

Windows Fundamentals:

Link to challenge: <https://academy.hackthebox.com/module/49>

(log in required)

Class: Tier 0 | Fundamental | General

Before we begin: throughout the module we will be requested to login to target windows machines.

The credentials and target IP will be provided for us by the module.

we will use xfreerdp with the command:

```
xfreerdp /v:<Target IP> /u:<username> /p:<password>  
/dynamic-resolution
```

Introduction

Introduction to Windows:

Question: What is the Build Number of the target workstation?

Answer: 19041

Method: first lets log-in to the windows target machine and open powershell.

And its done, enter the command:

```
Get-WmiObject -Class win32_OperatingSystem | select  
Version, BuildNumber
```

There we will see the build number on the right column:

```
PS C:\Users\htb-student> Get-WmiObject -Class win32_OperatingSystem | select Version, BuildNumber  
  
Version      BuildNumber  
-----  
10.0.19041  19041
```

Question: Which Windows NT version is installed on the workstation? (i.e. Windows X - case sensitive)

Answer: Windows 10

Method: we can run

```
[System.Environment]::OSVersion
```

For full NT version:

```
PS C:\Users\htb-student> [System.Environment]::OSVersion

Platform ServicePack Version      VersionString
-----
Win32NT           10.0.19041.0 Microsoft Windows NT 10.0.19041.0
```

Or

```
[System.Environment]::OSVersion.Version
```

For more detailed explanation for each number:

```
PS C:\Users\htb-student> [System.Environment]::OSVersion.Version

Major Minor Build Revision
-----
10     0     19041  0
```

However the module wants here only the Major number, maybe something to do with this from the module:

Operating System Names	Version Number
Windows 10, Server 2016, Server 2019	10.0

Either way while the official answer is 'Windows 10', more detailed answer will be 'Windows NT 10.0.19041.0'.

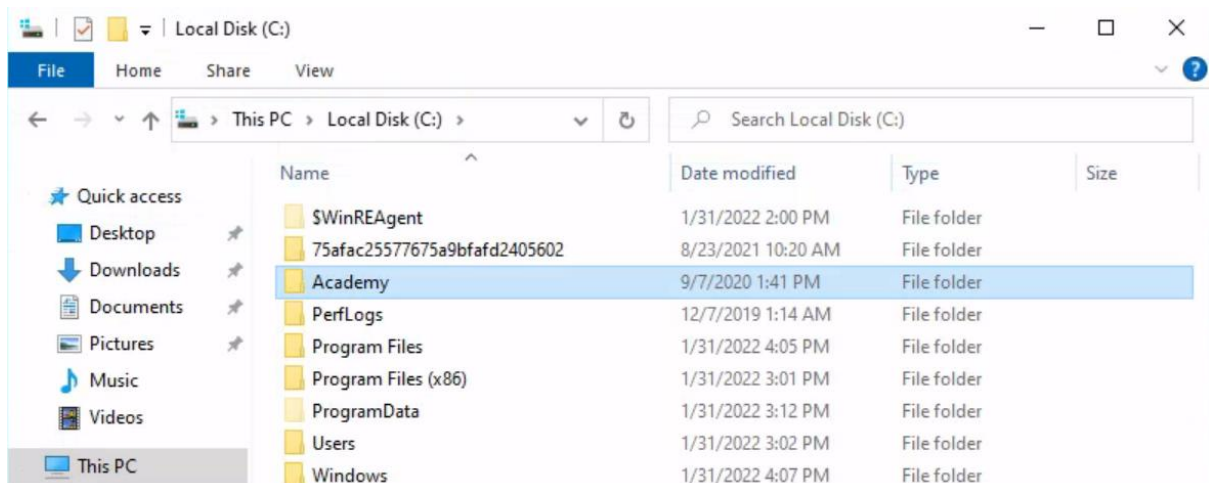
Core of the Operating System

Operating System Structure:

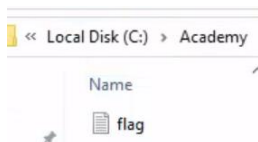
Question: Find the non-standard directory in the C drive. Submit the contents of the flag file saved in this directory

Answer: c8fe8d977d3a0c655ed7cf81e4d13c75

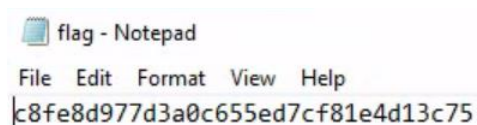
Method: login to the target Windows machine, go to C:\ drive:



We can observe the 'Academy' folder is not a default folder to C drive, lets enter it:



We see a flag:



File System:

Question: What system user has full control over the c:\users directory?

