



Eric Mwenda

Windows Fundamentals

<https://academy.hackthebox.com/achievement/596337/49>

The screenshot shows the HTB Academy interface. On the left is a sidebar with user information (coderic, Free, 60), navigation links (Dashboard, Exams, Modules, Paths, Academy x HTB Labs), and achievement sections (My Achievements, My Certificates, My Badges). The main content area is titled "WINDOWS FUNDAMENTALS" and features a large "Windows Fundamentals" logo. Below it, a summary states: "This module covers the fundamentals required to work comfortably with the Windows operating system." It has a 5-star rating and was created by mrb3n with co-authors LTNBOB. A "Start" button is visible. The bottom section, "Module Summary," explains the module's purpose and what it covers, listing "Windows Operating system structure" and "The Windows file system" as topics.

This is the command I shall use to reach the labs windows environment.
`xfreerdp /v:10.129.160.72 /u:htb-student /p:Academy_WinFun!`

The screenshot shows a terminal window titled "FreeRDP: 10.129.72.95". The session is connected to a Windows 10 desktop environment. The desktop background is blue with a white user icon placeholder. The taskbar at the bottom shows icons for File Explorer, Task View, and other applications. In the terminal window, the user has run the command "xfreerdp /v:10.129.160.72 /u:htb-student /p:Academy_WinFun!". The output shows the session establishing and authenticating, with logs indicating certificate verification failure due to self-signing and successful logins for "htb-student" and "Administrator". The terminal also shows the user navigating to their home directory and running "sudo su" to become root.

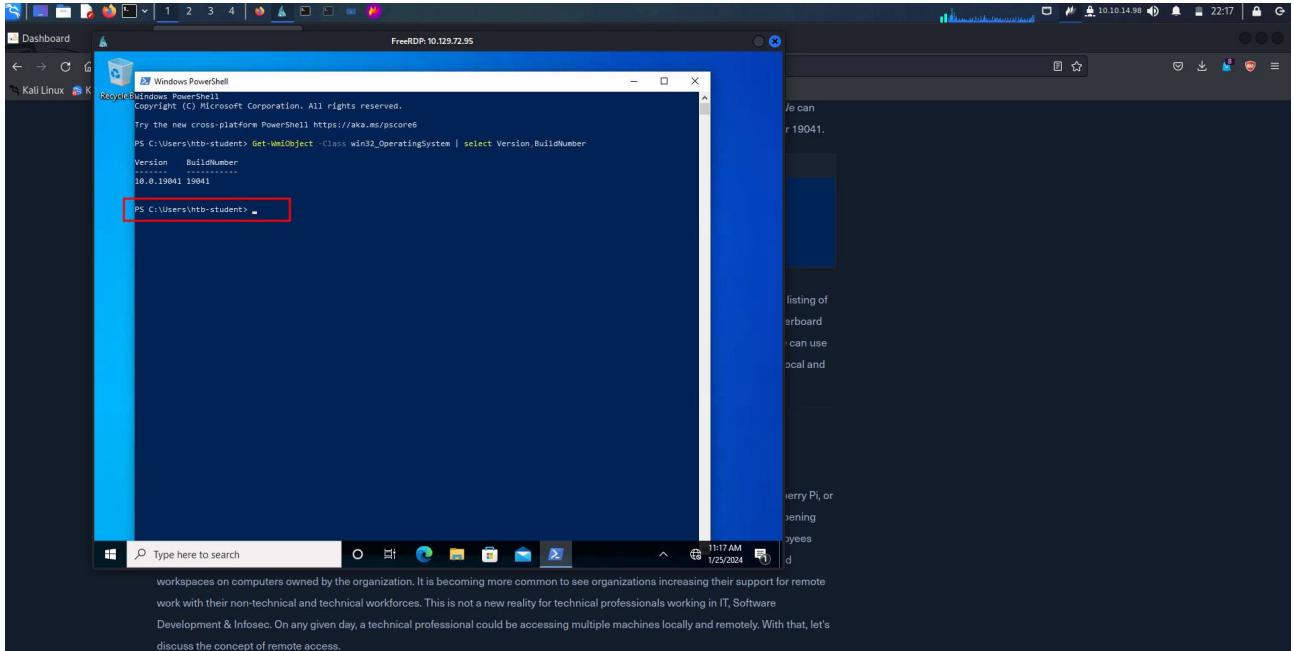
Introduction to Windows

What is the Build Number of the target workstation?

On the notes section we have an example of how to lock at the Build Number, so I wrote the exact command on power shell and here it is:-

Command used:- Get-WmiObject -Class win32_OperatingSystem | select Version,BuildNumber

ANS: 19041



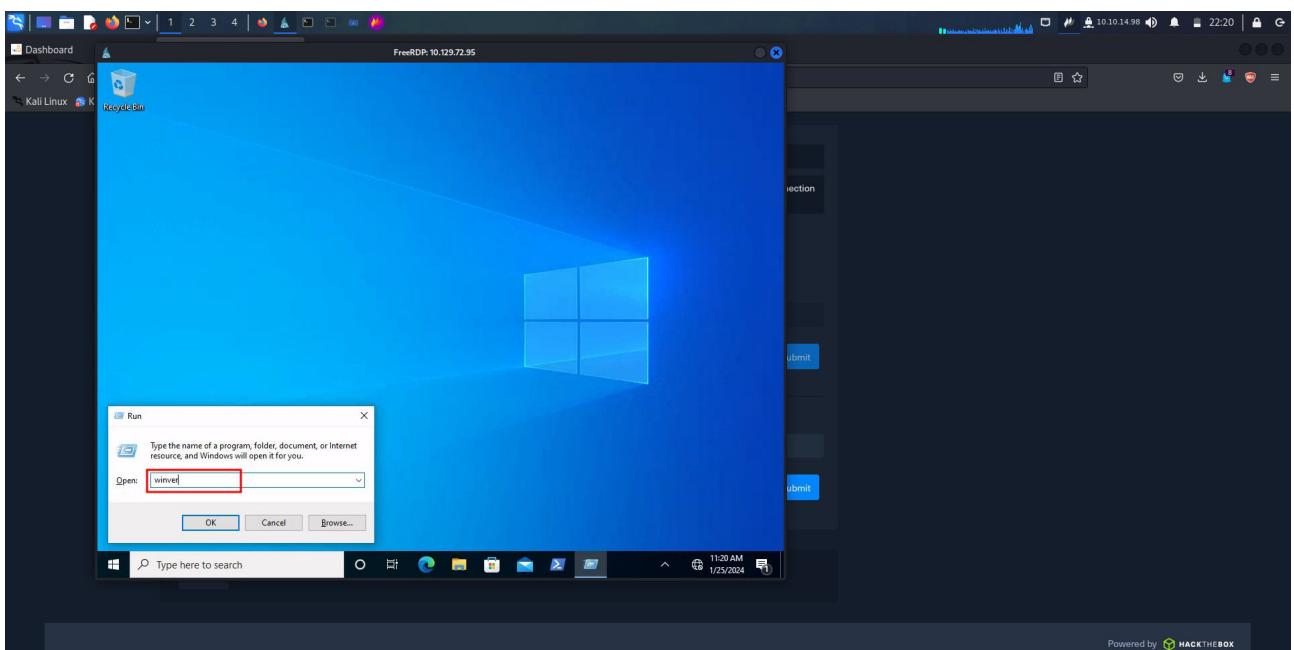
Which Windows NT version is installed on the workstation? (i.e. Windows X - case sensitive)

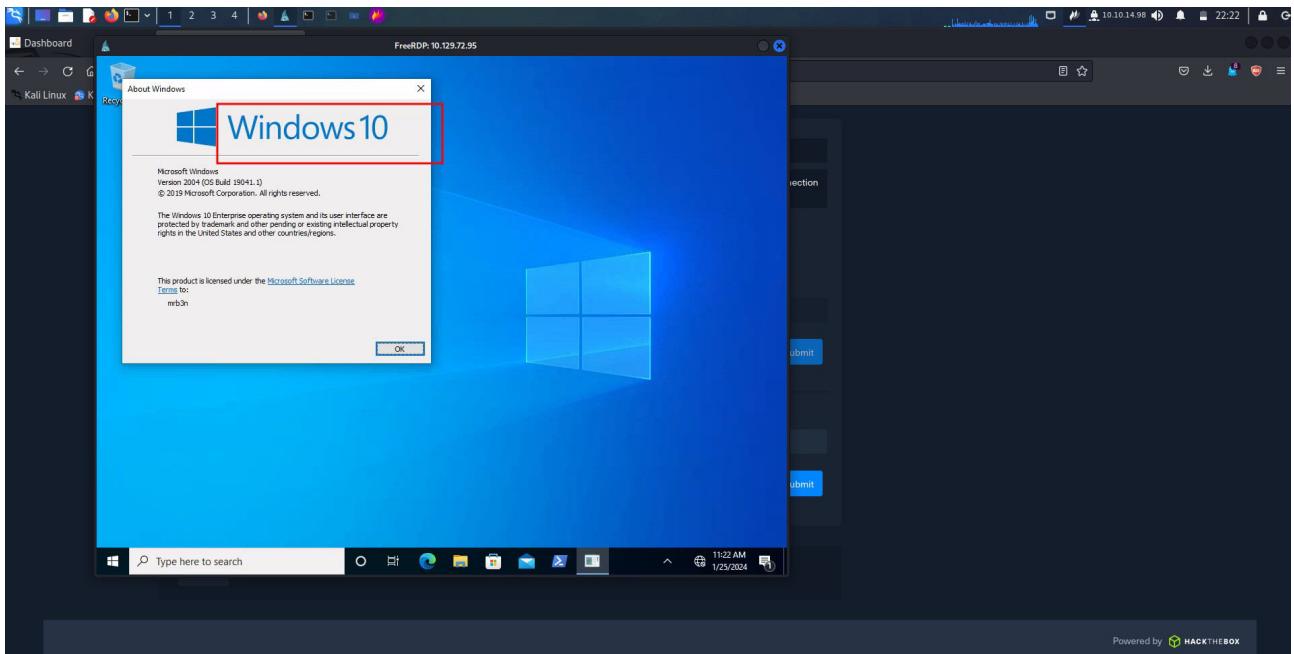
Command used:- **WIN + R** – this is a shortcut to opening the Run program in windows.

I typed “winver” on the search bar and hit Enter.

This command displayed the Windows NT version installed.

ANS: Windows 10





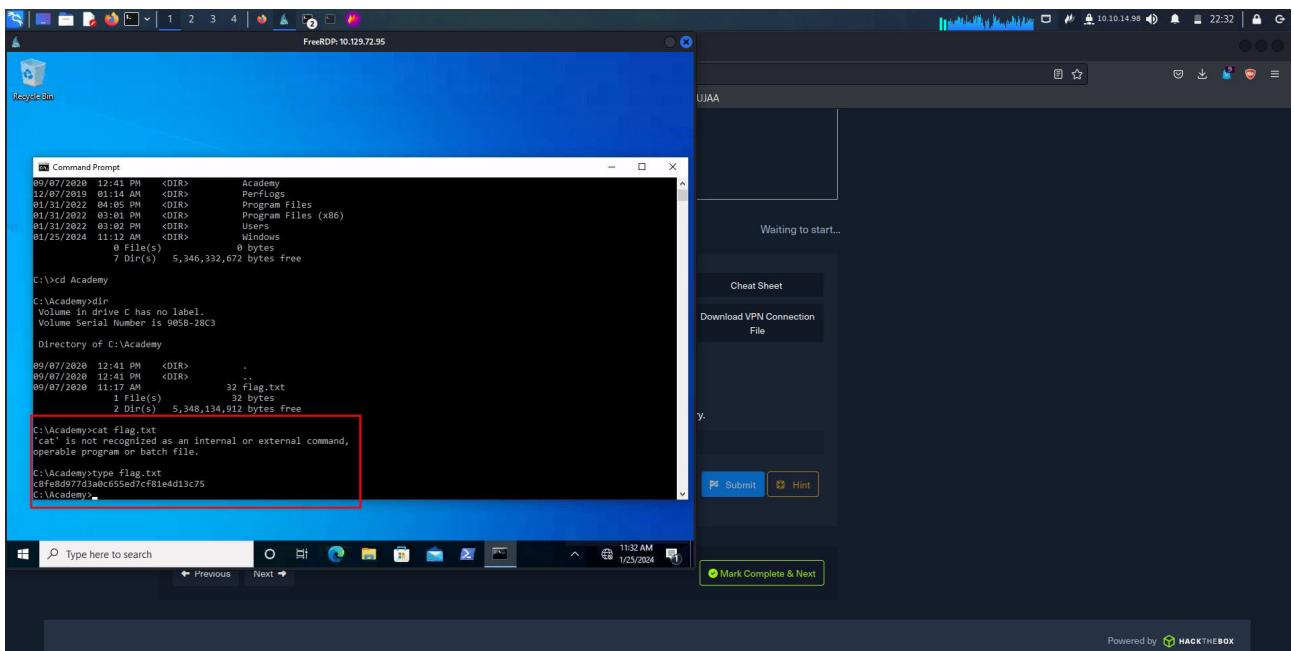
Operating System Structure

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

I already know that the file am looking for is in the C: drive and because am in a different folder I used "cd .." to move backwards till I arrive at Drive C:. Using dir I list all files in this folder, but there is no flag file. Of all available files, Academy folder seems to be appealing and on looking inside I found the "flag.txt" file, all I have to do is read the file contents.

