

# JBL LAB3: Configuring Windows File System Permissions

## Lab #3 Lab Challenge & Analysis

---

### Table of Contents

<b>Part 1: Analysis &amp; Discussion:</b> .....	<b>1</b>
<b>Networking</b> .....	<b>2</b>
<b>Faculty</b> .....	<b>2</b>
<b>Students</b> .....	<b>2</b>
NET303: Network Design and Management.....	2
NET404: Network Forensics.....	2
<b>Security</b> .....	<b>2</b>
SEC303: Advanced Cryptography.....	2
SEC404: Security Policies and Procedures.....	2
<b>Programming</b> .....	<b>2</b>
PRO303: Information Structures with Java.....	2
PRO404: Information Structures with Python.....	2
<b>Part 2: Tools and Commands:</b> .....	<b>3</b>
<b>Part 3: Challenge Exercise:</b> .....	<b>4</b>
<b>1. Remove Permissions</b> .....	<b>4</b>
<b>2. Creating Security Groups for Security Department</b> .....	<b>4</b>
Setting groups for Security Department:.....	4
Set Group Permissions.....	5
<b>Part 2: Tools and Commands for Security</b> .....	<b>6</b>
<b>Below I have used the command: Get-ChildItem -Path "C:\ SindyMorel\Security" -Recurse   Get-Acl</b> .....	<b>6</b>
<b>Part 3: Challenge Exercise – Remove Permissions from Security Department</b> .....	<b>6</b>

**Part 1: Analysis & Discussion:** Comparison of folder structure vs Get-ACL commands.

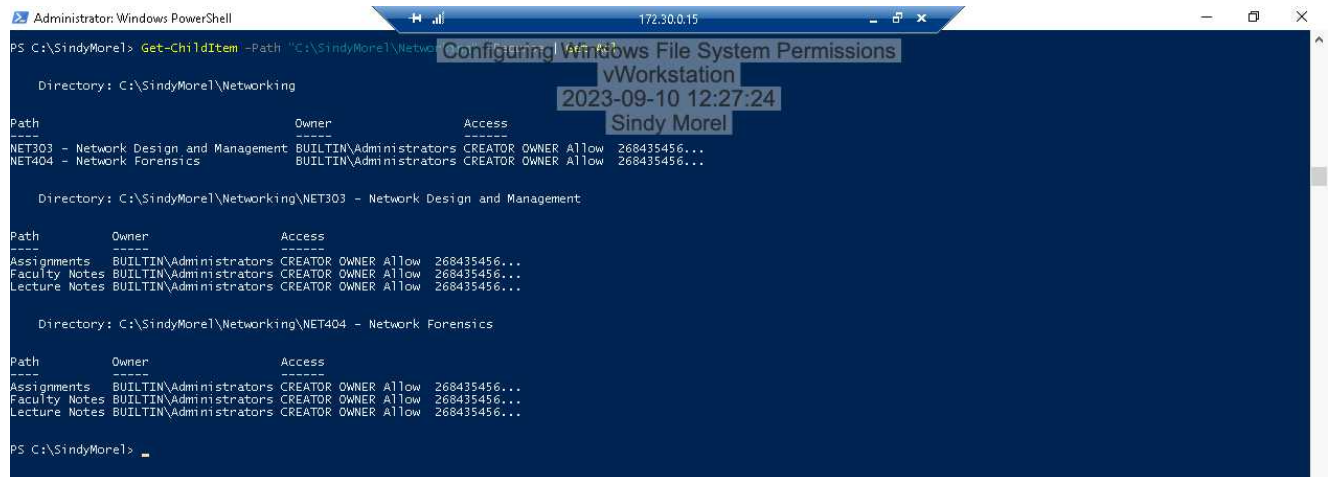
Networking	Faculty	Students
<b>NET303: Network Design and Management</b>		
Assignments	Full Control	Read Only
Faculty Notes	Full Control	
Lecture Notes	Full Control	Read Only
<b>NET404: Network Forensics</b>		
Assignments	Full Control	Read Only
Faculty Notes	Full Control	
Lecture Notes	Full Control	Read Only
<b>Security</b>		
<b>SEC303: Advanced Cryptography</b>		
Assignments	Full Control	Read Only
Faculty Notes	Full Control	
Lecture Notes	Full Control	Read Only
<b>SEC404: Security Policies and Procedures</b>		
Assignments	Full Control	Read Only
Faculty Notes	Full Control	
Lecture Notes	Full Control	Read Only
<b>Programming</b>		
<b>PRO303: Information Structures with Java</b>		
Assignments	Full Control	Read Only
Faculty Notes	Full Control	
Lecture Notes	Full Control	Read Only
<b>PRO404: Information Structures with Python.</b>		
Assignments	Full Control	Read Only
Faculty Notes	Full Control	
Lecture Notes	Full Control	Read Only

