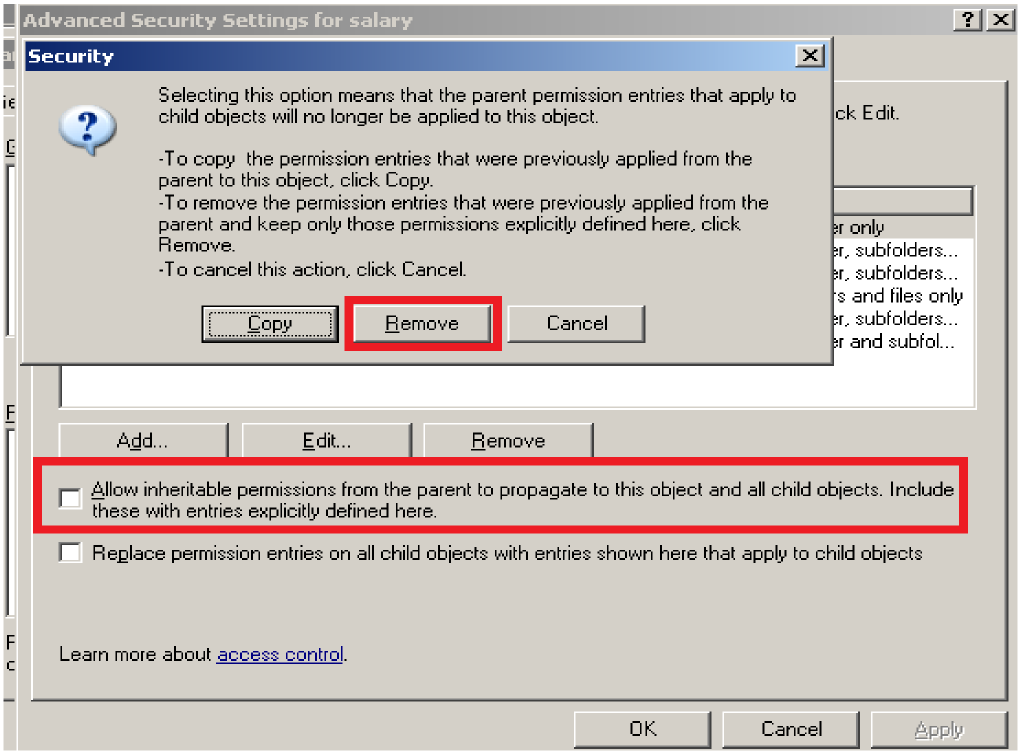
- Administrators (MSEC\Administrators)
- CREATOR OWNER
- SYSTEM
- Users (MSEC\Users)

Permissions for Administrators	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□

For special permissions or for advanced settings, click Advanced.

Figure 27: The Advanced Tab

25. Uncheck the checkbox next to **Allow inheritable permissions from the parent to propagate…** as shown below. Click **Remove** when the Security dialog window appears.



Advanced Security Settings for salary

Security

Selecting this option means that the parent permission entries that apply to child objects will no longer be applied to this object.

-To copy the permission entries that were previously applied from the parent to this object, click Copy.
-To remove the permission entries that were previously applied from the parent and keep only those permissions explicitly defined here, click Remove.
-To cancel this action, click Cancel.

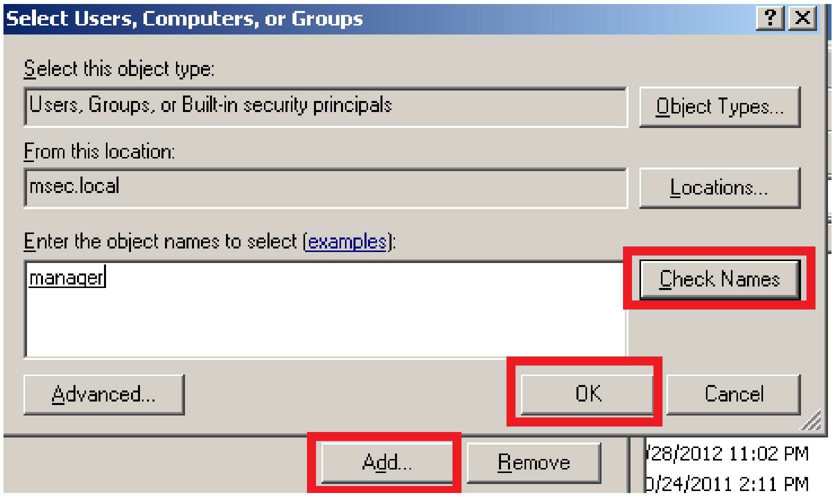
☐ Allow inheritable permissions from the parent to propagate to this object and all child objects. Include these with entries explicitly defined here.

☐ Replace permission entries on all child objects with entries shown here that apply to child objects

Learn more about access control.

Figure 28: Removing Permissions

26. Click **Add**. Type the word **manager**, click **check names** and click **OK**. The Permission Entry dialog window will appear. In the Permissions list, next to **Full Control**, click the checkbox beneath **Allow** and click **OK.**



Select Users, Computers, or Groups

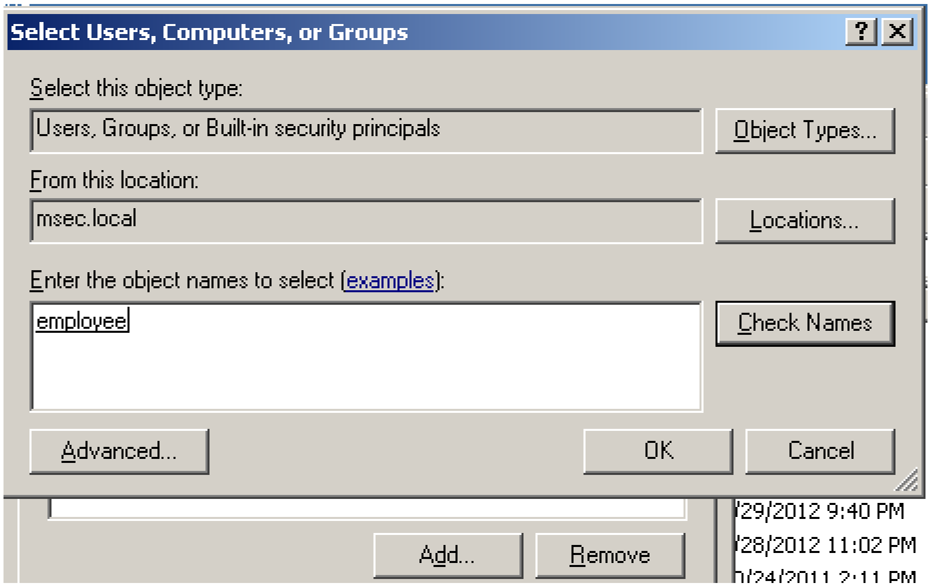
Select this object type:
Users, Groups, or Built-in security principals

From this location:
msec.local

Enter the object names to select (examples):
manager

Figure 29: Adding Users to the Salary ACL

27. Click **Add**. Type the word **employee**, click **check names** and click **OK**. The Permission Entry dialog window will appear. In the Permissions list, next to **Full Control**, click the checkbox beneath **Allow** and **c**lick **OK.** We will change the permissions later.



Select Users, Computers, or Groups

Select this object type: Users, Groups, or Built-in security principals

From this location: msec.local

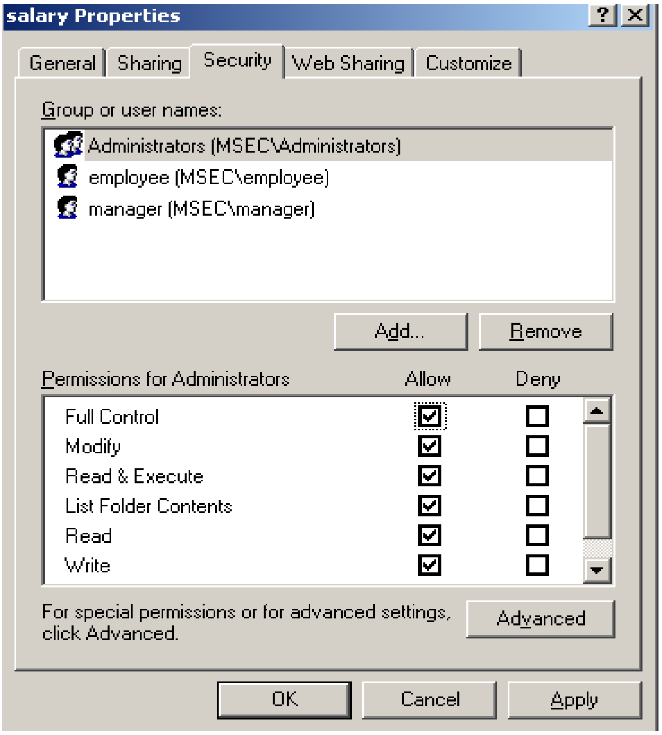
Enter the object names to select (examples): employee

Figure 30: Adding Users to the Salary ACL

Return to the security tab of the salary folder properties by clicking **OK** on the Advanced Security Settings for salary window. After clicking ok, you should see the permissions for the following users and groups:

- Administrators
- Manager
- Employee

28. Click **Administrators**. Click **Allow** next to **Full Control** (you will see other check options appear).



Group or user names:

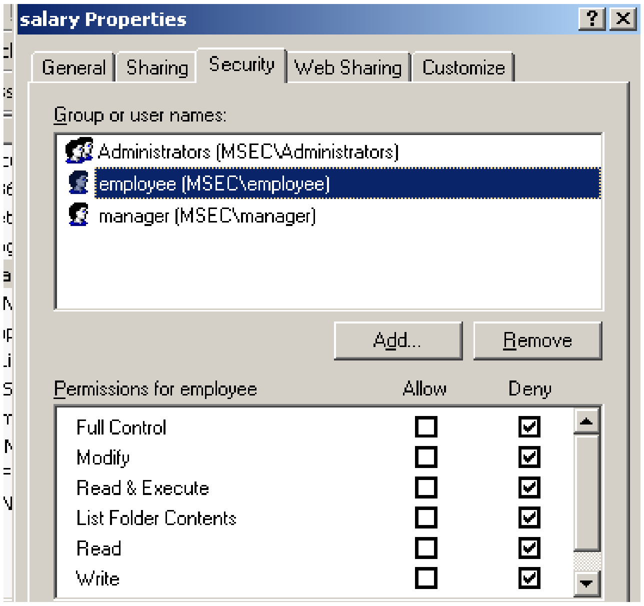
Administrators (MSEC\Administrators)
employee (MSEC\employee)
manager (MSEC\manager)

Permissions for Administrators	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□

For special permissions or for advanced settings, click Advanced.