I am tempted to use cat for Linux environments, which results to an error actually, since this is a windows environment. For windows, the correct command to read this file is "type"

Command Used: "type flag.txt". **ANS: c8fe8d977d3a0c655ed7cf81e4d13c75**

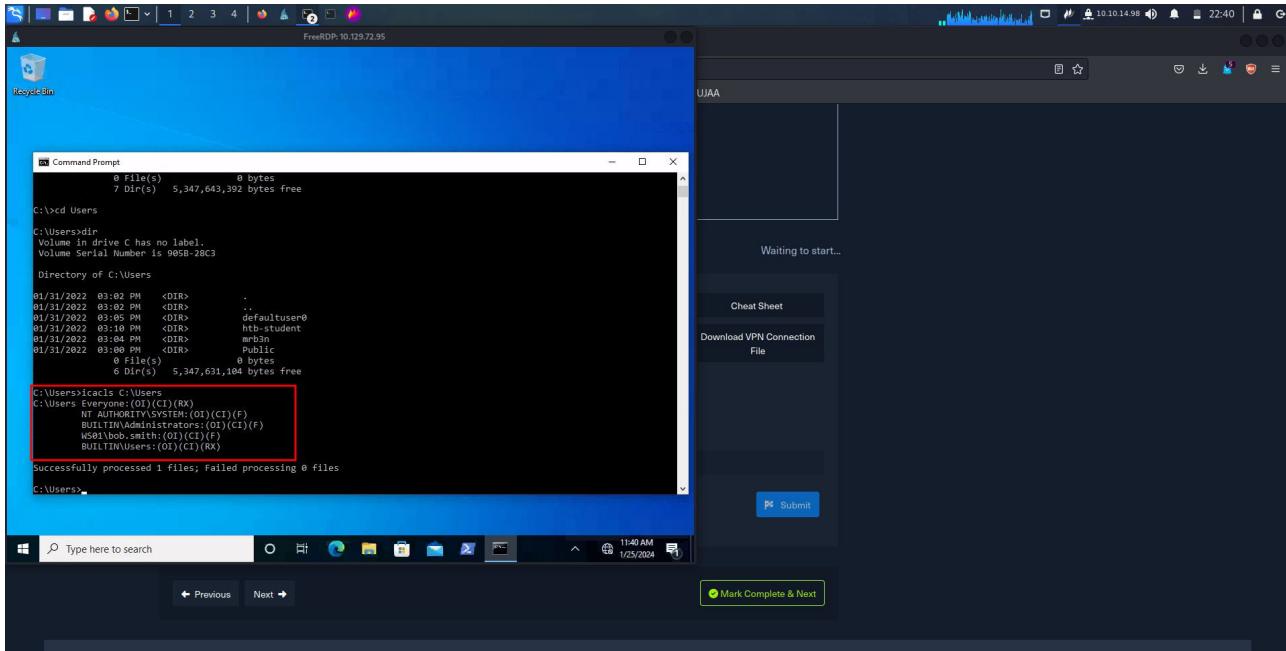


File System

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

First I will have to move into the users directory, then after that is to run command:- `icacls C:\Users` giving away the user in the system with full control.

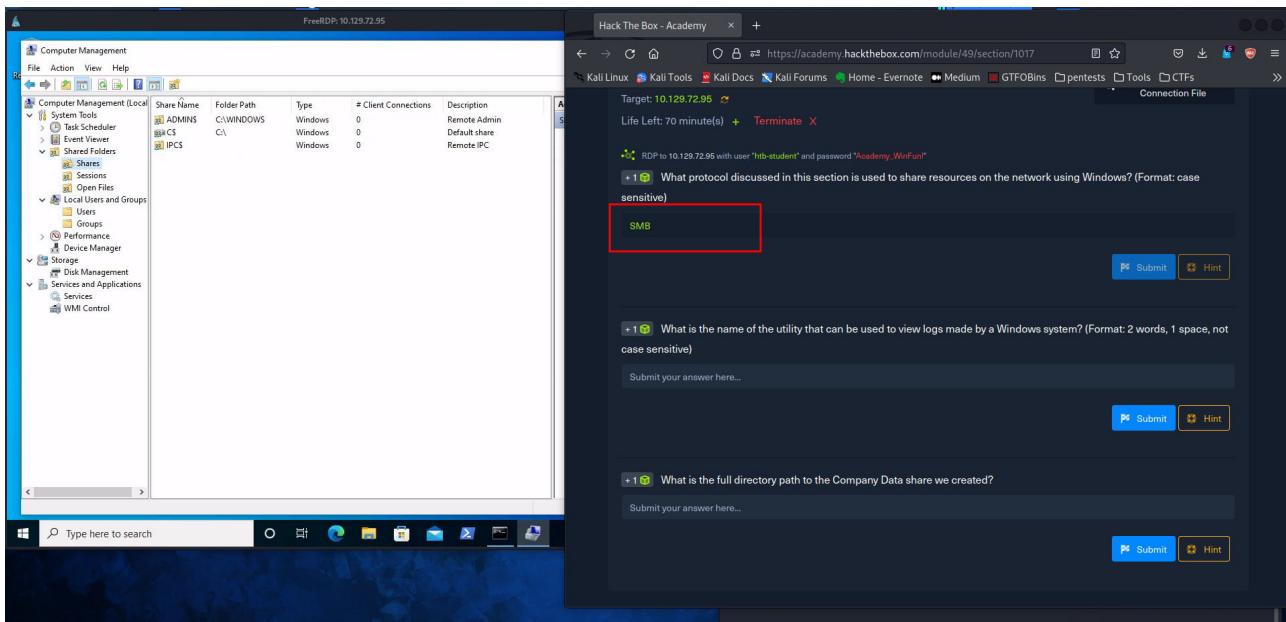
ANS: bob.smith



NTFS vs. Share Permissions

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

The answer is **SMB**



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)

The answer is: Event Viewer

The screenshot shows a dual-monitor setup. On the left monitor, a Windows desktop environment is visible with a taskbar at the bottom. On the right monitor, a browser window titled "Hack The Box - Academy" is open, displaying a challenge page for module 49 section 1017. The challenge asks: "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)". The answer "Event Viewer" is highlighted in red in the input field. The browser also shows other questions and a success message: "Success! Congratulations! You earned 1 cubes!".

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

Referencing the notes this was the path for the company data that was created.

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

The screenshot shows a dual-monitor setup. On the left monitor, a Windows desktop environment is visible with a taskbar at the bottom. On the right monitor, a browser window titled "Hack The Box - Academy" is open, displaying a challenge page for module 49 section 1017. The challenge asks: "What is the full directory path to the Company Data share we created?". The answer "C:\Users\htb-student\Desktop\Company Data" is highlighted in red in the input field. The browser also shows other questions and a note about net share command usage.

Computer Management

File Action View Help

System Tools

Task Scheduler

Share Name Folder Path Type # Client Connections Description

Administrator C:\WINDOWS Windows 0 Remote Admin Default share

Administrator C:\Windows 0 bytes

Administrator C:\ 0 Dir(s) 5,347,631,184 bytes free

C:\Users\htb-student> net share

Everyone (O:D|C|I|RX)

NT AUTHORITY\SYSTEM:(O|(C|(F))

BUILTIN\Administrators:(O|(C|(F))

WSB1bob.smith:(O|(C|(F))

BUILTIN\Users:(O|(C|(F))

Successfully processed 1 files; Failed processing 0 files

C:\Users\htb-student> netsh share

'netshare' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\htb-student> net share

Share name Resource Remark

.....

IPC\$ C:\ Default share Remote IPC

ADMIN\$ C:\WINDOWS Remote Admin

The command completed successfully.

C:\Users\htb-student>

FreeRDP: 10.129.72.95

Hack The Box - Academy

https://academy.hackthebox.com/module/49/section/1017

+1 What protocol discussed in this section is used to share resources on the network? (Format: case sensitive)

Success

Congratulations! You earned 1 cubes!

Submit Hint

+1 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)

Event Viewer

Submit Hint

+1 What is the full directory path to the Company Data share we created?

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

Submit Hint

Previous Next

Mark Complete & Next

Windows Services & Processes

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.

HINT: Its a pdf editing service.

Commands used:- `Get-Service | Where-Object {$_ .Name -like "*reader*"} |fl`

fl – Displays the property on a different line. From the hint given it is a pdf editing service, therefore it has to be Foxit Reader.

ANS: FoxitReaderUpdateService.exe

```
PS C:\Users\htb-student> Get-Service | Where-Object {$_ .Name -like "*reader*"} |fl
```

```
You must provide a value expression following the "-eq" operator.
At line:1 char:40
+ Get-Service | Where-Object {$_ .Name - like "*reader*"
+-----^
Unexpected token 'like' in expression or statement.
At line:1 char:40
+ Get-Service | Where-Object {$_ .Name - like "*reader*"} |fl
+-----^
ParentContainsErrorRecordException
+ FullyQualifiedErrorId : ExpectedValueExpression
```

```
PS C:\Users\htb-student> Get-Service | Where-Object {$_ .Name -like "*reader*"} |fl
```

Status	Name	DisplayName
Running	FoxitReaderUpdate...	Foxit Reader Update Service

```
PS C:\Users\htb-student> Get-Service | Where-Object {$_ .Name -like "*reader*"} |fl
```

```
You must provide a value expression following the "-eq" operator.
At line:1 char:40
+ Get-Service | Where-Object {$_ .Name - like "*reader*"} |fl
+-----^
You must provide a value expression following the "-eq" operator.
At line:1 char:40
+ Get-Service | Where-Object {$_ .Name - like "*reader*"} |fl
+-----^
Unexpected token 'like' in expression or statement.
+ CategoryInfo          : ParserError: (:) [], ParentContainsErrorRecordException
+ FullyQualifiedErrorId : ExpectedValueExpression
```

```
PS C:\Users\htb-student> Get-Service | Where-Object {$_ .Name -like "*reader*"} |fl
```

Name	DisplayName
FoxitReaderUpdateService	Foxit Reader Update Service

Waiting to start...