In this structure, I have specified that **faculty** members should have Full Control permissions for all folders, including **Lecture Notes, Faculty Notes, and Assignments**. **Students**, on the other hand, are granted **Read-Only permissions** for **Lecture Notes and Assignments** folders, which allows them to view but not modify the contents.

To compare this design to the results of the Get-ACL command, I would need to execute the Get-ACL command for each folder and subfolder in the structure and review the returned ACL to ensure that the permissions match the design. I would repeat this command for each folder and subfolder in the structure to verify that the specified permissions are correctly applied in your file system.

**Part 2: Tools and Commands:** PowerShell Get-Command listing permissions on a directory.

- Below I have used the command: `Get-ChildItem -Path "C:\SindyMorel\Networking" -Recurse | Get-Acl`



```
Administrator: Windows PowerShell
PS C:\SindyMorel> Get-ChildItem -Path "C:\SindyMorel\Networking" -Recurse | Get-Acl

Directory: C:\SindyMorel\Networking

Path      Owner      Access
-----
NET303 - Network Design and Management BUILTIN\Administrators CREATOR OWNER Allow 268435456...
NET404 - Network Forensics             BUILTIN\Administrators CREATOR OWNER Allow 268435456...

Directory: C:\SindyMorel\Networking\NET303 - Network Design and Management

Path      Owner      Access
-----
Assignments BUILTIN\Administrators CREATOR OWNER Allow 268435456...
Faculty Notes BUILTIN\Administrators CREATOR OWNER Allow 268435456...
Lecture Notes BUILTIN\Administrators CREATOR OWNER Allow 268435456...

Directory: C:\SindyMorel\Networking\NET404 - Network Forensics

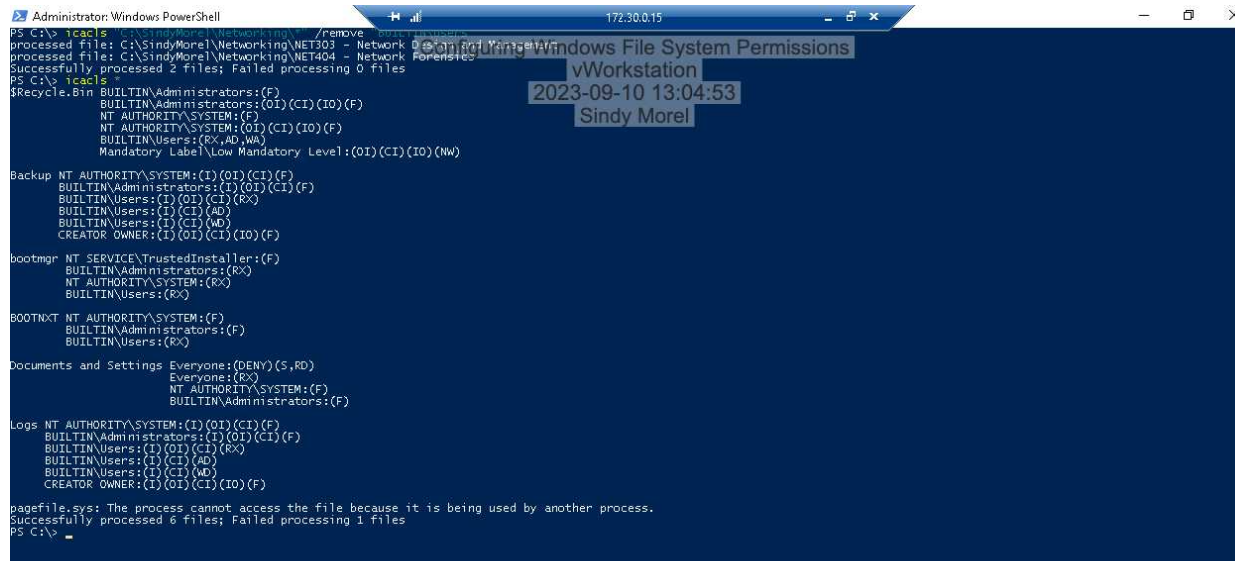
Path      Owner      Access
-----
Assignments BUILTIN\Administrators CREATOR OWNER Allow 268435456...
Faculty Notes BUILTIN\Administrators CREATOR OWNER Allow 268435456...
Lecture Notes BUILTIN\Administrators CREATOR OWNER Allow 268435456...

PS C:\SindyMorel>
```