Figure 31: The Administrators Access Control List

29. Click **employee**. Click **Deny** next to **Full Control** (you will see other check options appear).



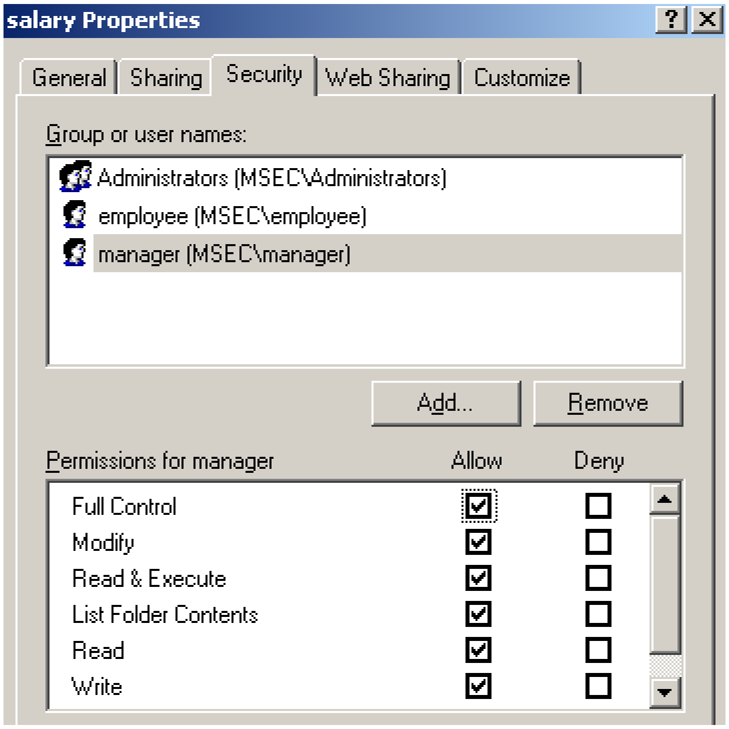
Group or user names:

Administrators (MSEC\Administrators)
employee (MSEC\employee)
manager (MSEC\manager)

Permissions for employee	Allow	Deny
Full Control	□	☑
Modify	□	☑
Read & Execute	□	☑
List Folder Contents	□	☑
Read	□	☑
Write	□	☑

Figure 32: The employee Access Control List

30. Click **manager**. Click **Allow** next to **Full Control**. (if necessary) Click **OK**.
    After clicking OK, click **Yes** to the Security Warning that asks you if you want to continue.



Group or user names:

- Administrators (MSEC\Administrators)
- employee (MSEC\employee)
- manager (MSEC\manager)

Permissions for manager	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□

Figure 33:: The manage Access Control List

1.2 Conclusion

When the NTFS file system is utilized on a Windows system, permissions can be set on files and folders. Permissions to files and folders can be assigned to users and groups on a local system as well as domain users if a computer is part of Windows domain.

1.3 Discussion Questions

1. How are NTFS permissions configured on a Windows system?
2. What command allows you to add a user from the command line?
3. What command can be utilized to create a file from the command line?
4. What needs to be done if you want to append information to a file?

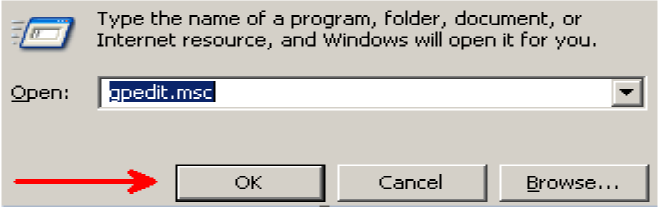
2 Configuring Auditing for Object Access

Some people have the misconception that auditing for object access is automatically configured for files and folders on NTFS drives. Auditing is critical to monitoring and maintaining the security of a system. Auditing can keep track of object access, user account management, logon events, and other activity. On most Windows systems, the amount of auditing the system does by default is limited. A network administrator has the ability to enable additional auditing. Insufficient auditing can be a security issue.

2.1 Enabling Auditing on a Windows Systems

A lack of auditing can be an issue if security incidents are not being discovered. The default audit policy can differ on computers depending on the version of the operating system. Security Templates can be applied to systems to change their audit settings, or an administrator can manually go in and turn on auditing for any given policy.

1. To view the Audit Policies on the **Windows 2k3 Server Internal Victim Machine**, open the Group Policy editor. Click **Start**, click **Run**, and type **gpedit.msc** in the box, and then click **OK**.

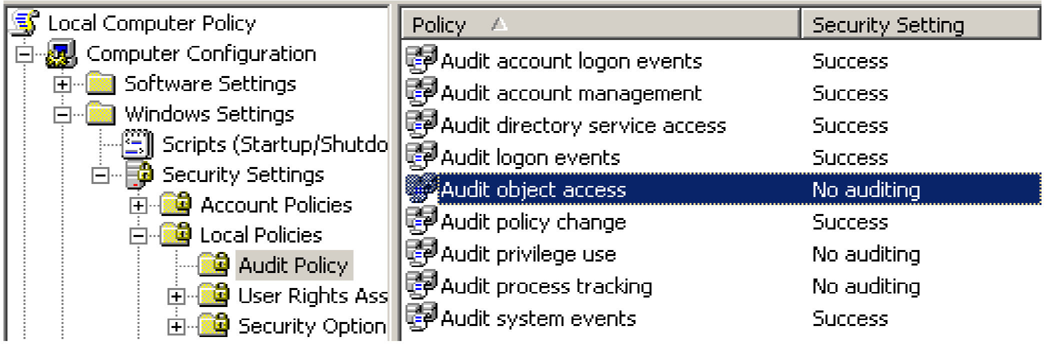


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: gpedit.msc

Figure 34: Launching the Group Policy Editor

2. Navigate to the following location within the Group Policy Editor: **Local Computer Policy>Computer Configuration>Windows Settings>Security Settings> Local Policies>Audit Policy.** View the Policy and Security Settings in the right pane.

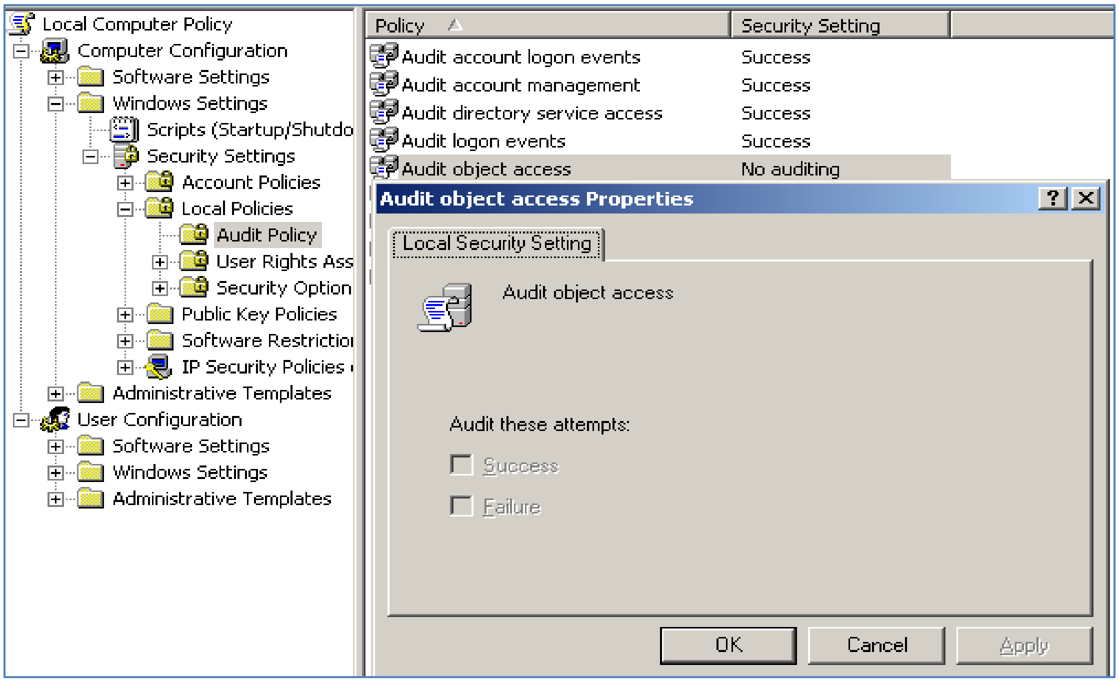


Policy	Security Setting
Audit account logon events	Success
Audit account management	Success
Audit directory service access	Success
Audit logon events	Success
Audit object access	No auditing
Audit policy change	Success
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	Success

Figure 35: Viewing the Default Audit Policy

Notice that auditing is not turned on for **Audit object access**. This presents a problem from a security standpoint, because if an unauthorized or authorized users attempts to access resources on the system, there will be no records of these attempts.

3. Double-click on the **Audit object access** policy within the Group Policy Editor. Notice that the checkboxes are grayed out. This machine is a Domain Controller, so Group Policy must be configured in Active Directory. Click the **OK** button. Go up to **File** in the menu bar, and select **exit**.



Policy	Security Setting
Audit account logon events	Success
Audit account management	Success
Audit directory service access	Success
Audit logon events	Success
Audit object access	No auditing

Audit object access Properties

Local Security Setting

Audit object access

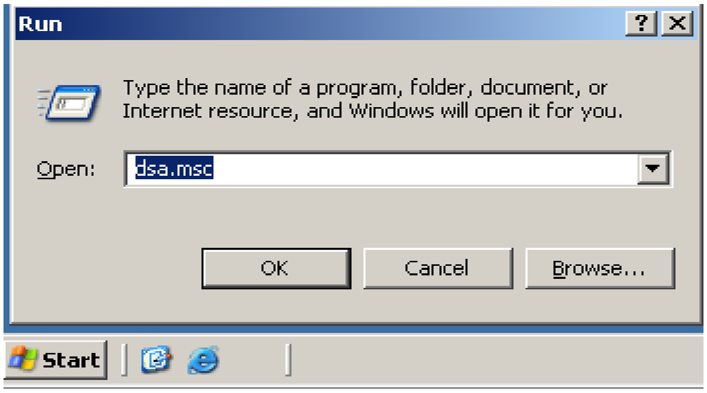
Audit these attempts:

□ Success

□ Failure

Figure 36: Viewing the Default Audit Policy

4. To open Active Directory Users and Computers on the Domain Controller, click on the **Start** button, click **Run**, and type **dsa.msc**, and then click **OK**.


Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: dsa.msc

Figure 37: Launching Active Directory

5. Expand the **msec.local** domain and go to **Domain Controllers.**

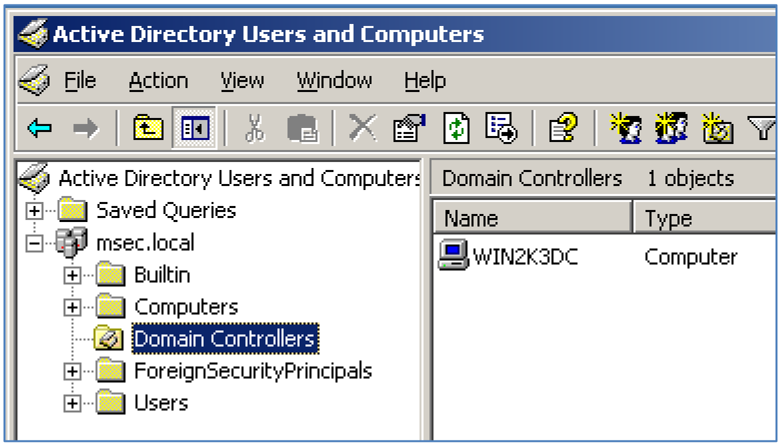

Active Directory Users and Computers
File
Action
View
Window
Help
Active Directory Users and Computers
Saved Queries
msec.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Users
Domain Controllers 1 objects
Name
Type
WIN2K3DC
Computer

Figure 38: Properties on the Domain Controllers

6. Right-click on **Domain Controller** and go to **Properties.**

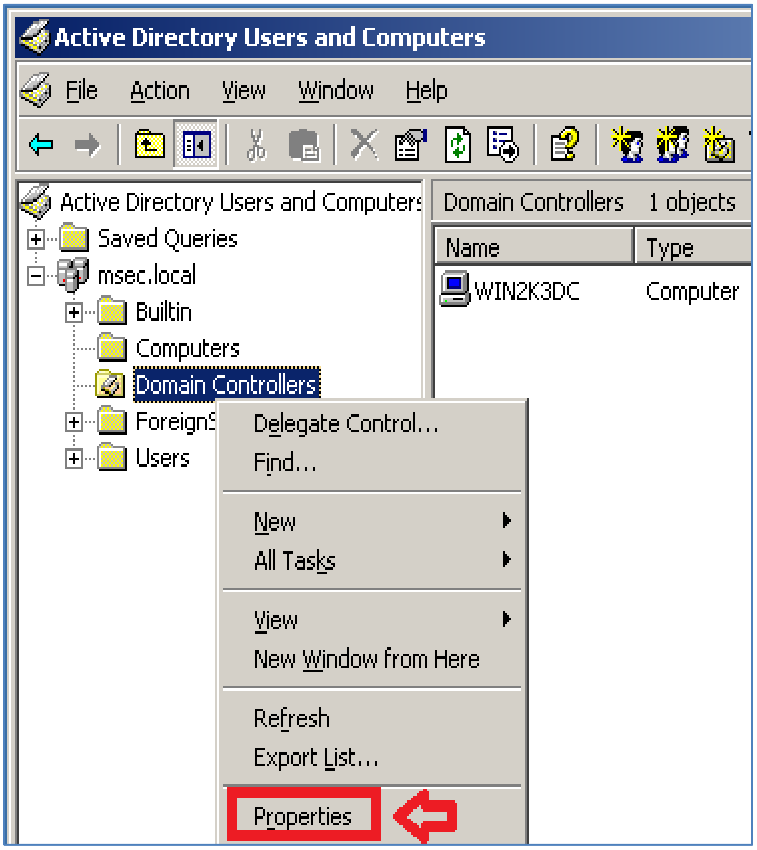
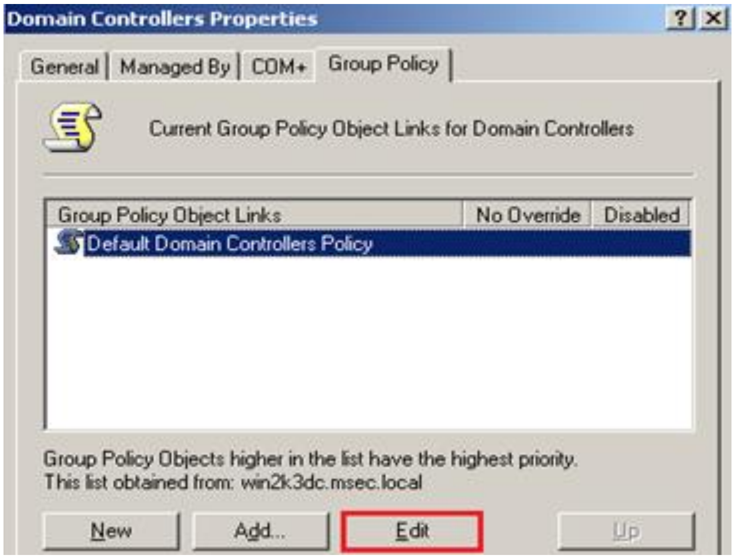


Figure 39: Properties on the Domain

7. Click the **Group Policy** tab at the top, then click **Edit** to edit the Default Domain Controllers Policy.



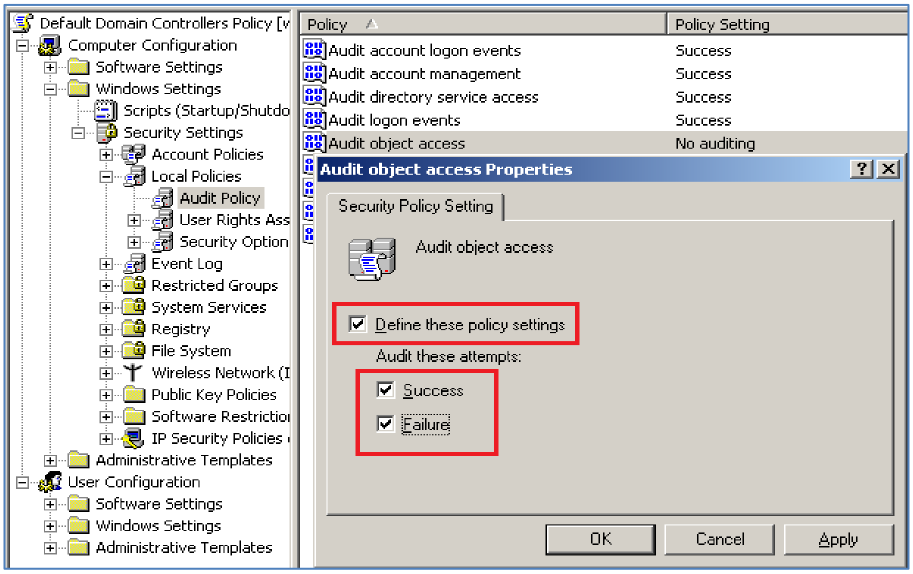
Current Group Policy Object Links for Domain Controllers

Group Policy Object Links	No Override	Disabled
Default Domain Controllers Policy		

Group Policy Objects higher in the list have the highest priority.
This list obtained from: win2k3dc.msec.local

Figure 40:   Edit the Default Domain Controllers Policy

8. Navigate to the following location within the Group Policy Editor: **Default Domain Controllers Policy>Computer Configuration, Windows Settings> Security Settings> Local Policies, Audit Policy**. View the Policy and Security Settings in the right pane.
9. Double-click on the **Audit Object Access** policy in the right-hand pane.
10. Check **Define these policy settings**. Check the **Success** and **Failure** checkboxes.
11. Click **OK**. Go up to **File** in the menu bar, and select **exit** to quit. Click **OK** and close the Active Directory Users and Computers window.



Policy	Policy Setting
Audit account logon events	Success
Audit account management	Success
Audit directory service access	Success
Audit logon events	Success
Audit object access	No auditing

Audit object access

☑ Define these policy settings

Audit these attempts:

☑ Success

☑ Failure

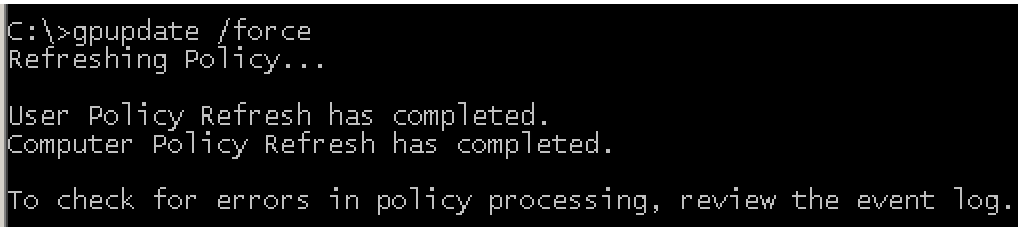
Figure 41: Default Audit Object Access Settings for Domain

Success Audits will be logged in the Event Viewer when those who are permitted to access objects are able to use the resources successfully. Failed audits are logged when users try to access resources which they have not been granted access to.