Cheat Sheet

Download VPN Connection File

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

htsService.exe

Submit Hint

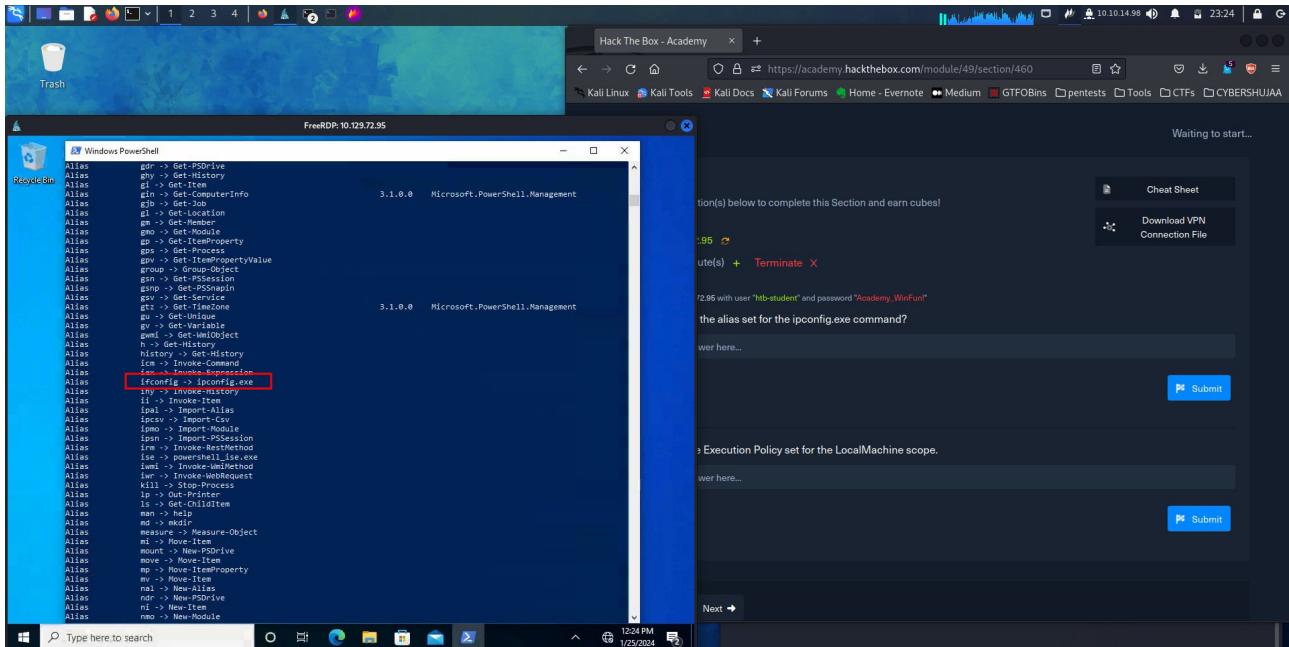
Mark Complete & Next

Interacting with the Windows Operating System

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

Command used:- get-allias

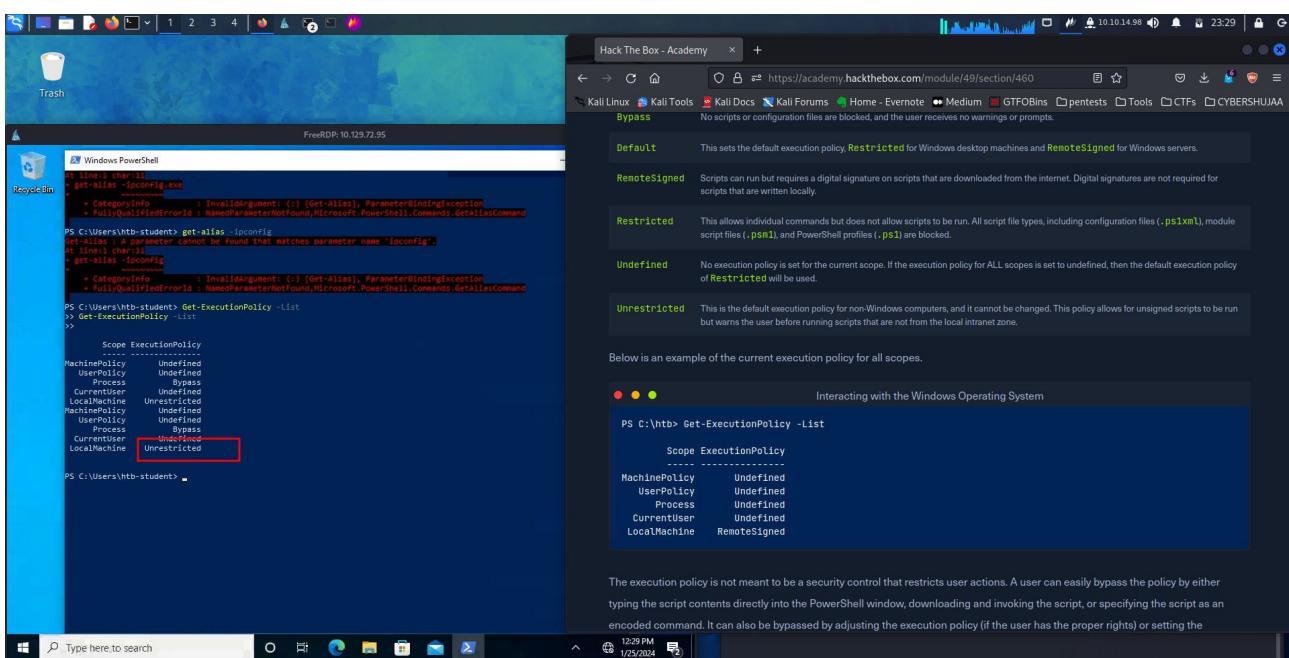
ANS: ifconfig



Find the Execution Policy set for the LocalMachine scope.

Command used:- Get-ExecutionPolicy -List

ANS: Unrestricted

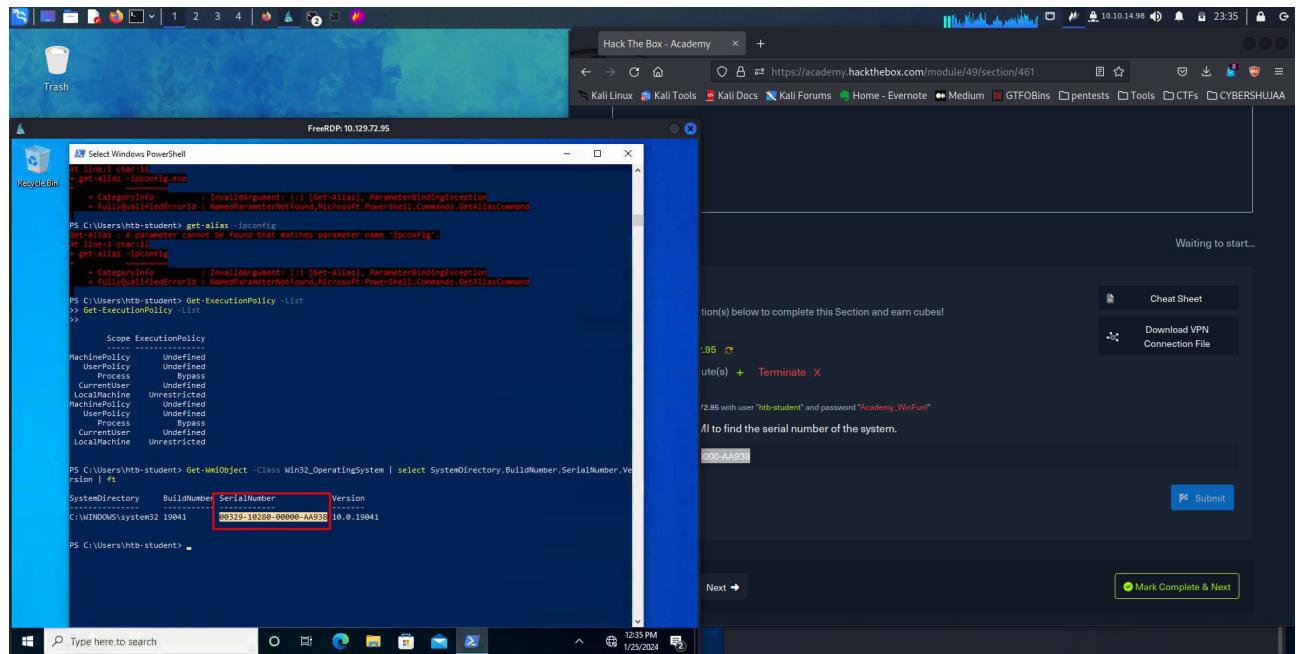


Windows Management Instrumentation (WMI)

I used WMI to find the serial number of the system.

Command used:- Get-WmiObject -Class Win32_OperatingSystem | select SystemDirectory, BuildNumber, SerialNumber, Version | ft

ANS: 00329-10280-00000-AA938

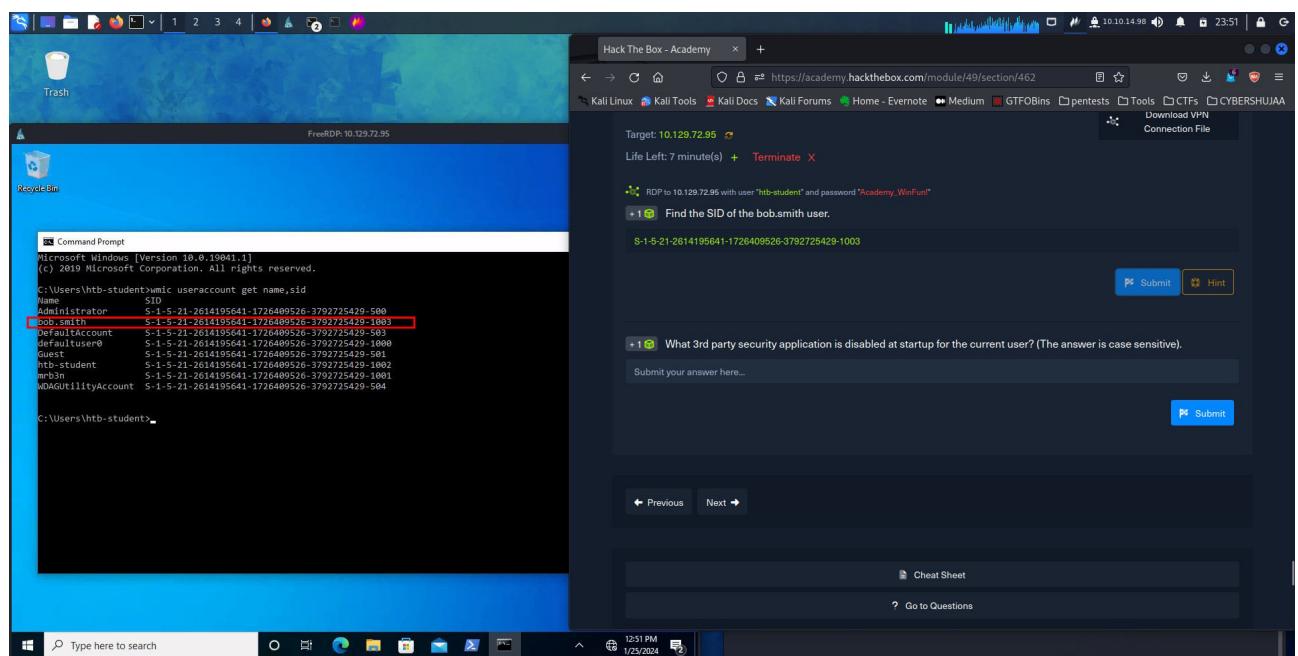


Windows Security

Find the SID of the bob.smith user.

Command used;- wmic useraccount get name,sid

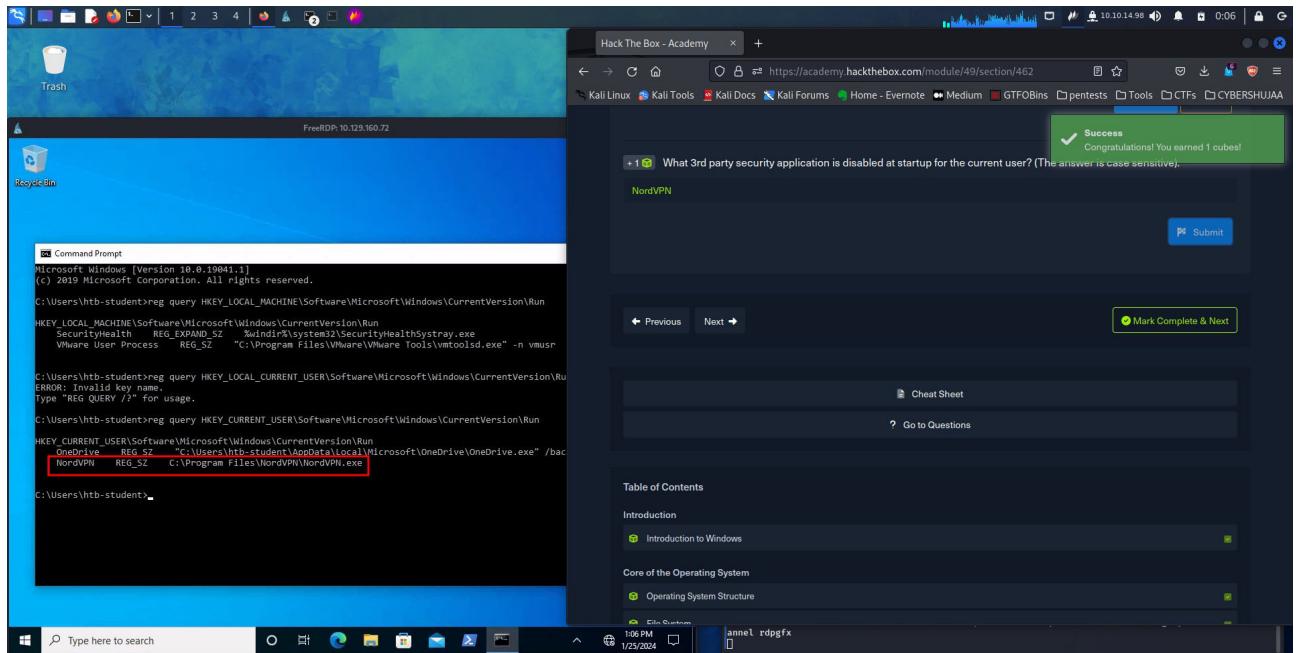
ANS: S-1-5-21-2614195641-1726409526-3792725429-1003