Mandliya. (2023, April 6). *PowerShell - Get Permissions on Folder and Subfolders - Java2Blog*. Java2Blog. Retrieved September 10, 2023, from <https://java2blog.com/powershell-get-permissions-on-folder-and-subfolders/>

## Part 3: Challenge Exercise:

### 1. Remove Permissions



```
Administrator: Windows PowerShell
PS C:\> icacls /remove
processed file: C:\SindyMorel\Networking\NET305 - Network Forensics
processed file: C:\SindyMorel\Networking\NET404 - Network Forensics
Successfully processed 2 files; Failed processing 0 files
PS C:\> icacls
Recycle.Bin BUILTIN\Administrators:(F)
              NT AUTHORITY\SYSTEM:(F)
              NT AUTHORITY\SYSTEM:(OI)(CI)(IO)(F)
              BUILTIN\Users:(Rx,AD,WX)
              Mandatory Label\Low Mandatory Level:(OI)(CI)(IO)(NW)

Backup NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
        BUILTIN\Administrators:(I)(OI)(CI)(F)
        BUILTIN\Users:(I)(OI)(CI)(RX)
        BUILTIN\Users:(I)(CI)(AD)
        BUILTIN\Users:(I)(CI)(WD)
        CREATOR OWNER:(I)(OI)(CI)(IO)(F)

bootmgr NT SERVICE\TrustedInstaller:(F)
        BUILTIN\Administrators:(RX)
        NT AUTHORITY\SYSTEM:(RX)
        BUILTIN\Users:(RX)

BOOTNXT NT AUTHORITY\SYSTEM:(F)
        BUILTIN\Administrators:(F)
        BUILTIN\Users:(RX)

Documents and Settings Everyone:(DENY)(S,WD)
                        Everyone:(RX)
                        NT AUTHORITY\SYSTEM:(F)
                        BUILTIN\Administrators:(F)

Logs NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
      BUILTIN\Administrators:(I)(OI)(CI)(F)
      BUILTIN\Users:(I)(OI)(CI)(RX)
      BUILTIN\Users:(I)(CI)(AD)
      BUILTIN\Users:(I)(CI)(WD)
      CREATOR OWNER:(I)(OI)(CI)(IO)(F)

pagefile.sys: The process cannot access the file because it is being used by another process.
Successfully processed 6 files; Failed processing 1 files
PS C:\>
```

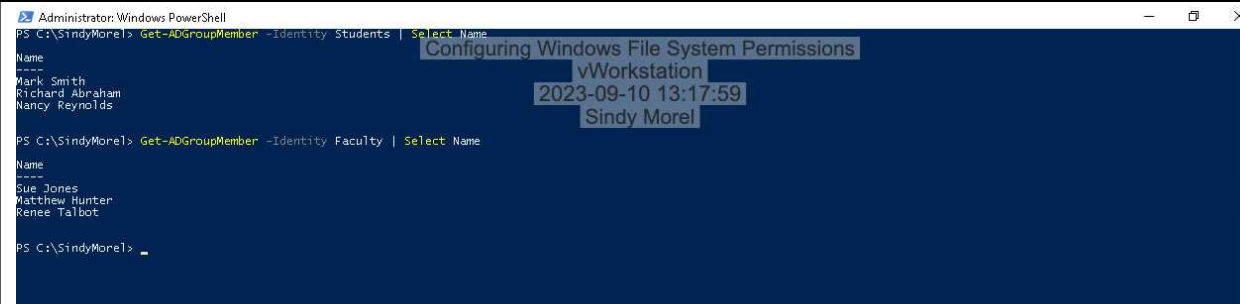
- Permissions have been removed.