9. Double-click on the shortcut to the command prompt on the server's desktop.

Figure 42: Opening the Command Prompt

10. Type the following command to refresh the machine's Group Policy settings: C:\gpupdate /force



```
C:\>gpupdate /force
Refreshing Policy...

User Policy Refresh has completed.
Computer Policy Refresh has completed.

To check for errors in policy processing, review the event log.
```

Figure 43: Refreshing Group Policy

11. On the **Windows 2k3 Server Internal Victim Machine,** click on **Start** button and select **My Computer**.

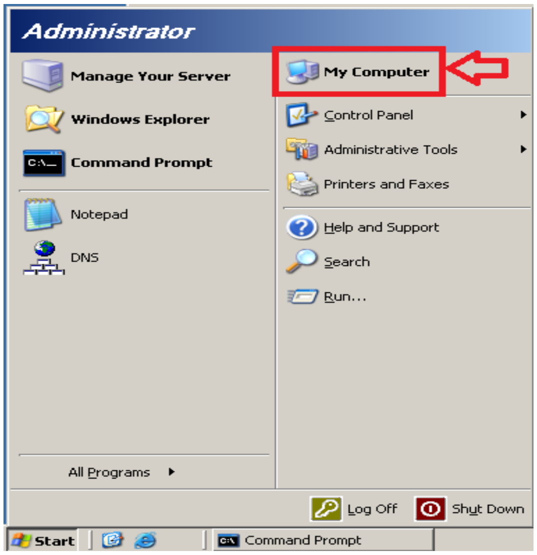


Figure 43: Selecting My Computer

12. Double-click on **Local Disk (C:)** to view the contents of the C: Drive.

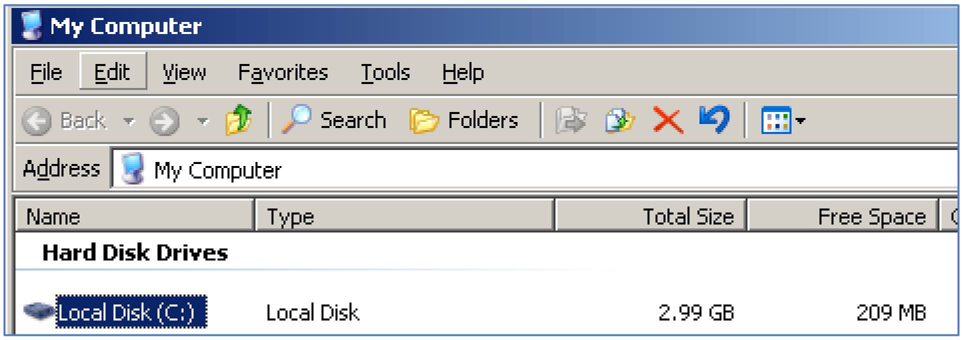

My Computer
File Edit View Favorites Tools Help
Back Search Folders
Address My Computer
Name Type Total Size Free Space
Hard Disk Drives
Local Disk (C:) Local Disk 2.99 GB 209 MB

Figure 44: Selecting the C: Drive

13. Right-click on the **salary** folder and select **properties** from the submenu.

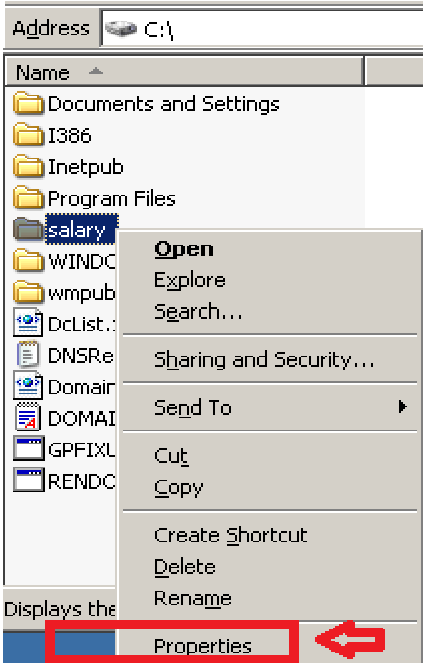


Figure 45: The Properties if the Salary Folder

14. In the properties of the Salary folder, click on the **Security** tab.

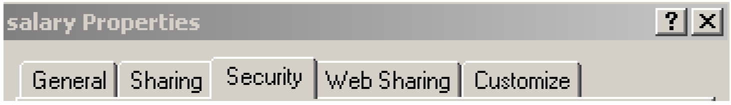
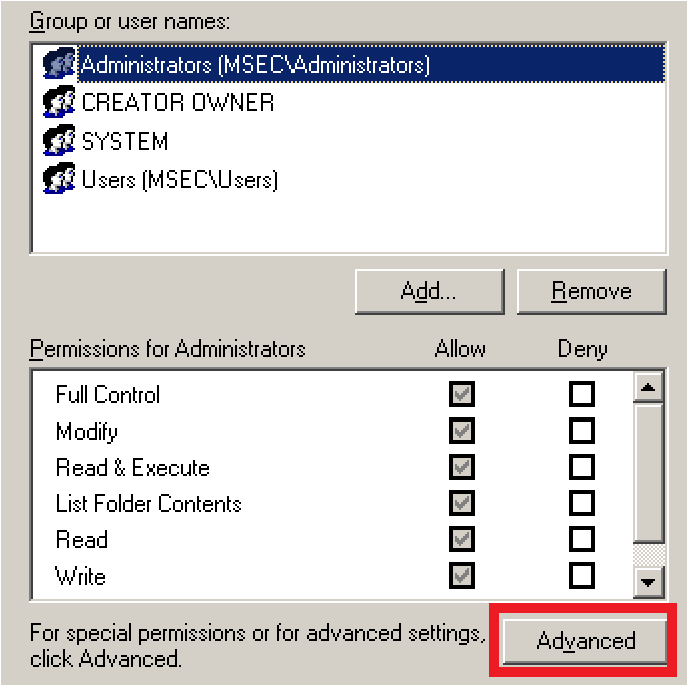


Figure 46: The Security Tab

15. Click the **Advanced** button to access advanced settings for the Salary folder.



Group or user names:

- Administrators (MSEC\Administrators)
- CREATOR OWNER
- SYSTEM
- Users (MSEC\Users)

Add... | Remove

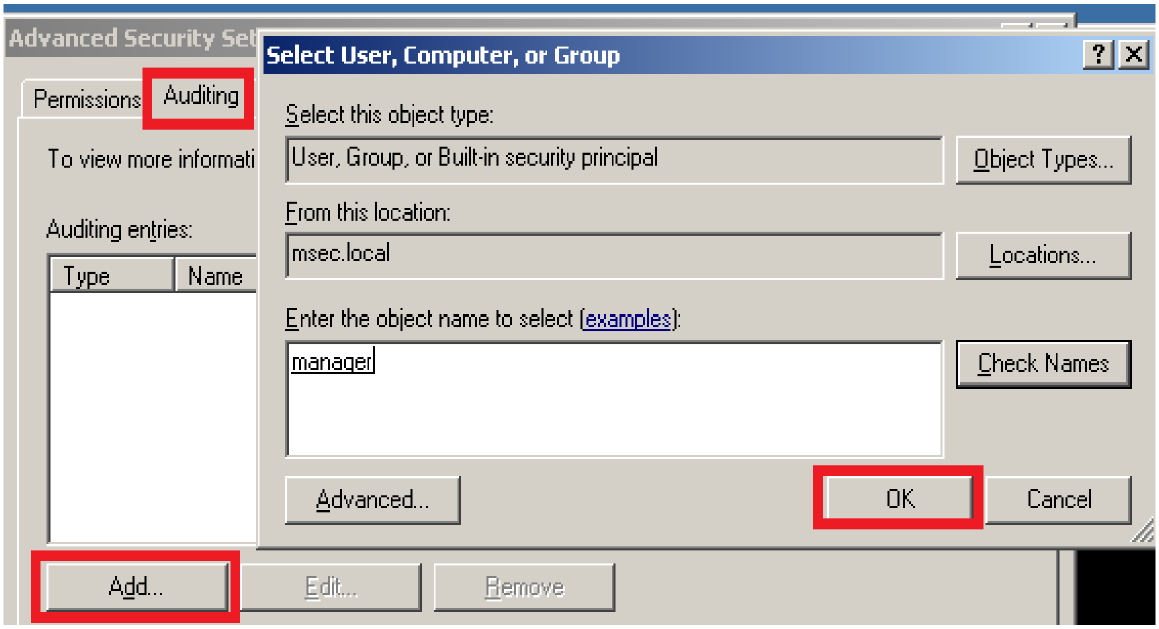
Permissions for Administrators	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□

For special permissions or for advanced settings, click Advanced.

Advanced

Figure 47: The Advanced button

16. Click the **Auditing** tab. Click **Add**. Type manager Click **Check Names**. Click **OK**.



Advanced Security Set

Permissions | Auditing

To view more informati

Auditing entries:

Type	Name

Add... | Edit... | Remove

Select User, Computer, or Group

Select this object type:

User, Group, or Built-in security principal | Object Types...

From this location:

msec.local | Locations...

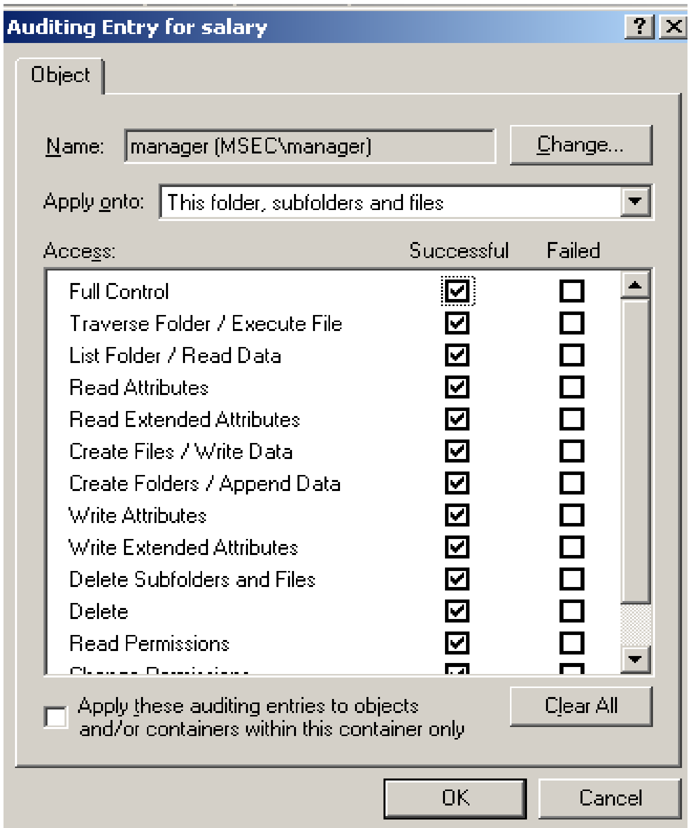
Enter the object name to select (examples):

manager | Check Names

Advanced... | OK | Cancel

Figure 48: Auditing Tab

17. Click the **Successful** Button to the right of **Full Control**. Click **OK**.



Auditing Entry for salary

Name: manager (MSEC\manager)