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

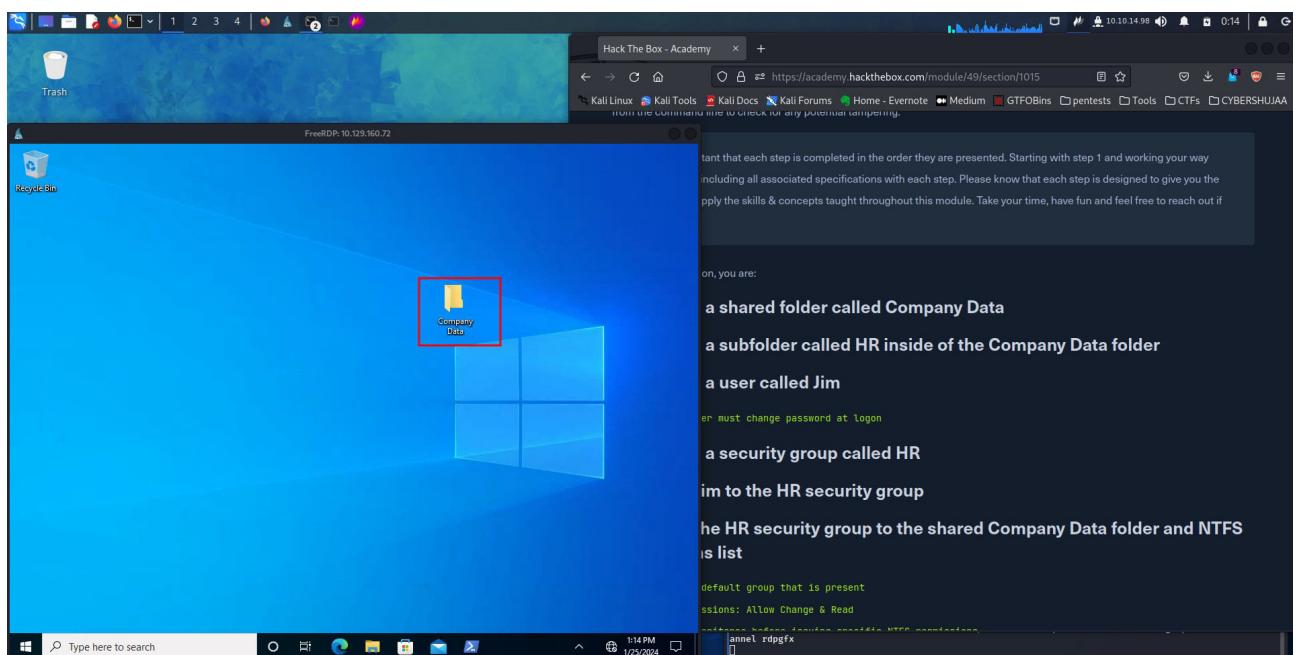
In the notes we searched for disabled at startup applications for the local machine, in this case we are looking for Current Users, Therefore using the command we used, what I needed to change was the user and there it was.

Command used:- reg query HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run. **ANS: NordVPN**

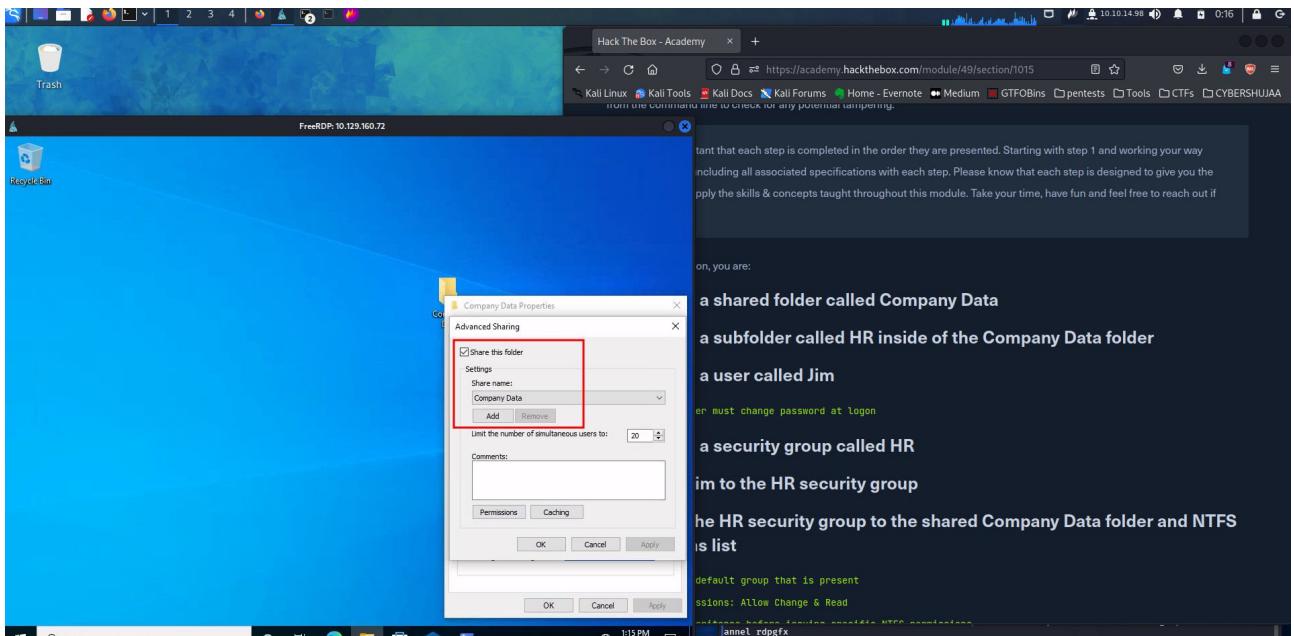


Skills Assessment - Windows Fundamentals

1. Creating a shared folder called Company Data. To do this, right click on the Desktop > New > Folder > Create a folder with the name Company Data.

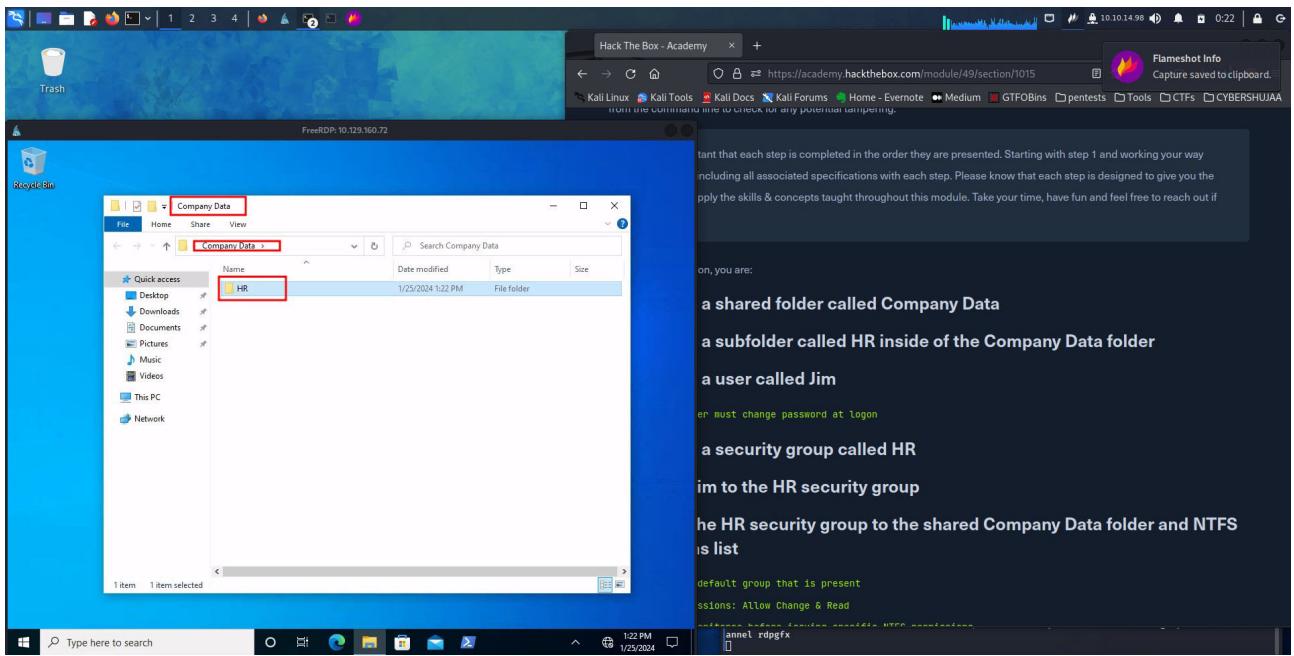


To share this folder right click on the folder > properties > Share Option > Check the share option > Apply > OK > close this widget.



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

To do this open the Company Data folder, Right click inside the folder > New > Folder, then call the newly created folder as HR.

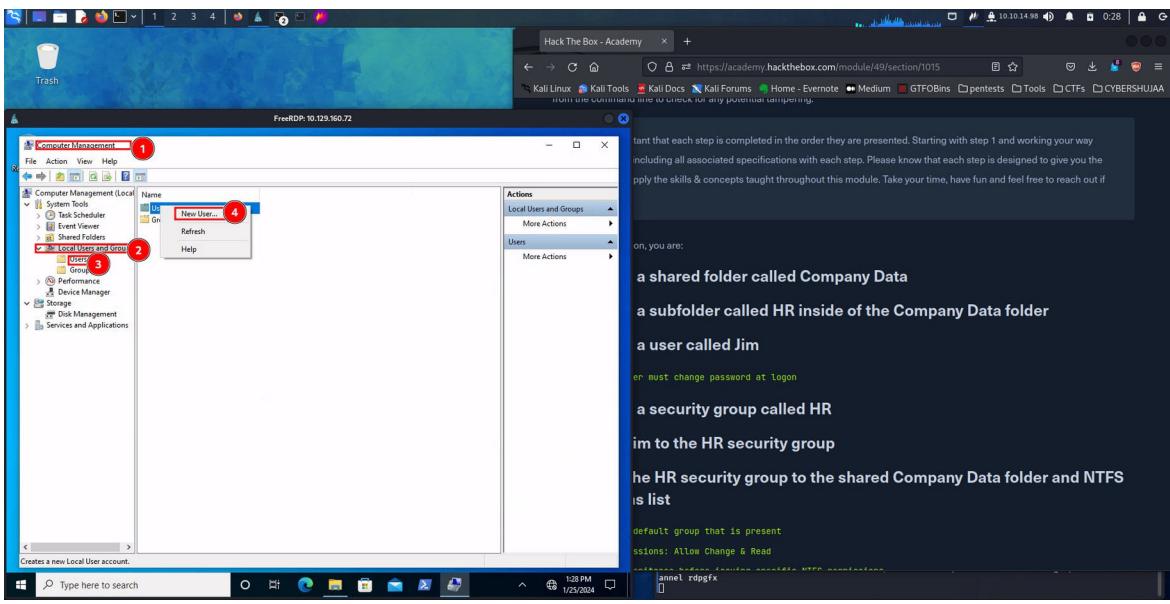


3. Creating a user called Jim. Uncheck: User must change password at logon

To do this go to Computer Management > Local Users and Groups > Users.

Right click on user.