(2021, August 11). *Icacs: The Ultimate Guide*. Icacs: The Ultimate Guide. Retrieved September 10, 2023, from <https://adamtheautomator.com/icacs/>

# Security Department

### 2. Creating Security Groups for Security Department

#### Setting groups for Security Department:



```
Administrator: Windows PowerShell
PS C:\SindyMorel> Get-ADGroupMember -Identity Students | Select Name
Name
----
Mark Smith
Richard Abraham
Nancy Reynolds

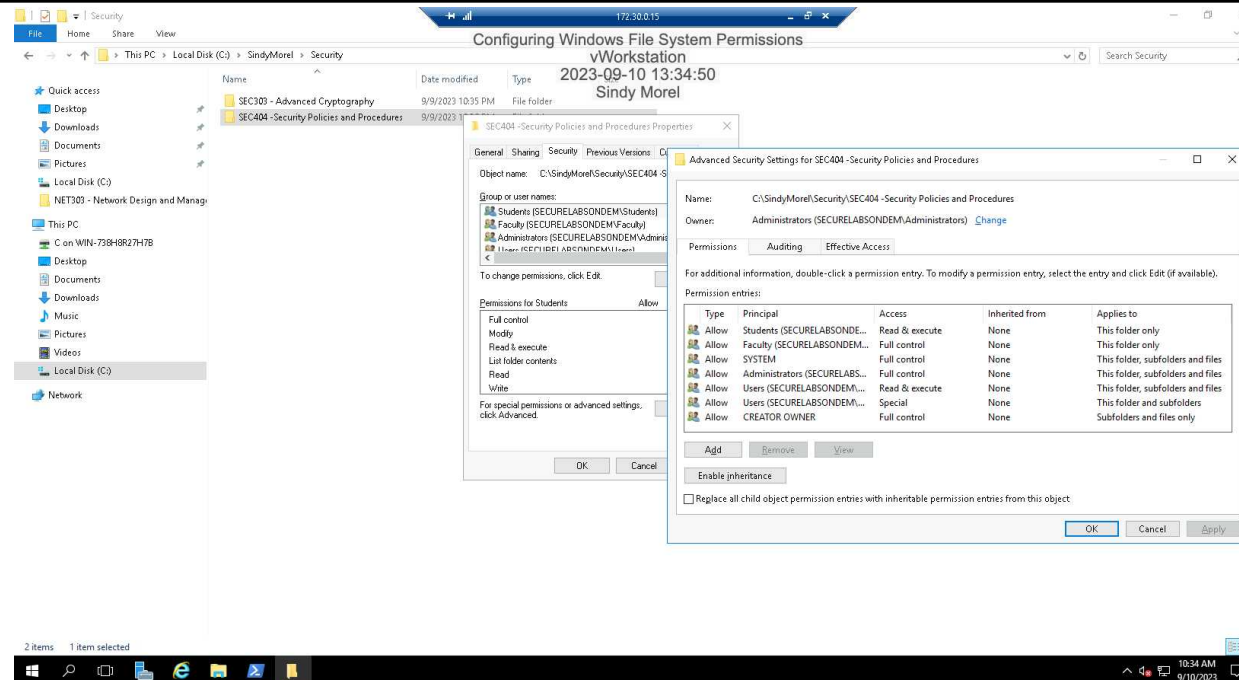
PS C:\SindyMorel> Get-ADGroupMember -Identity Faculty | Select Name
Name
----
Sue Jones
Matthew Hunter
Renee Talbot

PS C:\SindyMorel>
```