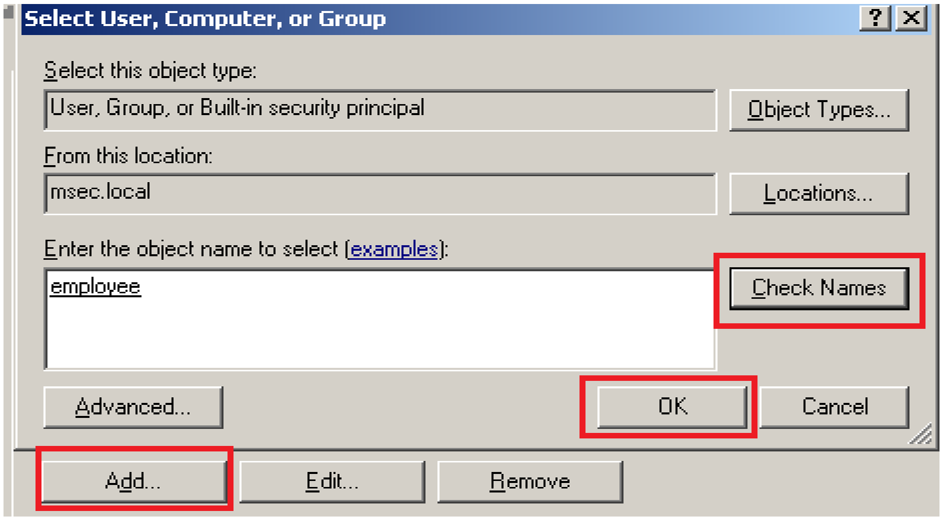
Apply onto: This folder, subfolders and files

Access:	Successful	Failed
Full Control	☑	□
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	☑	□

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

Figure 49: Configuring an Auditing Entry

18. Click **Add**. type **manager,** click **Check Names**. Click **OK**.



Select User, Computer, or Group

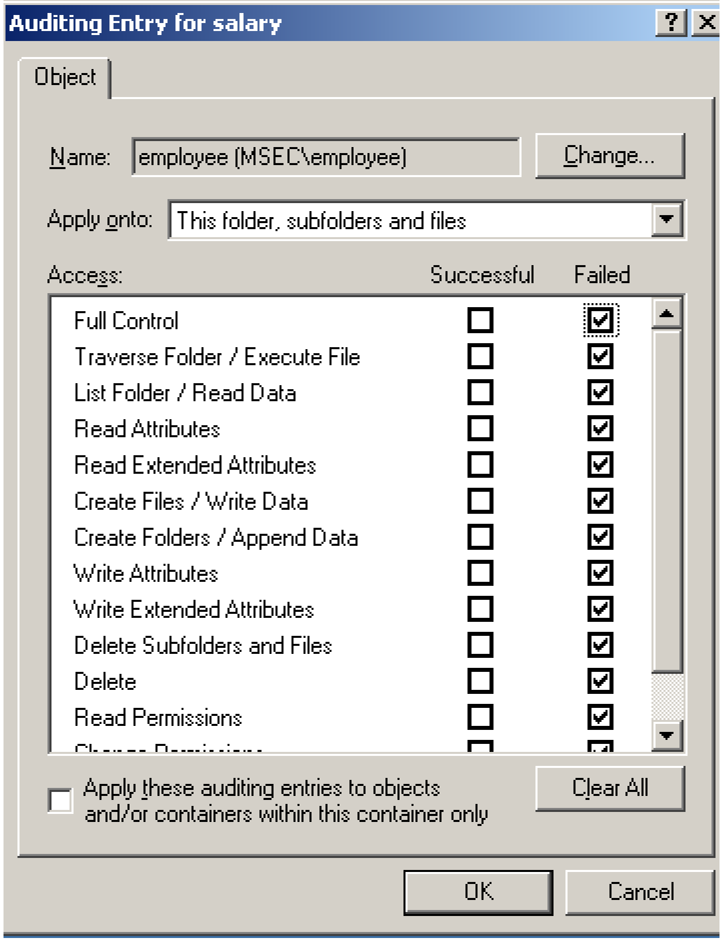
Select this object type: User, Group, or Built-in security principal

From this location: msec.local

Enter the object name to select (examples): employee

Figure 50: Configuring Auditing for Employee

19. Click the **Failed** Button to the right of **Full Control**. Click **OK**.



Auditing Entry for salary

Object

Name: employee (MSEC\employee)

Apply onto: This folder, subfolders and files

Access:	Successful	Failed
Full Control	□	☑
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	□	☑

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

Figure 51: Configuring Audit Entries for the Salary Folder

2.2 Conclusion

Auditing for object access is not automatically configured for files and folders on NTFS drives. Auditing is critical to monitoring and maintaining the security of a system. Auditing can keep track of object access. A network administrator has the ability to enable additional auditing. Insufficient auditing can be a security issue.

2.3 Discussion Questions

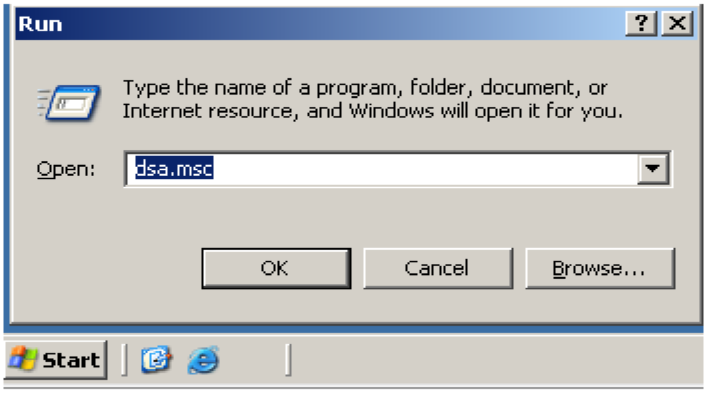
1. What is the purpose of auditing for failure events?
2. What does the command gpedit.msc do on a Windows system?
3. What does the command dsa.msc do on a Windows Domain Controller?
4. What command can be utilized to update Group Policy Settings?

3 Viewing the Security Log to Determine Security Incidents

The Event Viewer keeps track of incidents related to a computer's software, hardware, and security functions. The main logs of the Event Viewer are the Application, System, and Security. The Event Viewer provides critical information about security incidents.

3.1 Accessing Objects

1. To open Active Directory Users and Computers on the Domain Controller, click on the **Start** button, click **Run**, and type **dsa.msc**, and then click **OK**.

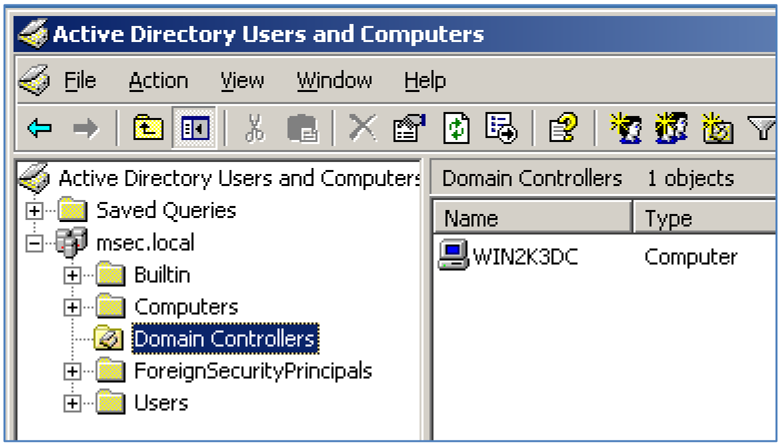

Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
OK
Cancel
Browse...
Start

Open: dsa.msc

Figure 52: Launching Active Directory

We will grant users the right to log on to the Domain Controller for the purposes of this exercise. Normally, non-administrative accounts do not log on to Domain Controllers.

2. Expand the **msec.local** domain and go to **Domain Controllers.**


Active Directory Users and Computers
File
Action
View
Window
Help
Active Directory Users and Computers
Saved Queries
msec.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Users
Domain Controllers 1 objects

Name	Type
WIN2K3DC	Computer

Figure 53: Properties on the Domain Controllers

3. Right-click on **Domain Controllers** and go to **Properties.**

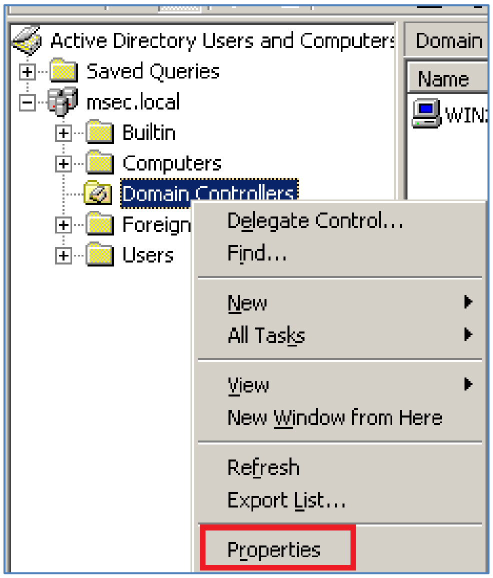
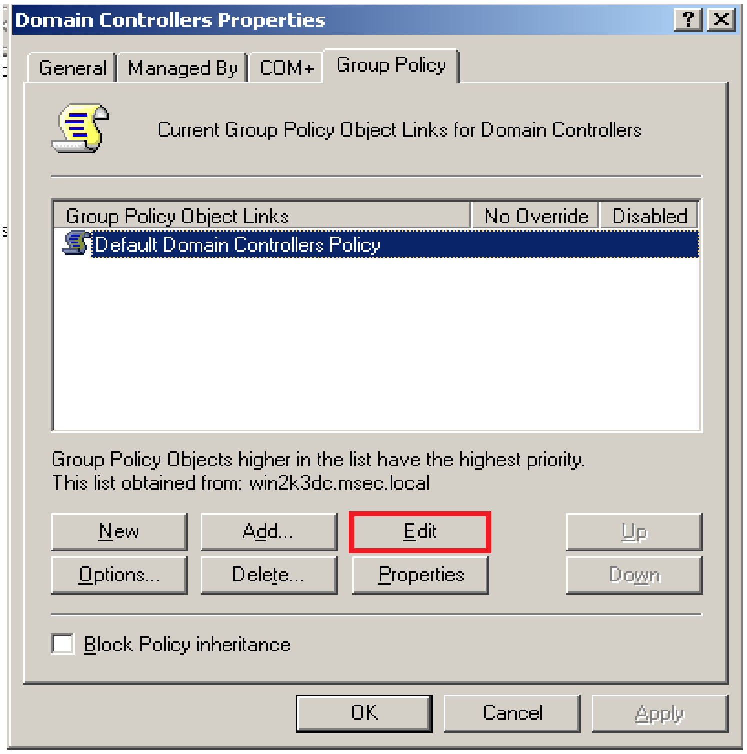