- Username: Jim
- Full name: Jim
- Check user to change password at next logon
- Password: jim1234



tant that each step is completed in the order they are presented. Starting with step 1 and working your way including all associated specifications with each step. Please know that each step is designed to give you the apply the skills & concepts taught throughout this module. Take your time, have fun and feel free to reach out if

on, you are:

a shared folder called **Company Data**

a subfolder called **HR** inside of the **Company Data** folder

a user called **Jim**

er must change password at logon

a security group called **HR**

im to the **HR** security group

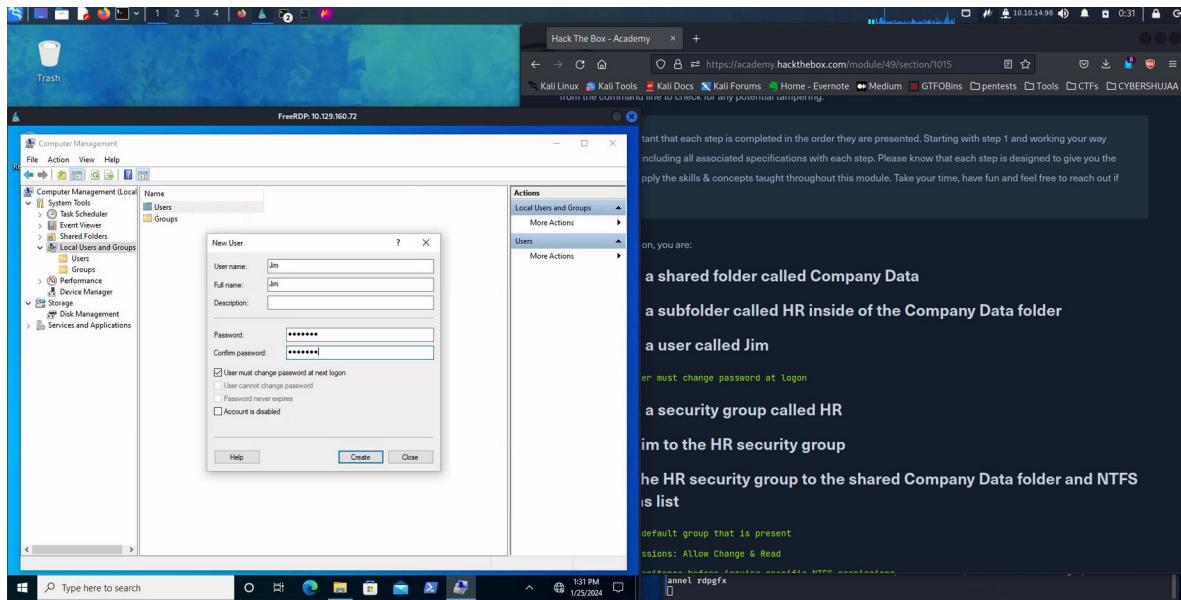
he **HR** security group to the shared **Company Data** folder and NTFS

is list

default group that is present

sessions: Allow Change & Read

annel rdpfx



tant that each step is completed in the order they are presented. Starting with step 1 and working your way including all associated specifications with each step. Please know that each step is designed to give you the apply the skills & concepts taught throughout this module. Take your time, have fun and feel free to reach out if

on, you are:

a shared folder called **Company Data**

a subfolder called **HR** inside of the **Company Data** folder

a user called **Jim**

er must change password at logon

a security group called **HR**

im to the **HR** security group

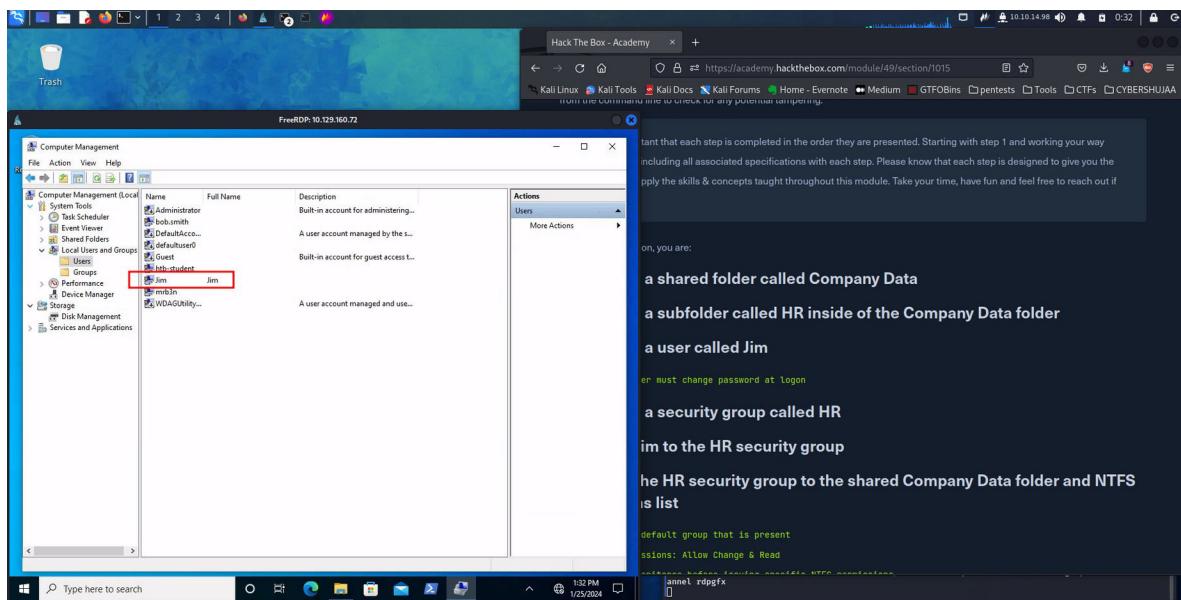
he **HR** security group to the shared **Company Data** folder and NTFS

is list

default group that is present

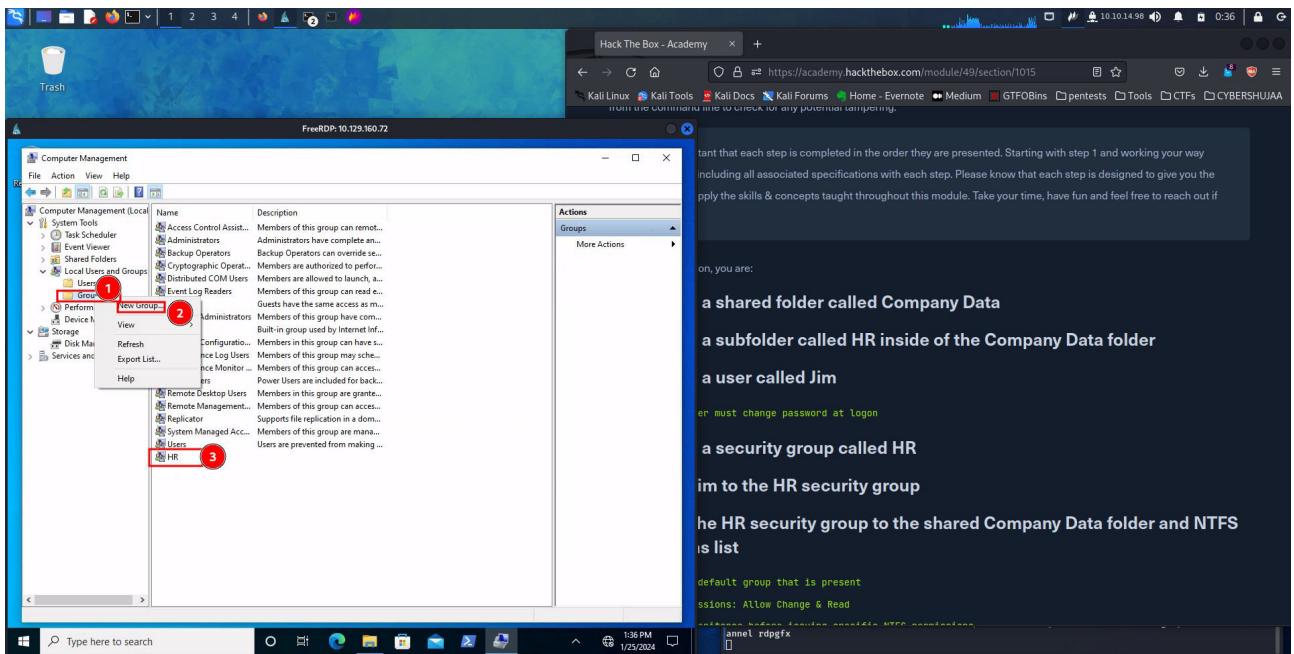
sessions: Allow Change & Read

annel rdpfx



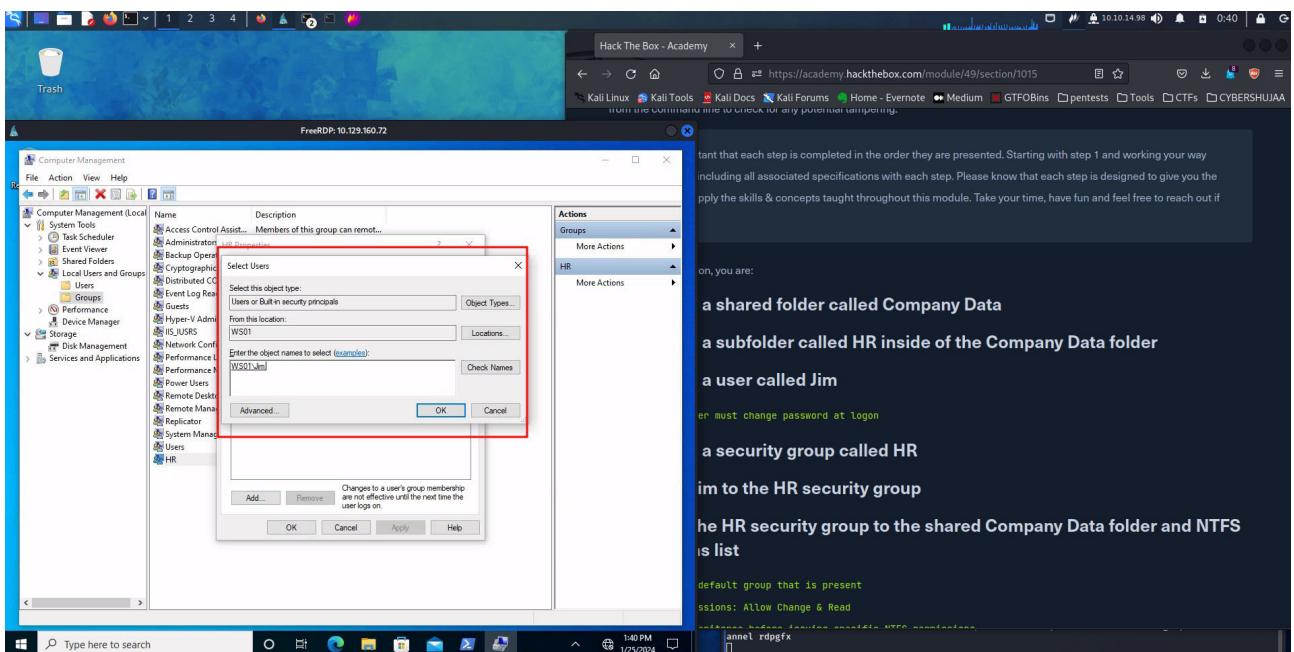
4. Creating a security group called HR

Click on Groups, Right Click then add new group (HR) then click on create button to finish.