Students & Faculty

## Set Group Permissions

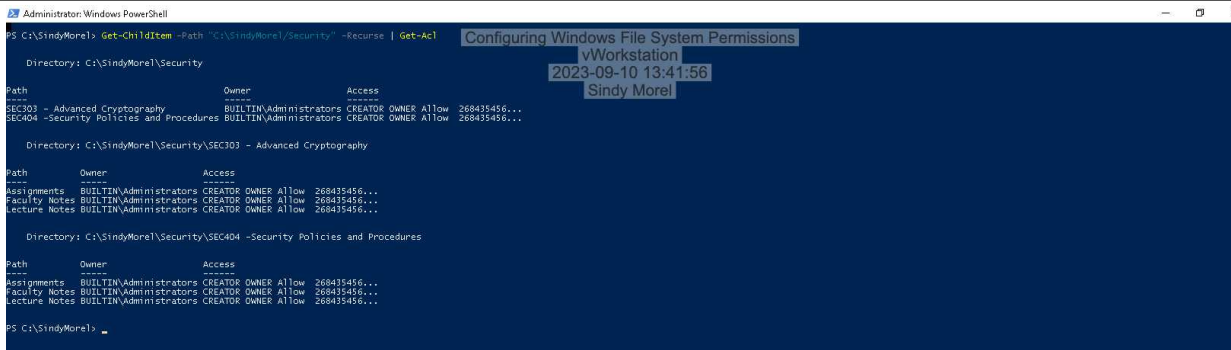
```
Administrator: Windows PowerShell
PS C:\SindyMorel> icacls "C:\SindyMorel\*" /inheritance:d /T
processed file: C:\SindyMorel\Networking
processed file: C:\SindyMorel\Programming
processed file: C:\SindyMorel\Security
processed file: C:\SindyMorel\Networking\NET303 - Network Design and Management
processed file: C:\SindyMorel\Networking\NET404 - Network Forensics
processed file: C:\SindyMorel\Networking\NET303 - Network Design and Management\Assignments
processed file: C:\SindyMorel\Networking\NET303 - Network Design and Management\Faculty Notes
processed file: C:\SindyMorel\Networking\NET404 - Network Forensics\Assignments
processed file: C:\SindyMorel\Networking\NET404 - Network Forensics\Faculty Notes
processed file: C:\SindyMorel\Networking\NET404 - Network Forensics\Lecture Notes
processed file: C:\SindyMorel\Programming\PRO 303 - Information Structures with Java
processed file: C:\SindyMorel\Programming\PRO 404 - Information Structures with Python
processed file: C:\SindyMorel\Programming\PRO 303 - Information Structures with Java\Assignments
processed file: C:\SindyMorel\Programming\PRO 303 - Information Structures with Java\Faculty Notes
processed file: C:\SindyMorel\Programming\PRO 404 - Information Structures with Python\Assignments
processed file: C:\SindyMorel\Programming\PRO 404 - Information Structures with Python\Faculty Notes
processed file: C:\SindyMorel\Programming\PRO 404 - Information Structures with Python\Lecture Notes
processed file: C:\SindyMorel\Security\SEC303 - Advanced Cryptography
processed file: C:\SindyMorel\Security\SEC404 - Security Policies and Procedures
processed file: C:\SindyMorel\Security\SEC303 - Advanced Cryptography\Assignments
processed file: C:\SindyMorel\Security\SEC303 - Advanced Cryptography\Faculty Notes
processed file: C:\SindyMorel\Security\SEC404 - Security Policies and Procedures\Assignments
processed file: C:\SindyMorel\Security\SEC404 - Security Policies and Procedures\Faculty Notes
processed file: C:\SindyMorel\Security\SEC404 - Security Policies and Procedures\Lecture Notes
Successfully processed 27 files; Failed processing 0 files
PS C:\SindyMorel> icacls "C:\SindyMorel\Security" /grant:r Faculty:F /T
processed file: C:\SindyMorel\Security
processed file: C:\SindyMorel\Security\SEC303 - Advanced Cryptography
processed file: C:\SindyMorel\Security\SEC404 - Security Policies and Procedures