Figure 54: Properties on the Domain

4. Click the **Group Policy** tab, then click **Edit** to edit the Default Domain Controllers Policy.



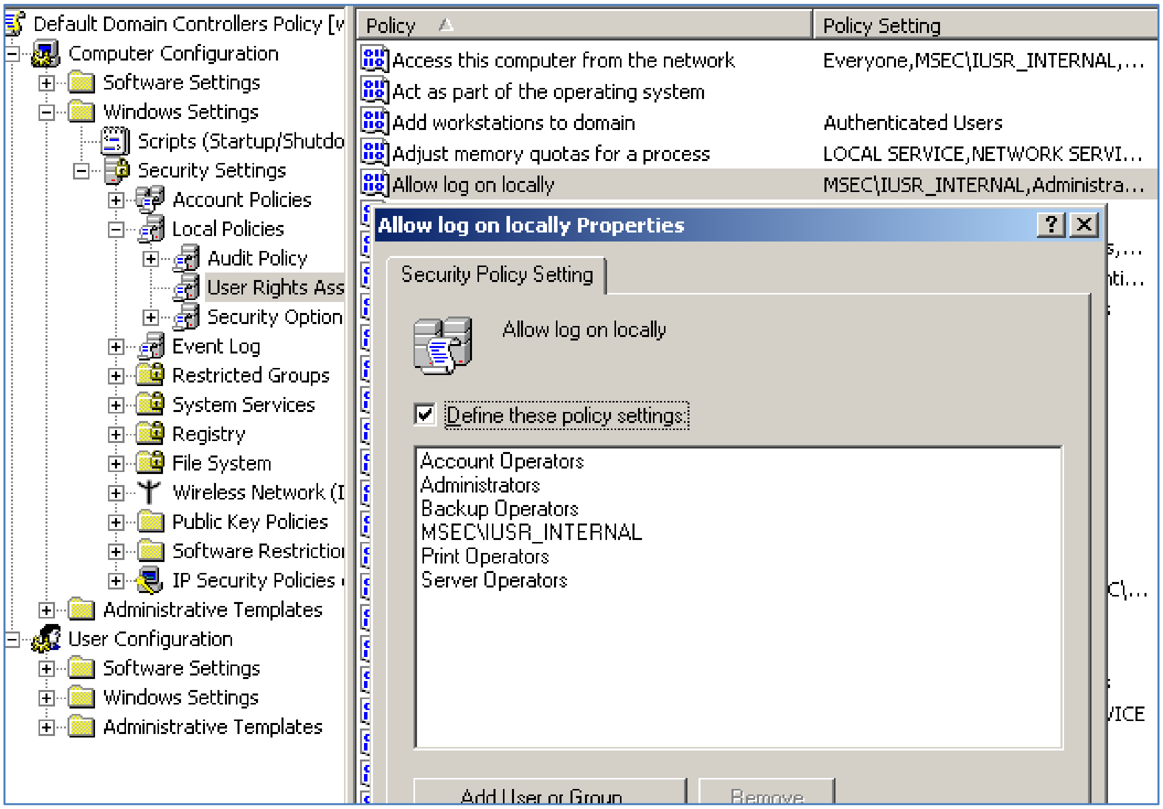
Current Group Policy Object Links for Domain Controllers

Group Policy Object Links	No Override	Disabled
Default Domain Controllers Policy		

Group Policy Objects higher in the list have the highest priority.
This list obtained from: win2k3dc.msec.local

Figure 55: Edit the Default Domain Controllers Policy

5. Navigate to the following location within the Group Policy Editor: **Default Domain Controllers Policy>Computer Configuration>Windows Settings> Security Settings>Local Policies>User Rights Assignment.** Find the **Allow log on locally** policy and double-click to open it.



Policy	Policy Setting
Access this computer from the network	Everyone,MSEC\IUSR_INTERNAL,...
Act as part of the operating system	
Add workstations to domain	Authenticated Users
Adjust memory quotas for a process	LOCAL SERVICE,NETWORK SERVI...
Allow log on locally	MSEC\IUSR_INTERNAL,Administra...

Allow log on locally Properties

Security Policy Setting

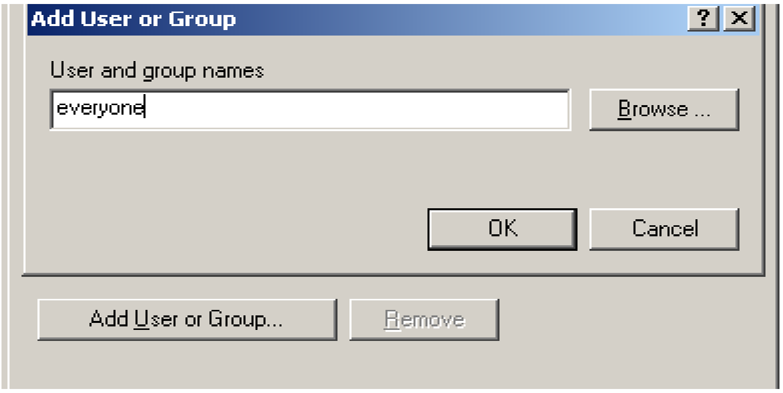
Allow log on locally

☑ Define these policy settings:

Account Operators
Administrators
Backup Operators
MSEC\IUSR_INTERNAL
Print Operators
Server Operators

Figure 56: Audit Object Access Settings

6. Click **Add User or Group**. Type **everyone** to add the everyone group and click **OK**. Click **OK**. Go up to **File** in the menu bar, and select **exit** to quit. Click **OK** on the Domain Controllers Properties window. Close Active Directory Users and Computers.


Add User or Group

User and group names

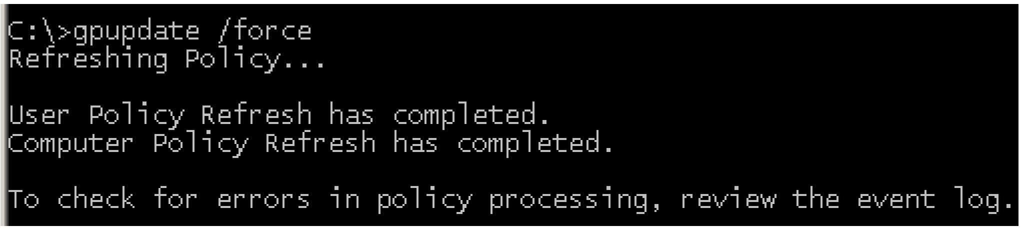
everyone

Figure 57: Default Audit Object Access Settings for Domain

7. Double-click on the shortcut to the command prompt on the server's desktop.

Figure 58: Opening the Command Prompt

8. Type the following command to refresh the machine's Group Policy settings: **C:\**gpupdate /force



```
C:\>gpupdate /force
Refreshing Policy...

User Policy Refresh has completed.
Computer Policy Refresh has completed.

To check for errors in policy processing, review the event log.
```

Figure 59: Refreshing Group Policy

9. Log off the server by clicking on the **Start** button and selecting **Log off** .

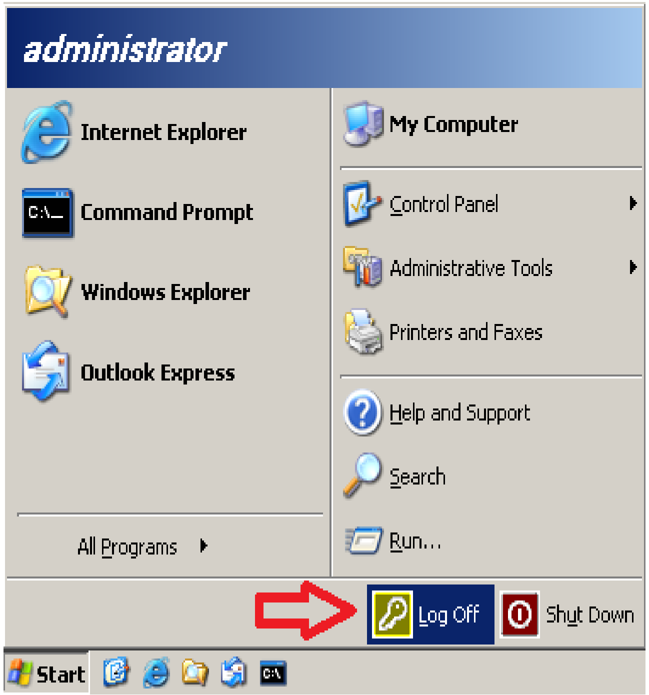
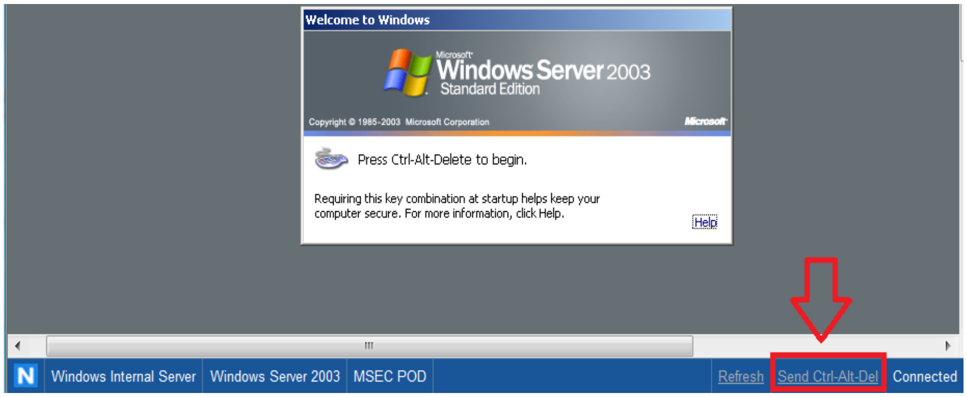


Figure 60: Logging off the Windows Server

10. Log on to the **Windows2k3 Server Internal Victim Machine.** Use the PC menu in the NETLAB+ Remote PC Viewer to send a **Ctrl-Alt-Del** (version 2 viewer), or click the **Send Ctrl-Alt-Del** link in the bottom right corner of the viewer window (version 1 viewer).


Welcome to Windows

Press Ctrl-Alt-Delete to begin.

Requiring this key combination at startup helps keep your computer secure. For more information, click Help.

Figure 61: CTRL-ALT-DEL

11. Log on with the username of **manager** and the password of **P@ssw0rd.**
12. Click on **Start** button and select **My Computer**.