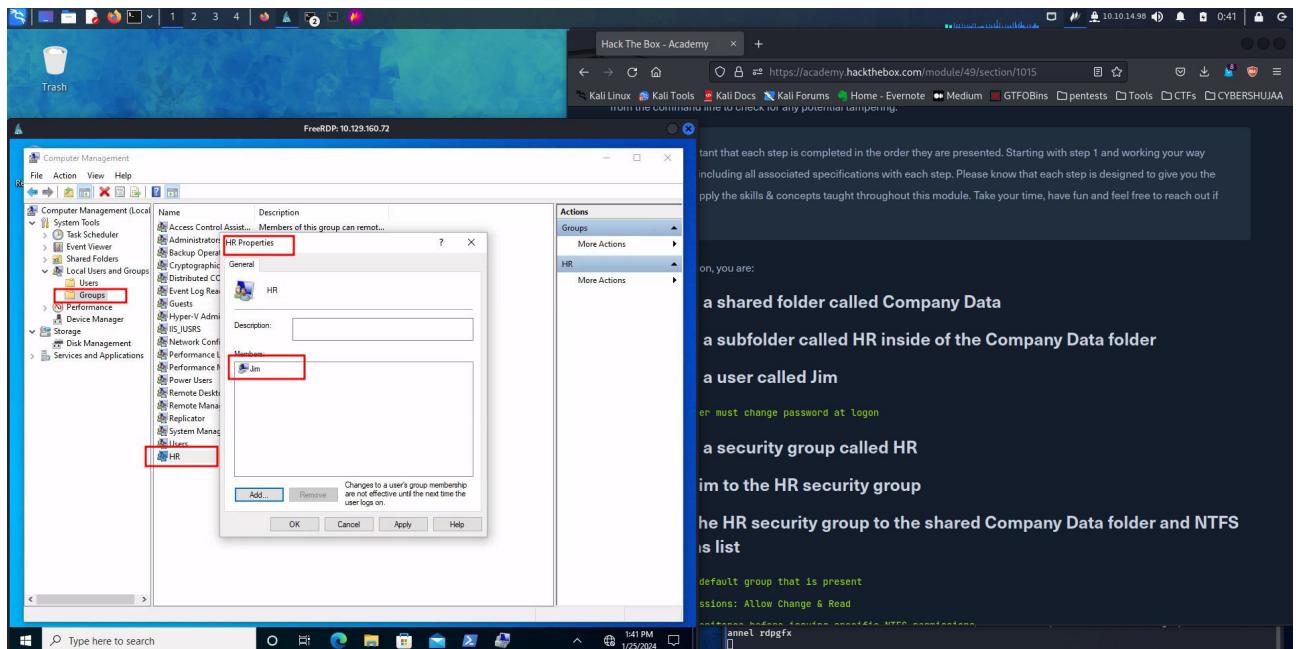


5. Adding Jim to the HR security group

To add Jim in the HR group, double click on Hr group > click on add, Type the name Jim > Check Names (Jim's name is auto selected) > click OK to add.



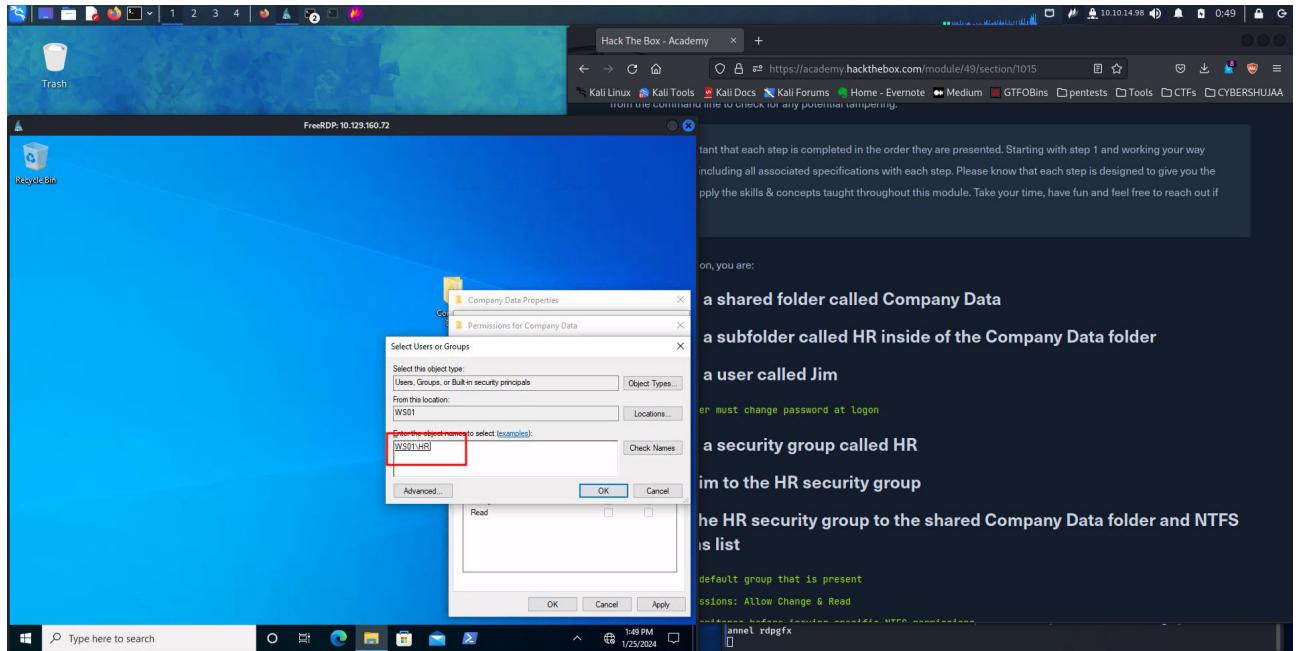
Click Apply > OK to finish adding Jim in HR Security group.



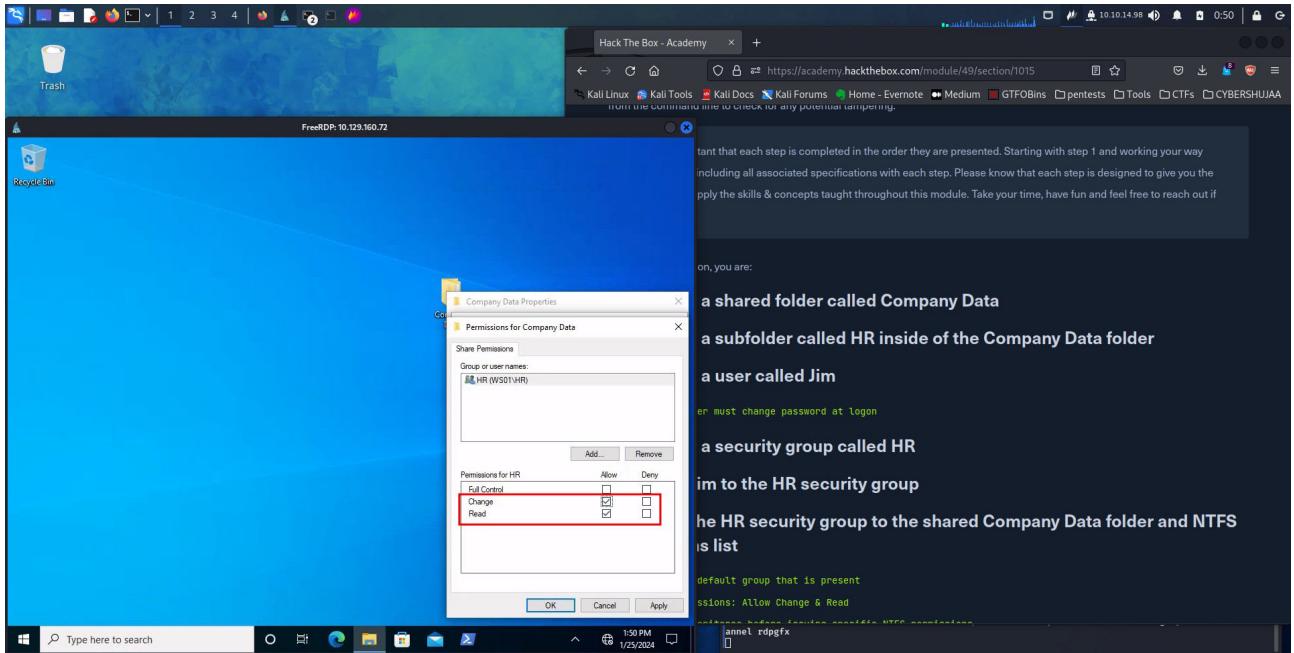
6. Adding the HR security group to the shared Company Data folder and NTFS permissions list

Remove the default group that is present – In this task what I need to do is to remove sharing to everyone and add HR

Properties > Sharing tab > Click Advanced sharing > permissions. From here I removed sharing for everyone and add HR group.