processed file: C:\SindyMorel\Security\SEC303 - Advanced Cryptography\Assignments
processed file: C:\SindyMorel\Security\SEC303 - Advanced Cryptography\Faculty Notes
processed file: C:\SindyMorel\Security\SEC303 - Advanced Cryptography\Lecture Notes
processed file: C:\SindyMorel\Security\SEC404 - Security Policies and Procedures\Assignments
processed file: C:\SindyMorel\Security\SEC404 - Security Policies and Procedures\Faculty Notes
processed file: C:\SindyMorel\Security\SEC404 - Security Policies and Procedures\Lecture Notes
Successfully processed 9 files; Failed processing 0 files
PS C:\SindyMorel> icacls "C:\SindyMorel\Security" /grant:r Students:RX /T
processed file: C:\SindyMorel\Security
processed file: C:\SindyMorel\Security\SEC303 - Advanced Cryptography
processed file: C:\SindyMorel\Security\SEC404 - Security Policies and Procedures
processed file: C:\SindyMorel\Security\SEC303 - Advanced Cryptography\Assignments
processed file: C:\SindyMorel\Security\SEC303 - Advanced Cryptography\Faculty Notes
processed file: C:\SindyMorel\Security\SEC303 - Advanced Cryptography\Lecture Notes
processed file: C:\SindyMorel\Security\SEC404 - Security Policies and Procedures\Assignments
processed file: C:\SindyMorel\Security\SEC404 - Security Policies and Procedures\Faculty Notes
processed file: C:\SindyMorel\Security\SEC404 - Security Policies and Procedures\Lecture Notes
Successfully processed 9 files; Failed processing 0 files
PS C:\SindyMorel> icacls "C:\SindyMorel\Security\SEC303 - Advanced Cryptography\Faculty Notes" /remove:ig Students
Successfully processed 2 files; Failed processing 0 files
PS C:\SindyMorel> icacls "C:\SindyMorel\Security\SEC404 - Security Policies and Procedures\Faculty Notes" /remove:ig Students
Successfully processed 1 files; Failed processing 0 files
PS C:\SindyMorel> icacls C:\SindyMorel\Security\SECURELABSONDEM\Students:(D)
SECURELABSONDEM\Faculty:(F)
NT AUTHORITY\SYSTEM:(OI)(CI)(F)
BUILTIN\Administrators:(OI)(CI)(F)
BUILTIN\Users:(OI)(CI)(D)
BUILTIN\Users:(CI)(D)
CREATOR OWNER:(OI)(CI)(IO)(F)
C:\SindyMorel\Security\SEC404 - Security Policies and Procedures SECURELABSONDEM\Students:(D)
SECURELABSONDEM\Faculty:(F)
NT AUTHORITY\SYSTEM:(OI)(CI)(F)
BUILTIN\Administrators:(OI)(CI)(F)
BUILTIN\Users:(OI)(CI)(D)
BUILTIN\Users:(CI)(D)
CREATOR OWNER:(OI)(CI)(IO)(F)
Successfully processed 2 files; Failed processing 0 files
PS C:\SindyMorel>
```