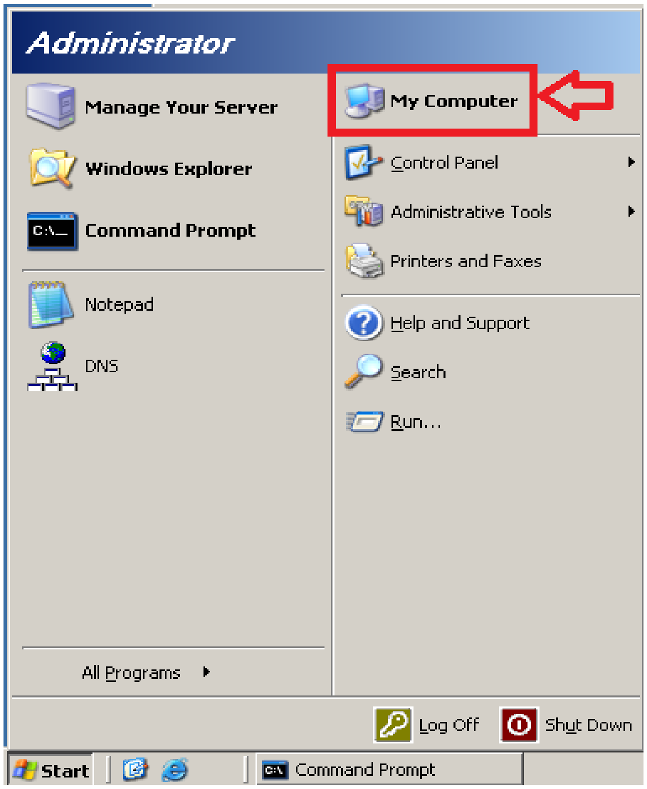


Figure 62: Selecting My Computer

13. Double-click on **Local Disk (C:)** to view the contents of the C: Drive.

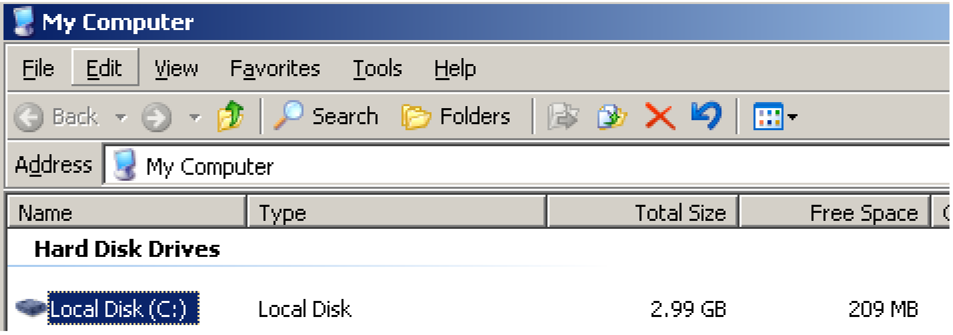

My Computer
File Edit View Favorites Tools Help
Back Search Folders
Address My Computer
Name Type Total Size Free Space
Hard Disk Drives
Local Disk (C:) Local Disk 2.99 GB 209 MB

Figure 63: Selecting the C: Drive

14. Double-click on the **Salary** Folder. The manager should get into the folder.

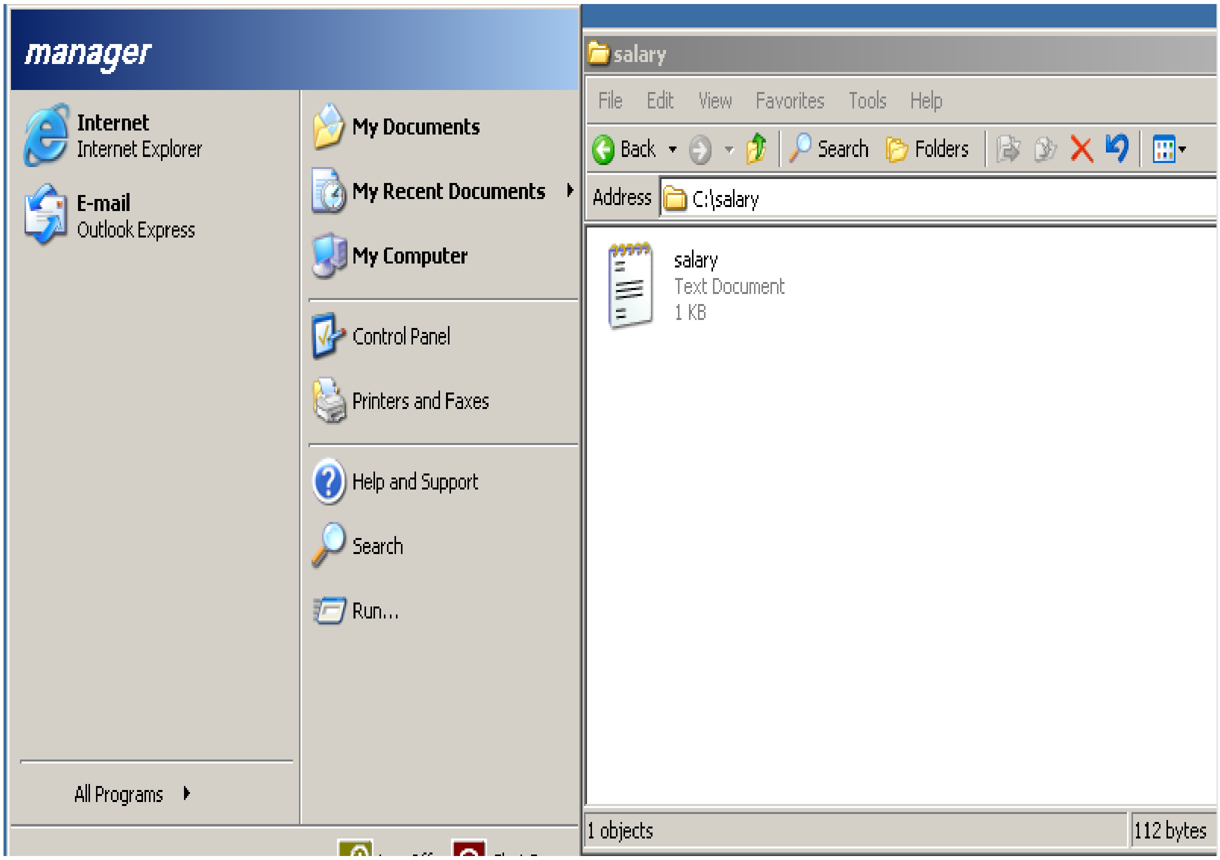


Figure 64: The Salary Folder

15. Log off the server by clicking on the **Start** button and selecting **Log off**.

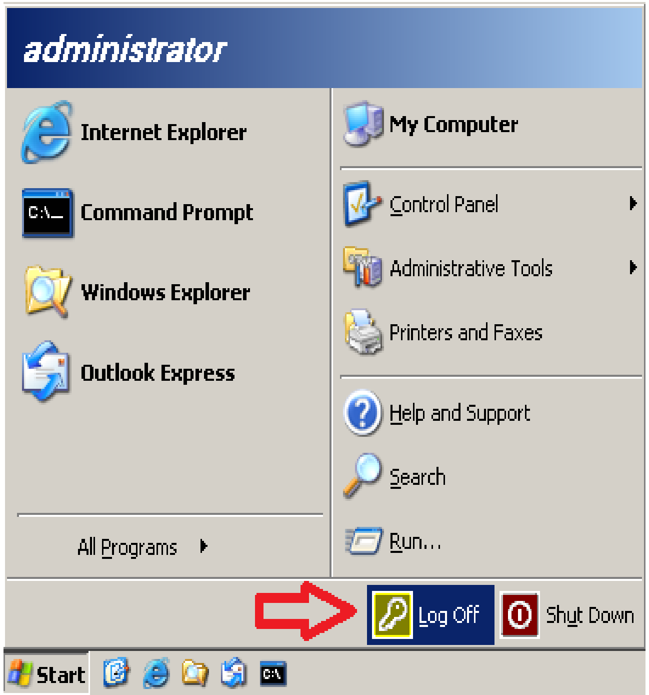


Figure 65: Logging off the Windows Server

16. Log on to the **Windows2k3 Server Internal Victim Machine.** Use the PC menu in the NETLAB+ Remote PC Viewer to send a **Ctrl-Alt-Del** (version 2 viewer), or click the **Send Ctrl-Alt-Del** link in the bottom right corner of the viewer window (version 1 viewer). Log on with the username of **employee** and the password of **P@ssw0rd.**
17. Click on the **Start** button and select **My Computer**.

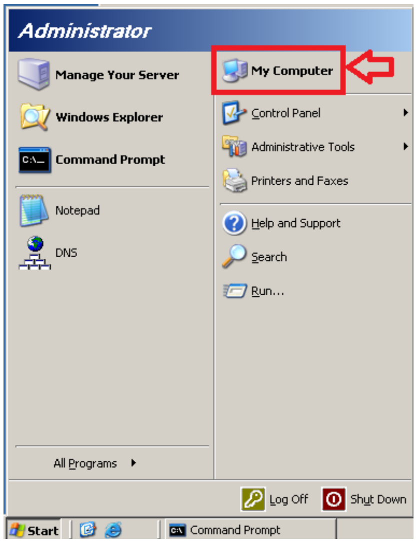
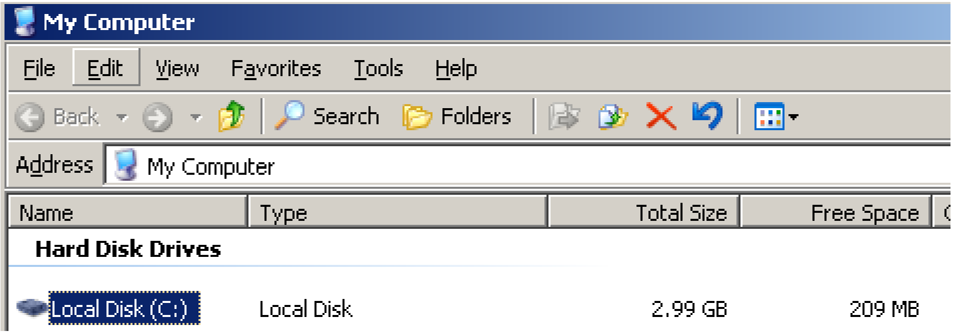


Figure 66: Selecting My Computer

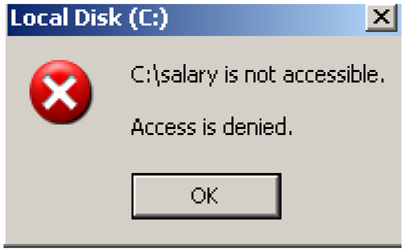
18. Double-click on **Local Disk (C:)** to view the contents of the C: Drive.