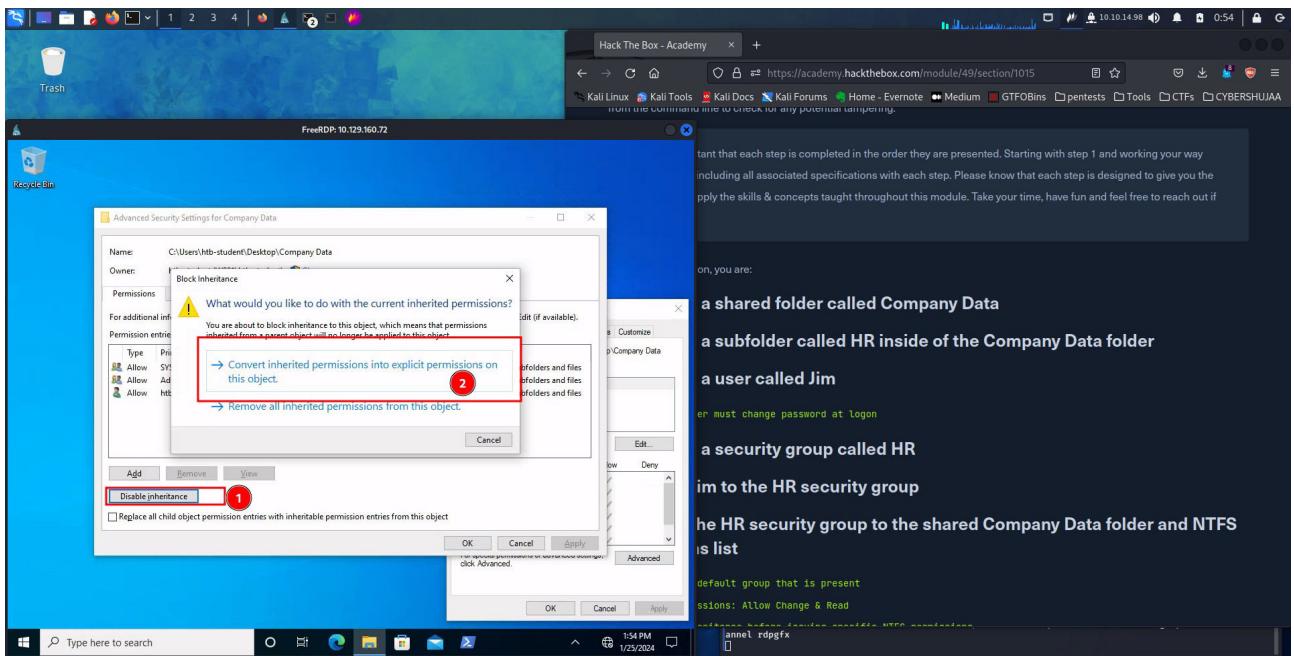


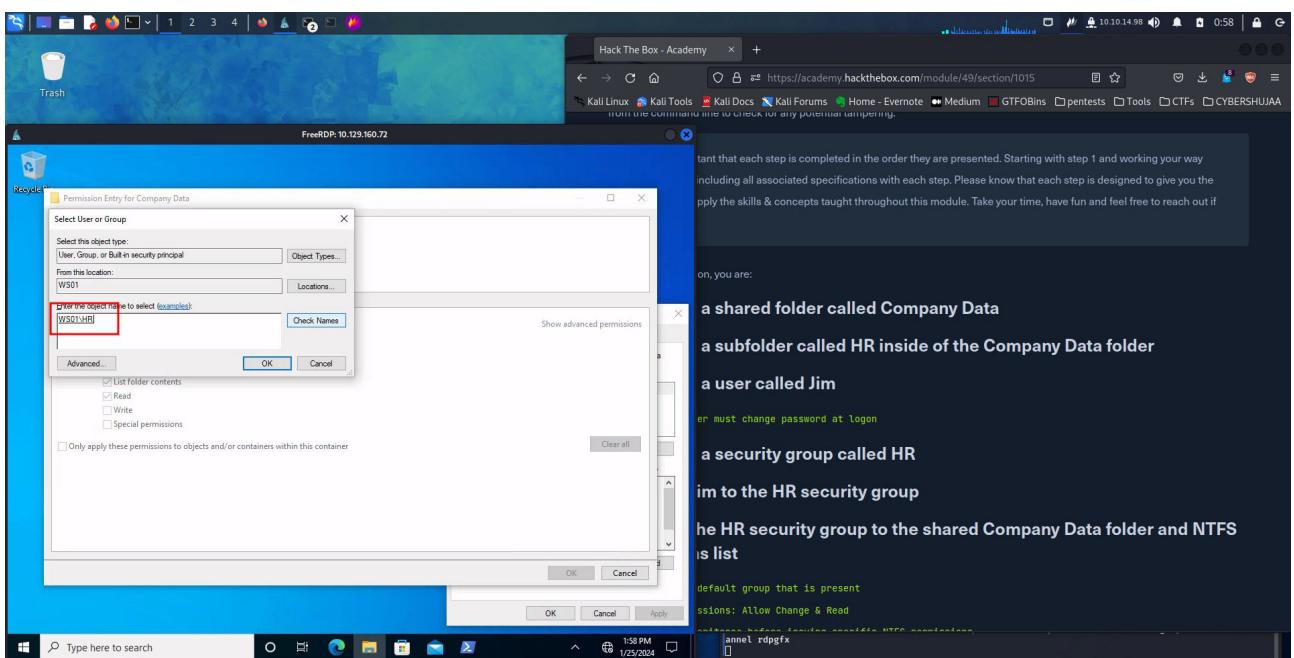
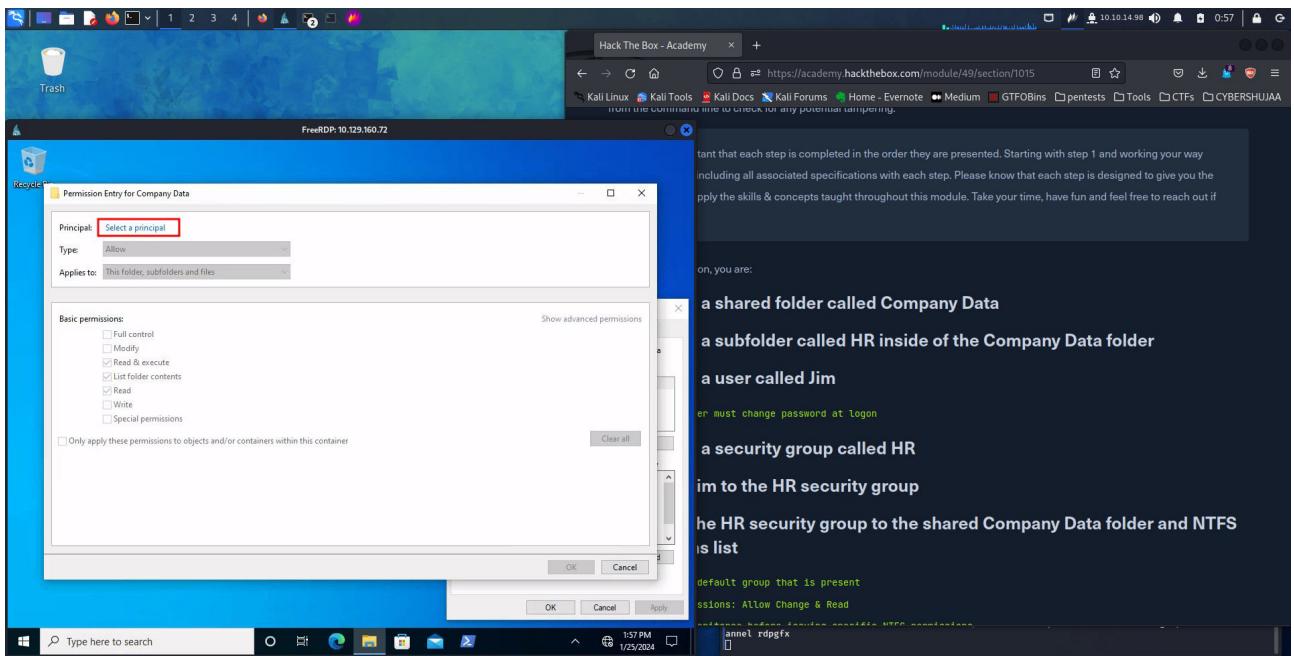
Share Permissions: Allow Change & Read



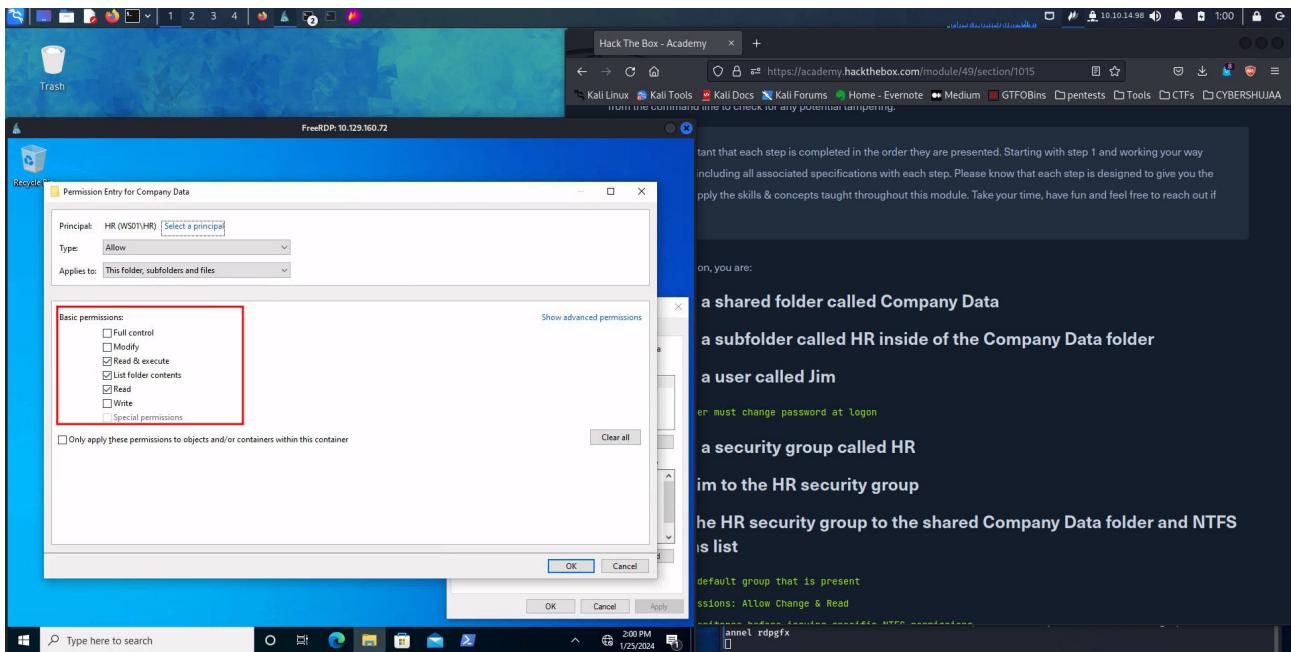
Disable Inheritance before issuing specific NTFS permissions

To do this I will right click on Company Data folder Click Properties > Security tab > Advanced > Disable Inheritance > Allow the prompt given > Click on Add > Select a principal > Add HR



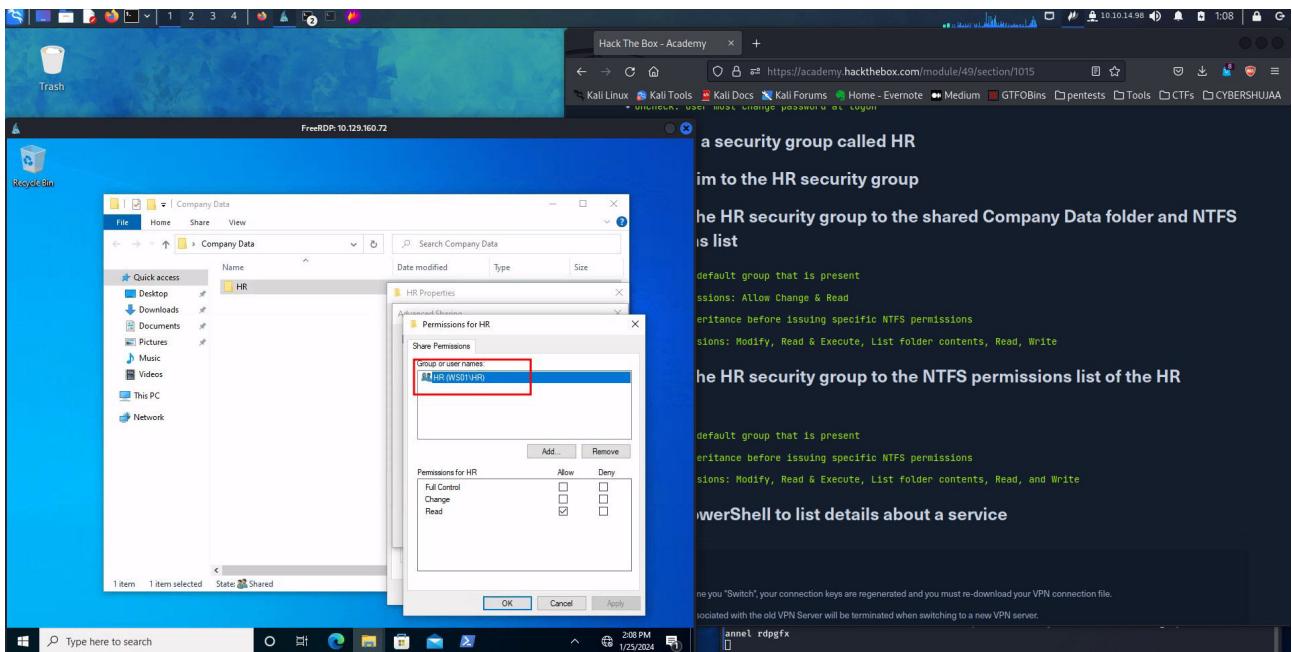


NTFS permissions: Modify, Read & Execute, List folder contents, Read, Write



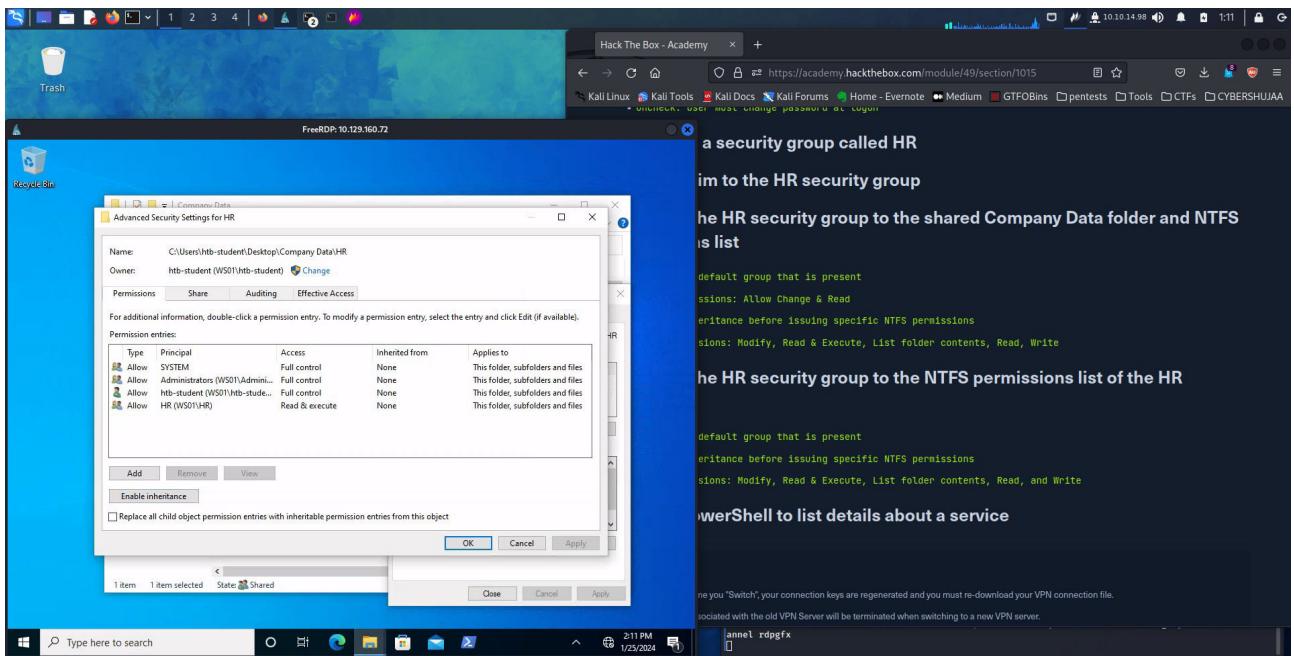
7. Adding the HR security group to the NTFS permissions list of the HR sub-folder Remove the default group that is present

To do this go to Company's Data folder > HR folder > Properties > Sharing tab > Advanced Sharing > Permissions check that the HR group is available and not default settings