Rights to Students modified to read and execute to specified folders and be removed from Faculty Notes.

## Part 2: Tools and Commands for Security

Below I have used the command: `Get-ChildItem -Path "C:\SindyMorel\Security" -Recurse | Get-Acl`



```
Administrator: Windows PowerShell
PS C:\SindyMorel> Get-ChildItem -Path "C:\SindyMorel\Security" -Recurse | Get-Acl

Directory: C:\SindyMorel\Security

Path                Owner                Access
-----
SEC303 - Advanced Cryptography BUILTIN\Administrators CREATOR OWNER Allow 268435456...
SEC404 - Security Policies and Procedures BUILTIN\Administrators CREATOR OWNER Allow 268435456...

Directory: C:\SindyMorel\Security\SEC303 - Advanced Cryptography

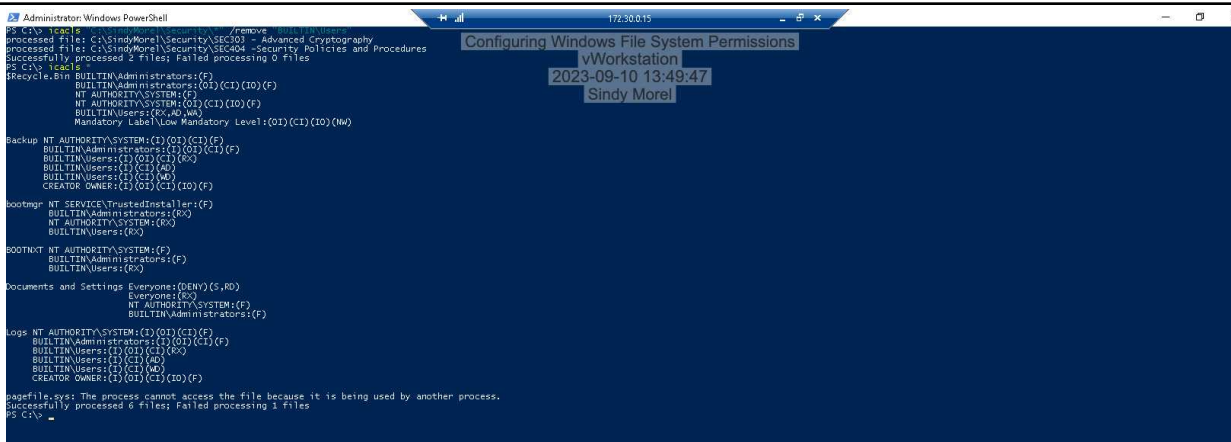
Path                Owner                Access
-----
Assignments BUILTIN\Administrators CREATOR OWNER Allow 268435456...
Faculty Notes BUILTIN\Administrators CREATOR OWNER Allow 268435456...
Lecture Notes BUILTIN\Administrators CREATOR OWNER Allow 268435456...

Directory: C:\SindyMorel\Security\SEC404 - Security Policies and Procedures

Path                Owner                Access
-----
Assignments BUILTIN\Administrators CREATOR OWNER Allow 268435456...
Faculty Notes BUILTIN\Administrators CREATOR OWNER Allow 268435456...
Lecture Notes BUILTIN\Administrators CREATOR OWNER Allow 268435456...

PS C:\SindyMorel>
```

## Part 3: Challenge Exercise – Remove Permissions from Security Department.



```
Administrator: Windows PowerShell
PS C:\> Remove-ACL -Path "C:\SindyMorel\Security" -Recurse
processed files: C:\SindyMorel\Security\SEC303 - Advanced Cryptography
processed files: C:\SindyMorel\Security\SEC404 - Security Policies and Procedures
Successfully processed 2 files; Failed processing 0 files
PS C:\> Get-ACL
$Recycle.Bin BUILTIN\Administrators:(F)
BUILTIN\Administrators:(OI)(CI)(IO)(F)
NT AUTHORITY\SYSTEM:(F)
NT AUTHORITY\SYSTEM:(OI)(CI)(IO)(F)
BUILTIN\Users:(O)(A)(W)
Mandatory Label\Low Mandatory Level:(OI)(CI)(IO)(NW)

Backup NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
BUILTIN\Administrators:(F)(OI)(CI)(F)
BUILTIN\Users:(I)(OI)(CI)(F)
BUILTIN\Users:(I)(CI)(F)
BUILTIN\Users:(I)(CI)(F)
CREATOR OWNER:(I)(OI)(CI)(IO)(F)

bootmgr NT SERVICE\TrustedInstaller:(F)
BUILTIN\Administrators:(F)
NT AUTHORITY\SYSTEM:(F)
BUILTIN\Users:(F)

BOOTNXT NT AUTHORITY\SYSTEM:(F)
BUILTIN\Administrators:(F)
BUILTIN\Users:(F)

Documents and Settings Everyone:(DENY)(S,RO)
Everyone:(F)
NT AUTHORITY\SYSTEM:(F)
BUILTIN\Administrators:(F)

Logs NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
BUILTIN\Administrators:(I)(OI)(CI)(F)
BUILTIN\Users:(I)(OI)(CI)(F)
BUILTIN\Users:(I)(CI)(F)
BUILTIN\Users:(I)(CI)(F)
CREATOR OWNER:(I)(OI)(CI)(IO)(F)

pagefile.sys: The process cannot access the file because it is being used by another process.
Successfully processed 6 files; Failed processing 1 file
PS C:\>
```

Permissions have been removed.