Name	Type	Total Size	Free Space
Hard Disk Drives			
Local Disk (C:)	Local Disk	2.99 GB	209 MB

Figure 67: Selecting the C: Drive

19. Double-click on the **Salary** Folder. The employee should get access is denied.



C:\salary is not accessible.

Access is denied.

Figure 68: Access Denied Salary Folder

20. Log off the server by clicking on the **Start** button and selecting **Log off** .

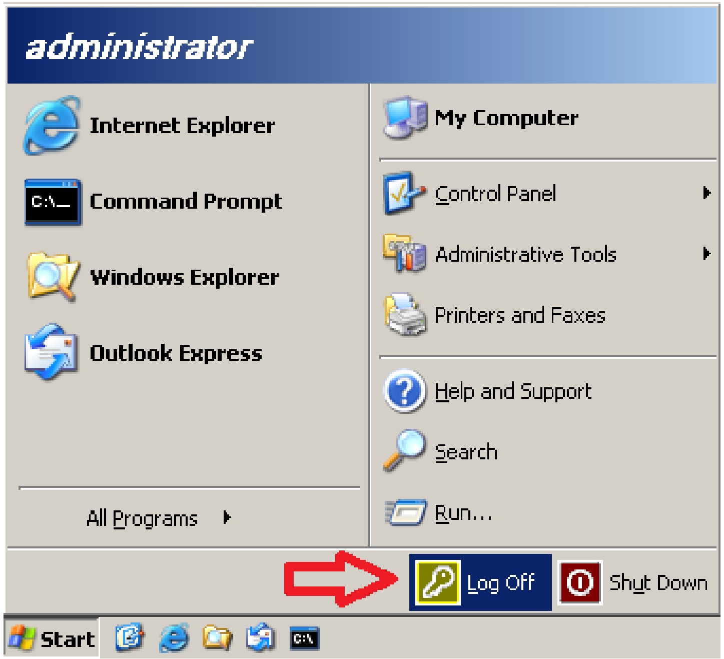
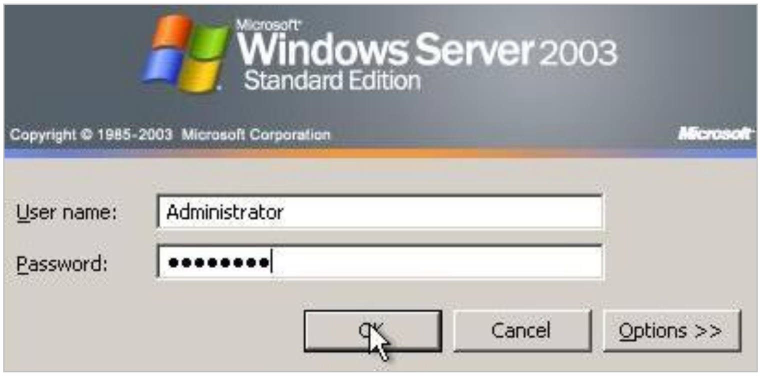


Figure 69: Logging off the Windows Server

21. Log on to the **Windows2k3 Server Internal Victim Machine.** Use the PC menu in the NETLAB+ Remote PC Viewer to send a **Ctrl-Alt-Del** (version 2 viewer), or click the **Send Ctrl-Alt-Del** link in the bottom right corner of the viewer window (version 1 viewer). Log on to the 2003 server with the username of **administrator** and the password of **password.**


Microsoft Windows Server 2003
Standard Edition
Copyright © 1985-2003 Microsoft Corporation
Microsoft
User name: Administrator

Password: ••••••••

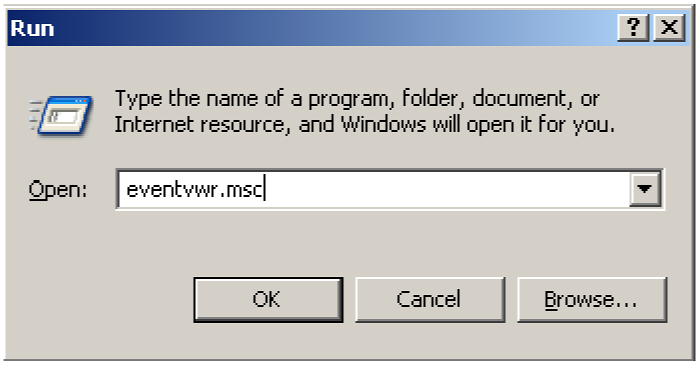
Figure 70: Logging back on to the Server

The 3 Main Logs within the Windows Event Viewer:

- Application Log
- Security Log
- System Log

The Application Log deals with issues related to the system's software. The System Log contains information about the computer's hardware. The Security log contains information about successful and failed attempts to access resources on the system.

22. Click on **Start**, then **run** and type **eventvwr.msc** to open the Event Viewer.

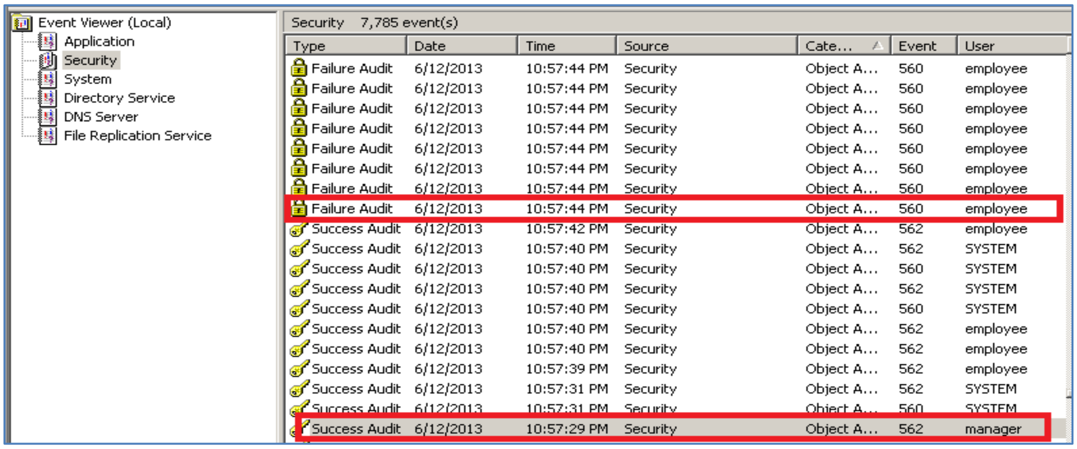


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: eventvwr.msc

Figure 71: Opening the Event Viewer

23. Click on the **Security** Log. Click the **Category** view column. Look for **Object Access**.



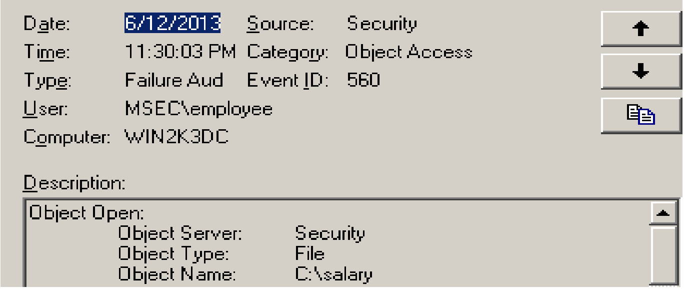
Event Viewer (Local)
- Application
- Security
- System
- Directory Service
- DNS Server
- File Replication Service

Security   7,785 event(s)

Type	Date	Time	Source	Cate...	Event	User
Failure Audit	6/12/2013	10:57:44 PM	Security	Object A...	560	employee
Failure Audit	6/12/2013	10:57:44 PM	Security	Object A...	560	employee
Failure Audit	6/12/2013	10:57:44 PM	Security	Object A...	560	employee
Failure Audit	6/12/2013	10:57:44 PM	Security	Object A...	560	employee
Failure Audit	6/12/2013	10:57:44 PM	Security	Object A...	560	employee
Failure Audit	6/12/2013	10:57:44 PM	Security	Object A...	560	employee
Failure Audit	6/12/2013	10:57:44 PM	Security	Object A...	560	employee
Failure Audit	6/12/2013	10:57:44 PM	Security	Object A...	560	employee
Success Audit	6/12/2013	10:57:42 PM	Security	Object A...	562	employee
Success Audit	6/12/2013	10:57:40 PM	Security	Object A...	562	SYSTEM
Success Audit	6/12/2013	10:57:40 PM	Security	Object A...	560	SYSTEM
Success Audit	6/12/2013	10:57:40 PM	Security	Object A...	562	SYSTEM
Success Audit	6/12/2013	10:57:40 PM	Security	Object A...	560	SYSTEM
Success Audit	6/12/2013	10:57:40 PM	Security	Object A...	562	employee
Success Audit	6/12/2013	10:57:40 PM	Security	Object A...	562	employee
Success Audit	6/12/2013	10:57:39 PM	Security	Object A...	562	employee
Success Audit	6/12/2013	10:57:31 PM	Security	Object A...	562	SYSTEM
Success Audit	6/12/2013	10:57:31 PM	Security	Object A...	560	SYSTEM
Success Audit	6/12/2013	10:57:29 PM	Security	Object A...	562	manager

Figure 72: The Security Log

24. Select any event and double-click to view more details about the event. There should be a Success Audit where the manager user accessed the salary folder and a Failure Audit where the employee user accessed the salary folder.



Date: 6/12/2013   Source: Security
Time: 11:30:03 PM   Category: Object Access
Type: Failure Aud   Event ID: 560
User: MSEC\employee
Computer: WIN2K3DC

Description:

```
Object Open:
        Object Server:      Security
        Object Type:        File
        Object Name:        C:\salary
```

Figure 73: Event Details

3.2 Conclusion

Once Auditing is set on a file or folder and auditing for object access is turned on, users' access to objects can be tracked. Failed audits are the result of users trying to access objects they do not have permission to view. Success Audits take place when a user who is given access to an object is able to successfully access that file or folder.

3.3 Discussion Questions

1. What are the three main logs found in the Windows Event Viewer?
2. What two types of Events can take place in the Security Log?
3. In normal circumstances, can regular users log on to Domain Controllers?
4. Where do you go to grant regular users the ability to log on a Domain Controller?

References

1. Event Viewer:
   http://support.microsoft.com/kb/308427

2. Gpupdate:
   http://technet.microsoft.com/en-us/library/bb490983.aspx

3. Echo Command:
   http://technet.microsoft.com/en-us/library/bb490897.aspx

4. Active Directory:
http://msdn.microsoft.com/en-us/library/windows/desktop/aa746492(v=vs.85).aspx

5. Group Policy:
   http://technet.microsoft.com/en-us/windowsserver/bb310732.aspx