Answer: bob.smith

Method: on the target machine, we run the cmd command:

```
hostname
```

to get the name of the computer, or the system:

```
C:\Users\htb-student>hostname  
WS01
```

Now that we know the computer name lets run the cmd commad:

```
icacls c:\users
```

where 'icacls' is the command that displayed (and can change) users permissions, for this purpose we are looking for a system user (a user of 'WS01') with the permission 'F', which stands for 'full access':

```
C:\Users\htb-student>icacls c:\users  
c:\users Everyone:(OI)(CI)(RX)  
          NT AUTHORITY\SYSTEM:(OI)(CI)(F)  
          BUILTIN\Administrators:(OI)(CI)(F)  
          WS01\bob.smith:(OI)(CI)(F)  
          BUILTIN\Users:(OI)(CI)(RX)  
  
Successfully processed 1 files; Failed processing 0 files
```

We can see the user which fills the requirements is 'bob.smith'.

NTFS vs. Share Permissions:

Question: What protocol discussed in this section is used to share resources on the network using Windows? (Format: case sensitive)

Answer: SMB

Method: 'The **Server Message Block protocol (SMB)** is used in Windows to connect shared resources like files and printers. It is used in large, medium, and small enterprise environments.'

Question: What is the name of the utility that can be used to view logs made by a Windows system? (Format: 2 words, 1 space, not case sensitive)

Answer: Event Viewer

Method: '**Event Viewer** is another good place to investigate actions completed on Windows. Almost every operating system has a logging mechanism and a utility to view the logs that were captured. Know that a log is like a journal entry for a computer, where the computer writes down all the actions that were performed and numerous details associated with that action. We can view the logs created for every action we performed when accessing the Windows 10 target box, as well as when creating, editing and accessing the shared folder.'

Question: What is the full directory path to the Company Data share we created?

Answer: C:\Users\htb-student\Desktop\Company Data

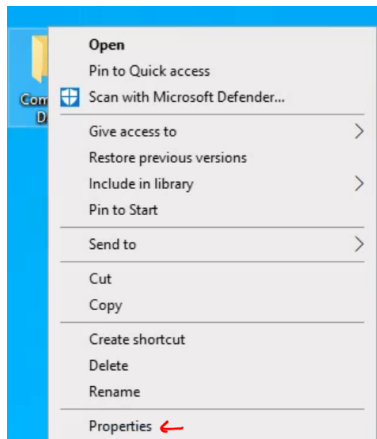
Method: on the target machine, we will begin by creating a share called 'Company Data'.

First, we will create in the desktop a folder called 'Company Data':

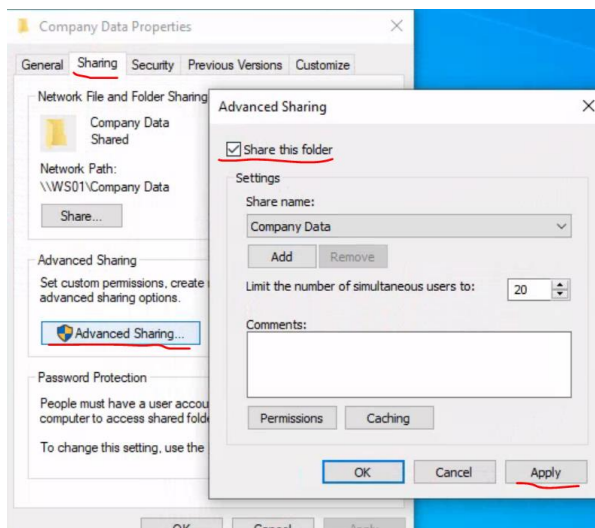


When its done, we need to share it:

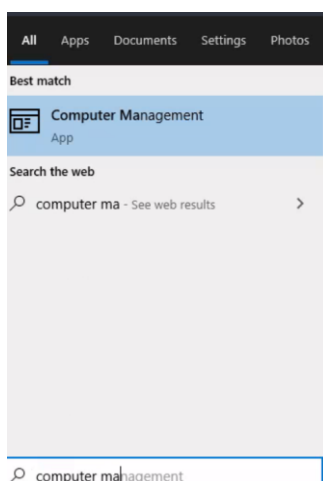
Right click on the folder → properties:



→ Sharing → Advanced Sharing → select yes for 'Share this folder' → Apply

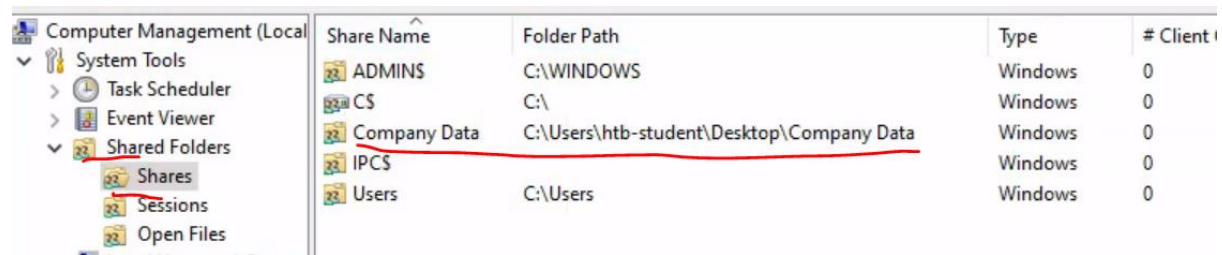


And we have a share ready, to view it we will go to computer management:



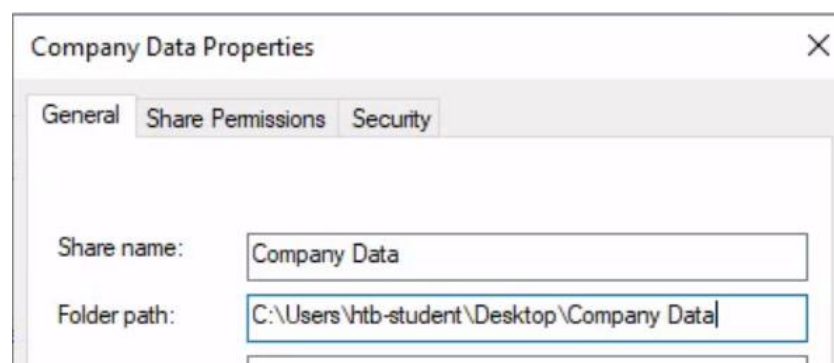
In 'Computer Management', we go to 'Shared Folders' → 'Shares'.

There we can observe the share we made 'Company Data' and its path



Share Name	Folder Path	Type	# Client
ADMIN\$	C:\WINDOWS	Windows	0
CS	C:\	Windows	0
Company Data	C:\Users\htb-student\Desktop\Company Data	Windows	0
IPC\$		Windows	0
Users	C:\Users	Windows	0

on it, we do right click → properties, and copy the path:



Working with Services & Processes

Windows Services & Processes:

Question: Identify one of the non-standard update services running on the host. Submit the full name of the service executable (not the DisplayName) as your answer.

Answer: FoxitReaderUpdateService.exe

Method: we run the powershell command:

```
Get-Process | Select-Object processname, path | Where-Object { $_.path -notlike 'C:\Windows\*' -and $_.path -ne $null -and $_.path -ne '' } | fl
```

The command will get the processes which their path is not of 'C:\Windows\' and is not blank either:

```
PS C:\WINDOWS\system32> Get-Process | Select-Object processname, path | Where-Object { $_.path -notlike 'C:\Windows\*' -and $_.path -ne $null -and $_.path -ne '' } | fl

ProcessName : FoxitReaderUpdateService
Path        : C:\Program Files (x86)\Foxit Software\Foxit Reader\FoxitReaderUpdateService.exe

ProcessName : MicrosoftEdgeUpdate
Path        : C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe

ProcessName : VGAuthService
Path        : C:\Program Files\VMware\VMware Tools\VGAuthService.exe

ProcessName : vmtoolsd
Path        : C:\Program Files\VMware\VMware Tools\vmtoolsd.exe

ProcessName : vmtoolsd
Path        : C:\Program Files\VMware\VMware Tools\vmtoolsd.exe

ProcessName : YourPhone
Path        : C:\Program Files\WindowsApps\Microsoft.YourPhone_1.21121.250.0_x64__8wekyb3d8bbwe\YourPhone.exe
```

The hint tells us that the answer is a process which related to PDF editing, that narrows down the answer to the first option. ('[Foxit Reader is a popular PDF viewer and editor](#)')

Interacting with Windows

Interacting with the Windows Operating System:

Question: What is the alias set for the ipconfig.exe command?

Answer: ifconfig

Method: open PowerShell on the target Windows machine, and enter the command:

```
Get-Alias | findstr ipconfig
```

We get all the aliases, and filter for 'ipconfig.exe':

```
PS C:\Users\htb-student> Get-Alias | findstr ipconfig
Alias                ifconfig -> ipconfig.exe
```

Question: Find the Execution Policy set for the LocalMachine scope.