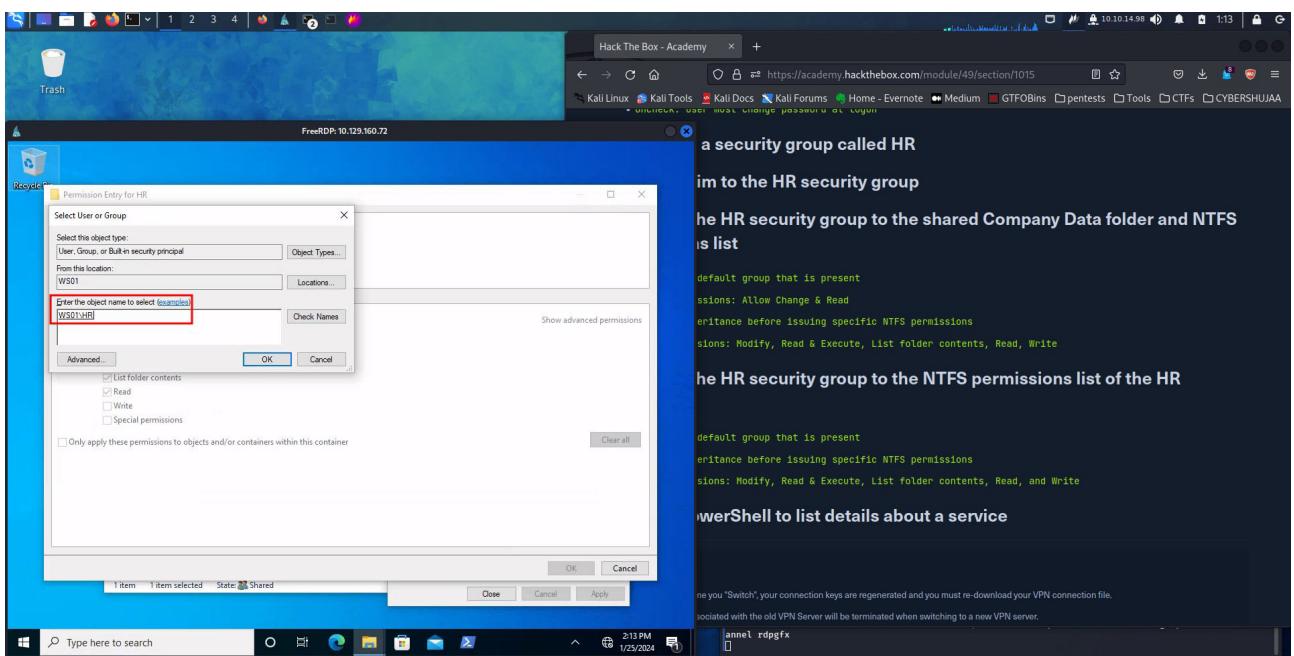


Disable Inheritance before issuing specific NTFS permissions

To do this go to HR folder > Properties > Security tab > Advanced > Disable Inheritance

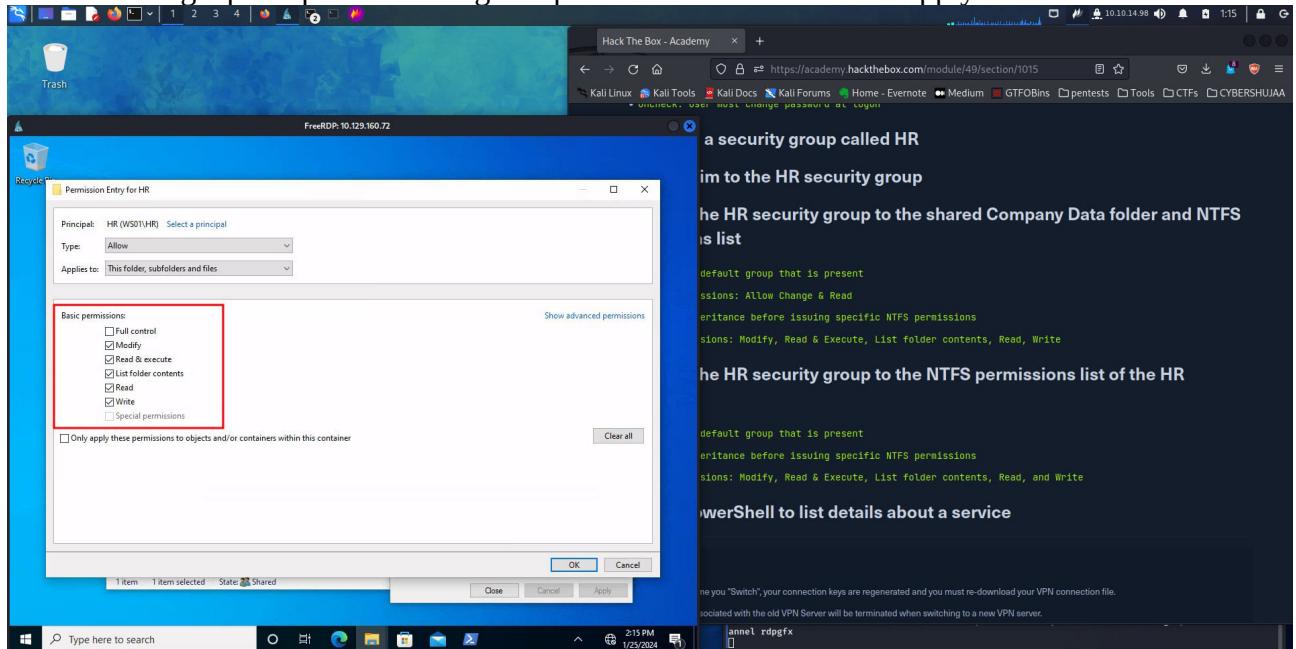


After Disabling Inheritance click on Add to select a principal add HR, click OK.



NTFS permissions: Modify, Read & Execute, List folder contents, Read, and Write

After selecting a principal allow the given permissions > Click OK > Apply > Close to exit



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

ANS: Everyone

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

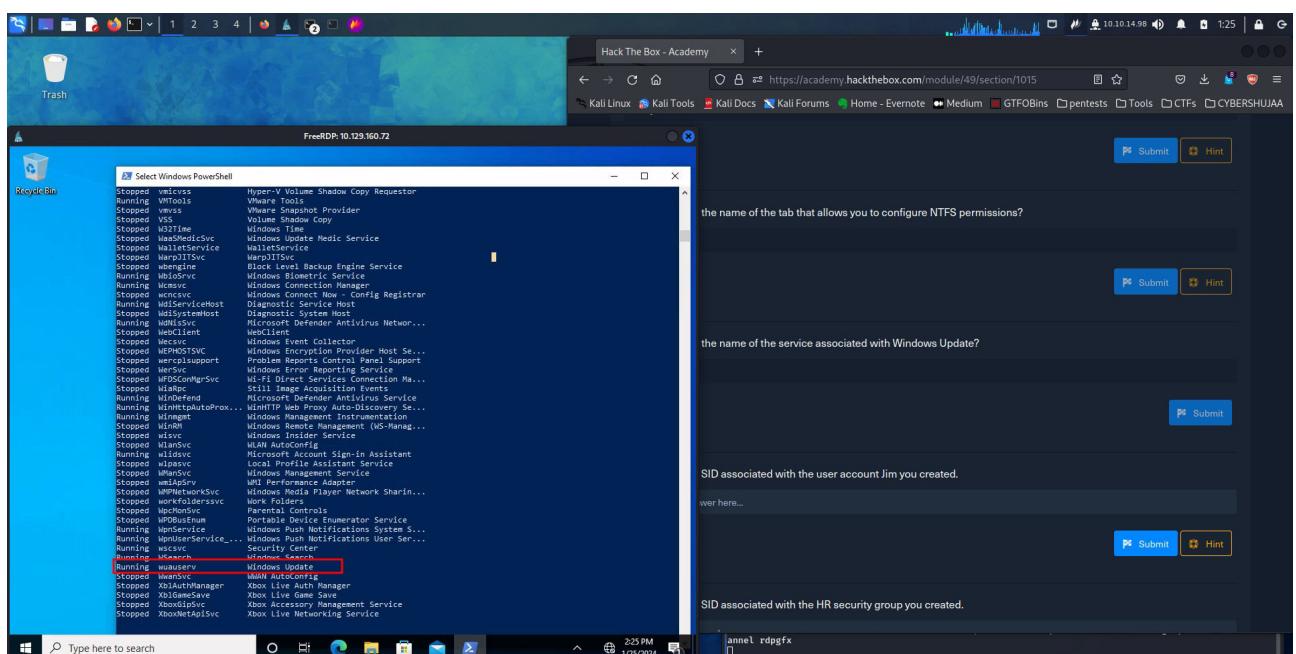
ANS: Security

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

Command used in power shell : Get-Service

This command lists all running commands, so we look for that service associated with windows update.

ANS: wuauserv



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

Command Used in Powershell:- `wmic useraccount get name,sid`

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

Windows PowerShell

```
PS C:\Users\htb-student> wmic useraccount get name,sid
Name          SID
Administrator S-1-5-21-2614195641-1726409526-3792725429-500
bob.smith    S-1-5-21-2614195641-1726409526-3792725429-1003
DefaultAccount S-1-5-21-2614195641-1726409526-3792725429-503
DefaultUser@0 S-1-5-21-2614195641-1726409526-3792725429-1000
Guest         S-1-5-21-2614195641-1726409526-3792725429-1001
htb-student   S-1-5-21-2614195641-1726409526-3792725429-1002
jim          S-1-5-21-2614195641-1726409526-3792725429-1006
mrB3n        S-1-5-21-2614195641-1726409526-3792725429-1005
WDAGUtilityAccount S-1-5-21-2614195641-1726409526-3792725429-504
PS C:\Users\htb-student>
```

Hack The Box - Academy

SID associated with the user account Jim you created.

J5641-1726409526-3792725429-1006

Submit Hint

SID associated with the HR security group you created.

Wer...

Submit Hint

Cheat Sheet

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

Command used in power shell:- `wmic group get name,sid`

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

Windows PowerShell

```
PS C:\Users\htb-student> wmic group get name,sid
Name          SID
Administrator S-1-5-21-2614195641-1726409526-3792725429-500
bob.smith    S-1-5-21-2614195641-1726409526-3792725429-1003
DefaultAccount S-1-5-21-2614195641-1726409526-3792725429-503
DefaultUser@0 S-1-5-21-2614195641-1726409526-3792725429-1000
Guest         S-1-5-21-2614195641-1726409526-3792725429-1001
htb-student   S-1-5-21-2614195641-1726409526-3792725429-1002
jim          S-1-5-21-2614195641-1726409526-3792725429-1006
mrB3n        S-1-5-21-2614195641-1726409526-3792725429-1005
WDAGUtilityAccount S-1-5-21-2614195641-1726409526-3792725429-504
PS C:\Users\htb-student> wmic group get name,sid
Name          SID
Administrators S-1-5-32-579
Backup Operators S-1-5-32-544
Cryptographic Operators S-1-5-32-551
Distributed COM Users S-1-5-32-569
Event Log Readers S-1-5-32-573
Guest          S-1-5-32-544
Hyper-V Administrators S-1-5-32-578
IIS_IUSC       S-1-5-32-580
Machine Configuration Operators S-1-5-32-556
Performance Log Users S-1-5-32-559
Performance Monitor Users S-1-5-32-558
Power Users    S-1-5-32-547
Remote Desktop Users S-1-5-32-555
Remote Management Users S-1-5-32-589
Replicator     S-1-5-32-552
System Managed Accounts Group S-1-5-32-581
Users          S-1-5-32-541
PS C:\Users\htb-student>
```

Hack The Box - Academy

✓ Success
Congratulations! You earned 1 cubes!

+1 List the SID associated with the user account Jim you created.

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

Submit Hint

+1 List the SID associated with the HR security group you created.

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

Submit Hint

Previous

Finish

Cheat Sheet

Conclusion

Windows has become a norm to most people especially to us doing penetration and testing we tend to love and prefer Linux but after this module, some of the practices that I have carried out have stirred me up to also want to learn how windows operating systems work especially from the fact that 70% of institutions use windows, I think its important to understand windows in the same manner I understand Linux.

In conclusion, this walk-through of Windows fundamentals in HTB Academy has provided essential concepts and practical skills for navigating and understanding the Windows operating system. From basic file operations to system configuration and security settings, I have gained valuable insights into the core elements of Windows environments. The hands-on exercises and step-by-step guidance have equipped me with the knowledge needed to troubleshoot common issues, manage user accounts, and secure a Windows system effectively.

I have enjoyed the task.

Thank You.