Answer: Unrestricted

Method: we run the powershell command:

```
Get-ExecutionPolicy -List | findstr LocalMachine
```

```
PS C:\Users\htb-student> Get-ExecutionPolicy -List | findstr LocalMachine
LocalMachine      Unrestricted
```

Windows Management Instrumentation (WMI):

Question: Use WMI to find the serial number of the system.

Answer: 00329-10280-00000-AA938

Method: on cmd, enter:

```
wmic os list brief
```

```
C:\Users\htb-student>wmic os list brief
BuildNumber  Organization  RegisteredUser  SerialNumber  SystemDirectory  Version
19041        mr3n          mr3n            00329-10280-00000-AA938  C:\WINDOWS\system32  10.0.19041
```

Diving Deeper & Close Out

Windows Security:

Question: Find the SID of the bob.smith user.

Answer: S-1-5-21-2614195641-1726409526-3792725429-1003

Method: login to windows target machine, adhering to the hint – we will use Wmi, and we run the PowerShell command:

```
Get-WmiObject -Class Win32_UserAccount -Filter "Name='bob.smith'" | Select-Object -ExpandProperty SID
```

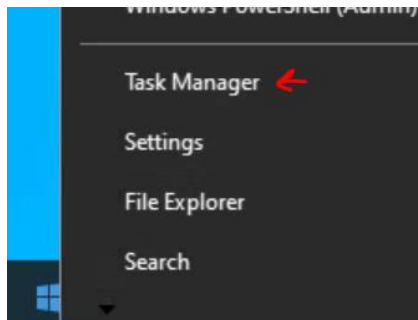
```
PS C:\Users\htb-student> Get-WmiObject -Class Win32_UserAccount -Filter "Name='bob.smith'" | Select-Object -ExpandProperty SID
S-1-5-21-2614195641-1726409526-3792725429-1003
```

Question: What 3rd party security application is disabled at startup for the current user? (The answer is case sensitive).

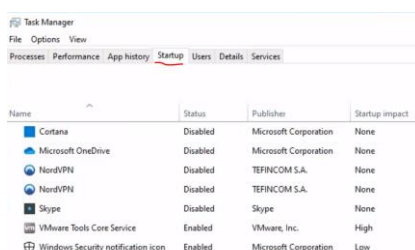
Answer: NordVPN

Method: Method 1:

Open the task manager (right click on windows icon):



And there go to startup



Name	Status	Publisher	Startup impact
Cortana	Disabled	Microsoft Corporation	None
Microsoft OneDrive	Disabled	Microsoft Corporation	None
NordVPN	Disabled	TEFINCOM S.A.	None
NordVPN	Disabled	TEFINCOM S.A.	None
Skype	Disabled	Skype	None
VMware Tools Core Service	Enabled	VMware, Inc.	High
Windows Security notification icon	Enabled	Microsoft Corporation	Low

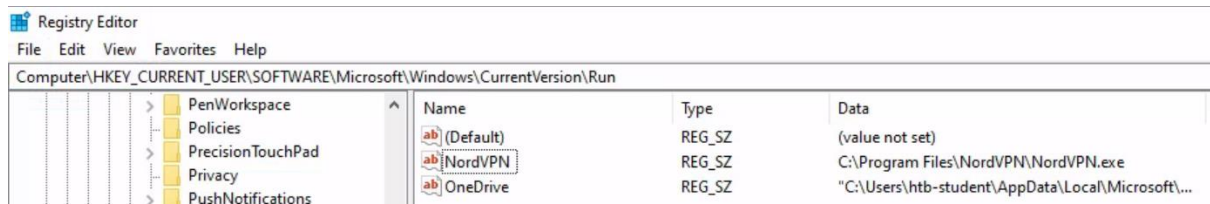
we can observe the only disabled app that is somewhat security-related is NordVPN.

Method 2:

Open the registry editor (require administrator privileges)

And go to

'Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run' (where the user's application that run on startup are listed:



Only one app is security related.

Method 3: run on powershell:

```
reg query  
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\  
Run
```

to conduct registry query on the same path from the previous method:

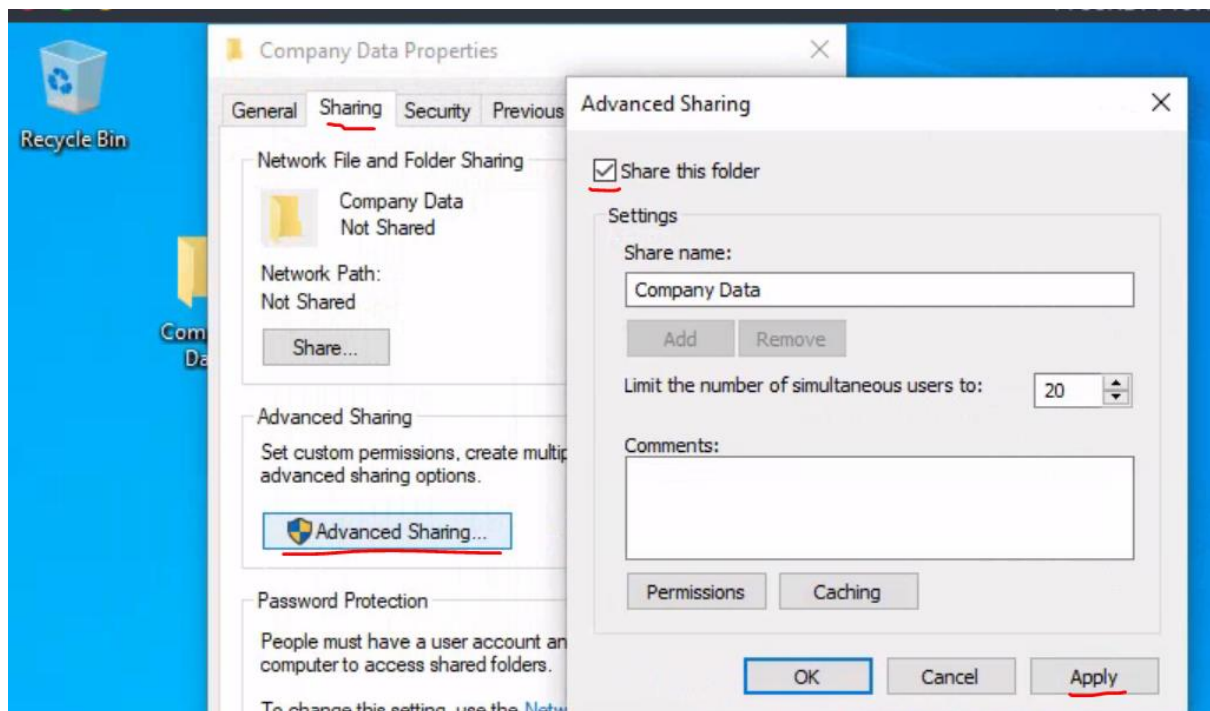
```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run  
OneDrive    REG_SZ    "C:\Users\htb-student\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background  
NordVPN     REG_SZ    C:\Program Files\NordVPN\NordVPN.exe
```

Skills Assessment - Windows Fundamentals:

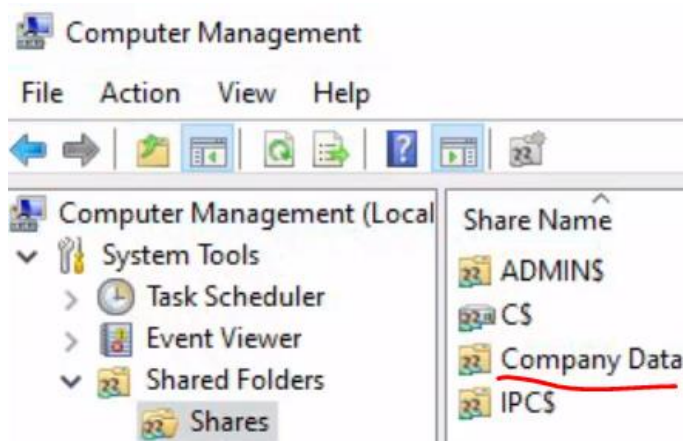
For the skill assessment, we need to construct the Windows environment by ourselves according to those steps:

1. Creating a shared folder called Company Data

We will retrace our steps to create a share from 'NTFS vs. Share Permissions' section:

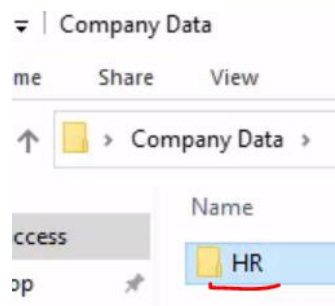


We can confirm its creation in 'Computer Management':



2. Creating a subfolder called HR inside of the Company Data folder

Right click in 'Company Data' folder, select 'Create Folder', name it 'HR':



3. Creating a user called Jim

- Uncheck: User must change password at logon

We will run in cmd as ADMINISTRATOR the commands:

```
net user Jim /add /passwordreq:no  
wmic useraccount where name='Jim' set PasswordExpires=FALSE
```

```
Administrator: Command Prompt  
Microsoft Windows [Version 10.0.19041.1]  
(c) 2019 Microsoft Corporation. All rights reserved.  
  
C:\WINDOWS\system32>net user Jim /add /passwordreq:no  
The command completed successfully.  
  
C:\WINDOWS\system32>wmic useraccount where name='Jim' set PasswordExpires=FALSE  
Updating property(s) of '\\WS01\ROOT\CIMV2:Win32_UserAccount.Domain="WS01",Name="Jim":'  
Property(s) update successful.
```

Or in powershell:

```
New-LocalUser -Name "Jim" -NoPassword  
Set-LocalUser -Name "Jim" -PasswordNeverExpires $true
```

4. Creating a security group called HR

We will run in cmd the command:

```
net localgroup HR /add
```

```
C:\WINDOWS\system32>net localgroup HR /add  
The command completed successfully.
```

Or in powershell:

```
New-LocalGroup -Name "HR"
```

5. Adding Jim to the HR security group

We will run in cmd the command:

```
net localgroup HR Jim /add
```

```
C:\WINDOWS\system32>net localgroup HR Jim /add  
The command completed successfully.
```

or in powershell:

```
Add-LocalGroupMember -Group "HR" -Member "Jim"
```

6. Adding the HR security group to the shared Company Data folder and NTFS permissions list

- Remove the default group that is present
- Share Permissions: Allow Change & Read
- Disable Inheritance before issuing specific NTFS permissions
- NTFS permissions: Modify, Read & Execute, List folder contents, Read, Write

We will run the powershell scripts:

Disable inheritance for the share folder:

```
$path = "C:\Users\htb-student\Desktop\Company Data"  
icacls "$path" /inheritance:d
```

```
PS C:\Users\htb-student> $path = "C:\Users\htb-student\Desktop\Company Data"  
>> icacls "$path" /inheritance:d  
processed file: C:\Users\htb-student\Desktop\Company Data  
Successfully processed 1 files; Failed processing 0 files
```

remove the default group:

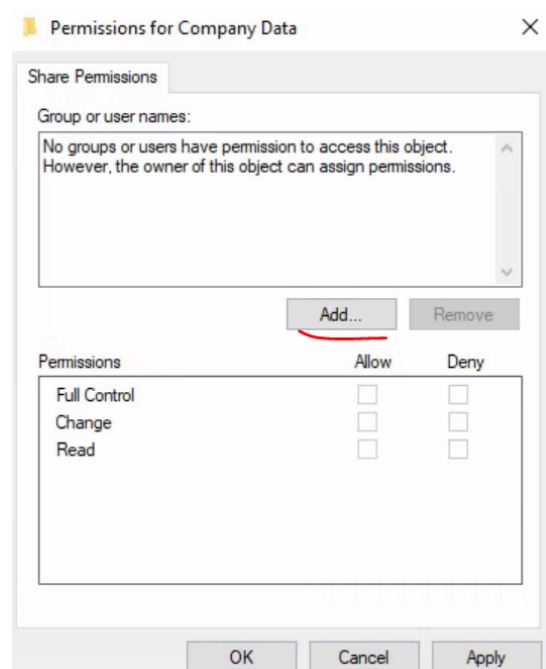
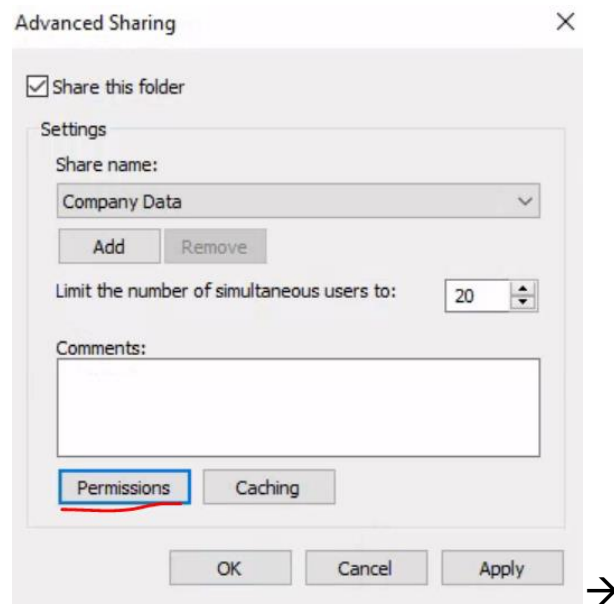
```
$path = "C:\Users\htb-student\Desktop\Company Data"  
icacls "$path" /remove "BUILTIN\Users"
```

```
PS C:\Users\htb-student> icacls "$path" /remove "BUILTIN\Users"  
processed file: C:\Users\htb-student\Desktop\Company Data  
Successfully processed 1 files; Failed processing 0 files
```

modify change permissions:

we will use GUI, enter the folder advanced sharing property (as before):

add the group 'HR' by selecting 'add', then on the window type 'HR' and select 'check names', and the end you should see this window state:



*remove any other group, if exists. *→

Select Users or Groups

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

From this location:
WS01

Enter the object names to select (examples):
WS01\HR

Advanced... OK Cancel

→

Permissions for Company Data

Share Permissions

Group or user names:
HR (WS01\HR)

Add... Remove

Permissions for HR

	Allow	Deny
Full Control	<input type="checkbox"/>	<input type="checkbox"/>
Change	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>

OK Cancel Apply

add NTFS permissions (open ADMINISTRATOR powershell):

```
$path = "C:\Users\htb-student\Desktop\Company Data"

$acl = Get-Acl $path
$hrGroup = "HR"

$permissions =
[System.Security.AccessControl.FileSystemRights]::Modify, `
[System.Security.AccessControl.FileSystemRights]::ReadAndExecute, `
[System.Security.AccessControl.FileSystemRights]::ListDirectory, `
[System.Security.AccessControl.FileSystemRights]::Read, `
[System.Security.AccessControl.FileSystemRights]::Write

$accessRule = New-Object
System.Security.AccessControl.FileSystemAccessRule($hrGroup,
$permissions, "ContainerInherit, ObjectInherit", "None",
"Allow")
$acl.SetAccessRule($accessRule)
Set-Acl $path $acl
```

```
PS C:\WINDOWS\system32> $path = "C:\Users\htb-student\Desktop\Company Data"
>>
>> $acl = Get-Acl $path
>> $hrGroup = "HR"
>>
>> $permissions = [System.Security.AccessControl.FileSystemRights]::Modify, `
>>                 [System.Security.AccessControl.FileSystemRights]::ReadAndExecute, `
>>                 [System.Security.AccessControl.FileSystemRights]::ListDirectory, `
>>                 [System.Security.AccessControl.FileSystemRights]::Read, `
>>                 [System.Security.AccessControl.FileSystemRights]::Write
>>
>> $accessRule = New-Object System.Security.AccessControl.FileSystemAccessRule($hrGroup, $permissions, "
ContainerInherit, ObjectInherit", "None", "Allow")
>> $acl.SetAccessRule($accessRule)
>> Set-Acl $path $acl
>>
PS C:\WINDOWS\system32>
```

7. Adding the HR security group to the NTFS permissions list of the HR subfolder

- Remove the default group that is present
- Disable Inheritance before issuing specific NTFS permissions
- NTFS permissions: Modify, Read & Execute, List folder contents, Read, and Write

Open powershell on ADMINISTRATOR:

Disable Inheritance for the HR Subfolder

```
$hrSubFolderPath = "C:\Users\htb-student\Desktop\Company Data\HR"
```

```
icacls "$hrSubFolderPath" /inheritance:d
```

```
PS C:\WINDOWS\system32> $hrSubFolderPath = "C:\Users\htb-student\Desktop\Company Data\HR"
>>
>> icacls "$hrSubFolderPath" /inheritance:d
processed file: C:\Users\htb-student\Desktop\Company Data\HR
Successfully processed 1 files; Failed processing 0 files
```

Remove Default Group:

```
$hrSubFolderPath = "C:\Users\htb-student\Desktop\Company Data\HR"
```

```
icacls "$hrSubFolderPath" /remove "BUILTIN\Users"
```

```
PS C:\WINDOWS\system32> $hrSubFolderPath = "C:\Users\htb-student\Desktop\Company Data\HR"
>>
>> icacls "$hrSubFolderPath" /remove "BUILTIN\Users"
processed file: C:\Users\htb-student\Desktop\Company Data\HR
Successfully processed 1 files; Failed processing 0 files
```

Add NTFS Permissions for the HR Group:

```
$hrSubFolderPath = "C:\Users\htb-student\Desktop\Company Data\HR"

$acl = Get-Acl $hrSubFolderPath
$hrGroup = "HR"

$permissions = [System.Security.AccessControl.FileSystemRights]::Modify, `
[System.Security.AccessControl.FileSystemRights]::ReadAndExecute, `
[System.Security.AccessControl.FileSystemRights]::ListDirectory, `
[System.Security.AccessControl.FileSystemRights]::Read, `
[System.Security.AccessControl.FileSystemRights]::Write

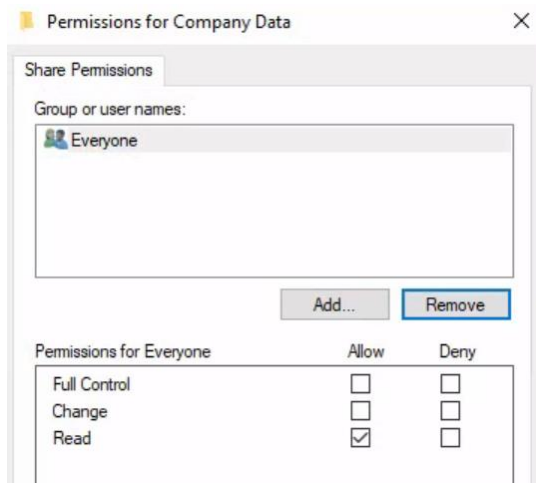
$accessRule = New-Object
System.Security.AccessControl.FileSystemAccessRule($hrGroup, $permissions,
"ContainerInherit, ObjectInherit", "None", "Allow")
$acl.SetAccessRule($accessRule)
Set-Acl $hrSubFolderPath $acl
```

```
PS C:\WINDOWS\system32> $hrSubFolderPath = "C:\Users\htb-student\Desktop\Company Data\HR"
>>
>> $acl = Get-Acl $hrSubFolderPath
>> $hrGroup = "HR"
>>
>> $permissions = [System.Security.AccessControl.FileSystemRights]::Modify, `
>> [System.Security.AccessControl.FileSystemRights]::ReadAndExecute, `
>> [System.Security.AccessControl.FileSystemRights]::ListDirectory, `
>> [System.Security.AccessControl.FileSystemRights]::Read, `
>> [System.Security.AccessControl.FileSystemRights]::Write
>>
>> $accessRule = New-Object System.Security.AccessControl.FileSystemAccessRule($hrGroup, $permissions, "
ContainerInherit, ObjectInherit", "None", "Allow")
>> $acl.SetAccessRule($accessRule)
>> Set-Acl $hrSubFolderPath $acl
PS C:\WINDOWS\system32>
```

Question: What is the name of the group that is present in the Company Data Share Permissions ACL by default?

Answer: Everyone

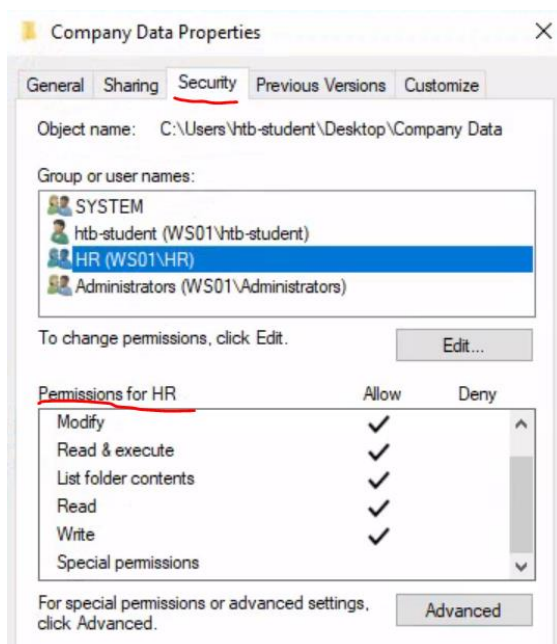
Method: here is a screenshot of 'Company Data' permissions before I changed anything in it:



Question: What is the name of the tab that allows you to configure NTFS permissions?

Answer: Security

Method: in Security tab, we will find the NTFS permissions control:



Question: What is the name of the service associated with Windows Update?

Answer: wuauserv

Method: we can use the powershell command:

```
Get-Service -DisplayName "Windows Update"
```

```
PS C:\WINDOWS\system32> Get-Service -DisplayName "Windows Update"

Status      Name      DisplayName
-----
Running     wuauserv   Windows Update
```

Question: List the SID associated with the user account Jim you created.

Answer: S-1-5-21-2614195641-1726409526-3792725429-1006

Method: we will use the powershell command:

```
Get-WmiObject -Class Win32_UserAccount -Filter "Name='Jim'" | Select-Object -ExpandProperty SID
```

```
PS C:\WINDOWS\system32> Get-WmiObject -Class Win32_UserAccount -Filter "Name='Jim'" | Select-Object -ExpandProperty SID
S-1-5-21-2614195641-1726409526-3792725429-1006
```

Question: List the SID associated with the HR security group you created.

Answer: S-1-5-21-2614195641-1726409526-3792725429-1007

Method: we will use the powershell command:

```
Get-WmiObject -Class Win32_Group -Filter "Name='HR'" | Select-Object -ExpandProperty SID
```

```
PS C:\WINDOWS\system32> Get-WmiObject -Class Win32_Group -Filter "Name='HR'" | Select-Object -ExpandProperty SID
S-1-5-21-2614195641-1726409526-3792725429-1007
```